electronics

MDPI

Article

A Novel Distributed Ledger Technology Structure for Wireless Sensor Networks Based on IOTA Tangle

Hongwei Zhang [1], Marzia Zaman [2,3], Brian Stacey [2,3] and Srinivas Sampalli [1,*]

[1] Faculty of Computer Science, Dalhousie University, Halifax, NS B3H 4R2, Canada; hn507820@dal.ca
[2] Research and Development, Cistel Technology, Ottawa, ON K2E 7V7, Canada; mzaman@teleai.ca (M.Z.); bstacey@teleai.ca (B.S.)
[3] TeleAI Corporation, Ottawa, ON K2E 7V7, Canada
* Correspondence: srini@cs.dal.ca

Abstract: Wireless Sensor Networks (WSNs) consist of many wireless sensor nodes for collecting and sensing information. Distributed Ledger Technologies (DLTs) such as Blockchain allow organizations to store and share data in a decentralized, immutable, and secure way through a network of distributed peer-to-peer users or computers. The application of DLT to the Internet of Things (IoT) can improve the efficiency of information transmission and network security. IOTA Tangle is a DLT developed for IoT to process transactions. WSN is a core technology for IoT, and the two have a lot in common in terms of applications. Many solutions for IoT applications can be implemented with WSNs. However, the sensor nodes in WSNs have limited processing speed, storage capacity, communication bandwidth, and energy consumption capabilities. Therefore, a lightweight solution needs to be designed according to the characteristics of WSNs, rather than directly applying Tangle. The similarities between IoT and WSNs determine that the Tangle can be an essential reference for designing new solutions. In this paper, we propose a new DLT structure based on Tangle named Fishing Net Topology (FNT). The aim is to meet the lightweight requirements of sensor nodes in WSNs. We compared FNT with Tangle in terms of the packet network structure and algorithm and also experimentally analyzed the waste rate in the FNT network. It is concluded that FNT can be used at a reasonable Rate based on the requirement of the WSN applications, and it can significantly reduce the computation while enhancing the security of WSNs. Due to its structural stability and algorithmic simplicity, FNT outperforms Tangle in WSNs.

Keywords: Wireless Sensor Networks (WSNs); Internet of Things (IoT); Distributed Ledger Technology (DLT); Blockchain; IOTA tangle; network topology; WSN security

check for updates

Citation: Zhang, H.; Zaman, M.; Stacey, B.; Sampalli, S. A Novel Distributed Ledger Technology Structure for Wireless Sensor Networks Based on IOTA Tangle. *Electronics* **2022**, *11*, 2403. https://doi.org/10.3390/electronics11152403

Academic Editor: Christos J. Bouras

Received: 6 July 2022
Accepted: 28 July 2022
Published: 1 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Wireless Sensor Networks (WSNs) consist of many sensor nodes deployed in specific environments for monitoring and collecting information and data. Nodes in WSNs are limited by their size, computational power, power consumption, and memory size [1], resulting in their vulnerability to various types of attacks. The sensor nodes are susceptible to vandalism, physical damage, or hardware problems. Further, the sensor nodes are susceptible to being compromised and controlled as malicious nodes, leading to data leakage or the generation of false data.

Distributed Ledger Technologies (DLTs), such as Blockchain, offer a decentralized, immutable and secure network of distributed peer-to-peer users or machines to store and process transactions securely [2]. DLT involves many computer technologies such as distributed systems, cryptography, data structures or consensus algorithms [3]. Information in DLT is distributed in a network of nodes, and updates or modifications generated in the network are immediately reflected in the ledgers of all participants [4].

IOTA is a DLT designed for the Internet of Things (IoT) that is energy-efficient, scalable, lightweight, and can be transacted over the Blockchain network without any fees [5]. IOTA

uses a Directed Acyclic Graph (DAG) architecture called the Tangle, so no blocks are used. Attaching a new transaction requires approval from two previously submitted transactions [6].

The IOTA technology uses DLT to enable IoT to improve network security, which provides a new idea for solving similar problems in WSNs. IOTA is designed for IoT, but WSNs are different from IoT because WSNs have a relatively simple architecture [5,7]. Constrained by hardware and software, WSNs need a lightweight solution. Therefore, refactoring and algorithm simplification for IOTA is a feasible solution.

We propose a new IOTA Tangle-based distributed ledger topology for WSN applications named Fishing Net Topology (FNT). In FNT, the network is divided into the Initial Network and the Formal Network, and the rate is specified according to the scale of WSNs. The network is initialized by gradually increasing the number of FNT nodes starting from one and then moving to the Formal Network to achieve a situation in which the two other FNT nodes approve each node. FNT still uses a node attachment idea similar to Tangle. New nodes need to be attached to the network by approving two specified nodes. FNT does not use the complex tip selection algorithm and cumulative weight calculation in IOTA. Instead, it uses a simple node index position calculation method to find tips for attachment, thus saving computing power to meet the energy-saving and lightweight requirements of WSNs.

Although the standardization of protocols is advanced, the main focus of our paper is different. What we propose is a network topology for data transmission designed for WSNs, which will validate and store the sensed data submitted by WSN nodes in the gateway in an application scenario. It enables WSNs to process information securely and efficiently under restricted sensor nodes. Current protocol standardization does not address this aspect, so we believe the proposal provides a new solution for the application of Blockchain and IOTA in WSNs.

The composition of this paper is as follows. Section 2 introduces the background and related work and briefly describes WSNs, IoT, Blockchain, and IOTA Tangle technologies. Section 3 describes the proposed FNT in detail, including its structure, components, algorithms, terminology explanation, and functions. Section 4 shows the comparison between FNT and Tangle and the experimental design and results. Section 5 summarizes the entire paper and mentions the shortcomings of FNT and subsequent improvement ideas.

2. Background and Related Work

2.1. Wireless Sensor Networks

Wireless Sensor Networks (WSNs) consist of many wireless sensor nodes deployed in specific environments to monitor and collect information and data. The sensor nodes in WSNs transmit data to the gateways, and the transmitted data are made available to the users via the Internet. Sensor nodes typically contain processors, memory, transceivers, sensors, positioning systems, and power supplies [8]. This self-configuring network has low requirements on infrastructure, so it is easy to deploy in many rough environments. WSNs have broad application prospects, such as in area monitoring, environmental sensing, transportation, structural monitoring, industrial monitoring, agricultural sector, military and healthcare applications [9]. WSNs can be used to collect data, such as temperature, humidity, air pressure, smoke, and light in the environment, based on the type and function of the wireless sensors included [10].

WSNs face many challenges due to the limitations of node processor performance, wireless network and physical environment [11]. Sensor nodes are deployed in unattended environments and are susceptible to accidental damage [12]. The use of wireless networks for communication makes them vulnerable to more malicious attacks than wired networks. Common attacks against WSNs include Denial of Service, Jamming attack, Hello Flood attack, Black Hole attack, and Sybil attack [12,13].

2.2. Internet of Things

Internet of Things (IoT) is a network infrastructure consisting of uniquely identifiable interoperable connected objects that communicate and exchange data with other devices and systems using technologies such as Radio Frequency Identification (RFID) technology and WSNs [14]. Several communication, network, sensing, and information processing devices are interconnected to form an IoT system [15]. IoT devices can communicate with each other and interact with users through the network by equipping various devices with components such as microcontrollers and communication transceivers [16]. IoT connects the physical and virtual worlds to sense, communicate, interact, and exchange data [17]. IoT can be applied to many fields such as smart homes, wearable devices, smart cities, healthcare, and industrial applications [18–21].

