electronics

MDPI

Article

Blockchain Based Smart Contracts for Internet of Medical Things in e-Healthcare

Ashutosh Sharma [1], Sarishma [2], Ravi Tomar [3], Naveen Chilamkurti [4] and Byung-Gyu Kim [5,*]

[1] School of Electronics and Electrical Engineering, Lovely Professional University, Jalandhar, Punjab 144001, India; sharmaashutosh1326@gmail.com

[2] Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248002, India; sarishmasingh@gmail.com

[3] School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, India; ravitomar7@gmail.com

[4] Department of Computer Science and Computer Engineering, La Trobe University, Melbourne 3086, Australia; n.chilamkurti@latrobe.edu.au

[5] Department of IT Engineering, Sookmyung Women's University, Seoul 04310, Korea

* Correspondence: bg.kim@sookmyung.ac.kr

Received: 21 May 2020; Accepted: 19 September 2020; Published: 1 October 2020

Abstract: The concept of Blockchain has penetrated a wide range of scientific areas, and its use is considered to rise exponentially in the near future. Executing short scripts of predefined code called smart contracts on Blockchain can eliminate the need of intermediaries and can also raise the multitude of execution of contracts. In this paper, we discuss the concept of Blockchain along with smart contracts and discuss their applicability in the Internet of Medical Things (IoMT) in the e-healthcare domain. The paper analyses the dimensions that decentralization and the use of smart contracts will take the IoMT in e-healthcare, proposes a novel architecture, and also outlines the advantages, challenges, and future trends related to the integration of all three. The proposed architecture shows its effectiveness with average packet delivery ratio, average latency, and average energy efficiency performance parameters when compared with traditional approaches.

Keywords: Blockchain; Internet of Things; smart contracts; decentralization; e-healthcare

1. Introduction

In 2008, a white paper was published by Satoshi Nakamoto [1] on Bitcoin, which primarily proposed a solution to the double spending problem found in economic transactions. The concept that formed the backbone for the functioning of Bitcoin was termed as Blockchain. Bitcoin amassed the economic market of more than 50 billion dollars [2] in less than ten years of its introduction and this massive success called for researchers to find more application areas for the concept. Blockchain thus got introduced into many areas of research and, in this paper, we will focus on how it can add on and change the prospects of the working of the Internet of Things through smart contracts.

Blockchain is a concept that enables the execution of transactions between two or more parties in a trustworthy manner without the need for any validating or trust authority in between. It has eliminated one entire tier, which was previously needed in order to transact or execute any instruction [3]. Blockchain works in a decentralized manner whereby a copy of data is found at every node and thus any new node can update itself from the network [4]. In recent times, Blockchain has covered the wide expanse of the market starting from finance, e-healthcare, public utilities, asset management, government regulations, real estate business, logistics, supply chain management [5]. This immense success is primarily attributed to its ability to work in a secure manner without the need for a trusting authority. With the rapid expansion of research, Blockchain 2.0 [6] is being proposed, which comprises more advanced and sophisticated versions of smart contracts and their applicability [7].

Smart contracts, which were proposed in 1993 by "Nick Szabo", are scripts or series of code that are put over the Blockchain for execution [8]. Using Blockchain as the base enables smart contracts to be executed in a faster and secure manner [9,10]. Using Blockchain to implement smart contracts may or may not be a good choice when it comes to the Internet of Things since different applications come with different specifications and some might not be able to work efficiently in the presence of Blockchain-based architecture [11].

Internet of Things is a term that evolved around when internet connectivity expanded its reach to physical devices of all ranges. These physical devices ranging from very small to big, when embedded with sensors [12], provide enhanced functionality, which can be used for multiple cases. These physical devices when embedded with sensors are then termed as 'things' in the Internet of Things. The term internet is used relatively as those things can have their own independent network or they can integrate with the global internet as well [13]. Emergence of new technologies, such as machine to machine communication, cyber physical systems, cloud computing, fog computing, smart sensors, and intelligent sensors, have led to an exponential growth rate in practical use cases. That is why the name Internet of Things has become a household name in many areas now [14]. IoT is so versatile in nature that everyone is finding their own meaning from it and thus it remains an evolving subject till now.

