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

IoT Security Using Blockchain Technology

[1]Prof. Dr. Latika Desai [2]Prof. Madhuri Kethari
[1]Head Dept. Artificial Intelligence and Data Science , [2]Assistant Professor AI-DS,
Dr. D. Y. Patil College of Engineering & Innovation, Varale, Talegaon, Pune, India

Abstract

A developing technological trend known as the Internet of Things (IoT) connects millions of physical objects from any location at any time. Since these firms are so profoundly concerned with their technological and security challenges, IoT devices have currently become a necessary component of everyday life. The blockchain system consists of a distributed digital ledger that is shared by a group of Internet users; recorded transactions in the ledger that have been verified and recorded cannot be changed or erased. In the near future, Bitcoin is anticipated to rank among the safest and most convenient payment options. The blockchain is made up of a group of blocks that are connected so that the hash of one block is contained in another block. An mistake affects the whole blockchain if information in any block of a blockchain is changed. Bitcoins are created through a process known as mining, in which workers attempt to solve a challenging mathematical equation. The miners are vying with one another to mine Bitcoin as quickly as they can and get the reward.

1. Introduction

One must be familiar with blockchain before we can explore why IoT and blockchain are arguably dependent on one another. While blockchain is both straightforward and intricate, we will focus on its fundamentals for the time being. Bitcoin and other cryptocurrencies are most frequently linked to the blockchain. However, it does transcend beyond those applications, as we can see from the implementation of Blockchain technology in a variety of fields, including politics, healthcare, and the Internet of Things. Blockchain, in its most basic form, is a database that is a collection of different records that many people own and maintain, as opposed to a single business, government, or individual. Each block in a blockchain chain in a blockchain symbolises a record, and the chain connects all the blocks. The Blockchain is preserved on a network of computers when it is established and is accessible to a wide range of users. This implies that no one may update or alter information by going backward in the chain. As a result, it is far more difficult for the chain to be altered, making it more secure than a database managed by a single party. We are starting to see Blockchain technology being evaluated for these purposes, even if we haven't completely seen it implemented in a voting or healthcare system. Theoretically, it would strengthen, safeguard, and automate a nation's electoral process.

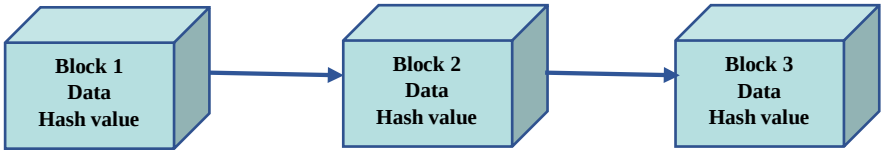

Figure 1: Blockchain

Integration of IoT and Blockchain: Challenges and Advantages

We can now apply IoT on a large scale, for instance through the creation of smart cities. With cities that are less congested, more energy-efficient, and more sustainable, these promise to improve the efficiency of our lives. This large deployment, however, confronts a number of difficulties:

- Security of networks. These networks might be a particularly alluring target for hackers because of the advancements provided by 5G networks and the connection it offers.
- While protecting privacy, data ownership, and data security, data from multiple sources must interact and integrate on an equal footing.
- Potentially vulnerable Internet of Things (IoT) devices, as a hacked device may be leveraged to target other networked devices.

As previously stated, the security design of present IoT systems is a basic issue. It uses a centralised client-server paradigm that is administered by a central authority, making it vulnerable to a single point of failure. Blockchain solves this issue by decentralising decision-making to a network of shared devices that operates on consensus. However, there are three primary difficulties to take into account while building the architecture for IoT devices in combination with a blockchain ledger:

a. Scalability. How to manage the enormous volumes of data generated by a wide network of sensors and potentially slower transaction processing rates or latency is one of the key challenges that IoT is presently facing. Setting up a clear data model in advance helps save time and avoid problems while implementing the solution.
b. Network security and transactional secrecy. On open blockchains, it is difficult to readily give the privacy of transaction history in the shared ledger for a network of IoT devices. This is due to the fact that transaction pattern analysis may be used to draw conclusions about the users' or devices' identities hidden behind public keys. Businesses should research their privacy needs to see whether hybrid or private blockchains will better meet those needs.
c. Sensors. By interfering with the accurate measurement of the requirements that must be completed in order to conduct a transaction, it is possible to jeopardise the dependability of IoT sensors. Securing a secure environment for data capture and transactions requires steps to preserve the integrity of IoT devices so that they cannot be changed by external interventions.

