*future internet*

MDPI

*Article*

# Evaluation of Blockchain Networks' Scalability Limitations in Low-Powered Internet of Things (IoT) Sensor Networks

**Kithmini Godewatte Arachchige *, Philip Branch and Jason But**

Department of Telecommunications, Electrical, Robotics and Biomedical Engineering, Swinburne University, Melbourne 3122, Australia; pbranch@swin.edu.au (P.B.); jbut@swin.edu.au (J.B.)
* Correspondence: kgodewattearachchige@swin.edu.au

**Abstract:** With the development of Internet of Things (IoT) technologies, industries such as healthcare have started using low-powered sensor-based devices. Because IoT devices are typically low-powered, they are susceptible to cyber intrusions. As an emerging information security solution, blockchain technology has considerable potential for protecting low-powered IoT end devices. Blockchain technology provides promising security features such as cryptography, hash functions, time stamps, and a distributed ledger function. Therefore, blockchain technology can be a robust security technology for securing IoT low-powered devices. However, the integration of blockchain and IoT technologies raises a number of research questions. Scalability is one of the most significant. Blockchain' scalability of low-powered sensor networks needs to be evaluated to identify the practical application of both technologies in low-powered sensor networks. In this paper, we analyse the scalability limitations of three commonly used blockchain algorithms running on low-powered single-board computers communicating in a wireless sensor network. We assess the scalability limitations of three blockchain networks as we increase the number of nodes. Our analysis shows considerable scalability variations between three blockchain networks. The results indicate that some blockchain networks can have over 800 ms network latency and some blockchain networks may use a bandwidth over 1600 Kbps. This work will contribute to developing efficient blockchain-based IoT sensor networks.

**Keywords:** blockchain; low-powered wireless sensor networks; IoT; scalability



**Citation:** Godewatte Arachchige, K.; Branch, P.; But, J. Evaluation of Blockchain Networks' Scalability Limitations in Low-Powered Internet of Things (IoT) Sensor Networks. *Future Internet* **2023**, *15*, 317. https://doi.org/10.3390/fi15090317

Academic Editor: Ashutosh Dhar Dwivedi

Received: 31 August 2023
Revised: 19 September 2023
Accepted: 19 September 2023
Published: 21 September 2023



## 1. Introduction

The Internet of Things (IoT) connects sensors, actuators, processes and people using low-powered networks and devices with a reliance on single-board computers and microcontrollers [1]. Blockchain technology is a security solution that has developed significantly over the last decade. With the modern developments of IoT technologies and blockchain technology, researchers have suggested that blockchain technology holds potential security capabilities to protect IoT end devices [2]. However, the integration of blockchain and IoT technologies raises a number of research issues, including blockchain network scalability [3].

IoT end devices are low-powered devices that generate sensor data and transmit over a network [4]. Network scalability refers to the ability of the blockchain network to accommodate a number of IoT devices and blockchain network traffic while maintaining the optimal network performance [4].

With the development of blockchain and wireless sensor networks, the network scalability of low-powered blockchain sensor networks is a critical consideration for expanding the network [5]. Our interest in blockchain for low-powered devices came about as a result of our work in IoT for healthcare. In one of the systems we worked on for healthcare, patients and their families may access a blockchain network to keep track of their relatives [5]. This can give rise to a significant issue, namely that the blockchain network generates a high volume of network traffic and causes a network failure [6]. However, blockchain use over low-powered sensor networks has great potential in other areas, such as energy production, vehicular networking, and other IoT applications [7].

Although there are promising security features of blockchain technology, scalability is still a key barrier when it comes to their implementation across wireless low-powered sensor networks. Blockchain network throughput, bandwidth, hash rate, latency, and data transaction rate are major aspects of a scalable blockchain network [7]. Understanding how the performance of different blockchains changes as the number of nodes increases is important. We explore this issue using an experimental test bed that runs three of the most popular blockchain algorithms [6].

Although blockchains provide security benefits, as most IoT networks are low-powered, the integration of blockchain technology may decrease network performance efficiency and cause unnecessary scalability issues. An increment in data transmission latency or data loss due to the increment of blockchain network users can create significant consequences, including a reduction in Quality of Service (QoS) [8]. Also, unnecessary latency of sensitive data transactions or data loss in healthcare may put lives at risk. As most IoT networks use wireless technologies for data transmission, bandwidth usage is also another key challenge [8]. Blockchains transmit data as a chain of blocks, and the bandwidth usage of blockchain networks may be higher compared to other peer-to-peer networks. Blockchain networks may require additional bandwidth capacity, and the higher usage of bandwidth may limit the network access for users [8].

Considering the importance of blockchain scalability, we have developed a blockchain network test bed using twenty blockchain nodes, and we have installed three commonly used blockchain algorithms to run on the test bed. We have analysed the network scalability with respect to blockchain network latency, block transaction rate, and bandwidth parameters [8]. The architecture of the research methodology is blended. We used experimental results collected from the test bed and statistical software tools to analyse the collected network latency, bandwidth usage, and block transaction rate data. All the data were generated during the experiments in a lab environment [9].

The remainder of this paper is structured as follows: In Section 2, we discuss blockchain technology. In Section 3, we look at blockchains in the healthcare sector. We provide an overview of related work in Section 4. Section 5 outlines our methodology and blockchain network prototype development, while Section 6 presents our results and evaluation. Section 7 concludes the paper and outlines future work we plan to carry out.

### *1.1. Research Architecture*

Figure 1 indicates the generic architecture of the research that we have used to develop the test environment and results parameters. In Figure 1, we present the installation and configuration process of the blockchain platforms on IoT low-powered end devices and blockchain security features that we have used to protect the blockchain sensor network. Also, we evaluate the scalability limitations of blockchain sensor networks using Hydrachain, Monero, and Duino coin blockchain platforms. The network latency, bandwidth usage, and block transaction rate were used to collect network scalability data.

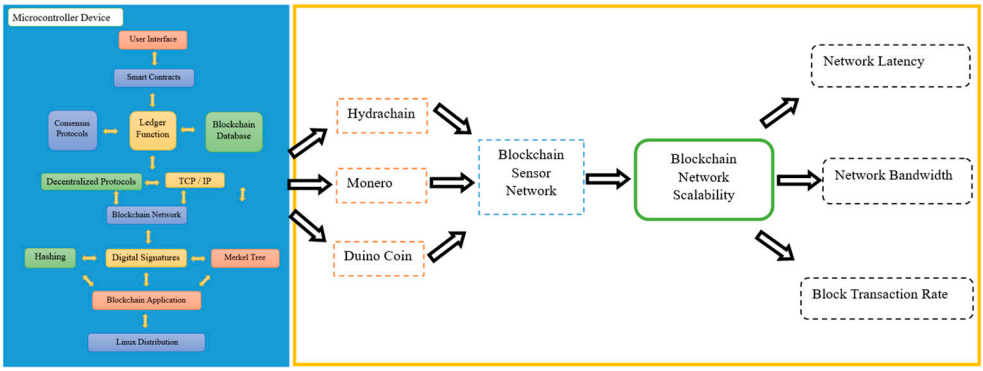


**Figure 1.** Research architecture.

### 1.2. Research Contributions

1. We identify the scalability limitations of blockchain-based sensor networks using real test bed experiments.
2. We evaluate the scalability variations of different blockchain networks that can be applied to avoid scalability bottlenecks of blockchain-based sensor networks.
3. We provide an overview of real test results using three key blockchain network scalability parameters. The parameters are network latency, block transaction rate, and network bandwidth.

## 2. Blockchain Technology

This section contains material of a background nature for readers less familiar with blockchain and can be skipped by readers familiar with basic blockchain concepts. The emergence of blockchain technology was first disclosed by a Japanese software program developer called Satoshi Nakamoto in 2008 [9]. Satoshi Nakamoto invented the first blockchain database by inventing the Bitcoin blockchain algorithm. However, Stuart Harber and W. Scott Stornetta envisioned the blockchain technology platform in 1991 [10]. Blockchain is a network security solution that operates on a digital ledger system. Blockchain uses encrypted data blocks to transmit over the network [11]. These blockchain networks are distributed and constructed with inherent security parameters such as cryptography, time stamps, hash function, anonymity, and digital signatures. Apart from the security parameters, blockchains typically use smart contracts, consensus protocols, and tokenization protocols to ensure the block transactions within the blockchain networks [10]. Blockchain networks are categorized into three main blockchain network types [11]. They can be understood as follows.

### 2.1. Public Blockchain Networks

Public blockchain networks are open and permissionless networks that anybody can access without approval. Permissionless blockchain networks have no central authority and provide full transparency of block transactions. The blockchain networks that are open to the public are known as permissionless blockchain networks [12]. Users have the ability to read, write, or modify transactions based on their needs. These particular types of blockchain networks are self-governed blockchains and enable users to utilize security measures like encryption, timestamps, anonymity, and hashes [11].

### 2.2. Private Blockchain Networks

Private blockchains are permissioned and restricted networks where participation is tightly controlled. These private blockchain networks provide limited blockchain services to users and are often used by organizations to maintain information privacy. User access is given only to validated and authenticated users [12]. Permissioned blockchain networks are another term for private blockchain networks. Moreover, chosen or authenticated users can only access the shared ledger [11].

### 2.3. Hybrid Blockchain Networks

Hybrid blockchain networks consist of the features of both private and public blockchain networks. Hybrid blockchain networks allow access to public users while maintaining restricted blockchain services [13]. Hybrid blockchain networks offer flexible and customizable blockchain services compared to private and public blockchain networks [13]. In the next section, we discuss the use of blockchain technology in healthcare.

## 3. Blockchain Technology in Healthcare

As an emerging information security solution, blockchain technology can potentially protect various industries' sensitive data and end devices, including healthcare [10]. Blockchain technology provides a wide range of security functions and applications that

helps to protect the healthcare sector from cyber intrusions, such as cryptography, hash function, anonymity, and digital signatures [14].

With the development of smart healthcare systems, the healthcare industry started using low-powered IoT smart devices to collect medical information and store health records [14]. As IoT devices are low-powered, sensitive medical information can be susceptible to cyber intrusions. The healthcare sector is looking for a robust information security solution, and blockchain technology can be a successful solution [7]. The healthcare sector also faces privacy issues, data corruption, theft of sensitive medical information and physical device damages, which can cause extreme consequences to lives [13].

Apart from these, the healthcare sector also faces data overload concerns, as IoT medical devices collect and process a lot of medical data. Data overload may cause bottlenecks in healthcare applications and data transmission. Also, as healthcare data are highly sensitive, there may be concerns with third-party integrated protocols [14]. With increasing cyber security threats, third-party protocols may raise privacy concerns and information theft.

Healthcare is a critical sector that deals with human lives, and data leakage or corruption may put lives at risk. Therefore, healthcare systems follow global standards. However, IoT systems still face global standardization concerns due to the ambiguity of ownership. The integration of multiple IoT devices becomes challenging in healthcare for standardization procedures [14].

