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

A method for combining different blockchains for the management of internet of things data

[1]Intizar Malik

J.P. Institute of Engineering and Technology, Meerut

[2]Ayan Rajput

Assistant Professor

Department of Computer Science & Engineering

J.P. Institute of Engineering and Technology, Meerut

Abstract

The Internet of Everything era presents increasingly difficult difficulties to data management due to the millions of internet of things (IoT) devices and links. The majority of currently available solutions use centralised systems to manage IoT devices, which raises concerns regarding IoT data security and privacy. Traditional sectors are sparking a tremendous wave of digitization as a result of the internet of things' (IoT) quick development. Due to its decentralisation, traceability, and non-tamper ability, blockchain has recently received a lot of attention in the IoT space. The Internet of Things (IoT) has gained popularity as a paradigm for computing technology. Through a range of applications, it is increasingly being used to facilitate human life processes. Recently, blockchain-based solutions have been developed to aid in overcoming these challenges. In this study, we propose a cross-chain integration system for managing IoT data across various blockchains. The significance of blockchain technology. First most widely used blockchain platforms for Internet of Things applications are also examined. Additionally, we discuss how blockchain technology can be used for a variety of Iot systems. We also explore new advances and alternatives for IoT environments. Finally, we discuss this field of study's difficulties and possible future directions. Various blockchain platforms each have unique advantages when it comes to managing IoT data. We provide a cross-chain system in this study to combine various blockchains for effective and safe IoT data management. Our method establishes a consortium blockchain as the command centre for an interactive decentralised access architecture. All IoT devices run on other blockchain platforms that have been specifically designed for different IoT scenarios. Based on the notary mechanism, For verification, our approach integrates trades done

throughout different channels. Based on the most important considerations, we suggest a blockchain taxonomy for Internet of Things applications.

Keywords: Blockchain, internet of things, artificial intelligence, data management

1. Introduction

Blockchain is the most effective technology for data security and privacy due of its characteristics like immutability and irreversibility. The blockchain resists data change [1]. Changes are communicated to all nodes so they can verify and update their specific ledger transcript if the ledger utilising transactions is changed. Once a transaction has been confirmed by every node in the network, it cannot be changed without also changing the blocks that came before and after it. As a result, blockchain transactions cannot be undone, and their data is continuously updated. A link, usually referred to as a chain, connects each block. The hash of the previous block is incorporated into the subsequent block in order to tour the chain in reverse chronological order. Blockchain functions in a distinctive way because it uses cryptographic features, a decentralised and distributed structure, and both. Where information security and secrecy are top network priorities, blockchain technology is preferable.

A networking technology known as the internet of things (IoT) links machines, controllers, and sensors. The Internet of Things (IoT) technology enables intelligent machine and the connectivity of objects, and it will undoubtedly assist humanity in moving toward a more advanced and practical future civilization. Millions of homes now have access to low-cost information devices thanks to the advancement of information technologyis growing exponentially. In 2020, there will likely be more than 25 billion linked devices, according to an estimate by IBM [2]. A centralised data centre is typically used in traditional IoT models to collect and process data from connected devices. High life-cycle expenses are a disadvantage of this approach, though. When there are tens of billions of IoT devices, the traditional IoT model may not be able to support the IoT ecosystem's expanding needs due to the high maintenance costs of centralised servers. Most businesses lack viable options for using their data to generate revenues in light of the ongoing collection of unstructured information. According to the McKinsey study, most IoT organisations are still unable to fully utilise their IoT data [3]. The first difficulty is enabling various technologies to cooperate transparently in order to achieve particular objectives by merging IoT data with other company data in databases. The enormous amount of IoT data and its increasing rate of generation are another major problem. Only a limited portion of these data, however, can be kept indefinitely [4]. IoT data security is the third issue. IoT devices produce and handle enormous volumes of data that are both privacy-sensitive and security- and safety-critical, making them tempting targets for various assaults [5]. Designing a practical and safe solution for IoT data management is desirable, to sum up.