In summary, maintaining the security and privacy of data sent between networks is a huge difficulty, and the combination of blockchain technology with IoT may hold the solution to these issues. The following are some advantages we discover from fusing blockchain with IoT:

- Data authenticity for quality assurance: Because blockchain technology is immutable, it may give a strong framework to procedures that can rapidly and precisely identify data alterations.
- Device tracking to identify errors: Because IoT networks may be quite large, it might be challenging to identify failure trends. Each IoT endpoint is given a distinct key by the blockchain system, which makes it easier to spot irregularities.
- IoT technology alone provides automation, but when combined with smart contracts, automatic replies may be approved through this network.
- Decentralization for increased security: Because the blockchain is decentralised, hackers won't be able to attack a single server and damage its data, regardless of the communication techniques employed.

- Usage logs for employee performance: Going beyond sensors, blockchain technology can track user behaviours to show you who used a device when and how. This allows you to better understand staff performance.

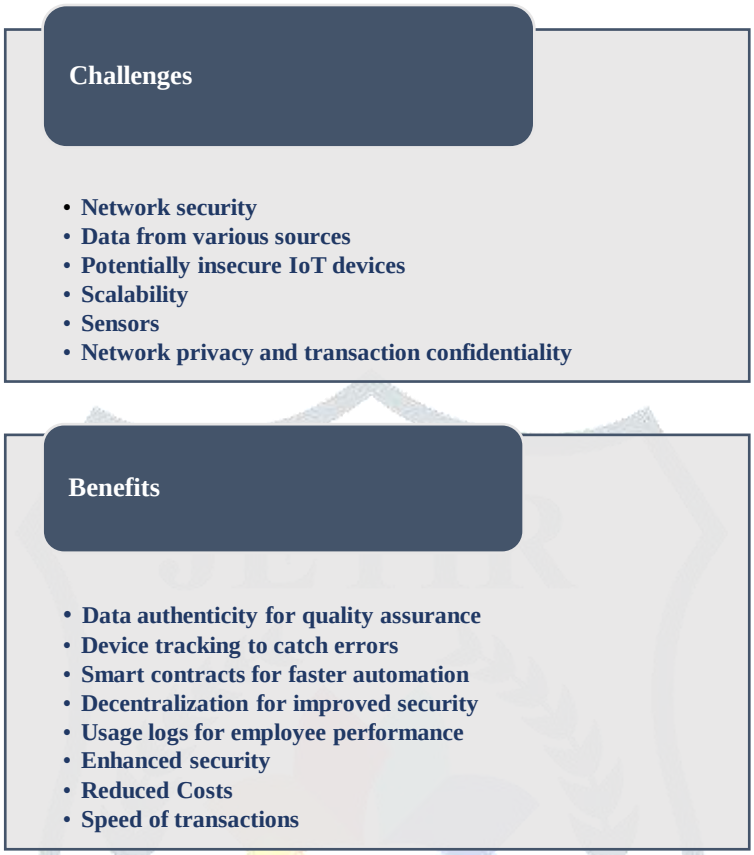

Figure 2: Challenges and Benefits of IoT and Blockchain Integration

The difference between IoT and Blockchain security is based on the items like privacy, bandwidth, system structure, scalability, resources, latency, and security as shown in table 1. Due to the lack of privacy in IoT devices blockchain technology ensures the privacy of the participating nodes. The IoT devices have limited bandwidth and resources whereas the blockchain has high bandwidth consumption. The system structure in IoT devices is centralized whereas in blockchain they are decentralized.

