International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 05 | May 2021 www.irjet.net p-ISSN: 2395-0072

Blockchain-Enabled Internet of Things

SreenithRangaswamy[1], HarshaAlavalapati[2]

[1,2] UG Students, Department of Computer Science and Engineering, Srinivasa Ramanujan Institute of Technology, Andhra Pradesh, India

---

Abstract - *The Internet of Things (IoT) as a concept has crossed the chasm from slideware to reality with many industries implementing IoT solutions. It is a giant network with connected devices- that are embedded with sensors, software, and other technologies to exchange data over the internet without human intervention. over the next decades billions of devices will come online and the amount of data the internet has to handle will grow massively, Around 30 billion devices will constantly stream data, which requires IT Infrastructure that goes for beyond the existing capacities of the internet in terms of dealing the massive amounts of secure data. The IoT system provides several advantages, however, the bottlenecks created by existing cloud-based IoT systems and issues surrounding the security risks of centralized architecture introduce numerous issues involving a single point of failure, security, privacy, transparency, and data integrity. Integrating IoT with Blockchain will counter all these issues. A decentralized approach to IoT devices could solve many current issues by adopting a standardized peer-to-peer communications model to process the hundreds of billions of transactions between devices. This paper majorly discusses the Integration of IoT with Blockchain and how various features of blockchain technology can be implemented as a service for various IoT applications.*

Key Words: **Blockchain, Internet of Things, Blockchain with IoT, security, privacy, IoT and Blockchain Integration.**

1. INTRODUCTION

IoT has gained popularity in recent years and currently has applications in many different areas including healthcare, insurance, supply chain management, home automation, industrial automation, and infrastructure management. The benefits of IoT range from cost saving to enabling businesses to make vital decisions and thus improve performance based on the data provided by the IoT devices. . Raw data from millions of things (IoT devices) is analyzed and provides meaningful insights that help in making timely and efficient business decisions. The usual IoT model is based on a centralized paradigm where IoT devices usually connect to a cloud infrastructure or central servers to report and process the relevant data back. This centralization poses certain possibilities of exploitation including hacking and data theft. Moreover, not having control of personal data on a single, centralized service provider also increases the possibility of security and privacy issues. While there are methods and techniques to build a highly secure IoT ecosystem based on the normal IoT model, there are specific much more desirable benefits that blockchain can bring to IoT. A blockchain-based IoT model differs from the traditional IoT network paradigm. Blockchain for IoT can help to build trust, reduce costs, and accelerate transactions. Additionally, decentralization, which is at the very core of blockchain technology, can eliminate single points of failure in an IoT network. Also, the peer-to-peer communication model provided by blockchain can help to reduce costs because there is no need to build high-cost centralized data centers or implementation of complex public key infrastructure for security. Devices can communicate with each other directly or via routers. Blockchain enables things to communicate and transact with each other directly and with the availability of smart contracts, negotiation, and financial transactions can also occur directly between the devices instead of requiring an intermediary, authority, or human intervention. With the explosion of billions of devices connecting to the internet, it is hard to imagine that centralized infrastructures will be able to cope with the high demands of bandwidth, services, and availability without incurring the excessive expenditure. Blockchain-based IoT will be able to solve scalability, privacy, and reliability issues in the current IoT model.

1.1 An Overview of IoT

The Internet of Things (IoT) for short has recently gained much traction due to its potentialfor transforming business applications and everyday life. IoT can be defined as a network ofcomputationally intelligent physical objects (any object such as cars, fridges, industrial sensors, and so on) that are capable of connecting to the internet, sensing real-world events or environments, reacting to those events, collecting relevant data, and communicating it over the internet. This simple definition has enormous implications and has led to exciting concepts, such as wearable's, smart homes, smart grids, smart connected cars, and smart cities, that are all based on this basic concept of an IoT device. After dissecting the definition of IoT, four functions come to light as being performed by an IoT device. These include sensing, reacting, collecting, and communicating. All these functions are performed by using various components on the IoT device. Sensing is performed by sensors. Reacting or controlling is performed by actuators, the collection is a function of various sensors, and communication is performed by chips that provide network connectivity. One thing to note is that all these components are accessible and controllable via the internet in the IoT. An IoT device on its own is perhaps useful to some extent, but if it is part of a broader IoT ecosystem, it is more valuable. A typical IoT can consist of many physical

objects connecting and to acentralized cloud server. This is shown in the following diagram

