IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 13, 2021, accepted September 1, 2021, date of publication September 10, 2021,
date of current version September 24, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3111923

Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey

LAKSHMANA KUMAR RAMASAMY[1], (Member, IEEE), FIROZ KHAN K. P.[2], AGBOTINAME LUCKY IMOIZE[3,4], (Member, IEEE), JOSHUA O. OGBEBOR[5], SEIFEDINE KADRY[6], (Senior Member, IEEE), AND SEUNGMIN RHO[7]

[1]Centre of Excellence for Artificial Intelligence and Machine Learning, Hindusthan College of Engineering and Technology, Coimbatore 641028, India
[2]Dubai Men's College, Higher Colleges of Technology, Dubai, United Arab Emirates
[3]Department of Electrical and Electronics Engineering, University of Lagos, Akoka, Lagos 100213, Nigeria
[4]Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University Bochum, 44801 Bochum, Germany
[5]Department of Electrical and Computer Engineering, School of Electrical Engineering and Computer Science, Louisiana State University, Baton Rouge, LA 70803, USA
[6]Department of Applied Data Science, Noroff University College, 4612 Kristiansand, Norway
[7]Department of Industrial Security, Chung-Ang University, Seoul 06974, South Korea

Corresponding author: Seungmin Rho (smrho@cau.ac.kr)

This work was supported in part by the Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE), The Competency Development Program for Industry Specialist, under Grant P0008703, and in part by the Ministry of Science and ICT (MSIT), South Korea, under the Information Technology Research Center (ITRC) Support Program IITP-2021-2018-0-01799 supervised by the Institute for Information & Communications Technology Planning & Evaluation (IITP).

ABSTRACT Wireless Sensor Networks (WSNs) are broadly applied for various applications in tracking and surveillance due to their ease of use and other distinctive characteristics compelled by real-time cooperation among the sensor nodes. In WSNs, security is becoming a critical issue, as the techniques for malicious node detection adopt a one-time, centralized decision-making approach. With this paradigm, errors are difficult to avoid, and reproducibility and traceability are challenging. Hence, malicious node discovery technologies in conventional WSNs cannot assure traceability and fairness of the detection method. Herein, this paper discusses an in-depth survey of a blockchain-based approach for malicious node detection, an exhaustive examination of the integration of blockchain techniques with WSNs (BWSN), and insights into this novel concept. This survey discusses the architecture, sector-wise applications, and uses of BWSN. Moreover, this survey describes malicious node detection based on BWSN in two parts: 1) the BWSN architecture for detecting the malicious nodes and 2) the smart contract aspects in malicious node detection. Next, this survey explains the contributions of blockchain for WSN data management, which involves online information aggregation and may include auditing, event logs, and storage for information analysis and offline query processing. This survey first presents the conventional WSN solutions then the blockchain-based WSN solutions for data management. Additionally, this survey discusses the contributions of blockchain for WSN security management. It first examines the centralized WSN models for security problems, followed by a discussion of the blockchain-based WSN solutions for security management, such as offering access control, preserving information integrity, guaranteeing privacy, and ensuring WSNs' node longevity.

INDEX TERMS Wireless sensor networks (WSNs), blockchain technology, malicious node detection, network security management, distributed consensus algorithm.

I. INTRODUCTION

Wireless sensor networks (WSNs) are generally composed of dispersed micro-devices (termed sensors), which may be embedded and possess simple or various sensing capabilities. These networks are widely used in various areas such as smart homes, military and industrial applications due to their wide range of coverage areas support, massive precision monitoring, remote monitoring, fast stabilization, high fault tolerance and ease of use and unique characteristics including self-organization [1].

However, sensor nodes are inherently limited, as they can only permit limited energy, processing capability, transmission range, and memory on board. Moreover, as a

The associate editor coordinating the review of this manuscript and approving it for publication was Tai-Hoon Kim.

consequence of these limitations, sensor nodes are vulnerable to compromise. Risks facing WSN security often arise from outside and inside the network, in which the proper network nodes are compromised and sometimes forced to act as malicious nodes. The ability to detect, contain, and purge in-network malicious nodes in good time is an equally essential concern for WSN security. Resolving the issues related to security has had a profound impact on the design and development trends of WSNs and has attracted wide attention in the literature.

Furthermore, various mechanisms for malicious nodes detection in wireless sensor networks have been proposed. For instance, Min and Ranxin [1] introduced a technique to detect Malicious node Detection using a Triangle Module fusion Operator (MDTMO), which can check selective forward attacks. This common network attack makes nodes discard all or certain data packets selectively so that the cluster head and base station cannot receive the full monitoring data. The MDTMO technique establishes packet loss send-receive and receive-forward membership functions based on the information packets sent to a node, obtained by the node, and forwarded by the same node. It then uses the triangle module fusion technique on the membership functions to detect a potentially malicious device. The base station (BS) device is alerted of the potentially compromised node, detects its channel and buffer occupancy, and tries to assess if the packet drops are due to network congestion. Suppose the WSN quality is better than the result in such congestion and data loss. In that case, it is regarded that the packets loss comes from a selective forward attack rather than jamming, and the device is labelled malicious.

Kimura *et al.* [2] proposed a method that detects malicious nodes via the collaboration of honest nodes to separate the detected malicious nodes via an inter-node vote logically. This approach is especially applicable in WSNs deployed inaccessible spaces prone to physical tampering rather than remote penetration. Often, attackers will attempt to steal encryption information or inject malicious sensor nodes into the network physically in these scenarios. Hence, there is no guarantee that encryption information is always protected, requiring the need for a malicious node detection approach that does not rely on encryption information.

Jaint *et al.* [3] also studied a common technique for malicious node detection – the weighted trust method – in a WSN containing sensing nodes (SN), cluster heads (CH), and forward nodes (FN) along with a BS. In the weighted trust approach, each sensor node is assigned a weight corresponding to the amount of trust associated, actively evaluated based on the node behaviour. In principle, the trust weight decreases every time the node presents false information and is then labelled malicious once the trust weight falls below a threshold. In the study, the data obtained by the sensor node were sent to CH; All CHs send the data to an FN, which sends it to the BS. The authors considered two situations, one with a single cluster head exclusive of a grid and another with a non-overlapping grid and numerous cluster heads. They found the weighted trust approach to be more rapid in the latter scenario. While similar malicious nodes detection approaches offer a practical resolution to the malicious node detection problem in WSN, none provides a mechanism to store the execution process of malicious nodes detection or to store the original node data for accurate traceability in the future. The emergence of smart contracts and blockchain techniques gives a novel route for detecting malicious devices in WSNs.

In addition, Blockchain permits peer-to-peer communication more quickly with the aid of a distributed ledger. Here, the distributed ledger is tamper-proof, which does not allow misinterpretation or wrong authentications. Furthermore, blockchain permits WSNs to execute transactions among the devices in cooperation and improves the confidentiality and trustworthiness of WSN data, making it more reliable. A smart contract can execute predefined processes when observed irregular behaviour or limit conditions are activated and organize complete process information into information blocks that can be tracked and proven. With the integration of blockchain in WSN, the data flow is safer and more trustworthy. Hence, in BWSNs, network harassment by malicious nodes cannot only be controlled, the traceability and transparency of the detection process can also be guaranteed. This two-fold advantage of BWSNs – data provenance and malicious node detection accuracy – forms the core of this work. Sidhu, Sapra and Dhaliwal, Rashid and Siddique provide more information on blockchain and smart contracts in WSN malicious node detection [4]–[6].

WSNs are inherently resource-constrained and lack the requirements for blockchain applications and smart contracts [7]. To this end, Ellul and Pace [8] outlined a reference design architecture and implementation of a split virtual machine for WSNs, where the computationally intensive operations in accessing the blockchain systems are offloaded to unconstrained nodes. Concerning the resource constraints in the Internet of things (IoT) networks, Pan *et al.* [9] proposed a blockchain-based edge chain framework in which unconstrained edge servers provide resource-constrained devices. The edge cloud resource pool is associated with each IoT device account and resource usage, and smart contracts are employed to organize resource access based on priority and past behaviour of the nodes. These research thrusts suggest that blockchain is gaining ground as a candidate technology for future WSNs.

However, there are other various blockchain-powered WSN solutions in the literature. For instance, Islam and Kundu [10] proposed a smart contract using blockchain to offer data security and personal privacy in a short-term home leasing scenario. Kang *et al.* [11] presented a blockchain and smart contract option for renewable power trading to execute transactions without third-party intervention. Using a smart contract framework, Zhang *et al.* [12] introduced an access control policy, including static access right validation based on predefined rules and behaviour-based access right evaluation, to achieve network security.

Therefore, this survey presents an analysis of BWSN in literature and a theoretical preamble on blockchain and WSN. Next, we present a detailed examination of the ability to integrate WSNs into the blockchain. Further to this, we offer an insightful view of the technological challenges restraining the application of BWSN. The main contributions are as follows:

1) This survey first discusses the introduction and applications of WSN, the classification of sensor nodes, and the numerous challenges related to energy, communication and routing, security, availability, operating system, hardware and software limitations, MAC Layer, and time synchronization issues.
2) Next, this survey presents an overview, the most important features, security analysis, and the various applications of the blockchain technique.
3) The focal point of this paper concentrates on the integration of blockchain with WSN (BWSN). This survey discusses the architecture, sector-wise applications, and uses of BWSN.
4) Moreover, this survey describes malicious node detection based on BWSN in two parts: 1) the BWSN architecture for detecting the malicious nodes and 2) the smart contract aspects in malicious node detection.
5) Next, this survey explains the contributions of blockchain for WSN data management, which involves online information aggregation and may include auditing, event logs, and storage for information analysis and offline query processing. This survey first presents the conventional WSN solutions then the blockchain-based WSN solutions for data management.
6) Additionally, this survey discusses the contributions of blockchain for WSN security management. It first examines the centralized WSN models for security problems, followed by a discussion of the blockchain-based WSN solutions for security management, such as offering access control, preserving information integrity, guaranteeing privacy, and ensuring WSNs' node longevity.

The remainder of the paper is organized as follows. Section 2 presents a general overview of wireless sensor networks and blockchain techniques. The integration of blockchain with WSN is described in Section 3. Section 4 offers the malicious node detection method using BWSN, while the contributions of blockchain for WSN Data management are explained in Section 5. Section 6 introduces the contributions of blockchain for WSN security management. Section 7 provides a comparison with previously published works. Section 8 describes the lessons learned from the survey, and finally, the paper is concluded in Section 9.

II. WIRELESS SENSOR NETWORKS AND BLOCKCHAIN TECHNIQUES

This section explains overview of WSN, Classifications of Wireless Sensor Nodes, WSN Challenges, Overview of blockchain techniques, Important blockchain Features, and blockchain security analysis

A. WIRELESS SENSOR NETWORKS

Modern-day sensors are ubiquitous; our daily lives are consumed with sensor-based applications in cars, cell phones, computers, electrical gadgets, factories, machines, wristwatches, and even in the human body. WSNs are generally summarized as a network of nodes that sense information jointly and, in general, allow interactions with remote computing devices, persons, and the nearby environment [13], as shown Fig. 1 shows the WSN architecture.

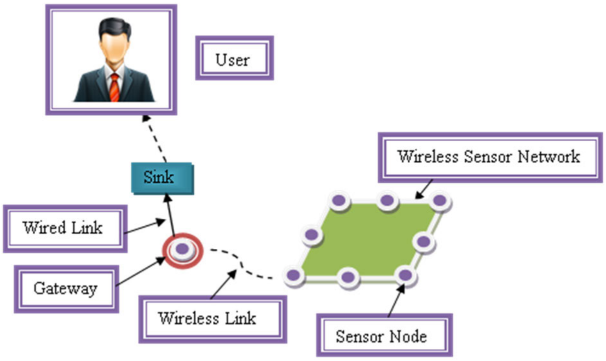


FIGURE 1. A typical WSN architecture.

In WSNs, all nodes are equipped with sensors to sense physical phenomena, such as temperature, light, pressure, humidity, and so on [14], to process information and then send them to a sink or base station for more processing and analyses. WSNs can be heterogeneous and may have thousands of tiny sensor nodes [15]. A single node usually contains extremely low processing, storage, and broadcasting capability [16]–[19]. Despite these limited features, these nodes are utilized within numerous commercial and military applications; their initial development was promoted in military applications for surveillance in battle zones.

Research on wireless sensor networks dates back to the 1980s when the United States Defense Advanced Research Projects Agency (DRPA) initiated the Distributed Sensor Network (DSN) program for the US military [20]. The distributed sensor network was anticipated to contain inexpensive cooperating nodes and achieve autonomous control [21]; however, technology was not as advanced as it was presumed to be [22]. Sensors were quite large (i.e. more massive than a shoebox), and their application was insufficient for several potential applications [23], [24]. However, the growth and progression in processing, micro-electro-mechanical, and transmission technologies have contributed to a significant shift in WSN research since then, bringing it closer to its pioneer vision.

The trend for WSN research improved in 1998 and incited the interest of scientists with worldwide participation. WSN research focused on network data processing and network technologies appropriate for the ad-hoc environment and highly dynamic sensor nodes at the beginning of this trend. Moreover, advancements in technology included the decreased size of sensor nodes and reduced costs, promoting the emergence of numerous civil applications as vehicular sensor networks, environment monitoring, and body sensors [25], [26]. Today, the utilization of WSNs can be prominently observed within the industrial automation sector, with almost 24 million wireless sensors and actuators around the globe.

For numerous applications, the location data of the nodes must be known. Since this data is not necessarily obtainable, there is great interest in methods for assessing the locations of individual nodes. The accuracy and computational complexity of such ''localization'' algorithms is still a major problem. But, there are cases where the nodes are located in one of some pre-determined conditions. In those cases, calculating the relative positions of the nodes relative to each other may be enough to decide their true positions. Yan *et al.* [27] proposed the energy-efficient node stabilization algorithm in optical WSN. Furthermore, Yan *et al.* [28] proposed a low energy PSO-based node positioning on the optical WSN.

In the next subsection, the WSN is first discussed briefly, and subsection 2.1.2 summarizes the challenges associated with WSNs.

1) CLASSIFICATIONS OF WIRELESS SENSOR NODES

Table 1 displays the classification of some WSN sensor nodes based on application.

TABLE 1. Classification of sensor nodes.

Classifications	Descriptions
Underwater WSN	Sensor nodes can be deployed below water. In underwater applications, WSN batteries cannot be easily replaced; thus, adequate pre-planning is important.
Underground WSN	Underground WSN organization is more challenging than terrestrial WSN as it involves careful planning. Sensor nodes can be placed deep underground, in the shallow soil, in mines, or within caves to track underground conditions like moisture content, vibration, and so on. As with underwater scenarios, battery charging and replacement cannot be easily achieved in this scenario.
Terrestrial WSN	In terrestrial WSNs, nodes can be deployed and dispersed almost consistently over an area with showed strategies. Using various routing protocols, energy minimization techniques are applicable within terrestrial WSNs.
Multi-Media WSN	This classification is based on the data generated by the sensor nodes. Sensor nodes can generate, store, and transmit multimedia information, such as videos, audio cameras, and microphones. High bandwidth, security, QoS, link quality, and power are needed for multimedia WSNs [29].
Mobile WSN	This classification is based on the mobility of the sensor nodes, which can sense the physical environment [30] and be self-configured while in motion. Mobile WSNs can supervise a specimen habitat, targeting, tracking, and surveillance within military applications.

2) WIRELESS SENSOR NETWORK CHALLENGES

The challenges of wireless sensor networks are briefly discussed as follows:

A. Energy

Sensors require some energy or power reserves to execute different operations when needed. Energy management is a principal issue in WSN [31], [32]. Nodes are usually operated with an attached battery, which has a limited capacity. This power is exhausted by sensing, collecting, processing, and broadcasting information to the sink node. The bulk part of energy utilization is generally due to transmission rather than instruction processing. On average, 3,000 instructions can be processed with a similar energy cost of transmitting a single bit over 100 m with radio. In addition, sensors are required to be active for sink node registration or BSs queries. During this time, nodes do not perform any valuable tasks while the energy used up is wasted. Hence, the energy available is expended during transmission, reception, and idle operation [33].

B. Communication and Routing

Determining a communication route to the BS from each sensor node is a challenging part of the network design. The objective generally is to keep the nodes alive for an extended period. Mostly, the nodes only support small coverage for communication; therefore, intermediary forwarding nodes are employed. The deployment strategy and routing protocols directly affect the communication profile and the overall performance of the WSN. WSN is dissimilar from traditional routing in other networks in different ways: nodes in WSNs operate wirelessly. Hence, there is no wired infrastructure, and wireless media is generally less reliable than wired media routing. WSN nodes typically pass information hop-by-hop to sink, directly to the base station, or using cluster heads when some local organization into cluster cells is employed.

C. Security

Security is another crucial issue in WSN. WSNs' data travel wirelessly through the air, and these wireless signals are open to everyone, allowing anyone to monitor and participate in the communication even without invitation [34]. Mostly, WSN nodes operate in the Independent Side Band (ISB) that is license-free. Thus, security is critical in commercial and military applications to prevent malicious attacks like unauthorized access and denial of service DoS attacks. Security requirements for WSNs can be categorized as follows:

- Information confidentiality: Confidentiality refers to an assurance of legal access to information. A major security issue in the wireless operated network is that the radio spectrum is an open medium [35] and can be easily monitored by anyone [36]. For instance, an attacker can sniff and interfere with the transmitted packet. The standard approach is to transmit all data only after encryption with a secret key that only intended receivers possess to maintain data confidentiality.

- Information authenticity: Moreover, a novel, misleading packet can be injected into the communication between nodes by an attacker if he somehow attains knowledge of the packet format in the WSN protocol stack. The injected packet then carries misleading or incorrect information. Surveillance, tracking, and environment monitoring applications can be hijacked by such injected incorrect information. To overcome this, standard approaches can be adopted to maintain data authenticity using message authentication codes, signatures, secret keys, and broadcasting authentication.
- Information integrity: Owing to the instability of wireless channels transmission, errors are inherent in WSNs. Information travelling in electromagnetic media can be changed due to signal fading, signal reflection, signal diffraction, scattering, and various kinds of noise, requiring re-transmissions. A high number of re-transmissions can be very expensive in terms of energy expenditure in the WSN. Data integrity can be ensured using message integrity codes.

D. Availability

The sustained lifetime of sensor nodes is essential, especially in critical applications. Expending energy for excess or unnecessary communication and computation runs down the battery power sensor nodes early on. To guarantee the availability of nodes, energy-efficient routing algorithms and protocols are essential.

E. Operating System (OS)

As sensor nodes have a limited amount of memory, implementing power and small dimensions, the sensor node operating system must provide essential resource management and memory management. It should be less complicated compared to traditional OS. Mantis OS, Nano-Q, and TinyOS are specifically configured for wireless sensor networks. However, enhancements are crucial to accommodate the trends in the WSN design paradigm.

F. Hardware and software issue

As sensor devices are limited in size with bounded memory space, the power and speed of executing program instructions are a problem for WSNs. Generally, the sensor device contains a sensor, microcontroller, power backup, and transceiver. The sensor gathers then broadcasts information to a microcontroller for processing. The microcontroller executes program instructions and broadcasts the collected data to the sink device through the transceiver. The microcontroller oversees the WSN protocols for communication and computation. Utilizing flash memory devices is recommended since flash memory is quick and cheap. To protect the microcontroller power, sensor nodes must run in three conditions: idle, active, and sleep modes.

G. MAC Layer Issue

In a wireless sensor network, much of the energy wastage occurs at the MAC layer due to collision, empty hearing packet overhead, and busty traffic. Idle nodes exhaust 50 to 100% of their power for receiving packets. The Sensor-MAC periodic hearing and rest protocol is proposed to defeat this issue. In this protocol, nodes are free to select their hearing and rest schedule, and the duty cycle is pruned to be active when essential. Nodes listen for data within a period, and if nothing is received, they select a schedule then send synchronization information to the BS. Other MAC protocols include Timeout MAC, Dynamic sensor MAC, and Traffic-Adaptive MAC, each adhering to a different protocol and having its pros and cons.

H. Time Synchronization

Sensor nodes in the field are controlled independently. Any time their local clocks are not coordinated with other nodes, ambiguity and uncertainty of the sensed information can result [37].

B. BLOCKCHAIN TECHNIQUES

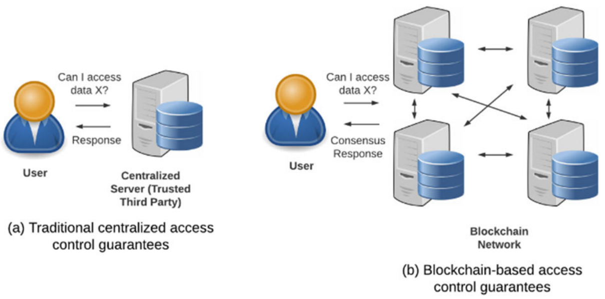
In this section, blockchain techniques are introduced briefly, and the most important features of blockchain are summarized. Furthermore, the security analysis in blockchain techniques and the categories based on their applications are presented.

1) OVERVIEW OF BLOCKCHAIN TECHNIQUES

Blockchain is a protected and distributed ledger that eases storing and tracing resources independent of a centralized third party authority [38]. Blockchain permits two parties to transmit and interchange messages in a peer-to-peer network [39] without the need for a sole trusted authority. It is verifiably safe against an attacker who attempts to mismanage the scheme and compromise the centralized controller [40], [41]. Resources can be either tangible (e.g. cars, money) or intangible (e.g. copyrights). In general, anything that contains a value can leverage a blockchain network to decrease its risks and safety hazards and decrease the cost of safety-related supervision [42], [43].

Blockchain technology has attracted much attention from industry and academia [44], [45], which began with Bitcoin, a cryptocurrency. Bitcoin garnered 180 billion dollars capitalization in 2018 [46], [47]. In 2016, in the Gartner report, blockchain technology attracted a billion dollars in enterprise and research investment, which is anticipated to increase shortly. The technique, at present, is used in numerous, common applications and steers the research in networking applications, such as the Internet of Things (IoT) [48]–[55], healthcare [56], [57], and cloud storage [58], [59]. Usually, blockchain technology proves its potential in any application that requires a centralized ledger [60]. A feasible instance that employs blockchain is the data network of Interbank and JP Morgan that provides quick, protected, and low-priced global expenses [61]. Also, IBM and supply chain systems currently evaluate their services capability using blockchain [62].

Potential blockchain applications in WSN include network supervision and authentication [63], security, privacy [64], confidentiality, provenance, and integrity. At present, these services are offered by a third-party broker or some less-effective non-distributed method. Blockchain technology can assure safety, which solves numerous conventional challenges as it provides an entirely distributed and verifiably authentic solution with consensus resolution [65]. Fig. 2 exemplifies the dissimilarities between the blockchain-based and conventional approaches to access control management [66]. A similar model could be applied to the other services in the WSN.



(a) Traditional centralized access control guarantees

(b) Blockchain-based access control guarantees

FIGURE 2. Differences between the blockchain-based and traditional centralized access management.

2) IMPORTANT BLOCKCHAIN FEATURES

The main features contributing to the compatibility and benefits of the blockchain technique in most application scenarios are shown in Table 2.

3) BLOCKCHAIN SECURITY ANALYSIS

Blockchain has also attracted research attention in decentralized networks due to its efficient anti-tampering feature; yet, it still shows vulnerabilities [70]. Common safety risks to blockchain are shown in Table 3.

Like WSN, the blockchain technique has broad applications in various areas, including verification, recognition, financial transactions, physical asset keys, intangible assets, and private and public records [85].

III. INTEGRATION OF BLOCKCHAIN WITH WSN

This section discusses the integration blockchain with WSN (BWSN) and its architecture, also explains the applications of BWSN.

A. BLOCKCHAIN-BASED WIRELESS SENSOR NETWORKS ARCHITECTURE

There are a rising number of instances of WSN and, thus, an increase in its chances of containing a higher amount of communicating nodes. This increased quantity of devices will lead to greater communication between devices, creating a wireless network. However, many difficulties would arise if this occurs since, in WSNs, the gathered information is generally stored in a central server. If the nodes desire to use some data in some other nodes, based on the centralized network structure, the information flow will occur through the central server. This execution flow is represented in Fig. 3. The rising needs of WSN and applications depict the bourgeoning WSN as a large-scale system for which the centralized server approach will not be practical. Blockchain technology provides a superior solution to the challenges faced by WSN.

TABLE 2. Important features of blockchain.

Features	Descriptions
Immutability	Peers approves all novel entries in the blockchain through decentralized consensus. The blockchain is almost tamper-proof; hence, all maintained entries in the blockchain are near-immutable. To change previous entries, attackers will have to compromise most of the nodes participating in the blockchain network, or else modifications in the block contents are easily detected.
Decentralization	Information transmission is authenticated and approved by a trusted major third party in a centralized network infrastructure. It suffers from the cost of protecting the centralized server in addition to performance bottlenecks. In the blockchain-based infrastructure, two devices can engage in transmissions, eliminating the reliance upon a middle device to keep data or grant approval [67], [68].
Auditability	All peers in a blockchain network have a blockchain copy and can consequently use all the time-stamped transaction data. This transparency allows peers to corroborate transactions with addresses of blockchain. Blockchain blocks are not the same in reality; therefore, the blockchain is pseudo-anonymous [69]. Although blockchain records blocks cannot be traced back to the owner, blockchain blocks can be held responsible, and deductions can be made on the transactions a particular blockchain block appoints.
Fault Tolerance	All the peers of a blockchain have the same replicas of ledger records. Some errors or information leaks in the blockchain network can be detected during decentralized consensus based on the replica saved in blockchain peers.

Many WSNs are built on the idea of forwarding information to a centralized server. The sensor nodes gather the data from the monitored environment and send the information broadcast to the central server through a wireless network. Similarly, large-scale WSNs need to gather information from the different sensor nodes. However, the processing power of available the wireless network's infrastructure may not be effective. For managing a huge amount of information on

TABLE 3. Blockchain security analysis.

Security Analysis	Explanation
Consensus Protocols Attacks	Attackers can destroy the consensus protocols, the framework for blockchain-based security [71], [72], by possessing a significantly vast chunk portion of the entire network's processing power. In severe cases, an attacker could manage to rebuild the chain [73]. The attacker, possessing more than half of the hash energy, could make blockchain agree on illegal blocks by resolving the consensus problem [74] quicker than the network peers sleep. At present, it has been verified that 33% of the hash energy is enough to overwhelm Proof of Work (PoW) [75].
Double Spending	Adversaries try to misguide the transaction receivers, e.g. in Bitcoin, to consume a similar coin. Likely attack approaches contain transmitting conflicting transactions [76] and pre-mining single or further blocks to obtain conflicting transactions approved by the blockchain [77].
Smart Contracts Vulnerability	Smart contracts are vulnerable because of the blockchain's bluntness and its irreversibility. Frauds and bugs are apparent to the adversaries and the public. Moreover, it is challenging to make up for bugs in organized, smart contracts owing to the blockchain's irreversibility. As an example, an assault on the Decentralized Independent Organization (DAO) in 2016, known as the attack of DAO, resulted in a divided Ethereum blockchain [78], [79].
Eclipse Attacks	Eclipse attacks refer to the P2P networks attacks where attackers monopolize all links to the genuine devices and prevent genuine devices from linking to some truthful peers. Eclipse attacks in the blockchain were initially higher in Bitcoin [80], [81] during the randomized protocol, in which a Bitcoin node-link [82] is labelled with a particular number of selected neighbours to maintain blockchain-associated functions and peer-to-peer interactions. The current Ethereum [83] label covers have been excellent against the eclipse attacks during the Kademlia peer-to-peer protocol acquired in Ethereum [84].
Distributed Denial of Service (DDoS) Attack	Adversaries could consume blockchain resources, such as network processing power, by initiating a coordinated attack. In 2016, attackers attained depreciated Ethereum Virtual Machine (EVM) commands to reduce the further processing of blocks. The enormous quantity of accounts created by the attackers led to a DDoS attack.
Programming Fraud	In programming source codes, the adversaries could use fraud to obtain blockchain properties, such as the piracy attack described in 2018 [78].
Privacy Key Leakage	The attackers could steal a private account key via conventional network attacks [78] or physically access the devices.