2.3. Distributed Ledger Technology and Blockchain

Distributed Ledger Technology (DLT) is the generic term for distributed digital systems to record transactions and use consensus algorithms to ensure data immutability [22]. DLT encompasses technologies such as Blockchain, IOTA Tangle, Hashchain, Sidechain, and Hashgraph [23].

Blockchain technology is a distributed and decentralized digital ledger containing transactions and events [24]. Blockchain consists of many blocks linked together in a timestamped chronological manner, and each block is divided into two parts: the block header and the block body. The block header contains the block version, Merkle tree root hash, timestamp, nBits, nonce, and parent block hash [25]. The block body contains mainly transaction information. Blockchain is tamper-proof and irreversible, and its security is guaranteed due to its distributed and decentralized features [26]. The famous application of Blockchain is cryptocurrency in the financial field. In addition, there are many applications such as IoT, energy, public administration, and healthcare [27].

Blockchains use decentralized consensus mechanisms to ensure data security, such as Proof of Work (PoW) [28]. PoW is the process of mining, and the network nodes used to calculate the hash values are the miners. Miners obtain different hash values by changing nonce in the block header, and when the hash value reaches the target, the new block will be broadcasted to other nodes to verify the hash value and attach it to Blockchains [25].

2.4. IOTA Tangle

IOTA Tangle is a DLT designed for IoT with high scalability, zero cost, quantum immunity, low energy consumption, and secure data transmission features [5]. Similar to Blockchain technology, IOTA has decentralized and tamper-proof features. Tangle is a Directed Acyclic Graph (DAG) for storing transactions [6]. Instead of using blocks and chains, transactions are associated with each other to form a DAG. The comparison of Blockchain and IOTA structures is shown in Figure 1. Tangle includes nodes that perform transaction submission and validation, genesis transactions that hold all transaction tokens, and transactions that include IOTA data [5].

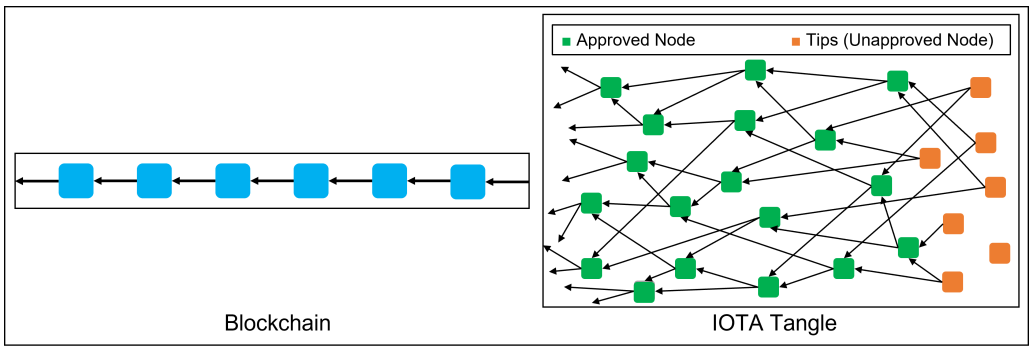


Figure 1. Structure comparison of Blockchain and IOTA Tangle.

In Tangle, new transactions submitted by clients need to go through three processes, transaction attachment, transaction propagation, and transaction confirmation [29]. Transaction attachment is achieved by approving two previously published and unapproved transactions, which are called Tips [30]. The Tips are selected according to the Uniform Random Tip Selection (URTS) algorithm and Markov Chain Monte Carlo (MCMC) algorithm [31]. Approved transactions are forwarded to neighboring nodes, and then Tangle synchronization is performed. Transaction validation is implemented using the Coordinator (COO), which is used to protect the Tangle from some attacks [29]. COO is the consensus mechanism in IOTA, which is emitted every two minutes to randomly select two new transactions for approval, and the transactions approved by the COO are considered fully trusted [30].

In Tangle, each transaction has its initial weight and cumulative weight. The cumulative weight is the sum of the weights of all the transactions that have directly or indirectly approved that transaction [29]. As more and more transactions are submitted and approved, the cumulative weight of a transaction increases.

Table 1 compares some of the characteristics of the traditional Blockchain with the IOTA Tangle. IOTA Tangle is a technology based on Blockchain, so it also includes some features of Blockchain. Some Blockchain features that are unsuitable for IoT have been improved to meet the needs of a large number of small transactions in IoT. Traditional Blockchains use mining to verify transactions, whereas in the IOTA Tangle, transactions are confirmed through tips checking and COO verification. The mining process has great requirements on the computing power of the device, and IoT devices that generate a large number of small transactions may not be able to mine, so the security mechanism of IOTA is more suitable for IoT.

Table 1. Comparison of some features of Blockchain and IOTA Tangle [5,30,32–35].

Features	Blockchain Technology	IOTA Tangle
Decentralized	Yes	Yes
Distributed	Yes	Yes
Tamper-proof	Yes	Yes
Scalability	Low	High
Latency	High	Low
Mining Process	Yes	No
Transaction Fee	Yes	No
Processing Time	Long	Short
Efficiency (transactions per second)	3–4	500–800
Suitable Transaction Type	General Transactions	Small Transactions
Transaction Validation	Miner	Self-validation
Throughput	Low	High
Resource Requirements	High	Low
Consensus (Proof of Work)	SHA256-Hash	Check Tangle Tips
Openness	Public Ledger	Public Ledger

2.5. Related Work

In [29], the researchers have analyzed actual transaction data published by the IOTA Foundation and compared it with theoretical data in the literature. They reconstructed 96 Tangles from the dataset. By analyzing their dimensions, in-degree distribution, cumulative weight, and transaction confirmation delay, they concluded that the actual transaction confirmation delay was very high. At the same time, they believed that the three influencing factors, namely the transaction arrival rate, the Tip Selection Algorithm (TSA), and the intervention of the COO, caused the performance of the actual results to be far from the simulation results. In addition, the computation of cumulative weights was complex and inefficient, which ultimately affected the tip selection and the performance of the entire network.

In [31], researchers described the structure and characteristics of the Tangle. They use computer simulations to analyze the evolution of cumulative weights and tip counts over time, resulting in a formula for the average tip count. They conclude that the growth of cumulative weights follows an exponential growth during the adoption phase, followed by a linear phase with the slope of λ. The TSA did not affect this result when α was small, and this significantly impacted the growth of cumulative weights for larger α. Due to the uncertainty of tip selection, the internal structure of the Tangle was also uncertain.

Ali, Vecchio et al. [36] have conducted an excellent survey on IoT and its challenges pertaining to network security, user privacy, data management, and standardization. Blockchain features can address several of these challenges. For example, the distributed nature of Blockchain can help in maintaining data backups and thus provide data integrity after an attack. The advantages of adaptability can help IoT devices to adapt to different application platforms and environments. The anonymity and tamper-evident characteristics can counter some network attacks that target modifying data. Blockchain does not require a trusted third party to process transactions but uses smart contracts that enable the counterparties to trust each other. Blockchain also has advantages over centralized data storage in terms of cost. Researchers have introduced many Blockchain-based IoT solutions, which show that Blockchain has significant advantages for addressing IoT challenges in terms of trust, network security, identity management, and data monetization.