Fig-1: a typical IoT Network

According to IoT Analytics,

In 2020, there are more IoT connections (e.g., connected cars, smart home devices, and connected industrial equipment) than there are non-IoT connections (smartphones, laptops, and computers). Of the 21.7 billion active connected devices worldwide, 11.7 billion (or 54%) will be IoT device connections at the end of 2020. By 2025, it is expected that there will be more than 30 billion IoT connections, almost 4 IoT devices per person on average.

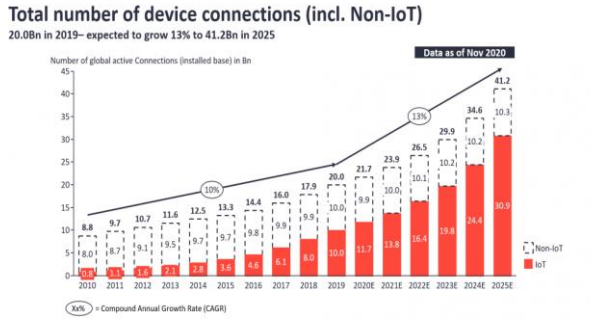

Fig-2: Internet of Things (IoT) growth from 2010 to 2025(expected)

Compared to an analysis performed in mid-2018, IoT Analytics has now raised its forecast for the number of connected IoT devices in 2025 (from 21.5 billion to 30.9 billion).

2. ARCHITECTURE OF IOT

IoT system uses the Centralized system which is currently the most widespread model for software applications. Centralized systems directly control the operation of the individual units and the flow of information from a single center. All individuals are directly dependent on the central power to send and receive information and to be commanded. The central network owner is a single point of contact for information sharing. In this approach, all the IoT devices and objects are connected, managed, and authenticated through a centralized server, which is typically a cloud server. Elements of IoT are spread across multiple layers, and various reference architectures exist that can be used to develop IoT systems. A five-layer model can be used to describe IoT, which contains a physical object layer, device layer, network layer, services layer, and application layer. Each layer or level is responsible for various functions and includes multiple components. These are shown in the below figure:

Application Layer Transportation, financial, insurance and many others
Management Layer Data processing, analytics, security management
Network Layer LAN, WAN, PAN, Routers
Device Layer Sensors , Actuators, smart devices
Physical Objects People, cars, homes etc. etc.

Fig-3: IoT five-layer model

All the above-mentioned layers are further examined in detail.

Physical object layer: These include any real-world physical objects. It includes people, animals, cars, trees, fridges, trains, factories, homes, and anything that is required to be monitored andcontrolled can be connected to the IoT.

Device layer: This layer contains things that make up the IoT such as sensors, transducers, actuators, smartphones, smart devices, and Radio-Frequency Identification (RFID) tags. There can be many categories of sensors such as body sensors, home sensors, and environmental sensors based on the type of work they perform. This layer is the core of an IoT ecosystem where various sensors are used to sense real-world environments. This layer includes sensors that can monitor temperature, humidity, liquid flow, chemicals, air, pressure, and much more. Usually, an Analog to Digital Converter (ADC) is required on a device to turn the real-world analog signal into a digital signal that a microprocessor can understand. Actuators in this layer provide the means to enable control of external environments, these components also require digital to analog converters to convert a digital signal into analog.

Network layer: This layer is composed of various network devices that are used to provide Internet connectivity between devices and to the cloud or servers that are part of

the IoT ecosystem. These devices can include gateways, routers, hubs, and switches. This layer can include twotypes of communication.

