JCTA Journal of Computing Theories and Applications ISSN:3024-9104

Review Article

A Comprehensive Study on Applications of Blockchain in Wireless Sensor Networks for Security Purposes

Mui D. Nguyen [1], Minh T. Nguyen [1,2,*], Thang C. Vu [3], Tien M. Ta [1], Quang A. Tran [2], and Dung T. Nguyen [3]

[1] Department of Electrical Engineering, Thai Nguyen University of Technology, Viet Nam; e-mail: ducmui@tnut.edu.vn, nguyentuanminh@tnut.edu.vn, zippotnut@tnut.edu.vn,
[2] Thai Nguyen University; e-mail: nguyentuanminh@tnu.edu.vn, quangta@tnu.edu.vn
[3] Department of Electronics Engineering, Thai Nguyen University of Information and Communication Technology, Viet Nam; e-mail : vcthang@ictu.edu.vn, ntdungcndt@ictu.edu.vn
* Corresponding Author: Minh T. Nguyen

Abstract: The paper evaluates potential applications of blockchain technology in enhancing the security and reliability of Wireless Sensor Networks (WSNs). The existing vulnerabilities in WSNs, such as concerns regarding data integrity and security, demand innovative security solutions. Through systematic analysis, this paper provides valuable insights to expand understanding of WSNs security, explaining the feasibility and benefits of deploying blockchain technology. Possible attacks in the networks are classified to point out either risks or potential solusions to protect the networks. By exploring the integration of Blockchain within WSNs, the paper highlights its potential to minimize various security risks. In addition, this work discusses the challenges and considerations associated with implementing Blockchain in WSNs. Overall, this paper contributes on securing WSNs and underscores the role of blockchain technology as a promising way for enhancing security of WSNs.

Keywords: Attacks; Blockchain security; Consensus; Node authentication; Wireless sensor networks.

1. Introduction

Wireless sensor networks (WSNs) facilitate many applications in different fields [1], [2]. The networks collect and process data and provide sensing values, including warnings for a lot of systems with high performance. WSNs are often deployed in areas that may not be accessible easily. This causes problems with maintaining and protecting the networks. In addition, the networks contain a huge number of small and low-cost devices that show a low capacity of security either at sensor nodes or the whole system. The operating system and the software may not be updated frequently with advanced technologies to protect the networks as well. This section aims to show the motivation for applying Blockchain to such networks and review the literature to clarify the applications of Blockchain in WSNs. Possible attacks and potentials of using Blockchain in WSNs are also provided.

1.1. Motivation

The roots of WSNs can be traced back to the late 20th century when advancements in Micro-Electro-Mechanical Systems (MEMS) and wireless communication laid the foundation for creating networks of small, autonomous sensors [2], [3]. Early applications focused on military surveillance and environmental monitoring, utilizing the ability of sensor nodes to collect data and communicate wirelessly over vast areas. Over time, WSNs found applications in various fields, including monitoring the environment, energy and resource management, smart monitoring and control within homes, healthcare monitoring, traffic and transportation monitoring, fire management and safety, water supply and water quality measurement, applications in smart agriculture, etc. To gain a better understanding of WSNs, let's analyze the structure of this network. In studies[4]–[6], the authors presented in detail the architecture of a WSN, including key components such as sensor nodes, sink nodes, the internet, data servers, and the analytics block, according to Figure 1. The process begins with the sensor nodes, which continuously monitor their surroundings and collect data using the built-in sensors like

Received: April, 13th 2024
Revised: July, 6th 2024
Accepted: July, 7th 2024
Published: July, 13th 2024

temperature, humidity, pressure, etc. Once the data is collected, the sensor nodes transmit it to other nodes or directly to the sink node in the network. Sink nodes are specialized nodes in the WSN that aggregate and process data before sending it to the internet or a local server for further analysis. The data transmitted by the sensor nodes to the sink node is then sent to the internet, making it accessible for various applications, such as real-time monitoring, data analytics, and visualization. The data can also be stored in a big data server or data center for historical analysis and long-term storage. Finally, data analytics tools and software are used to extract valuable insights and actionable information from the collected data. These insights can then be used to optimize processes, improve decision-making, and enhance overall system performance.

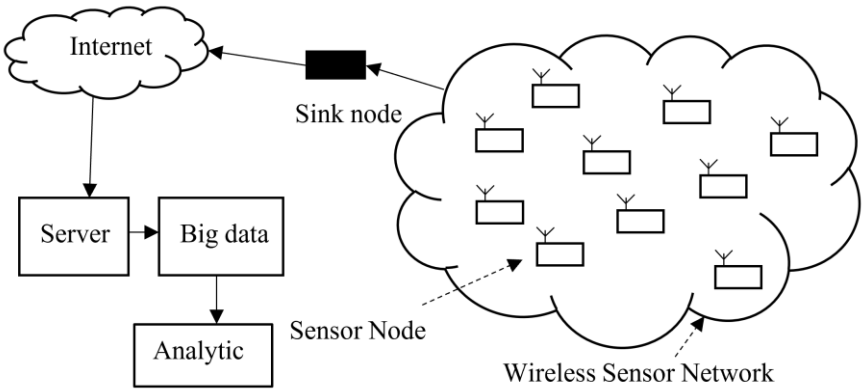

Figure 1. Traditional WSN architecture.

Despite the advancements in WSN technology, security challenges persist. Current literature often focuses on traditional security mechanisms that may not fully address the unique challenges posed by WSNs. Hence, this work aims to fill this gap by exploring the potential of blockchain technology to enhance the security and reliability of WSNs

1.2. Attacks in WSNs.

WSNs are vulnerable to various types of attacks due to their inherent characteristics, such as limited resources, distributed nature, and often hostile deployment environments. Attacks on WSNs can be classified into various categories based on different criteria. Categorizing attackers based on goals, performers, and layers. Goal-based attacks classify between passive and active attacks [7]–[9]. Performer-based attacks can be outside or inside [10]–[12]. Layer-based attacks target different network layers, including physical layers[11]–[13], data link layers[14]–[17], network layers[10], [14], transport layers[11], [18], and application layers [17], [19].

In order to classify the whole security problem, Figure 2 illustrates various possible attacks that may affect WSNs. Since the networks have many resource limitations, the attacks may happen in many ways, simultaneously in different parts.

Understanding these vulnerabilities is crucial for devising effective security measures, ensuring the network's security requirements in Section 1.3, and knowing how Blockchain can overcome these risks.

- Goal-Based Attacks: Attacks can be categorized as passive or active. Passive attacks involve eavesdropping, traffic monitoring, and traffic analysis on communication channels to intercept sensitive data without altering it. On the other hand, active attacks involve malicious manipulation of data or network operations to disrupt normal functioning or gain unauthorized access.
- Performer-Based Attacks: Attacks can originate from both outside and inside sources. Outside attackers may exploit vulnerabilities in the network from outside, while inside attackers may compromise nodes within the network to launch attacks or leak sensitive information.

- Layer-Based Attacks: Attackers may target different layers of the network protocol stack, including the physical, data link, network, transport, and application layers. Each layer presents unique vulnerabilities that attackers can exploit to compromise the network's security and integrity.

Routing-Based Attacks: Attackers specifically target the routing protocols to disrupt the network's communication and data transfer.