Pincheira and Vecchio [37] propose an architecture to integrate Blockchain into resource-constrained IoT sensors. The integration of Blockchain on sensing devices can make the collected data trustworthy by using the decentralized and tamper-proof features of Blockchain. The researchers analyzed and experimented with the proposed architecture based on real application scenarios of public utility management systems in terms of cost, memory footprint, processing time and power consumption. They concluded that the architecture is suitable for constrained IoT devices and that the application cost for utility management could be less than 1 USD per device per month.

In the area of agricultural traceability, Pincheira et al. [38] analyzed the impact of applying Blockchain to the IoT on its sensors. The researchers tested six IoT boards on the Ethereum and Hyperledger Sawtooth platforms in terms of disk usage, memory usage, processing time, and power consumption. The results showed that Blockchain applications for IoT outperformed Sawtooth on Ethereum. Pincheira et al. [39] proposed a technology framework for water management that is a combination of IoT and Blockchain. The experimental results show that the interaction between IoT and Blockchain causes 6% additional energy consumption in this application.

Due to the lack of relevant literature and research, we introduced simulation studies of the IOTA Tangle and current research cases on applying DLT to the IoT. The simulation studies on Tangle reflect some of the limitations of Tangle and its barriers to applications in WSN. IoT has many similarities to WSNs, and the studies mentioned above apply DLT to constrained IoT devices. While our research focuses on applying DLT to WSN devices, these research cases can be used as important references.

2.6. Problem Definition

As one of the technological foundations of IoT, WSNs have a more straightforward structure than IoT. WSNs are used to collect and provide data, and IoT technology is used to analyze the data collected from the Internet and present the information for user access [40]. WSN devices are mainly various types of sensors, while IoT devices include sensors and more complex devices. There are many devices in IoT that can generate a large number of small transactions. Bitcoin can only process seven transactions per second, and Ethereum can process 14 transactions per second [6]. This performance cannot meet IoT requirements, so IOTA Tangle is proposed as a Blockchain technology designed for IoT data transmission and security needs.

The differences between IoT and WSNs determine that IOTA Tangle is not the best solution for WSNs. WSN needs a new Blockchain technology that is more suitable for it,

so we propose a new Blockchain technology based on the IOTA Tangle idea for WSNs, called Fishing Net Topology (FNT). In Tangle, two old transactions are approved by a new transaction. FNT draws on this dual authentication idea to design a new network topology for the packets generated by WSNs, making them more secure and faster to transmit and store the data. To address the computational power deficiency of WSN nodes and the difference with IoT devices, the proposed FNT simplifies the TSA in Tangle and removes the computation of cumulative weights that consume computational power, so that WSN nodes do not need to perform complex computations and meet the energy-saving and lightweight requirements of WSNs.

3. Methodology

3.1. Fishing Net Topology

In Wireless Sensor Networks (WSNs), many sensor nodes transmit data to a gateway, making the data available to users through the Internet. We propose a Blockchain topology designed for WSN applications called Fishing Net Topology (FNT) because its structure is similar to a fishing net. In the gateway, we use the FNT structure to verify the data and make it available for secure and fast transmission, as shown in Figure 2.

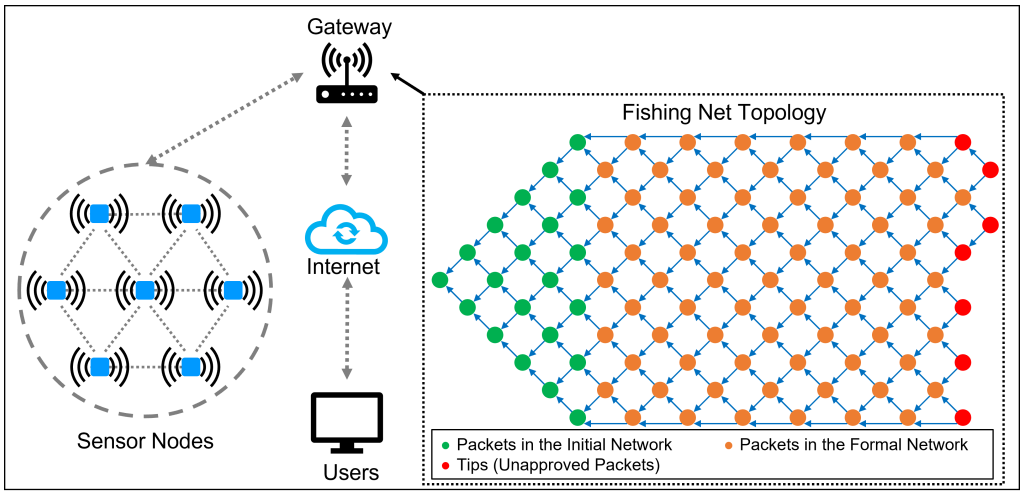


Figure 2. Wireless Sensor Networks and Fishing Net Topology.

In terms of structure, FNT is divided into two parts: the Initial Network and the Formal Network. The Initial Network is used to initialize the network to reach the maximum data packet throughput gradually, and after the initialization is completed, it enters the Formal Network. In FNT, each node represents a packet submitted by a sensor in WSNs at a point in time, and after the FNT node is created, it needs to approve two specified FNT nodes and thus be attached to the network. The two approved FNT nodes are called the Tips of that node. The FNT node also needs to be approved by two new FNT nodes afterward, and they are called Approvers of that FNT node.

3.2. Terminology

Figure 3 shows a case of FNT with a rate of 6 when 100 nodes are inserted. This figure is used as an example to explain some key terminologies.

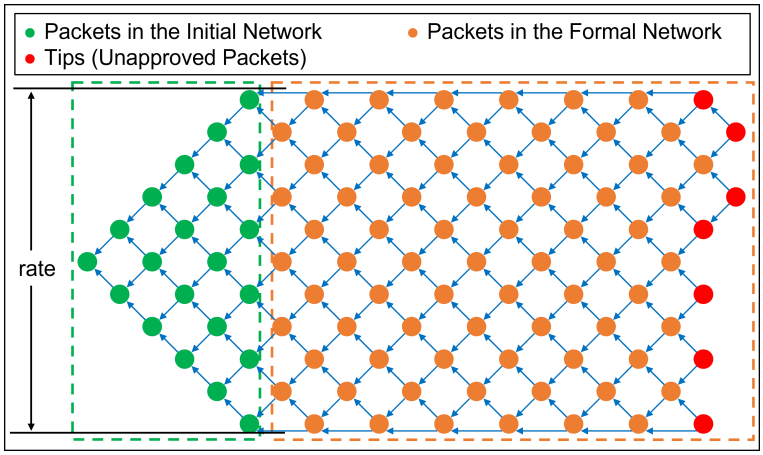


Figure 3. FNT case when the rate is 6 and 100 nodes are inserted.

3.2.1. Rate

The maximum height in the network structure is called the rate. The rate represents the packet throughput in the network and is the maximum number of packets passing through the network simultaneously.