The future of the IoT domain revolves around three key visions [15,16]—a vision oriented around things where embedded devices can keep track of anything over any period of time, a vision oriented around the internet where the emphasis is on connected devices and data, and the last is semantic oriented vision where raw data are transformed into meaningful data. The IoT market share is divided into some key areas manufacturing and business (40%), healthcare (30%), retail (8%) and security (7.7%) [17]. Formation of IoT networks is enabled by the presence of connectivity protocols, which connect different devices and collect data, implementation modules that define what has to be done with the data, and other recent technologies, such as cloud computing, big data, and artificial intelligence. With the increase in computation power and decrease in cost of equipment, the Internet of Things emerged as a game changer and enabled us to adopt a wide scale use of ICT (Information and Communication Technology) related applications [18]. The Internet of Things proposes to embed things having computation power, storage, and networking capabilities, and connect them to the internet so as to provide the users with varied services. The most popular IoT related applications [19] include logistics management, smart-home, health industry, smart-vehicles, facility management, automation, and smart-grids.

The following Table 1 showcases the trade-off when it comes to implementing Blockchain-based smart contracts in an Internet of Things based application.

However, when it comes to the Internet of Medical Things in e-healthcare, the Blockchain has to be slightly modified to work in a partially decentralized manner [20]. IoT applications work in a completely centralized manner, incurring significant consumption of resources, but Blockchain demands complete decentralization, which is not feasible to execute in most IoT applications [21]. A balance between the two needs to be achieved on the basis of the type of application that is being deployed. For applications that include billing, events, or some monetary changes, Blockchain can be directly implemented where a smart contract can dictate when and to whom service will be given and payment will be received.

Also, a smart contract has to carefully define as to when the contract will initiate and when it will be bought to a closure. Life cycle management issues have to be handled carefully so that we do not end up with incomplete hung contracts, which we cannot alter at a later date.

Table 1. Comparison between Blockchain and Internet of Things (IoT) demands with respect to certain features.

Features	Iot Based Smart Contracts	Blockchain
Network structure	Demands centralization	Demands decentralization
Transparency	Low, depends on the accessibility defined in the contract for individual classes of nodes	High in most of the cases, but can be restricted to application level
Cost	High as constant mediation is needed depending upon states of data	Low as it is self-executing and independent in nature
Security	Less secure, can be easily tampered	Very secure and tamper-proof
Scalability	Low, needs intervention and is expensive	Highly scalable as anyone can join anytime
Resource consumption	Low for data communication, high for sensing	High for communication and processing
Bandwidth consumption	Nodes have limited bandwidth	Demands high bandwidth amongst decision making nodes
Latency	Demands lower latency	Needs time for information processing, validating and mining

In this paper, the author's main goal is to outline how Blockchain works with smart contracts and how it can be integrated into the applications based on the Internet of Medical Things in e-healthcare so as to make informed choices about when and when not to use Blockchain-based contracts [22] in Figure 1. The paper also provides the major advantages that come along with this concept and the challenges that need to be addressed before we can move with the execution in a real world scenario [21].

