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

# A Bibliometric Analysis of Blockchain Use for the RPL Technology: A Systematic Literature Review

**Joshua Teddy Ibibo**

School of Computing, Edinburgh Napier University 10 Colinton Rd, Edinburgh EH10 5DT, United Kingdom

**Abstract:** ***Internet of Things (IoT) has been the most emerging technology in the last two decade because the number of smart intelligent sensors and its associated technologies has rapidly grown in both industrial and research prospectives. Recent trends have suggested convergence to WSNs becoming IPv6based. To this effect, the ROLL working group of the IETF is currently specifying an IPv6based unicast routing protocol for WSNs, denoted IPv6 Routing Protocol for Low power and Lossy Networks (RPL) of low power consumption, and other constraints of nodes in the network. In this study, we performed a Systematic Literature Review, evaluate, and identify the security issues that exist in the RPL network. Second, identity the use of blockchain technology in protecting the nodes in RPL network. Thirdly, as per blockchain technology, we provide some security solutions and provide robot blockchain taxonomy. The detailed analysis, including enabling technology and integration of IoT technologies, is explained. We review relevant works that have proposed Blockchain based solution to strength the security of RPL network. We further contribute to present, analyze, and compare best authentication solutions. Also, we present the solutions that integrate Blockchain. Finally, several research directions and open challenges are identified.***

**Keywords:** RPL, Blockchain, Attacks, IoT, Smart Contract

## 1. Introduction

The lightning fast development of miniaturized, electronic, and wireless communication technologies have all played a role in the incredible progress that our civilization has made. As a consequence of this, the number of electronic devices that are appropriate for use in many different domains has increased, the costs associated with their manufacturing have decreased, and there has been a paradigm shift from the physical world into the digital world. As a result, the manner in which we connect with one another and with the surrounding environment has changed as a direct result of our increased use of modern technology in an effort to acquire a deeper comprehension of the universe. The Internet of Things (IoT) is a collection of technologies, ranging from Wireless Sensor Networks (WSN) to Radio Frequency Identification (RFID), that enable the ability to perceive, interact with, and communicate over the Internet [1]. These technologies have come together to form what is known as the Internet of Things (IoT). IoT envisions a fully interconnected world in which physical objects are able to exchange data that they have measured and engage in conversation with one another. Because of this, it is now feasible to create a digital representation of the physical environment, which paves the way for the development of a wide range of intelligent applications that can be used in a number of different fields. These include things like smart cities, smart homes, smart wearables, smart healthcare, smart automobiles, smart grids, smart water, and smart environments, among other things. IoT solutions are now being implemented across a wide variety of domains, with the goals of enhancing productivity and digitizing various sectors. Applications that run on the IoT have extremely particular features; for example, they produce massive amounts of data, and they need to be connected to the internet and powered up for extended periods of time. This, in addition to the restrictions placed on memory, the capacity of computers and networks, and the amount of power that can be supplied, creates a significant number of difficulties. The massive growth of the IoT has to be backed up by standard methods and protocols in order to bring the level of heterogeneity that already exists in the field down to a more manageable level. This heterogeneity results in the formation of vertical silos and slows down the adoption of the internet of things. In spite of this, the IoT presents a number of obstacles, the most prominent of which is the heterogeneity of its components and the difficulty of integrating them. In addition, the data generated by these devices must also be trusted. The latest advances point in the direction of WSNs moving toward an IPv6based convergence. In light of this, the ROLL working group of the IETF is in the process of defining an IPv6based unicast routing protocol for WSNs. This protocol will be known as the IPv6 Routing Protocol for Low power and Lossy Networks (RPL), and it will minimize the amount of power that individual nodes in the network use [2]. The most recent research on RPL, which is presented in [2], only supports unicast trafic. However, RPL does not expressly offer support for any type of ”optimized broadcasting, ” which refers to the process of delivering the same data packet to all routers that are part of the WSN. In a wireless sensor network (WSN), one of the most essential applications of broadcasting is for a controller to request that all of the sensors in the WSN send their sensor information. This may be done, for example, to determine whether or not an alarming situation that was indicated by a single sensor is corroborated by other sensors in the WSN. Even if such a ”broadcast” might be achieved by the DODAG root conducting ”bulkunicast” to all of the sensors in the network, doing so would hardly be considered efficient since it would include the transmission of the identical packets more than once. The IoT, which is the parent network that links to other networks, is what provides low power and lossy networks its extensive diffusion (LLN). As was said earlier, various different industries have begun to implement internet linked IoT networks. These networks are made up of embedded sensors and intelligent devices and are connected to the internet. The RPL network’s performance and resource restrictions might be undermined by several

assaults, resulting to erroneous output from some network nodes, which in turn affects the network's topology as a whole.

In this research, we analyze and evaluate the current tactics being used in the area, as well as explore the most recent defenses and how to put them into use. The research will also highlight how trust based defenses using blockchain technology have recently been used to halt and detect topological assaults, as well as assessments and analyses of current tactics against common attacks on IoT devices like the RPL routing protocol's security vulnerability. Because blockchain technologies are able to monitor, coordinate, conduct transactions, and store information from a wide number of devices, they make it possible to develop apps that do not rely on a centralized cloud. Some businesses, such as IBM, have gone even farther and are discussing blockchain as a potential technology for democratizing the future IoT, due to the fact that it tackles the most pressing concerns now preventing its widespread adoption: An additional factor that contributes to a lack of confidence is the use of closed source code. When designing the next generation of IoT solutions, it is important to keep in mind the need of openness in order to boost both trust and security; hence, open source methodologies should be taken into consideration. It is important to note that open source code, just like closed source code, is still susceptible to bugs and exploits; however, because it can be monitored constantly by a large number of users, it is less likely to be modified maliciously by third parties. Despite this, many IoT solutions are still expensive due to the costs associated with the deployment and maintenance of centralized clouds and server farms. When a provider does not construct such an infrastructure themselves, the expense of it is transferred to intermediaries.

In the next sections of this essay, we will go further into the aforementioned topics and analyze how a comprehensive RPL security plan necessitates the inclusion of all of these aspects. There are a few existing studies on security challenges in ad hoc networks, and you can find them in [3, 4]. However, only a tiny fraction of each of these surveys focuses on blockchain in RPL. A recent study that provided an outline of the security concerns in RPL also included an assessment of the security issues in mobile ad hoc networks [5]. Nevertheless, the essay did not cover any topics related to cryptography or intrusion detection.

In addition, it only incorporated a tiny percentage of the existing literature on the subject of security in WSNs.

The main contributions of the paper are: In view of prior review, we aim to:

1) Provide a theoretical introduction to the RPL routing protocol and the blockchain technology;
2) Provide an in depth examination on the possibilities of adopting blockchain technology into the RPL protocol.
3) Elucidate the ways in which blockchain technology is being used in the RPL routing system.
4) A review and analysis of the blockchain technology, focusing particularly on its distinguishing characteristics and the outstanding questions it raises for RPL.
5) An investigation of the difficulties, possible advantages, and unanswered questions posed by the combination of blockchain technology and RPL

## 2. Blockchain and RPL Related Work

Despite this, the blockchain technology was not included at any point throughout the process. The authors in [6, 7, 8, 9, 10] highlight the domains of block chain based IoT security, while the authors in [11] give particular topics for blockchain based IoT solutions and the issues involved. They also present a summary of current research on the comprehensive decentralization of IoT through blockchains. The authors of [12] discuss contemporary research efforts for several sectors of application such as smart city, smart grids, and other similar topics. The authors of the article [13] give a study that discusses the many architectural approaches that may be used to incorporate blockchains into the internet of things. The authors [14] provide the results of an indepth investigation of the principles of networking that are involved in publicly distributed blockchains, including possible attacks and design compromises. In addition to this, they highlight the need for formal models to resolve design tradeoffs when creating public blockchains. The authors' contributions are interested in blockchain taxonomy and decentralized consensus [15, 16], as well as problems and research direction for blockchain for IoT [17, 18, 19, 20, 21, 22]. There have been a number of studies, including those [23, 24, 25, 26, 27] that presented an overview and taxonomy of attacks against RPL, that have indicated that RPL may be the target of a variety of DoS assaults. For Wireless Sensor Networks (WSN) and RPL based Internet of Things networks, a number of Intrusion Detection Systems (IDS) were also recommended [28, 29]. Both the paper by [30] and other prior work [27] include reviews of intrusion detection systems (IDSes) for the internet of things. Concerns around power consumption and latency were at the forefront of [31] research agenda. They presented a straightforward authentication mechanism based on a decentralized blockchain that might be used in a smart hospital. Authentication between devices and between devices and fog nodes may be guaranteed with the help of the proposed strategy, which utilizes a fog computing architecture. The authors also took use of the blockchain technology in order to benefit from the decentralized structure and cryptographic capabilities of the platform. The outcomes of the evaluation that were gathered show that making use of a fog architecture may help to speed up the process of preparing and transmitting an authentication request. Despite this, Khalid and his colleagues did not provide a formal verification of the proposed system.

A straightforward framework for authentication and authorization was given by Tahir et al. [32]. They used a probabilistic model for blockchain based Internet of Things networks. When it came time to do the authentication step, Tahir et al. made use of random numbers while taking into consideration both the homogeneous and heterogeneous IoT device types. They also focused on developing a fog computing architecture as a means to circumvent the limitations imposed by the blockchain. The authors of the study put the suggested method through its paces by using both the AVISPA (Automated Validation of Internet Security Protocols and Applications) tool as well as the

Cooja simulator. However, they did not reveal any of the recommended scheme's informal verification information. Kumari et al. [33] proposed the establishment of a decentralized, peer to peer trading platform for energy that would be built on the Ethereum blockchain. The primary objective of this tactic was to decrease the quantity of power generated by the grid in order to boost earnings for both prosumers and consumers alike. The authors evaluated the proposed method taking into consideration the data transfer rate, scalability, and cost of storage. The findings indicated that the strategy may be considered to have been effective. Current authentication methods are susceptible to adversarial attacks as a consequence of their dependence on a limited number of servers and a centralized authority for the networkwide registration and authentication of Internet of Things devices (IoT). [34] Utilizing blockchain technology, develop a decentralized authentication system that may be used for peer to peer Internet of Things networks. A network architecture that combines Internet of Things and cloud services should be able to benefit from the scheme by having more secure device authentication. The development of security problems among open sessions is giving those in the Internet of Things ecosystem cause for rising anxiety. Continuous authentication was developed to be a more effective authentication method than its predecessors by continuously validating the identities of users on an ongoing basis and identifying the precise moment an unauthorized attacker took control of the session. Having said that, there are still a lot of issues that need to be fixed. [35] plans to investigate the feasibility of using blockchain technology to provide the Internet of Things with continuous and real time authentication.

Existing analysis on the use of blockchain technology in a variety of domains has been provided by a number of writers. For instance, in [36, 37, 38], a comprehensive explanation of the principles of blockchain technology and smart contracts is offered, in addition to a helpful overview of the deployment and usage of BIoT solutions. The article does not go into depth about the attributes of the ideal BIoT architecture or about possible optimizations that may be made to generate BIoT applications. Despite the fact that it provides a lot of valuable information, the study does not go into detail on these topics. Despite the fact that it does not particularly address the ways in which blockchain technology may be used to the Internet of Things, [39] provides an interesting new piece of work. In that section, the writers provide an outline of the architecture as well as the numerous procedures that are involved in blockchain technology. In a manner similar to that of [27], [40] provides overviews of blockchain written by a range of academics while highlighting the technology's use in a variety of Big Data domains and industrial applications. A concluding remark is necessary for the systematic reviews that are described in [41] and [42], which investigate the topics that papers in the existing body of research that suggest the use of blockchain typically cover.

## 3. Literature Background

### 3.1 RPL Routing Protocol

A structure known as a Destination Oriented Directed Acyclic Graph (DODAG) is used by the RPL to facilitate the organization of resource constrained nodes included inside an LLN. The DODAG's root is represented by a Border Router (BR) that is always operational and functions in a manner similar to that of a gateway. Directed acyclic graphs (DAGs) are created by RPL in accordance with the Objective Function (OF). These DAGs are rooted at the sink, and they aim to reduce the amount of money spent traveling to the sink from any network node. It's possible that the objective of the OF is to bring down a certain measurement, such the hop count or the ETX (Expected Transmission count) [36]. A metric list may be found in reference [37], which can be accessed here. In order to build the routing topology in a manner that is compatible with the many different link/node metrics and limitations, the routing protocol has been designed with a high degree of flexibility and supports a wide range of OFs. This has been done in order to facilitate the construction of the routing topology. This is due to the fact that RPL might be used in a diverse assortment of contexts. Messages referred to as DAG Information Option (DIO) are started to be sent by the root of the DAG. Details such as the OF, DAGID, and rank of the broadcasting node are included in the DIO messages. The rank of the node is roughly equivalent to the node's distance from the backbone network. Any node that is connected to a backbone network or a node that is not part of an RPL implementation is eligible to perform the duties of a root or LBR (LLN Border Router), and it is given the rank of 1. When a node has obtained a DIO, it calculates its rank by taking into account both the position it held in the DIO and the amount of distance it needs to travel to reach the node in question. RPL offers a number of different rules for parent selection, and these rules are contingent on a number of different criteria, including the declared OF, the route cost, the rank, and the local quality of the connections. A potential parent is any other node in the tree that has a higher rank than the node being discussed [37].

When a node broadcasts its DIO, that node shares information with other nodes about its rank, its operating function, and the DAG it has joined. When a node joins the network, it has the option of either waiting to receive a DIO or alternatively multicasting a solicitation message known as the DIS. This causes the other nodes to start sending DIOs and enables the newly joined node to join the DAG. Additionally, in order to advertise their addresses and prefixes, nodes multicast Destination Advertisement Options, commonly known as DAOs, to the DAG parents of which they are children. When these DAOs are received, the nodes change the routing table in their own databases. When there is no entry in the routing table that corresponds to the destination, or when there is trafic destined for the root, a node will send a packet to the parent that it considers to be its most desirable. It is important to keep in mind that in order to stop a routing route loop from occurring, a node must not forward packets that have been routed further up the DAG to a node that has a higher rank. In the event that a parent is unable to receive the data, the node has the ability to transmit it to a sibling, which is defined as another node with the same rank. In this fashion, the packet goes up in the DAG until it reaches a parent that is shared by both the source and the destination for P2P routing, and then it moves down to the destination. As a consequence of the LBR

routinely transmitting DIO with a new sequence number (DAG Sequence Number), the DAG will be regenerated, and any broken connections will be repaired. When a node encounters a DIO that has a higher sequence number, it repeats the parent selection process based on the updated link cost and confidence in the parents. This provides the node with a better route to the root for the subsequent iteration. It is also helpful in the search for a parent in the case that a node's parent list becomes depleted as a consequence of failed probes or low confidence in the results of the probes. The method described above for resolving link discontinuity and discovering a new parent does, however, require a significant investment of work on the part of the researcher. When a connection between a parent and child has been corrupted or severed, the kid is obligated to wait for a new DAG Sequence Number to be generated [2]. During this pause in activity on the part of the youngster, which might extend for a few minutes or many hours, the situation will eventually resolve itself. A local repair method has been devised in order to address the problem of a node's inability to contact the DAG root via a route. This issue was brought to light when the node in question had connectivity issues. A "Poison" message is sent by the node as the initial step in the process of informing the children of the node about new parents. After that, it sends a DIS message so that when it gets a DIO from another node, it may join that node as its parent if the DIO was sent by that other node. With this approach, the only node that has to update its parent table is the one that does not have a route to the DAG root, and only a section of that node's subgraph needs to be edited as well. The problem is handled locally, so there is no need to wait for a global repair.

One root node and a number of sensor nodes are responsible for supporting each DODAG. The root node has the lowest possible rank, which is one. The sink node, also known as the root, is most often used to refer to the gateway that links the LLN to the IPv6 network. The construction of a DODAG is shown in Fig.1 as being handled by the root node of the RPL Network Topology. Additionally, a new DODAG is built at the root node, and it travels downhill to the leaf nodes.

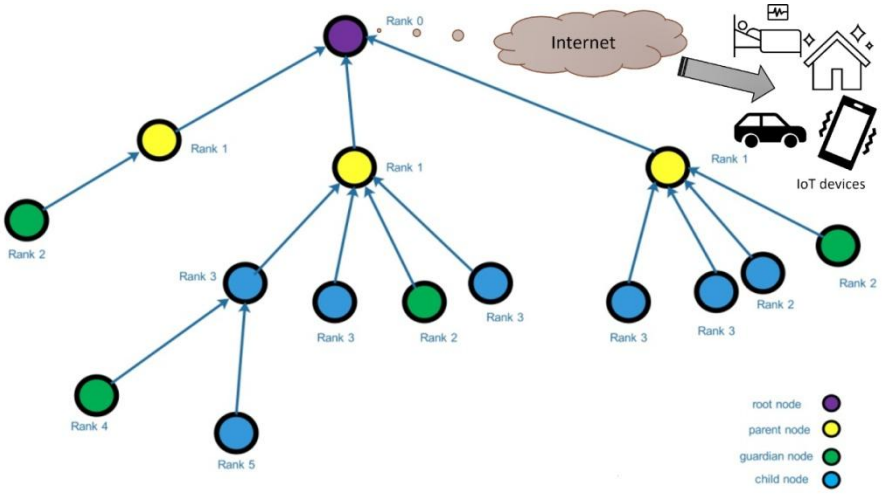


**Figure 1:** Shows the RPL network topology

The DODAG ID, the DODAG version number, the RPL instance ID, and the rank are the four key factors that identify a DODAG. DODAG ID is an identification that is differentiated from other identifiers by the IPv6 address of the root node. An identification for an RPL instance is referred to as an RPL Instance ID. An RPL instance is a network that might be made up of a single DODAG or several DODAGs. Multiple instances of RPL may operate simultaneously over a network, but despite this, they are conceptually distinct from one another. As can be seen in Figure 2, a node can only be a member of a single DODAG inside an instance, despite the fact that it may connect to many RPL instances. Within each DODAG, the nodes are connected to one another in a treelike fashion in line with the rankings that they have. The rank of each node in the DODAG tree indicates its location with respect to the node that serves as the tree's root.

### 3.2 Routing for Low Power and Lossy Network (RPL) Rank

A node's position within the DODAG is represented by its rank, which is an integer value. When traveling downstream through the DAG, the rank will grow, but it will fall when traveling upstream. Loops may be avoided and found more easily using RPL thanks to the use of rank in the language.

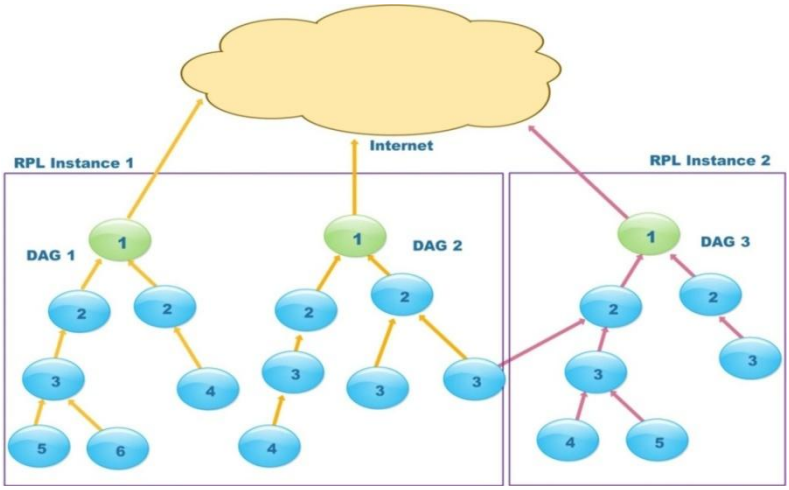


**Figure 2:** Shows the DODAG per instance

Nodes in a DODAG make use of the rank feature in order to differentiate themselves from both their parents and siblings. The nodes in a directed acyclic graph (DAG) that are next to a given node and have the same rank as it are referred to as that node's siblings. In most situations, the relationship between siblings is not represented in the DAG, and it is not always the case that siblings have the same father. A node with a higher rank that is attached to an adjacent node with a lower rank is referred to as a child (kid) node. This is because the child node has a higher rank. The rank of each RPL instance is calculated based on an Objective Function (OF) that has been specified in advance. RPL use OF as a measurement instrument in order to plot the most direct path to the source of the problem. In addition to discussing how to choose routes in a DODAG and optimize them, the OF explains how RPL nodes convert one or more metrics into rankings. The IETF ROLL workgroup has created two objective functions for the RPL protocol: the Minimum Rank with a Hysteresis Objective Function (MRHOF) RFC 6719 and the Objective Function Zero (OF0) RFC 6552. These two documents may be found in the RFC series. While MRHOF uses the ETX metric, OF0 uses the statistic known as "minimum hop counts" to choose the best parent and path to take.

### 3.3 Routing for Low Power and Lossy Network (RPL)Control Messages

RPL messages are described as a new form of Internet Control Message Protocol version 6 (ICMPv6) control messages. These messages have a structure that consists of three elements: form, Code, and Checksum. The structure of these fields may be seen in Figure 3 (A). The kind field is used to specify the kind of ICMPv6 control message being sent. The code field is used to identify the kind of RPL control message being sent. The checksum field is calculated in accordance with the guidelines outlined in [RFC4443].

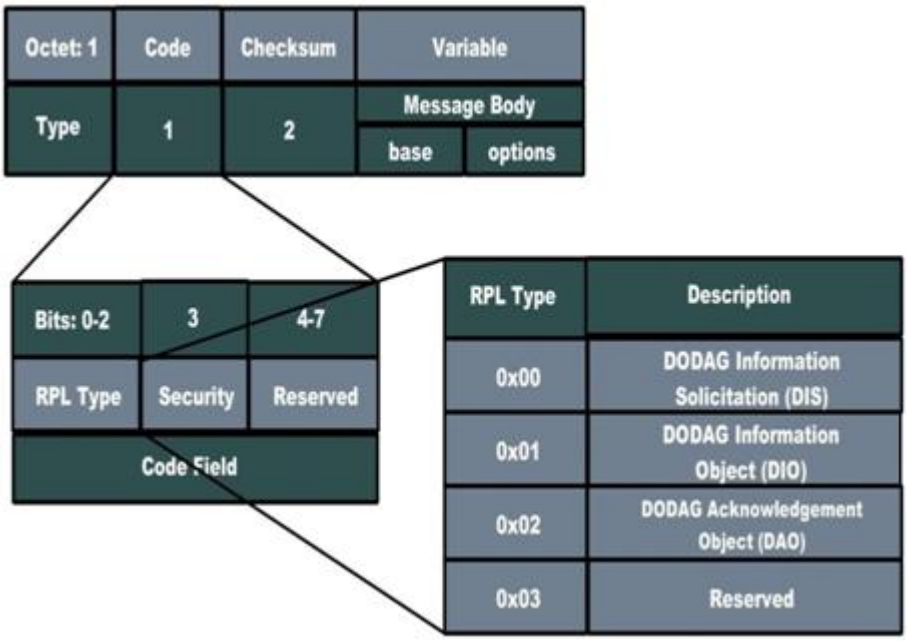


**Figure 3:** A. Shows the RPL Control Message, (Gaddour and Koubˆaa, 2012)

When requesting a DIO from an RPL node, the DIS message, which has the value 0x00 in hexadecimal, is the one that should be sent. When investigating neighbor nodes in neighboring DODAGs, you may make use of the DIS to

do so. In order to become part of the DODAG, a newly joined node must first broadcast DIS packets via multicast. The root transmits a DIO message that is multicast over the DODAG structure, which has the address 0x01 allocated to it. This action creates a new DAG. A node has to be able to discover an RPL instance, comprehend the setup settings of the instance, choose a DODAG parent set, and continue to maintain the DODAG. The DIO packet provides the important network data that a node requires. DIO is transmitted on a regular basis in order to facilitate connections between other nodes and the DODAG. The DAO message, which has the address 0x02, is used to convey information about the reverse route, which records the nodes that were traversed on the upward voyage. This information is utilized to reconstruct the path taken by the message. Aside from the DODAG root, every node in the network is responsible for sending DAO messages in order to alert their parents of their addresses and prefixes, as well as to update the routing tables with the prefixes of their offspring's prefixes. Once this DAO packet has been sent, a full route between the node and the DODAG root will have been created. A DAO packet is multiplexed in the opposite direction, from the destination to the source, whenever there is a route update. In order to acknowledge receipt of a unicast DAO packet, a DAO receiver (also known as a parent or DODAG root) must send out a DAOACK packet. See Fig.3 (B).

### 3.4 Building a DODAG in RPL

When constructing a DODAG, the process will begin at the root node OR LLN Border Router (LBR) from the gateway to the Internet. Many LBRs may exist in the network when a new ICMPv6 control message is sent for an RPL, such as DIO, DAO, or DIS. NOTE: The primary goal of RPL is to offer interoperability with IPV6 and to improve power consumption by removing loops in the network.

### 3.5 RPL Security Mechanisms

RPL is equipped with three primary options for its security mechanisms:

1) Unsecured when it comes to the transmission of RPL control messages, this system does not make use of any extra safety precautions.

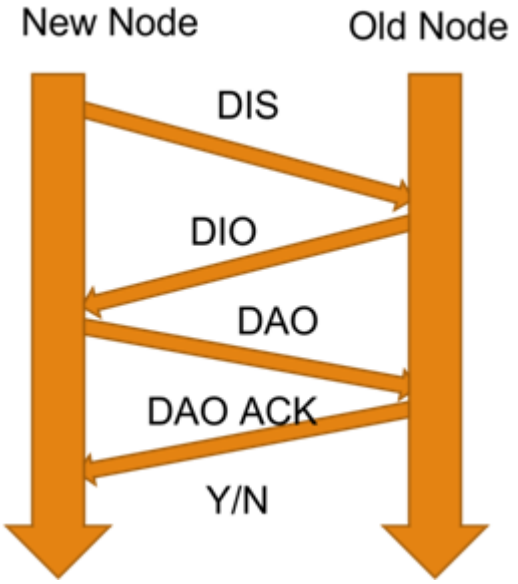


**Figure 4:** B. Shows the RPL Control Message

2) Preinstalled When a node joins an RPL instance using this mode, the keys necessary to process and output encrypted RPL messages are already preinstalled on the node, thus the node is able to do so immediately after joining.

**Authenticated**
Nodes that are operating in authorized mode contain preinstalled keys that are very similar to those that are operating in preinstalled mode; however, these nodes may only be used to join an RPL instance as a leaf node. However, the RPL defines a security method to protect against assaults from the outside on its routing control messages and topology. However, the RPL makes it very apparent that adopting this security mechanism is not mandatory.

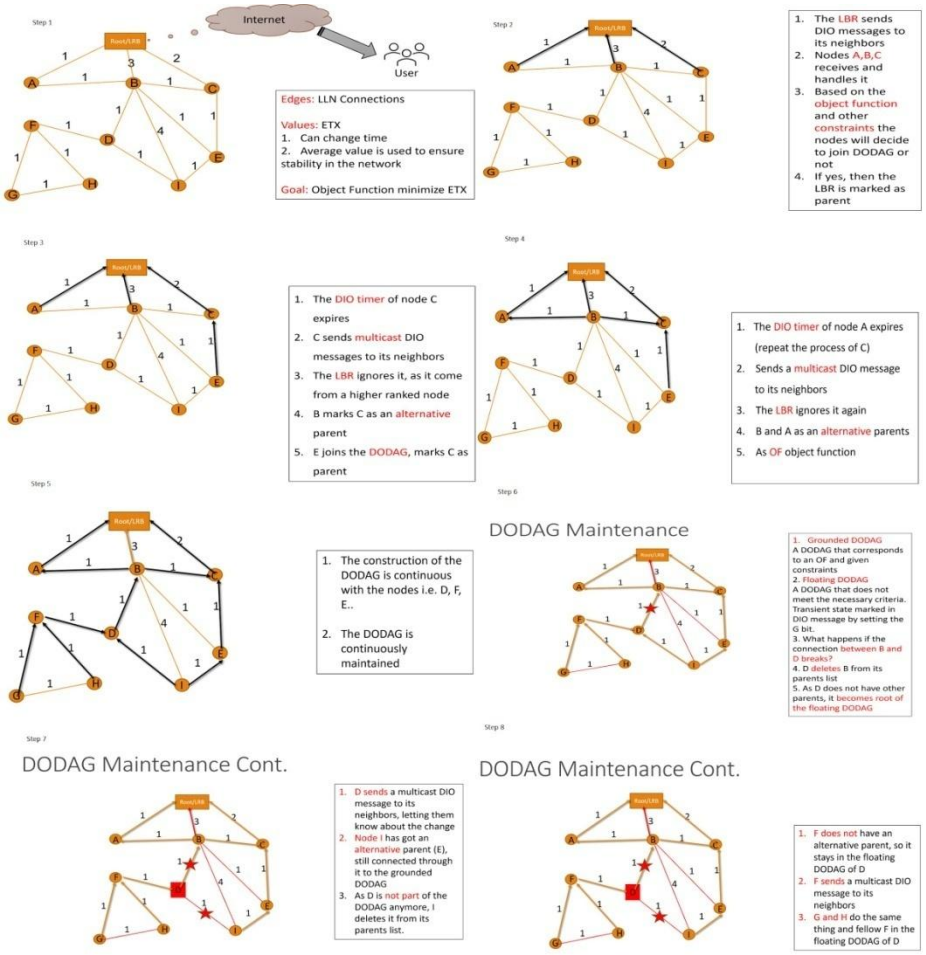


**Figure 5:** Part A: An example of how a DODAG construction is built and maintained.

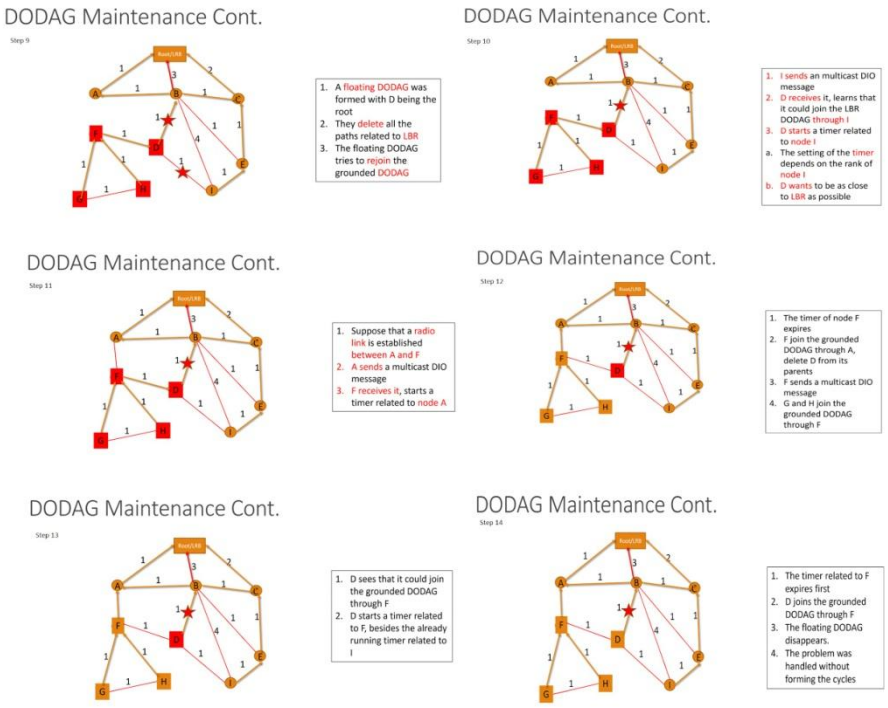


**Figure 6:** Part B: An example of how a DODAG construction is built and maintained

### 3.6 RPL Communication Model

RPL is capable of supporting three different communication models, which are as follows:

1) Point To Point (P2P) The point to point (P2P) routing capabilities offered by RPL may be used between any two nodes in the DODAG. i.e. In order to support peer to peer communication in an RPL network, an LBR must have the capability to transit packets prior to the packets being source routed to their respective

destinations.

2) Multi Point to Point (MP2P)
The vast majority of LLN applications make use of MP2P traffic as their principal flow of traffic. The vast majority of MP2P traffic is directed toward the border routers, which are critical nodes in the network architecture and serve as an interface for establishing connections to the Internet.
3) Point To Multi Point (P2MP)
The Point to Multi point Process is another word that is used in RPL. This process refers to trafic that is transferred from the root downstream to a number of nodes.

### 3.7 RPL Network Attacks

Due to deployment and resource limits, some more Internet of Things devices have been forced to function on reduced power. These constraints include the battery, storage capacity, memory, bandwidth, processing capabilities, and, most crucially, human interactions with these Internet of Things devices. As a direct consequence of this, the security mechanisms are rendered ineffective, and the devices become targets of cyber attacks. Attacks on RPL networks need to be categorized and ranked in order of priority, according to the impact they have on the topological network, in order to facilitate the development of efficient security solutions. These kinds of assaults have been broken down into three primary categories: resources, network, and trafic assaults.

1) Resources Based Attack (RBA) Are those kinds of attacks that force lawful nodes to carry out processing that is not necessary in an attempt to deplete their capabilities. The objective of this class of attacks is to deplete the node's resources, such as its battery, memory, and computing power. This kind of assault is composed of two parts: the direct RBA and the indirect RBA. Internal assaults are also known as flooding attacks, and they occur when a malicious node tries to do damage to the network by overloading it. The term "external attack, " on the other hand, refers to assaults such as version number attacks, DAG inconsistency attacks, and enhanced rank attacks, all of which involve the attacker using other nodes in order to build a large amount of network.
2) Network Based Attack (NBA) A family of attacks known as NBA, which may exploit the RPL protocol and target the network topology, can also target the network. Because of the attacker, the normal operation of the network is disrupted in a number of different ways. One of these ways is that the topology is less ideal than it would be during the normal integration of the network, and another is that a group of RPL nodes is isolated. In spite of this, there are two distinct types of NBA operations: suboptimization and solitary attacks. Sinkhole, Routing Information Replay, and Worst Parent Attacks are all examples of suboptimization attacks. These types of attacks cause the infrastructure to not converge towards the ideal shape (for example, ideal connections), which in turn results in below average network performance. During an isolating attack, a node in the RPL network, or a selection of nodes, will interface with the parent or root node either not at all or just partly. This includes Blackhole Attacks, Selective Forwarding Attacks, and DAO Inconsistency Attacks in Storing Mode.
3) Traffic Based Attack (TBA) A traffic based attack, also known as a TBA, is an attempt to get routing information by examining the characteristics and behaviors of something like the data that is being sent across a connection. This is the last form of attack that may be made against the RPL network architecture. In a way similar to that of a sniffe attack, the identification of parent child relationships attempts to acquire information about the RPL structure, such as its murky topology. The most common kinds of incidents that fall under this category are eavesdropping and theft related attacks.

### 3.8 Blockchain Technology

In 2008, Satoshi Nakamoto issued a paper in which he described his invention of Blockchain. Since that time, a number of computer programmers, cryptographers, and other scientists have been working on the idea of Blockchain in order to develop a cryptocurrency network known as Bitcoin [43]. Although blockchain started out as a tool for cryptocurrencies, it is not required to create a cryptocurrency in order to utilize a blockchain or to construct decentralized apps [43, 44]. Blockchain was first developed as a tool for digital currencies. A blockchain is exactly what it sounds like: a chain of blocks that have been timestamped and are linked together using cryptographic hashes. The following sections will discuss the fundamental qualities and operations of a blockchain in order to familiarize the reader with its inner workings and provide context. In a peer to peer (P2P) network, transactions are sent along, and some peers, known as miners, compile a batch of these transactions into a data structure known as a block. Once a new block has been compiled, it is sent across the P2P network, and if it is found to be legitimate, it is added to the chain of the blockchain's most recent completed block. Because each block has a link to the one that came before it, the overall structure is referred to as a blockchain. Once a certain amount of time has passed and a block has been saved to the blockchain, the transactions included inside the block are regarded as confirmed. A block is considered to be genuine if it has valid transactions and if miners have successfully solved a computationally difficult problem. This puzzle requires them to obtain a hash of the block that is less than a predetermined threshold. The miner who is first to build a valid block and find a valid solution to the puzzle will be the one to add the next block to the blockchain. This miner will be the one to add the next block to the network. The name given to this particular kind of mining is "Proof of Work. " The Proof of Work mechanism makes it possible to reach distributed consensus, which indicates that all of the nodes in the network have come to an agreement on the same version of the blockchain and that this version of the blockchain includes legitimate transactions. There is a possibility that this sequence of blocks could experience forks, which means that the chain will split into two distinct branches. However, as a result of Proof of Work, at some point in the future, one of the branches is going to be abandoned, and all of the nodes are going to concur on the same blockchain. In the event that the blockchain splits,

miners are required to extend the branch that is either the farthest along or has the most challenging Proof of Work. In addition, since it is secured via Proof of Work, the blockchain is very difficult to manipulate [41].

A blockchain contains a record of all transactions that have ever been made, and it is constantly updated as new ones are processed. All of the nodes in the network will check the validity of a newly created block whenever a new block is added to the chain. Through the use of an inverted reference that points to the previous block as its parent, a verified block will be added on to the end of the blockchain in an automated fashion. Since the hash value of the block that has been tampered with is considerably different from that of the block that has not been tampered with, any illegal changes that have been made to the block that has been created in the past may be quickly discovered using this method. Additionally, due to the fact that the blockchain is dispersed throughout the whole network, the behavior of tampering may also be readily recognized by other nodes in the network [42].

### 3.9 Blockchain Types

Public Blockchains, Private Blockchains, and Consortium Blockchains are the three primary categories of blockchains. These categories are based on the controlled data, the availability of such data, and the activities that may be carried out by a user.

1) Public Blockchain Public blockchains are completely decentralized in the sense that all members may contribute to the publication of new blocks and access the contents of the blockchain. Anyone is able to keep a copy of the public blockchain and participate in verifying new blocks, which is why this kind of blockchain is referred to as a permissionless or public blockchain. Devices participating in public blockchain networks have the option of actively validating newly created blocks or merely issuing transactions inside the ledger itself. Because public blockchains are intended to support the participation of a large number of nodes that remain anonymous, it is vital to take precautions against the possibility of malevolent activity. Solving a computationally dificult problem or staking one's own coin is required in order to publish new blocks on a public blockchain. Each transaction has a processing fee connected to it, which acts as an incentive for the peers who are striving to publish new blocks into the blockchain. since of this, it is impossible to hack the public blockchain since changing its data would require an excessive amount of resources. Every transaction contains a transaction fee as an incentive for the peer who verifies the transaction into a new block. This is due to the fact that thousands of other peers are engaged in the decentralized consensus. Some examples of this kind of blockchain include Ethereum, Hybrid Ledger Fabric, IOTA, and others such as Bitcoin.
2) Private Blockchains Private blockchains, in contrast to public blockchains, are governed by permissions, and every node that joins the network is a known member of a single organization. Private blockchains are best suited for use inside a single company or organization. They function as synchronized distributed databases that are designed to monitor and record the data transfers that take place between various groups of employees or persons. It is not necessary to use any kind of money or tokens in order for private blockchains to work, and there are no transaction costs associated with using private blockchains either. It is possible for an organization to roll back its blockchain to any time in the past since blocks in a private blockchain are published by delegated nodes inside the network. This makes a private blockchain less tamper resistant than a public blockchain.
3) Consortium Blockchains In the same way as private blockchains are permissioned networks, so too are consortium blockchains, which are also referred to as federated blockchains. Consortium networks cross the boundaries of different organizations and contribute to the upkeep of transparency among the various parties involved. The participating members of a consortium may utilize an auditable and reliably synchronized distributed database called a consortium blockchain. This database is intended to keep track of the data transactions that take place between the members of the consortium. A consortium blockchain operates in the same manner as a private blockchain in that there are no processing fees required, and publishing new blocks does not need a significant amount of computing resources. It is neither completely decentralized nor is it immune to censorship [45], despite the fact that it provides enable auditability and decreased latency in the processing of transactions.

**Smart Contract**

N. Szabo [46] first proposed the concept of a "smart contract" with the intention of "securing relationships on public networks". To handle transactions in accordance with predetermined terms and conditions, "smart contracts" are programmable apps that are recorded on the blockchain and do the necessary work. As a result, smart contracts are the digital version of conventional economic contracts that are made between a variety of different engaged organizations. A blockchain network does not need authorizing intermediates to verify that the criteria in a smart contract are followed. This is in contrast to conventional contracts, which are enforced by centralized authorizing bodies. Other forms of blockchains, such as Ethereum and Hyperledger, already have the capability to write smart contracts built right in. The code for a smart contract, after it has been deployed, is saved on the blockchain, and the functions that are defined inside the smart contract may be executed at any moment by any participant. Because they have their own accounts on the blockchain and their own blockchain addresses, smart contracts are sometimes referred to as "autonomous agents. " [47] This is because smart contracts have their own blockchain addresses and have their own accounts on the blockchain. Numerous applications in blockchain networks provide a wide range of functionality, utilities, and algorithmic processing capabilities by using smart contracts that are both safe and well written.

On the other hand, smart contracts have the potential to be applied to carry out a range of tasks inside a blockchain network, such as the following:

1) Serving as a resource for different types of smart

contracts. For instance, inheritance may be programmed into smart contracts in Ethereum. This allows for one contract to trigger operations programmed into another contract.
2) Providing space for storing application specific information, such as membership records, lists, or boolean states, among other things.
3) Eabling' multisig nature' transactions, in which a transaction is only completed when either a majority of participants or a certain proportion of participants agree to sign it, is a desirable goal.
4) Allowing for the execution of automatic transactions in response to predefined events.

**Use of Blockchain in RPL Protocol**

Creating a peer to peer (P2P) network that includes all of the nodes that are interested in using a blockchain is the first step that has to be taken before using a blockchain. Every node in the network is given two keys: a public key and a private key. A public key is used by other users to encrypt the messages that are sent to a node, and a private key enables a node to read encrypted messages that have been transmitted to it. As a result, one key is used for encrypting data, while another is used for decrypting data. These two keys are kept separate.

In actual application, the private key is what is used when signing transactions on a blockchain (that is, when approving such transactions), while the public key functions in the same way as a one of a kind address. The communications that have been encrypted with the matching public key can only be decrypted by the person who has the appropriate private key. Asymmetric cryptography is the term used to describe this method. It is beyond the scope of this study to provide a comprehensive analysis of the system's inner workings; nevertheless, the reader who is interested may find further information in [32] and [33]. After completing a transaction, a node will sign it and then broadcast it to the nodes that are immediately connected to it through a single hop. The fact that the transaction is signed in a unique manner (using the private key) makes it possible to authenticate it (only the user with a particular private key may sign it) and assures its integrity (if there is a mistake during the transmission of the data, it will not be decrypted). When the peers of the node that broadcasts the transaction get the signed transaction, they check to ensure that it is legitimate before retransmitting it to additional peers, which contributes to the transaction's propagation around the network. Miners are specialized nodes that are responsible for ordering transactions, packing them into blocks, and stamping the blocks with the current time. The network decides whether or not a transaction is genuine before it broadcasts it. A consensus method is necessary for the mining process since it determines which data are included in each block and which miners are chosen. When a miner is finished packing blocks, the blocks are sent out into the network and broadcast. The nodes on the blockchain will then use the appropriate hash to ensure that the broadcast block does in fact contain legitimate transactions and that it does in fact reference the block that came before it on the chain. In the event that such requirements are not met, the block in question is discarded. However, if these requirements are checked successfully, then the nodes add the block to their chain, thereby updating the transactions.

To be more specific, an author has to consider whether or not the following characteristics are required for an RPL IoT application in order to establish whether or not the use of a blockchain is acceptable.

1) Decentralization When there is not a reliable centralized system, Internet of Things applications need decentralization. The validation and authorization of data exchanges, also known as transactions, takes place at trusted central third party organizations in network infrastructures that are centralized. This results in additional expenses due to the need for centralized server maintenance as well as performance cost limitations. In infrastructures built on blockchain, two nodes may participate in transactions with each other without the requirement to put reliance upon a central organization to store records or execute authorisation. This eliminates the need for a trusted third party.
2) P2P exchanges The majority of communications in the Internet of Things go from individual nodes to gateways, which then forward the information on to a distant server or the cloud. Except for some applications, such as in intelligent swarming or in mist computing systems, communications between peers on the node level are really not very prevalent. This is the case even if such communications are possible. There are also alternative paradigms that make it easier for nodes on the same level to communicate with one another, such as what occurs in fog computing with the use of local gateways [48, 49].
3) Data Authentication and Integrity The data that is sent via IoT devices that are linked to the blockchain network will always be cryptographically proofed and signed by the genuine sender, who will have a oneofakind public key and GUID. This will ensure that the data that is sent has been authenticated and that it has not been tampered with in any way. In addition, the blockchain serves as a distributed ledger that records all transactions that are done to or by an Internet of Things device, making it possible to trace them in a safe manner.
4) Authentication, Authorization, and Privacy To be able to give single and multiparty authentication to an Internet of Things device, blockchain smart contracts have the capability to provide decentralized authentication rules and logic. When compared to conventional authorization protocols such as Role Based Access Management (RBAC), OAuth 2.0, OpenID, OMA DM, and LWM2M, smart contracts are able to give connected IoT devices with more effective authorization access rules while at the same time requiring a great deal less complexity than these other protocols. These protocols are used extensively in today's world for the authentication, authorisation, and administration of IoT devices. The usage of smart contracts, which establish the access rules, conditions, and time for allowing a particular person or group of users or machines to own, manage, or have access to data while it is either at rest or in transit, is another method that may be used to secure the privacy of the data. The smart contracts are able to define out who has the authority to update, upgrade, or patch the IoT

software or hardware; reset the Internet of Things device; provide new keypairs; begin a service or repair request; change ownership; and provide or reprovide the device.

5) Secure Communications The IoT application communication protocols such as HTTP, MQTT, CoAP, or XMPP, as well as routing protocols such as RPL and 6LoWPAN, do not have security built into them by design. When it comes to messaging and application protocols, these kinds of protocols need to be ”wrapped” inside other security protocols like DTLS or TLS in order to ensure that communication is kept safe. In a similar fashion, the IPSec protocol is frequently used in order to offer security for the RPL and 6LoWPAN protocols while routing data. Once an Internet of Things device has been installed and is linked to the blockchain network, it will have its own one of a kind GUID and asymmetric key pair. This eliminates the need for key management and distribution, which are both abolished entirely by blockchain technology. This will lead to a significant simplification of other security protocols, such as that of DTLS, as there will be no need to handle and exchange PKI certificates during the handshake phase of DTLS or TLS (or IKE in the case of IPSec) in order to negotiate the cipher suite parameters for encryption and hashing and to establish the master and session keys. This will lead to a significant reduction in the complexity of these other security protocols. As a result, lightweight security mechanisms that would suit and stratify the needs for the computing and memory resources of IoT devices become more realistic.
6) Address Space In contrast to the IPv6 address space, which has only 128 bits, the Blockchain address space has 160 bits [50]. The public key is hashed using ECDSA (Elliptic Curve Digital Signature Algorithm), which generates a blockchain address. This address is 20 bytes long and includes 160 bits. Using addresses of 160 bits, blockchain technology allows for the ofline generation and allocation of addresses for about 1.46 1048 Internet of Things devices. When assigning and allocating an address to an Internet of Things device, the likelihood of address collision is around 1048, which is regarded to be safe enough to supply a GUID (Global Unique Identifier) that does not need any registration or uniqueness verification. The Internet Assigned Numbers Authority (IANA) is one example of a centralized authority and governance system that can no longer exist thanks to blockchain technology. The Internet Assigned Numbers Authority (IANA) is now in charge of managing the distribution of IPv4 and IPv6 addresses around the globe. In addition, blockchain offers 4.3 billion more addresses in comparison to IPv6, which makes it a more scalable option for the Internet of Things than IPv6. In conclusion, it is important to point out that the memory and processing power of the majority of IoT devices are limited, and as a result, these devices are not suited to operate an IPv6 stack.

## 4 Blockchain Applications in RPL Routing Protocol

The blockchain technology has a wide range of potential applications in many industries and settings. According to Swan [51], the progression of the applicability of blockchain began with Bitcoin (blockchain 1.0), then went on to smart contracts (blockchain 2.0), and finally moved on to applications including justice, efficiency, and coordination (blockchain 3.0). When it comes to smart contracts, they are referred to as bits of code that are self suficient and decentralized, and when specific criteria are satisfied, the code will execute on its own. There are a variety of real world scenarios that lend themselves well to the implementation of smart contracts, including international financial transactions, mortgages, and crowd funding [52]. Ethereum is now the most popular blockchain based platform for executing smart contracts, despite the fact that it is also capable of running other distributed applications and interacting with more than one blockchain. In point of fact, Ethereum is defined by the fact that it is Turing complete, which is a mathematical term that suggests that Ethereum’s programming language can be used to model any other language. This ability allows Ethereum to function as a universal language simulator. It is beyond the scope of this study to provide a comprehensive explanation of how smart contracts function; however, any reader interested in learning more may find a pretty excellent description in [53]. Beyond cryptocurrencies and smart contracts, blockchain technologies have the potential to be implemented in a variety of domains (the most relevant of which are depicted in Figure 4) that involve Internet of Things applications [54], such as sensing [55], [56], data storage [57], [58], identity management [59], time stamping services [60], smart living applications [61], intelligent transportation systems [62], wearables [63], supply chain management [64], mobile crowd sensing [65], cyber law [66], and In addition, blockchain technology has applications in the field of Internet of Things agriculture. For instance, a traceability system for tracing the supply of agricultural and food products in China is provided in [68]. The purpose of the system is to improve both the safety and quality of food as well as to cut down on losses that occur throughout the logistics process. This goal will be accomplished via the use of Radio Frequency Identification (RFID) technology and a blockchain.

### 4.1 Blockchain Structure

A blockchain is a distributed ledger that is organized into blocks, each of which documents a transaction that took place on the network. The information pertaining to the transactions may be thought of as token transfers taking place inside a network or as any other type of data exchange. The header and the content of each block constitute the logical divisions that are made inside the block itself. The body of the block is where transactions are recorded, whereas the header of each block provides, among other elements, the identifier of the block that came before it. Transactions are stored inside the body of the block. As a consequence of this, the blocks are linked together in a chain that looks very much like a linked list, as can be seen in Figure 1 (a). The first building block in the chain is referred to as the ”genesis” block [69]. Because the identity of each block is determined by taking its cryptographic hash, it is important for the blockchain to have each block connected to the block that came before it. This helps the blockchain

fulfill the goal of having its contents be immutable. If a malicious hacker were to change the information included in an older block, that block's identity would no longer be legitimate, and as a domino effect, the parent block hashes contained in future blocks would also be rendered invalid. Therefore, in order for an adversary to successfully change the contents of a single block, they would need to modify the headers in all subsequent blocks and have this modification take place in the majority of the nodes in the network. This is necessary in order for the peers to establish consensus on this amended blockchain. The header of the block stores, in addition to the block's own identification and the identifier of the block that came before it, the date of when the block was published as well as the Merkle tree root for all of the transactions that are included inside the body of the block [70]. The use of the Merkle tree root makes the verification of transactions that take place inside a block substantially easier. To provide more context, the blockchain is a data structure that expands in a linear fashion, with increased transaction activity leading to larger sizes for newly created blocks. Peers check the legitimacy of transactions that have been recorded in a freshly published block as part of the process that underpins all consensus algorithms. Each of the transactions that occur inside a block are assigned their own unique identifier (transaction ID), which is a cryptographic hash of the information about the related transaction that is contained in the block. In the case that different nodes in the blockchain network produce legitimate blocks at the same time, the blockchain may split, and it then becomes problematic to maintain a single version of the blockchain that is considered to be canonical. The problem is solved by mainstream blockchain networks by only recognizing the longest fork to be canon [71], [72]. This means that all blocks released in the other forks are abandoned, also known as orphaned. Within the blockchain network, other elements in the block header provide information that is relevant to the consensus method that is being utilized.

## 5 Integration of Blockchain technology into RPL Routing Protocol

The development of the Internet of Things (IoT) has been significantly aided by the use of centralized cloud services; yet, when it comes to data transparency, there is an inherent requirement for trust, and there is a lack of total confidence. IoT customers do not have complete control over how the data they contribute will be utilized, and they do not have complete faith that their data will be handled appropriately since centralized cloud services function similarly to a black box for IoT services. In addition, centralized cloud services are susceptible to flaws as well as devastating assaults on their security. In the course of the development of the Internet of Things, the capability of the network edge is increasing at a faster rate than that of the cloud, as shown by fog and mist designs [73]. The Internet of Things (IoT) stands to gain from the decentralized network paradigms made available by blockchains. As a result, ongoing development of the IoT will no longer be dependent on the use of trusted centralized services, which will free up resources for other IoT related endeavors. However, blockchains are still in the early phases of research and development, and there are still a number of research obstacles for integrating RPLIoT and blockchains in a smooth way. It is difficult to achieve complete decentralization in the RPL IoT by using blockchains because of the wide variety of devices that are participating in the RPL routing protocol of the Internet of Things. As a result of resource limitations, the vast majority of devices that make up the RPL cannot host a copy of the blockchain or participate in validating new blocks for the blockchain. As a result, it is essential to make a decision on the roles that will be played by the various entities that make up the RPLIoT edge (such as devices, gateways, etc. ).

It is required to utilize certain design considerations concerning the level of RPLIoT devices' engagement in a blockchain network since it is vital to keep in mind the resource limits experienced by RPLIoT devices. The vast majority of devices that are connected to the internet of things do not have cryptographic capabilities, and they also do not fulfill the computing and storage requirements necessary to participate in blockchain consensus procedures. IoT edge devices are restricted to the function of basic transaction issuers so that they may work around the restrictions they have. The majority of these kinds of devices do not contain adequate storage capacities to be able to host the "headers only" version of the blockchain. IoT edge devices or gateways that are functioning as simple transaction issuers have verified blockchain IDs without the requirement to host a whole copy of the blockchain. Therefore, such edge devices are more controllable inside blockchain networks and may continue making contributions to the blockchain. Meanwhile, other full nodes in the blockchain network can carry out decentralized consensus and block validation.

## 6 Blockchain Solution For RPL Network

Introducing a blockchain solution to a Routing Protocol for Low Power and Lossy Networks (RPL) can bring several benefits, including enhanced security, trust, and transparency. Here is a high level overview of a blockchain based solution for an RPL network:

**a) Decentralization**
Blockchain is inherently decentralized, meaning there is no central authority or single point of control. In RPL networks, decentralization can enhance network resilience and fault tolerance. Nodes in the network can participate in the blockchain consensus process, ensuring distributed decision making and reducing the reliance on a single entity.

**b) Data Integrity and Auditing**
Blockchain ensures the immutability of data, providing an auditable record of all transactions and operations. In RPL networks, this characteristic can be leveraged to trace the history of routing changes, diagnose network issues, or conduct post incident analysis. It enables network administrators to identify anomalies, investigate security breaches, and ensure the integrity of the network.

**c) Blockchain for Providing RPL Security**
Due to the fact that every device that issues transactions has its own unique blockchain address, an Internet of Things solution that is based on blockchain technology is immune to fraudulent authentication. Because generating many

empty transactions results in transaction costs, consensus methods, which are employed in public blockchains, prohibit bad actors from initiating denial of service assaults [74]. Therefore, blockchains have the potential to cause a disruption in the security methods used by the internet of things (IoT) and to offer enhanced security solutions for the IoT stack. In the most recent body of research, a number of potential solutions to the problem of implementing access control regulations in the Internet of Things (IoT) without depending on a thirdparty service have been uncovered. Blockchain technology has the potential to increase the amount of security infrastructure that is readily available for the internet of things. A secure public key infrastructure that is more fault tolerant than centralized systems may be provided by using decentralized approaches such as [75]. Hashemi et al. [76] suggest a multilayer blockchain architecture, in which data storage and access control are carried out in various levels of the system. Zhang and Wen [77] provide a tokenized method for implementing access control in the Internet of Things by using blockchains and smart contracts. The primary objective of the paper is to create a blockchain based ebusiness model in which users may spend their own specialized cryptocurrency to acquire temporary access rights for physical or digital assets. This model will be the basis of the e business model. In the event that Bob needs access to the Internet of Things (IoT) data that Alice has stored, Bob may purchase the specialized cryptocurrency known as IoTCoin, pay Alice a sum that has been previously agreed upon, and then obtain the key to decrypt and access Alice's data for a certain length of time. Another tokenized method to access control is given in [78], in which users are assigned distinct roles, and access control rules put into smart contracts may be used to grant or revoke access rights for an IoT user's data. Similarly, [79] and Enigma [80] store chunks of encrypted data on the blockchain. Additionally, they employ a tokenized method and smart contract rules for permitting and denying access to stored IoT data. IoT users are able to give and revoke access to stored chunks of IoT data by means of functions defined in smart contracts, according to another model for access control that is proposed in [81]. This model is quite similar to the previous model. In [82], EsSamaali et al. propose using an overlay blockchain as a means of delivering an access control mechanism for large amounts of data. They make choices on the authorization of requests to access large amounts of data using programmable smart contracts. An adversary would seek to modify the records in the blockchain or generate fraudulent blocks in the blockchain, either containing bogus transactions or censoring transactions that have already happened in order to carry out a modification attack on an Internet of Things architecture that is supported by blockchain technology. In public blockchain systems, where the canonical records of the blockchain are preserved by widespread consensus, this is very difficult, if not impossible, to do. This provides further support for decentralizing the Internet of Things via the use of blockchains, since the features inherent to blockchains prohibit assaults that affect the integrity of data [83]. The structure of a multitiered blockchain is used by Dorri et al. [84] in order to keep a record of portions of Internet of Things data that are saved in the cloud. In this particular implementation of blockchain technology, the public overlay blockchain makes use of hashing to keep an immutable record of the data chunks that are kept in the cloud. In a similar fashion, [85] use the blockchain to store hashes of IPFS files that include IoT data. Because files in IPFS are content addressed using their hash, the contents that are saved in IPFS are incorruptible and cannot be changed. In reference number 86, we find a description of a data integrity service that is based on blockchain technology and that allows query based integrity tests to be carried out without the need for third party verification. In this implementation, the blockchain serves as an additional layer of protection, ensuring that data objects kept in the cloud retain their integrity at all times. Issuing queries and checking the information stored on the blockchain are two methods that may be used to identify any breaches in the integrity of the data. In their paper [87], Yang et al. presented a credibility evaluation system for the Internet of Vehicles that is based on blockchain technology. The solution that has been suggested is to implement a reputation system that is based on blockchain technology and that determines the trustworthiness of the messages that have been received based on the reputation of the sender. Since each transaction is signed by the issuer's private key, blockchain based apps already have builtin permission and secrecy capabilities. This is because the blockchain includes intrinsic addressing that involves public/private key pairs. A blockchain based public key infrastructure is used by Axon et al.

[88] in order to control Internet of Things devices. They did this with the help of smart contracts, which sent orders to the Internet of Things devices by utilizing the addresses of those devices stored on the blockchain. These instructions include modifying working rules and adding information about energy use to be stored on the blockchain. Cha et al. [89] make use of Ethereum blockchain technology in order to keep the communication between IoT gateways secret. The gateways were developed to control Bluetooth Low Energy (BLE) devices such as smart manufacturing equipment and wearable electronics. On behalf of the user, the gateway will handle any Bluetooth Low Energy (BLE) devices that have been linked to it and will communicate with those devices via smart contracts. The gateway stores information that is important to the devices, and all interactions with the Internet of Things are kept secure thanks to blockchain based signatures. Multitiered systems, such as [90], preserve access control regulations inside the blockchain header. At the same time, all users with access rights get encrypted chunks of data from the offchain data storage mechanism. A multitier approach with comparable characteristics can be found in Reference [91], which use IPFS as the offchain storing method. A data requester is provided with the access key to an Internet of Things (IoT) data file whenever IoT data contained in an IPFS file is permitted to be accessed by the data requester. As a result of the key being encrypted with the requester's public key, which the requester alone is able to decode, secrecy is ensured when utilizing a PKI that is based on blockchain technology. The blockchainbased security solutions that were developed and described above provide increased availability in the internet of things (IoT) by using the decentralized qualities that are inherent in blockchains. Because there are no centralized points of failure, solutions that enable on chain data storage often come equipped with a number of features that ensure data is

always accessible. The availability of its interaction records has been increased thanks to offchain storage solutions; nonetheless, the availability of the data that has been saved is reliant on the off chain storage techniques that are being employed. In this section, we will talk about some of the suggested solutions that feature one of a kind design components that contribute to the increased availability of the Internet of Things (IoT). Alphand et al. [92] present a blockchain based authorization mechanism for the Internet of Things with a greater degree of liveness owing to the inherent qualities of the blockchain, which they combine with the OSCAR (Object Security Architecture for the Internet of Things) [93] security model. This is possible because of the intrinsic features of the blockchain. In Bahga and Madisetti's [94] blockchain network, there are Internet of Things devices that have blockchain addresses. The purpose of this project is to create a manufacturing and intelligent industrial system that is based on blockchain technology. Users have the ability to give manufacturing instructions directly to devices in the form of transactions due to the fact that every device is part of the blockchain. The on demand manufacturing, machine diagnostics, and supply chain monitoring are just examples of the types of transactions that may take place here. The writers go through an example of using diagnostics and maintenance software on a machine. In the event that numerous computers inside the network develop problems, the decentralized nature of linked devices will allow the network continue to function normally. In the case that a defect does develop, the devices that are still operational will be able to report it.

**d) Smart Contracts**

Smart contracts are self executing agreements with predefined rules and conditions. They can automate processes and enforce rules in the blockchain network. In RPL networks, smart contracts can be utilized to define and enforce routing policies, automate network management tasks, or enable secure and authenticated communication between devices

**e) Consensus Mechanisms**

Blockchain relies on consensus mechanisms to agree on the state of the ledger and validate transactions. Different consensus algorithms, such as Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT), can be employed in the blockchain based RPL network. The choice of consensus mechanism should consider the energy efficiency, scalability, and latency requirements of low power networks.

## 7 Data Integrity and Auditing

Blockchain ensures the immutability of data, providing an auditable record of all transactions and operations. In RPL networks, this characteristic can be leveraged to trace the history of routing changes, diagnose network issues, or conduct post incident analysis. It enables network administrators to identify anomalies, investigate security breaches, and ensure the integrity of the network.

**a) Blockchain for Providing RPL Security Privacy**

The Internet of Things raises enormous concerns with regard to privacy when one considers the huge volume of data that is gathered, transported, and kept, as well as likely sold. In the most recent few years, decentralization has been a topic of investigation for questions about privacy. One of the first pre blockchain methods for decentralized anonymous authentication was published by Alcaide et al. [95], and it was based on a cryptographic method known as Zero Knowledge Proof of Knowledge (ZKPK). On the other hand, this technique has been called into question since it leaves the protocol open to attack in the event that an adversary poses as a real user during the data gathering phase of the protocol [96]. In more recent times, distributed ledgers, sometimes known as blockchains, have emerged as the leading candidate technology for decentralizing the Internet of Things. Blockchain technology lays the groundwork for decentralized networks and enables safe data transfer operations to be carried out without the requirement for any middlemen to perform authorizing and authenticating functions. As a result of the immutable recordkeeping characteristics of blockchains, which offer a feasible solution for managing IoT micropayments and data sharing, the creation of privacy preserving networks for IoT that make use of blockchain and smart contracts is a fruitful and active field of study. IoT data that is stored on chain as well as off chain is generally maintained encrypted, and restrictions for permitted access are enforced on the blockchain. Because all interactions that take place over the blockchain are publicly known and verifiable, it follows that IoT data that is stored onchain and off chain must also be kept secure. The first stage in the process of designing solutions that are private by design is to guarantee that users of IoT have ownership of their data. This gives consumers the ability to exercise control over how and when their data is accessed. Users also have the option of encrypting their data and keeping it secret while it is stored on a decentralized data medium. Zhang and Wen [97] offer a tokenized access model for Internet of Things (IoT) data ownership. Under this approach, individuals may make transactions to IoT data owners in exchange for access rights to the owners' encrypted data. In this scenario, users of the Internet of Things have full control over the data that they want to provide in return for services or monetary incentives, and they also have the ability to selectively express their IoT data. FairAccess [98], [99] is another solution that has been offered to enable private ownership of IoT data. This solution offers IoT owners with complete discretion over who they choose to provide access to their IoT data and is one of the proposed solutions for enabling private ownership of IoT data. The purpose of the PISCES framework [100] is to ensure data ownership and data governance so that privacy may be built into the system from the beginning. They specify the responsibilities of data controllers and data suppliers, and they employ something called a Privacy Validation Chain (PVC) to keep an auditable track of the events in which data is used. The incorporation of PVC blockchain guarantees that the rights that IoT users have over their data will be honored at all times. PlaTIBART [101] is a platform that has been suggested to be built on blockchain technology for Internet of Things applications that require data interactions. It gives you the tools and methods you need to develop and manage blockchain applications for the Internet of Things on private blockchains. They employ private blockchains because of the privacy characteristics it offers and the short amount of

time it takes for transactions to be finalized. In addition, they build off chain interactions for private data transfer events. Another option for the storing and distribution of data that is not on the chain is provided in [102]. Hashes of data chunks that are kept in a storage platform that is based on a trusted execution environment (TEE) may be logged by the authors of this work with the assistance of a private blockchain. In addition to this, they consider Intel SGX to be a component of the TEE in order to protect the confidentiality of the application code and the data generated by the internet of things. Additional research conducted by Kang et al. [103] and Li et al. [104] provides a solution for peer to peer energy trading in the IIoT and between linked hybrid automobiles. This system makes use of pseudonymous address updating inside a consortium blockchain. Local aggregators conduct block validation and may be held responsible in the event of fake block formation under their implementation of a modified version of the proof of work consensus method with looser limitations. The block validation process might take up to one minute, and the consortium blockchain provides a safe environment for the exchange of energy.

**b) Transparency and Trust**

Blockchain provides a transparent and immutable ledger where all transactions and operations are recorded. In the context of RPL, this transparency can enhance trust among nodes in the network. Each node can verify the integrity of routing information and ensure that it has not been tampered with. This characteristic is particularly valuable in environments where trust among devices is critical.

By incorporating these blockchain characteristics into RPL networks, it is possible to enhance security, trust, transparency, and resilience. However, it is essential to consider the specific requirements and constraints of RPL networks and adapt blockchain solutions accordingly to achieve the desired outcomes.

## 8 Blockchain Characteristics In RPL Network

When integrating blockchain technology into a Routing Protocol for Low Power and Lossy Networks (RPL), several characteristics of blockchain become relevant. Here are some key characteristics of blockchain in the context of RPL networks:

**a) Decentralization**

Blockchain is inherently decentralized, meaning there is no central authority or single point of control. In RPL networks, decentralization can enhance network resilience and fault tolerance. Nodes in the network can participate in the blockchain consensus process, ensuring distributed decision making and reducing the reliance on a single entity. Each transaction validation has historically been handled by a reputable third party in conventional transaction management systems, such as a bank or other kind of financial institution. This kind of centralization will always result in more costs, a performance bottleneck, and a single point of failure for centralized service providers. In contrast, blockchain enables the transaction to be certified between two peers without the authentication, jurisdiction, or interference done by the central agency. This results in a reduction in the service cost, mitigation of the performance bottleneck, and a reduction in the SPF vulnerability.

**b) Transparency & Trust**

Blockchain provides a transparent and immutable ledger where all transactions and operations are recorded. In the context of RPL, this transparency can enhance trust among nodes in the network. Each node can verify the integrity of routing information and ensure that it has not been tampered with. This characteristic is particularly valuable in environments where trust among devices is critical. Every user has the same level of access and interaction rights with the majority of public blockchain systems (such Bitcoin, Hyperleger fabric, and Ethereum), which means that anybody may join the network and participate in transactions. Additionally, each new transaction is verified and recorded on the blockchain, and as a result, it is accessible to each and every user. Because of this, the data stored on a blockchain is an open book to any user who may get access to it and validate the transactions that have already been completed on it.

**c) Traceability**

A timestamp, or date and time stamp, is appended to each transaction that is permanently stored on the blockchain. This timestamp records when the transaction really took place. After doing an analysis of the data contained inside the blockchain and noting the timestamps that correlate to each piece of information, users will be able to readily verify and track the sources of historical data items.

**d) Security**

Blockchain's security features, such as cryptographic hashing and digital signatures, can enhance the security of RPL networks. Transactions and routing information can be securely stored and validated using cryptographic techniques. By leveraging blockchain, RPL networks can mitigate risks associated with attacks, tampering, or unauthorized modifications of routing data

**e) Immutability**

A blockchain is made up of a series of blocks that are connected together in chronological order. Each link in the chain is effectively an inverted hash point of the block that came before it. If the block before it is modified in any way, all of the blocks that are created after it are rendered invalid. In the meanwhile, the hash of each and every transaction that has been committed is saved in the root hash of the Merkle tree. A new Merkle root is produced whenever there is any modification, no matter how minute, on any transaction. Because of this, it is simple to spot any attempt at fabrication. The integrity of the data may be guaranteed by the combination of the inverse hash point and the Merkle tree.

**f) Consensus Mechanisms**

Blockchain relies on consensus mechanisms to agree on the state of the ledger and validate transactions. Different consensus algorithms, such as Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT), can be employed in the blockchain based RPL network. The choice of consensus mechanism should consider the energy eficiency, scalability, and latency

requirements of low power networks.

**g) Nonrepudiation**
It is important to keep in mind that the private key is what is used to place the signature on the transaction, and that the public key is what allows other people to view the signature and verify it. Because of this, the person who initiated the transaction cannot back out of the cryptographically signed transaction.

**h) Smart Contracts:**
Smart contracts are self executing agreements with predefined rules and conditions. They can automate processes and enforce rules in the blockchain network. In RPL networks, smart contracts can be utilized to define and enforce routing policies, automate network management tasks, or enable secure and authenticated communication between devices.

**i) Privacy:**
Blockchain networks typically provide pseudonymity and privacy to participants. While the data on the blockchain is transparent, the identities behind the transactions can remain anonymous or pseudonymous. However, in RPL networks, preserving privacy while maintaining the necessary transparency and trust in routing information is a challenge that needs to be addressed. Research in privacy preserving techniques within blockchain based RPL is essential.

**j) Data Integrity and Auditing:**
Blockchain ensures the immutability of data, providing an auditable record of all transactions and operations. In RPL networks, this characteristic can be leveraged to trace the history of routing changes, diagnose network issues, or conduct postincident analysis. It enables network administrators to identify anomalies, investigate security breaches, and ensure the integrity of the network.

## 9 Blockchain Challenges & Limitations

There are a number of technical obstacles and constraints that have been uncovered in relation to the blockchain technology. The following are seven of the limits and technological hurdles that the author [105] outlines for potential applications of Blockchain technology in the future:

**a) Security**
There is a risk of a 51% attack on the Blockchain as it now exists. In a 51% attack, a single entity would have full control of the majority of the network's mining hashrate and would be able to change Blockchain. This would allow the entity to get complete access to the blockchain. More investigation into safety and security is required if this problem is to be resolved.

**b) Wasted Resources**
Bitcoin mining consumes an enormous amount of energy (around $15 million per day), which is wasted. The work required for Proof of Work contributes to the waste generated by Bitcoin. Proof of stake is one of the solutions that are available in certain business sectors. Proof of effort is a consensus algorithm that determines the chance of mining a block based on the amount of effort that a miner puts in [106]. In contrast, the resource that is evaluated in Proof of Stake is the quantity of Bitcoin that a miner has [106]. For instance, a user who owns 1% of the Bitcoin network has the ability to mine 1% of the "Proof of Stake blocks. " In order to mine blocks in Blockchain in a more effective manner, it is necessary to find a solution to the problem of wasted resources.

**c) Usability**
It is not easy to utilize the Bitcoin application programming interface (API) for constructing services. It is essential to work on making Blockchain's application programming interface (API) more user friendly for developers. It's possible that this is similar to REST APIs.

**d) Latency**
At the moment, it takes around ten minutes to finish a single transaction on Bitcoin since doing so generates a block of transactions with appropriate security. Because the time spent on a block has to be suficient enough to balance the expense of double spending assaults, it is necessary to increase the total amount of time spent on it. A case of double spending occurs when an individual spends their money successfully more than once [107]. Bitcoin prevents double spending by validating each transaction that is uploaded to the block chain. This checks to see whether the inputs for the transaction have been spent in the past. whether they haven't, then the transaction is approved. Because of this, latency is now a significant problem with blockchain. The generation of a block and the confirmation of the transaction should take place in a matter of seconds while preserving the system's integrity. In comparison to Blockchain, it just takes a few seconds to complete a transaction using a credit card like VISA, which is a significant benefit.

**e) Throughput**
At the moment, the maximum throughput that can be achieved on the Bitcoin network is equal to 7 tps, which stands for transactions per second. VISA, which has 2, 000 tps, and Twitter, which has 5, 000 tps, are both examples of transaction processing networks. When the number of transactions that take place on the Blockchain climbs to comparable levels, the throughput of the Blockchain network will need to be boosted.

**f) Size and bandwidth**
At this time (February 2016), the size of a Blockchain on the Bitcoin network is more than 50, 000 megabytes. When the transaction throughput reaches VISA levels, the blockchain's potential annual growth might reach 214 petabytes per second. The Bitcoin community operates on the presumption that the size of a single block is 1 megabyte (MB), and that a new block is generated once every ten minutes [108]. Because of this, there is a limit on the total number of transactions that may be processed inside a single block, which is typically about 500 transactions [109]. If the Blockchain is going to be able to govern a greater number of transactions, problems with its size and bandwidth will need to be resolved.

**g) Versioning, hard forks, multiple chains**

There is a greater likelihood of a 51% assault occurring on a chain that is tiny in size and has a limited number of nodes. When chains are broken apart for administrative or versioning reasons, this raises even another concern.

## 10 Motivations of Using Blockchain in RPL Network

In the following, we will discuss several significant motivating factors that have contributed to the RPL network's adoption of blockchain technology.

1) To begin, one of the primary advantages of blockchain technology is that it is decentralized. Blockchain makes it possible to establish decentralized RPL networks and incorporates a greater number of distributed elements, which may include RSUs, automobiles, and even individuals. In the same breath, these dispersed companies are able to autonomously run their own business processes. The operational concepts of the existing RPL network, which are mostly based on centralized decision making, will be adapted for use in a decentralized setting and will undergo simplification in the process. The decentralization, in the long run, will result in improved user experiences for vehicle service providers.
2) Second, blockchain technology does away with the need to rely on cloud based or similar systems for the storage and administration of data. In addition, blockchain technology, when combined with smart contracts, makes it possible to eliminate the need for various third party organizations, such the central service manager, control center, administrators, and trusted intermediates. Instead, members in the blockchain network may manage the transactions on their own, which will result in decreased levels of energy usage.
3) Third, if RPL implements blockchain technology, it may be possible to mitigate some security risks, including interruption, single point of failure, and availability assaults. This is as a result of the synchronization and replication of the blockchain that takes place amongst all of the peer nodes that are connected to the network. As a result, the services are able to continue operating normally even in the event that one or more than one of the nodes have been corrupted. On the other hand, the blockchain technology relies on contemporary cryptographic procedures to guarantee that the same security and privacy qualities are maintained. In point of fact, blockchain places an emphasis on the increased security and privacy afforded to RPL networks by encryption.
4) Fourth, blockchain offers a high level of immutability for RPL services and situations. This is because in blockchain, the blocks maintain a chain to link with one other via the hash values of each block record. The immutability aspect of blockchain has the potential to prevent data tampering and change, and it also helps ensure that audits are carried out appropriately. With the assistance of smart contracts, it also makes it possible to implement and enforce any rules or scripts that have been predefined in advance.
5) Fifthly, blockchain enables two parties to engage in peer to peer (p2p) commerce and sharing, as well as communication with one another. P2P networks enable service requesters and suppliers to directly communicate with one another, which is beneficial to both parties. This peer to peer functionality is very helpful for RPL applications since it enables secure data and resource sharing between cars and RSUs. The fact that the entities in the p2p network do not need to communicate with any intermediate leads, in the end, in applications and services with minimal latency.
6) Sixth, the RPL facilitates communication between diverse organizations that may or may not have mutual trust. Blockchain technology, which utilizes innovative consensus processes, is able to build a high level of confidence even among organizations that cannot be completely relied upon.
7) In addition to consensus procedures, smart contracts have the potential to play a significant part in resolving trust concerns that arise throughout the process of decision making in the absence of a trusted institution. In addition, the scripts that are used in smart contracts contribute to the development of an automated and decentralized system.
8) In conclusion, the permissionless nature of the public blockchain makes it accessible to any and all businesses. Consequently, the use of public blockchains has the ability to throw open the door to complete access to the data that is recorded in blockchain. It also has the potential to increase the openness of the RPL environment.

## 11 Research Methodology

For the purpose of this study, the research approach that was used was a systematic mapping study. A systematic mapping study's objectives are to offer an overview of a research field, to determine whether or not there is evidence from previous research, and to quantify the quantity of evidence [110]. In this investigation, we make use of the method of systematic mapping that was laid forth by Petersen et al. [111]. When looking for publications that are relevant to the topic, we also follow the requirements for a systematic literature review that are provided by Kitchenham and Charters [110]. Because we wanted to investigate the previously conducted research that is associated with Blockchain technology, we decided to employ a technique called systematic mapping as our research approach. We would be able to discover and map research topics connected to Blockchain technology and RPL IoT with the assistance of the findings of the mapping study.

### a) Database Selection

There are a great number of databases for study in the scientific field, and each of these databases collects the contributions
made by a different researcher.

The Scopus database was used for this particular investigation. More than 3096 peerreviewed journals are included in this resource, and they come from some of the most prestigious publishing companies in the world, including Springer, Elsevier, Taylor & Francis, IEEE, and Emerald. Scopus is a more complete database than Web of Science (WoS), which is also an important and well recognized database but only contains articles from journals

that are ISI indexed.

**b) Screening of relevant papers**

All of the publications that were found in the searches required to have their real relevance evaluated [110] since it was not guaranteed that they would be relevant to the research. The screening of articles was the following step after doing the searches in the Scopus databases according to the prescribed process. A method that was influenced by Dyb and Dingsyr [112] was used by our team in order to filter the relevant publications. During the first step of the screening process, the titles of the articles were evaluated to determine whether or not they met the criteria for inclusion in the study. Studies that did not relate to the main issue of the investigation were disqualified. For instance, the search protocol yielded articles relating to Blockchain, RPL, RPL assaults, and IoT in various Scopus domains. These publications had a different meaning than the key phrases that were utilized in the RPL routing protocol. It was obvious that these studies did not fall within the parameters of our mapping research, which was a sufficient justification for excluding them. However, in other instances, it was impossible to evaluate the relevance of the research based on the title of the paper alone. Whenever one of these circumstances arose, we moved the article on to the subsequent step for more reading. During the second round, we examined the abstracts of all of the papers that had made it through the first phase. In addition, we used distinct criteria for the inclusion and rejection of papers while doing our screening. We made the decision to exclude the following kinds of papers: (1) papers that did not have full text available; (2) papers whose primary language was not English; (3) papers that discussed Blockchain in a context other than the RPL routing protocol; (4) papers that were duplicates; (5) papers that were posters; and (6) publications that are not literature reviews. After ensuring that a piece of writing satisfied all six of the exclusion criteria, we reviewed its abstract to determine whether or not it was primarily concerned with the use of Blockchain technology to the RPL routing protocol. If this was the case, we made the decision to accept the paper in the subsequent screening round.

After locating the relevant publications by way of abstracts, the next step of the procedure for a mapping research is keywording. At this point, we implemented the procedure that was outlined by Petersen et al. [111]. Keywording was done in two phases. The first thing that we did was read the abstract, after which we determined the keyword selection and the ideas that best expressed the contribution of the study [111]. The next thing we did was establish a deeper degree of comprehension based on the terms we had chosen [111]. When we were mapping the research, we clustered the information using the keywords, and we formed categories from those clusters. After the categories were grouped together, we went back through and read each of the chosen articles. Following the reading, we then revised the categories or developed new ones as necessary, depending on whether or not the article provided any new information. As a consequence of this, we were able to create a hierarchical map of grouped categories using all of the relevant publications from the study subject.

**c) Keywords selection Collection results**

The authors selected a significant number of keywords to be coupled with the term ”blockchain” in order to achieve their goal of generating an entire literature study on the blockchain technology that is utilized in the RPL routing protocol. These keywords include RPL, RPL attack, and IoT. A search was conducted using the ”document search” feature of Scopus by combining the AND and OR connectors in the following way: (blockchain AND RPL) OR (blockchain AND RPL Attack) OR (blockchain AND IoT). The results of the initial inquiry came back with a total of 3096 articles. In order to have an understanding of the contribution that each term had to this result, the number of pages that were obtained by conducting the searches individually should be looked at. In light of the fact that it was conceivable for there to be some duplications in this scenario, it is not surprising that a larger number (namely 4050) was obtained. The first round of inclusion and exclusion decisions were made using the names of the recovered articles after applying the six screening criteria to relevant studies. The author read each of the paper’s titles, and then the number of papers that were ultimately chosen was narrowed down to 44. According to the abstracts, each of the accepted papers dealt with some aspect of Blockchain technology. This was the criterion for selection. On the other hand, we came to the conclusion that some of the papers need more clarification and should be advanced to the next phase of the selection process. In the last step of the article selection process, three writers read every single manuscript. This led to the selection of 32 publications, all of which were considered primary papers for the purposes of this research.

**d) Publication year, source and geographic distribution**

The publication year distribution of the chosen main publications is shown in Figure 1. It is interesting to note that every single one of the chosen articles was published after the year 2013. This demonstrates that the Blockchain as a study field is one that is really fresh and brand new. When looking at the publication year distribution in further detail, we see that out of all of the chosen papers, only two articles (five percent) were published in the year 2017, followed by twenty papers
(fiftynine percent) between 2018 and 2021, and finally twelve papers (thirtysix percent) in 2023. This demonstrates that the number of publications produced each year is rising, but many articles have not been included this year, which implies that there is also a growing interest in the technology behind Blockchains. This should not come as a surprise given that the RPL routing protocol incorporates the concept of blockchain technology.

Figure 6 illustrates the geographical spread of the articles that were chosen for further consideration. The most number of articles, seven, were published by academic institutions or private businesses in the United States of America and Italy. After this, the two nations that published the most were Malaysia with 6 papers, followed by India, Saudi Arabia, the United Kingdom, and China with 5 papers each. Malaysia was the most frequent publishing country. The remaining nations each had four publications or less published in scientific journals. The fact that Blockchain technology has garnered academic attention in a variety of countries is shown by the geographic dispersion of the main papers that

were chosen.

**e) Publication type and channel**

The different kinds of publications that the chosen articles were comprised of are shown in Figure 3. The term ”publication type” refers to the medium in which the article was first made available for public consumption. This mapping research took into account a variety of publishing formats, including conference proceedings, a book chapter, an article, and a review. The vast majority of the articles were presented at conferences (3) (7.0%) or were included as book chapters (2.3%). The remaining publications were published either as an article (seven, or 16.3%) or as a review (thirtytwo, or 74.4%).

**f) Limitations of the systematic mapping study**

The most significant drawbacks of a systematic mapping research are linked to publishing bias, selection bias, inaccurate data extraction, and incorrect categorization [113].

The term “publication bias” refers to the issue in which good findings are more likely to be published than negative ones. This is due to the fact that unfavorable results either take longer to be published or are mentioned in other publications to a lower level [110] [113]. In order to identify as many publications as possible and solve this concern, the search technique that we developed made use of a number of well known scientific databases. Because of this, the number of publications that we were able to uncover for this mapping project rose, which in some ways also raised the likelihood that we would find papers that included unfavorable outcomes. It is likely that research has been carried out in the industry and published as white papers or undertaken internally inside firms; this is despite the fact that blockchain technology is a relatively new issue in the computer science industry and academia. As a result, not all of the research that has been done on the technical components of Blockchain will likely be included in this mapping study. However, since we limited our search to just scientific databases for applicable research, we were able to compile a collection of publications that were likely of a better quality.

The terms ”inaccuracy in data extraction” and ”misclassification” allude to the likelihood that the same information is extracted in a variety of ways by various reviewers [113]. In order to solve this problem, we designed a paper retrieval procedure that included three authors. Each of the three writers read over the abstracts of the publications that were considered for inclusion in the study, and then they each provided their recommendation for whether or not the work should be included. When it became clear that the viewpoints did not coincide, we had a conversation to determine whether or not the particular piece of writing in question ought to be included or left out. In addition, the classifications of the articles were carried out in person over a number of sessions. over these meetings, the three authors discussed and generated mappings and classifications for each of the 41 main papers that were chosen.

## 12 Open Research Issues of Blockchain in RPL

When discussing the application of blockchain in the Routing Protocol for Low Power and Lossy Networks (RPL), there are several open research issues that deserve attention. RPL is a routing protocol designed for resourceconstrained networks, such as those found in Internet of Things (IoT) environments. Integrating blockchain technology with RPL can offer benefits such as improved security, trust, and transparency. However, there are still challenges and open research issues that need to be addressed. Here are a few of them:

**a) Scalability:**

Blockchain networks often face scalability issues due to the decentralized nature of the technology. In RPL, where devices have limited processing power and memory, scalability becomes even more crucial. Research is needed to explore eficient consensus mechanisms, data storage techniques, and transaction processing methods that can mitigate scalability challenges in blockchain based RPL implementations [114].

**b) Energy Eficiency:**

Energy eficiency is a critical concern in lowpower networks, as devices are typically batterypowered. Blockchain networks, especially those that rely on proofofwork (PoW) consensus algorithms, can be computationally intensive and energyconsuming. Finding ways to reduce the energy consumption of blockchain operations within RPL while maintaining security and consensus integrity is an important research area.

**c) Latency:**

In RPL, low latency is often required to ensure timely communication in IoT applications. However, blockchain networks typically involve multiple rounds of consensus and transaction verification, which can introduce latency. Developing mechanisms to reduce latency in blockchain based RPL systems, such as optimizing consensus algorithms or leveraging offchain techniques, is an ongoing research challenge.

**d) Security Vulnerability**

Despite the fact that introducing blockchain technologies into RPLIoT may enhance the security of RPL through the encryption and digital signature offered by blockchains, the security of Blockchain is still a big worry owing to the weaknesses of IoT systems and blockchain systems. On the one hand, there is an increasing trend toward introducing wireless networks into industrial environments due to the practicability and scalability of wireless communication systems. However, because to the open nature of the wireless medium, the Internet of Things is vulnerable to a variety of inherent security flaws in the RPL routing protocol. These flaws include the Version number attack, DAO inconsistency, DAO Insider attack, Sybil and Blackhole attack, and others. In addition, owing to the resource limits of the RPL protocol, traditional heavy weighted encryption methods may not be practical for use with IoT [115]. A dispersed environment makes it difficult to handle encryption keys, which are essential to the operation of encryption algorithms. In the meanwhile, blockchain systems have their own security flaws, such as bugs in their smart contracts’ programming [116]. In

particular, the paper [117] demonstrates how a malicious node might take advantage of the border gateway protocol routing architecture to hijack blockchain communications, which in turn causes a greater delay in the broadcasting of blocks. The study of [118] also demonstrates that an assault on a decentralized autonomous organization (DAO) stole Ethereum worth 50 million by exploiting a flaw in smart contracts.

**e) Privacy Leakage**

The transaction records that are maintained in blockchains may maintain a certain level of data privacy thanks to several measures that are included in blockchain technology. For instance, transactions in blockchain are carried out using users' IP addresses rather than their true identities, which helps to maintain a level of anonymity for those involved. In addition, in order to protect the anonymity of users, blockchain generates accounts that are only used once. However, these protective mechanisms are not as strong as they may be. For instance, the research presented in [119] demonstrates that user pseudonyms may be deciphered by studying and inferring the various transactions that are connected with one common user. According to [120], the entire storing of transaction data on blockchain might also lead to the possible leaking of private information.

**f) Fault Tolerance:**

RPL is designed to handle the dynamic nature of IoT networks, including device failures and network disruptions. Blockchainbased RPL systems should be resilient to failures and able to recover quickly in such scenarios. Exploring faulttolerant mechanisms and consensus protocols that can adapt to the constraints of RPL networks is an important area of research.

**g) Governance and Standards:**

The integration of blockchain with RPL requires defining governance models, consensus rules, and standards for interoperability. Research is needed to develop effective governance frameworks and consensus mechanisms that can be adopted in RPL based blockchain networks while considering the unique requirements and constraints of low power networks. These are just a few examples of the open research issues in applying blockchain to RPL. Continued research and innovation in these areas will help overcome the challenges and pave the way for efficient and secure blockchain based routing solutions in low power networks.

## 13 Conclusion & Future Study

We conducted a Systematic Literature Review to investigate the factors that impact the blockchain's flexibility, integrity, and anonymity in order to have a better understanding of how the blockchain is used in the RPL routing protocol. The ultimate goal of our study is to combine blockchain technology and peer to peer networking to develop an Internet of Things that is designed to be private and does not depend on centralized organizations to manage device data. Within the scope of this research project, we investigate the feasibility of combining blockchain technology with the RPL routing system. We are referring to the amalgamation of blockchain technology and RPL here. We have compiled a large corpus of research on the topic for your perusal. To begin, we will provide a high level overview of blockchain technology, with special attention to RPL. Following that, we will discuss the benefits of using blockchain technology and demonstrate its organizational framework. The difficulties that have been encountered in blockchain research with regard to next generation networks are then spoken about. In addition to this, we discuss several possible uses of blockchain technology and set out some uncharted territory for future blockchain research. We went through many different blockchain applications and technology. Even though only a small number of them are expressly developed for the Internet of Things, we uncovered a variety of use cases for a private and decentralized data management that are congruent with the purpose of our study. We made the discovery that large blockchain systems, like as Bitcoin, are the safest in terms of integrity and adaptability, but that these types of systems are less appropriate for the Internet of Things owing to the issues associated with scaling. When it comes to maintaining users' anonymity, we found that the blockchain can only provide a guarantee of pseudonymity. In the work that we have planned for the future, we will be analyzing blockchains that are currently in existence and that are secure and scalable. Based on the blockchains that prove to be the most useful, we will construct a layered architecture for Internet of Things applications. This will allow us to meet the problems of maintaining data integrity and adjusting to changing conditions. We will investigate mixing procedures in addition to looking at other possible approaches in order to better protect the privacy of individuals and achieve anonymity.

## References

[1] D. Estrin et al., "Instrumenting the World with Wireless Sensor Networks, " Proc. Int'l. Conf. Acoustics, Speech and Signal Processing, Salt Lake City, UT, May 2001.
[2] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J. P. and Alexander, R., 2012. RPL: IPv6 routing protocol for lowpower and lossy networks (No. rfc6550).
[3] F. Stajano and R. J. Anderson, "The Resurrecting Duckling: Security Issues for Adhoc Wireless Networks, " Proc.7th Int'l. Wksp. Security Protocols, London: SpringerVerlag, 2000, pp.17294.
[4] Y. C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing, " IEEE Security Privacy Special Issue: Making Wireless Work, vol.2, no.3, May/June 2004, pp.2839.
[5] D. Djenouri, L. Khelladi, and N. Badache, "A Survey on Security Issues in Mobile Ad Hoc and Sensor Networks, " IEEE Commun. Surveys and Tutorials, vol.7, no.4, 2005
[6] G. Paul, P. Sarkar, and S. Mukherjee, "Towards a more democratic mining in Bitcoins, " inProc.10th Int. Conf. Inf. Syst. Security (ICISS), Hyderabad, India, Dec.2014, pp.185203.
[7] Ralph C Merkle. A digital signature based on a conventional encryption function. In Conference on the Theory and Application of Cryptographic Techniques, Springer, 1987, pp.369378
[8] Maxmen, "Ai researchers embrace bitcoin technology to share medical data, "Nature, Mar.2018, vol.555,

pp.293294.
[9] Biggs John. Hackers release source code for a powerful DDoS app called Mirai, October 2016.
[10] T. M. Fern´andezCaram´es and P. FragaLamas, “A review on the use of blockchain for the Internet of Things, ”IEEE Access, vol.6, pp.3297933001, 2018.
[11] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, “Decentralized consensus for edgecentric Internet of Things: A review, taxonomy, and research issues, ”IEEE Access, vol.6, pp.1513 1524, 2018.
[12] Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, “Blockchain and IoT integration: A systematic survey, ”Sensors, vol.18, no.8, p.2575, 2018
[13] Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, and Mubashir Husain Rehmani, “Applications of Blockchains in the Internet ofThings: A Comprehensive Survey”, IEEE COMMUNICATIONS SURVEYS TUTORIALS, 2019, VOL.21, NO.2, pp.16761717.
[14] T. Neudecker and H. Hartenstein, “Network layer aspects of permissionless blockchains, ”IEEE Commun. Surveys Tuts., to be published, doi: 10.1109/COMST.2018.2852480.
[15] M. Conoscenti, A. Vetr`o, and J. C. De Martin, “Blockchain for theInternet of Things: A systematic literature review, ” inProc. IEEE/ACS13th Int. Conf. Comput. Syst. Appl., 2016, pp.16.
[16] R. B. Uriarte and R. De Nicola, “Blockchainbased decentralized cloud/fog solutions: Challenges, opportunities, and standards, ”IEEECommun. Standards Mag., vol.2, no.3, pp.2228, Sep.2018
[17] Reyna, C. Mart´ın, J. Chen, E. Soler, and M. D´ıaz, “On blockchain and its integration with IoT. Challenges and opportunities, ”Future Gener. Comput. Syst., vol.88, pp.173190, Nov.2018
[18] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, “Untangling blockchain: A data processing view of blockchain systems, ”IEEE Trans. Knowl. Data Eng., vol.30, no.7, pp.1366 1385, Jul.2018
[19] KHALED SALAH, M. HABIB UR REHMAN, NISHARA NIZAMUDDIN, and ALA ALFUQAHA, “Blockchain for AI: Review andOpen Research Challenges”, IEEE Access, 2019, Vol 7, pp.1012710149.
[20] Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko, and Y. Alexandrov, “Smart check: Static analysis of ethereum smart contracts, ” inProc. IEEE/ACM 1st Int. Workshop Emerg. Trends Softw. Eng. Blockchain (WETSEB), May/Jun.2018, , pp.916.
[21] X. Boyen, C. Carr, and T. Haines, “Graphchain: A blockchainfree scalable decentralised ledger, ” inProc.2nd ACM Workshop Blockchains, Cryptocurrencies, Contracts, 2018, pp.2133
[22] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, andV. Sassone, “PBFT vs proofofauthority: Applying the CAP theorem to permissioned blockchain, ” inProc. ITASEC, 2018, pp.111.
[23] L. Wallgren, S. Raza, T. Voigt, Routing attacks and countermeasures in the RPLbased internet of things, Int. J. Distrib. Sens. Netw.2013 (2013) 11.
[24] Aris, S. F. Oktug, S. B. O. Yalcin, Internetofthings security: denial of service attacks, in: Proceedings of the 23th Signal Processing and Communications Applications Conference (SIU), 2015, pp.903906, doi: 10.1109/SIU.2015.7129976.
[25] P. Pongle, G. Chavan, A survey: attacks on RPL and 6Lowpan in IOT, in: Proceedings of the International Conference on Pervasive Computing (ICPC), 2015, pp.16.
[26] Mayzaud, R. Badonnel, I. Chrisment, A taxonomy of attacks in RPLbased internet of things, Int. J. Netw. Secur.18 (3) (2016) 459473, .
[27] Arı ¸s, S. F. Oktug, ˘ T. Voigt, Security of Internet of Things for a Reliable Internet of Services, Springer International Publishing, Cham, pp.337370, doi: 10.1007/978331990415313.
[28] S. Otoum, B. Kantarci, H. T. Mouftah, Detection of known and unknown intrusive sensor behavior in critical applications, IEEE Sens. Lett.1 (5) (2017) 14, doi: 10.1109/LSENS.2017.2752719.
[29] S. Otoum, B. Kantarci, H. Mouftah, Adaptively supervised and intrusionaware data aggregation for wireless sensor clusters in critical infrastructures, in: Proceedings of the IEEE International Conference on Communications (ICC), 2018, pp.16, doi: 10.1109/ICC.2018.8422401.
[30] B. Zarpelo, R. S. Miani, C. T. Kawakani, S. C. de Alvarenga, A survey of intrusion detection in internet of things, J. Netw. Comput. Appl.84 (2017) 2537, doi: 10.1016/j. jnca.2017.02.009. /
[31] Khalid, U. ; Asim, M. ; Baker, T. ; Hung, P. C. K. ; Tariq, M. A. ; Rafferty, L. A decentralized lightweight blockchainbased authentication mechanism for IoT systems. Clust. Comput.2020, 23, 20672087.
[32] Tahir, M. ; Sardaraz, M. ; Muhammad, S. ; Saud Khan, M. A Lightweight Authentication and Authorization Framework for BlockchainEnabled IoT Network in HealthInformatics. Sustainability 2020, 12, 6960.
[33] Kumari, A. ; Chintukumar Sukharamwala, U. ; Tanwar, S. ; Raboaca, M. S. ; Alqahtani, F. ; Tolba, A. ; Sharma, R. ; Aschilean, I. ; Mihaltan, T. C. BlockchainBased PeertoPeer Transactive Energy Management Scheme for Smart Grid System. Sensors 2022, 22, 4826.
[34] Haqani, E. A. ; Baig, Z. ; Jiang, F. A Decentralised BlockchainBased Secure Authentication Scheme for IoT Devices. In Inventive Systems and Control; Lecture Notes in Networks and Systems; Suma, V., Baig, Z., Kolandapalayam
[35] Shanmugam, S., Lorenz, P., Eds. ; Springer Nature: Singapore, 2022; pp.123144.22. Hussain AlNaji, F. ; Zagrouba, R. CABIoT: Continuous authentication architecture based on Blockchain for internet of things. J. King Saud Univ. Comput. Inf. Sci.2022, 34, 24972514.
[36] J. Vasseur, M. Kim, K. Pister, and H. Chong, “Routing metrics used for path calculation in low power and lossy networks,

draftietfrollroutingmetrics04 (work in progress), ” December 2009.
[37] Tripathi, J., De Oliveira, J. C. and Vasseur, J. P., 2010, October. Applicability study of RPL with local repair in smart grid substation networks. In 2010 First IEEE international conference on smart grid communications (pp.262267). IEEE.
[38] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things, ” IEEE Access, vol.4, pp.22922303, 2016.
[39] Z. Zheng, S. Xie, H. Dai, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends, ” in Proc. IEEE Int. Congr. Big Data, Big Data Congr., Honolulu, HI, USA, Jun.2017, pp.557564. [40] E. Karafiloski and A. Mishev, “Blockchain solutions for big data challenges: A literature review, ” in Proc. IEEE Int. Conf. Smart Technol., Ohrid, Macedonia, Jul.2017, pp.763768.
[40] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, “Blockchain technology innovations, ” in Proc. IEEE Technol., Eng. Manage. Conf. (TEMSCON), Santa Clara, CA, USA, Jun.2017, pp.137141.
[41] M. Conoscenti, A. Vetro`, and J. C. De Martin, “Blockchain for the Internet of Things: A systematic literature review, ” in Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA), Agadir, Morocco, Nov. /Dec.2016, pp.16.
[42] J. YliHuumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where is current research on blockchain technology?—A systematic review, ” PLoS ONE, vol.11, no.10, p. e0163477, 2016.
[43] M. R. Biktimirov, A. V. Domashev, P. A. Cherkashin, A. Y. Shcherbakov, Blockchain technology: Universal structure and requirements, Autom. Doc. Math. Linguist.51 (6) (2017) 235238.
[44] S. Raval, Decentralized Applications: Harnessing Bitcoin’s Blockchain Technology, 1st ed. Newton, MA, USA: O’Reilly Media, Aug.2016
[45] Z. Zheng, S. Xie, H. N. Dai, and H. Wang, “Blockchain challenges and opportunities: A survey, ” Int. J. Web Grid Services, vol.14, no.4, pp.123, 2017.
[46] N. Szabo, “Formalizing and securing relationships on public networks, ” First Monday, vol.2, no.9, 1997.
[47] J. A. T. Fairfield, “Smart contracts, bitcoin bots, and consumer protection, ” Washington Lee Law Rev. Online, vol.71, no.2, pp.3550, 2014.
[48] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog computing and its role in the Internet of Things, ” presented at the 1st edition MCC Workshop Mobile Cloud Comput., Helsinki, Finland, Aug.2012, pp.1316.
[49] M. Sua´rezAlbela, T. M. Fern´andezCaram´es, P. FragaLamas, and L. Castedo, “A practical evaluation of a highsecurity energyeficient gateway for IoT fog computing applications, ” Sensors, vol.17, no.9, p.1978, Aug.2017
[50] Antonopoulos A. M. Mastering Bitcoin: Unlocking Digital CryptoCurrencies (first ed. ), O’Reilly Media, Inc. (2014)
[51] M. Swan, Blockchain: Blueprint for a New Economy, 1st ed. Newton, MA, USA: O’Reilly Media, Jan.2015
[52] T. Swanson. Consensusasaservice: A Brief Report on the Emergence of Permissioned, Distributed Ledger System. Accessed: Apr.10, 2018. [Online]. Available: http://www. ofnumbers. com/wpcontent/uploads/2015/04/Permissioneddistributedledgers. pd
[53] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things, ” IEEE Access, vol.4, pp.22922303, 2016
[54] M. Conoscenti, A. Vetr`o, and J. C. De Martin, “Blockchain for the Internet of Things: A systematic literature review, ” in Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA), Agadir, Morocco, Nov. /Dec.2016, pp.16
[55] W¨orner and T. von Bomhard, “When your sensor earns money: Exchanging data for cash with Bitcoin, ” in Proc. UbiComp Adjunct, Seattle, WA, USA, Sep.2014, pp.295298.
[56] Y. Zhang and J. Wen, “An IoT electric business model based on the protocol of Bitcoin, ” in Proc.18th Int. Conf. Intell. Next Gener. Netw., Paris, France, Feb.2015, pp.184191.
[57] S. Wilkinson et al. Storj a PeertoPeer Cloud Storage Network. Accessed: Apr.10, 2018. [Online]. Available: https://storj. io/storj. pdf
[58] G. Ateniese, M. T. Goodrich, V. Lekakis, C. Papamanthou, E. Paraskevas, and R. Tamassia, “Accountable storage, ” in Proc. Int. Conf. Appl. Cryptogr. Netw. Secur., Kanazawa, Japan, Jul.2017, pp.623644.
[59] Wilson and G. Ateniese, “From pretty good to great: Enhancing PGP using Bitcoin and the blockchain, ” in Proc. Int. Conf. Netw. Syst. Secur., New York, NY, USA, Nov.2015, pp.368375.
[60] [66] B. Gipp, N. Meuschke, and A. Gernandt, “Decentralized trusted timestamping using the crypto currency Bitcoin, ” in Proc. iConf., Newport Beach, CA, USA, Mar.2015, pp.15.
[61] Han, H. Kim, and J. Jang, “Blockchain based smart door lock system, ” in Proc. Int. Conf. Inf. Commun. Technol. Convergence (ICTC), Jeju Island, South Korea, Dec.2017, pp.11651167.
[62] Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, “Blockchainbased dynamic key management for heterogeneous intelligent transportation systems, ” IEEE Internet Things J., vol.4, no.6, pp.18321843, Dec.2017.
[63] M. Siddiqi, S. T. All, V. Sivaraman, “Secure lightweight contextdriven data logging for bodyworn sensing devices, ” in Proc.5th Int. Symp. Digit. Forensic Secur. (ISDFS), Tirgu Mures, Romania, 2017, pp.16.
[64] N. Kshetri, “Can blockchain strengthen the Internet of Things?” IT Professional, vol.19, no.4, pp.6872, 2017.
[65] C. Tanas, S. DelgadoSegura, and J. HerreraJoancomart´ı, “An integrated reward and reputation mechanism for MCS preserving users’ privacy, ” in Proc.10th Int. Workshop Data Privacy Manage., Secur. Assurance, vol.9481. New York, NY, USA: SpringerVerlag, 2016, pp.8399
[66] Wright and F. P. De. (Mar.2015). Decentralized

Blockchain Technology and the Rise of Lex Cryptographia. Accessed: Apr.10, 2018. [Online]. Available: https://ssrn. com/abstract=2580664

[67] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy, " Telecommun. Policy, vol.41, no.10, pp.10271038, 2017.

[68] Tian, "An agrifood supply chain traceability system for China based on RFID blockchain technology, " in Proc.13th Int. Conf. Service Syst. Service Manage. (ICSSSM), Kunming, China, Jun.2016, pp.16.

[69] P. Mueller, A. Rizk, and R. Steinmetz. (2017). BlockChain a New Foundation for Building Trustworthy and Secure Distributed Applications (DAPP's) of the Future. Accessed: Dec.12, 2018 [Online]. Available: http://dspace. icsy. de: 12000/dspace/handle/ 123456789/432

[70] R. C. Merkle, "A digital signature based on a conventional encryption function, " in Proc. Adv. Cryptol. (CRYPTO), 2000, pp.369378.

[71] S. Nakamoto. Bitcoin: A PeertoPeer Electronic Cash System. Accessed: Dec.12, 2018. [Online]. Available: http://bitcoin. org/bitcoin. pdf

[72] Wood, "Ethereum: A secure decentralised generalised transaction ledger, " Zug, Switzerland, Ethereum Project, Yellow Paper, 2014

[73] P. G. Lopez et al., "Edgecentric computing: Vision and challenges, " ACM SIGCOMM Comput. Commun. Rev., vol.45, no.5, pp.3742, Sep.2015. [Online]. Available: http://doi. acm. org/10.1145/2831347.2831354

[74] Halpin and M. Piekarska, "Introduction to security and privacy on the blockchain, " in Proc. IEEE Eur. Symp. Security Privacy Workshops (EuroSPW), Paris, France, 2017, pp.13.

[75] L. M. Axon and M. Goldsmith, PBPKI: A Privacy Aware BlockchainBased PKI, vol.6, SCITEPRESS, 2016, doi: 10.5220/0006419203110318.

[76] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, "World of empowered IoT users, " in Proc. IEEE 1st Int. Conf. Internet Things Design Implement. (IoTDI), Berlin, Germany, 2016, pp.1324.

[77] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the Internet of Things, " PeertoPeer Netw. Appl., vol.10, no.4, pp.983994, 2017.

[78] Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Fairaccess: A new blockchainbased access control framework for the Internet of Things, " Security Commun. Netw., vol.9, no.18, pp.59435964, 2016.

[79] T. Le and M. W. Mutka, "CapChain: A privacy preserving access control framework based on blockchain for pervasive environments, " in Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP), Jun.2018, pp.5764.

[80] G. Zyskind, O. Nathan, and A. Pentland. (2015). Enigma: Decentralized Computation Platform With Guaranteed Privacy. Accessed: Dec.12, 2018. [Online]. Available: https://enigma. co/enigmaf ull. pdf

[81] T. Le and M. W. Mutka, "CapChain: A privacy preserving access control framework based on blockchain for pervasive environments, " in Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP), Jun.2018, pp.5764.

[82] EsSamaali, A. Outchakoucht, and J. P. Leroy, "A blockchainbased access control for big data, " Int. J. Comput. Netw. Commun. Security, vol.5, no.7, p.137, 2017.

[83] H. Park and J. H. Park, "Blockchain security in cloud computing: Use cases, challenges, and solutions, " Symmetry, vol.9, no.8, p.164, 2017.

[84] Kang et al., "Enabling localized peertopeer electricity trading among plugin hybrid electric vehicles using consortium blockchains, " IEEE Trans. Ind. Informat., vol.13, no.6, pp.31543164, Dec.2017.

[85] S. Ali, K. Dolui, and F. Antonelli, "IoT data privacy via blockchains and IPFS, " in Proc.7th Int. Conf. Internet Things, 2017, Art. no.14.

[86] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data, " in Proc. IEEE Int. Conf. Web Services (ICWS), Honolulu, HI, USA, 2017, pp.468475.

[87] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchainbased reputation system for data credibility assessment in vehicular networks, " in Proc. IEEE 28th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC), 2017, pp.15.

[88] M. Axon and M. Goldsmith, PBPKI: A Privacy Aware BlockchainBased PKI, vol.6, SCITEPRESS, 2016, doi: 10.5220/0006419203110318.

[89] S. C. Cha, J. F. Chen, C. Su, and K. H. Yeh, "A blockchain connected gateway for BLEbased devices in the Internet of Things, " IEEE Access, vol.6, pp.2463924649, 2018

[90] Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home, " in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops), 2017, pp.618623.

[91] S. Ali, K. Dolui, and F. Antonelli, "IoT data privacy via blockchains and IPFS, " in Proc.7th Int. Conf. Internet Things, 2017, Art. no.14.

[92] Alphand et al., "IoTchain: A blockchain security architecture for the Internet of Things, " in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Barcelona, Spain, 2018, pp.16.

[93] M. Vucini ˇ c´ et al., "OSCAR: Object security architecture for the Internet of Things, " Ad Hoc Netw., vol.32, pp.316, Sep.2015.

[94] Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things, " J. Softw. Eng. Appl., vol.9, no.10, p.533, 2016.

[95] Alcaide, E. Palomar, J. MonteroCastillo, and A. Ribagorda, "Anonymous authentication for privacypreserving IoT target driven applications, " Comput. Security, vol.37, pp.111123, Sep.2013.

[96] X. J. Lin, L. Sun, and H. Qu, "Insecurity of an anonymous authentication for privacypreserving IoT targetdriven applications, " Comput. Security, vol.48, pp.142149, Feb.2015

[97] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the Internet of Things, " PeertoPeer Netw. Appl., vol.10, no.4, pp.983994, 2017.

[98] Ouaddah, A. A. Elkalam, and A. A. Ouahman,

"Towards a novel privacypreserving access control model based on blockchain technology in IoT, " in Proc. Europe MENA Cooper. Adv. Inf. Commun. Technol., 2017, pp.523533.

[99] Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Fairaccess: A new blockchainbased access control framework for the Internet of Things, " Security Commun. Netw., vol.9, no.18, pp.59435964, 2016.

[100] N. Foukia, D. Billard, and E. Solana, "PISCES: A framework for privacy by design in IoT, " in Proc.14th Annu. Conf. Privacy Security Trust (PST), 2016, pp.706713.

[101] M. A. Walker, A. Dubey, A. Laszka, and D. C. Schmidt, "PlaTIBART: A platform for transactive IoT blockchain applications with repeatable testing, " in Proc.4th Workshop Middleware Appl. Internet Things, 2017, pp.1722.

[102] G. Ayoade, V. Karande, L. Khan, and K. Hamlen, "Decentralized IoT data management using blockchain and trusted execution environment, " in Proc. IEEE Int. Conf. Inf. Reuse Integr. (IRI), Jul.2018, pp.1522.

[103] J. Kang et al., "Enabling localized peertopeer electricity trading among plugin hybrid electric vehicles using consortium blockchains, " IEEE Trans. Ind. Informat., vol.13, no.6, pp.31543164, Dec.2017.

[104] Z. Li et al., "Consortium blockchain for secure energy trading in industrial Internet of Things, " IEEE Trans. Ind. Informat., vol.14, no.8, pp.36903700, Aug.2018.

[105] Swan M. Blockchain: Blueprint for a New Economy. "O'Reilly Media, Inc. "; 2015.

[106] Proof of Stake; 2016. Accessed: 04/04/2023. https://en. bitcoin. it/wiki/Proof of Stake.

[107] Doubles pending; 2016. Accessed: 24/04/2023. https://en. bitcoin. it/wiki/Doublespending.

[108] Bitcoinwiki; 2015. Accessed: 24/4/2023. https://en. bitcoin. it

[109] Antonopoulos AM. Mastering Bitcoin: unlocking digital cryptocurrencies. "O'Reilly Media, Inc. "; 2014.

[110] Kitchenham B, Charters S. Guidelines for performing Systematic Literature Reviews in Software Engineering; 2007.

[111] Petersen K, Feldt R, Mujtaba S, Mattsson M. Systematic Mapping Studies in Software Engineering. In: Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering. EASE'08. Swinton, UK, UK: British Computer Society; 2008. p.6877. Available from: http://dl. acm. org/citation. cfm?id=2227115.2227123.

[112] Dyb˚a T, Dingsøyr T. Empirical studies of agile software development: A systematic review. Information and Software Technology.2008; 50 (910): 833859. http://dx. doi. org/10.1016/j. infsof.2008.01.006.

[113] Fernandez A, Insfran E, Abraho S. Usability evaluation methods for the web: A systematic mapping study. Information and Software Technology.2011; 53 (8): 789817. http://dx. doi. org/10.1016/j. infsof.2011.02.007.

[114] Reyna, C. Mart´ın, J. Chen, E. Soler, and M. D´ıaz, "On blockchain and its integration with IoT. Challenges and opportunities, " Future Gener. Comput. Syst., vol.88, pp.173190, Nov.2018.

[115] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in InternetofThings, " IEEE Internet Things J., vol.4, no.5, pp.12501258, Oct.2017.

[116] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems, " Future Gener. Comput. Syst., to be published. [Online]. Available: http://www. sciencedirect. com/science/article/pii/S0167739X17318332

[117] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies, " in Proc. IEEE Symp. Security Privacy (SP), San Jose, CA, USA, 2017, pp.375392.

[118] S. Adhami, G. Giudici, and S. Martinazzi, "Why do businesses go crypto? An empirical analysis of initial coin offerings, " J. Econ. Bus., vol.100, pp.6475, Nov. /Dec.2018. [Online]. Available: http://www. sciencedirect. com/science/article/pii/S0148619517302308

[119] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin, " IEEE Commun. Surveys Tuts., vol.20, no.4, pp.34163452, 4th Quart., 2018

[120] Dorri, S. S. Kanhere, and R. Jurdak, "MOFBC: A memory optimized and flexible blockchain for large scale networks, " Future Gener. Comput. Syst., vol.92, pp.357373, Jan.2019. [Online]. Available: http://www. sciencedirect. com/science/article/pii/S0167739X17329552