IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204335 |

Blockchain Solutions for Authentication and Authorization of IoT Devices

Vedika Thakur, Tanuja Tabib, Harshada Salvi

PG Student, Dept. of M.C.A., FAMT, Mumbai University, Ratnagiri, Maharashtra, India

PG Student, Dept. of M.C.A., FAMT, Mumbai University, Ratnagiri, Maharashtra, India

Guide & A.P., Dept. of M.C.A., FAMT, Mumbai University, Ratnagiri, Maharashtra, India

ABSTRACT: The Internet of Things and Blockchain are two technologies that have been gaining popularity since their creation. For all features of IoT to become fully functional in practice, there are several obstacles such as scalability, authorization, authentication, and security due to the critical and sensitive nature of the data they generate. To overcome this problem Blockchain-based authentication and access control systems can be used. Blockchain is a decentralized database that records every transaction made on a network. The integration of blockchain technology with IoT presents a promising solution to address the challenges of scalability, authorization, authentication, and security.

KEYWORDS: Blockchain technology; smart contracts; distributed ledger; IOT device security; cyber attacks

I. INTRODUCTION

The Internet of Things (IoT) provides intelligent solutions by linking physical objects through the Internet. IoT has the potential to revolutionize various domains such as intelligent residences, healthcare, urban planning, Wireless Sensor Networks (WSN), agriculture, etc.

In IoT, every physical or virtual device should be accessible and generate content retrievable by users irrespective of their location. Advanced communication technologies like cellular networks, ZigBee, and Bluetooth enhance reliability and reduce latency in IoT systems. However, it's crucial that only authenticated and authorized users utilize the system to mitigate security risks such as data theft and manipulation.

Security concerns pose significant barriers to widespread IoT deployment. Blockchain technology, stemming from cryptocurrency, is regarded as a revolutionary concept. Its decentralized and distributed nature makes it an apt solution to enhance device-to-device communication security challenges.

Integrating blockchain with IoT offers manifold benefits. Blockchain's decentralized and immutable nature improves the security of IoT devices by eliminating single points of failure and ensuring data integrity. With blockchain, IoT ecosystems gain transparency and accountability, as all transactions are recorded on an unalterable ledger.

Cryptographic techniques facilitate secure authentication and communication between devices, while smart contracts automate access control policies. Combining blockchain and IoT enhances security, transparency, and reliability, paving the way for more robust IoT deployments.

II. LITERATURE REVIEW

Securing IoT devices is tough because most lack resources, there are so many of them, they're all different, and there's no standard way to handle them. These devices often collect lots of our data, raising big privacy worries. Some experts suggest dividing data into different privacy zones and having a Home Security Hub check before letting devices join, but they don't think about the possibility of devices bypassing the hub.

Another study focused on smart homes talked about how sensors gather data and send it to the main hub, but they didn't offer any solutions. Some people suggest sending as little data as possible or even adding noise to protect privacy, but that might mess up services, especially in smart homes. So, even though there are some ideas out there for securing IoT

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204335 |

and keeping our data private, we still have to figure out how to deal with devices that have limited resources and how to balance privacy with sharing data.

Blockchain is like an unchangeable record book that keeps track of transactions for things like Bitcoin. People in the network, known by their Public Key, work together to manage the blockchain. Some special people, called miners, add new transactions to the blockchain by solving tough puzzles. This process is called mining. Blockchain is useful for solving security and privacy problems in IoT because it's decentralized, anonymous, and secure.

III. OVERVIEW OF BLOCKCHAIN STRUCTURE

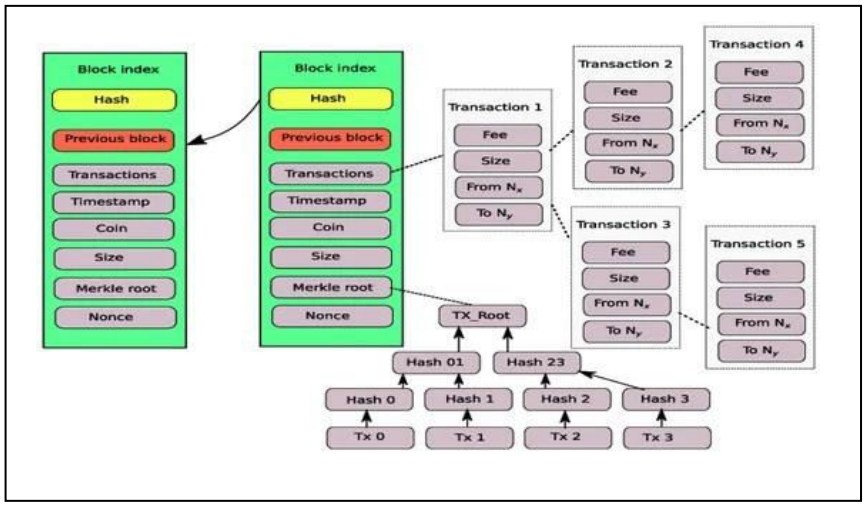
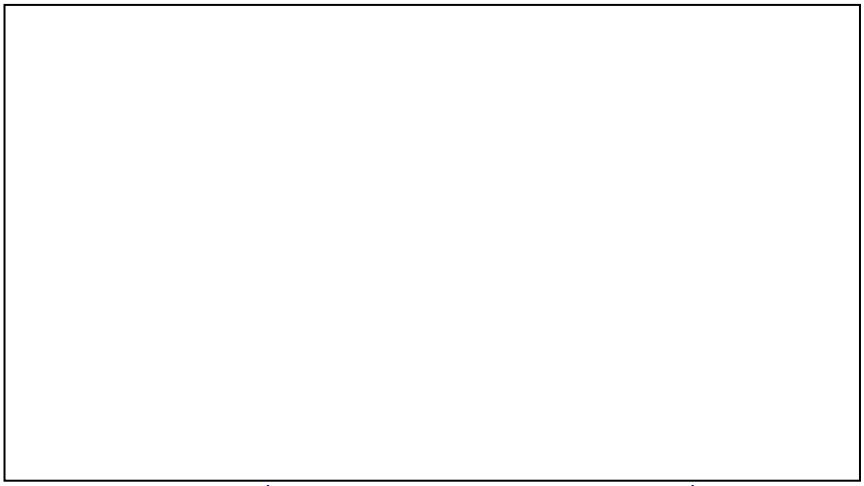


Fig 1. Blockchain Structure

A blockchain functions as a decentralized, distributed ledger utilized for logging transactions across a network of computers. Transactions are structured through a Merkle tree, enabling streamlined verification of transaction integrity. Picture a digital ledger spread across numerous computers.

Every block holds a batch of transactions alongside a cryptographic hash of the preceding block. This framework ensures the secure and transparent storage of data within the blockchain. This makes it safe and clear. It's built like a linked list, with each block containing transactions. Transactions are sorted in a way that makes check in Instead of having one person in charge, it's run by many computers. Every block has a hash code that connects it to the previous one, making it secure. Lots of copies of the ledger are kept by different computers, making it hard to mess with. Every transaction has a digital signature, making it reliable. Overall, it's a safe and clear way to store and handle data without relying on one person.