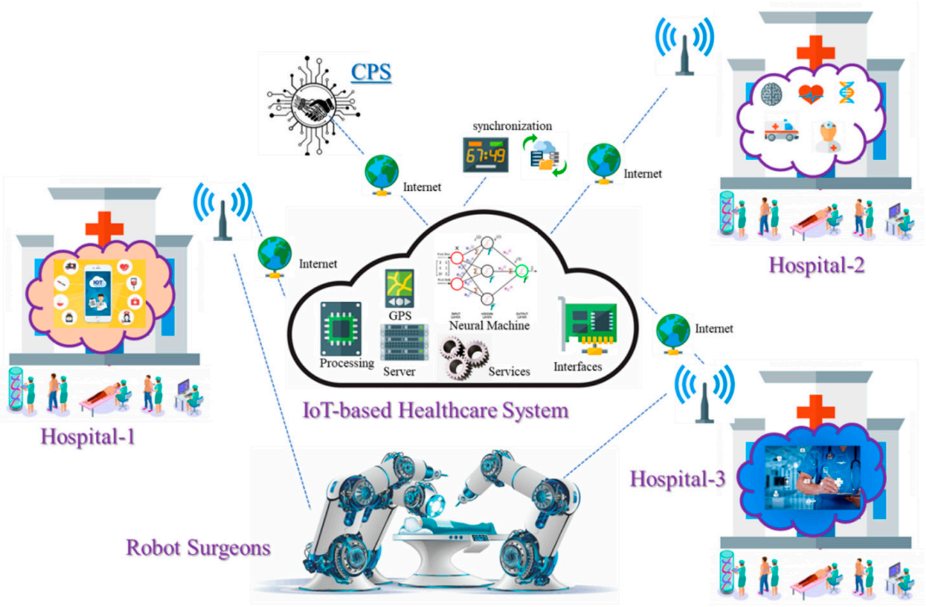


Figure 1. Internet of Medical Things (IoMT) enabled e-healthcare services.

We have up until now, elaborated upon the concepts of Blockchain, Internet of Medical Things, how they work and what the benefits are. However, there are many open questions that require answering before one can even think of implementing smart contracts for their IoMT application areas [23]. The potential key questions are as follows:

Why use Blockchain-based smart contracts for IoMT applications?
What is the novel way to transition to such system with respect to IoMT infrastructure?
How will the front-end of the application maintain the data and process requests without compromising security?
How to handle heterogeneity of devices and data before it is sent to smart contracts?
How to balance the centralization and decentralization aspects of IoMT application with respect to the demands?

In order to answer all these questions, we propose a novel architecture for the implementation of smart contracts based on the Internet of Medical Things (IoMT) in e-healthcare to show the usage of applications. The IoMT end devices will be put in place, which will sense the required data with respect to the application demands. These nodes will be pre-programmed as to how they should send or process the data. We also outline the future research trends and the related security details.

Organization

The paper is structured as follows: Section 2 dives into the basic grounds on which Blockchain works in the e-healthcare, and ends with the application grouping and the benefits of using Blockchain. Section 3 elaborates the proposed architecture for the proposed approach. Section 4 includes the results and discussion of performance parameters. Finally, a conclusion has been drawn in Section 5 followed by recent technologies with future applications.

2. Literature Review

As the name suggests, Blockchain is made up of a chain of blocks, which are time stamped and are identified by a cryptographic hash [23]. A timestamp allows a sequential ordering of blocks and the hash is used to uniquely identify a block. The parent block of the chain is called Genesis [24], and further blocks all contain cryptographic hashes of previous blocks thereby maintaining the chain. Any node that has access to this reverse linked data structure can know the state of data and gain access to it anytime from anywhere [25].

The nodes in the Blockchain all have a unique set of public and private keys that is assigned to them when they join the network. The use of asymmetric cryptography lets us bring authentication, non-repudiation and integrity into the network. Whenever a transaction takes place, it is signed by the user's private key and is broadcasted to the neighbors. The transaction received by the other nodes are crosschecked and validated using the public key before they relay it further into the network. The invalid transactions are discarded. After an agreed upon period of time, all the transactions in that time window are accumulated and packaged into a time stamped block by some of the nodes, which are referred to as miners. When the new block is mined, other nodes verify whether the block contains valid transitions or not, if yes the block is broadcasted and if no, the block is discarded. This process keeps on repeating after predetermined intervals of time. The nodes execute in a trustless environment in the beginning and trust is slowly achieved by the emergence of transactions and blocks. As such all the transactions are validated before relaying and similarly the blocks are mined by nodes that have a certain trust level. So, it is said that the trust in a Blockchain emerges as a property within the network [26,27].

The nodes within the Blockchain have to agree upon a unanimous set of orderly transactions so that they can mine the block and update the Blockchain after periodic intervals. In an ideal scenario, agreeing on the block mined by a maximum number of nodes is the solution [28,29]. However, the Sybil attack, i.e., insertion of multiple nodes by a single user to bias the decision on mining the block, is a major threat. Once a block is mined using a miner, and transactions are locked, they cannot be reversed [30]. That is how Blockchain maintains security, as the asymmetric key combination is used to validate the transactions so that later on, no one can deny their role in the transactions. The body of the block comprises of the set of transactions along with the transaction counter where the size of transactions determines the number of transactions a block can hold [28,29].

According to Gartner's hype cycle, Blockchain is currently at its peak use where deployment and development are at the highest level possible. The majority of domains are working on its applicability in one field or other because of its numerous benefits. Many authors, however, believe in the traditional centralized architecture to be more effective for their use [30,31], which is still a better bet on multiple fronts. Anyhow, we present some application areas where smart contracts can be executed in a decentralized manner. Maintaining trust in the network is a priority for many parties and Blockchain stands well on that, regardless of the other threats. Some of the application areas for the same are given as:

- Supply chain management; tracking goods, supplier identity and reputation, intelligent transport systems [6], smart vehicles [27,28], road traffic management [32].
- Healthcare [33], smart maintenance and diagnostics [34], integrated management systems [35,36].
- Smart agriculture [37] and farming, smart energy/grids [38], smart environment [39], smart homes [40,41], smart clothing [42,43], etc.
- E-democracy and E-governance [43,44], defense and public safety [45] law-enforcement [46], professional responsibility [47].
- Copyright protection [48], real estate market [49], record management [50], asset management [51], product certification [52], insurance claims [53].
- Financial trading, industry 4.0 [54], logistics [55,56], and cyber security [57].

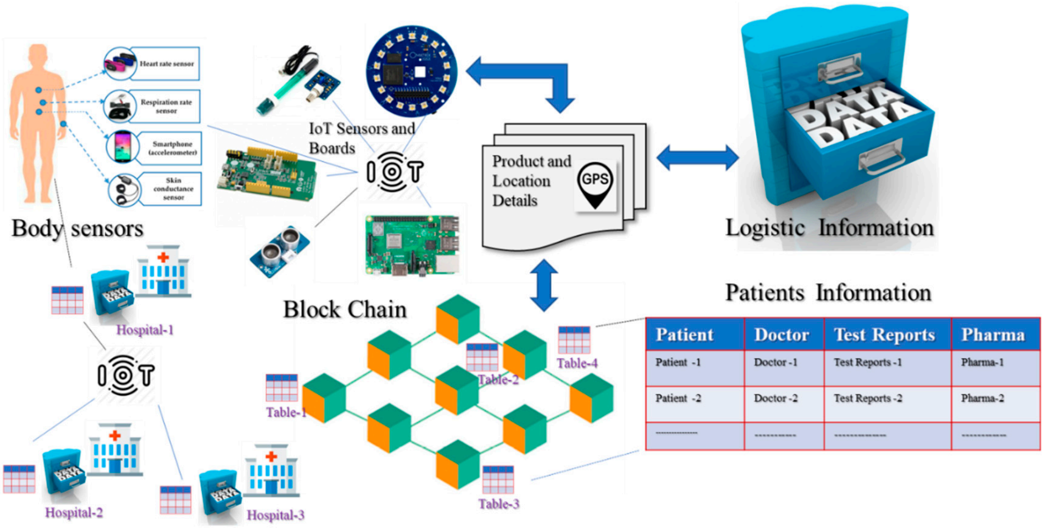
Due to huge usage of Blockchain in each and every application, authors have also proposed a secured healthcare system to provide security to the patient's confidential data over the cloud [33]. Various authors provided several frameworks to integrate security mechanisms to transfer data over the cloud [21,34], and later incorporate Blockchain in healthcare to transfer data over the cloud due to the problem of key management. The centralized key management system issues in healthcare for security have been replaced with decentralized Blockchain technology. Also, authors in [58] highlighted the use and role of Blockchain in the decentralized healthcare system where each trace or log file has been maintained properly [20]. This system replaced the brokerage and intermediate cost. In addition to this, authors have also proposed architecture for medical record exchange by introducing an advanced Blockchain technique. The proposed approach has been designed to meet the interactive norms and healthcare growth demands in new social forms. The authors claim an efficient approach by reducing the intermediates during the exchange of medical or patient records. Therefore, all the above-discussed literature motivates authors to show the use case of Blockchain-based e-healthcare applications and propose a novel architecture.

3. Proposed Architecture

In this paper, we are dealing with the emergence of IoT with healthcare with the help of a medical sensor and therefore have hybridized the IoT as the Internet of Medical Things (IoMT) [58]. The IoMT infrastructure boosts the healthcare sector over the internet and is named e-healthcare [59]. The proposed system model incorporated the application of smart contracts for the IoMT in e-healthcare, as shown in Figure 2.

Smart contracts can be used in the domain of IoMT where the number of nodes are increasing by millions with time [60] and the need to monitor and implement the contracts is becoming increasingly difficult. Blockchain can be used to ease this effort as it eliminates the need for intermediaries. The brokers or intermediaries present in the network for information validation and decision making consume a lot of resources such as computation and time. The Blockchain eliminates the use of these intermediaries by preparing the participating nodes itself to work collectively on their behalf [61]. Reduction in computations, time, and energy are the major factors for the motivation to integrate the Blockchain with IoMT in e-healthcare to increase the life of sensors nodes. Prime use of this lies in the asset management whereby assets can be embedded with smart contracts, which define who owns what at what point of time. Also, all the transactions work on a set of variable inputs, which can be defined deterministically as per the requirements. When implementing it with the Internet of Medical Things, the things in the network can work as an automated independent unit and produce results effectively.

Smart contracts can be embedded in the things where they will be having a unique address within the Blockchain network. Whenever set environment variables take on the value that agrees with the input criteria of a smart contract, then the corresponding code will execute. A smart contract can also be triggered by addressing a transaction directly to it. As the chain is connected, the same sets of instructions are executed on the other nodes as well. All the transactions execute independently and once executed, they cannot be reversed so that the chain becomes tamper-proof and irrevocable [62]. In order to revoke any transaction, a counter transaction has to be performed or a hard fork needs to be done. Smart contracts implemented over Blockchain excel in applications where data management transactions are greater in number. This case is the ideal scenario for IoMT related services as there is a huge amount of data being generated and its processing is still limited [59]. Blockchain helps to automate this process leading to faster and efficient data execution, processing and storage.



Patient	Doctor	Test Reports	Pharma
Patient -1	Doctor -1	Test Reports -1	Pharma-1
Patient -2	Doctor -2	Test Reports -2	Pharma-2
-------------	----------	------------	----------

Figure 2. Blockchain architecture for Internet of Medical Things (IoMT) in e-healthcare.

There are some points to be kept in mind while dealing with smart contracts which are listed as:

- There are two types of models that can be used to implement smart contracts. One is a transaction based model whereby the prime focus is on executing transactions to which variables are fed as input. The second one is an account based model where the smart contract itself has an account and can take custody of the assets it is dealing with on the Blockchain.
- All possible outcomes of the smart contract should be properly coded so that it becomes full proof and also avoids the possibility of falling into a hung state.
- A smart contract has to be deterministic, i.e., it should always reach the same output given the same set of inputs.
- Every node has the ability to crosscheck the transactions and the state of the system, which leads us to maintain consistency in the system.
- Any code or transaction once executed cannot be reverted; however, we can make the changes by executing more code. This maintains a state of security in the system as it becomes tamper-proof and thus makes the overall chain more secure.
- The transactions are signed messages, which let others know about who did what at what point of time.

In short, smart contracts are basically self-verifying, tamper-proof, and self-verifying scripts of code, which can run independent, automated procedures, provide enhanced level of security, eliminate the need of a trusted intermediary, and are cheap to implement [44]. Using the points of smart contracts, the working model of IoMT in e-healthcare is shown in Figure 3.

