International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Overview of Application and Development of Blockchain and IOT Technology in Aadhar Card System

Shilpa G. Kshirsagar

Abstract: ***Recently as there is development in technology, developments have risen in government sector also. One of them is the unique identification card-Aadhaar Card which is widely used in India for various purposes. Use of Blockchain technology and IOT will enhance Aadhaar Card system which is widely used in India. A blockchain is digitally distributed, decentralised, public ledger that exists across a network. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party. Blockchain Based Aadhaar uses Blockchain platform for securing Aadhaar information. Similarly, IOT (Internet Of Things) describes the network of physical object-"things" that are embedded with sensors, software and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. Unique Identification of Aadhar number through UID sensor is also possible through IOT. After successful authentication, a device can be authorized and can be granted access to shared resources. The need for validating a device requesting data transfer to avoid data privacy breaches that may compromise confidentiality and integrity. Blockchain and artificial intelligence (AI) both are extensively being used as an integrated part of IoT networks for security enhancements.***

Keywords: Aadhar Card System, Blockchain, IOT, Unique Identification Number (UID Number), authentication, authorization, Artificial Intelligence (AI)

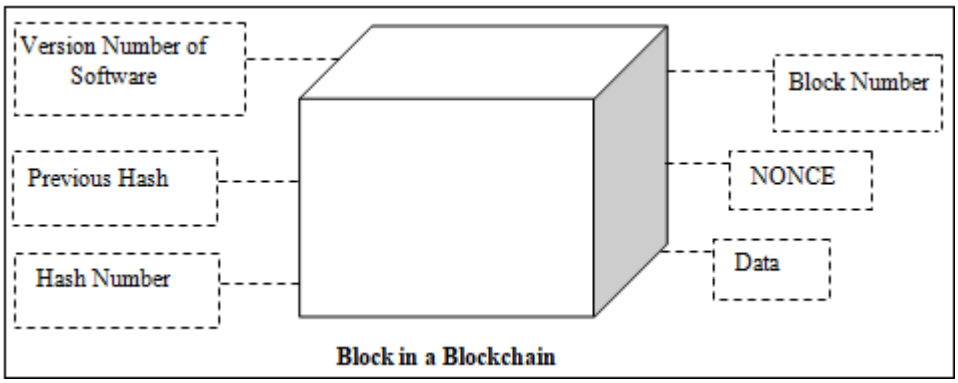
1. Introduction

1.1 Blockchain Technology

It is a system which was actually designed to include a record of transactions made in bitcoin or another cryptocurrency and maintained across several computers that are linked in a peer-to-peer network. Blockchain technology can be used to secure access to identify information while improving access for those who need it in different industries. It is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.

Blocks in a blockchain are data structures within the blockchain database, where transaction data in a blockchain are permanently recorded. A block records some or all of the most recent transactions not yet validated by the network. Once the data are validated, the block is closed. The main elements of a block in a blockchain are the head of the block that is divided into six components: the version number of the software, the hash of the previous block, the root hash of the Merkle tree.

Miners create new blocks on the chain through a process called mining. In a blockchain every block has its own unique nonce and hash, but also references the hash of the previous block in the chain, so mining a block isn't easy, especially on large chains.



Block in a Blockchain

Blockchain Based Aadhaar uses Blockchain platform for securing Aadhaar information. The system stores the Aadhaar data in a group of computers interconnected to each other. The Blockchain uses a hashing function to transform the data and produces a hash code. The hash code ensures the identity of user is kept secure. The data is stored in blocks in the nodes. The system also uses Ethereum Smart Contracts to ensure to only the authenticated data is accessed by the third parties. The Blockchain based Aadhar uses distributed databases (decentralized databases) math and cryptography to record transactions, transactional data is secured and the data is stored in distributed small chunks and spreads across the entire network of computers, and so it is difficult to hack these systems than hacking the centralized or traditional servers.

IOT Technology: The IoT is the result of a lot of devices operating in coordination with each other, sometimes asynchronously or agnostic of each other. They operate at different levels, and each take custody of different aspects of data's journey to and from the internet. The most numerous type of device in the IoT can be referred to as the node. These are all the devices that are providing sensor data, or devices that are being controlled from the cloud.

Nodes tend to be either lightweight sensor devices, which primarily gather status information over a pre-programmed interval, or middleweight devices which also offer controllable functions

The IoT node as we know it today, in its most minimal use case, can be a sensor embedded in an object that is never serviced again across the life of the device. They can be wireless and operated on a coin cell battery for years. What seemed impossible just a few years ago is now quickly becoming standard. And that's thanks to incredible innovations in low-power operation of wireless modules.

The ability to put a sensor into virtually anything and give it years of battery life is the primary driver for the explosion of smart devices that we see now. It also creates a challenge, because a low power wireless hub is needed that can support lots of devices connecting infrequently. And there are lots of approaches to doing that, which we refer to as gateways.

The IoT gateway is the central hub for sensors that collects their data, and they come in many forms. They interface directly with sensors and provide the path for that data to go to the cloud. Gateways can be designed to operate in so many ways that it can be hard to generalize.