First, there are horizontal means of communication, which include radio, Bluetooth, Wi-Fi, Ethernet, LAN, ZigBee, and PAN, and can be used to provide communication between IoT devices. Second, we have communication to the next layer, which is usually through the internet and provides communication between machines and people or other upper layers. The first layer can optionally be included in the device layer as it physically is residing on the device layer where devices can communicate with each other at the same layer.

Management layer: This layer provides the management layer for the IoT ecosystem. This includes platforms that enable the processing of data gathered from the IoT devices and turn that into meaningful insights. Also, device management, security management, and data flow management are included in this layer. It also manages communication between the device and application layers.

Application layer: This layer includes applications running on top of the IoT network. This layer can consist of many applications depending on the requirements such as transportation, healthcare, financial, insurance, or supply chain management. This list, of course, is not an exhaustive list by any stretch of the imagination; there is a myriad of IoT applications that can fall into this layer. The existing centralized model of IoT system provides several advantages to connect and communicate with a wide variety of devices that are managed by the central server. On the other hand, it is said that there are many challenges to the adoption of IoT at scale. These are mainly because of the design of today's internet and the intermittent connectivity of today's networks. Several aspects apply to IoT systems that affect their architecture and implementation, as follows:

Table -1: Summary of challenges in IoT centralized model

Challenge	Description
Scalability	Scale for IoT system applies in terms of the numbers of sensors and actuators connected to the system, in terms of the networks which connect them, in terms of the amount of data associated with the system and its speed of movement, and also in terms of the amount of processing power required.
Big Data	Many more advanced IoT systems depend on the analysis of vast quantities of data. The ability to mine existing data for new insights and the need to combine different datasets in novel ways are characteristics likely to be part of an IoT system.
Real-Time	IoT systems often function in real-time; data flows in continually about events in progress and there can be a need to produce timely responses to that stream of events. There is a parallel need to ensure that corrupted data is detected and not used whether introduced by faulty sensors or malicious action since the use of corrupted data could cause harm and damage to humans, equipment, and the environment.
Security and Privacy	The question of the security and trustworthiness of distributed heterogeneous IoT systems is a hard problem whose solutions must scale and evolve with the systems. Data protection is necessary, including significant privacy concerns regarding data that relate to individuals. Gaining assurance that these systems are safe, secure, and resilient and uphold their stakeholder's expectations about privacy is especially challenging.
Compliance	Providing confidence about the operation of these IoT systems is necessary both due to the regulations of specific industries, sectors, and verticals and also the norms and expectations of the stakeholders of the IoT systems.

3. BLOCKCHAIN TECHNOLOGY

Blockchain is a peer-to-peer, distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.

Block is among the primary components of the blockchain. Each block comprises a set of transactions. The blocks were chained together by storing a unique hash value of the preceding block in the existing block. This link blocks together like a chain. The hash function is used to validate the data integrity of the content of each block. The hash function is a mathematical problem that minors need to crack to find a block. The reason to use the hash function is that it is collision-free in which it is very hard to create two identical hashes for two different digital data. So, assigning a hash value for each block can serve as a way to identify the block and also validate its contents.

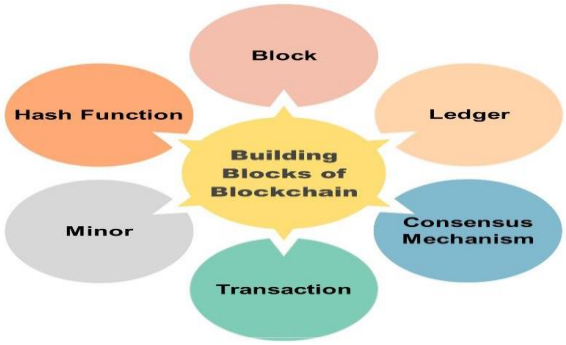

Fig-5: Building Blocks of a Blockchain

A transaction is the smallest unit of process or operation in which a set of transactions are combined and stored in a block. A certain transaction cannot be added to the block unless the majority of the participating nodes in the blockchain network record their consent. The size of a transaction is important for minors as small transactions require less power and are easier to validate. Minors are computers/agents that attempt to solve a complex mathematical problem (typically, a form of hash functions) to explore a new block. Discovering a new block is started by broadcasting new transactions to all nodes, and then each node combines a set of transactions into a block and operates to discover the block's proof-of-work. If a node discovers a block, then the block will be broadcasted to all the nodes to be verified