Smart contracts have emerged as entities that are completely autonomous and of which the behavior is totally predictable. So, before any node engages in the contract, they can know all about the terms and way of execution of the contract [35]. The main application of it comes for the networks where complete transparency is required. Such systems are currently validated by a third party as a trusted source. The Blockchain struck at this particular wheel and eliminated the need of trusted intermediaries [26].

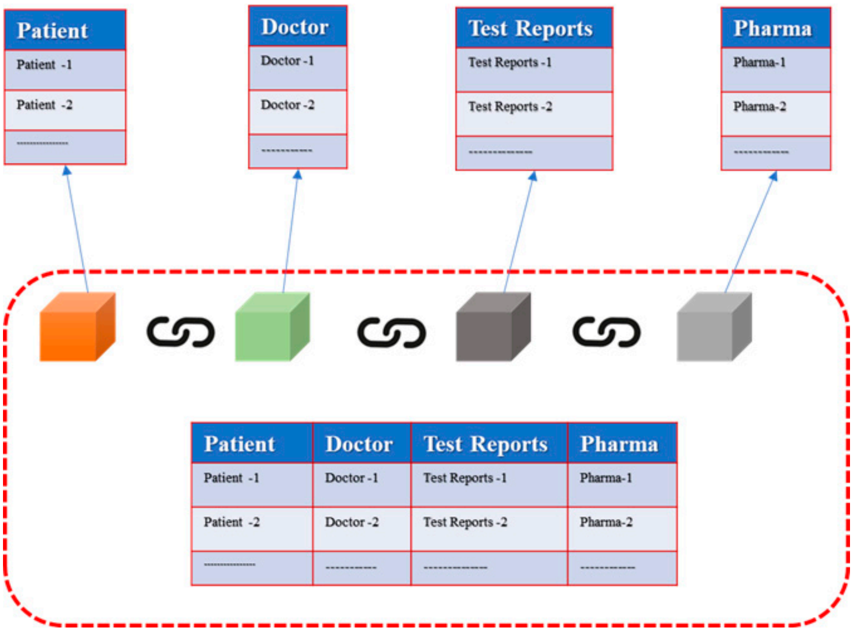


Figure 3. Decentralized Blockchain-based smart contracts for an IoMT framework in e-healthcare.

Working of Blockchain Based Smart Contracts for IoMT in e-Healthcare

The decentralized Blockchain-based smart contracts for IoMT in e-healthcare constitutes all the information related to each transaction of the patient with its records, such as doctor details, prescription list and medication details, and pathology lab test reports. Each record holder acts as a block where data move from one block to another block forming a chain. In this chain there is always a hash as the initial point and with one move a hash is always added with the message [63]. To implement Blockchain-based smart contracts for IoMT in e-healthcare Algorithm 1 has been proposed as shown below:

Algorithm 1: Blockchain-based smart contracts for IoMT in e-healthcare

```
Input:    Delay, Capacity, Energy, Data traffic
Output:   Data transmitted with the Blockchain in e-healthcare

Begin {
Step 1:   Declaration of variables
Step 2:   Set the threshold values of legitimacy for a miner with energy ($E_{THM}$)
Step 3:   Set the threshold value of legitimacy for block with energy ($E_{THB}$)
Step 4:   if ($E_{THM} \geq$ Threshold)
Step 5:   if ($E_{THB} \geq$ Threshold)
The hash of the block added to the data and authentication has been conducted with the next block in the chain.
Step 6:   else
Hash of previous block compromised and removed. //Go to Step 5
Step 7:   End if
Step 8:   End if
Step 9:   Data transmitted with the Blockchain-based smart contract for IoMT in e-healthcare
} End
```

The hash always recognizes the block because this hash is a very unique number. Also, there is always a hash of the previous block to make a chain within blocks. To understand the concept of Blockchain-based smart contracts for IoMT in e-healthcare, if a patient goes in for the treatment of a disease then all data will be stored in each block [28]. If anyone wants to tamper with the data then the next hash will get changed. This will give the wrong hash to the next block. So, the malicious activity will come into notice of everyone, and if anyone wants successful tamper with the data, they will always need to tamper with all the subsequent blocks, which is practically not possible. This is how the Blockchain-based smart contract in terms of hash works in the IoMT e-healthcare. In the next section, we will discuss the role of the miner and performance analysis with the help of results [28].