Two disruptive technologies of the twenty-first century that stand out in terms of the attention and fervour they have received are cryptography and artificially intelligence (AI) [6]. However, blockchain and AI are two distinct technologies that have been integrated. Technologies and research surrounding blockchains are still in their infancy.A blockchain's broad structure, including its fundamental block components, is depicted

in Figure 1 [7]. Version details, a nonce value, the preceding block's hash value, a timestamp, the Merkle root, and transactions make up each block. The blockchain's version number is used to track modifications and updates over the course of the protocol. Miners will encounter once as a part of mining, which is a random number. In order to mine the block, one must first solve the mathematical conundrum.

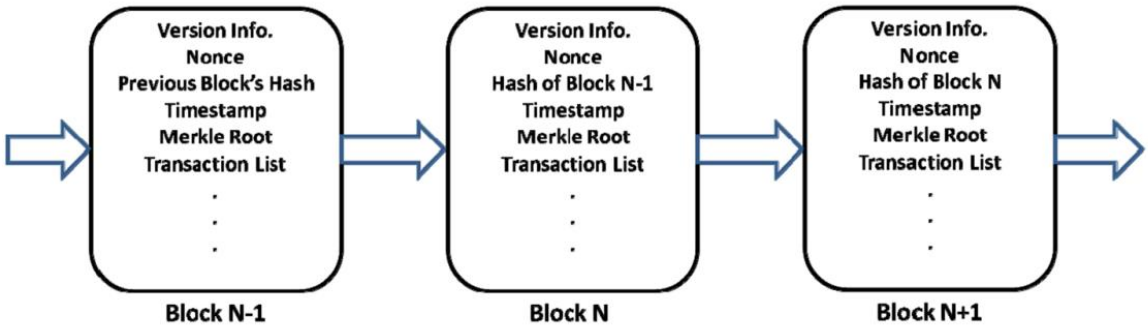

Figure 1: General structure of blockchain

1.1 Blockchain Modes

The blockchain strategy is a decentralised platform that enables data sharing among users of a peer-to-peer network. Blockchains can be categorised as partially decentralised (permissioned blockchain) or totally decentralised (as non-permissioned blockchains). The blockchain approach is a decentralised platform that permits data sharing among users of a peer-to-peer network. Blockchains can be characterised as partially decentralised (permissioned blockchain) or entirely decentralised (as non-permissioned blockchains) (permissionless blockchain). Additionally, the database can be a collaboration blockchain, a private blockchain, or a share important based on different concepts, like authentication and access control techniques [8] (see Table 1).

Table 1: Comparison of blockchain modes.

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

1.2 Artificial Intelligence

Despite the fact that humanity has always sought to comprehend how intelligence works, the word "AI" was first used in 1956. Managers and academics have recently shown a resurgence of interest in the topic of artificial intelligence. Currently, AI is a wide and active field with many beneficial implications and latest scientifictopics [9, 10]technology, including web searches, social network content filtering, e-commerce website suggestions, and an increasing number of consumer goods, including cameras and smartphones. Deep learning is another one of the technologies that are currently popular. Deep learning has grown

significantly over the past few years thanks to larger datasets and more potent processors. Different modules are arranged in various layers in the deep learning architecture. Each of these layers has the ability to learn and alter the input data. In a number of fields, Classifiers techniques such as image classification, speech synthesis, and visual machine vision are used has advanced the state of the art. Another branch of artificial intelligence that focuses on designing intelligent multi-agent systems is swarm intelligence. This area of study is motivated by swarms that have developed a unified behaviour in nature, such as ants or termites. Swarm systems can now be used in a wide area. Examples include using a swarm of mobile micro robots to transport huge and heavy things, using swarm robots in various ways in the agriculture industry, and possibly even using them as toy robots or for entertainment.