Similarly, the integration of various devices can impede the adoption of IoT in the healthcare sector. This obstacle arises from the fact that the manufacturers of these devices have yet to establish a common framework for creating communication protocols and standards [15]. This concern also may cause data-protection concerns in healthcare.

Most IoT smart devices use wireless connectivity as the primary data-transmission technology. The wireless connectivity uses primary data security features such as data encryption. However, due to the increment of cyber threats, wireless technologies are more prone to cyber threats, including packet sniffing, Wi-Fi jamming, encryption cracking, and Wi-Fi phishing [15]. Concerning these cyber security threats, blockchain technology offers enhanced security features that promise the protection of data transmission technologies. However, as blockchains use a variety of security and privacy protection features such as anonymity, cryptography, and hash functions, the respective concerns, including privacy, can be addressed. Also, blockchains use ledgers to store block transaction records that can be used for audit purposes [16].

Blockchain technology can be operated for a wide range of networking purposes, such as medical data collection, digitalized patient tracking, and Ambient Assisted Living Systems [16]. Blockchain technology provides an additional security layer on network connections, IoT end devices, and user accounts [17].

Most blockchain platforms are open-source, providing legal licenses to customize as per requirements [17]. Blockchain researchers can use these open-source blockchain platforms to develop numerous automated blockchain applications for commercial purposes. However, the integration of blockchain technology and low-powered IoT healthcare-based wireless networks can be challenging due to scalability limitations [17]. Blockchains typically require high network bandwidth, and the limitations of particular blockchain networks can increase the latency while decreasing the block transactions [17].

Therefore, in this paper, we analyse blockchain network scalability limitations using real-world experiments and provide experimental results, which may help the healthcare industry to use blockchain technology to mitigate cyber intrusions. We discuss the related work in the next section.

## 4. Related Work

Oscar Novo explains that scalability poses a significant challenge when it comes to improving the access management of IoT systems based on blockchain technology [18]. The study focuses on maximizing scalability by employing various access-management

configurations. The researchers emphasize that blockchain-based IoT systems have limited access-management capabilities due to resource sharing and permission restrictions [18]. The study introduces a flexible access management system based on blockchain technology, which operates on a decentralized digital ledger. According to the authors, this system offers several benefits, including isolated managerial domains, access control policies, and continuous administrative functions [18]. Additionally, this paper highlights that the proposed system is energy-efficient and cost-effective compared to other commercially available access management systems. The authors also implement a cross-platform communication system to validate interactions among IoT devices [18]. The paper concludes that utilizing blockchain access management configurations is a viable approach to enhancing scalability capabilities and performance capacities. To develop the blockchain-based access management system, the authors adopt the CoAP management interface developed by the Internet Engineering Task Force (IETF) [18].

As stated by Sanjeev Dwivedi et al., the main objective of IoT-based smart home automation systems is to enhance and simplify people's lives [19]. These systems utilize a variety of smart consumer products and sensors to provide convenience. The authors explain that the IoT industry incorporates automated electrical appliances, wearable electronics, and tracking devices across various sectors such as agriculture, healthcare, and energy [19]. However, due to their limited processing capacity, IoT devices are susceptible to security attacks. The authors have identified four major categories of IoT-related attacks, namely physical attacks, network attacks, software attacks, and data attacks [19]. To address these security concerns, the authors suggest that blockchain technology can serve as a robust solution. Blockchain has the potential to mitigate security issues like unauthorized access, privacy breaches, data tampering, and malicious actions [19]. Additionally, the authors highlight the advantages of blockchain technology in enhancing industrial productivity and efficiency within the manufacturing sector. They also propose that smart contracts can offer a secure environment for processing data and ensuring data integrity [19].

According to Hong-Ning Dai, cybersecurity threats to IoT technologies arise from issues such as poor compatibility, limited processing power, and insecure data transmissions [20]. Dai and the other authors of the study investigated the potential use of blockchain technology in IoT systems and put forth a novel architecture called Blockchain of Things (BCoT) [20]. They also examined the applicability of blockchain technology in conjunction with 5G cellular connections. The authors assert that the utilization of IoT cyber-physical systems presents challenges due to the wide array of devices and systems, complex networks, diverse IoT data, and resource limitations [20]. However, they also highlight the opportunities that blockchain technology can offer in addressing these challenges. The paper underscores the capability of blockchain technology to validate IoT data and establish a mutually trusted cyber system based on blockchain [20]. The authors introduce four key metrics for BCoT: interoperability, traceability, reliability, and autonomic interactions. Interoperability refers to the seamless exchange of information between IoT systems, while traceability pertains to the ability to track data blocks [20]. Reliability encompasses the quality of network services and IoT data availability. Autonomic interactions involve the ability to engage with trusted IoT systems. As emphasized by the authors, BCoT can be a potential solution for untrusted IoT networks [20].

According to a study by Amreen Ashraf et al., Hyperledger Fabric (HLF) is a widely used blockchain platform that offers permissioned blockchain services [21]. The study focuses on identifying performance bottlenecks of HLF in IoT systems, as HLF is hosted by the Linux Foundation. The authors emphasize that the scalability limitations of HLF can result in performance issues in the system [21]. The study highlights that large-scale distributed ledger systems like HLF present various research challenges, such as throughput, latency, network size, and data transfer rates [21]. The authors evaluate the scalability and propose a blockchain-based framework for large-scale IoT systems [21]. According to the authors, blockchain applications have merged with IoT and communication technologies

to create sensor-based systems on a large scale, including air quality monitoring [21]. The authors also mention that blockchain offers promising protection for availability, confidentiality, and integrity, but integrating blockchain and IoT technologies poses challenges [21]. The authors contribute to showcasing the importance of Distributed Ledger Technologies (DTL) and enhancing the cryptographic primitives of DTL systems. Additionally, they evaluate blockchain-based plugins and HLF payment transactions [21]. The issue of network scalability of blockchain on sensor networks with low-powered devices has not been researched in any depth.

According to Hongchen Guo et al., decentralized blockchains have been widely used for IoT systems to secure data management [22]. As the authors emphasized, most existing works have ignored user privacy, which can cause severe privacy issues. As per the authors, privacy concerns may limit the wide use of IoT systems in any domain [22]. The authors have proposed a Policy-hidden Fine-grained Redactable Blockchain (PFRB) solution to cover the research gap [22]. This solution allows users to match the existing blockchain policies and policy contents. As the authors have highlighted, PFRB is successful against plaintext attacks. The authors have used the Policy-based Chameleon Hash technique (PCH) to design the PFRB [22]. Also, the authors have emphasized the practical use case scenario of PFRB in smart healthcare systems.

According to Peter W. Eklund, Distributed Ledger Technologies (DLTs) represent a new digital ecosystem that can be a possible solution for limitations in traditional cyber-physical systems [23]. Authors have investigated the scalability limitations of different blockchain networks, including Bitcoin, Hyperledger Fabric, Multichain, and Ethereum. As the authors have emphasized, the throughput of different blockchain networks varies based on their architecture [23]. Also, the response time of blockchain networks can be over 500 s. According to the results of the paper, the throughput of some blockchain networks may reach 660,000 blocks per second, while others reach 3–5 blocks per second [23].

According to Enrico Corradini et al., IoT has become pervasive in day-to-day life. As the authors have highlighted, the protection of smart devices and their autonomy are the most significant challenges [24]. However, researchers have identified the blockchain as a possible solution to address those concerns. In this paper, the authors have proposed a two-tier blockchain framework to enhance the autonomy and security of IoT smart devices. The authors have grouped the IoT smart devices into two groups [24]. The first-tier blockchain operates locally, while the second-tier stores transaction values. The authors have considered smart home contexts with lower physical space and criticality. The authors have used suitable trust and reputation-measurement techniques to assess the reliability of IoT smart devices [24]. Also, the authors have used blockchain technology to certify transactions and to identify the anomaly behaviors of smart objects. The first tier implements a local IoT solution, while the second tier concerns the whole global IoT system. As per the authors, this approach guarantees the security of community interactions while dealing with potential inter-community attacks [24]. The test results are stored in the local blockchain. Also, the authors expect to address the security goals of confidentiality, integrity, and availability concerns by this new approach [24].

In the study conducted by Tomasz Hyla et al., it was emphasized that as cyber-attacks and cybercrimes continue to evolve, it is crucial to ensure the security of digital health systems and have a mechanism in place to identify abnormal behaviours within these systems [25]. The authors propose that a permissioned blockchain architecture can effectively safeguard electronic health systems, providing reliability and accountability. Additionally, modern blockchain applications are designed to detect anomalous behaviours in blockchain networks, making it feasible to utilize blockchain technology in sensor networks to enhance data integrity and accountability [25]. This can be achieved through the implementation of an integrity-protection service model, which aims to ensure transparency in blockchain transactions within a permissioned network. By implementing this model in a sensor network, both security and performance aspects can be assessed [25].

According to Ashutosh Dhar Dwivedi et al., medical data security and the secure transmission of health information have become vital components of analysing medical big data [26]. As per the authors, the development of IoT technologies has led to the advancement of medical big data mining and analysis. These technologies utilize health sensors based on IoT to gather patient data for analysis. The authors have mentioned that health sensors are interconnected through the internet, forming IoT-based health sensor networks [26]. However, sensitive health information and health systems remain targets for cyber threats. The occurrence of cyber-attacks poses challenges to data integrity and accountability. To address this issue, blockchain technology has been proposed as a potential solution for protecting sensitive information against cyber-attacks by the authors [26]. The utilization of blockchain technology helps to mitigate privacy and confidentiality risks, as all block data transactions are safeguarded using encryption algorithms [26].

The purpose of the literature review is to show that there is a gap in the literature that this paper fills, as only a limited number of research papers have been published regarding scalability. Also, there has been very little research conducted to evaluate blockchain scalability using real test systems. Most existing related works have missed the importance of scalability that may occur in real blockchain systems. To bridge this gap, we have developed a blockchain-based sensor network to evaluate the scalability concerns. Our test results show the blockchain network parameters, including the blockchain architecture and number of users, can impact the scalability factor of blockchain networks.

Our approach is based on experiments using real systems that can be used as a reference to develop similar blockchain-based sensor networks that consider scalability issues. Although researchers have identified blockchain as a potential security solution for IoT sensor networks, most existing blockchain applications are incompatible with commercially available IoT low-powered devices. We consider this a critical concern in this research paper, and our study shows that every blockchain application is not a possible solution for IoT low-powered devices. We discuss the research methodology and test bed development of the blockchain network prototype in the next section.