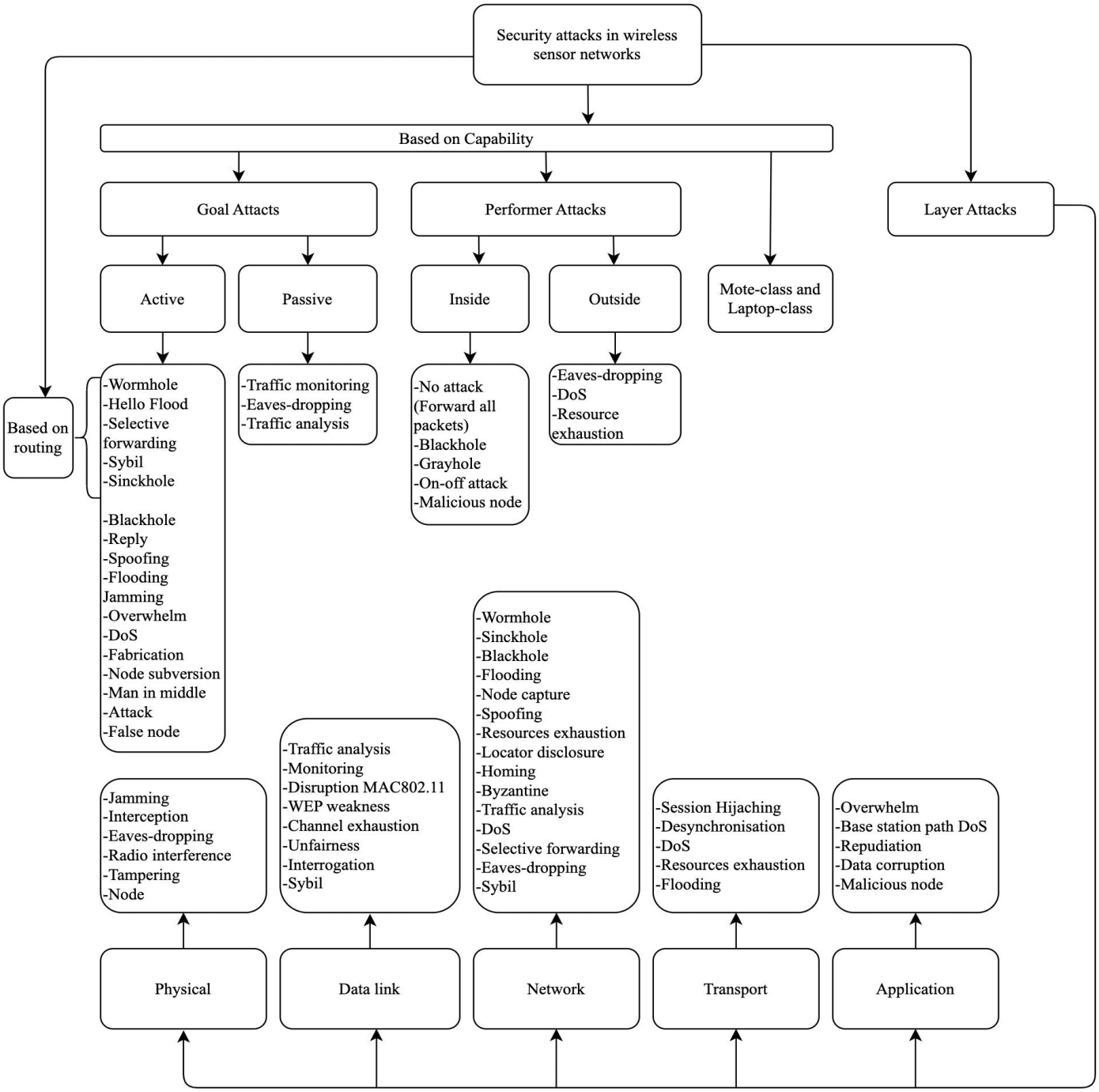

Figure 2. Possible Attacks in WSNs.

These attacks pose significant challenges to the security and reliability of WSNs, requiring robust cryptographic mechanisms, intrusion detection systems, and secure routing protocols to mitigate their impact and ensure the integrity and confidentiality of the data collected by the sensor nodes.

1.3. Security requirements

In [7], [9], [20]–[24], a sensor network must meet particular needs to ensure safe communication. Basic security needs for WSNs include availability, confidentiality, integrity, data freshness, and authentication. Additionally, self-organization, time synchronization, and secure localization are important aspects:

- Data Authentication: WSNs are susceptible to various security threats due to their distributed and resource-constrained nature. Data authentication is crucial in WSNs to ensure the integrity and authenticity of the information collected from sensor nodes.
- Data Confidentiality: Ensuring data confidentiality in WSNs is crucial to protect sensitive information from unauthorized access or eavesdropping. WSNs often operate in open and potentially hostile environments, making data encryption and confidentiality measures essential.
- Data Integrity: Ensuring data integrity in WSNs is essential to guarantee that the data collected and transmitted by sensor nodes has not been altered or tampered with during its journey through the network.
- Availability: Ensuring availability in WSNs is critical to maintaining the functionality and reliability of the network. Availability refers to the ability of the system to provide services and operate effectively, even in the face of various challenges, such as node failures, communication disruptions, or malicious attacks.
- Data Freshness: Data freshness in WSNs refers to the timeliness or recency of the data collected by sensor nodes. In many applications, having up-to-date information is crucial for making informed decisions.
- Self-Organization: Self-organization in WSNs refers to the capability of the network to autonomously and dynamically organize itself without external control or central coordination. The goal is to adapt to changing conditions, optimize network performance, and efficiently achieve common objectives.
- Time Synchronization: Time synchronization is essential in WSNs to ensure that sensor nodes consistently and accurately perceive time. Accurate time synchronization is crucial for coordinating data fusion, event ordering, and scheduling tasks in a distributed and collaborative environment.
- Secure Localization: Secure localization in WSNs involves ensuring the accuracy and trustworthiness of the location information obtained by sensor nodes. Localization is critical for many WSN applications, such as tracking, monitoring, and environmental sensing. However, it is susceptible to various security threats, including attacks on the localization algorithms or the compromise of location information.

1.4. Potentials of using Blockchain in WSNs

Blockchain technology can be used in WSNs to enhance data integrity and security. In [25]–[27], The concept of Blockchain emerged in 2008 with the publication of a whitepaper by an individual or group operating under the pseudonym Satoshi Nakamoto. It introduced the idea of a decentralized, distributed ledger that records transactions across a network of computers. The first practical implementation of Blockchain came with Bitcoin in 2009, serving as a decentralized digital currency. Blockchain technology gained traction due to its ability to ensure transparency, immutability, and security in recording transactions without the need for intermediaries like banks or governments. Beyond cryptocurrencies, Blockchain has found applications in various sectors, including supply chain management, healthcare, finance, and now, in securing WSNs. The Blockchain system acts as the base layer for data integrity, ensuring accurate and secure data transmission from the sensors to the analytics node. In Figure 3, The blockchain system consists of several interconnected nodes. Each node maintains a copy of the entire Blockchain. These nodes validate new transactions and add them to the Blockchain once verified. These systems provide secure, transparent, and efficient means of recording and managing data. In the context of the Internet of Things (IoT) and WSNs, blockchain technology can provide powerful tools for collecting, storing, and analyzing sensor data.