The proposed algorithm has been used to compute the secured and authentic data transmission without any participation of a legitimate node. The proposed algorithm is beneficial where the security of private medical data is the top priority.

4. Results and Discussion

The proposed system has been implemented and simulated over MATLAB Simulink comprising an 8-GB RAM Intel(R) Core™ i5–7400 CPU among 3.00-GHz processor, and Windows 10 Operating System. In this paper, we have presented the smart contract based framework for the trusted blocks. In the simulation environment, we have mentioned each node with a block and each block ensures the trust between each block. Also, to test the proposed model, the compromised blocks have also been added in the e-healthcare system model but still the proposed framework has been used to provide the e-healthcare. Table 2 has been used to show the network parameter used in the MATLAB Simulink tool for the experiment. The whole grey attack has been used to show the legitimate nodes in the network and the level of trust in the network. The delay and capacity of each link participated in the chain between two consecutive blocks has been generated with the normal distribution as [1,100] in seconds (s) and bits per seconds (bits/s) [44].

Table 2. Network parameters used in MATLAB Simulink for the experiment.

Sr. No.	List of Network Attributes	Attribute Values
1	Total nodes (blocks)	100, 200 and 300
2	Total links (chains) formulated	4600, 18,500 and 41,500
3	Network size	1000 m × 1000 m
4	Information traffic	1024 bits
5	Simulation time	120 s
6	Energy associated with nodes (blocks)	10 J

The experiment has been conducted with three different sets of nodes with the formulation of three different sets of links. In each set of nodes, there are always known blocks, and the links in these blocks formulate chains [33]. A dataset with the information traffic size of 1024 Bits has been transmitted over a Blockchain with e-healthcare data. Each node (Block) is associated with 10 Joules of energy, which is the trust value for the measure of security. A threshold 6 Joules of energy associated with nodes (blocks) has been set as the least amount of blocks to be considered non-malicious nodes. Similarly, the miner (node) block has been set with the threshold of 4 Joules.

To perform the malicious activities in the network, each set of nodes (blocks) has been added with a set of malicious nodes, i.e., (5, 25, 50), as well as malicious miners, i.e., (10, 50, 100) due to the whole grey attack. In e-healthcare, whenever a doctor or medical practitioner gives the prescription list to a patient, these details are sent to each miner in the network. The complete experiment architecture with Blockchain is shown in Table 3.

Now the data generated from each block have been authenticated with the hash as well as miner data. If the authentication of the blocks failed then the legitimacy of the previous block is taken out. In this paper, the percentage improvement of the proposed algorithm has been compared the traditional conventional approach [63]. Here, various performance parameters have been considered in terms of average packet delivery ratio (throughput), average latency, and average energy. The detailed results and discussion have been discussed with the conventional method.

Table 3. Network configuration with miners and number of nodes (blocks) with malicious nodes (blocks) and miners.

Network with Different Nodes (Blocks)	Malicious Nodes (Blocks)	Miner Nodes (Blocks)
100	5	10
200	25	50
500	50	100

4.1. Average Packet Delivery Ratio (Throughput)

In this performance parameter, the data traffic has been sent over all three different networks and the proposed algorithm has been compared with the existing traditional method. The results have been shown in Figure 4 for the performance parameter average packet delivery ratio and results show that the proposed algorithm outperforms well as compared to the exiting conventional method. This is because, whenever the data have been compromised, the next node is never able to authenticate (still this has been considered in our proposed method), therefore due to the large block degree, the data have been reversed from the malicious nodes.