## 5. Research Methodology

The methodology of this research is a hybrid research methodology. This study has used test bed experimental results and quantitative analysis methods. A real test bed was used to collect experimental scalability data and evaluate data using statistical software tools [27]. This research aims to analyse the scalability limitations of blockchain-based IoT sensor networks that can lead to network bottlenecks [28]. To evaluate the scalability limitations of each blockchain network, we have upscaled the blockchain network from seven blockchain nodes to twenty blockchain nodes. We have used the sensor network latency, block transaction rate, and network bandwidth as the key evaluation parameters. High latency and bandwidth usage can cause failures in low-powered sensor networks used in the IoT, consequently impacting network performance efficiency [29]. Therefore, network latency and bandwidth are key parameters of network scalability to evaluate. We have used Linux MPSTAT, DSTAT tools, and the Wireshark program to collect network latency and bandwidth usage data [29]. Also, we have used blockchain application data logs to collect block transaction rate data as blockchain applications record all data block transactions. All experimental results were collected from the test bed in a lab environment, and we describe our test bed and resources in this section.

### *5.1. Blockchain Network Prototype*

All the experiments were conducted in a lab environment using the blockchain network prototype, and actual results were generated during the experiments. The architecture of the prototype blockchain network was developed using seven Raspberry Pi 3B and thirteen Orange Pi Zero devices [29]. Due to the supply shortage of Raspberry Pi devices, we had to use Orange Pi Zero devices as an alternative solution, and Orange Pi Zero devices also have similar specs to Raspberry Pi 3B devices and run the same operating

system [30]. We installed Hydrachain, Monero, and Duino coin blockchain algorithms on each single-board computer to compare the scalability limitations of each blockchain algorithm [29]. The main reasons behind choosing Hydrachain, Monero, and Duino coin blockchain platforms are the fewer hardware-software compatibility issues compared to other blockchain platforms, the low power consumption, the open-source platforms, and the flexible programmability [29]. Also, we have used low-powered sensors to collect sensor data and transmit them over the blockchain network. The blockchain network is connected over a wireless router [29]. Comparatively, IoT end devices and sensors are low-powered devices, as most IoT devices are battery-powered [29]. Power consumption is a critical consideration of this research, as blockchains are not feasible because they consume large amounts of power [29]. IoT devices are expected to survive for longer periods without a battery replacement [29]. Figure 2 shows a diagram of the prototype blockchain sensor network.

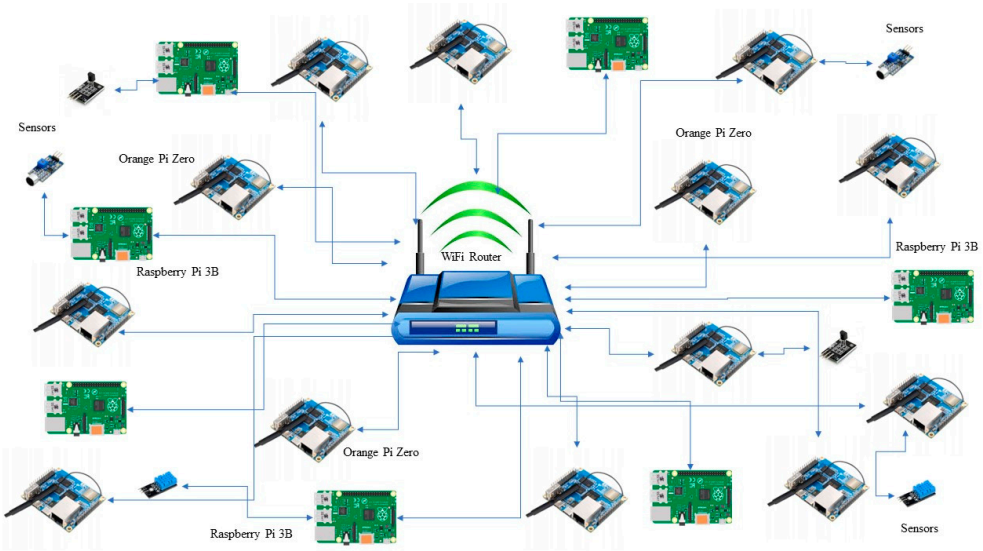


**Figure 2.** Prototype blockchain sensor network.

All blockchain algorithms are installed on an ARM-based Linux operating system and sensors are connected via General-Purpose Input–Output (GPIO) pins [30,31]. The main advantage of Hydrachain, Monero, and Duino coin applications is that users are able to implement their own private network [32,33]. However, to install Hydrachain, Monero, and Duino coin applications on ARM-based Linux operating systems, we had to install additional setup packages and Python libraries. A set of installation commands needed to be followed, and the Linux command line was used to insert application installation commands [34]. To install the Hydrachain, Monero, and Duino coin blockchain applications on single-board computer devices, essential Python library packages and github protocols are needed. Also, to run the Hydrachain blockchain application, "daemon tools" are essential. We have analysed the blockchain scalability limitations of three blockchain algorithms while scaling up the number of blockchain nodes [35].

### *5.2. Resources*

We provide an overview of hardware and software resources that we have used to develop our test bed in this section.

#### 5.2.1. Orange Pi

Orange Pi devices are open-source single-board computers powered by Allwinner H616 64-bit Quad core cortex A53 processor [30]. Also, Orange Pi devices consist of Mali G31 MP2 GPU and 512 MB or 1 GB DD3 RAM [30]. These devices support both Wi-Fi and ethernet networking features. Also, Orange Pi devices have Micro HDMI and 3.5 mm

audio support. Most Orange Pi devices are powered by a USB type C 5 V interface and provide USB 2.0 input and output ports [30].

Orange Pi single-board computers are supported by most ARM-based Linux versions, such as Ubuntu, Debian, and Android. Orange Pi also has a wide range of products, from Zero to Orange Pi 5B. The hardware capabilities and software support of these devices can vary [30]. However, Orange Pi is also a widely used single-board computer for prototyping and creative innovations. Some Orange Pi devices are equipped with Bluetooth 5.0. The Orange Pi Zero devices consist of 39 pin headers for General-Purpose Input–Output (GPIO), Universal Asynchronous Receiver Transmitter (UART), and Serial Peripheral Interface (SPI) [30].

#### 5.2.2. Raspberry Pi

Raspberry Pi is a single-board computer series developed by the Raspberry Pi Foundation. Raspberry Pi devices are integrated with ARM-compatible CPU architecture and powered by ARM Linux operating systems [31]. The common ARM Linux operating systems that can be installed on Raspberry Pi devices are Ubuntu, Raspbian, RetroPi, and Manjaro. The Raspberry Pi board series started from Raspberry Pi Pico to Raspberry Pi 4 model B. Raspberry Pi contains a Broadcom CPU [31]. Raspberry Pi full computer devices typically consist of all necessary RAM, USB, and LAN connections that can be used to implement a complete network. Raspberry Pi devices have 40 GPIO pins to connect sensors and actuators physically [31].

#### 5.2.3. Hydrachain Blockchain

The Hydrachain blockchain is an open-source blockchain platform developed as an Ethereum blockchain extension. The Hydrachain blockchain contains its consortium blockchain setup and provides private blockchain network services [32]. Also, the Hydrachain blockchain algorithm is a programmable blockchain platform that can be used to set up its own private blockchain network [32]. The Hydrachain blockchain also has a decentralized network architecture and uses Hydra Bridge Defenders to identify anomalies of the connected blockchain nodes. Hydrachain is compatible with all widely used operating systems, including Microsoft Windows and Linux [32].

#### 5.2.4. Monero Blockchain

The Monero blockchain is also an open-source blockchain platform that provides a decentralized network architecture. Monero blockchains also use a publicly distributed ledger as the core ledger system [33]. The Monero blockchain was developed using a Cryptonote protocol and validates data transactions over a network called RandomX. The Monero blockchain algorithm uses ring signatures to validate blocks and uses stealth IP addresses to hide legitimate IP addresses [33]. The Monero blockchain is also compatible with all widely used operating systems, including IOS, Microsoft Windows, and Linux [33].

#### 5.2.5. Duino Coin Blockchain

The Duino coin blockchain is a newly emerged blockchain solution specifically designed for low-powered computing devices, including Arduino, ESP32, ESP8266, and Raspberry Pi [34]. The Duino coin blockchain algorithm has been developed using DUCO-S1 and XXHASH programs to operate the blockchain algorithm on low-powered devices. The Duino coin blockchain is also an open-source blockchain platform that provides programmable interfaces [34]. The Duino coin blockchain algorithm uses the SHA-1 encryption algorithm to encrypt blocks.

### *5.3. Data Collection Parameters*

We provide an overview of data-collection parameters that we have used to collect data using our experimental test bed.

#### 5.3.1. Network Latency

Network latency is the term used to describe the delay in transmitting data within a blockchain network. It represents the amount of time it takes for blocks to be delivered across the network. Blockchain networks that have longer delays will experience higher latency [36]. This increased latency can result in failure for low-powered sensor networks that are utilized in the Internet of Things (IoT), which in turn affects the overall efficiency of the network's performance [36]. As a result, assessing network latency is a crucial factor in determining the scalability of a network.

#### 5.3.2. Bandwidth Usage

Network bandwidth is the maximum data rate or capacity at which data can be transferred within a network [36]. It is determined by the number of data that can be transmitted over a blockchain network within a specific time period. Bandwidth is commonly measured in bits per second (bps) [36,37]. The network bandwidth plays a critical role in determining the speed at which sensor data can be transmitted and received over the blockchain network [37]. Consequently, evaluating the blockchain network's bandwidth is an essential factor in assessing network scalability.

#### 5.3.3. Data Transaction Rate

The block transaction rate (BTR) is the number of blocks transferred between blockchain nodes during a specific time frame [37]. The BTR is usually measured in blocks per second. In a low-powered Internet of Things blockchain sensor network, the rate at which data are transmitted is crucial to avoid network failures due to performance problems with the blockchain algorithm. However, it is necessary to assess the block transaction rate in order to comprehend the varying data-transmission rates of various blockchain algorithms [37]. We discuss the results and evaluation in the next section.

## 6. Results and Evaluation

In this section, we analyse the scalability limitations of the Hydrachain, Monero, and Duino coin blockchain networks. Also, we scaled up the blockchain network from seven blockchain nodes to twenty blockchain nodes. We analyse the scalability of blockchain networks via the latency, bandwidth, and block transaction rate parameters [38].

### *6.1. Blockchain Network Latency Analysis*

In this section, we analyse the network latency using our test bed. We used seven blockchain nodes, fifteen blockchain nodes, and twenty blockchain nodes to measure the latency of different blockchain networks. Figure 3 shows blockchain networks' latency variability in terms of blockchain network run time.

The results in Figure 3 show that the latency of the seven Hydrachain blockchain network is less than 300 ms. The network with fifteen blockchain nodes has indicated a latency between 300 ms and 400 ms. Also, the graph shows over 400 ms of network latency with twenty blockchain nodes [39]. This indicates the increment of blockchain nodes causes the increment of the Hydrachain blockchain's network latency.

As per the results in Figure 3, the Monero blockchain algorithm has indicated higher latency than the Hydrachain blockchain algorithm. As Figure 3 shows, the network with seven blockchain nodes has a latency between 400 and 600 ms. Also, the network with fifteen blockchain nodes has a latency between 600 and 800 ms. The network with twenty blockchain nodes has over 800 ms of network latency. This shows us that the Monero blockchain algorithm also increases the latency by increasing the number of nodes [39].

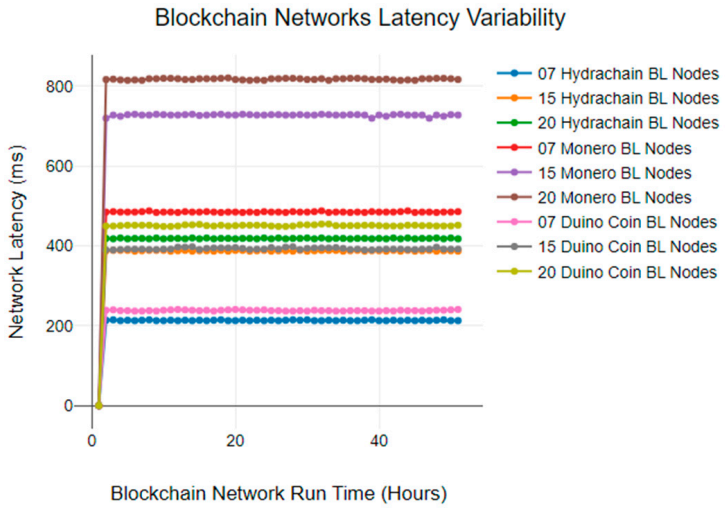


**Figure 3.** Latency variability of blockchain networks.

Also, as the results in Figure 3 show, the latency of the Duino coin blockchain network is lower than the Monero blockchain algorithm. As the figure indicates, the network with seven blockchain nodes has a latency of 200 ms to 300 ms. Also, the network with fifteen blockchain nodes shows a latency close to 400 ms. The network with twenty blockchain nodes has over 400 ms of latency. Figure 4 shows the latency standard deviations of blockchain networks.

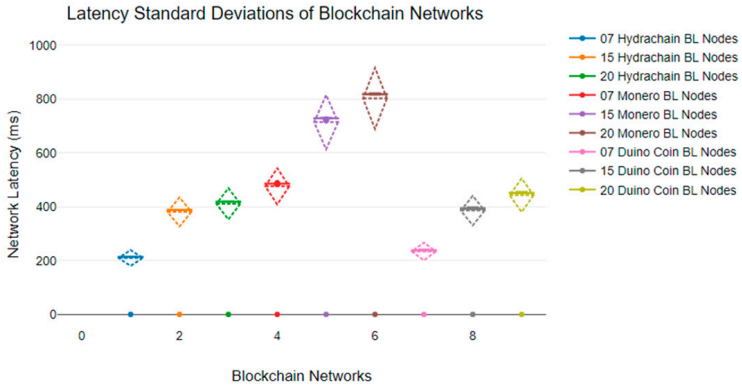


**Figure 4.** Latency standard deviations of blockchain networks.

The box plot graph in Figure 4 indicates the standard deviations of the blockchain networks' latency results with the box bounding the 25% and 75% percentiles. As per the results, the upper bound of the network with seven Hydrachain blockchain nodes is 215 ms, and the lower bound is 213 ms. The upper bound of the network with fifteen Hydrachain nodes is 389 ms, and the lower bound is 387 ms. Also, the network with twenty blockchain nodes has an upper bound of 420 ms and a lower bound of 418 ms.

The upper bound of the network with seven Monero blockchain nodes is 488 ms, and the lower bound is 485 ms. The upper bound of the network with fifteen Monero blockchain nodes is 730 ms, and the lower bound is 727 ms. Also, the upper bound of the Monero network with twenty blockchain nodes is 821 ms, and the lower bound is 815 ms.

The network with seven Duino coin blockchain nodes has an upper standard deviation bound of 241 ms and a lower bound of 237 ms. Also, the upper bound of the network with fifteen Duino coin blockchain nodes is 398 ms, and the lower bound is 391 ms. Also, the upper bound of the network with twenty Duino coin blockchain nodes is 455 ms, and the lower bound is 449 ms. Figure 5 shows the mean network latency in terms of the number of blockchain nodes [39].

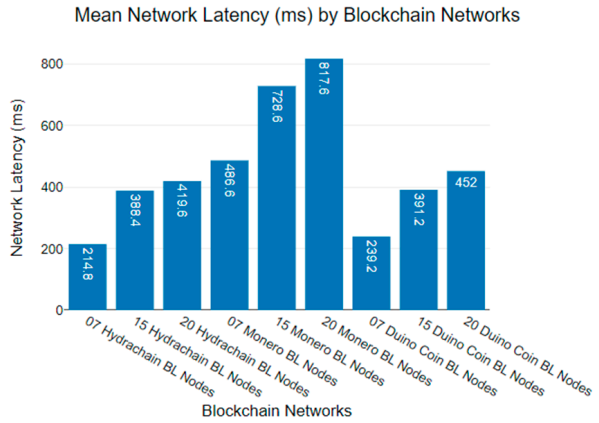


**Figure 5.** Mean blockchain networks latency variability.

As the results indicate, the mean latency of the seven-node Hydrachain blockchain network is 214.8 ms. The mean latency of the fifteen-node blockchain network is 388.4 ms, and the graph shows 419.6 ms latency for the network with twenty blockchain nodes [40].

As Figure 5 indicates, the network with seven Monero blockchain nodes has 486.6 ms of mean latency. Also, the blockchain network with fifteen blockchain nodes has 728.6 ms of mean latency, and the network with twenty blockchain nodes shows 817.6 ms mean latency [40]

The results in Figure 5 indicate that the mean network latency of the seven-node Duino coin blockchain network is 239.2 ms and the network with fifteen blockchain nodes has 391.2 ms of latency. Also, the network with twenty blockchain nodes shows 452 ms of latency. These results show that the latency has increased with the increment of the Duino coin blockchain nodes [40].

Figure 6 shows the overall mean network latency of the blockchain network. This analysis indicates that the increase in blockchain users causes an increase in the latency of the blockchain network. In summary, the Hydrachain blockchain algorithm shows the lowest network latency, and the Monero blockchain shows the highest network latency.

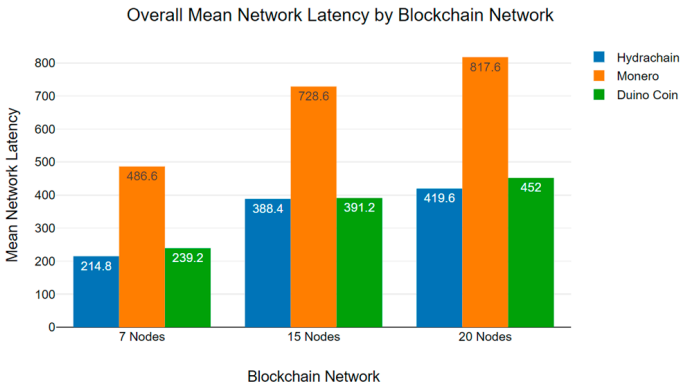


**Figure 6.** Overall mean latency of the networks.

Table 1 shows the network latency data sample of the Hydrachain, Monero and Duino coin blockchain networks. As Table 1 indicates, the network latency increases with the increase in the number of blockchain users. In the next section, we discuss the network bandwidth of three blockchain algorithms [41].

**Table 1.** Network latency data sample of blockchain networks.

| Hydrachain | | | Monero | | | Duino Coin | | |
|---|---|---|---|---|---|---|---|---|
| **07 Nodes** | **15 Nodes** | **20 Nodes** | **07 Nodes** | **15 Nodes** | **20 Nodes** | **07 Nodes** | **15 Nodes** | **20 Nodes** |
| 214 ms | 388 ms | 419 ms | 485 ms | 720 ms | 817 ms | 239 ms | 390 ms | 450 ms |
| 215 ms | 389 ms | 418 ms | 486 ms | 728 ms | 818 ms | 240 ms | 390 ms | 450 ms |
| 213 ms | 389 ms | 420 ms | 485 ms | 725 ms | 816 ms | 238 ms | 391 ms | 451 ms |
| 214 ms | 389 ms | 418 ms | 485 ms | 729 ms | 815 ms | 238 ms | 392 ms | 452 ms |
| 213 ms | 387 ms | 419 ms | 485 ms | 730 ms | 816 ms | 237 ms | 392 ms | 452 ms |
| 214 ms | 388 ms | 419 ms | 486 ms | 728 ms | 815 ms | 237 ms | 392 ms | 452 ms |
| 215 ms | 389 ms | 418 ms | 488 ms | 728 ms | 819 ms | 238 ms | 391 ms | 452 ms |
| 213 ms | 389 ms | 420 ms | 484 ms | 730 ms | 819 ms | 237 ms | 391 ms | 450 ms |
| 213 ms | 389 ms | 418 ms | 485 ms | 729 ms | 820 ms | 239 ms | 392 ms | 449 ms |
| 214 ms | 387 ms | 419 ms | 485 ms | 728 ms | 820 ms | 240 ms | 392 ms | 449 ms |

### *6.2. Blockchain Network Bandwidth Usage Analysis*

This section discusses the bandwidth usage of the Hydrachain, Monero, and Duino coin blockchain networks. Bandwidth is an essential parameter to assess the scalability of blockchain networks. We used blockchain networks with seven nodes, fifteen nodes, and twenty nodes to measure the bandwidth. Figure 7 shows the bandwidth usage of the Hydrachain blockchain networks in terms of the number of blockchain nodes [41].

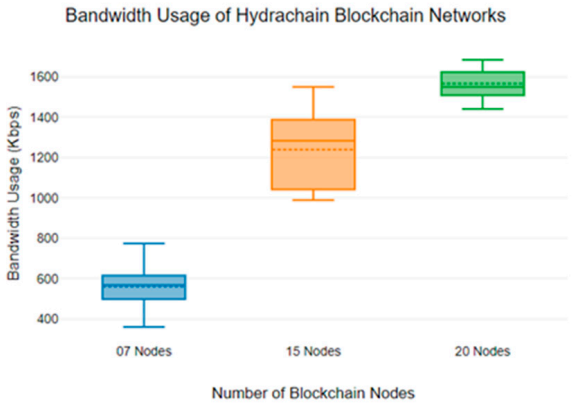


**Figure 7.** Hydrachain blockchain bandwidth usage.

As per the results in Figure 7, the bandwidth usage of the seven-node Hydrachain blockchain network varies between 400 Kbps and 800 Kbps. The Hydrachain blockchain network with fifteen nodes has a bandwidth usage from 1000 Kbps to 1600 Kbps. The network with twenty blockchain nodes has a bandwidth usage between 1400 Kbps and 1600 Kbps. With the results, we can emphasize that bandwidth usage increases with the increase in blockchain nodes.

Figure 8 shows the bandwidth usage of Monero blockchain networks. As per the results, the Monero network with seven blockchain nodes has a bandwidth usage deviation from 40 Kbps to 60 Kbps. Also, the network with fifteen Monero blockchain nodes has a bandwidth variation between 100 Kbps and 140 Kbps. The network with twenty blockchain nodes has a bandwidth usage between 80 Kbps and 160 Kbps [42]. These results show that the number of blockchain users causes the increment in bandwidth usage. Also, Monero blockchain networks' bandwidth usage is lower than the Hydrachain blockchain networks.

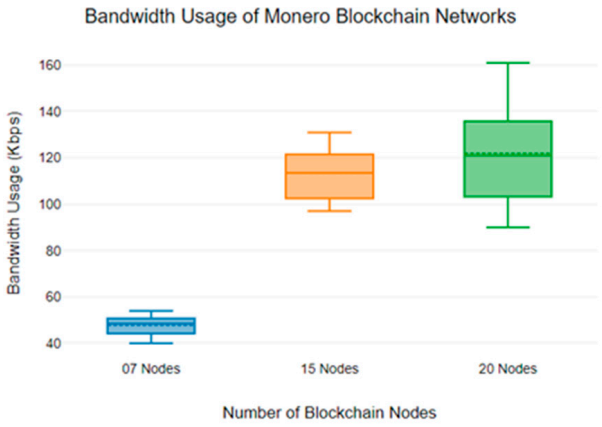


**Figure 8.** Monero blockchain bandwidth usage.

As Figure 9 shows, the bandwidth usage of the seven-node Duino coin blockchain network is 50 Kbps, and the network with fifteen nodes has a bandwidth deviation between 100 Kbps and 200 Kbps. Also, the network with twenty Duino coin blockchain nodes has a bandwidth deviation from 50 Kbps to 300 Kbps. These results show that the Duino coin blockchain networks have a lower bandwidth usage than the Hydrachain blockchain networks and a higher bandwidth usage than the Monero blockchain networks. Also, as results indicate, the bandwidth usage increases with the increase in blockchain network users [42].

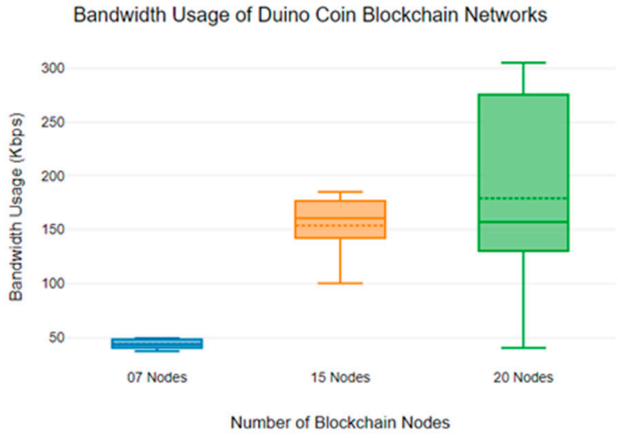


**Figure 9.** Duino coin blockchain bandwidth usage.

As Figure 10 shows, the mean bandwidth usage of the Hydrachain blockchain deviates from 559.6 Kbps to 1566.3 Kbps. The network with twenty blockchain nodes has the maximum mean bandwidth usage of 1566.3 Kbps. The network with seven blockchain nodes has the minimum mean bandwidth usage, which is 559.6 Kbps. The network with fifteen blockchain nodes has a mean bandwidth usage of 1239.2 Kbps [42].

As shown in Figure 10, the mean bandwidth usage of the Monero blockchain networks deviates from 47.8 Kbps to 121.9 Kbps. The maximum mean bandwidth usage was recorded as 121.9 Kbps at the network with twenty blockchain nodes, and the minimum was recorded as 47.8 Kbps at the network with seven blockchain nodes. The network with fifteen Monero blockchain nodes has a mean bandwidth usage of 113.5 Kbps [42].

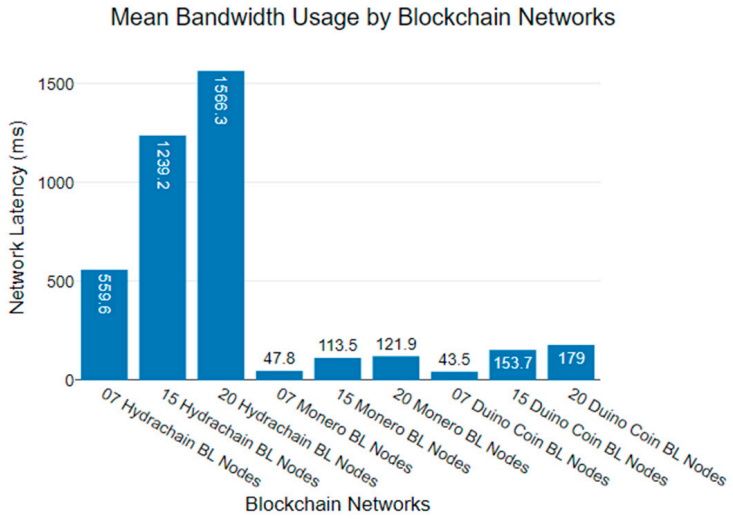


**Figure 10.** Mean blockchain network bandwidth usage.

As per the results in Figure 10, the network bandwidth of seven Duino coin blockchain nodes varies from 43.5 Kbps to 179 Kbps. The maximum bandwidth usage was recorded as 179 Kbps at the network with twenty Duino coin blockchain nodes, and the minimum was recorded as 43.5 Kbps at the network with seven blockchain nodes. The network with fifteen blockchain nodes has a mean bandwidth usage of 153.7 Kbps. Figure 10 summarizes all three blockchain algorithms' overall mean bandwidth usage [43].

As Figure 11 shows, the Hydrachain blockchain network has the highest bandwidth usage, and comparatively, the Monero blockchain algorithm has the lowest bandwidth usage. In summary, we can emphasize that the number of blockchain nodes or users affects bandwidth usage. The type of blockchain algorithm also causes bandwidth usage variations that can limit the scalability of blockchain networks.

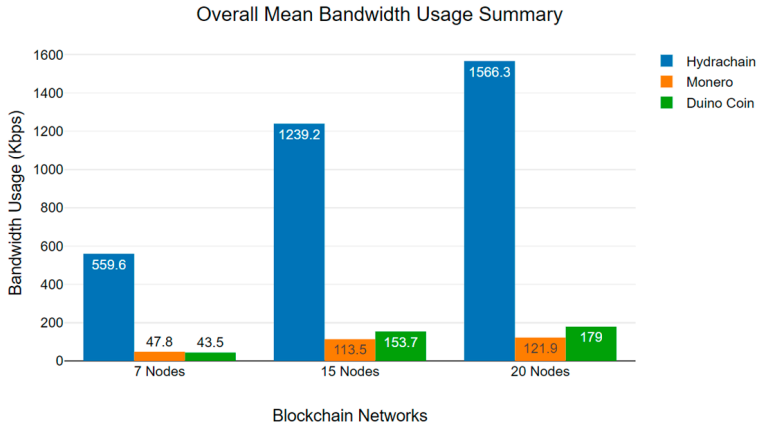


**Figure 11.** Overall mean blockchain network bandwidth usages.

Table 2 indicates a bandwidth usage data sample of Hydrachain, Moner, and Duino coin blockchain networks. As per the results, we can emphasize that the bandwidth usage of blockchain networks increases with the increase in the number of nodes. We discuss the variance of each blockchain network's block transaction rate in the next section.

**Table 2.** Bandwidth usage data sample of blockchain networks.

| Hydrachain | | | Monero | | | Duino Coin | | |
|---|---|---|---|---|---|---|---|---|
| **07 Nodes** | **15 Nodes** | **20 Nodes** | **07 Nodes** | **15 Nodes** | **20 Nodes** | **07 Nodes** | **15 Nodes** | **20 Nodes** |
| 410 Kbps | 1125 Kbps | 1655 Kbps | 43 Kbps | 112 Kbps | 120 Kbps | 51 Kbps | 100 Kbps | 155 Kbps |
| 628 Kbps | 1245 Kbps | 1548 Kbps | 49 Kbps | 119 Kbps | 128 Kbps | 49 Kbps | 112 Kbps | 143 Kbps |
| 553 Kbps | 1157 Kbps | 1577 Kbps | 53 Kbps | 124 Kbps | 136 Kbps | 49 Kbps | 128 Kbps | 115 Kbps |
| 498 Kbps | 1148 Kbps | 1471 Kbps | 48 Kbps | 120 Kbps | 154 Kbps | 48 Kbps | 147 Kbps | 149 Kbps |
| 673 Kbps | 1302 Kbps | 1470 Kbps | 46 Kbps | 127 Kbps | 138 Kbps | 50 Kbps | 140 Kbps | 144 Kbps |
| 768 Kbps | 1024 Kbps | 1489 Kbps | 46 Kbps | 110 Kbps | 133 Kbps | 50 Kbps | 143 Kbps | 78 Kbps |
| 728 Kbps | 1268 Kbps | 1602 Kbps | 51 Kbps | 111 Kbps | 158 Kbps | 51 Kbps | 157 Kbps | 280 Kbps |
| 612 Kbps | 1459 Kbps | 1631 Kbps | 52 Kbps | 133 Kbps | 155 Kbps | 49 Kbps | 159 Kbps | 245 Kbps |
| 558 Kbps | 1468 Kbps | 1624 Kbps | 47 Kbps | 128 Kbps | 157 Kbps | 48 Kbps | 166 Kbps | 251 Kbps |
| 790 Kbps | 1520 Kbps | 1659 Kbps | 45 Kbps | 131 Kbps | 129 Kbps | 49 Kbps | 154 Kbps | 267 Kbps |

### *6.3. Block Transaction Rate Analysis*

Block transaction rate (BTR) denotes the number of blocks that move from one blockchain node to another in a unit of time [44]. BTR is measured in blocks per second. In a low-powered IoT blockchain sensor network, the block transaction rate is critical to avoid network failures. In this section, we evaluate the blockchain transaction rates of each blockchain network using the same test bed.

As per the results in Figure 12, the Hydrachain blockchain network with seven blockchain nodes has 25 to 26 block transactions per second. The first blockchain node has a mean block transaction rate of 25.43 blocks per second, while the second node has a mean block transaction rate of 25.57 blocks per second. The third and fourth blockchain nodes have mean block transaction rates of 25.86 and 25.29 blocks per second, respectively, while the fifth and sixth nodes have mean block transaction rates of 25.57 and 25.71 blocks per second, respectively. The seventh node recorded a mean block transaction rate of 25.86 blocks per second [44].

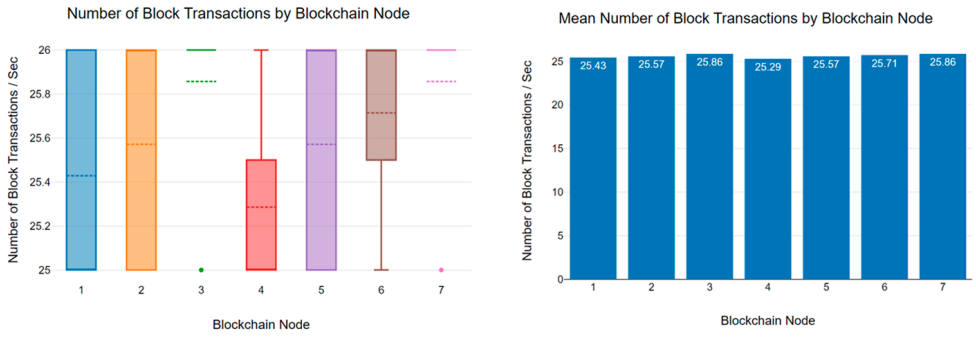


**Figure 12.** Block transaction rate of 7 Hydrachain blockchain nodes.

As the results indicate in Figure 13, the block transaction rate of the Hydrachain network with fifteen blockchain nodes deviates from 19 blocks per second to 22 blocks per second. The first, second, and third blockchain nodes have mean block transaction rates of 19.86, 20.57, and 20.43 blocks per second, respectively. Also, the fourth, fifth, and sixth nodes have mean block transaction rates of 20.57, 21.14, and 20.14 blocks per second, respectively. The 7th, 8th, and 9th nodes have a mean block transaction rates of 19.43, 19.43, and 20 blocks per second, respectively, while the 10th, 11th, and 12th nodes have a mean block transaction rate of 20.71, 20.67, and 21.29 blocks per second, respectively. The 13th, 14th, and 15th nodes have a mean block transaction rate of 19.33, 19.43, and 20.57 blocks per second.

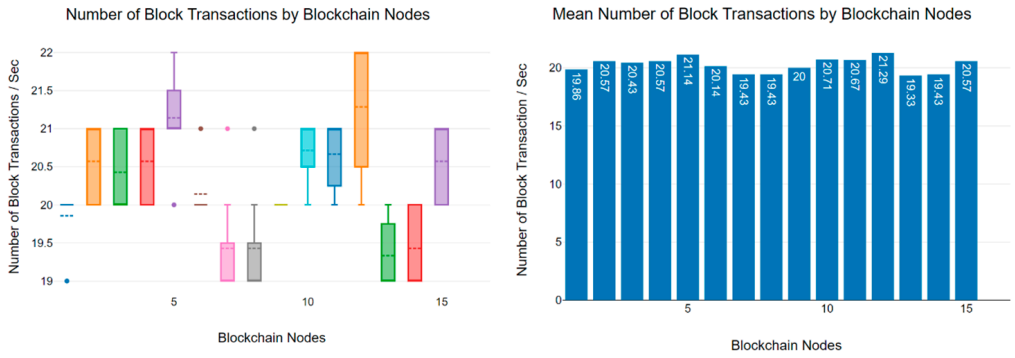


**Figure 13.** Block transaction rate of 15 Hydrachain blockchain nodes.

The results in Figure 14 indicate that the block transaction rate of the network with twenty Hydrachain blockchain nodes deviates from 12 blocks per second to 20 blocks per second. From the 1st node to the 5th node, the network has mean block transaction rates of 19.43, 15, 16.43, 14.43, and 15.71 blocks per second, while from the 6th node to the 10th node, the network has a mean block transaction of 16.86, 18.43, 16.43, 17.43, and 15.29 blocks per second, respectively. Also, from the 11th node to the 15th node, the network has a mean block transaction rate of 15.14, 18.71, 15.14, 15, and 18 blocks per second, while from the 16th node to the 20th node has a mean block transaction rate of 18, 16.29, 16.86, 15.57 and 18.57 blocks per second, respectively.

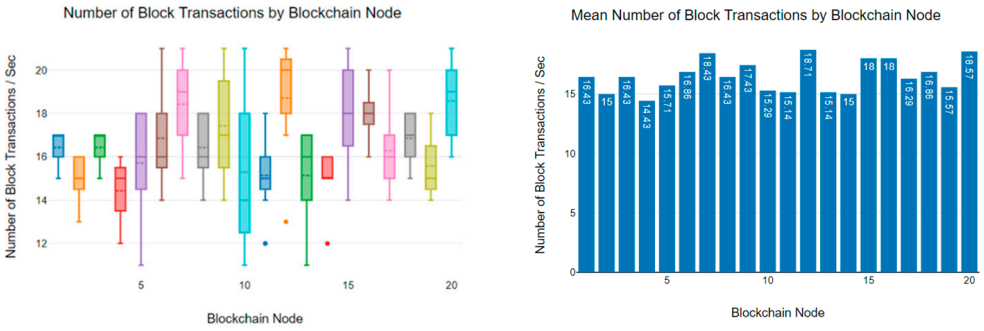


**Figure 14.** Block transaction rate of 20 Hydrachain blockchain nodes.

Figure 15 shows the number of block transactions per second by seven Monero blockchain nodes. As the results indicate, the Monero blockchain network with seven blockchain nodes transmits 50–100 blocks per second over the blockchain network. The results show that the Monero blockchain algorithm transmits more blocks than the Hydrachain blockchain algorithm. The first and second blockchain nodes have mean block transaction rates of 75.71 and 66.86 blocks per second, respectively, while the third and fourth blockchain nodes have recorded mean block transaction rates of 83.86 and 78.43 blocks per second, respectively. Also, the fifth and sixth blockchain nodes have mean block transaction rates of 78.43 and 70 blocks per second, respectively, while the seventh node has a mean block transaction rate of 75 blocks per second [44].

As per the results shown in Figure 16, the block transaction rate of the network with fifteen Monero blockchain nodes deviates from 35 to 75 blocks per second. Compared to the network with seven blockchain nodes, the block transaction rate of the fifteen blockchain node network was decreased. This indicates that with the increase in the number of blockchain users of the Monero blockchain network, the block transaction rate decreases. As the results show, the first, second, and third blockchain nodes have mean block transaction rates of 43.29, 47.71, and 43.14, while the fourth, fifth, and sixth nodes have mean block transaction rates of 59.43, 47, and 46.29 blocks per second, respectively. Also, from node 7 to node 10, the mean block transaction of the network was recorded as

50.29, 53.29, 41.29, and 51.43 blocks per second. The blockchain nodes 11 to 15 have mean block transaction rates of 51.57, 49.71, 48, 47.14, and 48.14 blocks per second, respectively.

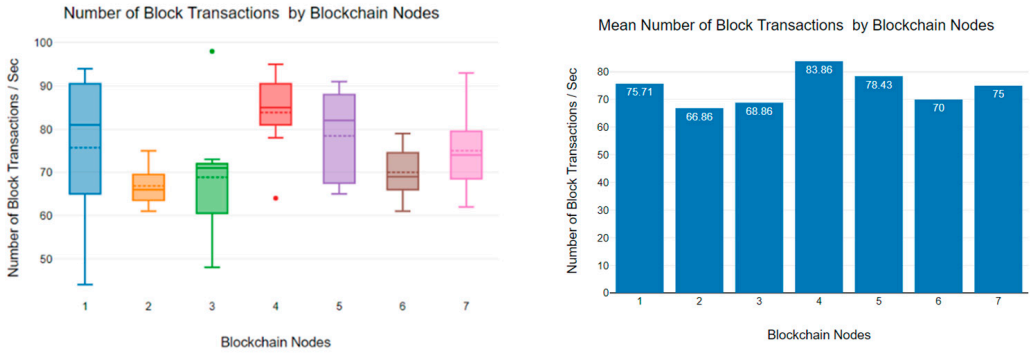


**Figure 15.** Block transaction rate of 7 Monero blockchain nodes.

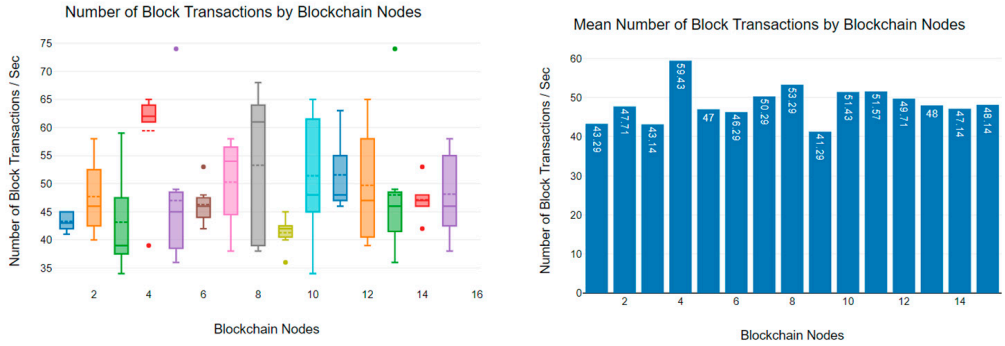


**Figure 16.** Block transaction rate of 15 Monero blockchain nodes.

Figure 17 shows the analysed results of the block transaction rate with twenty Monero blockchain nodes, and the results indicate that the block transaction rate deviates from 25 blocks per second to 50 blocks per second. We can highlight that compared to the fifteen-node blockchain network, there is a decrement in the block transaction rate when scaling up the blockchain network. Also, from the 1st blockchain node to the 5th blockchain node, the mean block transaction rates were recorded as 35.86, 31, 33.71, 39.14, and 38.14 blocks per second, while the mean block transaction rates of nodes from 6 to 10 were recorded as 30.86, 35.14, 28.71, 29 and 39 blocks per second. From the 11th node to the 15th node, the block transaction rates were recorded as 44.14, 32.43, 32, 30, and 31.43 blocks per second, while the mean block transaction rates of nodes 16th, 17th, 18th, 19th, and 20th were noted as 34.14, 36.57, 41.43, 33.71 and 33.57 blocks per second, respectively.