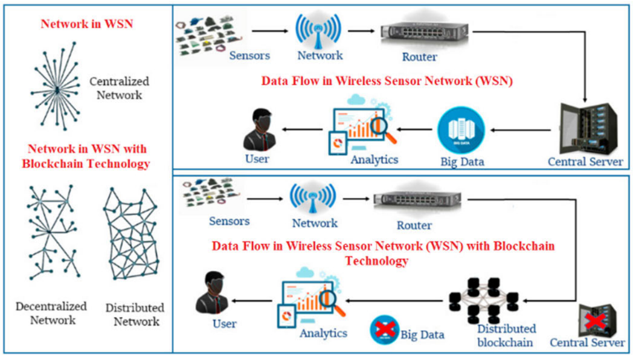


FIGURE 3. Centralized, decentralized, and distributed WSN and WSN data flow and BWSN data flow.

massive-scale WSN, it is essential to upgrade the wireless network structure. One of the best paths to achieve this is to set up a distributed network with capabilities for "Peer-to-Peer Networking (PPN), Disseminated File Distributing (DFS), and Independent Device Coordination (ADC)" operations [86].

Blockchain can take these three operations, enabling the WSN to trace many linked and networked nodes. Blockchain permits the WSN to execute transactions among the devices in collaboration, improving the confidentiality, trustworthiness, and reliability of WSN [87]. Also, peer-to-peer communication is permitted in a quicker route via the assistance of the distributed ledger, as displayed in Figure 3. The information flow pattern in BWSNs is dissimilar from sheer WSNs [88], whereby the distributed ledgers do not allow wrong authentications or misinterpretation in the information in the former. With the integration of blockchain in WSNs, information flow becomes safer and more trustworthy.

Blockchain technology has the following benefits for massive-scale WSNs: it allows for peer-to-peer communication opportunities; information is tamper-proof by design; it is extremely trustworthy and robust, possesses a record of historical transactions, and can hide private information; it permits self-directed processes via smart contracts and a disseminated file distribution system while eliminating dependence on a single authority, and it can be used to reduce costs and speed up transactions.

B. APPLICATIONS OF BLOCKCHAIN-BASED WIRELESS SENSOR NETWORKS

Table 4 demonstrates the application of WSN using blockchain [89].

IV. BLOCKCHAIN-BASED WIRELESS SENSOR NETWORKS MALICIOUS NODE DETECTION

This section presents the BWSN architecture for the detection of malicious nodes. It also outlines smart contract-based malicious node detection.

TABLE 4. Sector-Wise applications and uses for blockchain-based sensor networks.

Application Area	Instances
Smart City	Water and pollution information management, allowing transactions based on digital information, et al.
Business	Managing export and import information, software engineering, digital records, et al.
Food Retail Services	Online ordering, packing, shipping, delivery, transaction, and quality assurance information, et al.
Agriculture	Management of soil information, implementing records associated with agriculture information, delivery of agriculture commodities, etc.
Manufacturing	Management of products manufacture information, product packing information, products shipping information, et al.
Power	Power production information, power raw material information, and availability of resources information management, et al.
Distribution Logistics	Records storage and transport, sales records, digital money, utilized commodities, et al.
Healthcare	Storing the information of a genome, patients' digital reports, electronic healthcare records, prescription reports [90], et al.
Economics	Crypto-currency, money transfer [91], smart contracts, money deposits, et al.
Logistics and Transport	Vehicle tracing [92], logistics service identifiers, goods transport reports, toll information keeping, et al.

A. BLOCKCHAIN-BASED WIRELESS SENSOR NETWORKS ARCHITECTURE FOR DETECTION OF MALICIOUS NODES

The transition from a regular WSN to a BWSN is illustrated in Figure 4. As demonstrated in the first part of the figure, the regular WSN include the network controller, sensor nodes, and sink nodes [93]. The sensors perceive the desired indicators in their immediate environment in real-time and churn out useful monitoring information. Sensors forward the information to the associated sink nodes through the cellular link. The sink nodes collate the information sent by the sensor in its range of coverage, examine the sensor working condition in real-time, then forward the outcomes to the network controller through the backhaul network link.

As displayed in the bottom half of Fig. 4, the underlying structure of the WSN is adapted into the blockchain WSN, which contains four main devices, namely the contract supplying, CA, verification, and standard devices. The network controller is the contract issuing device in charge of issuing smart contracts. The sink nodes play the role of a verification device and CA device together. The CA device gives identity information based on the digital certificate to blockchain community members and can create or cancel an identity certificate of members.

The pre-chosen sink nodes are the verification device, primarily responsible for obtaining the supervising information gathered by the standard device, implementing the smart contract, verifying the transaction information validity, and updating and keeping the device information and the account status in the blockchain. Along with these, a piece of code, namely a smart contract, is organized on the distributed ledger that can manage the obtained exterior data. Specifically, the creation of all blocks is decided by pre-chosen devices and saved in a malicious node detection blockchain, Cmndb. The sensors are ordinary devices that merely upload the gathered supervising information.

Accordingly, the WSN whole structure can be mapped into the network of group blockchains for malicious nodes detection [94] in the blockchain network, which is formalized as follows: BWSN is a set of 8 tuples (N9C, sn, Sensor, Cmndb, T, SC,β, α), as shown in Table 5.

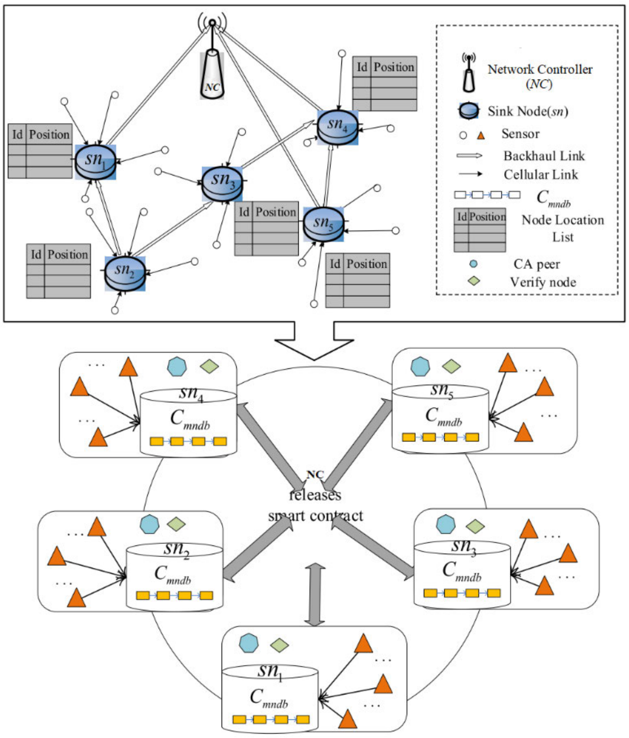


FIGURE 4. Blockchain-Based wireless sensor network structure for malicious nodes detection.

TABLE 5. Blockchain-Based wireless sensor networks 8-tuple set.

Tuple	Description
NC	The finite set of the network controller
Sn	Cluster heads finite set
Sensor	The finite set of sensors
Cmndb	Blockchain for detection of a malicious node
T	Sensors set of transaction.
SC	Cmndb smart contract
B	Nodes location list
α: Sec v SN --> Cmndb	Mapping from Cmndb to Sink node (SN) and nodes

To further distinguish the Cmndb blockchain, this work proposes block information using blockchain to detect the malicious node (Cmndb−BDS). It is different from the conventional wireless sensor networks, where discovery is untraceable. Cmndb−BDS maintains information on every transaction. The information structure is primarily separated into two segments. First, the block's header mainly includes the value of the former block's hash, where the hash value is utilized to link the former block and fulfills the requirements of the reliability of the Cmndbblockchain. Conversely, the body of the block includes the most critical data of the device in the block, such as ID, location, state, Forwarding Rate (FR), Delayed Transmission (DT), NS, NF, and Response Time (RT). These data are maintained mutually with the hash value of the former block and the block hash value formed by the random number.

Let D_1 to Dn denote each node information gathered by the node, the D1 node information hash pointer be denoted by Hash1, and Hash12 denote the Hash1 + Hash2 hash pointer. After The layer stack is appended, the unique Merkle root is created [95], [96]. Cmndbdoes did not merely utilize a "block + chain" chain information structure but, instead, stores the data gathered by all blocks in a Merkle Tree form [97]–[99] organized by a hash pointer. The block hash pointer is likely to change once the information of any block is altered, guaranteeing that the information cannot tamper. Additionally, based on the structure of the information of Cmndb−BDS, the information is stored in numerous nodes within the overall WSN to decrease the possibility of malicious manipulation, check fairness and protection, and enhance the discovery execution convenience.

B. MALICIOUS NODE DETECTION USING SMART CONTRACT

A smart contract is a programming code piece organized on a distributed ledger [60], managing the obtained data. The Cmndb blockchain leverages a smart contract platform [100] offered by Decentralized Application to raise its operability and flexibility.

The malicious sensor node discovery blockchain smart contract (Cmndb−SC) proposed in this survey includes the following relations [101]:

Cmndb-SC D (NC,sensor,sn,η, δ,QM,Cmndb - BDS)

Here,

- NC is the Cmndb−SC publisher.
- Sn is the node of aggregation, which the NC authorizes to vote.
- η is the node's reputation.
- δ is the indicator of malicious node assessment, which has FR, DT, and RT.
- QM is the positioning technique of WSNs.
- Cmndb−BDS is the Cmndb information structure.

To use a smart contract to detect malicious devices, the appropriate steps are given in Algorithm 1.

Algorithm 1 Malicious Node Detection in Smart Contract

```
Input   : Cmndb, Cmndb-SC, NC, sn, $\eta$, $\delta$, QM, Cmndb - BDS
Output  : Detected Malicious Nodes
Step 1  : NC provides Cmndb−SC to the whole network
Step 2  : NC authorizes sn to turn into a Cmndb−SC voter.
Step 3  : Sn situates the whole node in QM; therefore, the sensor ID
          and position are in one to one connection, then an entire node
          location list (NLL) is got.
Step 4  : Sn decides the sensor condition used in real circumstances.
Step 5  : Below the executing sensor condition, the gathered node data
          is computed to get the equivalent RT, FR, and DT.
Step 6  : Broadcast the RT, FR, and DT values to the Node Communication
          Quality (NCQ) purpose and compute the value of
          NCQ.
Step 7  : Compute the equivalent number of successful communications
          NS and number of failed communications NF values
          along with the NCQ value.
Step 8  : Compute the $\eta$ value.
Step 9  : Using the computed $\eta$, sn utilizes the Vote()function to choose
          the malicious node ID. The Vote()function is separated into
          three segments: First, along with the real scene, set a suitable
          threshold of voting (TV), Followed by, sn decide the $\eta$ range
          of everything in the coverage region sensors.
                if $\eta > TV$ then
                        node is malicious
                else
                        node is normal
                Lastly, the malicious node ID cast.
Step 10 : Along with the cast ID, appear in the NLL and detect the
          equivalent location of the node.
```

V. BLOCKCHAIN FOR WSN DATA MANAGEMENT

In the WSN, data management involves online information aggregation and includes auditing, event logs, storage for information analysis and offline query processing. Therefore, information management schemes are required to encompass these features and handle abstract multifaceted queries for high-level WSN applications [102]. In numerous WSN structures, information query processing is completed through a middleware layer between the application and network [103]. Because multiple WSN application domains are time-critical, WSN information management schemes must be time-conscious, despite the limited abilities of WSN nodes.

A. CONVENTIONAL WSN SOLUTIONS FOR DATA MANAGEMENT

In this subsection, several of the solutions for information management based on the WSN structure are reviewed. The instances where blockchain applications can give the information management service needed by the WSN are emphasized.

Solutions for data management using the WSN structure are typically decided during its development. In conventional WSNs, information is managed in a centralized style. Centralized solutions using the recent WSN structure range from service-oriented [104] to data-oriented [105] methods with the capacity for managing an enormous quantity of information [106] and the mobility of WSN information [107]. Despite their advantages, the difficulties observed in these centralized methods are that they do not concurrently give assurances for information accuracy and confidence in managing heterogeneous WSN information. Solutions for information management using the framework of Frequently Updated Time stamped and Structured (FUTS) [108] manages time stamping for information generation events but are deeply centralized. The general common feature of these solutions for information management is that they lack inherent features that give a layer of security and confidence crucial in WSN information management.

Several other solutions for information management in the conventional WSN structure utilize a partly decentralized method with distributed database services clusters. For example, Xiao *et al.* [109] employed the NoSQL database to save heterogeneous WSN information for various WSN information queries. As a related method in using distributed storage, another study [110] utilized an HDFS cluster that increased the scalability of WSN information management. However, the HDFS cluster does not give assurances of being tamper-proof. One more partially decentralized method with related faults is utilizing sub-servers to allow greater scalability [111].

Table 6 presents Data Management Solutions with a conventional WSN Infrastructure. Though these solutions tackle the centralized information management systems bottleneck, they do not accommodate large-scale traffic, which is obtainable with a blockchain network; thus, the authors do not assure creditability in WSN information management. The table shows that the information management structures guarantee information truthfulness and cater to the heterogeneity of WSN information.

TABLE 6. Solutions for data management with conventional WSN structure.