IV. WHY BLOCKCHAIN FOR IOT SECURITY



International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204335 |

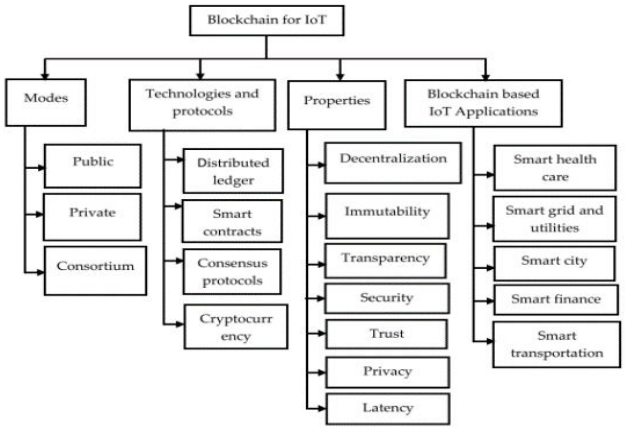


Fig 2. Blockchain For IOT

1. Blockchain Modes

The blockchain is a decentralized platform that is divided into three types public blockchain, a private blockchain, or a consortium blockchain based on various principles such as authentication and access control mechanisms.

Feature	Public Blockchain	Private Blockchain	Consortium Blockchain
Management	Non centralized	Centralized	Partially centralized
Access permission	Reading is public	Public/restricted	Public/restricted
Consensus determination	All miners	One organization	Selected set of nodes
Consensus process	Permission-based	Permission-based	Permission-free

Table 1. Blockchain Modes

2. Blockchain services and benefits for authentication and authorization of IoT applications

Blockchain Technologies and Protocols	Benefits for IoT Applications
Distributed ledger	Perform large of transactions Support IoT devices Offer data collection
Smart contracts	Enhance the autonomy of IoT devices Eliminate regulatory overheads Provide high level of collaboration and authority
Cryptocurrency	Control central authority Ensure integrity of transactional data Change business and finance directions
Consensus protocol	Manage and integrate information Support IoT applications Support agreement between vendors without need to central authority

Table 2. Blockchain Benefits for IOT Applications

2.1. Distributed Ledger

The distributed ledger is designed to work without a central administrator. This shared ledger helps people trust the system more. Since everyone is connected in a network where they share info directly, each pair of devices has enough space to help keep the ledger going. The connection layer makes sure sensors and devices can talk to each other.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204335 |

2.2. Smart Contracts

IoT data and blockchain can be united through smart contracts, and digital agreements coded to automate terms between parties. Stored on a blockchain, they ensure transparency and safety. Smart contracts verify data authenticity before storage, ensuring only genuine data is retained. This method offers a secure and reliable way to validate IoT data using blockchain.

2.3. Cryptocurrency

Cryptocurrency is a digital asset independent of central authority or financial backing, relying on encryption techniques for security. Blockchains ensure transparent transaction management. Despite scrutiny for illicit activities and exchange rate fluctuations, cryptocurrencies remain prevalent.

2.4. Consensus Protocol

Agreement methods in blockchain are crucial for managing and integrating information, especially in IoT applications. They ensure transaction validity without a central authority. Examples include Proof of Work (PoW) in Bitcoin and Ethereum, where miners validate transactions by solving puzzles, and Proof of Stake (PoS) in Cardano and Polkadot, where validators are chosen based on cryptocurrency holdings. Other methods include Delegated Proof of Stake (DPoS) in EOS and Practical Byzantine Fault Tolerance (PBFT) in permissioned blockchains like Hyperledger Fabric. Each method has its benefits and is tailored to specific blockchain needs.

3. Blockchain-Based IoT Applications

Blockchain has been integrated with different IoT applications to boost various performance aspects such as smart healthcare, supply chain, smart grids and utilities, smart cities, smart finance, smart transportation, smart homes, etc.

3.1. Food Supply Chain Traceability System

A traditional food supply chain involves five key players: (1) production, (2) processing, (3) warehousing, (4) distribution, and (5) retail. Ensuring food safety requires a reliable traceability system.

This system utilizes decentralized IoT technology to collect and exchange data about food items along the supply chain. Sensors and communication tools enable members to input, modify, and access information. Each food product is tagged with an RFID tag for unique identification, while members maintain digital profiles with location and role details. Data is stored in a blockchain accessible to all members, who receive public and private keys upon registration. The framework ensures real-time updates on food product safety, distributed across the network.