2. RELATED WORK

Data solutions for IoT are already the topic of some studies and activities. A cloud computing platform-based data storage system for IoT data was proposed by Jiang et al. [11]. Classifiers techniques such as image classification, speech synthesis, and visual machine vision are used. was created by Strohbach et al. [12], their deteriorating bandwidth and connectivity may have an impact on the level of service. Fog and mist computing are examples of edge-centric IoT-based technologies that provide distributed and decentralised solutions to the problems with cloud-centric approaches. A substantial number of IoT products for the industrial industry were assessed by Perera et al. [13]. To encourage all parties to contribute their edge resources, a decentralised consensus method like blockchain is necessary. Decentralized consensus systems use either blockchain or blockchainless directed acyclic graph technologies to operate as immutable public ledgers for financial accounting to their democratization, accountability, confidentiality, secure movement of wealth, and other advantages [14]. Yeow et al. [15] analysis of the advantages and disadvantages of modern decentralised consensus systems was presented along with a number of unresolved research questions on decentralised consensus for edge-centric IoT. A blockchain-based smart home framework was put forth by Dorri et al. [16] and its security was examined. Their approach results in negligible overhead compared to the security and privacy benefits. By creating shared services, Sun et al. [17] addressed blockchains and an interplanetary file system were used in the network architecture created by Ali et al. [18] to safeguard the anonymity of IoT data (IPFS). constructed using an application architecture comprising peer-to-peer data storage systems and blockchains, they developed a decentralised access paradigm for IoT data. However, a public blockchain is not particularly relevant to IoT applications due to issues including transaction fees. The system uses a decentralised with extremely low latency for micropayments. Blockchains and machines together make these gadgets into financially independent data exchange devices. Additionally, it lowers IoT operational costs, addresses security issues, and safeguards user privacy.

A decentralised access control mechanism for IoT devices was suggested in reference [19]. To lower the cost of communication between nodes, the approach utilised a single smart contract. Policy-based authorization was put into place by ACC by monitoring object behaviour. JC was employed to determine the improper behaviour and deliver the appropriate penalty. The two smart contracts mentioned above were registered using RC, which also offered update, remove, and other functions. Finally, the architecture was put into

practise using two Raspberry Pi, one PC, and one notebook. On Ethereum, a distributed application (DAPP) developed suggested in reference [20]. It mixes the Using bitcoin, it was possible to purchase and sell sensor information, with the SaaS business model. Reference [21] suggested a blockchain structure improvement. The private chain was employed in the company network to distributary handle the IoT device configuration files. It kept the device configuration information on a blockchain and used a smart contract to keep track of operations. According to reference [22], router node routing information is saved to blockchain in order to prevent tampering and tracking. An The Internet of Things accessibility control method based on attributes was suggested in reference [23], which saved attribute data via blockchain. In order to accommodate the IoT devices limited computational capacity and energy supply, this approach prevented authorization protocols streamlining and information leakage prevention. The distributed key management architecture (BDKMA) for multiple blockchains was suggested in reference [24], and a fog computing technique was added to cut down on the time of the multi-chain operation, improving the assurance of user privacy and security. Blockchain was used in reference [25] for the Internet of Vehicles' trust management. By combining two consensus procedures, it is possible to directly manipulate how tough bitcoin miners are, proof of work (PoW) and proof of stake (PoS), to achieve consensus more quickly. A fog computing-based authentication mechanism for road condition monitoring was proposed in reference [26]. A particular type of Edge-chain was put forth in reference [27], using the blockchain's cryptocurrency system capabilities with resource utilisation across accounts and IoT devices. Edge-chain developed a trust framework based on device behaviour to manage IoT devices and access resources from edge servers. A rights management system built on bitcoin was suggested in reference [28], allowing users to post and transfer access permissions. The benefit was that all users would be able to access the access policies, preventing any party from contesting their validity. Reference [29] created a cross-organizational RBAC based on Ethereum that merged blockchain with RBAC and allowed tiny organisations to join, allowing individuals to fully control their responsibilitieswas proposed in reference [30]. In reference [31], the EduRSS scheme was put up. It shared and stored student records on a blockchain based on Ethereum. A unique trust-based recommendation technique (TBRS) was proposed in Reference [32] to guarantee security and real-time data transmission in a vehicular CPS network. A blockchain paradigm based on hypergraphs was suggested in reference [33]. This concept organised storage nodes using hyperedge structures, converted global network data storage into local network storage, lowered storage consumption, and raised security. The approach propose implements light-nodes that serve as a gateway to address this problem. These light-nodes exclusively execute their own transactions' signing and transmitting functions. They do not have to locally store the entire blockchain because they are not a part of the consensus mechanism is a pertinent work on the pursuit of decentralisation, secure data storage, and IoT interoperability. For industrial IoT settings, authors describe a blockchain-based fair nonrepudiation service provisioning system. It is a sophisticated and intriguing system in which the block chain serves as both an intermediary for publishing services and a recorder of evidence.

3. Research Method

A systematic literature search (SLR) can be used to locate and evaluate "all accessible research linked to a certain research question, topic area, or phenomenon of interest," according to Kitchenham and Charters [34]. Providing the most thorough review of the combination solutions is one of the paper's stated goals. It was discovered that an SLR was an effective way to find all pertinent research and scientific activity. We used the methods outlined by Kitchenham and Charters [34] when conducting the SLR.

3.1 Bottleneck of the Blockchain-enabled IoT Architecture:

A blockchain-enabled IoT can be implemented effectively using the loose integration architecture without significantly altering the current IoT design. Data transfers among IoT peers and the consortium blockchain will, however, be transferred through all the IoT edge devices because they act as connecting points between IoT peers and the blockchain network.Given the sudden spike in data transfer requests. Allocating resources between the blockchain and IoT system at key network edge needs to be freshly built in order to solve this problem. Therefore, a crucial future path for creating blockchain-enabled IoT systems is data management, taking into account system dynamics, partial knowledge, management, and communication among bitcoin network and IoT devices. A learning-aided allocation of resources method used in a real-world case study to enhance intelligent data administration is presented in the following section.

4. Results and Discussion

Three major categories can be used to categorise the identified combo applications. Applications and use-cases that leverage the blockchain to support or improve current AI applications make up the first group. Due to this and prior studies, we gave this category the name "blockchain for AI." The second group, known as "AI for Blockchain," includes use cases where AI solutions are meant to enhance the blockchain. This covers both smart contracts and the mining process. The third category includes applications and platforms that integrate blockchain and AI while heavily emphasising how one facilitates or utilises technology through the other.As far as we are aware, this category has not yet been described in any previous research. Ethereum for AI The use cases that aim to promote AI methodologies and approaches using the blockchain make up the first major group. Research focusing on blockchain's potential for AI has been discovered most frequently. The following subcategories can be used to separate these applications:

- Blockchain-based data management
- Blockchain-based data marketplaces
- Blockchain-based AI architectures
- Blockchain-enhanced swarm systems
- Increase of transparency through the blockchain

AI architectures based on blockchain Akhil Goel et al. [35] suggest using the DeepRing architecture to secure deep neural networks using the blockchain. Convolutional neural networks (CNNs) use discrete

blocks that are organised randomly and carry data about the nearby valid blocks. The fact that DeepRing can register and identify all assaults on CNNs is a benefit of this architecture. At some point, tampering modifies corresponding block and all succeeding blocks, making changes or assaults immediately and plainly observable. The authors carried out tests to show how combining cryptocurrency and deep machine learning can produce tamper-proof models. Blockchain provides a foundation for a whole artificial intelligence that uses its own data, not only for data itself. These authors claim that the implementation of a swarming of Intelligent agents would result in the creation of a Church-Turing-Deutsch primary machine (AIAs). The authors assert that this would have an impact on financial markets, smart cities, the Internet of Everything (IoT), and targeted therapies. A blockchain might possibly be used to create some cellular automata, according to a prior publication. Such an implementation should be doable by simulating a naturally random generated mutational system and allowing a created genetic algorithm to evolve. The engagement with such a system via the blockchain will be made possible by specialised coins and tokens. Figure 2 shows IoT Architecture

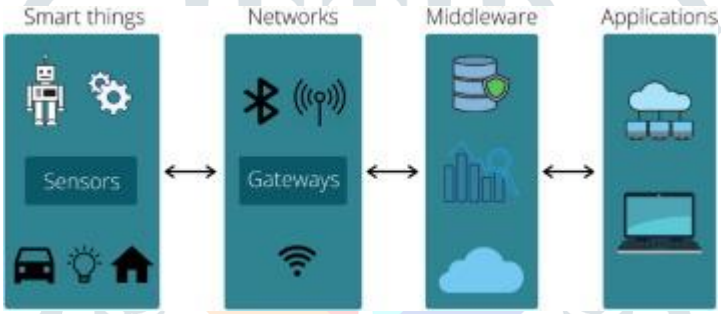

Figure 2: IoT Architecture

4.1 Functioning of the Blockchain

In order to employ blockchain technology, a peer-to-peer (P2P) network with the devices (users) interested in communicating over blockchain must be established. An individual node is a participating device. For each node, two keys public and private are produced. As the name suggests, a user creates a signature using a private key that is kept secret and is acknowledged by everyone else. Asymmetric cryptography is utilised to meet the information's security requirements, to put it briefly. To prevent data on a blockchain from possibly being abused or altered, private keys must be kept secure. A node starts the transaction, signs it with its private key, and then publishes it in the network for peer nodes to verify. Consensus algorithms the term for the verification techniques used vary between blockchain platforms according to their design goals. After receiving confirmation from peers, the transaction is collected by the miner to form a block, which is then added to the blockchain with a timestamp and unique ID (i.e. hash) to prevent future tampering. The hash of a newly inserted block is used to link it to a prior block, and subsequent blocks will link to this block, and so on. The general workflow of blockchain as it applies to the aforementioned description is shown in Figure 3 below.

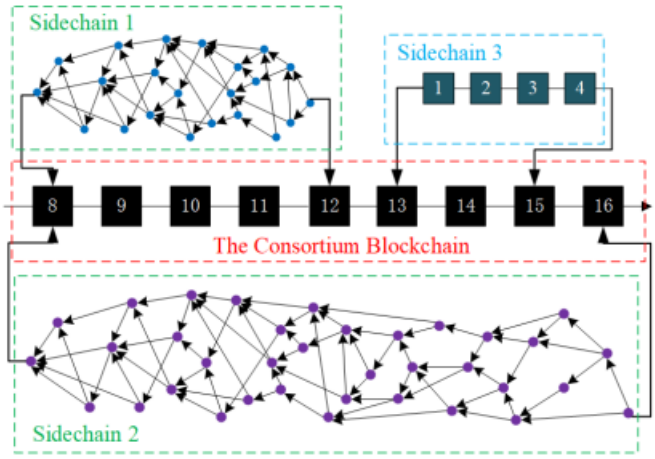

Figure 3: The blockchain structure.

4.2 Blockchain Principles

Blockchain uses a number of technologies that operate according to several protocols. The primary technologies and protocols are covered in this section and are compiled in Table 2. Blocks and transactions are the core components upon which a Blockchain is created, as it is evident from the previous section. The requirement for each network node to locally store the whole chain necessitates the use of a memory-efficient data structure that simultaneously ensures that the data saved in the chain are immutable and tamper-proof. Every block in Bitcoin (BC) has a hash that is both the root hash of a multi-level data structure called a Merkle Tree and the hash of its block-header, a data structure that contains a date, a nonce, and the hash of the preceding block in order to be scalable. A Merkle-Tree is a binary tree made up of a number of nodes with many leaf nodes at the bottom that contain the underlying data. Up until the root node, which is located at the top of the tree, each intermediate node holds the hash of its two descendants starting from the leaves. This data structure's major objective is to make it possible to quickly and ultimately piecemeal retrieve the necessary data from several network nodes. Additionally, the shared consensus and the hash algorithm used to create this structure guarantee that no changes may be made to the chain as a whole. Today, it is asserted, the long-term viability of this protocol's effectiveness is questionable.

Table 2: Blockchain services and benefits for 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

4.3 Blockchains in the IoT Scenario

The key contributions blockchain makes to the development of IoT applications are covered in this section. These contributions include high scalability, complete data privacy, interoperability, and orchestration of connected devices. The functions of blockchain in IoT are shown in Figure 4. There are many blockchain platforms available right now. The common consensus methods include practise byzantine fault tolerant (PBFT), proof of work (POW), proof of stake (POS), and IOTA (Tangle). We contrast and evaluate these popular blockchain systems and consensus algorithms functionality, security, and suitability for IoT situations. Makhdoom et al. [36] analysed the challenges and potential of blockchain and IoT integration. They concluded that the major difficulty is caused by the excessively rapid growth of IoT devices and the strength of transaction concurrency. The IoT's performance requirements are still not met by the current blockchain networks' performance. Preliminary study was done by Yi et al. [37] on both established and novel consensus techniques. They recommended Tender mint's implementation of Ether mint as an appropriate option for the IoT platform's blockchain technology. We are able to offer a large number of nodes, quick consensus (based on the BFT consensus algorithm), no transaction fees, and robust scalability—these are the four qualities for smart contracts that are suitable for Iot networks.

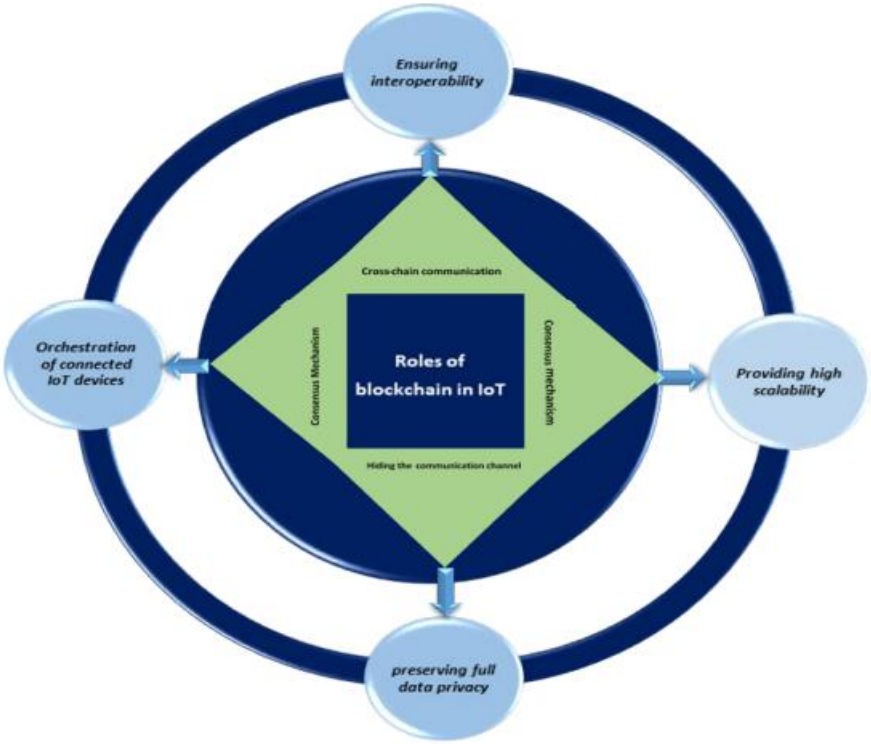

Figure 4: The role of blockchain in IoT applications.

Table 3 compares the blockchain development platforms currently in use for the IoT applications described in this section. The majority of platforms support smart contracts, which enable the extension of application logic beyond cryptocurrency transactions. Python, Java Script, and C++ are the most popular programming languages, and PoW and PBT are the most often used consensus techniques. The majority of platforms allow for both public and consortium rights, allowing for the creation of both global and consortium applications. Consensus algorithms are actually the key components that govern the block rates, consistency, scalability,

and security of blockchain-based IoT systems. Consensus methods based on PoW are thought to be the most secure in open networks. Pow, on the other hand, completely prohibits the idea of block mining on IoT devices due to its high computing requirements. High block generation speeds for IoT systems can be achieved with PBFT-based consensus techniques for private blockchains, although they have a lower participation rate for miners [38].

Table 3: Blockchain platforms.

Platform	Blockchain	Popularity & Active	Consensus Algorithm
Bitcoin	Public	High	PoW
Ethereum	Public and permissioned	High	PoW, PoS GHOST
Hyberledeger-Fabric	Private, Permissioned	High	PBTF
Multichain	Private, Permissioned	Medium	PBTF
Quorum	Public, Permissioned	High	Raft, IBFT
Lisk	Public and permissioned	Medium	DPoS
LiteCoin	Public	Low	Scrypt
HDAC	Public and permissioned	Low	EPoW
IOTA	Public, Permissioned	Low	PoW, TANGLE

The designed blockchain structure is shown in Figure 5. The blockchain structure of each side-chain varies depending on the platform it uses. As opposed to a continuous chain design.Each sub chain's responsibility is to keep track of sensor data generating activitiesin charge of keeping track of successful and unsuccessful data access requests made by one consortium member to another.

Our methodology also works with direct M2M transactions, a cutting-edge micropayment business model where IoT devices can start financial transactions and can get data from other IoT entities to maximise their functionality. In order to minimise significant harm from data centre failures to the overall IoT system, the model also includes trust mechanisms between devices.

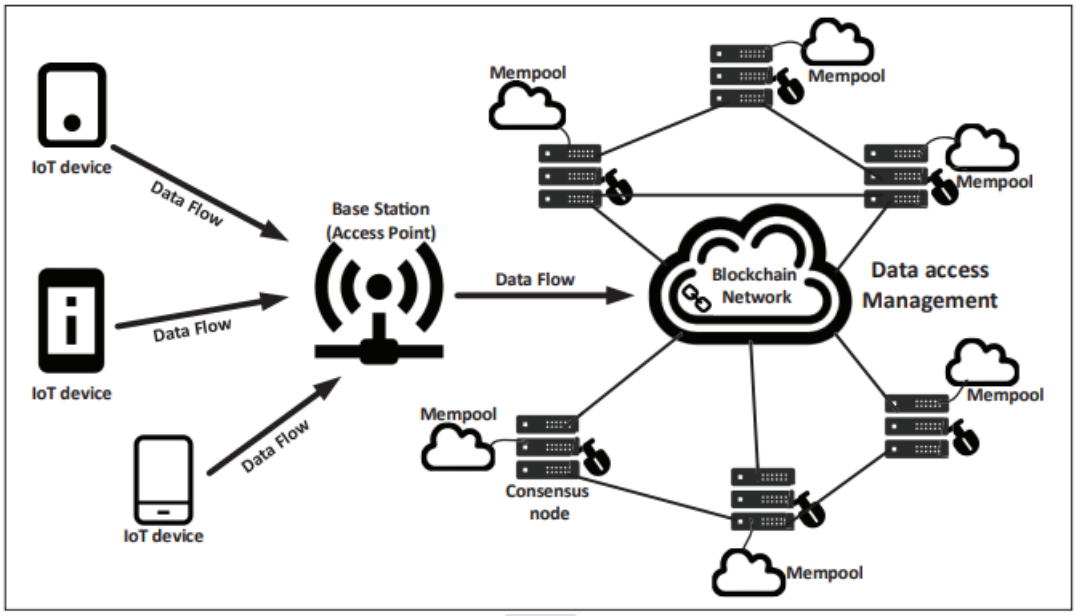

Figure 5: Schematics of blockchain-based transaction (data) transmission for IoT systems.

The blockchain networks can receive transactions from IoT devices sensing data. In the meantime, the IoT device must pay the transaction fee to cover the cost of the peer nodes energy usage in blockchain networks. From the standpoint of an IoT device, the blockchain may be thought of as a decentralised platform as a service. In many IoT applications, such as sensing data transmission in crowdsensing and power data transfer in smart grid, the proposed case study of data transmission can be utilised simply. The access point serves as the secondary receiver in a D2D connection with the SU, or the IoT device, as depicted in Figure 5.

5. Conclusion

We propose a cross-chain integration mechanism in this study to manage IoT data across several blockchains.We suggest a data access control paradigm and develop.We run tests to determine how effective our framework is. The experimental findings demonstrate that our framework is appropriate for managing IoT devices with minimal resources and that it is simple to deploy in IoT scenarios among various consortia. Furthermore, compared to the typical blockchain structure, our solution is more effective. We must give up some decentralisation relative to the current public blockchain topologies because of the centralization of the Tangle based on the coordinator compass deployment. The experiment has not yet been implemented on actual IoT devices; instead, it is based on software simulations. Crypto currency, in our opinion, will be crucial for Internet of Things applications. Developments in blockchain technology and how they might be used in IoT applications to enhance life satisfaction are hot topics in today's research community. However, there are a variety of issues and necessary restrictions that need to be looked into and resolved before using blockchain technology in Iot systems. Future applications for blockchain and artificial intelligence are very promising.The same is presumably true for the solutions and uses for blockchain and AI that include both technologies. On the one hand, there are approaches that leverage the blockchain to enable AI systems or to deal with the related challenges (blockchain for AI). In contrast, applications in the field of AI for blockchain aim to use AI and machine learning techniques to help solve blockchain-related problems.