In some cases, they may listen passively, and the sensor operates without even knowing the gateway is there. In some cases, they may establish bidirectional communication with the sensor, allowing the sensor to be controlled by the cloud through the gateway. A gateway may be a small unit collocated with the sensors on-site, or it may be the massive cellular tower miles away. Much of this depends on what wireless technology is used, all of which have advantages and disadvantages.

Most IoT devices communicate over either Wi-Fi, LTE, Bluetooth, or LoRaWAN. These technologies vary in their available throughput, their range, their power consumption, and more.

Selecting the right technology for a given use case is an important early decision for an IoT implementation, as well.

For those who are especially protective of their data, LoRaWAN may make the most sense as it allows you to build a private network without relying on a big public gateway, like a cellular tower.

If higher throughput is needed (like a group of security cameras that are capturing live video), a Wi-Fi gateway can provide coverage over a whole facility to capture that video and send over Ethernet to the server that catalogs that video.

Importantly, gateways are often multi-protocol for this reason. They gather sensor data over Bluetooth and send it to the internet over Ethernet. Connect industrial hardware over serial port to a gateway, and control that gateway via a Wi-Fi connection to the internet.

The purpose of a gateway is to bridge devices and make them accessible, and this very often means supporting multiple types of connectivity. Laird Connectivity's IG60, for example, supports Wi-Fi, Bluetooth, Ethernet, Serial, and USB connection, because retrofitting IoT connectivity to an existing system can mean having to resolve lots of different protocols and connector types to connect to the cloud.

The cloud aspect of IoT is where real intelligence happens, and what makes the IoT more than just a collection of devices talking to each other. The cloud is composed of the storage and processing in a data center that allows data to be pulled in from a gateway and to be manipulated or analyzed in software.

This tends to be a subscription type service such as Amazon Web Services or Microsoft Azure, although it's possible to host the cloud storage and computing independently on your own server. The major advantage of suppliers like Amazon and Microsoft is the worldwide access, content distribution, and ability to scale which enables very large and flexible IoT applications.

The cloud, more than anything, is about gaining insights into the data around us to make meaningful changes that make things better.

The cloud can be used to make all kinds of things work better, smarter, and more efficiently. It also allows tasks that would have required human time and effort to be automated, making people's lives easier and decreasing errors. The applications are truly limitless, and the cloud is what enables this.

The blockchain and IoT:-Blockchain-based IoT applications can be developed by using gateway nodes. These gateways serve as an abstraction layer between legacy systems and IoT devices. These gateways can communicate with each other to exchange data and can also verify blocks before adding them to the blockchain network.

UIDAI or any transaction done through Aadhar system, in a cardless way, its Information will be retained through nodes of IOT sensors and can be transferred into blockchain and distributed into a secured manner into entire network of computer system.

There are all sorts of devices in the IoT that can be used to connect Aadhar system, but they can very generally be broken down into three roles: Nodes, Gateways, and Cloud Services. Together, they form a chain that gets data where it needs to go: Nodes at the smart device, Gateways positioned within range to provide the uplink/downlink with the internet, and the Cloud to store data, manipulate it, and initiate actions down to nodes again.

Blockchain technology can help address these challenges by making IoT devices more secure and efficient. Because IoT devices have no authentication standards, they can damage critical infrastructure.

Blockchain can be used to ensure the integrity of sensor data, thereby preventing the duplication of malicious data. In addition to securing data, blockchain also allows devices to be uniquely identified. This is vital for ensuring the security of IoT devices.

However, common blockchain platforms require huge computational power. They also make the integration of IoT nodes difficult. A decentralized model can overcome these problems.

The current centralized model of blockchain is expensive, and it restricts the flow of data. The security of IoT networks cannot be ensured by a single gateway. Moreover, centralized infrastructure is expensive and not secure enough. Besides, one single gateway can be hacked, compromising the entire IoT network.

Final Thoughts

While there are challenges involved in integrating blockchain with the existing IoT system, once these hurdles are out of the way, the technology will pave the way for a trusted, secure, and efficient third generation of the Internet.

References

[1] https://en. wikipedia.org/wiki/Internet_of_things
[2] https://originstamp.com/blog/benefits-and-challenges-of-blockchain-in-iot/
[3] https://encyclopedia.pub/entry/8977
[4] https://www.investopedia.com/terms/b/block-bitcoin-block.asp#:~:text=Blocks%20are%20data%20structures%20within,validated%2C%20the%20block%20is%20closed
[5] https://d1wqtxts1xzle7.cloudfront.net/64499376/IRJET-V7I3254-with-cover-page-v2.pdf?Expires=1667825755&Signature=A~IyLBv9iUwoQtuRwf1jCRTYzgL0eJXtuVGY~beJQtOsaZ4LBqIA9B9ieleRyUMOCtT-Dyx65YCyZFCsRy8SxOpOHCvmrInCndCO4K4dQIqDp1ECtKOlSTW07SsArkvtEVLKR-UE0Dax2HBvWwtGTdRSDm7710QhNmpWGSO7mJ0-zat7OnhZs3fcxG5UBokai-Nra6dM-x74GH8af4zpPKmZbAIyp8V7lrRNEs2CiwLeClXYnMh4lIKjMSH1oCgCyUOGPS1jn~nY7VQynhZ0XHJrsvQCRuv1-FnnrrwKJeQNoArPcBD~hBxdr9kE8xpUShyxUnZ5iMhXMDVfrXm6Zg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA