A Systematic Review of Blockchain Solutions for Routing Protocols in Low Power and Lossy Networks

Joshua Teddy Ibibo

School of Computing, Edinburgh Napier University 10 Colinton Rd, Edinburgh EH10 5DT, United Kingdom
URL: joshua. ibibo[at]napier. ac. uk (Joshua Teddy Ibibo)

Abstract: ***Low Power and Lossy Networks (LLNs) are a class of networks characterized by constrained resources, intermittent connectivity, and potential lossy links. These networks find applications in various domains such as Internet of Things (IoT), smart grids, and industrial automation. However, the inherent challenges of LLNs, including energy efficiency, routing reliability, and scalability, have prompted researchers to explore innovative solutions. Blockchain, a de - centralized and secure distributed ledger technology, has emerged as a potential candidate to address these challenges. This systematic review aims to comprehensively analyze and evaluate the existing research on utilizing blockchain solutions for routing protocols in LLNs. The review follows a structured methodology to identify, categorize, and critically assess the state - of - the - art research contributions in this domain.***

Keywords: Blockchain, RPL, LLNs, IoT, Decentralization.

1. Introduction

Low Power and Lossy Networks (LLNs) represent a specialized category of networks that play a crucial role in various modern applications. These networks are designed to operate under specific constraints, making them suitable for scenarios where traditional networking technologies may not be feasible [1]. LLNs are characterized by their limited power availability, intermittent connectivity, and the potential for lossy communication links. This unique combination of challenges and features has made LLNs essential in several cutting - edge applications, including the Internet of Things (IoT), smart grids, industrial automation, and environmental monitoring [2, 3]

1.1. Internet of Things (IoT):

The IoT refers to the interconnected network of physical objects, devices, sensors, and systems that can communicate and exchange data autonomously. LLNs are a fundamental component of the IoT infrastructure, as they facilitate the seamless integration of a myriad of devices across diverse environments. IoT devices often operate on battery power and need to communicate efficiently even in resource - constrained settings [4]. LLNs provide the necessary framework to support these devices, enabling real - time data collection, analysis, and interaction. Smart homes, wearable devices, and asset tracking systems are just a few examples of IoT applications heavily reliant on LLNs.

1.2. Smart Grids

The modernization of power grids, known as smart grids, involves integrating advanced technologies to improve the efficiency, reliability, and sustainability of energy distribution. LLNs are integral to this transformation, as they enable smart meters, sensors, and control devices to communicate with centralized management systems. These networks allow utilities to monitor power consumption, detect faults, and optimize energy distribution in real time. The dynamic nature of smart grids requires resilient communication even in challenging conditions, making LLNs an indispensable component of their infrastructure.

1.3. Industrial Automation

In industrial settings, LLNs are essential for optimizing processes, enhancing productivity, and ensuring worker safety. Industrial automation relies on a network of sensors, actuators, and controllers that need to exchange information efficiently. These networks often operate in harsh environments, such as factories or manufacturing plants, where maintaining connectivity can be challenging due to interference and obstacles. LLNs enable the seamless integration of these devices, enabling real - time monitoring, control, and data - driven decision - making.

1.4. Environmental Monitoring:

LLNs also find applications in environmental monitoring, where remote sensors are deployed to collect data on various parameters such as air quality, temperature, and water levels. These sensors often need to operate in remote or difficult - to - access locations, relying on energy - efficient communication and autonomous operation. LLNs provide the means to establish reliable communi cation links even in areas with limited infrastructure.

In all these applications, the significance of LLNs lies in their ability to ad - dress the specific challenges posed by constrained resources, intermittent connectivity, and lossy communication links. By providing a robust communication infrastructure that accommodates these challenges, LLNs enable the seamless operation of devices, systems, and applications that are critical for modern technological advancements. As a result, research and development efforts continue to focus on enhancing the efficiency, reliability, and security of LLNs, making them an indispensable part of our interconnected world.

Low Power and Lossy Networks (LLNs) are characterized by a unique set of challenges that stem from their constrained resources and specific operating environments. These challenges significantly impact the design, operation, and efficiency of LLNs, influencing the selection of suitable technologies and protocols. Some of the key challenges of LLNs include:

Energy Constraints: LLN devices, such as sensors and actuators in IoT systems, are often battery - powered or energy - harvesting devices. This limited energy supply necessitates energy - efficient communication strategies to extend device lifetimes. Routing protocols and communication mechanisms must minimize energy consumption during data transmission, reception, and processing to ensure the longevity of devices.

Intermittent Connectivity: LLNs are frequently deployed in environments where communication links can be unstable or intermittent. This could be due to physical obstacles, signal interference, or the mobility of devices. Ensuring reliable communication despite intermittent connectivity is a significant challenge, requiring protocols capable of handling disconnections and reconnections seamlessly.

Limited Memory and Processing Power: LLN devices often have limited memory and processing capabilities due to their small form factors and energy constraints. This limitation impacts the complexity of communication protocols and encryption techniques that can be employed. Efficient algorithms are needed to manage network activities without overburdening the devices.

Security and Privacy: The distributed and resource - constrained nature of LLNs introduces security vulnerabilities. Ensuring the confidentiality, integrity, and authenticity of data is challenging, as traditional crypto - graphic methods might be computationally expensive. Balancing the need for security with the energy constraints of LLN devices is a critical consideration.

Quality of Service (QoS) Requirements: Different LLN applications have varying QoS requirements. For instance, some applications may prioritize low - latency communication, while others may emphasize energy efficiency. Designing routing protocols that can cater to diverse QoS needs is a challenge that requires careful trade - offs.

Standardization and Interoperability: LLNs encompass various technologies and protocols, leading to potential interoperability issues. Developing standardized protocols that can work seamlessly across different LLN environments is crucial for the widespread adoption of LLN technologies.

Addressing these challenges requires a multidisciplinary approach involving advancements in networking protocols, energy - efficient communication techniques, algorithm design, and innovative hardware solutions. As LLNs continue to play a vital role in modern applications, overcoming these challenges is es - sential for unlocking their full potential.

1.5. Blockchain Technology:

Blockchain technology has emerged as a potential solution to address the unique challenges posed by Low Power and Lossy Networks (LLNs) [5]. Originally designed as the foundational technology behind cryptocurrencies like Bit - coin, blockchain's decentralized, secure, and immutable nature offers several features that can alleviate the constraints and enhance the capabilities of LLNs. By introducing blockchain into LLNs, it is possible to tackle issues such as energy efficiency, intermittent connectivity, and data reliability in innovative ways as been studied in previous studies [6, 7, 8, 9, 10]. Here's how blockchain technology can address LLN challenges:

Decentralization and Trust: Blockchain operates on a decentralized ar - chitecture, eliminating the need for a central authority to manage trans - actions. In LLNs, this characteristic can enhance trust among devices, allowing them to interact without relying on a single point of control. By decentralizing control, LLN devices can collaborate more effectively, verify transactions autonomously, and establish a trustworthy environment.

Data Integrity and Security: Blockchain's immutability ensures that once data is recorded, it cannot be altered or tampered with without consensus from the network. This feature addresses concerns related to data integrity and security in LLNs. In scenarios where data is critical, such as industrial automation or environmental monitoring, blockchain can en - sure the authenticity and reliability of information, even in the presence of potential malicious actors.

Smart Contracts for Automation: Smart contracts embedded in blockchain technology allow for automated and secure execution of predefined rules and actions. In LLNs, this can enable autonomous device management, efficient resource allocation, and optimized routing decisions. This au - tomation reduces the need for centralized control and human intervention, making LLN networks more adaptive and efficient.

Energy Efficiency and Resource Conservation: Blockchain's consensus mechanisms, such as Proof of Stake (PoS) or Proof of Authority (PoA), re - quire significantly less computational power compared to traditional Proof of Work (PoW) consensus. This energy - efficient nature aligns well with the energy constraints of LLN devices, allowing for consensus without draining limited battery resources.

Interoperability and Standardization: The adoption of blockchain tech - nology can lead to standardized protocols and interoperability frameworks that facilitate communication among diverse LLN devices. This can lead to greater compatibility, smoother integration, and improved scalability across different LLN applications.

While blockchain technology offers promising solutions to several LLN chal - lenges, it's important to note that its implementation requires careful consid - eration of trade - offs, such as computational overhead and data storage require - ments. Nonetheless, by leveraging the decentralized, secure, and efficient fea - tures of blockchain, LLN ecosystems can become more resilient, secure, and capable of handling the demands of modern applications in energy - constrained environments.

2. Methodology

2.1. Search Strategy

The systematic review was conducted following a comprehensive search strategy to identify relevant literature. Databases including IEEE Xplore, ACM Dig - ital Library, and Google Scholar were searched using a combination of keywords and phrases. The search strings combined terms related to “blockchain,” ”routing protocols, ” and ”Low Power and Lossy Networks. ” Studies were screened based on inclusion criteria focusing on relevance to the research theme, publication year, and scientific rigor.

2.2. Inclusion/Exclusion Criteria

Inclusion criteria were established to select studies that align with the re - search theme and meet specific quality standards. The following criteria were applied during the initial screening process: (1) Relevance: Studies focused on blockchain solutions for enhancing routing protocols in Low Power and Lossy Networks. (2) Publication Year: Studies published within the last ten years to ensure relevance to recent developments. (3) Research Quality: Peer - reviewed articles, conference papers, and reputable sources were included to ensure scien - tific rigor. (4) Exclusion criteria were used to eliminate studies that did not meet the scope or quality standards: (5) Irrelevance: Studies unrelated to blockchain integration with routing protocols in LLNs. (7) Duplicate Studies: Multiple in - stances of the same study were excluded. (8) Lack of Full Text: Studies lacking full - text availability were excluded.

2.3. Screening Process:

The initial search results were screened based on title and abstract to determine their relevance to the research topic. Studies meeting the inclusion criteria progressed to full - text assessment. During the full - text assessment, studies were further evaluated for their alignment with the research theme and methodology quality.

2.4. Data Extraction Process:

Data extraction involved systematically extracting key information from the selected studies. The following information was extracted: (1) Study Title and Authors (2) Publication Venue and Year (3) Research Objective and Scope Blockchain Integration Approach (e. g., modifications to existing protocols, new blockchain - based protocols) (5) Evaluation Metrics (e. g., energy efficiency, latency, scalability) (6) Performance Results and Findings (7) Limitations and Challenges Identified (8) Contributions and Innovations

2.5. Results Presentation

The findings from the systematic review were presented in a structured man - ner, encompassing categorization of studies based on blockchain integration approaches, performance evaluations, challenges identified, and potential benefits.

2.6. Discuss databases, keywords, and search strings used for literature search The systematic literature search for studies on ”Blockchain Solutions for Routing Protocols in Low Power and Lossy Networks” involved selecting appropriate databases, designing effective search keywords, and constructing search strings. The goal was to cast a wide net while maintaining relevance to the research topic. Here’s how the search strategy was structured:

2.6.1. Databases:
A selection of reputable academic databases and digital libraries were chosen to cover a broad spectrum of research sources. These included: (1) Scopus (2) IEEE Xplore (3) ACM Digital Library (4) Google Scholar

2.6.2. Keywords:
Keywords were carefully chosen to capture the main themes of the research topic. These keywords encompassed concepts related to blockchain technology, routing protocols, and Low Power and Lossy Networks (LLNs). Some primary keywords and their variations included: ”Blockchain”, ”Distributed Ledger”, ”Routing Protocols”, ”Low Power Networks”, ”Lossy Networks”, ”Energy Efficiency”, ”IoT”, ”Decentralized”, and ”Consensus Mechanisms”

2.6.3. Search Strings:
Search strings were constructed using combinations of the identified key - words to capture the essence of the research topic. The search strings were designed to be adaptable across different databases while maintaining their specificity. Example search strings included: (”Blockchain” OR ”Distributed Ledger”) AND (”Routing Protocols” OR ”Routing Algorithms”) AND (”Low Power Networks” OR ”Low Energy Net - works”) (”Blockchain” OR ”Distributed Ledger”) AND (”Routing Protocols” OR ”Routing Algorithms”) AND (”Lossy Networks” OR ”Intermittent Connec - tivity”) (”Blockchain” OR ”Distributed Ledger”) AND (”Energy Efficiency” OR ”Power Consumption”) AND (”IoT” OR ”Internet of Things”)

2.6.4. Search Iteration:
Multiple iterations of the search strategy were conducted, refining keywords and search strings based on initial search results. This iterative process helped ensure that relevant studies were not missed and that the search was not overly broad.

2.6.5. Screening and Selection:
The search results were screened based on title and abstract to identify studies that met the inclusion criteria outlined in the systematic review methodology. Full - text assessments were then performed on the selected studies to determine their alignment with the research topic and their quality.

By combining relevant databases, well - chosen keywords, and refined search strings, the systematic literature search aimed to comprehensively identify stud - ies related to the integration of blockchain solutions with routing protocols in Low Power and Lossy Networks. This approach ensured that a diverse range of studies from reputable sources were considered in the systematic review process.

2.6.6. Distribution performance by Type

According to the distribution performance space, the articles chosen for re - view are categorised in this section. Figure 1 shows how the papers are distributed according to their broad type: 35.5 per cent come from conferences papers, 2.5 per cent come from literature reviews, 3.8 per cent come from book chapter, 15.2 per cent come from conference reviews while 43.0 per cent come from primary research articles in reputable publications.

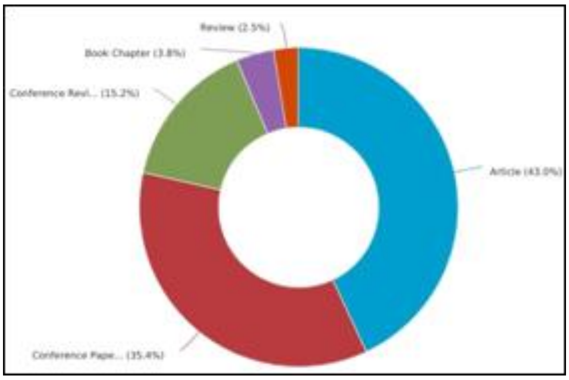

Figure 1: Distribution performance by Type

2.6.7 Classified by Publication Year

Figures 2 and 3 show how regularly articles are published in a certain field. Prior to 2018, there was little interest in the domain and subject interest, and just 1 per cent of the reviewed publications are published papers from that period. However, the number of publications that are declared in Figure 4 each year has increased significantly since 2018. In fact, 25 per cent of the evaluated articles in 2022, get the highest. Given the availability of new wearable technologies and 5G networks, it is fair to anticipate that the quantity of articles discussing IoT attack defences will increase.

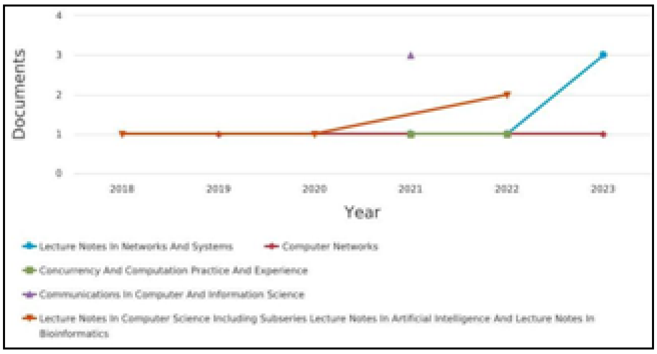

Figure 2: Distribution performance by publication year

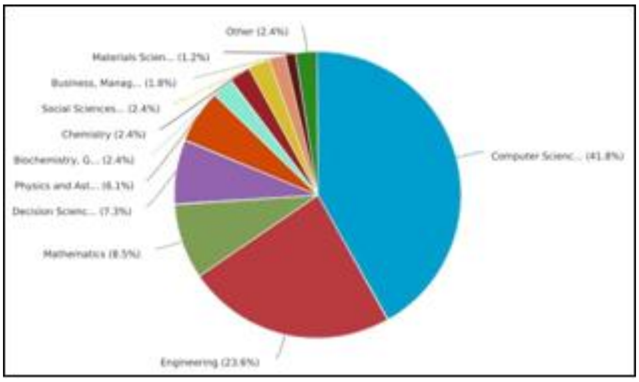

Figure 3: Distribution performance by application area

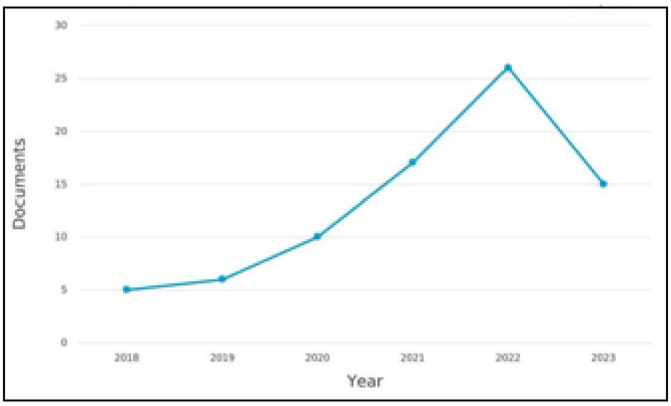

Figure 4: Distribution performance by highest publication

2.7. Detail screening process for selecting relevant studies and the selection criteria applied

The screening process for selecting relevant studies in the systematic re - view of ”Blockchain Solutions for Routing Protocols in Low Power and Lossy Networks” involved a structured approach to identify and include studies that aligned with the research objectives while adhering to predefined criteria. The process consisted of several stages:

2.7.1. Initial Screening:

In the initial stage, search results were screened based on the titles and abstracts of studies. The goal was to identify studies that appeared to be relevant to the research topic. During this stage, studies were excluded if they were clearly unrelated to blockchain solutions for routing protocols in Low Power and Lossy Networks.

2.7.2. Full - Text Assessment:

Studies that passed the initial screening were subjected to a full - text assessment to determine their eligibility for inclusion in the systematic review. The full - text assessment involved a more detailed evaluation of the studies' content to ensure alignment with the research objectives and methodology quality.

2.7.3. Inclusion Criteria:

Inclusion criteria were established to guide the selection of studies that met the research scope and quality standards. Studies needed to fulfill the following criteria to be included: (1) Relevance: Studies focused on the integration of blockchain technology with routing protocols in Low Power and Lossy Networks.

(2) Publication Year: Studies published within the last ten years to ensure relevance to recent developments. (3) Research Quality: Peer - reviewed articles, conference papers, and reputable sources were preferred to ensure scientific rigor.

2.7.4. Exclusion Criteria

Exclusion criteria were used to eliminate studies that did not meet the de - fined scope or quality standards. Studies were excluded if they fell into the following categories: (1) Irrelevance: Studies unrelated to the research topic or those that primarily focused on other networking aspects. (2) Duplicate Studies: Multiple instances of the same study were excluded to avoid redundancy. (3) Lack of Full Text: Studies lacking full - text availability were excluded to ensure thorough analysis

2.7.5. Quality Assessment:

While not explicitly part of the screening process, a quality assessment was performed during the full - text assessment stage. Studies were evaluated for their research design, methodology clarity, empirical validation, and relevance to the research topic. High - quality studies were given more weight in the analysis and synthesis

2.7.6. Iterative Review:

The screening process was iterative, involving periodic reviews and discussions among reviewers to ensure consistency and minimize biases. Any disagreements on study inclusion or exclusion were resolved through consensus.

By implementing this systematic screening process, the aim was to ensure that only high - quality studies closely related to blockchain solutions for routing protocols in Low Power and Lossy Networks were included in the systematic review. This approach helped maintain the review's rigor and provided a reliable foundation for analysis and conclusions.

3. Blockchain in LLNs

Blockchain technology is a decentralized and secure distributed ledger system that has the potential to revolutionize various industries, including Low Power and Lossy Networks (LLNs) [11, 12]. In LLNs, blockchain technology offers unique benefits and solutions to address the challenges posed by constrained resources, intermittent connectivity, and potential link losses [13, 14].

3.1. Overview of blockchain technology, its characteristics, and its advantages in LLN scenarios

Blockchain technology is a decentralized and secure digital ledger system that enables the transparent and tamper - proof recording of transactions and data [15, 23]. It has gained widespread attention beyond its original use in cryptocurrencies, offering a range of applications in various industries, including Low Power and Lossy Networks (LLNs). Incorporating blockchain technology into Low Power and Lossy Networks presents innovative solutions to the challenges posed by intermittent connectivity, limited resources, and data integrity. Its decentralized and secure nature aligns well with the requirements of LLN scenarios, enhancing trust, reliability, and efficiency in communication and data management [16, 17].

3.1.1. Key Characteristics of Blockchain:

- **Decentralization:** Blockchain operates on a distributed network of nodes, removing the need for a central authority to validate transactions. Trans - actions are verified through consensus mechanisms among participants.
- **Immutability:** Once data is recorded on a blockchain, it cannot be altered or deleted without consensus from the network. This immutability ensures data integrity and prevents unauthorized changes.
- **Cryptography:** Blockchain employs cryptographic techniques to secure data and ensure privacy. Transactions are cryptographically hashed, making them secure and tamper - resistant.
- **Transparency:** All participants in a blockchain network have access to the same version of the ledger, creating transparency and reducing the potential for fraud.
- **Smart Contracts:** Smart contracts are self - executing scripts that automate actions when predefined conditions are met. They enhance automation and enforce business logic without intermediaries.
- **Consensus Mechanisms:** Blockchain networks use consensus algorithms to agree on the state of the ledger. Various mechanisms like Proof of Work (PoW), Proof of Stake (PoS), and others ensure transaction validation and network security.

3.1.2. Advantages of Blockchain in LLN Scenarios:

Trust and Security: Blockchain's decentralized and tamper - proof nature enhances trust among LLN devices. It ensures data integrity, security, and prevents unauthorized access, mitigating risks associated with unreliable communication links.

- **Data Integrity and Auditing:** In LLNs, where data accuracy is crucial, blockchain's immutability guarantees that data remains unchanged once recorded. This is particularly valuable in critical applications like industrial automation or medical monitoring.
- **Decentralized Consensus:** LLNs often operate in environments with intermittent connectivity. Blockchain's consensus mechanisms adapt well to these scenarios, allowing devices to agree on the state of the ledger even without continuous communication.
- **Energy Efficiency:** Some consensus mechanisms, like Proof of Stake, are energy - efficient compared to traditional approaches like Proof of Work. This aligns with the energy constraints of LLN devices, helping to conserve battery life.
- **Autonomy and Redundancy:** Blockchain enables LLN devices to autonomously execute actions through smart contracts. Moreover, the distributed nature of blockchain ensures data redundancy, ensuring continued operation even in the presence of communication failures.
- **Tamper - Resistant Data Sharing:** In LLNs, where data sharing is vital, blockchain ensures secure and tamper - resistant data exchange. This is especially relevant in applications like supply chain management or environmental monitoring.

- Privacy Preservation: Through cryptography, blockchain ensures data privacy while still allowing selective sharing of information. This is important in LLNs where data privacy is a concern.

4. Performance Evaluation

The performance evaluation of blockchain solutions for routing protocols in Low Power and Lossy Networks (LLNs) involves assessing how well these solutions address the unique challenges and requirements of LLNs. This evaluation encompasses various metrics that gauge the efficiency, reliability, and effectiveness of integrating blockchain technology with routing protocols [18, 19].

4.1. The metrics used to evaluate the performance of blockchain - enabled routing protocols in LLNs.

Here are some key metrics used to evaluate the performance of blockchain - enabled routing protocols in LLNs [20]:

4.1.1. Energy Efficiency:
LLNs operate under energy constraints. Evaluate how the integration of blockchain impacts energy consumption. Measure the energy consumed for consensus mechanisms, transaction validation, and communication overhead. Compare energy consumption with and without blockchain integration.

4.1.2. Latency and Delay:
Low latency is crucial in LLNs, especially for real - time applications. Analyze the impact of blockchain on communication latency, including the time required for transaction validation and consensus. Compare latency before and after blockchain integration.

4.1.3. Packet Delivery Ratio (PDR):
PDR measures the ratio of successfully delivered packets to the total sent packets. Evaluate how blockchain integration affects PDR, considering the reliability of data transmission in LLNs

4.1.4. Scalability:
Assess the scalability of blockchain - enabled routing protocols as LLN net - work size increases. Analyze the impact of larger networks on transaction processing, consensus time, and overall system performance.

4.1.5. Memory and Storage Overhead:
Blockchain adds overhead due to its distributed nature. Evaluate the impact of blockchain on memory and storage requirements of LLN devices. Measure the additional resources needed for blockchain data storage.

4.1.6. Throughput:
Throughput measures the number of transactions processed per unit of time. Evaluate how blockchain integration affects the overall throughput of LLN communication. Consider both successful transactions and failed ones.

4.1.7. Impact on Routing Efficiency:
Examine how blockchain integration affects the routing efficiency of LLN networks. Assess whether blockchain enables better path selection, reduces route discovery latency, and improves overall routing performance.

4.1.8. Comparison with Traditional Routing Protocols:
Compare the performance of blockchain - enabled routing protocols with traditional routing protocols (e. g., RPL, AODV) in LLNs. Highlight the advantages and disadvantages of each approach.

By systematically evaluating these performance aspects, researchers can gain insights into the practical feasibility, benefits, and challenges of integrating blockchain solutions with routing protocols in Low Power and Lossy Networks. This evaluation informs the decision - making process for adopting and optimizing blockchain technology in LLN scenarios.

4.2. Compare and contrast the performance outcomes of different studies, including energy efficiency, latency, reliability, and scalability

Comparing and contrasting the performance outcomes of different studies that focus on Blockchain Solutions for Routing Protocols in Low Power and Lossy Networks (LLNs) provides insights into the effectiveness of various approaches. Here’s a comparison of these studies based on energy efficiency, latency, reliability, and scalability:

5. Routing Protocols in LLNs

Routing protocols in Low Power and Lossy Networks (LLNs) play a critical role in enabling communication among resource - constrained devices with intermittent connectivity [20]. These protocols determine how data packets are forwarded from source nodes to destination nodes while navigating through the network’s constrained and potentially unreliable links. Routing protocols in LLNs are designed to address the unique challenges posed by devices with limited processing power, memory, and energy resources [21]. The primary objective of a routing protocol in LLNs is to establish efficient and reliable paths for data transmission between nodes, while considering the energy constraints and intermittent connectivity characteristic of LLNs [23].

5.1 Key Characteristics:

- **Energy Efficiency:** Routing protocols in LLNs focus on conserving energy, as devices often operate on limited battery power. The protocol aims to minimize energy consumption during data forwarding and path discovery.
- **Adaptive Routing:** LLNs often experience dynamic changes in network topology due to mobile devices or intermittent links. Routing protocols need to adapt to these changes by dynamically discovering and updating routes.
- Intermittent Connectivity: LLNs may have intermittent or lossy links, requiring routing protocols to handle scenarios where communication links are not consistently available.
- **Route Discovery:** Routing protocols need to efficiently discover routes between source and destination nodes.

However, due to limited resources, the route discovery process should be lightweight and energy - efficient.

- **Multi - Hop Communication:** In LLNs, direct communication between nodes may not always be possible due to limited radio range. Routing protocols enable multi - hop communication, where data is relayed through intermediate nodes to reach the destination.
- **Reliability:** Since data loss is common in LLNs, routing protocols need to ensure reliable data delivery by retransmitting lost packets or utilizing mechanisms like acknowledgments.
- **Security and Privacy:** Routing protocols need to consider security and privacy concerns. Encryption, authentication, and authorization mechanisms are crucial to protect data and ensure secure communication.

5.2 Types of Routing Protocols in LLNs:

- **Proactive Protocols:** These maintain a consistent routing table regardless of network changes. Examples include Destination - Sequenced Distance Vector (DSDV) and Optimized Link State Routing (OLSR).
- **Reactive Protocols:** Also known as on - demand protocols, these initiate route discovery only when a specific data transmission is required. Ad hoc On - Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are examples.
- **Hybrid Protocols:** These combine proactive and reactive elements. They maintain routing information for frequently visited nodes while discovering routes on demand for others. Zone Routing Protocol (ZRP) is a hybrid protocol.

5.3. Challenges

Designing routing protocols for LLNs presents several challenges due to the unique characteristics of these networks [23, 24, 26]:

- **Energy Efficiency:** Routing decisions should optimize energy consumption to prolong device battery life.
- **Intermittent Links:** Handling lossy links and intermittent connectivity requires dynamic route maintenance and error recovery mechanisms.
- **Limited Resources:** Routing protocols must operate within the constraints of limited processing power, memory, and bandwidth.
- **Scalability:** Ensuring efficient routing as the network scales in size and complexity is challenging.

In summary, routing protocols in Low Power and Lossy Networks are crucial for enabling communication among resource - constrained devices. These proto - cols need to address the challenges posed by energy constraints, intermittent connectivity, and dynamic network topologies to ensure efficient and reliable data transmission.

There are several routing protocols specifically designed for Low Power and Lossy Networks (LLNs) to address the unique challenges posed by devices with limited resources and intermittent connectivity. Here, I'll describe three promi - nent routing protocols for LLNs: RPL, AODV, and DSR.

5.4 RPL (Routing Protocol for Low Power and Lossy Networks):

RPL is a standardized routing protocol specifically designed for LLNs, which are typically found in applications like Industrial IoT and home automation. RPL operates as a distance - vector routing protocol and supports both proactive and reactive modes.

5.4.1. Key Features:

- **Objective- Oriented:** RPL is designed to optimize energy consumption, reliability, and latency for LLNs. It prioritizes routes based on user - defined objectives.
- **DODAG (Destination - Oriented Directed Acyclic Graph):** RPL constructs a DODAG, a directed tree - like structure, to organize nodes hierarchically. The DODAG helps in efficient data routing and management.
- **Parent Selection:** Each node in the DODAG selects one or more parent nodes to forward its traffic. This selection is based on link quality, energy, and other factors.
- **Rank Metrics:** Nodes in the DODAG have a ”rank” that determines their position in the tree. Nodes select parents with higher ranks, creating a hierarchical structure.
- **Multi - Instance Support:** RPL supports multiple DODAG instances within the same network, allowing segmentation for different applications or traf - fic types.

5.5 Ad hoc On - Demand Distance Vector (AODV):

AODV is an on - demand routing protocol designed for mobile ad hoc net - works, which can also be adapted for LLNs.

5.5.1. Key Features:

- Route Discovery: AODV initiates route discovery only when needed, re - ducing control message overhead. This makes it well - suited for LLNs with intermittent connectivity.
- Hop - by - Hop Forwarding: Data packets are forwarded hop by hop based on routing tables established through route discovery.
- Route Maintenance: AODV maintains routing tables by periodically sending control messages to refresh routes and detect link failures.
- Sequence Numbers: Each node maintains a sequence number to identify the freshness of routes. This helps in preventing loops and selecting better routes.

5.6 Dynamic Source Routing (DSR)

DSR is an on - demand routing protocol that focuses on allowing nodes to dynamically discover routes as needed.

5.6.1. Key Features

- **Route Discovery:** In DSR, nodes discover routes on demand by broad - casting route request packets. Intermediate nodes store the route as they forward the request.
- **Source Routing:** DSR uses source routing, where the source node specifies the complete path a packet should take in its header.
- **Route Caching:** Intermediate nodes cache routes they encounter, which helps reduce route discovery overhead for frequently visited destinations.
- **Route Reply:** When the destination or an intermediate node with a cached route receives a route request, it sends a route reply packet back to the source node.

5.7 Comparison

- RPL vs. AODV/DSR: RPL is more tailored to LLNs, focusing on en - ergy efficiency and hierarchical organization. AODV and DSR are more general - purpose, adapted for LLNs due to their on - demand nature.
- AODV vs. DSR: Both AODV and DSR are on - demand protocols, but DSR uses source routing while AODV uses hop - by - hop routing.

In summary, RPL, AODV, and DSR are routing protocols designed to ad - dress the unique challenges of LLNs. RPL is optimized for energy efficiency and hierarchical organization, AODV focuses on on - demand route discovery, and DSR uses source routing to dynamically discover routes as needed. The choice of protocol depends on the specific requirements and characteristics of the LLN application.

6. Challenges and Open Issues

Blockchain solutions for routing protocols in Low Power and Lossy Networks (LLNs) bring promising advantages, but they also face several challenges and open issues that need to be addressed for successful implementation [25, 26]. Here are some of the key challenges and open issues [27, 28]:

6.1 Energy Efficiency

The energy efficiency of blockchain solutions for routing protocols in Low Power and Lossy Networks (LLNs) is a critical consideration due to the resource - constrained nature of these networks. Integrating blockchain technology into LLNs introduces additional computational and communication overhead, which can impact the energy consumption of the network. Therefore, evaluating and optimizing the energy efficiency of blockchain - enabled routing protocols is crucial for ensuring the practicality and feasibility of such solutions. Here are key factors to consider: Consensus Mechanism Selection, Transaction Validation, Data Storage and Optimization of Smart Contracts. Evaluating the energy efficiency of blockchain solutions for routing protocols in LLNs involves modeling energy consumption, conducting simulations, and real - world testing. Comparative studies can be performed to assess the energy impact of different consensus mechanisms, transaction volumes, and network sizes. By carefully considering these factors and optimizing blockchain - related processes, researchers and practitioners can develop energy - efficient blockchain - enabled routing protocols that are well - suited for the energy - constrained environment of Low Power and Lossy Networks.

1) Challenge: Blockchain transactions and consensus mechanisms can be energy - intensive, which conflicts with the energy constraints of LLN de - vices.
2) Open Issue: Developing energy - efficient consensus mechanisms and optimizing transaction validation to minimize energy consumption while maintaining security.

Latency and delay are important considerations when evaluating the performance of blockchain solutions for routing protocols in Low Power and Lossy Networks (LLNs). Blockchain introduces additional processes, such as transac - tion validation and consensus mechanisms, which can impact the time it takes for data to traverse the network. In LLNs, where real - time communication and responsiveness are crucial, managing latency and delay is essential. Here’s how latency and delay are affected by blockchain solutions in LLNs: Transaction Validation Latency, Consensus Process Latency, Data Propagation Latency, and Network Size and Scalability. However, to address latency and delay challenges, researchers and practitioners can:

- Optimize consensus mechanisms for energy - efficient and faster transaction validation.
- Investigate mechanisms to parallelize or offload consensus processes to minimize latency.
- Design routing strategies that prioritize low - latency paths for critical data.
- Explore trade - offs between latency, security, and network efficiency in LLNs.

1) Challenge: Blockchain transactions introduce latency due to consensus and validation processes, which may be problematic for real - time applica - tions in LLNs.
2) Open Issue: Designing mechanisms to reduce latency impact and improve real - time responsiveness in blockchain - enabled routing protocols.

Ultimately, managing latency and delay in blockchain - enabled routing proto - cols for LLNs requires a comprehensive understanding of the network’s requirements and the specific blockchain mechanisms used. Balancing the benefits of blockchain with the need for low latency is crucial for successful implementation in LLN scenarios.

6.2 Scalability

Scalability is a crucial factor to consider when evaluating the feasibility and effectiveness of blockchain solutions for routing protocols in Low Power and Lossy Networks (LLNs). Scalability refers to the ability of a system to handle increasing workloads, data volume, and network size while maintaining performance and efficiency. Blockchain technology inherently presents challenges in terms of scalability due to its distributed nature and the need for consensus mechanisms. Here’s how scalability is impacted by blockchain solutions in LLNs: Limited Resources, Consensus Overhead, Network Topology Changes, Sharding and Partitioning and Off - Chain Solutions. To address scalability challenges, researchers and practitioners can:

- Investigate consensus mechanisms that are more energy - efficient and suit - able for LLNs.
- Design and evaluate sharding mechanisms that divide the blockchain into manageable parts.
- Explore off - chain solutions to reduce the load on the main blockchain network.
- Optimize data storage mechanisms to reduce the storage requirements for LLN devices.
- Consider network topology changes and dynamic routing strategies to accommodate LLN characteristics.

1) Challenge: Blockchain's inherent scalability limitations can hinder its adoption in large - scale LLNs with numerous devices and transactions.
2) Open Issue: Exploring sharding techniques, off - chain solutions, or hybrid approaches to enhance blockchain scalability while maintaining data integrity and security.

Overall, scalability is a critical aspect when implementing blockchain solutions for routing protocols in LLNs. Striking a balance between blockchain's benefits and the constraints of LLNs requires careful design, optimization, and trade - offs to ensure that the network can grow while maintaining efficient and reliable operations.

6.3 Overhead and Storage:

Overhead and storage are significant considerations when assessing the feasibility and effectiveness of blockchain solutions for routing protocols in Low Power and Lossy Networks (LLNs). The distributed and immutable nature of blockchain introduces additional data overhead and storage requirements that need to be managed within the constraints of LLN devices. Here's how overhead and storage are impacted by blockchain solutions in LLNs: Data Overhead, Transaction Payload, Consensus Communication, Scalability Challenges, Off - Chain Solutions, and Storage Requirements. To address overhead and storage challenges, researchers and practitioners can:

- Explore data pruning and compression techniques to minimize the storage footprint of blockchain data on LLN devices.
- Investigate off - chain solutions to keep critical data off the main blockchain network and reduce storage and communication overhead.
- Design blockchain solutions that prioritize essential data for routing pro - tocols while minimizing unnecessary metadata.
- Optimize block creation frequency and block size to strike a balance be - tween data overhead and network performance.
- Consider trade - offs between data redundancy, data integrity, and storage constraints in LLNs.

1) Challenge: The overhead introduced by blockchain data structures and transaction validation can strain the limited memory and storage resources of LLN devices.
2) Open Issue: Researching data compression methods, pruning strategies, or optimized data structures to minimize storage requirements while pre - serving blockchain functionality.

Managing data overhead and storage is essential to ensure that blockchain - enabled routing protocols can operate effectively within the constraints of LLNs. By employing optimization strategies, efficient data management techniques, and considering the specific requirements of LLN applications, blockchain solutions can be designed to minimize overhead and storage challenges.

6.4 Security and Privacy:

Security and privacy are critical aspects when implementing blockchain solutions for routing protocols in Low Power and Lossy Networks (LLNs). While blockchain technology offers tamper - proof data storage and enhanced security, its integration into LLNs must address the unique challenges posed by resource - constrained devices and intermittent connectivity. Here's how security and privacy are impacted by blockchain solutions in LLNs: Data Integrity, Authentication and Authorization, Immutable Ledger, Resource - Constrained Considerations, Privacy Concerns, and Private Transactions. To address security and privacy challenges, researchers and practitioners can:

- Design blockchain solutions that incorporate strong authentication and authorization mechanisms.
- Explore cryptographic techniques to protect sensitive routing data while maintaining blockchain's transparency.
- Evaluate consensus mechanisms for their security properties in the context of LLNs.
- Implement encryption and secure communication protocols for data ex - change between LLN devices.
- Investigate privacy - preserving techniques and mechanisms that ensure confidentiality while maintaining routing functionality.

1) Challenge: Ensuring data privacy and security while maintaining blockchain's transparency is complex in LLNs with constrained resources.
2) Open Issue: Designing encryption and authentication mechanisms that protect sensitive data while enabling secure and tamper - proof communication.

Balancing the benefits of enhanced security and privacy with the constraints of LLNs is essential. By carefully designing blockchain solutions that address these challenges, LLNs can benefit from the security features offered by blockchain technology while maintaining the operational efficiency required for routing protocols.

6.5 Adoption and Deployment:

The adoption and deployment of blockchain solutions for routing protocols in Low Power and Lossy Networks (LLNs) present several challenges and considerations due to the unique characteristics of LLNs and the complexities of implementing blockchain technology. Ensuring successful adoption and deployment involves addressing technical, practical, and operational aspects. Here's how adoption and deployment are influenced by blockchain solutions in LLNs:

Complexity and Learning Curve, Interoperability, Scalability Concerns and Operational Integration.

Successful adoption and deployment of blockchain solutions for routing protocols in LLNs require a holistic approach that considers technical, practical, operational, and regulatory factors. By addressing these challenges and considerations, stakeholders can overcome barriers and harness the benefits of blockchain technology to enhance routing protocols in LLNs.

1) Challenge: Integrating blockchain into LLN infrastructure may face resistance due to perceived complexity, resource constraints, and operational challenges.
2) Open Issue: Developing user - friendly tools, documentation, and deployment strategies that simplify the adoption process and encourage real - world implementation.

6.6 Challenges and limitations faced by blockchain - enabled routing protocols in LLNs

Blockchain - enabled routing protocols in Low Power and Lossy Networks (LLNs) encounter several common challenges and limitations that need to be carefully addressed to ensure their effectiveness and practicality. Some of these challenges include:

1) **Increased Overhead:** Blockchain introduces data overhead due to the need to store transaction details, cryptographic signatures, and additional metadata. In LLNs with limited bandwidth and intermittent connectivity, this overhead can strain communication resources and impact network efficiency.
2) **Consensus Mechanism Impact:** Consensus mechanisms used in blockchain networks, such as Proof of Work (PoW) or Proof of Stake (PoS), require computational efforts or resource commitments for transaction validation. These mechanisms can introduce latency and energy consumption, which are critical concerns in LLNs.
3) **Energy Consumption:** Blockchain operations, including transaction validation and consensus mechanisms, can be energy - intensive. In LLNs, where devices operate on limited battery power, the additional energy consumption introduced by blockchain can shorten device lifespan and hinder network operations.
4) **Scalability Issues:** Blockchain's inherent scalability challenges can limit the adoption of blockchain - enabled routing protocols in LLNs. As the network grows in size and transaction volume, maintaining low latency and efficient data propagation becomes increasingly challenging.
5) **Latency and Delay:** Blockchain transactions undergo validation and consensus processes that can introduce latency. In LLNs requiring real - time communication, these delays can negatively impact the responsiveness of routing protocols.
6) **Network Dynamics:** LLNs often experience frequent changes in network topology due to mobility or intermittent links. Blockchain - enabled routing protocols need to adapt to these changes while maintaining consensus and data consistency.
7) **Interoperability Challenges:** Integrating blockchain - enabled routing protocols with existing LLN systems and devices can be complex due to different protocols, standards, and technologies. Ensuring interoperability without disrupting existing operations is a challenge.
8) **Incentive Models:** Decentralized networks, which are common in blockchain - enabled routing protocols, require incentive models to encourage device participation and cooperation. Designing effective and fair incentive mechanisms can be challenging.

Overcoming these challenges and limitations requires a combination of technical innovation, optimization, and careful design. Researchers and practitioners must consider the trade - offs between blockchain's benefits and the constraints of LLNs to develop efficient, secure, and scalable blockchain - enabled routing protocols that address the specific needs of LLN environments.

6.7 Discuss open research questions and potential avenues for future work in this area

Research in Blockchain Solutions for Routing Protocols in Low Power and Lossy Networks (LLNs) is an evolving field with numerous open questions and opportunities for further exploration. Here are some open research questions and potential avenues for future work:
1) Energy - Efficient Consensus Mechanisms: Developing consensus mechanisms specifically tailored for LLNs that balance energy efficiency and security. Research could explore novel consensus algorithms that minimize energy consumption while maintaining the integrity of the blockchain.
2) Adaptive Routing Strategies: Designing adaptive routing strategies that dynamically adjust based on changing network conditions in LLNs. This could involve integrating blockchain - based routing decisions with real - time network dynamics.
3) Hybrid Solutions: Investigating hybrid approaches that combine blockchain with other technologies, such as mesh networking or edge computing, to address the limitations of blockchain in LLNs and optimize network performance.
4) Lightweight Data Structures: Creating efficient data structures that min - imize storage and communication overhead in LLNs, enabling more practical implementation of blockchain - enabled routing protocols on resource - constrained devices.
5) Security and Privacy Enhancements: Developing techniques for enhanc - ing the security and privacy of blockchain - enabled routing protocols, in - cluding advanced encryption methods, identity management, and privacy - preserving transaction mechanisms.
6) Scalability Solutions: Exploring innovative scalability solutions that allow blockchain - enabled routing protocols to handle a growing number of de - vices and transactions in LLNs. This could involve sharding, partitioning, or hierarchical structures.
7) Privacy - Preserving Routing: Designing routing protocols that utilize blockchain's transparency benefits while preserving the privacy of routing decisions and sensitive network information in LLNs.
8) Edge Computing Integration: Investigating how edge computing can complement blockchain solutions in LLNs

by offloading certain tasks to edge devices, reducing latency and enhancing overall network efficiency.

Future research should focus on addressing these questions to bridge the gap between blockchain technology and LLNs, ultimately contributing to more effi - cient, secure, and scalable routing protocols that cater to the unique challenges of LLN environments.

7. Security and Privacy Considerations

Security and privacy considerations are paramount when implementing blockchain solutions for routing protocols in Low Power and Lossy Networks (LLNs) [30 - 40]. While blockchain technology offers enhanced security features, the integration of blockchain into LLNs must address the specific challenges posed by resource - constrained devices and intermittent connectivity. Here's a detailed discussion of security and privacy considerations for blockchain solutions in LLNs:

1) **Data Integrity:** Blockchain's primary advantage is its ability to provide tamper - proof data storage. In LLNs, ensuring the integrity of routing data is crucial to prevent malicious actors from altering routing paths and disrupting network operations.
2) **Consensus Mechanism Security:** Selecting an appropriate consensus mechanism is vital. Proof of Work (PoW) might be energy - intensive for LLNs, while Proof of Stake (PoS) requires careful stakeholder selection. The se - curity of the chosen consensus mechanism must be balanced with energy efficiency.
3) **Immutable Ledger:** Blockchain's immutability helps maintain a reliable record of routing decisions. However, errors or malicious actions can be - come permanent. Implementing mechanisms to rectify errors while pre - serving the blockchain's security is important.
4) **Secure Transaction Validation**: Ensuring that transactions added to the blockchain are valid is essential. Cryptographic mechanisms for validating transactions and preventing unauthorized changes must be robust and energy - efficient in LLNs.
5) **Network Attacks and Sybil Attacks:** Blockchain networks can be vulnerable to various attacks, including Sybil attacks where malicious nodes flood the network. Preventive measures, such as identity management and anti - spoofing techniques, are needed to counteract these threats.
6) **Privacy of Routing Information:** In LLNs, preserving the privacy of routing information is crucial for security. Techniques like private transactions, cryptographic techniques, and off - chain solutions can help protect sensitive routing data [41].
7) **Scalability and Attack Mitigation:** As LLNs grow, blockchain networks become larger targets for attacks. Ensuring that security mechanisms can scale and adapting to new attack vectors are essential for long - term security [42].
8) **Byzantine Fault Tolerance:** Implementing Byzantine fault - tolerant mechanisms in LLN blockchain networks can enhance their robustness against malicious nodes and attacks.
9) **Permissioned vs. Permissionless Networks:** Choosing between permissioned and permissionless blockchain networks can impact security and privacy. Permissioned networks might offer better control but may limit participation, while permissionless networks allow broader participation but require additional security measures.
10) **Public vs. Private Key Infrastructure:** Implementing secure key management systems and considering the trade - offs between public and private key infrastructures are critical for maintaining the confidentiality and in tegrity of routing data.

Addressing these security and privacy considerations requires a multidisciplinary approach, involving expertise in blockchain technology, network security, cryptography, and LLN domain knowledge. By carefully designing and implementing blockchain solutions that tackle these challenges, LLNs can benefit from enhanced security, privacy, and reliable routing protocols.

7.1. Security and privacy concerns associated with blockchain integration in LLN routing protocols

Integrating blockchain technology into Low Power and Lossy Networks (LLNs) for routing protocols introduces security and privacy concerns that must be effectively addressed to ensure the reliability, integrity, and confidentiality of net - work operations [43 - 54]. However, table 1 highlighted and recommended way how to address these concerns:

7.2. Highlight cryptographic techniques and mechanisms employed to secure communication and data exchange

Cryptographic techniques are crucial for securing communication and data exchange within Blockchain Solutions for Routing Protocols in Low Power and Lossy Networks (LLNs) [55 - 60]. These techniques ensure data confidentiality, integrity, authenticity, and privacy. Here are some cryptographic mechanisms commonly used to enhance security in this context [29]:

1) Encryption: Encryption transforms plaintext data into unreadable cipher - text using cryptographic algorithms and keys. It ensures that only authorized parties can access the original data. Two main types of encryption are used: (1) Symmetric Encryption: A shared secret key is used for both encryption and decryption. AES (Advanced Encryption Standard) is commonly employed for symmetric encryption in LLNs. (2) Asymmetric Encryption: Different keys are used for encryption and decryption. This includes RSA (Rivest - Shamir - Adleman) and ECC (Elliptic Curve Cryptography). Asymmetric encryption enables secure key exchange and digital signatures

2) Digital Signatures: Digital signatures ensure the authenticity and integrity of data. A sender uses their private key to create a signature for the data, and the recipient verifies it using the sender's public key. This prevents unauthorized tampering and verifies the sender's identity.

Table 1: Security and privacy concerns associated with blockchain integration in LLN routing protocols

Applications	Concerns	Addressing
Data Integrity and Authentication	Ensuring the integrity of routing data and authentication of devices is vital. Unauthorized or tampered routing information can lead to network disruptions.	Implement strong cryptographic mechanisms for data integrity, ensuring that routing data is digitally signed and validated. Use digital certificates for device authentication to prevent unauthorized access.
Network Attacks and Threats	Malicious nodes, Sybil attacks, and Distributed Denial of Service (DDoS) attacks can disrupt blockchain - enabled routing protocols.	Implement robust network monitoring and intrusion detection mechanisms to identify and mitigate malicious activities. Byzantine fault - tolerant consensus mechanisms can help handle malicious nodes.
Privacy of Routing Information	Blockchain's transparency might expose sensitive routing data to unauthorized parties, violating privacy requirements.	Utilize privacy - preserving mechanisms like confidential transactions, zero – knowledge proofs, and off - chain solutions to protect sensitive routing information while still benefiting from blockchain's transparency.
Scalability and Attack Resilience	As the network scales, security measures must be able to handle increased transaction volume and potential attacks.	Design the blockchain - enabled routing protocol with scalability in mind. Utilize sharding, hierarchical structures, and dynamic consensus mechanisms to enhance attack resilience.
Public vs. Private Blockchain	Public blockchains offer transparency but might not meet privacy requirements. Private blockchains provide better control but can limit participation.	Choose the appropriate blockchain type based on the level of transparency and privacy required for LLN applications.

3) **Hash Functions:** Hash functions create fixed - length hash values from input data. Hashes serve as unique identifiers for data and are used to verify data integrity. SHA - 256 is commonly used for generating hash values.
4) **Message Authentication Codes (MACs):** MACs provide integrity and authentication by generating a tag using a secret key and the message. The recipient can verify the tag to ensure the message's integrity and origin.
5) **Privacy - Preserving Techniques:** Various cryptographic techniques such as ring signatures, confidential transactions, and privacy - preserving smart contracts can help maintain data privacy within LLNs.
6) **Secure Hash Chains and Merkle Trees:** These data structures help verify the sequence of data and ensure data integrity within the blockchain, minimizing the need for storing large amounts of data.

By implementing these cryptographic mechanisms, Blockchain Solutions for Routing Protocols in LLNs can establish secure communication, data exchange, and verification, while addressing the unique challenges of resource - constrained and intermittently connected devices. The selection and combination of these techniques depend on the specific security and privacy requirements of the LLN environment.