Methods	Integrity	Heterogeneity	Storage	Architecture
WSN applications using a framework for data-centric [105]	×	×	Cloud	Partially Decentralized
Access framework with Service Oriented and data-oriented [104]	✓	✓	Cloud/ Local	Centralized
A storage platform based on a massive scale object [106]	✓	×	Cloud	Partially Decentralized
WSN architecture for mobility support [107]	✓	×	Cloud/Local	Centralized
NoSQL-based huge WSN data storage solution [109]	×	✓	Cloud	Partially Decentralized
FUTS framework [108]	×	✓	Cloud	Centralized
Multi-sensor object tracking information for proficient storage [110]	×	✓	Cloud	Partially Decentralized
Framework for query optimization and unified storage for WSN data [111]	✓	×	Cloud/Local	Partially Decentralized

B. BLOCKCHAIN-BASED WSN SOLUTIONS FOR DATA MANAGEMENT

Although scalability and latency remain a direct challenge for information storage with blockchains, information management frameworks for WSN using blockchains have the advantages of wide imposed information credibility and non-reliance on semantics to logging WSN information formation actions. With distributed storage methods, like interplanetary File Systems (IPFS), executed along with blockchains, the WSN bulk information can be saved off-chain while keeping immutable logs and linked to the information inside the blockchain. Blockchain-based solutions are visualized to be at the least partly distributed. The WSN information of the user is maintained safe and private, exclusive of third-party interference for service provision.

In the literature, numerous works leverage the essential features of blockchain to enhance information management for the WSN. For instance, the study [112] leveraged the auditability and immutability of blockchain records for saving gathered information from drones based on general cloud service. Although the information storage itself can be decentralized, based on a distributed database, the blockchain's essential benefit is tamper-proofing and information integrity.

Olivera *et al.* [114] proposed a structure for saving medical records using blockchain exclusively for keeping reports and inquiries while employing available WSN information storage methods for hosting WSN information. The author's proposed solution is built in three stages: (i) off-chain based cloud information storage on Decentralized Hash Tables (DHT); (ii) blockchain-based method for the WSN information access control saved in the DHT [113], and (iii) the WSN edge devices. DHT devices request the blockchain for its benefits when it requests information. Methods that maintain the storage off-chain significantly decrease the storage needs of the nodes that keep all the blockchain copies. In the same way, [72] blockchain records leverage auditability to improve the distribution of saved information without authorizing intermediaries.

Off-chain storage with related solutions has shown promising for a distributed information management method in the WSN. For instance, a cloud blockchain with a multi-tiered structure was proposed to store WSN information [42]. In this reference, private blockchains linked to a cover public blockchain utilize cloud-based solutions for saving and recollecting blocks. The proposed structure in [115] utilizes the IPFS distributed storage method to protect WSN information, while the hashes of saved files of IPFS are stored in the blockchain. The IPFS files are blocked based on the file hash itself, therefore guaranteeing the integrity of the information.

Lu *et al.* [116] introduced FairAccess, a multi-layered framework that concentrates on confidentiality, dependability, and integrity, as a blockchain-enabled WSN structure. FairAccess has definitions of the transaction for allowing and withdrawing user WSN information for decentralized access control. FairAccess appends an individual storage layer for storage, where information is saved in off-chain decentralized storage systems.

Doku and Rawat [117] proposed Pledge, which uses a node's network operational Decentralized Hash Tables (DHT) for saving WSN information in the off-chain storage space. The information is accessible by the blockchain through access control policies, which are written in the blockchain. The dissimilarity between Pledge and FairAccess is a pair of key-values, where the user ID denotes the key, and the value indicates the encrypted information chunk [72].

Xu *et al.* [118] offered a blockchain-based storage system named Sapphire for the analytics of WSN with smart contracts. Information from WSN nodes is saved as attributes with objects that can be queried to examine application information. In terms of improvement, Sapphire offers up-to-date analytics on WSN information without a widespread WSN information transfer. For various WSN devices (light, regular and super), Sapphire has numerous roles that categorize devices using their restrictions and capacities.

Aslam and Javaid [119] proposed the Ethereum blockchain for safely transmitting WSN information saved in Oraclize, recollecting that WSN information from Oraclize through Ethereum blockchain broker accounts requires extra transaction costs. Powered by blockchain, CSIRO Australia Researchers offered an information credibility service [52] that confirms the WSN information integrity. Table 7 shows the blockchain-based WSN Solutions for Data Management.

TABLE 7. Blockchain-Based WSN solutions for data management.

Method	Integrity	Heterogeneity	Storage	Architecture
Blockchain-based secure electronic Medical record framework [114]	✓	×	On-chain/Local	Decentralized
Blockchain-based drone data management framework [112]	✓	✓	On-chain/Cloud	Partially Decentralized
Sharing and auditable data storage framework based on blockchain [72]	✓	✓	Cloud	Decentralized
Lightweight, scalable blockchain for WSN [42]	✓	✓	Off-chain/Cloud	Decentralized
WSN data privacy through blockchain [115]	✓	✓	Off-chain	Decentralized

The startup Datum provides a NoSQL database-based platform trained by a blockchain ledger, which supports the high-performance information management of the WSN. Datum uses the BigchainDB and disseminated storage platforms, IPFS and Ethereum smart contracts for programmable logic. The platform aims to send protected and unknown storage of prearranged information from social networks and a WSN device, for example, wearables and smart homes [120], to the storage platforms. For decentralized blockchain-based methods, this study offers solutions that contain high throughput record maintenance in a private blockchain and insights into how blockchain can be applied to check information integrity and transparency in applications that require auditable records.

VI. BLOCKCHAIN FOR WSN SECURITY MANAGEMENT

This section examines the security risks faced by the centralized WSN structure and how this study leverages the security advantages of a blockchain-based WSN to decentralize the WSN.

A. SECURITY PROBLEMS OF CENTRALIZED WSN MODELS

The security challenges of the WSN arise from its continuously expanding edge [121]. In a WSN, devices at the edge are possible breakdown points where attacks like Distributed Denial-of-Service (DDoS) could be established [122], [123]. At the WSN edge, infected nodes could collaborate to crash the WSN service provision, as observed in the botnet attack in August 2016 [124]. In the latest attack, the Mirai botnet developed and raised the most potent attack in opposition to WSN security by compromising the WSN nodes and creating malicious traffic in the order of Tbps [124]. Subsequently, after the Mirai botnet source code was openly released, an abundance of attacks followed, the most notable is October 2016 attack, which brought down numerous standard websites for many hours.

Another threat to the service availability of WSN arises from its centralized configuration [125]. A central point of failure is a risk to accessibility and authorization, and confidentiality [126]. A centralized WSN does not offer built-in measures to ensure that the provider will not abuse or tamper with users' WSN information. In a data-driven economy, WSN privacy must be ensured [127]. WSNs must confront these privacy attacks that arise from the spoofing of identity, the examination of traffic and routing data, and attacks on reliability assurance, such as the Byzantine routing data attack and modification attacks [128].

Information reliability in a centralized WSN configuration is challenging in applications where decisions are based on the received information due to possible injection attacks, resulting in information modification, downtime, and information stealing. Guaranteeing safety is vital in applications where anticipated information automatically initiates processes involving financial transactions. In WSNs, new safety solutions employ third-party security services. Using blockchain for safety policy enforcement and keeping the WSN interactions in an openly auditable report, exclusive of a third party, has proven extremely beneficial for the WSN.

B. BLOCKCHAIN OFFERS SECURITY FOR WSN

With the merits of the decentralized infrastructure, fault-tolerance, auditability, and in-built security in opposition to DDoS attacks, blockchain has demonstrated safety benefits in networks like Bitcoin. In public blockchains, the consensus protocols are utilized and hinder malicious nodes from launching a DoS attack; creating numerous void transactions can incur huge transaction fees [129]. A WSN solution based on blockchain beats fake verification since all node-published transactions have addresses of the blockchains. Therefore, blockchain can disrupt the WSN safety mechanism and gives enhanced security solutions to the WSN stack.

1) Offering Access Control through Blockchain

Current research has observed numerous proposed solutions to enforce Access Control policies in WSN without depending on the third party's service. Blockchain can enhance the security infrastructure of available WSN; a solution like in [88] gives a protected public-key infrastructure that is more fault-tolerant than the centralized solution.

Ding *et al.* [130] offered a framework of multi-layer blockchain, where information records and access controls are executed in individual layers. In this framework, the three layers include i) a decentralized blockchain-based information storage system where a user with a particular blockchain can input their WSN information; ii) a stream of messaging that allows negotiation among two parties; and iii) an access control mechanism for contributors with varying roles. In the blockchain, the information saved is encrypted, and only the contributors with access benefits can decrypt it.

Another study proposed a related model for access control [122], where a WSN user can be allowed to access or be blocked from protected WSN chunks of information using operations written in smart contracts. Feng *et al.* [123] utilized a blockchain to establish an access control mechanism for massive information. The authors utilized programmable smart contracts to inform authorization decisions for user demands on enormous information. As another solution [130], the author utilized a local blockchain linked to an open overlay blockchain, in which user privilege decisions are saved inside the blockchain, making them openly provable. Therefore, it is effortless to discover illegal user attempts.

Naz *et al.* [131] outlined a scheme that controls access by dropping any transaction that emerges from an unauthorized user or eliminating the attacker from the blockchain network altogether. The authors offer a comprehensive policy for blockchain contribution to preventing the Sybil attack [132]. Al Breiki *et al.* [133] offered an access control resolution based on blockchain for information saved in off-chain DHT. The blockchain stores privilege for various users for the saved information in DHT.

2) Maintaining Information Reliability through Blockchain

To establish a modification attack in a WSN structure enabled by blockchain, an attacker would try to change the blockchain records or make a fake block in the blockchain. This task is nearly impractical in blockchain open implementations, where the authoritative record of the blockchain is maintained using distributed consensus. It creates a situation for decentralizing the WSN access to the blockchain, while inherent properties avoid attacks and compromise information reliability [52].

Kandah *et al.* [136] utilized a multi-layer blockchain framework to save pieces of WSN information in the cloud. Fernández-Caramés and Fraga-Lamas [134] presented a smart city solution [135] based on blockchain, where the blockchain's in-built immutability characteristics ensure the reliability of the saved information. The blockchain in this solution utilizes hash [137] to record immutable saved information pieces in the cloud. A similar study [131] utilized the blockchain to put in IPFS file hashes that include WSN information.

Yang *et al.* [138] proposed a mechanism for credibility assessment on blockchain-based Internet of Vehicles. In [139], embedded WSN nodes obtain protected firmware through a network of blockchain. The proposed system utilizes peer-to-peer technology for sending updates of the firmware and assures the reliability of the firmware set up in the embedded nodes. Steger *et al.* [140] provided evidence for the idea of a protected distribution of software updates on the internet of vehicles, accessing the layered architecture of blockchain for scalability. Correspondingly, Gai *et al.* [141] utilized the blockchain to put software updates in a transaction so that WSN nodes can obtain updates in a secure, peer-to-peer style.

3) Guaranteeing Privacy through Blockchain

Blockchain has an inherent allowance for private or public key pairs. Accordingly, blockchain-based applications have confidentiality and authorization features, as the private key issuers sign all transactions. Kim *et al.* [88] leveraged a Public Key Infrastructure (PKI) based on blockchain for WSN nodes control. The authors utilized a smart contract that issued instructions to the WSN nodes for accessing their blockchain addresses.

Alotaibi *et al.* [142] offered a privacy solution for smart power grid transactions. The goal is not merely to maintain the distributed data among two confidential parties but also to conceal the power manufacturer's identity [143]. The author recommends creating and changing blockchain addresses for the power manufacturers to conceal the manufacturer's identity in totality.

Lee *et al.* [144] utilized a blockchain, Ethereum, to preserve privacy among gateways of WSN. The WSN gateways are configured to control Bluetooth Low Energy (BLE) devices like smart factories and wearable devices. The gateway keeps virtual nodes' data and all communications with the WSN in secret signatures. A multi-layer solution similar to [130] maintains access control policies inside the header of the blockchain. However, each user with user privilege obtains encrypted pieces of information from the off-chain information storage method.

Reference [131] provides a related multilayer resolution that utilizes IPFS as the off-chain storage method. Each time an information petitioner is permitted access to WSN information saved in IPFS files, the authors provide the keys to use the files. The keys encrypt the petitioners' public key access that only the petitioner can decrypt; therefore, privacy is ensured by accessing blockchain-based PKI.

4) Developing WSN Availability through blockchain

In the WSN, the proposed blockchain-based solutions for security enhance availability by the properties of decentralization inbuilt in Blockchain. An off-chain storage solution enhances the availability of communications records [145], but the saved information availability is dependent on the off-chain storage methods utilized. At this point, several distinctive proposed solutions that contribute to WSN availability are examined.

Hammi *et al.* [146] proposed a mechanism for authorization based on blockchain for the WSN using a higher degree of aliveness because of the in-built characteristics of blockchains, coupled with the OSCAR (Object Security Architecture) [130] form for security. Kandah *et al.* [136] proposed a multi-tiered blockchain resolution to manage safety problems with resource-constrained WSN nodes.

Naz *et al.* [131] utilized a blockchain method with a multi-tiered framework in addition to a smart contract to provide access control functions. For the storage of WSN information, the authors employed off-chain storage, namely IPFS. In supply chain and logistics use cases, blockchain can give protected logistics data to clients [147].

Table 8 shows the general areas of WSN security through blockchain, including access control, information reliability, availability, privacy, and protected software update dissemination.

VII. COMPARISONS WITH PREVIOUS PUBLISHED WORKS

This paper introduces a review of blockchain technology and its integration with conventional WSNs, or blockchain-based wireless sensor networks (BWSNs). This work provides a review of malicious node detection processes and implementation of WSNs and demonstration of node data, including its verification and detection. Furthermore, this survey discusses specific applications, particularly in access control, and outlines the limitations of BWSNs.

There are several published papers on the use of blockchain in WSNs. For instance, Buldin *et al.* [149] presented a study on the trends of blockchain-based WSNs for industrial applications, which allow the transmission and recording of information obtainable with the blockchain model, guaranteeing immutability of the information and utilization of smart contracts.

For data provenance, Zeng *et al.* [150] proposed an energy-efficient and secure data provenance scheme based on blockchain. Data provenance is required to ensure that data originating from a node has not been compromised along the path through which it travels. Still, conventional data provenance schemes involve many encodings and sometimes compression, which can be heavy on an already constrained network. In [150], source information is distributed across devices according to the packet path, and the proof can be recalled through the BS query execution. A supervisory network based on edge devices, comprised of high-performance devices, is organized near the Wireless Sensor Network, maintaining the WSN's provenance information in a blockchain-based database. The authenticity and security of the provenances are then secured.