Table 1: Comparison between IoT and Blockchain

Items	IoT	Blockchain
Privacy	Lack of privacy	Ensures the privacy of the participating nodes
Bandwidth	IoT devices have limited bandwidth and resources	High bandwidth consumption
System Structure	Centralized	Decentralized
Scalability	IoT is considered to contain a large number of devices	Scales poorly with a large network
Resources	Resource restricted	Resource consuming
Latency	Demands low latency	Block mining is time-consuming
Security	Security is an issue	Has better security

2. Related Work

Blockchain and the Internet of Things are the two ideas that are causing a stir in both the commercial and technological worlds (IoT). While Alamri et al. [3] noted that the two are now on every technology professional's lips and that there is still more to say about them, Jesus et al. [2] asserted that merging them will transform the way we conduct business. IoT refers to the ongoing rise in the number of data-gathering devices entering private households or commercial settings. Blockchain is a distributed, encrypted ledger designed to create immutable, real-time registries. In addition to the centralised issue, Dorri, et al. [4] noted that the majority of IoT devices have resource constraints and privacy concerns, which makes them less suitable with the demands of sophisticated automated systems. They put out a blockchain-based solution to address the IoT security and privacy concerns as well as to address the drawbacks of the prior considered proposals. They made the case that the Blockchain is a useful and practical solution for addressing IoT security and privacy concerns. Without a doubt, blockchain has scalability, latency, and bandwidth problems. In order to solve these problems, Dorri et al. [4] created a lightweight, scalable blockchain (LSB) for IoT security and privacy using a smart home environment.

The digital currency bitcoin has gained international notoriety. People have shown tremendous interest in the cryptocurrency Bitcoin in recent years. Many people have established Bitcoin mining businesses, and other businesses have started accepting Bitcoin as payment. Since Bitcoin has only been around for a few years, there is still a lot of study being done on the cryptocurrency[5]. There are now a few research articles that discuss many facets of Bitcoin, including its mining, security, and various assaults on mining pools. Every component of the Bitcoin protocol was covered in Satoshi Nakamoto's [6] 2009 AD white paper. Although the Bitcoin is considered to be the first digital money, David Chaum initially suggested the idea of cryptocurrencies and the cryptographic methods that underlie them in his paper in 1983 [7]. Proof of Work, the consensus mechanism used by Bitcoin, was conceptualised by Cynthia Dwork and Moni Naor in their article from 1992 [8]. By utilising the blockchain idea, decentralisation in Bitcoin is made possible, which aids in the resolution of the double spending issue [9]. The Internet of Things idea is emerging and growing swiftly. IoT handles a different invention that enables real and virtual objects to interact and be connected to one another, resulting in new digital services that increase our enjoyment. The IoT framework has certain advantages, but the current integrated architecture has a number of drawbacks, including concerns with security, protection, simplicity, and data integrity[10]. IoT adopters now feel vulnerable due to security issues brought on by the rapid development and use of IoT advancements. These issues obstruct future IoT deployment advances in their implementation strategies. To identify such issues, moving the IoT towards distributed ledger technology may be the best course of action. The Blockchain is one of the typical and well-known types of such innovation. Combining blockchain technology with IoT might have countless benefits.

3. Methodology

The Internet of Things can benefit from the three core characteristics of blockchain technology as a data structure: dispersion, immutability, and decentralization (IoT). Since blockchain is distributed, data are duplicated across several machines. This aspect increases the difficulty of hacking because there are more potential targets. Since users in IoT ecosystems may submit and retrieve data from many devices, the redundancy in storage enabled by blockchain technology increases security and improves data access. Any alteration to the recorded data may be immediately recognized because to the immutability of blockchain technology. When storing data from IoT devices, however, the decentralized nature of blockchain technology might be a significant problem. Using blockchain in the IoT context to store access records and permissions is an alternative option. In particular, the distributed and decentralized features of blockchain make huge data storage costs. As an alternative, the data might be kept in a central location while blockchain technology is used to track data access. After that, users have an immutable data structure that allows them to track who has accessed their data and when. Going a step further, data access rights granted by users may be stored using blockchain technology. The flowchart of transactions of cryptocurrency using blockchain is shown in figure 3.