3.2.2. Layer

The columns in the network structure are called layers, and the first layer has one FNT node, the second layer has two, and so on. The number of layers in the Initial Network is equal to the rate. The number of FNT nodes in the first layer is one, and the last layer equals the rate. The number of FNT nodes in the first layer of the Formal Network is one less than the rate, in the second layer is equal to the rate, and so on.

3.2.3. Initial Network

The shape of the Initial Network is an equilateral triangle, with one FNT node in the first layer and two in the second layer. The number of FNT nodes in each layer is one more than the previous layer until the number of FNT nodes in a layer equals the rate. This means that the Initial Network part is over. The purpose of the Initial Network is to initialize the network so that it operates at maximum throughput. The Initial Network is considered the dataset formed during the initial phase of WSNs deployment, so the data here are considered secure and valid.

3.2.4. Formal Network

As the central part of FNT, the maximum throughput is achieved in the Formal Network. Not every layer of this part operates at maximum throughput because of the need to leave a free space so that each FNT node can be attached twice, thus enabling dual authentication of packets.

3.3. FNT Node

3.3.1. FNT Node Structure

FNT node refers to the packet that contains the sensor data. An FNT node should contain three parts of information, node information, sensor information, and data collected by sensors. As shown in Figure 4, the node information contains the node ID, timestamp and its Tips and Approvers. Sensor information includes its ID, current operating status, and location. The data collected by the sensor needs to indicate its data type. Depending on the actual application of different WSNs, the information contained in the nodes may vary.

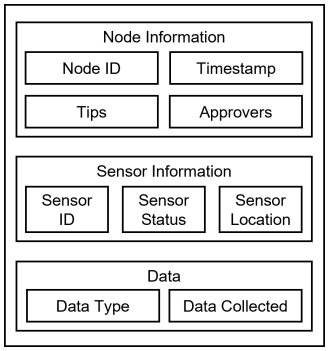


Figure 4. FNT node structure.

3.3.2. Tips and Approvers

FNT Node refers to the packet that contains the sensor data. The Tip is an entity in the FNT that may be approved by the new node. The Approver is an entity in the FNT that approves the new node.

The Tip is an unapproved FNT node in the network, and they need to be approved by later FNT nodes, thus confirming the security of its data. Each Tip needs to be approved by two other nodes. The first node has no Tip. FNT Nodes on the edge of the Initial Network have only one Tip.

Approvers refer to the two later FNT nodes that approve the specified FNT node in the network. When a new node is created, it does not have an Approver, and it needs to wait for the subsequent nodes to approve it. Every FNT node should have two Approvers, which means every node needs to be approved twice.

As shown in Figure 5, taking node 22 as an example, its Tips are nodes 16 and 17, and its Approvers are nodes 27 and 28.

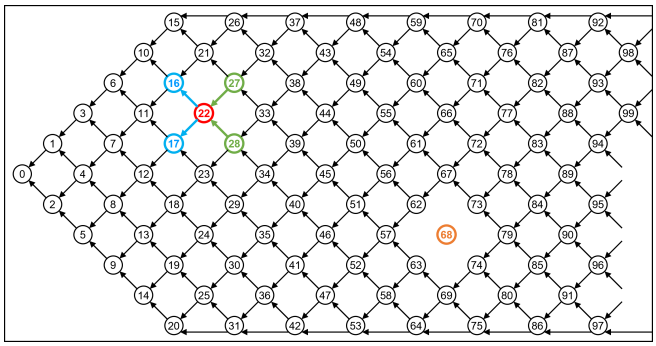


Figure 5. Tips, Approvers, and FNT node detach.

3.4. FNT Node Detach

In WSNs, if a sensor node is attacked or malfunctions, that node may produce erroneous data. If the data are submitted to the dataset, it can threaten the security and integrity of the entire dataset. Therefore, packet detaches are provided in FNT for tracing the malicious sensor nodes. Based on the tamper-proof property of the Blockchain, the malicious packet submitted to FNT cannot be simply deleted. FNT can isolate the malicious packet by detaching it from all related packets while the data are still viewable and still kept in the dataset. The network administrator can adopt some security strategies to deal with the data of the malicious packet to ensure it will not affect the entire dataset. As shown in Figure 5, the malicious packet 68 is detached from the network, while the other packets are not affected.

3.5. Tip Selection Algorithms

Figure 6 shows a case of FNT with a rate of four. The left is the Tip selection algorithm in the Initial Network, and the right is the Tip selection algorithm in the Formal Network.

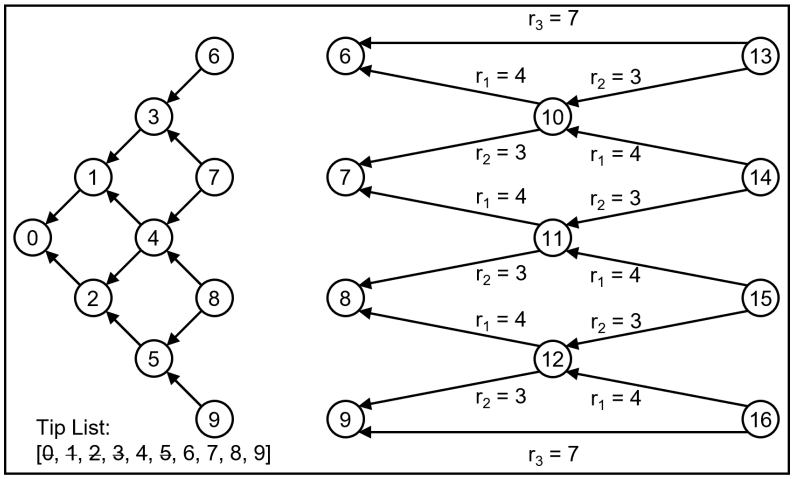


Figure 6. Tip selection algorithms for the Initial Network and the Formal Network.

3.5.1. Tip Selection Algorithm in the Initial Network

In the Initial Network, each new FNT node is added to the Tip List and attached to the network, and the Tips for that node are also assigned. Node 0 has no Tips, and the nodes on the edge have only one Tip, which means that each arrow sent from the node represents one Tip selection. If a node is attached twice in the Tip List, it will be removed. When a new node is created, it is first added to the Tip List, then the first element in the Tip List is viewed and attached. At this point, the element is attached by two nodes, the current node and the previous node, it is removed from the Tip List, and then the first element in the Tip List is updated. Thus, each Tip selection will select the first element in the Tip List until the element is attached twice. Then it is no longer a Tip and becomes a normal node.

3.5.2. Tip Selection Algorithm in the Formal Network

The first layer has one less node than the rate, so at this layer, the index of node subtracting r_1 gives the index of the first Tip and subtracting r_2 gives the index of the second Tip. The number of nodes in the second layer is equal to the rate. The index of the first Tip of the node at the top is obtained by subtracting r_3 from its index, and the index of the second Tip is obtained by subtracting r_2 from its index. The index of the first Tip of the node at the bottom is obtained by subtracting r_3 from its index, and the index of the second Tip is obtained by subtracting r_1 from its index. The indexes of the two Tips of the other nodes are their index subtracting r_1 and r_2, respectively. The next part of the Formal Network has the same method of Tip selection as the first and second layers described above.