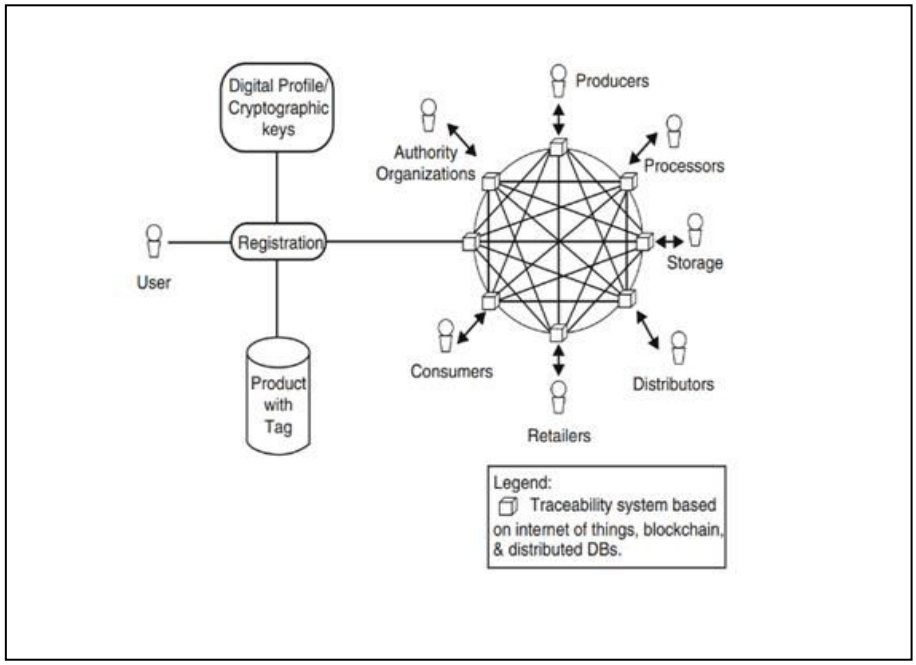


Fig 3. Framework For Food Supply Chain Traceability System

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204335 |

3.2. Smart Homes

Smart home setups enable homeowners to optimize resource usage. They typically include various IoT devices and sensors. Like conventional IoT setups, smart home architectures comprise (1) sensors and gadgets, (2) communication networks, and (3) cloud services.

Blockchain-based architectures feature a local blockchain stored on a capable node called a "miner." These miners handle both internal and external communication within the smart home network. Furthermore, local storage is utilized to store blockchain ledgers. An evaluation is conducted to gauge blockchain technology's performance in smart home environments.

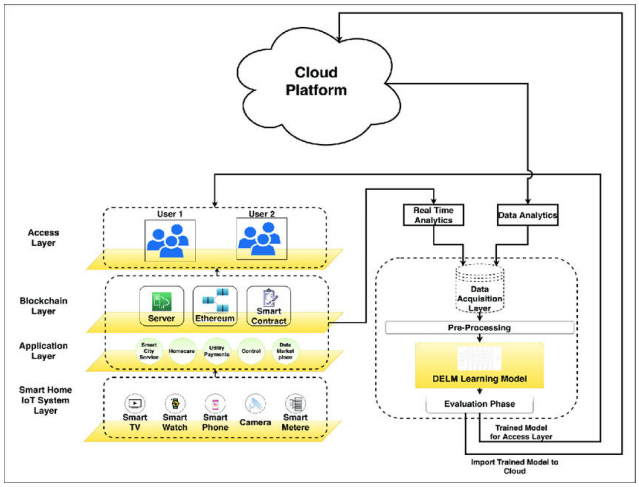


Fig 4. Smart Home System

3.3. Smart City

Smart cities are like big puzzles that use technology to solve problems and make life better for everyone. They use things like sensors and computers to gather lots of information and figure out ways to do things more efficiently and save money. The smart city system collects tons of data from different sources and analyzes it using special databases. Keeping people's privacy safe in smart cities is tricky, but some technologies can help, like differential privacy and encryption. These technologies make sure that data can be shared safely between different parts of the city. Smart contracts are also used in smart cities that run on blockchain.