Wang *et al.* [151] focused on blockchain-based information collection and visualization in WSNs. Their study

TABLE 8. WSN security methods based on blockchain.

General Areas of WSN Security through Blockchain	Solution	Essential Features
	Kim et al. [88]	PKI based on blockchain
	Ding et al. [130]	Split blockchain for access control and storage of data
	Riabi et al. [122]	Access control using functions of smart contract
Access Control	Feng et al. [123]	overlay blockchain used for access control in big data
	Ding et al. [130]	Policies for access control are written in the header of the block
	Naz et al. [131]	Policies for access control written in smart contracts for files of IPFS
	AlBreiki et al. [133]	DHT for stored data, smart contracts used for access control
	Fernández-Caramés and Fraga-Lamas[134]	Blockchain records with tamper evidence
	Kandah et al. [136]	Multi-layered blockchain framework for keeping a record of pieces of WSN information
	Naz et al. [131]	In blockchain transactions, keys sharing for addressing IPFS content
Data Integrity	Liu et al. [52]	Blockchain-based querying for proving the credibility of cloud-based information
	Yang et al. [138]	Blockchain-based reputation scheme on for the reliability of arriving messages
	Yohan et al. [139]	safe firmware updates for embedded WSN nodes in a blockchain network
	Steger et al. [140]	Software updates for smart cars based on overlay blockchain
	Gai et al. [141][148]	Software updates security and storage in blockchains for IoT devices
Confidentiality	Kim et al. [88]	PKI based on blockchain
	Alotaibi et al. [142]	Distribution System Operators (DSOs) are used to maintain addressing of blockchain
	Lee et al. [144]	Gateways for permitting communications between blockchain and linked BLE nodes
	Ding et al. [130]	Distributed encrypted information with contributors over a multi-tiered blockchain structure
	Naz et al. [131]	Distributed encrypted file hash of IPFS with contributors over a public blockchain
	Hammi et al. [146]	Blockchain-based fault tolerance for the authorization model
Availability	Kandah et al. [136]	Multi-tiered blockchain solution to manage safety problems with resource-limited WSN nodes
	Naz et al. [131]	Transactions for the IPFS file used over public Ethernet blockchain

combined WSN sensing with the blockchain technique, which handles all mobile databases as blocks. Each block will first discover its limit of sensor information and then concatenate it for other blocks and its individual measurement information. In this scheme, each block device saves the sensor information of the whole WSN. The information uploaded by these sensor devices is then visualized and analyzed.

Marchang *et al.* [152] proposed a routing protocol based on a private communication blockchain framework for a real-time high data sensing scenario. The proposed routing protocol, termed Load Balancing Multi-Hop (LBMH), improves battery life by decreasing the overhead due to block updates. However, the authors note that due to the local storage and power of the sensor nodes, blockchain in WSNs may never turn into a reality. On the other hand, Lazrag *et al.* [153] suggested a routing protocol based on a blockchain framework and traffic load balancing technique that also reduces interference in WSNs and IoT. It is assumed that the network nodes sense several events, creating massive information that is, of necessity, held over many packets. They introduced a routing protocol that utilizes blockchain technology to provide a distributed memory among the network's nodes, showing the practicability of the scheme.

Kumar and Paris [154] presented a blockchain-based deterministic filtering scheme that seeks to sieve out fabricated or false data injected by an adversary at the intermediate nodes in terms of malicious node detection. While the proposed scheme decreases the storage and communication overhead due to security keys, as it obviates the need for key interchange among sensor devices, malicious attacks can be so overwhelming that they drain the network's energy as the nodes are not isolated. Furthermore, the scheme's success is contingent on the immunity of the intermediary forwarding nodes to attack.

None of the previous studies focused on blockchain integration in WSNs, which promoted this study. This paper outlines a broader picture of the position, including the possibilities and challenges of the blockchain technology in WSNs' data management and security viz. malicious node data detection. Table 9 summarizes a variety of existing works based on the integration of blockchain with WSNs. Overall, an exhaustive survey of the current works is presented with a discourse about the varied profits and challenges associated with blockchain execution in WSN.

VIII. LESSONS LEARNED

A deep understanding of the blockchain-based approach to malicious node detection arrives through this survey. Moreover, an exhaustive study of the integration of blockchain techniques with WSN, termed BWSN, provides This various insights into blockchain-based wireless sensor networks. The ideas examined here introduce a new perspective to view BWSN architecture for malicious nodes discovery. Also, this survey contributes to blockchain-based WSN solutions for

TABLE 9. Recent articles on blockchain-based WSN.

Motivations for Blockchain Integration with WSN	Recent Articles	Addressed in this Survey
To create next-generation networks	[149]	✓
For secure data provenance	[150], [155]	✓
For information collection and analysis	[151], [156]	✓
To improve the battery life of the sensor node	[152]	✓
For optimal and secure routing	[153]	✓
For en-route filtering of false data	[154]	✓
For malicious node detection	[1]–[3], [157]	✓

data management, drawing upon several lessons, including, but are not limited to, the following.

i. Blockchain in Networks and IoTs: Experimental evaluation of blockchain in wireless sensor networks is currently an issue for further research because the available experimental results appear one-sided and not generic. For such networks and systems utilizing IoTs, enhancing the working algorithms is a key requirement to achieve the desired privacy protection. In blockchain applications in vehicular networks, current branching techniques are restricted by many duplicate SCs embedded in blocks. It indicates that increasing the load on the network will lead to a rapid increase in the number of duplicate SCs per block. In addition to this, the duplicate SCs lodged in blocks often lead to wasted processing power and storage. It opens up new research on enhancing the storage and processing capabilities of the blockchain systems applied in vehicular networks. In terms of blockchain applications in IoTs, most algorithms presented in the existing literature do not achieve the desired level of performance, especially for the single management hub scenario. Toward this end, some authors have proposed improved system models to utilise cache memory at edge nodes efficiently. However, some of these schemes only ensure the privacy and protection of IoT data but fail to guarantee the privacy and protection of users [158]. It would be interesting to conduct cutting edge research in this domain to improve the privacy and protection of network users.

ii. Blockchain-Based Storage Requirements: In most of the existing schemes, each node stores a distinct encoded packet, such that the errors in the single node can be easily propagated to a large area. It disproves the validity of the assumption that the adversary cannot compromise more than half of the blockchain's resources in the blockchain. To this end, the trade-off between storage efficiency and the capacity of the packet would require further investigation. Further, less space is required in storage for most practical application scenarios of wireless sensor networks. The normal sensor nodes or the cluster heads do not require storage except for buffering, as the normal sensor nodes do not require much storage space for queuing. However, robust permanent storage for maintaining the blocks is a key requirement worthy of further investigation in blockchain technology. Regarding battery life expectancy, the amount of energy consumed is huge for the Gateway/Sink, cluster heads and potential cluster heads when blockchain technology is adopted. In wireless sensor nodes, energy consumption is derived when the sensor network is in the activation mode using only two active sensor nodes, yielding about 100 bytes per packet at a constant rate. Therefore, blockchain applications will exhaust the limited, constrained bandwidth and limited battery life, yet this requires further research. Last, in blockchain technology in Ethereum networks, gas is a special unit applied to determine how much work action or a series of actions a miner performs. It is derived from the number of computer instructions executed by the Ethereum transaction, and the instability in the gas does not appear to vary greatly [159]. However, an Ethereum platform trading or contract execution of every operation needs a certain amount of gas, and the cost of the gas is dependent on the computational resource's requirements. In this case, to pay the blockchain miner, the gas will be converted into the equivalent ether currency. Therefore, the energy consumption problem is still an open issue that needs to be investigated.

iii. Blockchain-Based Data Sharing: Blockchain has the potential of incurring huge computational overhead. Mining is performed on both DataChain and BehaviorChain. Also, some methods proposed in the literature lack the relevant incentive mechanisms to reward ethers or tokens whenever the new dataset is made available to encourage the participants to stay in line with the specified terms. In most cases, the strategies to prevent several attacks in overlay networks require a huge community of research and development. For example, data are stored on the database in healthcare systems, and latency overhead becomes a huge concern. In particular, fine-grained access control is usually not provided to a client for data sharing. In most cases, a patient's manual approval is requested each time data are accessed. It results in a huge overhead of operation and undesirable latency in data access for the requester. Healthcare providers are compelled to manually upload data on directory and blockchain networks, resulting in inefficient operations. The need to conduct further research in this domain becomes imperative.

iv. Blockchain-Based Key Parameters Analyses: The application of blockchain technology's decentralised storage feature helps distribute the workload to the network, thereby enhancing the formation of a chain structure chronologically. However, such systems still require robust research and development efforts to improve the distribution of the workload. Also, a smart contract is usually added to the blockchain in the form of a digitized code. The smart contract code starts automatically when the contract trigger criteria are reasonably satisfied. Again, the loss of information asymmetry, resulting from the time difference in the entire wireless sensor network, could be mitigated by authenticating the malicious sensor node and recording it in the blockchain network in time [158]. However, model security in most blockchain-based security systems still poses a major threat that necessitates further investigation. Moreover, applying a distributed chained data structure to trace sensor node information recorded in each block on the chain to be independent of the previous block is still an open issue. The previous information in the block usually affects the node information of the next block in direct proportion. Therefore, the complexity lies in attempting to tamper with the past sensor data. In this scenario, the local data recorded by the sensor node would require over a 50% change in the previous data, which can be very expensive in terms of computational complexity.

A. LIMITATIONS OF BWSN

Note that BWSN has the following limitations:

1) It involves massive energy expenditure as each transaction needs powerful hardware resources.
2) Scalability is a key limitation of BWSN. It is because authentication of transactions by most nodes takes some time for verification.
3) Another drawback of BWSN is the complexity of the blockchain and the need for a comprehensive node's network.
4) Privacy protection is another major challenge ahead of BWSN.

IX. CONCLUSION

This paper discussed recent trends in blockchain technology, focusing on recent studies on blockchain-based wireless sensor networks (BWSNs). The survey outlines the key features of blockchain technology as a distributed ledger with verified and unchanged transaction records. It achieves immutability through a distributed consensus mechanism. Voted consensus results will be stored in distributed blockchains. However, in BWSNs, some important protocols for malicious node detection generally adopt a once-time centralized routing procedure, making the original information irreversible, challenging the reproduction and verification of the execution and preventing complications. Furthermore, the paper discusses the benefits of smart contracts that enhance blockchain and the greater number of BWSN nodes for malicious node detection and localization. Finally, the paper provides key lessons on blockchain-based applications in networks and IoTs, data sharing, storage requirements, malicious node detection, and data security. In the future, Blockchain will be able to integrate with other popular networks such as the Internet of Things, Mobile Adhoc Network, Vehicle Adhoc Network, Cloud Computing and so on.

DATA AVAILABILITY

No data was used in this survey paper.

REFERENCES

[1] L. Min and G. Ranxin, "Malicious nodes detection algorithm based on triangle module fusion operator in wireless sensor networks," in *Proc. IEEE 4th Adv. Inf. Technol., Electron. Automat. Control Conf. (IAEAC)*, Dec. 2019, pp. 118–121, doi: 10.1109/IAEAC47372.2019.8997710.

[2] Y. Kimura, E. Nii, and Y. Takizawa, "Cooperative detection for falsification and isolation of malicious nodes through inter-node vote for wireless sensor networks in open environments," in *Proc. Global Inf. Infrastruct. Netw. Symp. (GIIS)*, Dec. 2019, pp. 1–3, doi: 10.1109/GIIS48668.2019.9044952.

[3] B. Jaint, V. Singh, L. K. Tanwar, S. Indu, and N. Pandey, "An efficient weighted trust method for malicious node detection in clustered wireless sensor networks," in *Proc. 2nd IEEE Int. Conf. Power Electron., Intell. Control Energy Syst. (ICPEICES)*, Oct. 2018, pp. 1183–1187, doi: 10.1109/ICPEICES.2018.8897307.

[4] I. A. A. E.-M. And and S. M. Darwish, "Towards designing a trusted routing scheme in wireless sensor networks: A new deep blockchain approach," *IEEE Access*, vol. 9, pp. 103822–103834, 2021.

[5] D. Sivaganesan, "A data-driven trust mechanism based on blockchain in IoT sensor networks for detection and mitigation of attacks," *J. Trends Comput. Sci. Smart Technol.*, vol. 3, no. 1, pp. 59–69, May 2021.

[6] K. Shah and D. Jinwala, "Privacy preserving secure expansive aggregation with malicious node identification in linear wireless sensor networks," *Frontiers Comput. Sci.*, vol. 15, no. 6, pp. 1–9, Dec. 2021.

[7] A. J. Manuel, G. G. Deverajan, R. Patan, and A. H. Gandomi, "Optimization of routing-based clustering approaches in wireless sensor network: Review and open research issues," *Electronics*, vol. 9, no. 10, p. 1630, Oct. 2020, doi: 10.3390/electronics9101630.

[8] J. Ellul and G. J. Pace, "AlkylVM: A virtual machine for smart contract blockchain connected Internet of Things," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Feb. 2018, pp. 1–4, doi: 10.1109/NTMS.2018.8328732.

[9] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, "EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4719–4732, Jun. 2019, doi: 10.1109/JIOT.2018.2878154.

[10] M. N. Islam and S. Kundu, "Poster abstract: Preserving IoT privacy in sharing economy via smart contract," in *Proc. IEEE/ACM 3rd Int. Conf. Internet-Things Design Implement. (IoTDI)*, Apr. 2018, pp. 296–297, doi: 10.1109/IoTDI.2018.00047.

[11] E. S. Kang, S. J. Pee, J. G. Song, and J. W. Jang, "A blockchain-based energy trading platform for smart homes in a microgrid," in *Proc. 3rd Int. Conf. Comput. Commun. Syst. (ICCCS)*, Apr. 2018, pp. 472–476, doi: 10.1109/CCOMS.2018.8463317.

[12] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1594–1605, Apr. 2019, doi: 10.1109/JIOT.2018.2847705.