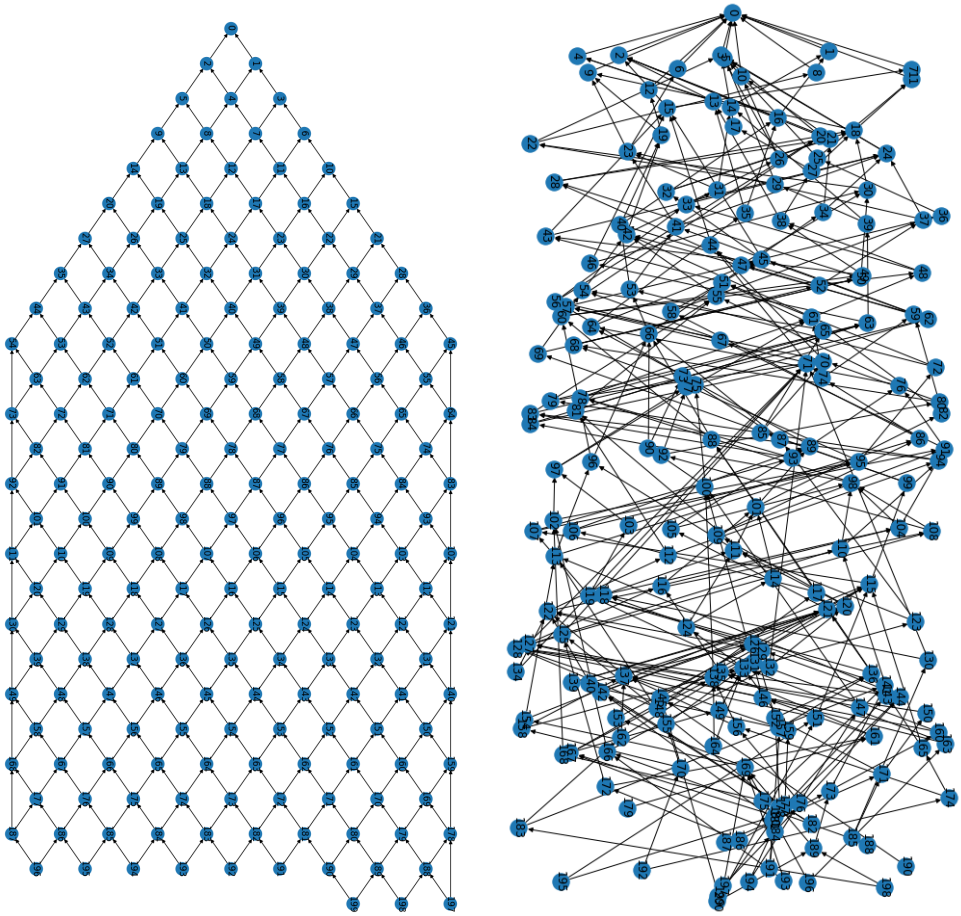
$$r_1 = rate$$
$$r_2 = rate - 1$$
$$r_3 = r_1 + r_2$$

4. Results and Discussion

4.1. Compare with the Tangle

The difference in Tip Selection Algorithm (TSA) determines a very different structure of FNT and Tangle. Tangle uses MCMC and URTS algorithms as examples of tip selection strategies [31]. These strategies make each tip selection very random, accounting for the increased time and efficiency cost, which also complicates the structure of Tangle. In contrast, FNT avoids using complex tip selection algorithms and instead appends them with simple node index computation. In addition, each new node has predefined tips in the network, so there is no selection process. This also saves much time and computational

effort. Figure 7a,b show a comparison of the structure of FNT and Tangle, with FNT being more concise and straightforward.



(**a**) (**b**)

Figure 7. Structure comparison of FNT and Tangle. (**a**) FNT structure. (**b**) Tangle structure [41].

The cumulative weight is essential in Tangle because the TSA relies heavily on cumulative weights. However, this becomes one of the most complex calculations in Tangle. In Tangle, each transaction is assigned an initial weight, and when a new transaction is attached to this transaction, the weight of this transaction becomes the sum of the weights of the two transactions. Therefore, the cumulative weight is the sum of the weights of all the transactions that are directly and indirectly attached to that transaction [29]. It can be seen that the calculation of the cumulative weight of a transaction requires traversing all its attachers in the network, which is a very complex calculation. Since the complex TSA is discarded, FNT also does not rely on cumulative weights.

Taking a network with a rate of six and 100 nodes as an example, Figure 8a,b shows the cumulative weights of each node under the two structures of FNT and Tangle, respectively. The trend of the cumulative weights in the figures also reflects the difference between the two structures. FNT has a more straightforward structure, so the trend of the cumulative weights is stable. While Tangle has a complicated structure, the cumulative weight trend is unstable. The above examples are only used to compare the differences between the two structures. FNT does not use cumulative weights.

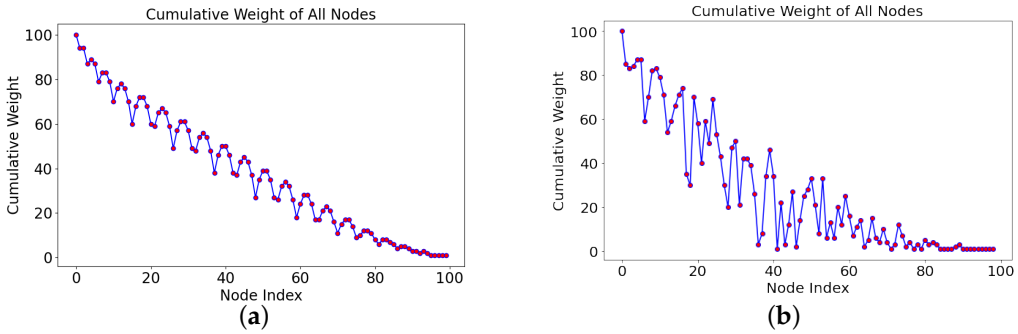


Figure 8. Comparison of the cumulative weights of the nodes in FNT and Tangle. (**a**) Cumulative weights in FNT. (**b**) Cumulative weights in Tangle [41].

4.2. Waste Rate

In FNT, each node needs to be approved by two other FNT nodes. To implement this strategy, not every layer in the FNT structure can operate at the maximum rate, and some positions in the structure are wasted. In order to maximize the utilization of FNT, we can find the optimal solution by calculating the waste rate. The main waste occurs in the Initial Network, assuming an FNT with a rate of 10. The first layer has only one node, resulting in a waste of nine nodes, and the second layer results in a waste of eight nodes. The last layer of the Initial Network has no waste. Moreover, there is a waste of one node in every second layer in the Formal Network.

r = Rate.
T_n = The number of FNT nodes in the Initial Network.
S = The number of FNT nodes in the network.
F = The number of FNT nodes in the case where nodes are fully placed in every layer.
W = The waste of FNT node placements in some layers.
WR = Waste rate.

$$S = F - W \tag{1}$$

$$T_n = \binom{r+1}{2} = \frac{(r+1)!}{2!(r+1-2)!} \tag{2}$$

$$F = r^2 + 2r * \frac{S - T_n}{2r - 1} \tag{3}$$

$$W = r^2 - T_n + \frac{S - T_n}{2r - 1} \tag{4}$$

$$WR = \frac{W}{F} \tag{5}$$

The waste rate WR can be calculated by Equation (5), using the number of wasted nodes divided by the total number of nodes in the complete arrangement.