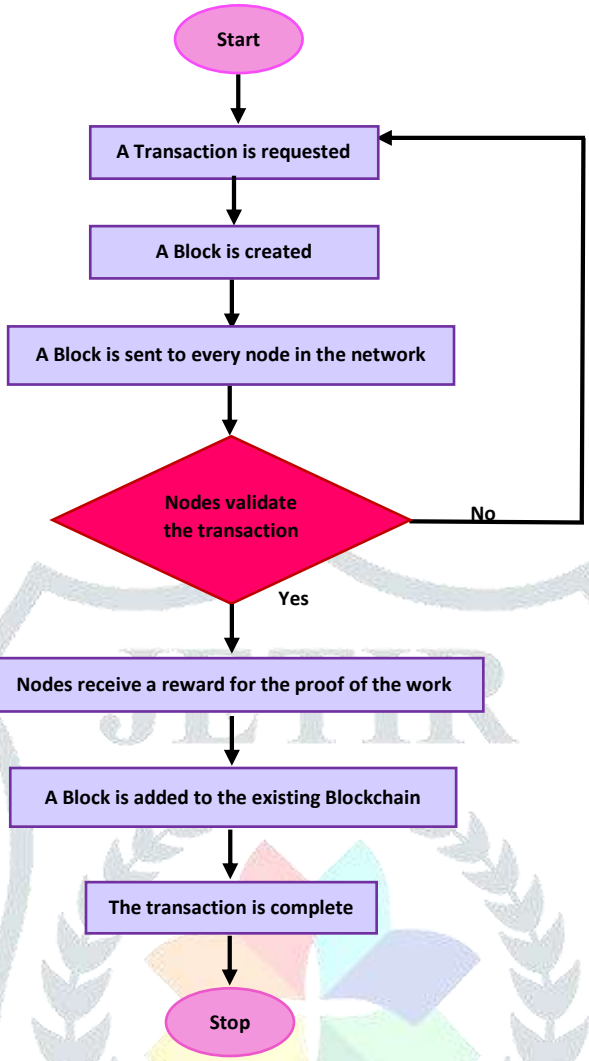

Figure 3: Flowchart of Transaction of cryptocurrency in the blockchain

4. Implementing Blockchain in python

Step 1: Defining the Blockchain

```
class Block():
    data = None
    hash = None
    nonce = 0
    previous_hash = "0" * 64

    def __init__(self, data, number =0):
        self.data = data
        self.number = number

    def hash(self):
      return updatehash(
        self.previous_hash,
        self.number,
        self.data,
        self.nonce
    )

    def __str__(self):
      return str("Block#: %s\nHash: %s\nPrevious:%s\nData: %s\nNonce: %s\n" %(
      self.number,
      self.hash(),
      self.previous_hash,
      self.data,
      self.nonce
      ))
```

The output of the Blockchain

```
Block#: 1
Hash: 60e05bd1b195af2f94112fa7197a5c88289058840ce7c6df9693756bc6250f55
Previous:0000000000000000000000000000000000000000000000000000000000000000
Data: hello world
Nonce: 0
```

Step 2: Mining Blocks

```
def mine(block_number, transactions, previous_hash, prefix_zeros):
    prefix_str = '0' * prefix_zeros
    for nonce in range(MAX_NONCE) :
        text = str(block_number) + transactions + previous_hash + str(nonce)
        new_hash = SHA256(text)

        if new_hash.startswith(prefix_str):
            print(f"Yay! Successfullt mined bitcoins with nonce value:{nonce}")
            return new_hash

    return BaseException(f"Couldn't find correct has after trying {MAX_NONCE} times")
```

The output of the bitcoin mining

```
start mining
Yay! Successfullt mined bitcoins with nonce value:86459
end mining. Mining took: 0.2717165946960449 seconds
00000cdeeaff775a245b31eafceb8371ef768379477f0d42e73f1827d523bd99
```