In [28], [29], the paper explores three categories of blockchain networks: public, private, and consortium. A fully decentralized structure characterizes the public Blockchain, enabling unrestricted participation from any node. In contrast, the private Blockchain operates on a

permission-based model, selectively allowing nodes to participate. The consortium blockchain represents a semi-decentralized network collectively managed by multiple organizations. In [30], [31], the paper delves into the role of miners in the Blockchain, highlighting their responsibility for transaction verification through consensus. The discussion encompasses various consensus algorithms, such as Proof of Authority (PoA), Proof of Work (PoW), and Proof of Stake (PoS). PoW involves nodes solving a mathematical puzzle to identify miner nodes, with the first solver adding a new block, incurring high computational costs. In contrast, PoA relies on preselected validators for block and transaction validation, reducing the need for extensive computational capabilities in miner selection. PoS entails miners with the highest coin holdings validating and mining blocks. In [32]–[35], the key concepts include:

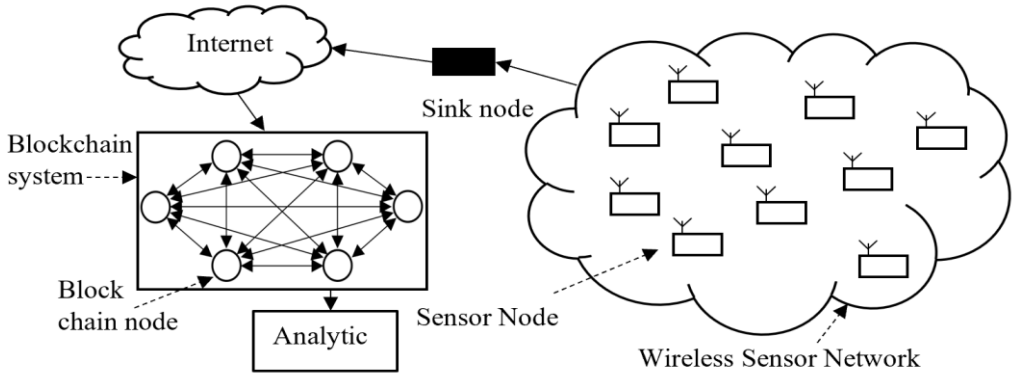

Figure 3. Blockchain-based WSN architecture[33].

- Transaction: A representation of a user's operation, denoted as a tuple (from, to, value, sig). Here, from the sender's public key to is the destination public key, value denotes the transaction content, and sig stands for the digital signature. For example, data sent from Node A to Node B can be treated as a transaction.
- Block: Essentially a compilation of transactions (T) enriched with additional data, including a timestamp and the previous block's hash. All transactions find their record within blocks, serving as concise containers for transactional data.
- Blockchain: Depicted as a tuple (G, B), where G symbolizes the original state, and B = [b1, b2, b3, ...] forms an ordered list of blocks. Establishing and sustaining a blockchain necessitates collaborative contributions from all participating nodes.
- Merkle Tree: Known as a hash tree, it deploys a hash function for mapping variable-length data into fixed-length data. Each block holds a hash value stored in the leaves of the Merkle tree.
- Consensus Protocol: This entails collaborative computation to secure agreement across all blockchain members. The consensus method determines the inclusion of a block in the chain.

Comparison of WSN systems without blockchain technology to WSN systems that include Blockchain. Traditional WSNs with a centralized control mechanism can be vulnerable to tampering and attacks. These systems often lack traceability and transparency, which are crucial for ensuring trust and accountability in WSN operations. On the other hand, WSNs incorporating Blockchain technology offer enhanced security through decentralization and immutability. This decentralized approach eliminates the risk of a single point of failure and enables dynamic trust establishment and consensus mechanisms. Additionally, Blockchain-based WSNs provide improved traceability through blockchain ledgers and offer self-executing security policies.

This paper is a systematic analysis of existing literature. The review process is precise and transparent, with clearly defined inclusion criteria to capture relevant studies effectively, so one potential limitation lies in the coverage of existing literature. The urgency of this review is driven by the increasing importance of securing WSNs and the potential of blockchain technology to address security concerns. The rest of this paper is organized as follows. Section 2 explores secure Blockchain applications in WSNs, detailing encryption methods, security in

the routing, security models, detecting compromised nodes, and consensus algorithms to enhance WSN security. Section 3 evaluates the problems. Section 4 discusses WSN security challenges and suggestions for future research directions. Finally, conclusions and future work are provided in Section 5.

Table 1. A security comparison between without Blockchain and without Blockchain in WSNs.

Security Aspect	WSN With Blockchain	WSN Without Blockchain
Traceability and transparency	Providing high traceability through a distributed ledger, preventing transaction tampering	Lack of traceability and transparency, high risks for fraud and data loss
Centralization and trust	Decentralized, reducing attack risks from a single point, uniform in transaction validation	Vulnerability to single-point attacks reduced reliability in case of incidents.
Key management and authentication	Utilizing blockchain-based encryption, secure key management, robust authentication mechanism	Traditional key management is susceptible to attacks.

2. Secure blockchain applications for WSNs

2.1. Blockchain-based encryption methods

Encryption methods for WSNs are designed to secure communication and data transmission within these networks. WSNs often consist of numerous sensor nodes that collect and exchange data, making it essential to protect the information from unauthorized access or tampering. In [36], two encryption methods are introduced for securely transmitting secret information, with only the intended node able to decrypt it. In addition, the paper [37] proposes a secure key management mechanism utilizing Blockchain for operations like registration and cluster formation among nodes. The Base Station (BS) is a central entity that assigns unique identities to nodes and generates public-private key pairs.

Additionally, [38] addresses information security issues in WSNs and ensures the confidentiality of transmitted data. The BCE-WSN algorithm, a block-based encryption solution, is proposed. The BCE-WSN algorithm aims to provide robust encryption mechanisms explicitly tailored for the resource-constrained nature of WSNs while maintaining high levels of security. Now let's examine an encryption method based on the BCE-WSN algorithm to gain a better understanding.

Algorithm 1. BCE-WSN Encryption [38]

INPUT: N: set of node; 1^k: a spatial variable; KeyGen(1^k): generate a pair key; Sign(sk,m): signature for node n; Ver(vk,m,σ): verification for the signature
OUTPUT: hash value for transactions for node A to Node B

Generate a spatial variable m $\leftarrow$ setup(1^k)
For $tx_i \in Tansaction[i]$ do
$(sk_i, pk_i) \leftarrow KeyGen(m, tx_i)$
    $\sigma \leftarrow Sign(sk, m\_i)$
    If Ver(vk,m,σ) = 1
        Return true
    else
        Return false
    End if
End for
Return σ

The algorithm comprises four components. In Figure 4, Key Pair Generation: An anonymous method generates a key pair for each sensor node in WSNs, with the node's ID serving as the public key. Transmitted information is encrypted using the public key. Encryption: Utilizes an asymmetric encryption algorithm, taking plaintext and the node's private key as input to generate ciphertext. The ciphertext, though not guarded, is transmitted across all

WSN nodes. Signature: The sender node encrypts transaction data using its ID as the public key, generating encrypted ciphertext for transmission. This signature method prevents forgery and ensures data integrity. Verification: As all nodes' public keys in the WSNs are public, any node can verify information authenticity through the network's public keys. Determines whether the source node sends the information. If verification is successful, the information is transmitted to the target node and recorded in the blockchain system. In the event of verification failure, the information is rejected. By following this methodology, WSNs can employ Blockchain to secure data transmission, manage encryption keys, and ensure the integrity and authenticity of collected data.

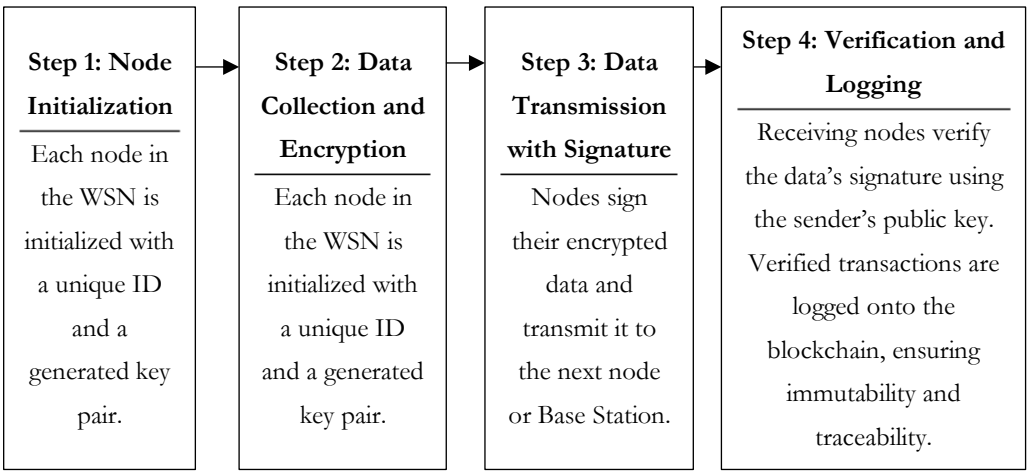

Figure 4. Four Steps of BCE-WSN Encryption

2.2. Security in the routing

It aims to enhance the reliability and accuracy of information by identifying and discarding false or irrelevant data before it reaches its final destination. En-route filtering schemes play a crucial role in optimizing network efficiency, conserving resources, and ensuring the integrity of transmitted data in the context of Wireless Sensor Networks. A study [39] introduces a novel blockchain-based deterministic en-route filtering scheme for WSNs. The proposed scheme efficiently drops false reports without needing key exchange between sensor nodes, thereby reducing key storage overhead and communication overhead. Various filtering schemes have been proposed to address false reports in networks.

In probabilistic schemes like SEF and PCREF described in [40] and [41], respectively, sensor nodes share keys with several intermediate nodes at a consistent probability. This enables false reports to traverse diverse hops before being discarded. Nevertheless, this method results in a significant overhead in key storage. Alternatively, within deterministic frameworks like IHA and CDEF, as discussed in [42] and [43], sensor nodes exclusively exchange keys with intermediate nodes responsible for establishing the route to the sink. However, these approaches entail transmitting reports along a predetermined path, and the feasibility of implementing such schemes in contemporary WSNs remains debatable. Hybrid schemes of LBRS in [42] and LEDS in [43] integrate both probabilistic and deterministic approaches, establishing key exchanges with select sensor nodes within a designated network segment.

Table 2. The effectiveness of En-route filtering schemes [39].

Method	Filtering Effectiveness	Key Storage Load	Communicati on Load	Dynamic Networks
[39]	Very good	Very low	Moderate	Yes
[40]	Poor	High	High	Yes
[41]	good	High	Very High	No
[44]	good	Low	Moderate	No
[45]	good	Moderate	Moderate	Yes
[42]	Moderate	Moderate	High	No
[43]	Moderate	Moderate	High	No

En-route filtering schemes in Table 2 reveal significant differences in performance and suitability for Wireless Sensor Networks (WSNs). In [39], The method emerges as the most efficient and adaptable option, demonstrating excellent filtering effectiveness, minimal key storage load, moderate communication load, and compatibility with dynamic networks. This method offers a balanced and practical solution for secure data transmission in WSNs. On the other hand, the SEF method in [40] is notably less effective, with poor filtering capability and high resource demands, making it less suitable despite its compatibility with dynamic networks. In [41], the PCREF method shows good effectiveness but imposes heavy burdens on key storage and communication, and its lack of support for dynamic networks further limits its applicability. The IHA method in [39] and the CDEF method in [40] achieve good filtering effectiveness with lower resource requirements, but only CDEF supports dynamic networks, making it a more versatile choice. LBRS method in [42] and the LEDS method in [43] offer moderate filtering effectiveness and key storage load but are hindered by high communication loads and unsuitability for dynamic environments. Overall, the analysis underscores the importance of selecting an en-route filtering scheme that balances effectiveness, resource efficiency, and adaptability to dynamic network conditions. The method in [39] is highlighted as the most promising approach for optimizing security and performance in WSNs.

These hybrid schemes demonstrate balanced filtering efficiency on average, accompanied by a reasonable overhead in key storage. Research [46] presents a novel approach incorporating Blockchain into the routing phase, deploying stored transactions to optimize routing decisions. Blockchain acts as a decentralized ledger where transactions and network states are recorded in a secure and immutable manner. Each block in the Blockchain contains transactions, which can include information about the status of nodes within the WSN. Each node in the WSN updates its status (active or inactive) on the Blockchain. When a node becomes inactive (due to low battery, damage, or any other reason), it sends a status update recorded in the Blockchain. These updates ensure that the network map remains current and reflective of the actual state of the network. When a node needs to send data, it queries the Blockchain to identify active nodes through the network map. This helps in selecting the optimal path for data transmission, avoiding inactive nodes that could cause delays or data loss

Additionally, the Signal-to-Interference-plus-Noise Ratio (SINR) concept is introduced in the subsequent discussion to determine the quality of a wireless communication link. Equation (1) is applied alongside the load traffic to ascertain the routing cost to the next hop.

$$SINR_{(i,j)} = \left(\frac{P_i}{d_{i,j}^{a}}\right) / \left(N_0 + \sum_{\substack{k=1 \\ k \neq i}}^{n} \frac{P_k}{d_{k,j}^{a}}\right), \quad (1)$$

where, P_i represents the transmission power of the i^{th} node, $d_{i,j}$ denotes the distance between two nodes i and j, a signifies the path loss exponent, N_0 stands for the power of additive white Gaussian noise.

The cost function is defined as follows.

$$Cost_j = SINR_{(i,j)}/(1 + \theta_j), \quad (2)$$

where, j represents the index of the subsequent hop, $SINR_{(i,j)}/(1 + \theta_j)$ refers to the Signal-to-Interference-plus-Noise Ratio (SINR), θ_j represents the traffic load of the j^{th} node.

The central aim is to achieve a balance in traffic distribution and minimize interferences in the routing phase. To accomplish this goal, emphasis is placed on formulating a cost function designed to optimize the selected path.

Upon detecting an event, the source node (k) assembles a list of inactive nodes and computes the routing cost for each utilizing Equation (2). Subsequently, Dijkstra's algorithm is utilized to ascertain the most efficient path. Following this, a chain verification is conducted for each node along the chosen path. If the verification proves successful for all nodes, source node k asserts ownership, and the transaction is logged onto the Blockchain. In the event of verification failure, untrusted nodes are discarded, prompting the definition of a new optimal path. If a valid path to the sink cannot be established, the source node awaits active nodes, communicating with the sink through the first channel to join the waiting queue.

In [47], the process of blockchain contractual routing entails source nodes employing smart contracts to solicit routes from gateways or destination nodes within a predefined

timeframe. In [48], the authors suggest a routing scheme that integrates blockchain and reinforcement learning, aiming to improve the efficiency and security of WSNs. In [46], after selecting the optimal path for each node, the source node performs chain verification, discarding all untrusted nodes that have not been verified. This filtration approach ensures that each chosen node in a path connecting source nodes to the sink maintains a pristine connection history by excluding nodes associated with malicious peers. In [49], the authors propose a secure routing approach that utilizes blockchain-based encryption and trust evaluation. This proposed mechanism facilitates real-time and energy-efficient data delivery from Sensor Nodes (SNs) to Base Stations (BSs).

2.3. Security models

In [50], the authors presented a trust model for wireless sensor networks incorporating blockchain technology. This model utilizes an innovative approach to identify malicious nodes in WSNs, incorporating Blockchain, Smart Contracts (SC), and the QM method to pinpoint the precise location of detected malicious nodes in 3D space. The network is structured into clusters, where Cluster Heads (CHs) oversee network management and blockchain maintenance. Detection of malicious nodes is achieved through a voting process in a blockchain-based distributed network. In [51], the authors utilize Blockchain to improve security within WSNs, with a particular emphasis on gateway nodes. The proposed model suggests deploying a blockchain at the mid-level of WSNs, utilizing gateway sensors as active nodes that store complete copies of the Blockchain. The Ethereum blockchain model is implemented through the truffle framework, and the solidity language is employed to develop a Smart Contract (SC) designed to provide distinct functions for individual nodes, thereby ensuring node authentication.

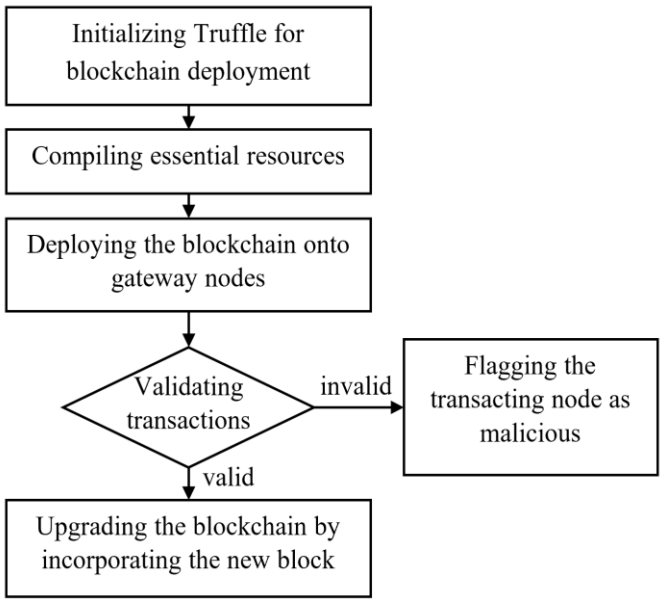

Figure 5. Workflow of the model using truffle [46].

This workflow describes the process of using Truffle in Figure 5, a popular Ethereum development framework, to deploy and manage a blockchain-based wireless sensor network. Here's a breakdown of the steps:

- Initializing Truffle for blockchain deployment: This step involves setting up and configuring a new Truffle project for blockchain deployment. This includes selecting a consensus algorithm, setting up the network configuration, and defining the smart contracts that will be deployed on the Blockchain.
- Compiling essential resources: Once the Truffle project is set up, the next step is compiling the smart contracts and other resources deployed on the Blockchain. This may include data structures, functions, and other components that are necessary for the operation of the wireless sensor network.

- Deploying the Blockchain onto gateway nodes: After the resources have been compiled, they are deployed onto the gateway nodes that will form the backbone of the wireless sensor network. These nodes manage the Blockchain and facilitate communication between the sensors and the rest of the network.
- Validating transactions: Once the Blockchain is up and running, transactions are submitted to the network for validation. These transactions may include sensor readings, configuration changes, or other data that needs to be recorded on the Blockchain. The gateway nodes are responsible for validating these transactions to ensure they are valid and conform to the network rules.
- Invalid/valid: As transactions are validated, they are marked as either invalid or valid. The network rejects invalid transactions, while valid transactions are incorporated into the Blockchain.
- Upgrading the Blockchain by incorporating the new block: The network is upgraded to incorporate the new data as new blocks are added to the Blockchain. This may include updating smart contracts, modifying network parameters, or implementing new features.
- Flagging the transacting node as malicious: If a node is found to be submitting invalid transactions or otherwise behaving maliciously, it may be flagged and removed from the network. This helps to ensure the integrity and security of the wireless sensor network.

2.4. Detecting compromised nodes

Compromised nodes can be used to launch attacks, steal data, or disrupt network operations, so detecting compromised nodes in WSNs is a crucial task to ensure the integrity and security of the network. In [52], the authors propose a method to transform sink nodes into a blockchain system, utilizing three systems for identifying malicious nodes, including a based heuristic intrusion detection system (RNN-IDS), a signature-based system, and a voting-based system, as illustrated in Figure 6.

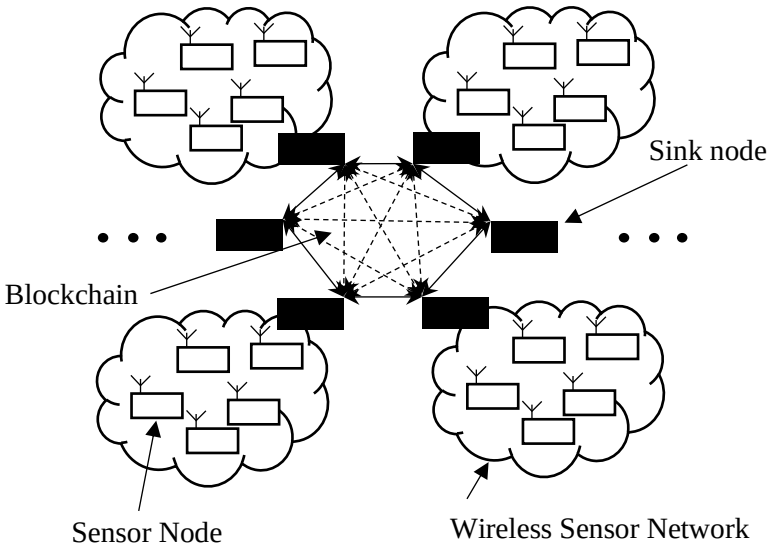

Figure 6. Transforming sink nodes into a blockchain system

The sink node performs the workflow of malicious sensor node detection below using a Heuristic detection system and signature-based system to detect malicious sensor nodes.

In Figure 7, the sink node receives a message from the sensor node (SN). This message is then processed to calculate its hash value. The sink node verifies if the hash value is already present and valid on the Blockchain. This step ensures the integrity and authenticity of the message. The sink node checks for potential malicious activity by applying heuristics to identify potential malicious activity. If the node doesn't exhibit suspicious behavior, it proceeds to the next step. Sink note uses a signature method to verify the message's authenticity and the sensor node further. If the sensor node is malicious based on the analysis and verification, the sink node updates the record on the Blockchain to reflect its status. This involves a voting

mechanism among network nodes to confirm the malicious node's status. If the malicious node is confirmed, the sink node drops the connection and prevents further communication.

In [53], identifying and eliminating malicious nodes within a WSN have become crucial, and blockchain technology has been applied to address this task effectively. By utilizing smart contracts, where all system agreements are encoded, Blockchain becomes a feasible solution to tackle these challenges. In research [53], a blockchain-based model has been applied to identify malicious nodes. However, integrating the Proof of Work (PoW) consensus mechanism into the model incurs significant computational costs.

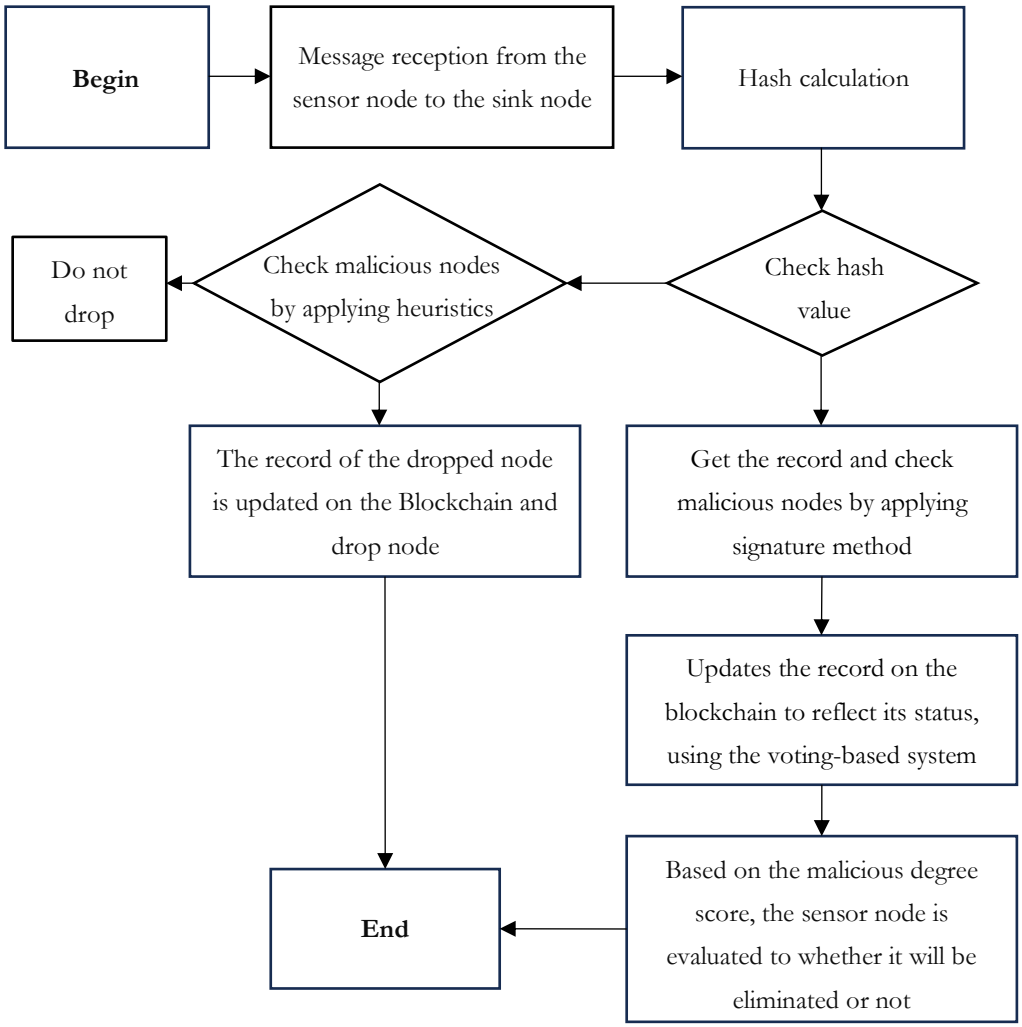

Figure 7. Workflow of malicious sensor node detection

In [47], a new method is introduced, utilizing a lightweight blockchain to equip a WSN coordinator to identify compromised nodes and ensure robust protection for sensitive data and node activities in critical situations. This method is optimized for WSNs with numerous nodes and a flowing node.

Specifically, the sink node monitors applications, collects and stores data from other nodes, and then transmits it to auxiliary networks. The system employs a blockchain system, supervised by a ledger within the sink node, managing tasks such as message verification and data storage. These blockchains are organized based on the diminishing trustworthiness of stored data.

This method establishes trust levels for WSN device nodes, impacting the choice of Blockchain for storing node data in the ledger. Nodes below the trust threshold will face being rejected from participating in their consensus system by the flowing node until intervention or verification from the operator occurs. Adjustments to trust scores are made based on the results of message checks from the ledger, and this threshold can be fine-tuned to suit application requirements and changing security needs.

2.5. Consensus algorithms

Consensus algorithms are important in ensuring agreement in distributed or decentralized networks. In [49], these algorithms ensure key aspects such as decentralized management, majority structure, authentication, integrity, non-repudiation, Byzantine fault tolerance, and performance optimization. While the public Blockchain of Bitcoin relies on the "proof of work" principle, there are various consensus protocols such as Proof of Existence (PoE), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Elapsed Time (PoET), Proof of Activity (combining proof of work and proof of stake), Proof of Importance, and Proof of Storage, providing alternative methods.

In [54], a rapid deployment of a consensus-based blockchain system model has been proposed. This model supports fast verification of information sources and instant verification of its accuracy for nodes in WSNs. The flexible integration of these consensus algorithms provides the ability to optimize the performance of the blockchain system in processing data from sensor nodes while ensuring integrity and reliability in distributed and fault-tolerant environments.

In [38], The authors select a consensus algorithm, namely Hierarchical BFT (Byzantine Fault Tolerance), based on a private blockchain for implementation in WSNs. This choice is made due to its suitability for WSN environments, offering good scalability and the potential to enhance the output performance of the blockchain system. Hierarchical BFT ensures robustness against Byzantine failures, making it particularly suitable for use in scenarios where node reliability is crucial. By employing this consensus algorithm, the Author aims to optimize the overall efficiency and reliability of data processing within the WSN, thereby enhancing its functionality and effectiveness in real-world applications.

Algorithm 2. The hierarchical BFT consensus algorithm [38].

```
INPUT: original network topology, the number of layers, the number in a cluster
OUTPUT: consistency results of all nodes
initialize the network topology of the current round
for i =1 to k do
    while(true)
        if Node[i] is valid
            if i<k
                find k neighbors in the network
                do BFT algorithm
                find the leader node
                return the leader node id and local result
            end if
        end if
        form the second layer network topology
    repeat do local BFT algorithm
    until to the top level
end for
return consistency results
```

The Hierarchical BFT Consensus Algorithm is designed to achieve consensus in a distributed network of nodes, even in the presence of Byzantine faults. Here is a description of how the algorithm works.

1. The algorithm takes the original network topology, the number of layers in the hierarchy, and the number of nodes in each cluster as input. The output of the algorithm is the consistency of results for all nodes.
2. Initialize the network topology for the current round.
3. For each round, do the following: a. While true, repeat the following steps: i. If the current node is valid, find k neighbors in the network and perform the Byzantine Fault Tolerance (BFT) algorithm to ensure the node is not faulty. ii. If the number of nodes in the cluster (k) is less than the current node, find the leader node among the nodes in the cluster. iii. Return the leader node ID and local result. b. Form the second layer network topology and repeat the local BFT algorithm until reaching the top level.
4. Return the consistency results.

The algorithm uses a hierarchical approach to achieve consensus. Each node is part of a cluster, and the clusters are organized into layers. The nodes in each cluster perform the BFT algorithm to ensure they are not faulty. Then, they elect a leader node and return its ID and local result. The leader nodes from each cluster form the second layer, and the process is repeated until reaching the top level. The algorithm ensures that all nodes in the network agree on the same result, even in the presence of Byzantine faults.

3. Evaluations

Evaluating various aspects concerning secure blockchain applications for WSNs reveals several strengths and areas for improvement. Firstly, the section on blockchain-based encryption methods provides a comprehensive overview of techniques, including the BCE-WSN algorithm.

Secondly, the discussion on security in routing introduces deterministic en-route filtering schemes and compares filtering approaches but could benefit from deeper scalability analysis and exploration of security threats.

Thirdly, the presentation of security models integrating blockchain technology offers detailed methodologies.

Fourthly, the section on detecting compromised nodes introduces a lightweight blockchain-based method.

Finally, the exploration of consensus algorithms highlights their role in ensuring reliability. Overall, while the sections provide valuable insights, further research is needed to address practical implementation concerns and enhance the credibility of discussed methods through empirical validation.

4. Challenges and Opening Issues

The deployment of Blockchain enhances traceability and transparency, but it also leads to increased data volume and processing requirements for nodes in the network. This can affect performance and energy consumption, especially in resource-constrained environments like WSNs. While Blockchain provides secure key management and robust authentication mechanisms, deploying and maintaining such a system can be complex. Consensus among nodes and key management in a distributed environment requires flexibility and efficiency, posing challenges in building a cohesive and manageable blockchain network infrastructure.

Integrating Blockchain can impact the performance of WSN systems, especially in networks with a large number of nodes and high communication frequencies. Additionally, blockchain consensus mechanisms like Proof of Work can incur significant computational costs and energy consumption, posing challenges to network performance and fault tolerance. To be fair, another comparison between WSNs deploying Blockchain and traditional networks is provided in Table 3.

Table 3. A comparison between two types of WSNs (with and without Blockchain)

Blockchain integrated WSNs	Traditional WSNs
High-security levels	Low-security levels
Requires more computational capacity for data processing and data storage.	Low computational capacity
Distributed ledger	Client-Server architecture
High energy consumption	Low energy consumption
Decentralized networks	Centralized networks
Complicated to implement and maintain	Quite simple to implement and maintain

With the development of electronic and computing technologies, we believe that the problems, as shown in Table 3, can be solved to support the networks with Blockchain. Hence, the networks can provide higher quality of services as an increasing demand of all customers. In summary, applying Blockchain in WSNs offers many benefits but presents numerous challenges that must be addressed to ensure effectiveness and security in this complex and dynamic environment.

5. Conclusions and Future Work

The paper presents specific applications of blockchain technology in WSNs, including blockchain-based encryption methods, security models, secure localization, intrusion detection, and consensus algorithms. These studies all emphasize the diversity and creativity in applying Blockchain to enhance the security and performance of WSNs. Additionally, the paper introduces some unique methods, such as integrating Blockchain into routing to optimize processes and using smart contracts to identify malicious nodes. A consensus-based blockchain system model is proposed to verify information and ensure quick accuracy in WSNs.

In exploring consensus algorithms, future research could involve conducting a comparative analysis of their performance and applicability in WSNs, considering factors like scalability, energy efficiency, and fault tolerance. Optimizing consensus algorithms tailored explicitly for WSNs or exploring novel consensus mechanisms to address emerging challenges would be important future research directions.

Author Contributions: Conceptualization: Minh T. Nguyen. and Mui D. Nguyen; methodology: Mui D. Nguyen.; software: Minh T. Nguyen.; validation: Thang C. Vu, Tien M. Ta,. and Z.Z.; formal analysis: Quang A. Tran, Dung T. Nguyen; investigation: Minh T. Nguyen.; resources: Mui D. Nguyen.; data curation: Minh T. Nguyen.; writing—original draft preparation: Mui D. Nguyen.; writing—review and editing: Minh T. Nguyen; visualization: Quang A. Tran, Dung T. Nguyen; supervision: Thang C. Vu; project administration: Tien M. Ta; funding acquisition: Minh T. Nguyen.

Funding: This research received no external funding

Data Availability Statement: Data can be shared based on any requests to the corresponding authors.

Acknowledgments: The authors would like to thank Thai Nguyen University of Technology, Thai Nguyen University, Ministry of Education and Training (Project B2023-TNA-16), Viet Nam for the support.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Comput. Networks*, vol. 52, no. 12, pp. 2292–2330, Aug. 2008, doi: 10.1016/j.comnet.2008.04.002.

[2] Q. Wang and I. Balasingham, "Wireless Sensor Networks - An Introduction," in *Wireless Sensor Networks: Application-Centric Design*, InTech, 2010. doi: 10.5772/13225.

[3] L. B. Ruiz, J. M. Nogueira, and A. A. F. Loureiro, "MANNA: a management architecture for wireless sensor networks," *IEEE Commun. Mag.*, vol. 41, no. 2, pp. 116–125, Feb. 2003, doi: 10.1109/MCOM.2003.1179560.

[4] M. Tuan Nguyen, K. A. Teague, and N. Rahnavard, "CCS: Energy-efficient data collection in clustered wireless sensor networks utilizing block-wise compressive sensing," *Comput. Networks*, vol. 106, pp. 171–185, Sep. 2016, doi: 10.1016/j.comnet.2016.06.029.

[5] I. Khan, F. Belqasmi, R. Glitho, N. Crespi, M. Morrow, and P. Polakos, "Wireless sensor network virtualization: early architecture and research perspectives," *IEEE Netw.*, vol. 29, no. 3, pp. 104–112, May 2015, doi: 10.1109/MNET.2015.7113233.

[6] M. T. Nguyen and K. A. Teague, "Distributed DCT based data compression in clustered wireless sensor networks," in *2015 11th International Conference on the Design of Reliable Communication Networks (DRCN)*, Mar. 2015, pp. 255–258. doi: 10.1109/DRCN.2015.7149022.

[7] D. Martins and H. Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey," in *2010 13th International Conference on Network-Based Information Systems*, Sep. 2010, pp. 313–320. doi: 10.1109/NBiS.2010.11.

[8] M. Nguyen, C. Nguyen, and H. T. Tran, "A Framework of Deploying Blockchain in Wireless Sensor Networks," *EAI Endorsed Trans. Ind. Networks Intell. Syst.*, vol. 9, no. 32, p. e3, Aug. 2022, doi: 10.4108/eetinis.v9i32.1125.

[9] D. G. Padmavathi and M. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," *Int. J. Comput. Sci. Inf. Secur.*, vol. 4, no. 1, Sep. 2009, [Online]. Available: http://arxiv.org/abs/0909.0576

[10] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2–3, pp. 293–315, Sep. 2003, doi: 10.1016/S1570-8705(03)00008-8.

[11] Y. Sun, Z. Han, and K. J. R. Liu, "Defense of trust management vulnerabilities in distributed networks," *IEEE Commun. Mag.*, vol. 46, no. 2, pp. 112–119, Feb. 2008, doi: 10.1109/MCOM.2008.4473092.