3.1 Key elements of Blockchain

Peer-to-Peer

The term peer-to-peer means that there is no central controller in the network, and all participants talk to each other directly. This property allows for cash transactions to be exchanged directly among peers without third-party involvement.

Distributed ledger technology

All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.

Cryptographically-secure

In a blockchain, the ledger is cryptographically secure, which means that cryptography has been used to provide security services that make this ledger secure against tampering and misuse. These services include non-repudiation, data integrity, and data origin authentication.

Immutable records

No participant can change or tamper with a transaction after it's been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.

Smart contracts

To speed transactions, a set of rules — called a smart contract — is stored on the blockchain and executed automatically. A smart contract is a piece of code stored on the blockchain that enables the automation of complex business logic.

3.2 Benefits of Blockchain

- **Decentralization**: This is a core concept and benefit of the blockchain. There is no need for a trusted third party or intermediary to validate transactions; instead, a consensus mechanism is used to agree on the validity of transactions.
- **Transparency and trust**: Because blockchains are shared and everyone can see what is on the blockchain, this allows the system to be transparent. As a result, trust is established. This is more relevant in scenarios such as the disbursement of funds or benefits where personal discretion about selecting beneficiaries needs to be restricted.
- **Immutability**: Once the data has been written to the blockchain, it is extremelydifficult to change it back. It is not genuinely immutable, but because changing data is so challenging and nearly impossible; this is seen as a benefit to maintaining an immutable ledger of transactions.
- **High availability**: As the system is based on thousands of nodes in a peer-to-peernetwork, and the data is replicated and updated on every node, the system becomes highly available. Even if some nodes leave the network or become inaccessible, the network as a whole continues to work, thus making it highly available. This redundancy results in high availability.
- **Highly secure**: All transactions on the blockchain are cryptographically secured and thus provide network integrity.
- **Faster dealings**: Blockchain can play a vital role by enabling the quick settlement oftrades. Blockchain does not require a lengthy process of verification, reconciliation, and clearance because a single version of agreed-upon data is already available on a shared ledger between financial organizations.
- **Cost-saving**: As no trusted third party or clearinghouse is required in the blockchain model, this can massively eliminate overhead costs in the form of the fees which are paid to parties.

4. BLOCKCHAIN INCLUSION IN IOT ARCHITECTURE

The aforementioned five-layer IoT model can be adapted to a blockchain-based model by adding a blockchain layer on top of the network layer. This layer will run smart contracts, and provide security, privacy, integrity, autonomy, scalability, and decentralization services to the IoT ecosystem. The management layer, in this case, can consist of only software related to analytics and processing, and security and control can be moved to the blockchain layer. This model can be visualized in the following diagram:

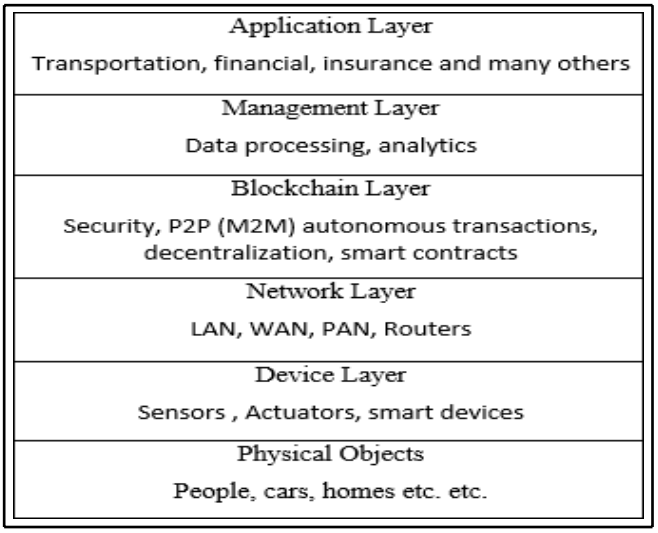

Fig-5: Blockchain-based IoT Model

In this model, other layers would perhaps remain the same, but an additional blockchain layer will be introduced as middleware between all participants of the IoT network. It can also be visualized as a peer-to-peer IoT network after abstracting away all the layers mentioned earlier. This model is shown in the following diagram where all devices are communicating and negotiating with each other without a central command and control entity:

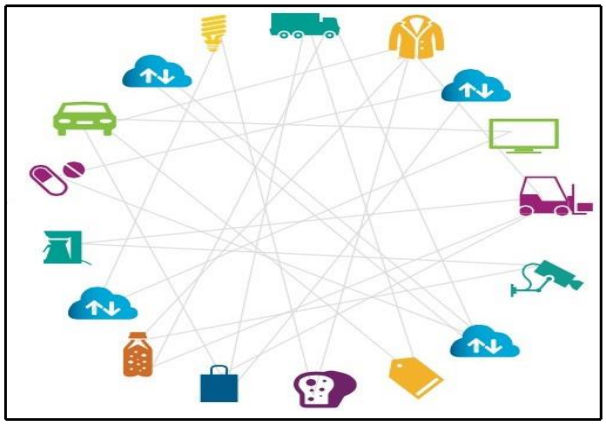

Fig-6: Blockchain-based direct communication model

It can also result in cost-saving which is due to easier device management by using a blockchain-based decentralized approach. The IoT network can be optimized for performance by using blockchain. In this case, there will be no need to store IoT data centrally for millions of devices because storage and processing requirements can be distributed to all IoT devices on the blockchain. This can result in completely removing the need for large data centers for processing and storing the IoT data.

5. CONCLUSION

First IoT was discussed, which is a revolutionary technology on its own; and by combining it with the blockchain, several fundamental limitations can be addressed, which brings about tremendous benefits to the IoT industry. More focus has been given to IoT as it is the most prominent and most ready candidate for adopting blockchain technology. It utilizes a decentralized approach that delivers better efficiency and eliminates the single point of failure. Moreover, blockchain delivers better security and data integrity through tamper-proof and immutability features. The integration of blockchain with IoT can resolve issues of the IoT centralized system and provide a good way for future developments. Blockchain can provide a solution by allowing devices to communicate with each other directly in a secure manner and even request firmware and security updates from each other. On a blockchain network, these communications can be recorded immutably and securely which will provide auditability, integrity, and transparency to the system. There are clear benefits that can be reaped with the convergence of IoT and blockchain and a lot of research and work in academia and industry are already in progress. There are various projects already proposed providing blockchain-based IoT solutions.

REFERENCES

[1] Atlam, H.F.; Azad, M.A.; Alzahrani, A.G.; Wills, G. A Review of Blockchain in Internet of Things and AI. *Big Data Cogn. Comput.* **2020**, *4*, 28.

[2] IoT Analytics: State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time Available online: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

[3] Fabiano, N. Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (Smart Data), Exeter, UK, 21–23 June 2017; pp. 727–734.

[4] Conoscenti, M.; Vetro, A.; De Martin, J.C. Peer to Peer for Privacy and Decentralization in the Internet of

Things. In Proceedings of the 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), Buenos Aires, Argentina, 20–28 May 2017; pp. 288–290.

[5] Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303.

[6] Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411.

BIOGRAPHIES

"R.Sreenith, pursuing Bachelors at Srinivasa Ramanujan Institiute of Technology, Ananthapuramu, India. His area of interest includes Blockchain technology, Computer Networks. "

"**A.SreeHarsha**, pursuing Bachelors at Srinivasa Ramanujan Institiute of Technology, Ananthapuramu, India. His area of interest includes Blockchain technology, Cyber Security. "