Step 3: Bitcoin Mining with three Blocks

```
    def __init__(self, previous_block_hash, transaction_list):
        self.previous_block_hash = previous_block_hash
        self.transaction_list = transaction_list

        self.block_data = "-".join(transaction_list) + "-" + previous_block_hash
        self.block_hash = hashlib.sha256(self.block_data.encode()).hexdigest()

t1 = "Anna sends 2 NC to Mike"
t2 = "Bob sends 4.1 NC to Mike"
t3 = "Mike sends 3.2 NC to Mike"
t4 = "Daniel sends 0.3 NC to Anna"
t5 = "Mike sends 1 NC to Charlie"
t6 = "Mike sends 5.4 NC to Daniel"

initial_block = NeuralCoinBlock("Initial String", [t1, t2])
print(initial_block.block_data)
print(initial_block.block_hash)

second_block = NeuralCoinBlock(initial_block.block_hash, [t3, t4])
print(second_block.block_data)
print(second_block.block_hash)

third_block = NeuralCoinBlock(second_block.block_hash, [t5, t6])
print(third_block.block_data)
print(third_block.block_hash)
```

The output of the three blocks

```
Anna sends 2 NC to Mike-Bob sends 4.1 NC to Mike-Initial String
ac7c14de74c73ddea0bd7d122af9874da86a5900c006a79aaf7dbf0cf9cd38d2
Mike sends 3.2 NC to Mike-Daniel sends 0.3 NC to Anna-ac7c14de74c73ddea0bd7d122af9874da86a5900c006a79aaf7dbf0cf9cd38d2
d3da18e7c1ec0ad942225a3cdc94d9599c3c60eab513808dd5e8fcbd643dcc83
Mike sends 1 NC to Charlie-Mike sends 5.4 NC to Daniel-d3da18e7c1ec0ad942225a3cdc94d9599c3c60eab513808dd5e8fcbd643dcc83
05af93cf887f7486bb4a337b53cd99f0f31293a573146a711e2b088fd48f3159
```

5. Conclusion

As a result, despite the enormous promise of emerging technologies like blockchain and the Internet of Things, businesses are cautious to use them for security and technical concerns. IoT and Blockchain will continue to advance into a universally accepted standard, despite the fact that some are mixing them to see whether they may reduce business risks and security issues. IoT systems built on blockchain may face some difficulties down the road, but more companies are using them. In conclusion, the implementation of IoT systems will be made possible in a variety of ways thanks to blockchain. Blockchain technology still has a long way to go before it is widely used in the business, despite these minor shortcomings, but it does provide some special advantages.

References

[1] Adanma Cecilia Eberendu1 , Titus Ifeanyi Chinebu2 “CAN BLOCKCHAIN BE A SOLUTION to IOT TECHNICAL and SECURITY ISSUES” International Journal of Network Security & Its Applications (IJNSA) Vol.13, No.6, November 2021 DOI: 10.5121/ijnsa.2021.13609 123

[2] E. F. Jesus, V. R.L Chicarino, C.V.N De Albuquerque, and A A. de A. Rocha. "A survey of how to use blockchain to secure internet of things and the stalker attack." Security and Communication Networks April, 2018.

[3] M. Alamri, N. Z. Jhanjhi, and M. Humayun. "Blockchain for Internet of Things (IoT) research issues challenges & future directions: A review." Int. J. Comput. Sci. Netw. Secur vol. 19 May, 2019: pp. 244-258.

[4] A. Dorri, S. S. Kanhere, R.Jurdak, and P.Gauravaram. "Blockchain for IoT security and privacy: The case study of a smart home." In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), March. 2017. pp. 618-623. IEEE.

[5] May 2019 Analysis of Bitcoin Cryptocurrency and Its Mining Techniques Suman Ghimire

[6] S. Nakamoto, "Bitcoin: A peer-to-Peer Electronic Cash System," 2009.

[7] D. L. Chaum, "Untraceable Electronic Mail, Return Address, and Digital Pesudonyms," 1983.

[8] C. D. a. M. Naor, "Pricing via Processing or Combatting Junk Mail," 1992.

[9] U. W. Chohan, "The Double spending Problem and Cryptocurrencies".

[10] Implementation of Blockchain in IoT Rasmeet Kaur and Aleem Ali 28 march 2022, research gate

[11] D. He, S. Li, C. Li et al., “Security analysis of cryptocurrency wallets in android-based applications,” IEEE Network, vol. 34, no. 6, pp. 114–119, 2020

[12] A. Sunyaev, “Distributed ledger technology,” Internet Computing, Springer, Cham, pp. 265–299, 2020.