The number of FNT nodes in the complete arrangement case can be calculated using Equation (3). The Initial Network is an equilateral triangle, a square under the complete arrangement, and the number of nodes is the square of the rate. The number of nodes in the Formal Network equals the total number of nodes by subtracting the number of nodes in the Initial Network. The number of nodes in the Formal Network is divided by the number of nodes in one group to obtain the number of groups. Then, multiplying by twice the rate gives the number of nodes in the Formal Network under the complete arrangement. This gives the total number of nodes F under the complete arrangement.

The number of wasted FNT nodes is calculated by Equation (4). The waste of the Initial Network is obtained by subtracting the actual number of nodes from the number of nodes of the Initial Network under the complete arrangement. Each group of the Formal

Network represents one waste, so the number of groups is equal to the waste of the Formal Network. This gives the waste of the entire network W.

4.3. Results

We use an example with a rate of five and 100 FNT nodes inserted to show the calculation process for the waste rate data shown in the subsequent figures and tables. The waste rate obtained in this case is 16.2791%.

$$\begin{aligned} WR &= \frac{W}{F} \\ &= \frac{r^2 - T_n + \frac{S-T_n}{2r-1}}{r^2 + 2r * \frac{S-T_n}{2r-1}} \\ &= \frac{r^2 - \binom{r+1}{2} + \frac{S-\binom{r+1}{2}}{2r-1}}{r^2 + 2r * \frac{S-\binom{r+1}{2}}{2r-1}} \\ &= \frac{r^2 - \frac{(r+1)!}{2!(r+1-2)!} + \frac{S-\frac{(r+1)!}{2!(r+1-2)!}}{2r-1}}{r^2 + 2r * \frac{S-\frac{(r+1)!}{2!(r+1-2)!}}{2r-1}} \\ &= \frac{5^2 - \frac{(5+1)!}{2!(5+1-2)!} + \frac{100-\frac{(5+1)!}{2!(5+1-2)!}}{2*5-1}}{5^2 + 2*5 * \frac{100-\frac{(5+1)!}{2!(5+1-2)!}}{2*5-1}} \\ &\approx 0.162791 \\ &= 16.2791\% \end{aligned} \tag{6}$$

Figure 9a,b show the waste curves at rates of 5 and 10, respectively, and S represents the number of FNT nodes in the networks. The same rate causes the curves to overlap. In the figures, the cumulative waste rate decreases. When the rate is five, with 1000 nodes, the waste rate is 10.71%. When the rate is 10, with 100,000 nodes, the waste rate is 5.04%.

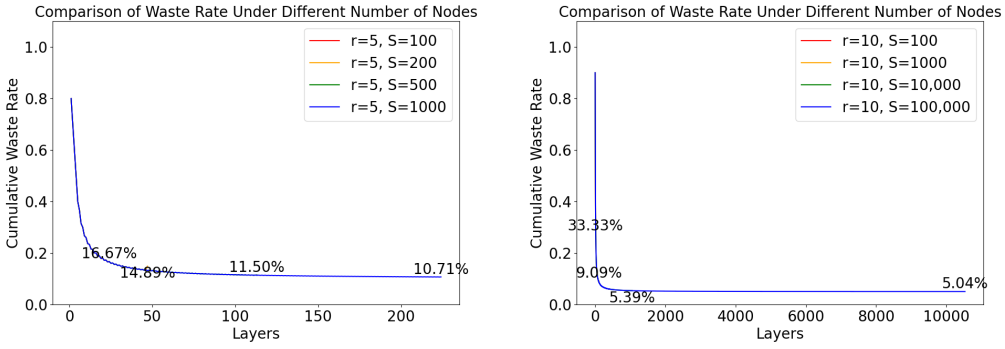
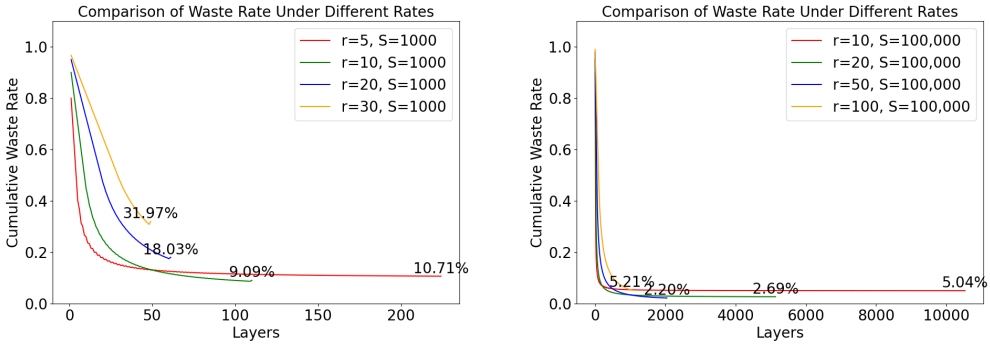


Figure 9. Comparison of the waste rate under the different number of FNT nodes. (**a**) Rate is 5. (**b**) Rate is 10.

Figure 10a shows the comparison of waste rates when there are 1000 nodes, and the rates are 5, 10, 20, and 30, respectively. With 1000 nodes, the optimal rate is between 5 and 10. Figure 10b shows the comparison of waste rates when there are 100,000 nodes, and the rates are 10, 20, 50, and 100, respectively. With 100,000 nodes, the optimal rate is between 50 and 100. The specific optimal rate value can be calculated within this range.



(**a**) (**b**)

Figure 10. Comparison of the waste rate under the different rates. (**a**) 1000 FNT Nodes. (**b**) 100,000 FNT Nodes.

In Table 2, the waste rate of FNT composed of the different number of FNT nodes and different rates is shown. Experiments ranged in rates from 5 to 1000 and the number of nodes from 100 to 1,000,000.

Table 2. The waste rates under the different rates, and number of FNT nodes.

WR	S = 100	S = 1000	S = 10,000	S = 100,000	S = 1,000,000
r = 5	16.2791%	10.6700%	10.0674%	10.0067%	10.0007%
r = 6	18.1548%	9.4203%	8.4432%	8.3443%	8.3344%
r = 10	32.1429%	8.6538%	5.3785%	5.0380%	5.0038%
r = 15	51.0549%	11.9210%	4.2667%	3.4275%	3.3428%
r = 20	65.1786%	17.3729%	4.2240%	2.6752%	2.5175%
r = 25	74.7097%	23.8835%	4.7388%	2.2809%	2.0282%
r = 30	81.0897%	30.7512%	5.6302%	2.0779%	1.7079%
r = 50	92.3846%	55.0000%	11.6071%	2.1739%	1.1187%
r = 100	98.0100%	83.1356%	33.2215%	5.1478%	0.9852%
r = 120	98.6130%	87.6753%	41.6959%	7.0010%	1.1168%
r = 150	99.1101%	91.7631%	52.7646%	10.2910%	1.4275%
r = 200	99.4987%	95.2043%	66.5268%	16.7362%	2.1867%
r = 500	99.9198%	99.2040%	92.5725%	55.5011%	11.1605%
r = 600	99.9443%	99.4461%	94.7246%	64.2388%	15.2818%
r = 700	99.9591%	99.5926%	96.0704%	70.9763%	19.6909%
r = 800	99.9687%	99.6879%	96.9642%	76.1599%	24.2439%
r = 900	99.9753%	99.7533%	97.5865%	80.1737%	28.8196%
r = 1000	99.9800%	99.8001%	98.0363%	83.3139%	33.3222%

Due to space limitations, this table only shows some combinations of rates and packet numbers. As can be seen in Table 2, the greater the number of packets, the lower the waste rate for the same rate. However, a higher rate does not result in a lower waste rate for the same number of packets. At a rate of 10, the waste rate decreases as the number of packets increases, from 32.1429% at 100 packets to 5.0038% at one million packets, and will continue to decrease. When there are one million packets, the lowest waste rate occurs between 50 and 120, which is about 0.9852%. At this point, the waste rate is already below 1%. Such a combination of rate and number of packets is considered optimal, as its waste rate is minimal. More accurate optimal rates, which are not shown in the table, require further calculations between 50 and 120.