Fig 5. Smart City

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204335 |

V. BLOCKCHAIN-BASED PLATFORMS FOR IOT

Platform	Blockchain	Popularity and Active	Consensus Algorithm	Pricing	Supported Language	Smart Contracts
Bitcoin	Public	High	POW	Free per transaction	Script and C++	No
Etherium	Public and Permissioned	High	POW,POS GHOST	Ether for transaction and computational service	Python,Go,C++,Java Script	Yes
Hyperledger Fabric	Private , Permissioned	High	PBFT	Open source price	Python,Golang and Java	Yes
Multichain	Private , Permissioned	Medium	PBFT	Free open source price	Python,C#,Java Script,PHP,Ruby	Yes
Quorum	Public and Permissioned	High	KATT,IBFT	Fees per transaction	Python,Go ,C++ and Java Script	Yes
List	Public and Permissioned	Medium	DPOS	Fees per transaction	Javascript	Yes
Litecoin	Public	Low	Scrypt	Fees per transaction	C++	No
HDAC	Public and Permissioned	Low	POW	Fees per transaction	Web Assembly	Yes
IOTA	Public and Permissioned	Low	POW,TANGLE	Pricing not clear yet	Python ,C,Javascript	No

Table 3. Blockchain Platforms

1. Bitcoin Platform

Bitcoin is a widely known blockchain platform that features a prominent digital currency, facilitating decentralized transactions without the need for intermediaries or third parties. Many IoT platforms utilize bitcoins for microtransactions, serving as a digital wallet for transactions. Most IoT platforms rely on the widely accepted and dependable solution of smart contracts, which offer enhanced security for overseeing and documenting all interactions in transactions without the constraints of Script language.

2. Ethereum Platform

Ethereum is like a big computer system that's open for anyone to use and manage. It's built on blockchain technology, which means it's decentralized and not controlled by any single person or company. This system is flexible and can easily work with new technologies and IoT applications, because of its smart contracts feature. Lots of people use Ethereum, and there's a big community that helps create new apps in different programming languages like Go, C++, and Python. Ethereum uses special methods to agree on things, which helps make IoT apps faster and easier to use with blockchain.

3. Hyperledger-Fabric Platform

The Hyperledger-Fabric platform is a widely adopted open-source platform (constructed using the Golang and Java languages) that enables developers to create blockchain applications using a modular architecture strategy. Hyperledger Fabric operates as a permissioned network, offering data confidentiality functionality to encrypt transactions, preventing unauthorized individuals from altering them.

4. Multichain Platform

Multichain is a private blockchain platform, building on Bitcoin's core API for financial transactions. It offers application development, privacy, and control in peer-to-peer networks. With support for various programming languages and both API and command-line interfaces, it's adaptable for open or closed networks. Ideal for IoT data collection, given its permissioned structure.

5. Quorum

Quorum, an open-source blockchain, initially an Ethereum add-on, is popular in finance, offering fast transactions (up to 100 per sec.). It's permissioned, supporting public and private transactions with straightforward consensus. It's widely used across industries.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204335 |

6. Lisk
Lisk is a widely used open-source blockchain framework that empowers developers to construct and customize decentralized system services using JavaScript. It enables individuals to possess and develop personalized sidechains that can evolve into full-fledged applications. Lisk is currently undergoing development and offers three primary tools: Lisk Commander, Lisk Element, and Lisk Core.

7. Litecoin
Litecoin is an open-source blockchain platform functioning as a decentralized payment network. It's a cryptocurrency that is notable for faster transaction confirmations and improved storage efficiency. Achieved through shorter block generation times and a memory-intensive proof of work mechanism, Litecoin produces blocks every 2.5 minutes compared to Bitcoin's 10 minutes, addressing Bitcoin's storage limitations.