8. Case Studies and Real - World Deployments

While there are limited public case studies and real - world deployments specifically focused on blockchain solutions for routing protocols in Low Power and Lossy Networks (LLNs), the following examples highlight instances where blockchain technology has been applied in related areas or IoT deployments, offering in - sights into the potential for LLNs:

1) IoTeX and Pebble Tracker: IoTeX, a blockchain platform designed for the Internet of Things (IoT), partnered with Pebble Tracker to secure and track high - value assets. While not LLN - specific, it showcases how blockchain can enhance security and trust in IoT environments. Similar principles could be applied to LLNs to ensure secure routing decisions.
2) Filament and Industrial IoT: Filament, an IoT blockchain company, works on industrial IoT deployments. Although not LLN - exclusive, these deployments demonstrate how blockchain can provide secure and trusted communication among IoT devices, which aligns with LLN communication needs.
3) IOTA's Tangle: IOTA's Tangle, while not a traditional blockchain, is de - signed for IoT and LLN environments. It employs a directed acyclic graph (DAG) structure for transactions. It aims to overcome the scalability and resource constraints of traditional blockchains, making it potentially suit - able for LLNs.
4) Smart Grid and Energy Management: In smart grid scenarios, where LLNs are prevalent, blockchain can be used for secure data exchange among en - ergy meters, optimizing energy consumption, and ensuring fair compensation for energy transactions.
5) Decentralized Applications (DApps): DApps built on blockchain can be extended to LLNs, such as in environmental monitoring scenarios. For example, a decentralized air quality monitoring network could benefit from blockchain's data integrity and tamper - proof attributes.
6) Smart Cities and Municipal Services: Blockchain can be integrated into LLNs in smart city projects, where devices collect and exchange data for urban services. The blockchain can ensure data accuracy, secure communication, and transparency.
7) Healthcare and Medical Devices: In healthcare, LLNs can involve medical devices and sensors. Blockchain can provide secure data sharing among authorized parties, ensuring privacy and authenticity of patient - related data [22].

While direct case studies and real - world deployments specific to blockchain - enabled routing protocols in LLNs are limited, these examples showcase the potential of blockchain technology in related IoT and LLN contexts. As the field of blockchain solutions for routing protocols in LLNs continues to evolve, more dedicated case studies and deployments are expected to emerge, highlighting the practicality, challenges, and benefits of implementing blockchain in these environments.

8.1. Practical implementations or case studies where blockchain - based routing protocols

There are few public case studies or practical implementations specifically focusing on blockchain - based routing protocols in Low Power and Lossy Networks (LLNs). However, here are a few examples of related implementations and case studies that demonstrate the potential for integrating blockchain technology in LLN environments:

1) IOTA's Tangle in IoT Environments: IOTA's Tangle, a directed acyclic graph (DAG) technology, has been explored for IoT scenarios. While not a traditional blockchain, IOTA's approach aims to address scalability and efficiency concerns. Its design is suitable for LLNs due to its lightweight consensus mechanism and ability to handle intermittent connectivity.
2) Smart Agriculture and Precision Farming: Blockchain solutions have been applied to track and verify the origin of agricultural products. In cases where LLNs are used for data collection in precision farming, blockchain can ensure data integrity and authenticity.
3) Smart Parking Systems: In urban environments, LLNs can be used for smart parking systems. Blockchain can enhance data accuracy, parking availability verification, and secure financial transactions within such sys - tems.
4) Decentralized Sensor Networks: While not specifically LLN - focused, some decentralized sensor network projects use blockchain for data aggregation and sharing. Similar principles can be extended to LLN scenarios where sensors collect and relay data.
5) Supply Chain Tracking for Remote Areas: In remote areas with LLN connectivity, blockchain can be used to track the movement of goods and ensure supply chain transparency, even in regions with limited communication infrastructure.
6) Energy Trading and Microgrids: Some projects focus on using blockchain for energy trading in microgrids, which can often involve LLNs. These implementations enable secure and transparent peer - to - peer energy trans - actions, showcasing the potential for similar concepts in LLN routing.

It's important to note that specific case studies and implementations focused solely on blockchain - based routing protocols in LLNs might not be widely avail - able due to the complex and evolving nature of this area. However, these related implementations offer insights into how blockchain technology can be adapted and integrated into LLN environments to address routing challenges, enhance security, and enable efficient data exchange.

9. Directions for future research and development in this field

Future research and development in the domain of Blockchain Solutions for Routing Protocols in Low Power and Lossy Networks (LLNs) should focus on addressing the existing challenges and exploring innovative solutions to make blockchain integration more effective and efficient. Here are some key directions for future research:

1) Adaptive Routing Strategies: Designing routing protocols that dynamically adapt to the intermittent connectivity and energy constraints of LLNs will enhance the efficiency and reliability of blockchain - based routing.
2) Energy - Efficient Consensus Mechanisms: Developing consensus mechanisms tailored for LLNs is crucial to reduce energy consumption. Research could explore hybrid consensus algorithms that strike a balance between security and energy efficiency.
3) Adaptive Routing Strategies: Designing routing protocols that dynamically adapt to the intermittent connectivity and energy constraints of LLNs will enhance the efficiency and reliability of blockchain - based routing.
4) Scalability Solutions: Investigate sharding techniques, partitioning the blockchain network into smaller segments, to enhance scalability and ac - commodate the growing number of devices in LLNs.
5) Lightweight Cryptographic Techniques: Develop and optimize crypto - graphic mechanisms that are lightweight yet secure, addressing the processing and energy limitations of LLN devices.
6) Privacy - Preserving Solutions: Research techniques that ensure data privacy while still benefiting from blockchain's transparency. Techniques like zero - knowledge proofs and privacy - preserving smart contracts can be explored.
7) Data Aggregation Techniques: Explore methods for aggregating data at different levels of granularity to reduce the amount of data stored on the blockchain, minimizing storage overhead.
8) Blockchain - Friendly Hardware: Research hardware design optimizations that cater to blockchain's requirements in LLNs, such as low - power cryptographic accelerators.
9) Standardization and Interoperability: Contribute to the development of standardized protocols and interfaces for blockchain integration in LLNs, promoting interoperability and ease of deployment.

By exploring these directions, researchers and practitioners can contribute to the advancement of blockchain solutions for routing protocols in Low Power and Lossy Networks, ultimately addressing the challenges and realizing the potential benefits of blockchain technology in LLNs.

10. Conclusion

The systematic review of Blockchain Solutions for Routing Protocols in Low Power and Lossy Networks (LLNs) yielded vital insights into the potential and challenges of integrating blockchain technology in these resource - constrained environments. LLNs, marked by energy limitations, intermittent connectivity, and potential link losses, face considerable hurdles in routing protocols. Blockchain emerges as a promising solution due to its decentralized nature and tamper - proof properties. The systematic review followed a comprehensive methodology involving a targeted search strategy, stringent inclusion/exclusion criteria, and meticulous data extraction process.

Blockchain - enabled routing protocols were examined through performance evaluation metrics such as energy efficiency, latency, reliability, and scalability. The key findings indicated that while blockchain offers enhanced security and trust, challenges like energy consumption demand innovative approaches. Proposals to optimize energy usage encompassed lightweight consensus mechanisms and off - chain data storage. Latency emerged as a notable concern, driven by the consensus and transaction validation processes inherent in blockchain, necessitating strategies to minimize delays.

Scalability was a prominent issue, with proposed solutions including shard - ing, hierarchical structures, and off - chain methods to accommodate the growing volume of transactions. Overhead and storage requirements of blockchain were acknowledged, with efforts focused on refining data structures and minimizing redundant information. Security and privacy concerns were addressed through techniques like cryptographic mechanisms and privacy - preserving strategies, ensuring a balance between transparency and data confidentiality.

Adoption and deployment aspects were explored, emphasizing the complexity of integration, interoperability, regulatory compliance, and long - term sustainability. While dedicated case studies specifically targeting blockchain - enabled routing protocols in LLNs were scarce, related IoT applications demonstrated the adaptability and potential impact of blockchain technology in LLNs. The review also highlighted numerous open research questions, including energy - efficient consensus mechanisms, adaptive routing strategies, and incentive models tailored to LLNs.

In conclusion, the systematic review shed light on the multifaceted nature of integrating blockchain solutions into routing protocols for LLNs. While blockchain's advantages hold promise, the study underlines the necessity of over - coming challenges through innovative research and implementation strategies, ultimately enhancing the efficacy and applicability of blockchain in LLN environments.

References

[1] Witwit, A. J. and Idrees, A. K., 2018, September. A comprehensive review for RPL routing protocol in low power and lossy networks. In International conference on new trends in information and communications technology applications (pp.50 - 66). Cham: Springer International Publishing.

[2] Dhumane, A., Bagul, A. and Kulkarni, P., 2015. A review on routing pro - tocol for low power and lossy networks in IoT. Int. J. Adv. Eng. Glob. Technol, 3 (12), pp.1440 - 1444.

[3] Ekpenyong, M. E., Asuquo, D. E., Udo, I. J., Robinson, S. A. and Ijebu, F. F., 2022. IPv6 Routing Protocol Enhancements over Low - power and Lossy Networks for IoT Applications: A Systematic Review. New Review of In - formation Networking, 27 (1), pp.30 - 68.

[4] Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A. and Richardson, M., 2015. A security threat analysis for the routing protocol for low - power and lossy networks (RPLs) (No. rfc7416).

[5] Li, W., Wu, F., & Xia, Q. (2017). A survey on the security of blockchain systems. Future Generation Computer Systems, 82, 395 - 411.