In summary, having an optimal rate for different numbers of packets can minimize the waste of the network. Thus, when establishing FNT, predicting the number of packets that may be generated based on the size of the WSNs can help users determine an optimal rate so that users can choose the most appropriate WSN plan based on actual demand and budget.

5. Conclusions and Recommendations

Based on the technical background of WSNs, IoT, Blockchain, and IOTA Tangle, we proposed Fishing Net Topology (FNT). FNT meets the energy-saving and lightweight requirements of WSNs. This paper elaborates on the structure, algorithm, and features of FNT. The comparison with Tangle and the experimental analysis of the waste rate of the FNT for different rates and the number of FNT nodes conclude that choosing a reasonable rate can significantly reduce waste and computation. FNT improves on two shortcomings of IOTA Tangle. First, it discards the complex tip selection algorithm and uses only a simple calculation of the node index to find tips and attach them. Second, the calculation of cumulative weights is not required in FNT. These improvements allow FNT to save computations and costs.

The FNT waste rate for different rates and the number of packets is shown in the figures and tables. At the same rate, the higher the number of packets, the lower the overall waste rate, and eventually, the trend will stabilize, as waste will persist. Calculating the optimal rate for the different number of packets of FNT is critical, and the choice of different rates can lead to a dramatic change in the result. We used the waste rate calculation formula and calculated the waste rate of some FNTs shown in Table 2, from the maximum waste rate close to 100% to a minimum of less than 1%. We can see that under the same packet number, as the rate increases, the waste rate decreases gradually to the minimum value and then starts to increase. We can obtain the minimum value of the waste rate, and the corresponding rate is the optimal rate.

The application scenario of FNT is shown in Figure 2. In WSNs, many sensor nodes are deployed in a specific environment for collecting and sensing data. Each sensor node should upload packets to the gateway at a preset time interval. The size of the FNT is also specified according to the user's demand for the size of the WSNs, so its rate is preset. In the gateway, the submitted packets are attached to the FNT. Each packet needs to be validated against the data of its two Tips, also previously submitted packets. Since it is not attached by other packets, it is temporarily called Tips. Packets that pass the two Approvers validation become general FNT nodes. As more and more packets are attached to the FNT and verified by more and more packets, the authenticity of the data in the whole network is guaranteed. Users can access the FNT and its data stored in the gateway and more operations through the Internet.

In applying FNT, a reasonable rate should be calculated to save costs depending on the demand for WSNs. The cost of implementing FNT is mainly in the network service. FNT has no additional demand on the hardware of WSN nodes, so there is no additional cost. Higher network speed and bandwidth lead to more expenses, and the selection of the best rate in FNT is to refer users to choosing network services to reduce expenses. FNT aims to reduce the computation of WSN nodes while providing a secure and reliable data storage and transmission solution.

During the design of FNT, we took inspiration from the DAG structure of the IOTA Tangle and made many structural design attempts. Some of these solutions achieve higher network utilization but lack security, while others are faster processing but lack scalability. After comparison, we chose the current FNT structure. The FNT structure starts with one initial node, and each subsequent layer has one more node than the previous one until it reaches a preset rate value and completes the initialization. We need to verify each node twice to improve security, so the FNT structure is obtained. In the Formal Network, to enable each FNT node to be approved twice, it can be noticed that one FNT node position is wasted every two layers. This means that not every layer is operating at the maximum rate. Despite the waste, this approach can effectively improve packet security. In addition, the main challenge we face is how to measure the performance of FNT. We have calculated the waste in the network through formula derivation and program simulation. There should also be more measures that need to be improved in future studies.

FNT relies on a stable and lightweight security mechanism. When a new FNT node is attached, it must approve its Tips. The approval process requires first determining the

operational and security status of the sensor nodes, and second the authenticity of the data contained in the packet. This requires creating a data model to estimate the range of data the sensor may acquire, which relies on historical sensing data from the environment in which the sensor is located. In future research, we plan to create this security model based on machine learning. The model will use a series of algorithms and historical data analysis to determine the authenticity of the data in the nodes to avoid polluting the entire dataset with data generated by malicious nodes. Therefore, in future work, we need to develop and validate a security model for data validation to improve the security of using FNT. There is also a need to evaluate the performance of FNT from more perspectives and add more metrics. We also need to identify the problems and improve them through practical applications.

Author Contributions: Conceptualization, H.Z., S.S. and M.Z.; methodology, H.Z.; project administration, H.Z., S.S. and M.Z.; software, H.Z.; supervision, S.S. and M.Z.; visualization, H.Z.; writing—original draft, H.Z.; writing—review and editing, H.Z., S.S., M.Z. and B.S. All authors have read and agreed to the published version of the manuscript.

Funding: The authors gratefully acknowledge the support in part by the Natural Sciences and Engineering Research Council (NSERC) and industry partners Norleaf Networks and Cistel Technology Inc., through a Collaborative Research Grant.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The essential functions and algorithms of the Fishing Net Topology project have been implemented using Python code and published to GitHub as an open-source platform, which can be found at https://github.com/Hongwei-Z/FishingNetTopology (accessed on 23 June 2022).