[12] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 867–880, May 2012, doi: 10.1016/j.jnca.2011.03.005.
[13] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, May 2005, pp. 46–57. doi: 10.1145/1062689.1062697.
[14] W. Xu, W. Trappe, and Y. Zhang, "Channel surfing," in *Proceedings of the 6th international conference on Information processing in sensor networks - IPSN '07*, 2007, p. 499. doi: 10.1145/1236360.1236423.
[15] E. Shih *et al.*, "Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks," in *Proceedings of the 7th annual international conference on Mobile computing and networking*, Jul. 2001, pp. 272–287. doi: 10.1145/381677.381703.
[16] M. T. Nguyen and K. A. Teague, "Mobile distributed compressive sensing for data collection in wireless sensor networks," in *2015 International Conference on Advanced Technologies for Communications (ATC)*, Oct. 2015, pp. 188–193. doi: 10.1109/ATC.2015.7388317.
[17] A. Woo and D. E. Culler, "A transmission control scheme for media access in sensor networks," in *Proceedings of the 7th annual international conference on Mobile computing and networking*, Jul. 2001, pp. 221–235. doi: 10.1145/381677.381699.
[18] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 74–81, Jan. 2008, doi: 10.1109/MPRV.2008.6.
[19] B. Parno, A. Perrig, and V. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," in *2005 IEEE Symposium on Security and Privacy (S& P'05)*, 2005, pp. 49–63. doi: 10.1109/SP.2005.8.
[20] J. Grover and S. Sharma, "Security issues in Wireless Sensor Network — A review," in *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Sep. 2016, pp. 397–404. doi: 10.1109/ICRITO.2016.7784988.
[21] Y.-T. Wang and R. Bagrodia, "SenSec: A Scalable and Accurate Framework for Wireless Sensor Network Security Evaluation," in *2011 31st International Conference on Distributed Computing Systems Workshops*, Jun. 2011, pp. 230–239. doi: 10.1109/ICDCSW.2011.26.
[22] A. S. K. Pathan, Hyung-Woo Lee, and Choong Seon Hong, "Security in wireless sensor networks: issues and challenges," in *2006 8th International Conference Advanced Communication Technology*, 2006, pp. 6 pp. – 1048. doi: 10.1109/ICACT.2006.206151.
[23] M. T. Nguyen and K. A. Teague, "Compressive sensing based energy-efficient random routing in wireless sensor networks," in *2014 International Conference on Advanced Technologies for Communications (ATC 2014)*, Oct. 2014, pp. 187–192. doi: 10.1109/ATC.2014.7043381.
[24] H. Modares, R. Salleh, and A. Moravejosharieh, "Overview of Security Issues in Wireless Sensor Networks," in *2011 Third International Conference on Computational Intelligence, Modelling & Simulation*, Sep. 2011, pp. 308–311. doi: 10.1109/CIMSim.2011.62.
[25] T. C. Vu, M. T. Nguyen, V. T. Nguyen, and Q. C. Le, "Approach New Framework of Compressive Sensing Based Secret Sharing in Wireless Sensor Network: Theory and Applications," in *Advances in Information and Communication Technology*, 2024, pp. 26–34. doi: 10.1007/978-3-031-50818-9_4.
[26] J. H. Larrier, "A Brief History of Blockchain," in *Transforming Scholarly Publishing With Blockchain Technologies and AI*, 2021, pp. 85–100. doi: 10.4018/978-1-7998-5589-7.ch005.
[27] A. A. Maksutov, M. S. Alexeev, N. O. Fedorova, and D. A. Andreev, "Detection of Blockchain Transactions Used in Blockchain Mixer of Coin Join Type," in *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, Jan. 2019, pp. 274–277. doi: 10.1109/EIConRus.2019.8656687.
[28] A. E. Guerrero-Sanchez, E. A. Rivas-Araiza, J. L. Gonzalez-Cordoba, M. Toledano-Ayala, and A. Takacs, "Blockchain Mechanism and Symmetric Encryption in A Wireless Sensor Network," *Sensors*, vol. 20, no. 10, p. 2798, May 2020, doi: 10.3390/s20102798.
[29] R. Khalid, M. W. Malik, T. A. Alghamdi, and N. Javaid, "A consortium blockchain based energy trading scheme for Electric Vehicles in smart cities," *J. Inf. Secur. Appl.*, vol. 63, p. 102998, Dec. 2021, doi: 10.1016/j.jisa.2021.102998.
[30] S. N. G. Gourisetti, M. Mylrea, and H. Patangia, "Evaluation and Demonstration of Blockchain Applicability Framework," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1142–1156, Nov. 2020, doi: 10.1109/TEM.2019.2928280.
[31] O. Samuel and N. Javaid, "GarliChain: A privacy preserving system for smart grid consumers using blockchain," *Int. J. Energy Res.*, vol. 46, no. 15, pp. 21643–21659, Dec. 2022, doi: 10.1002/er.7040.
[32] İ. Gazioğlu, T. Vu Van, A. F. Büyük, T. Eren, L. A. Tuan, and C. Oana, "Real-Life Demonstration of Blockchain Based Flexibility Trading Between FSPs and DSO," in *2023 Asia Meeting on Environment and Electrical Engineering (EEE-AM)*, Nov. 2023, pp. 01–05. doi: 10.1109/EEE-AM58328.2023.10395779.
[33] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, Jun. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.
[34] C. V. N. U. B. Murthy, M. L. Shri, S. Kadry, and S. Lim, "Blockchain Based Cloud Computing: Architecture and Research Challenges," *IEEE Access*, vol. 8, pp. 205190–205205, 2020, doi: 10.1109/ACCESS.2020.3036812.
[35] H. Pervez, M. Muneeb, M. U. Irfan, and I. U. Haq, "A Comparative Analysis of DAG-Based Blockchain Architectures," in *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)*, Dec. 2018, pp. 27–34. doi: 10.1109/ICOSST.2018.8632193.
[36] P. Godsiff, "Bitcoin: Bubble or Blockchain," in *Agent and Multi-Agent Systems: Technologies and Applications*, 2015, pp. 191–203. doi: 10.1007/978-3-319-19728-9_16.
[37] M. H. Kumar, V. Mohanraj, Y. Suresh, J. Senthilkumar, and G. Nagalalli, "Retraction Note to: Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. S1, pp. 639–639, Apr. 2023, doi: 10.1007/s12652-022-04293-y.
[38] L. Feng, H. Zhang, L. Lou, and Y. Chen, "A Blockchain-Based Collocation Storage Architecture for Data Security Process Platform of WSN," in *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD))*, May 2018, pp. 75–80. doi: 10.1109/CSCWD.2018.8465319.

[39] A. Kumar and A. R. Pais, "Blockchain based En-Route Filtering of False Data in Wireless Sensor Networks," in *2019 11th International Conference on Communication Systems & Networks (COMSNETS)*, Jan. 2019, pp. 1–6. doi: 10.1109/COMSNETS.2019.8711352.
[40] Fan Ye, H. Luo, Songwu Lu, and Lixia Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 4, pp. 839–850, Apr. 2005, doi: 10.1109/JSAC.2005.843561.
[41] X. Yang, J. Lin, W. Yu, P.-M. Moulema, X. Fu, and W. Zhao, "A Novel En-Route Filtering Scheme Against False Data Injection Attacks in Cyber-Physical Networked Systems," *IEEE Trans. Comput.*, vol. 64, no. 1, pp. 4–18, Jan. 2015, doi: 10.1109/TC.2013.177.
[42] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward resilient security in wireless sensor networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, May 2005, pp. 34–45. doi: 10.1145/1062689.1062696.
[43] Kui Ren, Wenjing Lou, and Yanchao Zhang, "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks," *IEEE Trans. Mob. Comput.*, vol. 7, no. 5, pp. 585–598, May 2008, doi: 10.1109/TMC.2007.70753.
[44] Sencun Zhu, S. Setia, S. Jajodia, and Peng Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004*, pp. 259–271. doi: 10.1109/SECPRI.2004.1301328.
[45] A. Kumar and A. R. Pais, "A New Combinatorial Design Based Data En-Route Filtering Scheme for Wireless Sensor Networks," in *2018 Twenty Fourth National Conference on Communications (NCC)*, Feb. 2018, pp. 1–6. doi: 10.1109/NCC.2018.8600153.
[46] H. Lazrag, A. Chehri, R. Saadane, and M. D. Rahmani, "A Blockchain-Based Approach for Optimal and Secure Routing in Wireless Sensor Networks and IoT," in *2019 15th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, Nov. 2019, pp. 411–415. doi: 10.1109/SITIS.2019.00072.
[47] G. Ramezan and C. Leung, "A Blockchain-Based Contractual Routing Protocol for the Internet of Things Using Smart Contracts," *Wirel. Commun. Mob. Comput.*, vol. 2018, pp. 1–14, Nov. 2018, doi: 10.1155/2018/4029591.
[48] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, "A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for Wireless Sensor Networks," *Sensors*, vol. 19, no. 4, p. 970, Feb. 2019, doi: 10.3390/s19040970.
[49] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Jan. 2017, pp. 1–5. doi: 10.1109/ICACCS.2017.8014672.
[50] W. She, Q. Liu, Z. Tian, J.-S. Chen, B. Wang, and W. Liu, "Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks," *IEEE Access*, vol. 7, pp. 38947–38956, 2019, doi: 10.1109/ACCESS.2019.2902811.
[51] R. Chanana, A. K. Singh, R. Killa, S. Agarwal, and P. S. Mehra, "Blockchain Based Secure Model for Sensor Data in Wireless Sensor Network," in *2020 6th International Conference on Signal Processing and Communication (ICSC)*, Mar. 2020, pp. 288–293. doi: 10.1109/ICSC48311.2020.9182776.
[52] M. A. Almaiah, "A New Scheme for Detecting Malicious Attacks in Wireless Sensor Networks Based on Blockchain Technology," in *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*, 2021, pp. 217–234. doi: 10.1007/978-3-030-74575-2_12.
[53] W. Tiberti, A. Carmenini, L. Pomante, and D. Cassioli, "A Lightweight Blockchain-based Technique for Anti-Tampering in Wireless Sensor Networks," in *2020 23rd Euromicro Conference on Digital System Design (DSD)*, Aug. 2020, pp. 577–582. doi: 10.1109/DSD51259.2020.00095.
[54] D. Kraft, "Difficulty control for blockchain-based consensus systems," *Peer-to-Peer Netw. Appl.*, vol. 9, no. 2, pp. 397–413, Mar. 2016, doi: 10.1007/s12083-015-0347-x.