[13] J. del Rio, D. M. Toma, E. Martinez, T. C. O'Reilly, E. Delory, J. S. Pearlman, C. Waldmann, and S. Jirka, "A sensor web architecture for integrating smart oceanographic sensors into the semantic sensor web," *IEEE J. Ocean. Eng.*, vol. 43, no. 4, pp. 830–842, Oct. 2018, doi: 10.1109/JOE.2017.2768178.

[14] W. Lu, Y. Gong, X. Liu, J. Wu, and H. Peng, "Collaborative energy and information transfer in green wireless sensor networks for smart cities," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1585–1593, Apr. 2018, doi: 10.1109/TII.2017.2777846.

[15] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017, doi: 10.1109/JIOT.2017.2740569.

[16] S. E. Khediri, A. Thaljaoui, A. Dallali, and A. Kachouri, "Clustering algorithm in wireless sensor networks based on shortest path," in *Proc. 30th Int. Conf. Microelectron. (ICM)*, Dec. 2018, pp. 335–338, doi: 10.1109/ICM.2018.8704059.

[17] K. Dhote and G. M. Asutkar, "Optimization of routing techniques in wireless sensor network using queue management," in *Proc. Devices Integr. Circuit (DevIC)*, Mar. 2017, pp. 500–504, doi: 10.1109/DEVIC.2017.8074000.

[18] P. Verma, S. Shaw, K. Mohanty, P. Richa, R. Sah, and A. Mukherjee, "A survey on hierarchical based routing protocols for wireless sensor network," in *Proc. Int. Conf. Commun., Comput. Internet Things (ICIoT)*, Feb. 2018, pp. 338–341, doi: 10.1109/IC3IoT.2018.8668160.

[19] C. Xu, Z. Xiong, G. Zhao, and S. Yu, "An energy-efficient region source routing protocol for lifetime maximization in WSN," *IEEE Access*, vol. 7, pp. 135277–135289, 2019, doi: 10.1109/ACCESS.2019.2942321.

[20] N. Ahmad, A. Hussain, I. Ullah, and B. H. Zaidi, "IoT based wireless sensor network for precision agriculture," in *Proc. 7th Int. Electr. Eng. Congr. (iEECON)*, Mar. 2019, pp. 1–4, doi: 10.1109/iEECON45304.2019.8938854.

[21] Y. Wu, J. C. Chen, L. P. Qian, J. W. Huang, and X. M. S. Shen, "Energy-aware cooperative traffic offloading via device-to-device cooperations: An analytical approach," *IEEE Trans. Mobile Comput.*, vol. 16, no. 1, pp. 97–114, Jan. 2017, doi: 10.1109/TMC.2016.2539950.

[22] L. Wang, F. Hu, Z. Ling, and B. Wang, "Wireless information and power transfer to maximize information throughput in WBAN," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1663–1670, Oct. 2017, doi: 10.1109/JIOT.2017.2734682.

[23] H. Yetgin, K. T. K. Cheung, M. El-Hajjar, and L. H. Hanzo, "A survey of network lifetime maximization techniques in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 828–854, 2nd Quart., 2017, doi: 10.1109/COMST.2017.2650979.

[24] T. Qiu, K. Zheng, M. Han, C. L. P. Chen, and M. Xu, "A data-emergency-aware scheduling scheme for Internet of Things in smart cities," *IEEE Trans. Ind. Informat.*, vol. 14, no. 5, pp. 2042–2051, May 2018, doi: 10.1109/TII.2017.2763971.

[25] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Blockchain leveraged task migration in body area sensor networks," in *Proc. 25th Asia–Pacific Conf. Commun. (APCC)*, Nov. 2019, pp. 177–184, doi: 10.1109/APCC47188.2019.9026409.

[26] A. L. Imoize, T. Oyedare, M. E. Otuokere, and S. Shetty, "Software intrusion detection evaluation system: A cost-based evaluation of intrusion detection capability," *Commun. Netw.*, vol. 10, no. 4, pp. 211–229, 2018, doi: 10.4236/cn.2018.104017.

[27] Z. Yan, A. Mukherjee, L. Yang, S. Routray, and G. Palai, "Energy-efficient node positioning in optical wireless sensor networks," *Optik*, vol. 178, pp. 461–466, Feb. 2019.

[28] Z. Yan, P. Goswami, A. Mukherjee, L. Yang, S. Routray, and G. Palai, "Low-energy PSO-based node positioning in optical wireless sensor networks," *Optik*, vol. 181, pp. 378–382, Mar. 2019.

[29] T. Liu, X. Wang, and L. Zheng, "A cooperative SWIPT scheme for wirelessly powered sensor networks," *IEEE Trans. Commun.*, vol. 65, no. 6, pp. 2740–2752, Jun. 2017, doi: 10.1109/TCOMM.2017.2685580.

[30] F. Gandino, R. Ferrero, and M. Rebaudengo, "A key distribution scheme for mobile wireless sensor networks: *q*-*s*-composite," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 34–47, Jan. 2017, doi: 10.1109/TIFS.2016.2601061.

[31] S. A. Imam, M. K. Singh, V. K. Sachan, A. Choudhary, and A. M. Zaidi, "An energy-efficient data transmission scheme based on DSC-MIMO for wireless sensor network," in *Proc. 2nd IEEE Int. Conf. Integr. Circuits Microsyst. (ICICM)*, Nov. 2017, pp. 309–312, doi: 10.1109/ICAM.2017.8242191.

[32] J. O. Ogbebor, A. L. Imoize, and A. A.-A. Atayero, "Energy efficient design techniques in next-generation wireless communication networks: Emerging trends and future directions," *Wireless Commun. Mobile Comput.*, vol. 2020, Mar. 2020, Art. no. 7235362, doi: 10.1155/2020/7235362.

[33] O. Alamu, A. Gbenga-Ilori, M. Adelabu, A. Imoize, and O. Ladipo, "Energy efficiency techniques in ultra-dense wireless heterogeneous networks: An overview and outlook," *Eng. Sci. Technol., Int. J.*, vol. 23, no. 6, pp. 1308–1326, Dec. 2020, doi: 10.1016/j.jestch.2020.05.001.

[34] E. Choudhari, K. D. Bodhe, and S. M. Mundada, "Secure data aggregation in WSN using iterative filtering algorithm," in *Proc. Int. Conf. Innov. Mech. Ind. Appl. (ICIMIA)*, Feb. 2017, pp. 1–5, doi: 10.1109/ICIMIA.2017.7975603.

[35] X. Liu, M. Jia, X. Zhang, and W. Lu, "A novel multichannel Internet of Things based on dynamic spectrum sharing in 5G communication," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 5962–5970, Aug. 2019, doi: 10.1109/JIOT.2018.2847731.

[36] J. C. Kwan and A. O. Fapojuwo, "Radio frequency energy harvesting and data rate optimization in wireless information and power transfer sensor networks," *IEEE Sensors J.*, vol. 17, no. 15, pp. 4862–4874, Aug. 2017, doi: 10.1109/JSEN.2017.2714130.

[37] K. Fan, Y. Ren, Z. Yan, S. Wang, H. Li, and Y. Yang, "Secure time synchronization scheme in IoT based on blockchain," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1063–1068, doi: 10.1109/Cybermatics_2018.2018.00196.

[38] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.

[39] M. Conoscenti, A. Vetro, and J. C. De Martin, "Peer to peer for privacy and decentralization in the Internet of Things," in *Proc. IEEE/ACM 39th Int. Conf. Softw. Eng. Companion (ICSE-C)*, May 2017, pp. 288–290, doi: 10.1109/ICSE-C.2017.60.

[40] R. Abe, H. Watanabe, S. Ohashi, S. Fujimura, and A. Nakadaira, "Storage protocol for securing blockchain transparency," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2018, pp. 577–581, doi: 10.1109/COMPSAC.2018.10298.

[41] K. Leo Brousmiche, A. Durand, T. Heno, C. Poulain, A. Dalmieres, and E. B. Hamida, "Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchain," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1281–1286, doi: 10.1109/Cybermatics_2018.2018.00223.

[42] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623, doi: 10.1109/PERCOMW.2017.7917634.

[43] G. B. Mermer, E. Zeydan, and S. S. Arslan, "An overview of blockchain technologies: Principles, opportunities and challenges," in *Proc. 26th Signal Process. Commun. Appl. Conf. (SIU)*, May 2018, pp. 1–4, doi: 10.1109/SIU.2018.8404513.

[44] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2017, pp. 2567–2572, doi: 10.1109/SMC.2017.8123011.

[45] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019, doi: 10.1109/ACCESS.2019.2903554.

[46] S. S. Hazari and Q. H. Mahmoud, "A parallel proof of work to improve transaction speed and scalability in blockchain systems," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2019, pp. 916–921, doi: 10.1109/CCWC.2019.8666535.

[47] W. Yiying and Z. Yeze, "Cryptocurrency price analysis with artificial intelligence," in *Proc. 5th Int. Conf. Inf. Manage. (ICIM)*, Mar. 2019, pp. 97–101, doi: 10.1109/INFOMAN.2019.8714700.

[48] N. Fotiou, I. Pittaras, V. A. Siris, S. Voulgaris, and G. C. Polyzos, "Secure IoT access at scale using blockchains and smart contracts," in *Proc. IEEE 20th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2019, pp. 1–6, doi: 10.1109/WoWMoM.2019.8793047.

[49] K. Shehzad, M. Afrasayab, M. Khan, M. A. Mushtaq, R. L. Ahmed, and M. M. Saleemi, "Use of blockchain in Internet of Things: A systematic literature review," in *Proc. Cybersecur. Cyberforensics Conf. (CCC)*, May 2019, pp. 165–171, doi: 10.1109/CCC.2019.00012.

[50] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018, doi: 10.1109/JIOT.2018.2812239.

[51] G. C. Polyzos and N. Fotiou, "Blockchain-assisted information distribution for the Internet of Things," in *Proc. IEEE Int. Conf. Inf. Reuse Integr. (IRI)*, Aug. 2017, pp. 75–78, doi: 10.1109/IRI.2017.83.

[52] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jun. 2017, pp. 468–475, doi: 10.1109/ICWS.2017.54.

[53] O. J. A. Pinno, A. R. A. Gregio, and L. C. E. De Bona, "ControlChain: Blockchain as a central enabler for access control authorizations in the IoT," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6, doi: 10.1109/GLOCOM.2017.8254521.

[54] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey, "Towards better availability and accountability for IoT updates by means of a blockchain," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Apr. 2017, pp. 50–58, doi: 10.1109/EuroSPW.2017.50.

[55] S. Mishra and A. K. Tyagi, "Intrusion detection in Internet of Things (IoTs) based applications using blockchain technolgy," in *Proc. 3rd Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)*, Dec. 2019, pp. 123–128, doi: 10.1109/I-SMAC47947.2019.9032557.

[56] A. Ekİn and D. Ünay, "Blockchain applications in healthcare," in *Proc. 26th Signal Process. Commun. Appl. Conf. (SIU)*, May 2018, pp. 1–4, doi: 10.1109/SIU.2018.8404275.

[57] A. Bhawiyuga, A. Wardhana, K. Amron, and A. P. Kirana, "Platform for integrating Internet of Things based smart healthcare system and blockchain network," in *Proc. 6th NAFOSTED Conf. Inf. Comput. Sci. (NICS)*, Dec. 2019, pp. 55–60, doi: 10.1109/NICS48868.2019.9023797.

[58] P. G. Lopez, A. Montresor, and A. Datta, "Please, do not decentralize the internet with (permissionless) blockchains!" in *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2019, pp. 1901–1911, doi: 10.1109/ICDCS.2019.00188.

[59] P. Rimba, A. B. Tran, I. Weber, M. Staples, A. Ponomarev, and X. Xu, "Comparing blockchain and cloud services for business process execution," in *Proc. IEEE Int. Conf. Softw. Archit. (ICSA)*, Apr. 2017, pp. 257–260, doi: 10.1109/ICSA.2017.44.

[60] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "OmniLedger: A secure, scale-out, decentralized ledger via sharding," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 583–598, doi: 10.1109/SP.2018.000-5.

[61] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, and A. Seneviratne, "A delay-tolerant payment scheme based on the Ethereum blockchain," *IEEE Access*, vol. 7, pp. 33159–33172, 2019, doi: 10.1109/ACCESS.2019.2903271.

[62] H. Lu, K. Huang, and M. Azimi, "Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks," *IEEE Access*, vol. 7, pp. 41426–41444, 2019, doi: 10.1109/ACCESS.2019.2907695.

[63] D.-M. Nguyen, Q.-H. Luu, N. Huynh-Tuong, and H.-A. Pham, "MB-PBA: Leveraging Merkle tree and blockchain to enhance user profile-based authentication in E-learning systems," in *Proc. 19th Int. Symp. Commun. Inf. Technol. (ISCIT)*, Sep. 2019, pp. 392–397, doi: 10.1109/ISCIT.2019.8905114.

[64] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, May 2017, pp. 468–477, doi: 10.1109/CCGRID.2017.8.

[65] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *Proc. 41st Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2018, pp. 1545–1550, doi: 10.23919/MIPRO.2018.8400278.

[66] W. Liu, S. S. Zhu, T. Mundie, and U. Krieger, "Advanced blockchain architecture for e-health systems," in *Proc. IEEE 19th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Oct. 2017, pp. 1–6, doi: 10.1109/HealthCom.2017.8210847.

[67] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 98–103, doi: 10.1109/TrustCom/BigDataSE.2018.00025.

[68] X. Liu, H. Huang, F. Xiao, and Z. Ma, "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4101–4112, May 2020, doi: 10.1109/JIOT.2019.2957421.

[69] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 5, pp. 840–852, Oct. 2018, doi: 10.1109/TDSC.2016.2616861.

[70] T. T. Huynh, T. D. Nguyen, and H. Tan, "A survey on security and privacy issues of blockchain technology," in *Proc. Int. Conf. Syst. Sci. Eng. (ICSSE)*, Jul. 2019, pp. 362–367, doi: 10.1109/ICSSE.2019.8823094.

[71] G. Kumar, R. Saha, M. Rai, R. Thomas, and T. H. Kim, "Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6835–6842, Aug. 2019, doi: 10.1109/JIOT.2019.2911969.

[72] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1 pp. 858–880, 1st Quart., 2019, doi: 10.1109/COMST.2018.2863956.

[73] X. Yang, Y. Chen, and X. Chen, "Effective scheme against 51% attack on proof-of-work blockchain with history weighted information," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 261–265, doi: 10.1109/Blockchain.2019.00041.

[74] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2018, doi: 10.1109/ACCESS.2019.2896108.

[75] S. Pachal and S. Ruj, "Rational mining of bitcoin," in *Proc. 11th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2019, pp. 1–8, doi: 10.1109/COMSNETS.2019.8711445.

[76] S. Xu, J. Yuan, Y. Li, X. Liu, and Y. Zhang, "Super payment channel for decentralized cryptocurrencies," in *Proc. IEEE Conf. Dependable Secure Comput. (DSC)*, Nov. 2019, pp. 1–8, doi: 10.1109/DSC47296.2019.8937619.

[77] L. Che, X. Liu, and Z. Li, "Fast screening of high-risk lines under false data injection attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4003–4014, Jul. 2019, doi: 10.1109/TSG.2018.2848256.

[78] X. Wang, X. Zha, G. Yu, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Attack and defence of Ethereum remote APIs," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6, doi: 10.1109/GLOCOMW.2018.8644498.

[79] S. Rouhani and R. Deters, "Performance analysis of Ethereum transactions in private blockchain," in *Proc. 8th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Nov. 2017, pp. 70–74, doi: 10.1109/ICSESS.2017.8342866.

[80] A. E. Yves-Christian, B. Hammi, A. Serhrouchni, and H. Labiod, "Total eclipse: How to completely isolate a bitcoin peer," in *Proc. 3rd Int. Conf. Secur. Smart Cities, Ind. Control Syst. Commun. (SSIC)*, Oct. 2018, pp. 1–7, doi: 10.1109/SSIC.2018.8556790.

[81] V. Chicarino, C. Albuquerque, E. Jesus, and A. Rocha, "On the detection of selfish mining and stalker attacks in blockchain networks," *Ann. Telecommun.*, vol. 75, nos. 3–4, pp. 143–152, Apr. 2020, doi: 10.1007/s12243-019-00746-2.

[82] Q. Wang, X. Li, and Y. Yu, "Anonymity for bitcoin from secure escrow address," *IEEE Access*, vol. 6, pp. 12336–12341, 2018, doi: 10.1109/ACCESS.2017.2787563.

[83] K. R. Ozyilmaz and A. Yurdakul, "Designing a blockchain-based IoT with Ethereum, swarm, and LoRa: The software solution to create high availability with minimal security risks," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 28–34, Mar. 2019, doi: 10.1109/MCE.2018.2880806.

[84] S. Henningsen, D. Teunis, M. Florian, and B. Scheuermann, "Eclipsing Ethereum peers with false friends," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Jun. 2019, pp. 300–309, doi: 10.1109/EuroSPW.2019.00040.

[85] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

[86] S. Ali, G. Wang, B. White, and R. L. Cottrell, "A blockchain-based decentralized data storage and access framework for PingER," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 1303–1308, doi: 10.1109/TrustCom/BigDataSE.2018.00179.

[87] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: Challenges and directions," *IEEE Secur. Privacy*, vol. 16, no. 4, pp. 38–45, Jul. 2018, doi: 10.1109/MSP.2018.3111245.

[88] T.-H. Kim, R. Goyat, M. K. Rai, G. Kumar, W. J. Buchanan, R. Saha, and R. Thomas, "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks," *IEEE Access*, vol. 7, pp. 184133–184144, 2019, doi: 10.1109/ACCESS.2019.2960609.

[89] U. Majeed, L. U. Khan, I. Yaqoob, S. A. Kazmi, K. Salah, and C. S. Hong, "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," *J. Netw. Comput. Appl.*, vol. 16, May 2021, Art. no. 103007.

[90] R. Wang, H. Liu, H. Wang, Q. Yang, and D. Wu, "Distributed security architecture based on blockchain for connected health: Architecture, challenges, and approaches," *IEEE Wireless Commun.*, vol. 26, no. 6, pp. 30–36, Dec. 2019, doi: 10.1109/MWC.001.1900108.

[91] S. Dhumwad, M. Sukhadeve, C. Naik, M. K. N., and S. Prabhu, "A peer to peer money transfer using SHA256 and Merkle tree," in *Proc. 23RD Annu. Int. Conf. Adv. Comput. Commun. (ADCOM)*, Sep. 2017, pp. 40–43, doi: 10.1109/ADCOM.2017.00013.

[92] A. A. Yusuf, D. K. Basuki, S. Sukaridhoto, Y. P. Pratama, F. B. Putra, and H. Yulianus, "ArmChain—A blockchain based sensor data communication for the vehicle as a mobile sensor network," in *Proc. Int. Electron. Symp. (IES)*, Sep. 2019, pp. 539–543, doi: 10.1109/ELECSYM.2019.8901530.

[93] L. Xu, R. Collier, and G. M. P. O'Hare, "A survey of clustering techniques in WSNs and consideration of the challenges of applying such to 5G IoT scenarios," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1229–1249, Oct. 2017, doi: 10.1109/JIOT.2017.2726014.

[94] H. Mayadunna, S. L. De Silva, I. Wedage, S. Pabasara, L. Rupasinghe, C. Liyanapathirana, K. Kesavan, C. Nawarathna, and K. K. Sampath, "Improving trusted routing by identifying malicious nodes in a MANET using reinforcement learning," in *Proc. 17th Int. Conf. Adv. ICT Emerg. Regions (ICTer)*, Sep. 2017, pp. 1–8, doi: 10.1109/ICTER.2017.8257821.

[95] Y. Zou and M. Lin, "FAST: A frequency-aware skewed Merkle tree for FPGA-secured embedded systems," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, Jul. 2019, pp. 326–331, doi: 10.1109/ISVLSI.2019.00066.

[96] Q. Li, "Research on E-commerce user information encryption technology based on Merkle hash tree," in *Proc. Int. Conf. Robots Intell. Syst. (ICRIS)*, Jun. 2019, pp. 365–369, doi: 10.1109/ICRIS.2019.00098.

[97] J. Kan and K. S. Kim, "MTFS: Merkle-tree-based file system," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 43–47, doi: 10.1109/BLOC.2019.8751389.

[98] B. Sharma, C. N. Sekharan, and F. Zuo, "Merkle-tree based approach for ensuring integrity of electronic medical records," in *Proc. 9th IEEE Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Nov. 2018, pp. 983–987, doi: 10.1109/UEMCON.2018.8796607.

[99] A. Auvolat and F. Taïani, "Merkle search trees: Efficient state-based CRDTs in open networks," in *Proc. 38th Symp. Reliable Distrib. Syst. (SRDS)*, Oct. 2019, pp. 221–22109, doi: 10.1109/SRDS47363.2019.00032.

[100] S. Ali, G. Wang, M. Z. A. Bhuiyan, and H. Jiang, "Secure data provenance in cloud-centric Internet of Things via blockchain smart contracts," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Oct. 2018, pp. 991–998, doi: 10.1109/SmartWorld.2018.00175.

[101] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. Leung, "Decentralized applications: The blockchain-empowered software system," *IEEE Access*, vol. 6, pp. 53019–53033, 2018, doi: 10.1109/ACCESS.2018.2870644.

[102] K. Kayiram, R. Surana, and R. Gururaj, "Energy efficient data management in wireless sensor networks," in *Proc. IEEE 1st Int. Conf. Energy, Syst. Inf. Process. (ICESIP)*, Jul. 2019, pp. 1–6, doi: 10.1109/ICESIP46348.2019.8938241.

[103] F. Aliyu, S. Umar, and H. Al-Duwaish, "A survey of applications of artificial neural networks in wireless sensor networks," in *Proc. 8th Int. Conf. Modeling Simulation Appl. Optim. (ICMSAO)*, Apr. 2019, pp. 1–5, doi: 10.1109/ICMSAO.2019.8880364.

[104] T. Fronimos, S. Lalis, M. Koutsoubelias, and T. Bartzanas, "Unified service-oriented access for WSNs and dynamically deployed application tasks," in *Proc. IEEE 1st Int. Conf. Internet-Things Design Implement. (IoTDI)*, Apr. 2016, pp. 247–252, doi: 10.1109/IoTDI.2015.25.

[105] W. V. Vargas, A. Munoz-Arcentales, and J. S. Rodríguez, "A distributed system model for managing data ingestion in a wireless sensor network," in *Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2017, pp. 1–5, doi: 10.1109/CCWC.2017.7868434.

[106] A. Karaki, A. Nasser, C. A. Jaoude, and H. Harb, "An adaptive sampling technique for massive data collection in distributed sensor networks," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 1255–1260, doi: 10.1109/IWCMC.2019.8766469.

[107] V. Singh and R. B. Lohani, "Mobility aware energy efficient clustering for wireless sensor network," in *Proc. IEEE Int. Conf. Electr., Comput. Commun. Technol. (ICECCT)*, Feb. 2019, pp. 1–6, doi: 10.1109/ICECCT.2019.8869231.

[108] Y. Qin and Q. Z. Sheng, "Big data analysis and IoT," in *Encyclopedia of Big Data Technologies*, S. Sakr and A. Zomaya, Eds. Cham, Switzerland: Springer, 2018, pp. 1–12.

[109] S. Xiao, T. Li, B. Guo, and Z. Huang, "Cloud platform wireless sensor network detection system based on data sharing," *Cluster Comput.*, vol. 22, no. S6, pp. 14157–14168, Nov. 2019, doi: 10.1007/s10586-018-2260-6.

[110] M. Hajeer and D. Dasgupta, "Handling big data using a data-aware HDFS and evolutionary clustering technique," *IEEE Trans. Big Data*, vol. 5, no. 2, pp. 134–147, Jun. 2019, doi: 10.1109/TBDATA.2017.2782785.

[111] M. Farsi, M. A. Elhosseini, M. Badawy, H. A. Ali, and H. Z. Eldin, "Deployment techniques in wireless sensor networks, coverage and connectivity: A survey," *IEEE Access*, vol. 7, pp. 28940–28954, 2019, doi: 10.1109/ACCESS.2019.2902072.

[112] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in IoT using blockchain," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2017, pp. 261–266, doi: 10.1109/MILCOM.2017.8170858.

[113] A. Anjum, M. Sporny, and A. Sill, "Blockchain standards for compliance and trust," *IEEE Cloud Comput.*, vol. 4, no. 4, pp. 84–90, Jul. 2017, doi: 10.1109/MCC.2017.3791019.

[114] M. T. de Oliveira, L. H. A. Reis, R. C. Carrano, F. L. Seixas, D. C. M. Saade, C. V. Albuquerque, N. C. Fernandes, S. D. Olabarriaga, D. S. V. Medeiros, and D. M. F. Mattos, "Towards a blockchain-based secure electronic medical record for healthcare applications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6, doi: 10.1109/ICC.2019.8761307.

[115] S. Ali, N. Javaid, D. Javeed, I. Ahmad, A. Ali, and U. M. Badamasi, "A blockchain-based secure data storage and trading model for wireless sensor networks," in *Advanced Information Networking and Applications*. Cham, Switzerland: Springer, 2020, pp. 499–511, doi: 10.1007/978-3-030-44041-1_45.

[116] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018, doi: 10.1109/ACCESS.2018.2864189.

[117] R. Doku and D. Rawat, "Pledge: A private ledger based decentralized data sharing framework," in *Proc. Spring Simulation Conf. (SpringSim)*, Apr. 2019, pp. 1–11, doi: 10.23919/SpringSim.2019.8732913.

[118] Q. Xu, K. Aung, Y. Zhu, and K. Yong, "A blockchain-based storage system for data analytics in the Internet of Things," in *New Advances in the Internet of Things* (Studies in Computational Intelligence). Berlin, Germany: Springer, 2018, pp. 119–138.

[119] F. Aslam and N. Javaid, "Blockchain-based secure data sharing platform for research data rights management over the Ethereum network," ResearchGate, Tech. Rep., Jul. 2019. Accessed: Aug. 14, 2021. [Online]. Available: https://www.researchgate.net/publication/334696593

[120] S. A. Imam, A. Choudhary, A. M. Zaidi, M. K. Singh, and V. K. Sachan, "Cooperative effort based wireless sensor network clustering algorithm for smart home application," in *Proc. 2nd IEEE Int. Conf. Integr. Circuits Microsyst. (ICICM)*, Nov. 2017, pp. 304–308, doi: 10.1109/ICAM.2017.8242190.

[121] M. K. Singh, S. I. Amin, S. A. Imam, V. K. Sachan, and A. Choudhary, "A survey of wireless sensor network and its types," in *Proc. Int. Conf. Adv. Comput., Commun. Control Netw. (ICACCCN)*, Oct. 2018, pp. 326–330, doi: 10.1109/ICACCCN.2018.8748710.

[122] I. Riabi, Y. Dhif, H. K. B. Ayed, and K. Zaatouri, "A blockchain based access control for IoT," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 2086–2091, doi: 10.1109/IWCMC.2019.8766506.

[123] L. Feng, H. Zhang, L. Lou, and Y. Chen, "A blockchain-based collocation storage architecture for data security process platform of WSN," in *Proc. IEEE 22nd Int. Conf. Comput. Supported Cooperat. Work Design ((CSCWD))*, May 2018, pp. 75–80, doi: 10.1109/CSCWD.2018.8465319.

[124] A. Wani and S. Revathi, "DDoS detection and alleviation in IoT using SDN (SDIoT-DDoS-DA)," *J. Inst. Eng. India, B*, vol. 101, no. 2, pp. 117–128, Apr. 2020, doi: 10.1007/s40031-020-00442-z.

[125] C. Ding and L. Shen, "Design and implementation of programmable nodes in software defined sensor networks," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–5, doi: 10.1109/VTCSpring.2017.8108545.

[126] A. Karakaya and S. Akleylek, "A survey on security threats and authentication approaches in wireless sensor networks," in *Proc. 6th Int. Symp. Digit. Forensic Secur. (ISDFS)*, Mar. 2018, pp. 1–4, doi: 10.1109/ISDFS.2018.8355381.