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

References

1. Singh, M.K.; Amin, S.I.; Imam, S.A.; Sachan, V.K.; Choudhary, A. A Survey of Wireless Sensor Network and its types. In Proceedings of the 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 12–13 October 2018; pp. 326–330. [CrossRef]
2. Suciu, G.; Nădrag, C.; Istrate, C.; Vulpe, A.; Ditu, M.C.; Subea, O. Comparative Analysis of Distributed Ledger Technologies. In Proceedings of the 2018 Global Wireless Summit (GWS), Chiang Rai, Thailand, 25–28 November 2018; pp. 370–373. [CrossRef]
3. Antal, C.; Cioara, T.; Anghel, I.; Antal, M.; Salomie, I. Distributed ledger technology review and decentralized applications development guidelines. *Future Internet* **2021**, *13*, 62. [CrossRef]
4. Bouras, M.A.; Lu, Q.; Zhang, F.; Wan, Y.; Zhang, T.; Ning, H. Distributed ledger technology for eHealth identity privacy: State of the art and future perspective. *Sensors* **2020**, *20*, 483. [CrossRef] [PubMed]
5. Bhandary, M.; Parmar, M.; Ambawade, D. A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle. In Proceedings of the 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 10–12 June 2020; pp. 827–832. [CrossRef]
6. Shabandri, B.; Maheshwari, P. Enhancing IoT Security and Privacy Using Distributed Ledgers with IOTA and the Tangle. In Proceedings of the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 7–8 March 2019; pp. 1069–1075. [CrossRef]
7. Khalil, N.; Abid, M.R.; Benhaddou, D.; Gerndt, M. Wireless sensors networks for Internet of Things. In Proceedings of the 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Singapore, 21–24 April 2014; pp. 1–6. [CrossRef]
8. Numan, M.; Subhan, F.; Khan, W.Z.; Hakak, S.; Haider, S.; Reddy, G.T.; Jolfaei, A.; Alazab, M. A Systematic Review on Clone Node Detection in Static Wireless Sensor Networks. *IEEE Access* **2020**, *8*, 65450–65461. [CrossRef]
9. Zawaideh, F.; Salamah, M. An efficient weighted trust-based malicious node detection scheme for wireless sensor networks. *Int. J. Commun. Syst.* **2019**, *32*, e3878. [CrossRef]
10. Ram Prabha, V.; Latha, P. Fuzzy trust protocol for malicious node detection in wireless sensor networks. *Wirel. Pers. Commun.* **2017**, *94*, 2549–2559. [CrossRef]
11. Zia, T.; Zomaya, A. Security Issues in Wireless Sensor Networks. In Proceedings of the 2006 International Conference on Systems and Networks Communications (ICSNC'06), Tahiti, French Polynesia, 29 October–3 November 2006; p. 40-40. [CrossRef]

12. Salau, A.O.; Marriwala, N.; Athaee, M. Data security in wireless sensor networks: Attacks and countermeasures. In *Mobile Radio Communications and 5G Networks*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 173–186.
13. Du, X.; Chen, H.-H. Security in wireless sensor networks. *IEEE Wirel. Commun.* **2008**, *15*, 60–66. [CrossRef]
14. binti Mohamad Noor, M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294. [CrossRef]
15. Da Xu, L.; He, W.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243.
16. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of Things for Smart Cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. [CrossRef]
17. Porkodi, R.; Bhuvaneswari, V. The internet of things (IOT) applications and communication enabling technology standards: An overview. In Proceedings of the 2014 International Conference on Intelligent Computing Applications, Coimbatore, India, 6–7 March 2014; pp. 324–329.
18. Elijah, O.; Rahman, T.A.; Orikumhi, I.; Leow, C.Y.; Hindia, M.N. An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges. *IEEE Internet Things J.* **2018**, *5*, 3758–3773. [CrossRef]
19. Adamu, A.A.; Wang, D.; Salau, A.O.; Ajayi, O. An integrated IoT system pathway for smart cities. *Int. J. Emerg. Technol.* **2020**, *11*, 1–9.
20. Salau, A.O.; Chettri, L.; Bhutia, T.K.; Lepcha, M. IoT based smart digital electric meter for home appliances. In Proceedings of the 2020 International Conference on Decision Aid Sciences and Application (DASA), Sakheer, Bahrain, 8–9 November 2020; pp. 708–713.
21. Rana, A.K.; Salau, A.O.; Sharma, S.; Tayal, S.; Gupta, S. *Internet of Things: Energy, Industry, and Healthcare*; CRC Press: Boca Raton, FL, USA, 2021.
22. Farahani, B.; Firouzi, F.; Luecking, M. The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *J. Netw. Comput. Appl.* **2021**, *177*, 102936. [CrossRef]
23. Akhtar, Z. From blockchain to hashgraph: Distributed ledger technologies in the wild. In Proceedings of the 2019 International Conference on Electrical, Electronics and Computer Engineering (UPCON), Aligarh, India, 8–10 November 2019; pp. 1–6.
24. Chatterjee, R.; Chatterjee, R. An Overview of the Emerging Technology: Blockchain. In Proceedings of the 2017 3rd International Conference on Computational Intelligence and Networks (CINE), Odisha, India, 28 October 2017; pp. 126–127. [CrossRef]
25. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564. [CrossRef]
26. Viriyasitavat, W.; Hoonsopon, D. Blockchain characteristics and consensus in modern business processes. *J. Ind. Inf. Integr.* **2019**, *13*, 32–39. [CrossRef]
27. Abou Jaoude, J.; George Saade, R. Blockchain Applications – Usage in Different Domains. *IEEE Access* **2019**, *7*, 45360–45381. [CrossRef]
28. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
29. Guo, F.; Xiao, X.; Hecker, A.; Dustdar, S. Characterizing IOTA Tangle with Empirical Data. In Proceedings of the GLOBECOM 2020-2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6. [CrossRef]
30. Silvano, W.F.; Marcelino, R. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. *Future Gener. Comput. Syst.* **2020**, *112*, 307–319. [CrossRef]
31. Kusmierz, B.; Staupe, P.; Gal, A. Extracting Tangle Properties in Continuous Time via Large-Scale Simulations. Technical Report. Working Paper. 2018. Available online: https://assets.ctfassets.net/r1dr6vzfxhev/4T4IAlxk9ym0eWco0UoQIQ/90094e746745b89253eb3636b4ad1597/Extracting_Tangle_Properties_in_Continuous_Time_via_Large_Scale_Simulations_V2.pdf (accessed on 10 May 2022).
32. Hao, Y.; Li, Y.; Dong, X.; Fang, L.; Chen, P. Performance Analysis of Consensus Algorithm in Private Blockchain. In Proceedings of the 2018 IEEE Intelligent Vehicles Symposium (IV), Changshu, China, 26–30 June 2018; pp. 280–285. [CrossRef]
33. Zhou, Z.; Li, R.; Cao, Y.; Zheng, L.; Xiao, H. Dynamic Performance Evaluation of Blockchain Technologies. *IEEE Access* **2020**, *8*, 217762–217772. [CrossRef]
34. Fan, C.; Ghaemi, S.; Khazaei, H.; Musilek, P. Performance Evaluation of Blockchain Systems: A Systematic Survey. *IEEE Access* **2020**, *8*, 126927–126950. [CrossRef]
35. Schueffel, P. Alternative Distributed Ledger Technologies Blockchain vs. Tangle vs. Hashgraph-A High-Level Overview and Comparison. Tangle vs. Hashgraph-A High-Level Overview and Comparison (15 December 2017). 2017. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144241 (accessed on 28 June 2022).
36. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of Blockchains in the Internet of Things: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1676–1717. [CrossRef]
37. Pincheira, M.; Vecchio, M. Towards Trusted Data on Decentralized IoT Applications: Integrating Blockchain in Constrained Devices. In Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 7–11 June 2020; pp. 1–6. [CrossRef]
38. Pincheira, M.; Vecchio, M.; Giaffreda, R. Benchmarking Constrained IoT Devices in Blockchain-Based Agri-Food Traceability Applications. In *International Congress on Blockchain and Applications*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 212–221.

39. Pincheira, M.; Vecchio, M.; Giaffreda, R.; Kanhere, S.S. Exploiting constrained IoT devices in a trustless blockchain-based water management system. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020; pp. 1–7. [CrossRef]
40. Worlu, C.; Jamal, A.A.; Mahiddin, N.A. Wireless sensor networks, internet of things, and their challenges. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 556–566.
41. Nghia, M. TangleSimulator. 2018. Available online: https://github.com/minh-nghia/TangleSimulator (accessed on 10 May 2022).