8. HDAC Technology
HDAC is a publicly permissioned blockchain platform focusing on IoT contracts and payment solutions. It facilitates machine-to-machine (M2M) transactions for IoT devices like smart vehicles, homes, and utilities. HDAC supports Web Assembly language for multi-language programming. Currently in development, it will debut as an IoT contract for smart homes.

9. IOTA
IOTA is an open-source blockchain platform with a unique block less distributed ledger concept called Tangle. Unlike traditional blockchains, IOTA uses Tangle, a directed acyclic graph structure, to validate transactions in parallel without fees. This allows for high transaction rates and supports IoT devices without discouraging participation.

VI. CONCLUSION

Blockchain technology has a significant impact on the authentication and authorization of IOT devices. Many IoT devices are at risk of cyberattacks, and the decentralized nature of blockchain technology facilitates seamless communication and data exchange.
Some important blockchain platforms, like Hyperledger Fabric and Ethereum, are good for IoT. These platforms offer robust frameworks for building decentralized applications (dApps) that can seamlessly integrate with IoT devices, enabling efficient data management and transaction processing while maintaining the confidentiality and integrity of sensitive information.
By using blockchain, IoT devices can share data more securely without needing a central authority. This can make things safer and more efficient. As blockchain and IoT keep improving, they'll likely team up to make our connected devices even better and safer.

REFERENCES

1. Houshyar Honar Pajooh and M. A. Rashid, ‘A Security Framework for IoT Authentication and Authorization based on Blockchain Technology’, IEEE International Conference On Trust, Security And Privacy In Computing And Communications, 2019.
2. Ahmad K. Al Hwaitat, Mohammed Amin Almaiah, Aitizaz Ali, Shaha Al-Otaibi, Rima Shishakly, Abdalwali Lutfi and Mahmaod Alrawad, ‘A New Blockchain-Based Authentication Framework for Secure IoT Networks’, MDPI, Basel,Switzerland, 2029
3. Khaled Salah, ‘Blockchain for IoT Security and Privacy’,International Journal Of Communication And Technology, 2017
4. Abdelzahir Abdelmaboud, Abdelmuttlib Ibrahim Abdalla Ahmed, Mohammed Abaker, Taiseer Abdalla Elfadil Eisa, Hashim Albasheer, Sara Abdelwahab Ghorashi and Faten Khalid Karim, ‘Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions’, MDPI, Basel,Switzerland, 18 February 2022
5. Achraf Fayad, Badis Hammi, Rida Khatoun, ‘An adaptive authentication and authorization scheme for IoT's gateways: a blockchain-based approach, Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), 2018
6. Alia Al Sadawi, Mohamed S. Hassan, And Malick Ndiaye, ‘A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges, 2021
7. Fahad Alkurdi, Ibrahim Elgendi , Kumudu S. Munasinghe, Dharmendra Sharma and Abbas Jamalipour, ‘Blockchain in IoT Security: A Survey, International Telecommunication Network and Application Conference, 2018
8. Udit Agarwal, Vinay Rishiwal, (Senior Member, Ieee), Sudeep Tanwar, (Senior Member, Ieee), Rashmi Chaudhary, (Member, Ieee), Gulshan Sharma4, Pitshou N. Bokoro, And Ravi Sharma,‘Blockchain Technology for Secure Supply Chain Management: A Comprehensive Review’ , IEEE, 2022
9. Haiping Si, Changxia Sun, Yanling Li, Hongbo Qiao, Lei Shi , ‘IoT information sharing security mechanism based on blockchain technology, Elsevier, 2022
10. Mohammad Maroufi, Reza Abdolee, and Behzad mozaffari tazekand,‘On the Convergence of Blockchain and Internet of Things (IoT), 2019

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details