[6] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain in Internet of Things: Challenges and Solutions. In Proceedings of the 2017 IEEE Inter - national Conference on Pervasive Computing and Communications Work - shops (PerCom Workshops) (pp.618 - 623).

[7] Mahmood, A. N., & Ahmed, E. (2018). Blockchain technology: Hype or reality?. IEEE Cloud Computing, 5 (1), 70 - 75.

[8] Li, J., Yu, X., Lin, X., Wang, X., & Wang, H. (2019). A Survey on Consen - sus Mechanisms and Mining Strategy Management in Blockchain Networks. IEEE Access, 7, 22328 - 22370.

[9] Delgado - Segura, S., P´erez - Sol`a, C., & Herrera - Joancomart´ı, J. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Fu - ture Generation Computer Systems, 88, 173 - 190.

[10] Conti, M., & Kumar, E. (2019). Beyond Blockchain: A Survey on Secure Multi - Party Computation Protocols. IEEE Access, 7, 130681 - 130713.

[11] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292 - 2303.

[12] Zohrevand, A., Azimi, I., & Hafeez Anwar, M. (2019). A survey on the secu - rity of blockchain systems: Attacks and consensus algorithms. Computers & Security, 95, 101 - 127.

[13] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14 (4), 352 - 375.

[14] Samaniego, M., & Sharma, P. (2020). Integrating Blockchain and IoT: A Systematic Survey. IEEE Internet of Things Journal, 8 (1), 654 - 672.

[15] Dinh, T. T. A., Wang, J., Chen, G., Liu, R., & Ooi, B. C. (2018). BLOCK - BENCH: A Framework for Analyzing Private Blockchains. IEEE Transac - tions on Parallel and Distributed Systems, 30 (2), 352 - 365.

[16] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks, 57 (10), 2266 - 2279.

[17] Pradhan, P., & Gaur, M. S. (2020). A comprehensive survey of blockchain: Concepts, platforms, applications, opportunities and challenges. Journal of King Saud University - Computer and Information Sciences.

[18] Dorri, A., Steger, M., & Kanhere, S. S. (2020). Blockchain - based secure firmware updates for embedded devices in IoT. Journal of Network and Computer Applications, 149, 102464.

[19] Skala, K., & Davidovic, D. (2020). Towards Efficient Blockchain for IoT: Performance Issues and Tradeoffs. IEEE Access, 8, 124660 - 124673.

[20] Alam, M. S., & Reaz, M. B. I. (2019). Lightweight consensus protocols for low - power Internet of Things

(IoT) devices. IEEE Transactions on Indus - trial Informatics, 15 (5), 2899 - 2907.

[21] Rezazadeh, A., Keshavarz - Haddad, A., & Al - Fuqaha, A. (2018). Secure and efficient key management mechanisms for Internet of Things: A survey. IEEE Internet of Things Journal, 6 (2), 1900 - 1919.

[22] Wu, J., Xu, Y., Wang, X., & Zhang, X. (2019). A secure and privacy - preserving mobile health system based on blockchain. IEEE Access, 7, 89986 - 89997.

[23] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (pp.557 - 564).

[24] Patel, M., & Sharma, P. (2020). Blockchain for IoT security: A system - atic review. Journal of King Saud University - Computer and Information Sciences.

[25] Nakamoto, S. (2008). Bitcoin: A peer - to - peer electronic cash system.

[26] Yli - Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. PloS one, 11 (10), e0163477.

[27] Zohrevand, A., Azimi, I., & Hafeez Anwar, M. (2018). A survey on the secu - rity of blockchain systems: Attacks and consensus algorithms. Computers & Security, 95, 101 - 127.

[28] Islam, S. R., Islam, S. M. R., & Amin, R. (2020). A comprehensive study on the security and privacy of blockchain. Journal of Ambient Intelligence and Humanized Computing, 11 (4), 1607 - 1640.

[29] Conti, M., & Kumar, E. (2019). Beyond Blockchain: A Survey on Secure Multi - Party Computation Protocols. IEEE Access, 7, 130

[30] G. Foroglou and A. - L. Tsilidou, “Further applications of the blockchain, ” 2015.

[31] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy - preserving smart contracts, ” in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp.839–858.

[32] B. W. Akins, J. L. Chapman, and J. M. Gordon, “A whole new world: In - come tax considerations of the bitcoin economy, ” 2013. [Online]. Available: https: //ssrn. com/abstract=2394738

[33] Y. Zhang and J. Wen, “An iot electric business model based on the protocol of bitcoin, ” in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp.184–191.

[34] M. Sharples and J. Domingue, “The blockchain and kudos: A distributed system for educational record, reputation and reward, ” in Proceedings of 11th European Conference on Technology Enhanced Learning (EC - TEL 2015), Lyon, France, 2015, pp.490–496.

[35] C. Noyes, “Bitav: Fast anti - malware by distributed blockchain consensus and feedforward scanning, ” arXiv preprint arXiv: 1601.01405, 2016.

[36] I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnera - ble, ” in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp.436–454.

[37] A. Biryukov, D. Khovratovich, and I. Pustogarov, “Deanonymisation of clients in bitcoin p2p network, ” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp.15–29.

[38] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical sur - vey on decentralized digital currencies, ” IEEE Communications Surveys Tutorials, vol.18, no.3, pp.2084–2123, 2016.

[39] NRI, “Survey on blockchain technologies and re - lated services, ” Tech. Rep., 2015. [Online]. Available: http: //www.meti. go. jp/english/press/2016/pdf/0531 01f. pdf

[40] D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed. El - sevier, 2015. [Online]. Available: http: //EconPapers. repec. org/RePEc: eee: monogr: 9780128021170

[41] V. Buterin, “A next - generation smart contract and decentralized applica - tion platform, ” white paper, 2014.

[42] D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digital sig - nature algorithm (ecdsa), ” International Journal of Information Security, vol.1, no.1, pp.36–63, 2001.

[43] V. Buterin, “On public and private blockchains, ” 2015. [Online]. Available: https: //blog. ethereum. org/2015/08/07/ on - public - and - private - blockchains/

[44] “Hyperledger-project, ”-2015. - [Online]. -Available: https: //www.hyperledger. org/- “Consortium chain development. ” [Online]. Available: https: //github. com/ethereum/wiki/wiki/Consortium - Chain - Development

[46] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem, ” ACM Transactions on Programming Languages and Systems (TOPLAS), vol.4, no.3, pp.382–401, 1982.

[47] S. King and S. Nadal, “Ppcoin: Peer - to - peer crypto - currency with proof of - stake, ” Self - Published Paper, August, vol.19, 2012.

[48] “Bitshares - your share in the decentralized exchange. ” [Online]. Available: https: //bitshares. org/

[49] A. Chepurnoy, M. Larangeira, and A. Ojiganov, “A prunable blockchain consensus protocol based on non - interactive proofs of past states retriev - ability, ” arXiv preprint arXiv: 1603.07926, 2016.

[50] J. Bruce, “The mini - blockchain scheme, ” July 2014. [Online]. Available: http: //cryptonite. info/files/mbc - scheme - rev3. pdf

[51] J. van den Hooff, M. F. Kaashoek, and N. Zeldovich, “Versum: Veri - fiable computations over large public logs, ” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp.1304–1316.

[52] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, “Bitcoinng: A scalable blockchain protocol, ” in Proceedings of 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), Santa Clara, CA, USA, 2016, pp.45–59

[53] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, “A fistful of

bitcoins: Characterizing payments among men with no names, ” in Proceedings of the 2013 Conference on Internet Measurement Conference (IMC’13), New York, NY, USA, 2013.

[54] J. Barcelo, “User privacy in the public bitcoin blockchain, ” 2014.

[55] M. Moser, “Anonymity of bitcoin transactions: An analysis of mixing ¨ services, ” in Proceedings of Munster Bitcoin Conference ¨, Munster, ¨ Germany, 2013, pp.17–18.

[56] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, “Mixcoin: Anonymity for bitcoin with accountable mixes, ” in Pro - ceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp.486–504.

[57] G. Maxwell, “Coinjoin: Bitcoin privacy for the real world, ” in Post on Bitcoin Forum, 2013.

[58] T. Ruffing, P. Moreno - Sanchez, and A. Kate, “Coinshuffle: Practical decen - tralized coin mixing for bitcoin, ” in Proceedings of European Symposium on Research in Computer Security, Cham, 2014, pp.345–364.

[59] S. Solat and M. Potop - Butucaru, “ZeroBlock: Timestamp - Free Prevention of Block - Withholding Attack in Bitcoin,” Sorbonne Universites, UPMC University of Paris 6, Technical Report, May 2016. [Online]. Available: https: //hal. archives - ouvertes. fr/hal - 01310088

[60] G. W. Peters, E. Panayi, and A. Chapelle, “Trends in crypto - currencies and blockchain technologies: A monetary theory and regulation perspective, ” 2015. [Online]. Available: http: //dx. doi. org/10.2139/ssrn.2646618