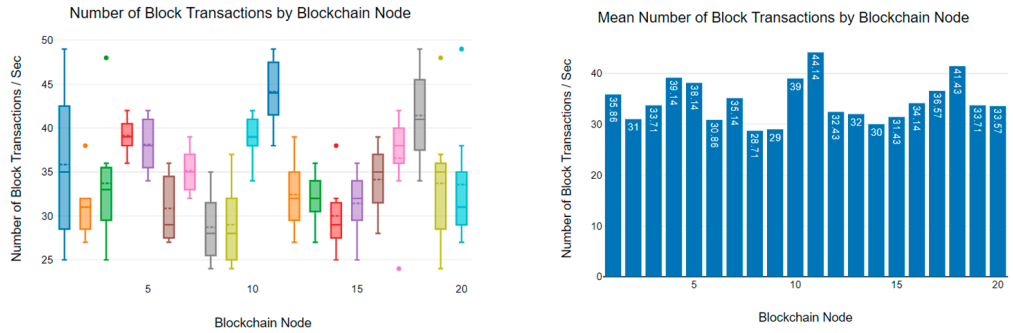


**Figure 17.** Block transaction rate of 20 Monero blockchain nodes.

As the results in Figure 18 show, the block transaction rate of the seven-node Duino coin blockchain network deviated from 54 blocks per second to 64 blocks per second. The

Duino coin network recorded a lower block transaction rate than the Monero blockchain network. However, the Duino coin block transactions rate is higher than the Hydrachain block transaction rate. As per the results in Figure 18, the first blockchain node has a mean block transaction rate of 59.29, while the second and third nodes have mean block transaction rates of 60 and 58.86 blocks per second, respectively. The fourth and fifth Duino coin blockchain nodes have mean block transaction rates of 61.43 and 62 blocks per second, while the sixth and seventh nodes have mean block transaction rates of 59.43 and 62.29 blocks per second, respectively.

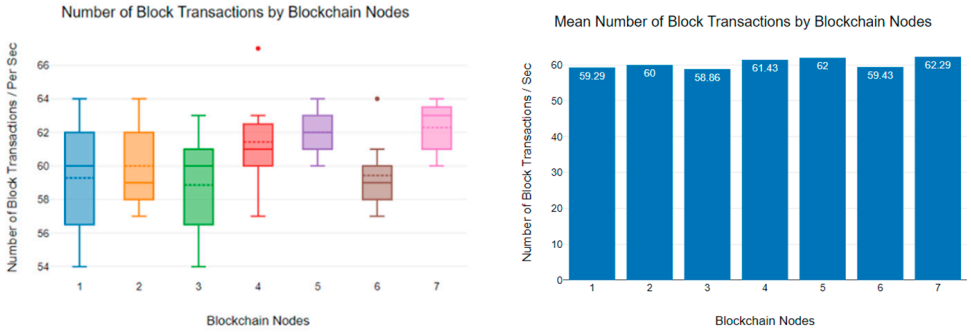


**Figure 18.** Block transaction rate of 7 Duino coin blockchain nodes.

Also, as per the results shown in Figure 19, the block transaction rate of the network with fifteen Duino coin blockchain nodes has a deviation from 10 to 50 blocks per second. The mean block transaction rates of first five nodes were recorded as 25, 26.29, 32.86, 26.86, and 31.57 blocks per second. The nodes from 6 to 10 have mean block transaction rates of 24, 27.14, 24.14, 30.71, and 27.14 blocks per second, respectively. Also, from the 11th node to the 15th node, the mean block transaction rates were recorded as 24.14, 26.71, 23.71, 35.14, and 30.5 blocks per second, respectively [45].

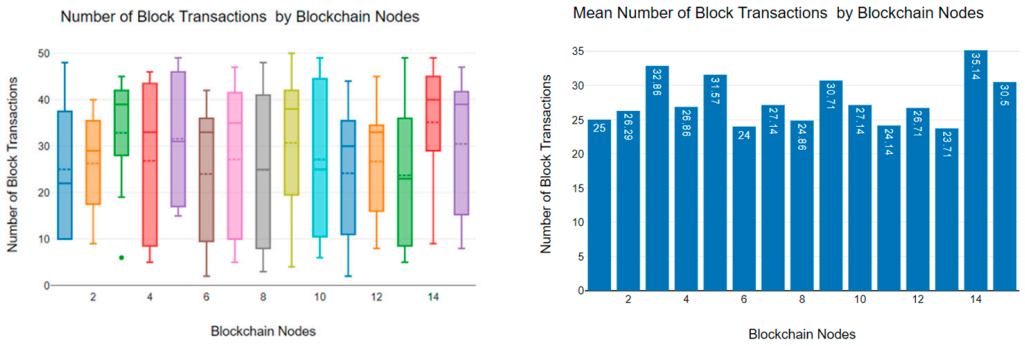


**Figure 19.** Block transaction rate of 15 Duino coin blockchain nodes.

The block transaction rate of the network with twenty Duino coin blockchain nodes in Figure 20 deviated from 14 to 26 blocks per second. As the results indicate, the mean block transaction rates of the blockchain nodes from the first blockchain node to the fifth node were recorded as 23.57, 23.71, 23, 20.71, and 21.43 blocks per second. Nodes 6 to 10 have mean block transaction rates of 16.43, 23.71, 21.29, 19, and 16.43 blocks per second. Also, the results show that nodes from 11 to 15 have mean block transaction rates of 23.43, 21.86, 24.43, 20.86, and 19.14 blocks per second while the 16th, 17th, 18th, 19th, and 20th nodes have mean block transaction rates of 20.57, 16.57, 22.29, 24.43 and 22.43 blocks per second. We can emphasize that the block transaction rate gradually decreases with the increase in blockchain nodes.

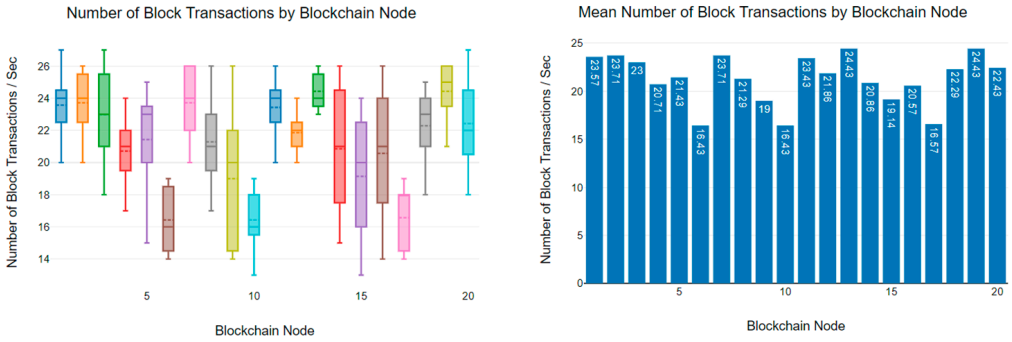


**Figure 20.** Block transaction rate of 20 Duino coin blockchain nodes.

Figure 21 summarizes the average mean block transactions through the blockchain network. As per the results, Monero blockchain networks reached higher block transaction rates compared to the Hydrachain and Duino coin blockchain networks. In summary, we can emphasize that the number of blockchain users affects the overall block transaction rate and the scalability of blockchain networks. Table 3 shows a data sample of the block transaction rates of the Hydrachain, Monero, and Duino coin blockchain networks.

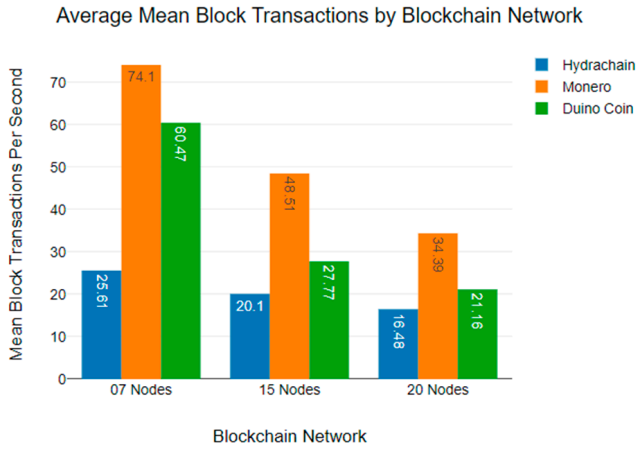


**Figure 21.** Summary of average mean block transaction rates.

**Table 3.** Sample of block transaction rate data of blockchain networks.

| Hydrachain | | | Monero | | | Duino Coin | | |
|---|---|---|---|---|---|---|---|---|
| **07 Nodes** | **15 Nodes** | **20 Nodes** | **07 Nodes** | **15 Nodes** | **20 Nodes** | **07 Nodes** | **15 Nodes** | **20 Nodes** |
| 25 | 21 | 13 | 53 | 39 | 28 | 61 | 15 | 14 |
| 25 | 21 | 19 | 51 | 45 | 33 | 56 | 21 | 18 |
| 25 | 20 | 17 | 67 | 38 | 30 | 63 | 17 | 15 |
| 25 | 20 | 18 | 73 | 61 | 31 | 60 | 13 | 14 |
| 26 | 22 | 14 | 62 | 64 | 28 | 64 | 15 | 23 |
| 25 | 21 | 14 | 65 | 55 | 40 | 58 | 28 | 16 |
| 25 | 21 | 14 | 81 | 52 | 34 | 57 | 19 | 26 |
| 26 | 21 | 15 | 70 | 59 | 32 | 62 | 24 | 15 |
| 25 | 19 | 18 | 74 | 60 | 44 | 55 | 21 | 22 |
| 25 | 22 | 18 | 66 | 64 | 31 | 62 | 20 | 22 |

As per the results, we can emphasize that the block transaction rate decreases with the increase in the node number. Most low-powered IoT applications use wireless technologies for data transmission, and the impact of network scalability limitations can be a critical consideration [46]. The deployment of blockchain-based sensor networks also faces the

impact of scalability limitations [46]. As per the results, the latency, bandwidth usage, and data block transaction rates vary based on the blockchain network architecture and number of users. The results indicate that the increment of blockchain nodes significantly increases the latency of blockchain networks. The deployment of blockchain-based IoT sensor networks in industries, including healthcare, is critical as the latency or loss of sensitive data can have significant consequences [46]. Also, the latency or loss of sensitive medical data can put lives at risk. It is important to understand the scalability capabilities of different blockchain networks before the deployment of blockchain-based IoT sensor networks in any industry [46]. The results of this research provide an overview of the scalability limitations that can occur with the use of Hydrachain, Monero, and Duino coin blockchain networks. However, the results will contribute toward preventing scalability bottlenecks of blockchain-based IoT sensor networks. Not only healthcare but also supply chain, automotive, and manufacturing sectors can be impacted by the scalability limitations of blockchain-based IoT sensor networks, and this research will help to overcome these scalability limitations [47]. We discuss the conclusions and future possible research avenues in the next section.

## 7. Conclusions and Future Research

The Internet of Things (IoT) and blockchain are emerging technologies that have raised many new research avenues. Blockchain technology holds substantial potential to protect low-powered IoT end devices [47]. However, integrating blockchain and IoT technologies raises several research questions, including scalability limitations. The integration of blockchain and IoT technologies may address many of the cyber security issues [48].