[127] K. Bhaskaran, P. Ilfrich, D. Liffman, C. Vecchiola, P. Jayachandran, A. Kumar, F. Lim, K. Nandakumar, Z. Qin, V. Ramakrishna, E. G. Teo, and C. H. Suen, ''Double-blind consent-driven data sharing on blockchain,'' in *Proc. IEEE Int. Conf. Cloud Eng. (ICE)*, Apr. 2018, pp. 385–391, doi: 10.1109/IC2E.2018.00073.

[128] A. A. Frohlich, R. M. Scheffel, D. Kozhaya, and P. E. Verissimo, ''Byzantine resilient protocol for the IoT,'' *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2506–2517, Apr. 2019, doi: 10.1109/JIOT.2018.2871157.

[129] L. Almon, M. Riecker, and M. Hollick, ''Lightweight detection of denial-of-service attacks on wireless sensor networks revisited,'' in *Proc. IEEE 42nd Conf. Local Comput. Netw. (LCN)*, Oct. 2017, pp. 444–452, doi: 10.1109/LCN.2017.110.

[130] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, ''A novel attribute-based access control scheme using blockchain for IoT,'' *IEEE Access*, vol. 7, pp. 38431–38441, 2019, doi: 10.1109/ACCESS.2019.2905846.

[131] M. Naz, F. A. Al-Zahrani, R. Khalid, N. Javaid, A. M. Qamar, M. K. Afzal, and M. Shafiq, ''A secure data sharing platform using blockchain and interplanetary file system,'' *Sustainability*, vol. 11, no. 24, p. 7054, Dec. 2019, doi: 10.3390/su11247054.

[132] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, ''Consortium blockchain for secure energy trading in industrial Internet of Things,'' *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018, doi: 10.1109/TII.2017.2786307.

[133] H. Al Breiki, L. Al Qassem, K. Salah, M. H. U. Rehman, and D. Sevtinovic, ''Decentralized access control for IoT data using blockchain and trusted oracles,'' in *Proc. IEEE Int. Conf. Ind. Internet (ICII)*, Nov. 2019, pp. 248–257, doi: 10.1109/ICII.2019.00051.

[134] T. M. Fernández-Caramés and P. Fraga-Lamas, ''A review on the use of blockchain for the Internet of Things,'' *IEEE Access*, vol. 6, pp. 32979–33001, 2018, doi: 10.1109/ACCESS.2018.2842685.

[135] S. Kushch and F. Prieto-Castrillo, ''Blockchain for dynamic nodes in a smart city,'' in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Apr. 2019, pp. 29–34, doi: 10.1109/WF-IoT.2019.8767336.

[136] F. Kandah, B. Huber, A. Altarawneh, S. Medury, and A. Skjellum, ''BLAST: Blockchain-based trust management in smart cities and connected vehicles setup,'' in *Proc. IEEE High Perform. Extreme Comput. Conf. (HPEC)*, Sep. 2019, pp. 1–7, doi: 10.1109/HPEC.2019.8916229.

[137] C.-N. Yang, T.-J. Lin, S.-Y. Wu, S.-S. Lin, and W. Bi, ''Cost effective hash chain based key pre-distribution scheme for wireless sensor network,'' in *Proc. IEEE 18th Int. Conf. Commun. Technol. (ICCT)*, Oct. 2018, pp. 518–522, doi: 10.1109/ICCT.2018.8600178.

[138] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, ''A blockchain-based reputation system for data credibility assessment in vehicular networks,'' in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–5, doi: 10.1109/PIMRC.2017.8292724.

[139] A. Yohan and N.-W. Lo, ''FOTB: A secure blockchain-based firmware update framework for IoT environment,'' *Int. J. Inf. Secur.*, vol. 19, no. 3, pp. 257–278, Jun. 2020, doi: 10.1007/s10207-019-00467-6.

[140] M. Steger, A. Dorri, S. S. Kanhere, K. Römer, R. Jurdak, and M. Karner, ''Secure wireless automotive software updates using blockchains: A proof of concept,'' in *Advanced Microsystems for Automotive Applications*. Cham, Switzerland: Springer, 2018, pp. 137–149, doi: 10.1007/978-3-319-66972-4_12.

[141] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, ''Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks,'' *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019, doi: 10.1109/JIOT.2019.2904303.

[142] B. Alotaibi, ''Utilizing blockchain to overcome cyber security concerns in the Internet of Things: A review,'' *IEEE Sensors J.*, vol. 19, no. 23, pp. 10953–10971, Dec. 2019, doi: 10.1109/JSEN.2019.2935035.

[143] O. Samuel, N. Javaid, M. Awais, Z. Ahmed, M. Imran, and M. Guizani, ''A blockchain model for fair data sharing in deregulated smart grids,'' in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–7, doi: 10.1109/GLOBECOM38437.2019.9013372.

[144] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, ''A blockchain-based smart home gateway architecture for preventing data forgery,'' *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, p. 9, Mar. 2020, doi: 10.1186/s13673-020-0214-5.

[145] N. Zhou, M. Wu, and J. Zhou, ''Volunteer service time record system based on blockchain technology,'' in *Proc. IEEE 2nd Adv. Inf. Technol., Electron. Autom. Control Conf. (IAEAC)*, Mar. 2017, pp. 610–613, doi: 10.1109/IAEAC.2017.8054088.

[146] M. T. Hammi, P. Bellot, and A. Serhrouchni, ''BCTrust: A decentralized authentication blockchain-based mechanism,'' in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6, doi: 10.1109/WCNC.2018.8376948.

[147] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, ''Performance optimization for blockchain-enabled industrial Internet of Things (IIoT) systems: A deep reinforcement learning approach,'' *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3559–3570, Jun. 2019, doi: 10.1109/TII.2019.2897805.

[148] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, ''Addressing security and privacy issues of IoT using blockchain technology,'' *IEEE Internet Things J.*, vol. 8, no. 2, pp. 881–888, Jan. 2021, doi: 10.1109/JIOT.2020.3008906.

[149] I. D. Buldin, M. G. Gorodnichev, S. S. Makhrov, and E. N. Denisova, ''Next generation industrial blockchain-based wireless sensor networks,'' in *Proc. Wave Electron. Appl. Inf. Telecommun. Syst. (WECONF)*, Nov. 2018, pp. 1–5, doi: 10.1109/WECONF.2018.8604408.

[150] Y. Zeng, X. Zhang, R. Akhtar, and C. Wang, ''A blockchain-based scheme for secure data provenance in wireless sensor networks,'' in *Proc. 14th Int. Conf. Mobile Ad-Hoc Sensor Netw. (MSN)*, Dec. 2018, pp. 13–18, doi: 10.1109/MSN.2018.00009.

[151] S.-Y. Wang, Y.-J. Hsu, and S.-J. Hsiao, ''Integrating blockchain technology for data collection and analysis in wireless sensor networks with an innovative implementation,'' in *Proc. Int. Symp. Comput., Consum. Control (ISC)*, Dec. 2018, pp. 149–152, doi: 10.1109/IS3C.2018.00045.

[152] J. Marchang, G. Ibbotson, and P. Wheway, ''Will blockchain technology become a reality in sensor networks?'' in *Proc. Wireless Days (WD)*, Apr. 2019, pp. 1–4, doi: 10.1109/WD.2019.8734268.

[153] 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 *Proc. 15th Int. Conf. Signal-Image Technol. Internet-Based Syst. (SITIS)*, Nov. 2019, pp. 411–415, doi: 10.1109/SITIS.2019.00072.

[154] A. Kumar and A. R. Pais, ''Blockchain based en-route filtering of false data in wireless sensor networks,'' in *Proc. 11th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2019, pp. 1–6, doi: 10.1109/COMSNETS.2019.8711352.

[155] T. C. S. Priya and A. K. Durga, ''Clustering-based blockchain technique for securing wireless sensor networks,'' in *Data Engineering and Communication Technology*. Singapore: Springer, 2020, pp. 461–471.

[156] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, and J. Wang, ''Incentive mechanism of data storage based on blockchain for wireless sensor networks,'' *Mobile Inf. Syst.*, vol. 2018, Aug. 2018, Art. no. 6874158, doi: 10.1155/2018/6874158.

[157] 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.

[158] F. Tariq, M. Anwar, A. R. Janjua, M. H. Khan, A. U. Khan, and N. Javaid, ''Blockchain in WSNs, VANets, IoTs and healthcare: A survey,'' in *Web, Artificial Intelligence and Network Applications*, vol. 1150, L. Barolli, F. Amato, F. Moscato, T. Enokido, and M. Takizawa, Eds. Cham, Switzerland: Springer, 2020, pp. 267–279.

[159] 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.

LAKSHMANA KUMAR RAMASAMY (Member, IEEE) is currently pursuing the post-doctoral fellowship with Thu Dau Mot University, Vietnam. He is working as the Head of the Center of Excellence for Artificial Intelligence and Machine Learning at Hindusthan College of Engineering and Technology, Tamil Nadu, India. He is also working as the Offshore Director of Research and Development (AI) at a Canadian-Based company (ASIQC) in the Vancouver region of British Columbia, Canada. He represents the Technical Group Committee—National Cyber Defence Research Centre (NCDRC), Government of India. He holds the certification in data science from John Hopkins University, USA. He is certified as an Amazon Cloud Architect from Amazon Web Services. He is the Founding Member of IEEE SIG of Big Data for Cyber Security and Privacy, IEEE. He serves as a core member of the Editorial Advisory Board of Artificial Intelligence Group, Cambridge Scholars Publishing, U.K. He is also the ACM Distinguished Speaker and IEEE Brand Ambassador.

FIROZ KHAN K. P. was born in Kerala, India, in 1974. He received the B.Sc. degree in electronics from Bharathiar University, Coimbatore, India, in 1991, the master's degree in information technology from the University of Southern Queensland, Australia, in 2006, the second master's degree (Hons.) in information networks and computer security from New York Institute of Technology, Abu Dhabi, United Arab Emirates, in 2016, and the Ph.D. degree in computer science from The British University in Dubai, Dubai, United Arab Emirates, with a focus on researching ransomware detection. In 2001, he joined the Computer Information Science Department, Higher Colleges of Technology, as a Teaching Technician and became a Faculty Member, in 2005. He is currently holding a Lecturer position, with security and networking being his primary areas of teaching. His current research interests include computer security, machine learning, deep learning, and computer networking and blockchain.

AGBOTINAME LUCKY IMOIZE (Member, IEEE) received the B.E. degree (Hons.) in electrical and electronics engineering from Ambrose Alli University, Nigeria, in 2008, and completed the M.Sc. degree in electrical and electronics engineering and communication engineering in Lagos, Nigeria, in 2012. He is currently a Lecturer with the Department of Electrical and Electronics Engineering, University of Lagos, Nigeria. Before joining the University of Lagos, he was a Lecturer at the Bells University of Technology, Nigeria. He worked as the Core Network Products Manager at ZTE Corporation, Nigeria, from 2011 to 2012, and as a Network Switching Subsystem Engineer at Globacom, Nigeria, from 2012 to 2017. He was awarded the Fulbright Fellowship as a Visiting Research Scholar at the Wireless@VT Laboratory, Bradley Department of Electrical and Computer Engineering, Virginia Tech, USA, where he worked under the supervision of Prof. R. Michael Buehrer, from 2017 to 2018. He is currently a Research Scholar at Ruhr University Bochum, Germany, under the Nigerian Petroleum Technology Development Fund (PTDF) and German Academic Exchange Service (DAAD) through the Nigerian-German Postgraduate Program. He has co-edited one book and coauthored over 40 wireless communication papers in peer-reviewed journals and conferences. His research interests include beyond 5G and 6G wireless communication, wireless sensor networks, blockchain technology, and artificial intelligence. He is a Registered Engineer with the Council for the Regulation of Engineering in Nigeria (COREN) and a Nigerian Society of Engineers (NSE) Member.

JOSHUA O. OGBEBOR completed the B.Sc. degree in electrical and electronics engineering in Akoka, Lagos. He is currently pursuing the degree with the Department of Electrical and Computer Engineering, Louisiana State University, Baton Rouge, USA. He has been involved in projects on wireless systems design and control systems. His research interests include multi-agent systems and reinforcement learning-based controls.

SEIFEDINE KADRY (Senior Member, IEEE) received the bachelor's degree from Lebanese University, in 1999, the M.S. degree from the University of Reims, France, in 2002, and the EPFL, Lausanne, the Ph.D. degree from Blaise Pascal University, France, in 2007, and the H.D.R. degree from the University of Rouen Normandy, in 2017. He is currently a Full Professor of data science with Noroff University College, Norway. He is also an ABET Program Evaluator of computing and an ABET Program Evaluator of engineering technology. His current research interests include data science, education using technology, system prognostics, stochastic systems, and probability and reliability analysis.

SEUNGMIN RHO received the B.Sc. degree in computer science from Ajou University, South Korea, in 2001, and the M.Sc. and Ph.D. degrees in information and communication technology from the Graduate School of Information and Communication, Ajou University, in 2003 and 2008, respectively. Before joining the Computer Science Department, Ajou University, he spent two years in the industry. He visited the Multimedia Systems and Networking Laboratory, The University of Texas at Dallas, from 2003 to 2004. From 2008 to 2009, he was a Postdoctoral Research Fellow with the Computer Music Laboratory, School of Computer Science, Carnegie Mellon University. From 2009 to 2011, he was a Research Professor with the School of Electrical Engineering, Korea University. In 2012, he was an Assistant Professor with the Division of Information and Communication, Baekseok University. From 2013 to 2018, he was an Assistant Professor with the Department of Media Software, Sungkyul University. He is currently a Faculty Member of the Department of Industrial Security, Chung-Ang University, South Korea. His current research interests include database, big data analysis, music retrieval, multimedia systems, machine learning, knowledge management, and computational intelligence. He has published more than 180 articles in refereed journals and conference proceedings in these areas. He has been involved in more than 20 conferences and workshops as various chairs and more than 30 conferences/workshops as a Program Committee Member.