Little research has been conducted to identify the scalability limitations of blockchain-based, low-powered, wireless sensor networks [48]. We have analysed the scalability of Hydrachain, Monero, and Duino coin blockchain networks to contribute to this research gap. Based on the experimental results of the research, we can emphasize that the scalability of blockchain-based, low-powered sensor networks can vary due to the number of blockchain nodes and the type of blockchain algorithm [48].

The integration of blockchain and IoT opens future research possibilities. One of the possible new research avenues is the performance analysis of different blockchain algorithms on IoT single-board computers [49]. Another possible research area is the energy consumption of blockchain networks. The integrity and security anomaly detection of blockchain sensor networks would be another future research avenue. Finally, the scalability analysis of low-powered sensor networks may play a key role in addressing future IoT-based research issues [49].

**Author Contributions:** In this paper, the idea and primary evaluations were conducted by K.G.A., P.B. and J.B. supervised the experiments conducted and the analysis of the paper. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** All datasets generated during the study are available upon request from the primary author.

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

## References

1. Alam, S.; De, D. Analysis of Security Threats in Wireless Sensor Network. *Int. J. Wirel. Mob. Netw.* **2014**, *6*, 35–46. [CrossRef]
2. Dharani, A.; Khaliq-ur-Rehman Raazi, S.M. Integrating Blockchain with IoT for Mitigating Cyber Threat In Corporate Environment. In Proceedings of the 2022 Mohammad Ali Jinnah University International Conference on Computing (MAJICC), Karachi, Pakistan, 27–28 October 2022; pp. 1–6.

3. Alazzawi, L.; Elkateeb, A. Performance Evaluation of the WSN Routing Protocols Scalability. *J. Comput. Syst. Netw. Commun.* **2008**, *2008*, 481046. [CrossRef]
4. de Brito Gonçalves, J.P.; Spelta, G.; da Silva Villaça, R.; Gomes, R.L. IoT Data Storage on a Blockchain Using Smart Contracts and IPFS. In Proceedings of the 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 22–25 August 2022; pp. 508–511.
5. Godawatte, K.; Branch, P.; But, J. Use of blockchain in health sensor networks to secure information integrity and accountability. *Procedia Comput. Sci.* **2022**, *210*, 124–132. [CrossRef]
6. Roman, V.; Ordieres-Mere, J. [WiP] IoT Blockchain Technologies for Smart Sensors Based on Raspberry Pi. In Proceedings of the 2018 IEEE 11th Conference on Service-Oriented Computing and Applications (SOCA), Paris, France, 20–22 November 2018; pp. 216–220.
7. Forkan, A.R.M.; Branch, P.; Jayaraman, P.P.; Ferretto, A. An Internet-of-Things Solution to Assist Independent Living and Social Connectedness in Elderly. *Trans. Soc. Comput.* **2019**, *2*, 14. [CrossRef]
8. Tahir, M.; Sardaraz, M.; Muhammad, S.; Saud Khan, M. A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics. *Sustainability* **2020**, *12*, 6960. [CrossRef]
9. Hewa, T.; Gür, G.; Kalla, A.; Ylianttila, M.; Bracken, A.; Liyanage, M. The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions. In Proceedings of the 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 17–20 March 2020.
10. Yiyang, C.; Takashio, K. A Floating Calculation Revamp For the Ethereum Blockchain-Based IoT Systems. In Proceedings of the 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), Yokohama, Japan, 26 October–11 November 2022; pp. 1–6.
11. Huang, Z.; Su, X.; Zhang, Y.; Shi, C.; Zhang, H.; Xie, L. A Decentralized Solution for IoT Data Trusted Exchange Based-on Blockchain. In Proceedings of the 3rd IEEE International Conference on Computer and Communications, Chengdu, China, 13–16 December 2017.
12. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for Internet of Things. *Comput. Commun.* **2019**, *136*, 10–29. [CrossRef]
13. She, W.; Liu, Q.; Tian, Z.; Chen, J.-S.; Wang, B.; Liu, W. Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks. *IEEE Access* **2019**, *7*, 38947–38956. [CrossRef]
14. Kabir, R.; Hasan, A.S.M.T.; Islam, M.R.; Watanobe, Y. A Blockchain-based Approach to Secure Cloud Connected IoT Devices. In Proceedings of the 2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD), Dhaka, Bangladesh, 27–28 February 2021; pp. 366–370.
15. Moinet, A.; Darties, B.; Baril, J.-L. Blockchain based trust & authentication for decentralized sensor networks. *arXiv* **2017**, arXiv:1706.01730.
16. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT Integration: A Systematic Survey. *Sensors* **2018**, *18*, 2575. [CrossRef]
17. Liang, X.; Shetty, S.; Tosh, D.; Bowden, D.; Njilla, L.; Kamhoua, C. Towards Blockchain Empowered Trusted and Accountable Data Sharing and Collaboration in Mobile Healthcare Applications. *EAI Endorsed Trans. Pervasive Health Technol.* **2018**, *4*, e3. [CrossRef]
18. Novo, O. Scalable Access Management in IoT Using Blockchain: A Performance Evaluation. *IEEE Internet Things J.* **2019**, *6*, 4694–4701. [CrossRef]
19. Dwivedi, S.K.; Roy, P.; Karda, C.; Agrawal, S.; Amin, R. Blockchain-Based Internet of Things and Industrial IoT: A Comprehensive Survey. *Secur. Commun. Netw.* **2021**, *2021*, 7142048. [CrossRef]
20. Dai, H.N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A Survey. *IEEE Internet Things J.* **2020**, *6*, 8076–8094. [CrossRef]
21. Amreen Ashraf, W.E. Authentication in IoT devices using blockchain technology: A Review. In Proceedings of the 4th IET International Smart Cities Symposium, Online Conference, Bahrain, 21–23 November 2021; p. 4.
22. Guo, H.; Tao, X.; Zhao, M.; Wu, T.; Zhang, C.; Xue, J.; Zhu, L. Decentralized Policy-Hidden Fine-Grained Redaction in Blockchain-Based IoT Systems. *Sensors* **2023**, *23*, 7105. [CrossRef]
23. Eklund, P.W.; Beck, R. Factors that Impact Blockchain Scalability. In Proceedings of the 11th International Conference on Management of Digital EcoSystems, Limassol, Cyprus, 12–14 November 2019; pp. 126–133.
24. Corradini, E.; Nicolazzo, S.; Nocera, A.; Ursino, D.; Virgili, L. A two-tier Blockchain framework to increase protection and autonomy of smart objects in the IoT. *Comput. Commun.* **2022**, *181*, 338–356. [CrossRef]
25. Hyla, T.; Pejaś, J. eHealth Integrity Model Based on Permissioned Blockchain. *Future Internet* **2019**, *11*, 76. [CrossRef]
26. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef]
27. Ellahi, R.M.; Wood, L.C.; Bekhit, A.E.-D.A. Blockchain-Based Frameworks for Food Traceability: A Systematic Review. *Foods* **2023**, *12*, 3026. [CrossRef]
28. Jamil, F.; Ahmad, S.; Iqbal, N.; Kim, D.-H. Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals. *Sensors* **2020**, *20*, 2195. [CrossRef]
29. Arachchige, K.G.; Branch, P.; But, J. Evaluation of Correlation between Temperature of IoT Microcontroller Devices and Blockchain Energy Consumption in Wireless Sensor Networks. *Sensors* **2023**, *23*, 6265. [CrossRef]
30. Orange Pi—Orange Pi Official Website—Orange Pi Development Board, Open Source Hardware, Open Source Software, Open Source Chip, Computer Keyboard. Available online: http://www.orangepi.org/ (accessed on 22 August 2023).
31. Raspberry Pi. Available online: https://www.raspberrypi.com/ (accessed on 22 August 2023).

32. Solving the "Total Supply Problem". Available online: https://hydrachain.org/ (accessed on 17 August 2023).
33. The Monero Project. Available online: https://www.getmonero.org/ (accessed on 17 August 2023).
34. Coin—A Simple, Eco-Friendly, Centralized Coin. Available online: https://duinocoin.com/ (accessed on 17 August 2023).
35. Guerrero-Sanchez, A.E.; Rivas-Araiza, E.A.; Gonzalez-Cordoba, J.L.; Toledano-Ayala, M.; Takacs, A. Blockchain Mechanism and Symmetric Encryption in A Wireless Sensor Network. *Sensors* **2020**, *20*, 2798. [CrossRef] [PubMed]
36. Fang, W.; Zhang, W.; Chen, W.; Pan, T.; Ni, Y.; Yang, Y. Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 2643546. [CrossRef]
37. Madhusudan Singh, A.S. Shiho Kim Blockchain: A Game Changer for Securing IoT Data. In Proceedings of the IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018.
38. Hao, X.; Yeoh, P.L.; Wu, T.; Yu, Y.; Li, Y.; Vucetic, B. Scalable Double Blockchain Architecture for IoT Information and Reputation Management. In Proceedings of the 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 14 June–31 July 2021; pp. 171–176.
39. Mori, S. Secure caching scheme by using blockchain for information-centric network-based wireless sensor networks. *J. Signal Process.* **2018**, *22*, 97–108. [CrossRef]
40. Vikram, A.; Kumar, S. Mohana, Blockchain Technology and its Impact on Future of Internet of Things (IoT) and Cyber Security. In Proceedings of the 2022 6th International Conference on Electronics, Communication and Aerospace Technology, Coimbatore, India, 1–3 December 2022; pp. 444–447.
41. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef]
42. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. *Blockchain Technology Overview*; NIST: Gaithersburg, MD, USA, 2018.
43. Stamatellis, C.; Papadopoulos, P.; Pitropakis, N.; Katsikas, S.; Buchanan, W.J. A Privacy-Preserving Healthcare Framework Using Hyperledger Fabric. *Sensors* **2020**, *20*, 6587. [CrossRef] [PubMed]
44. Truong, H.T.T.; Almeida, M.; Karame, G.; Soriente, C. Towards Secure and Decentralized Sharing of IoT Data. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 176–183.
45. Premkumar, R.; Sathya, P.S. A Blockchain based Framework for IoT Security. In Proceedings of the 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 8–10 April 2021; pp. 409–413.
46. Zhang, X.; Liu, C.; Chai, K.K.; Poslad, S. A Challenge-Response Assisted Authorisation Scheme for Data Access in Permissioned Blockchains. *Sensors* **2020**, *20*, 4681. [CrossRef]
47. Sun, S.; Tang, H.; Du, R. A Novel Blockchain-Based IoT Data Provenance Model. In Proceedings of the 2022 2nd International Conference on Computer Science and Blockchain (CCSB), Wuhan, China, 28–30 October 2022; pp. 46–52.
48. Peral, J.; Gallego, E.; Gil, D.; Tanniru, M.; Khambekar, P. Using Visualization to Build Transparency in a Healthcare Blockchain Application. *Sustainability* **2020**, *12*, 6768. [CrossRef]
49. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]