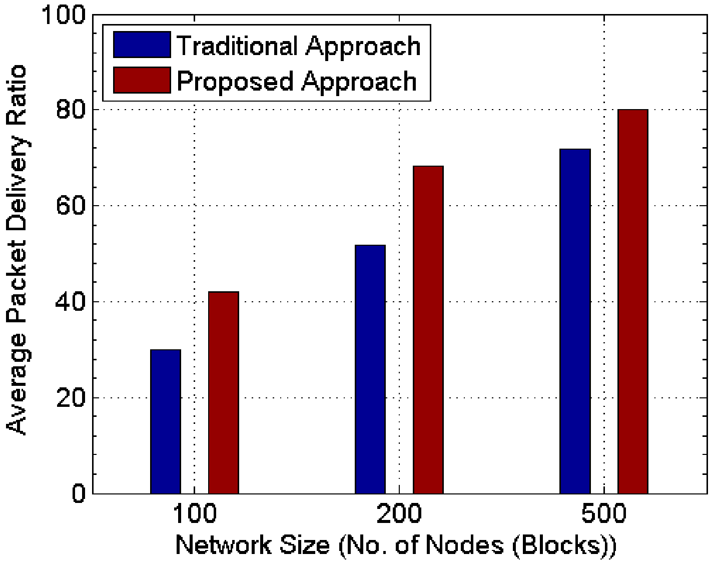


Figure 4. Comparison of average Packet Delivery Ratio (PDR) for the traditional approach and proposed approach.

The proposed algorithm can approach the 100% packet delivery ratio but for this the authentication of blocks needs to be checked before moving forward the data to the next node.

4.2. Average Latency

The proposed method has been also simulated for the average latency (s) for the data transmission with a malicious and compromised node (blocks). The proposed method has been also compared with the existing traditional approach [48]. The results have been shown in Figure 5, which shows that the proposed algorithm has more average latency as compared to proposed algorithm. This might be the case because the data from the compromised block with malicious activities has been asked to retransmit for the next block and can be authentic with the help of a miner block.

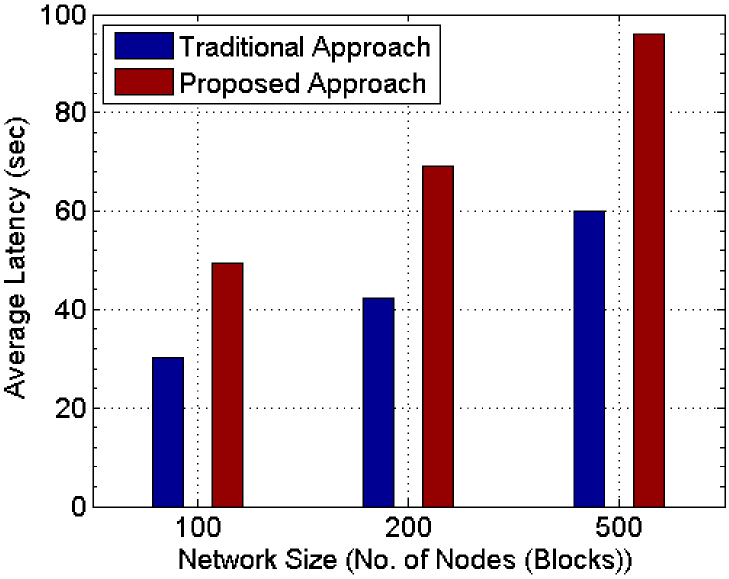


Figure 5. Comparison of average latency for the traditional approach and proposed approach.

4.3. *Average Energy Efficiency*

The average energy efficiency (bits/s/joule) is also one of the major performance parameters to check the improvement in the average energy efficiency [44]. The selection of specific miners has been used for authentication as well as data transmission.

In the proposed approach (method), the average energy efficiency of the proposed method is more than the existing method as shown in Figure 6. This can be also due to the fact that the proposed algorithm will check each node (block) with a specific miner, which has the least threshold value of 4 Joules.

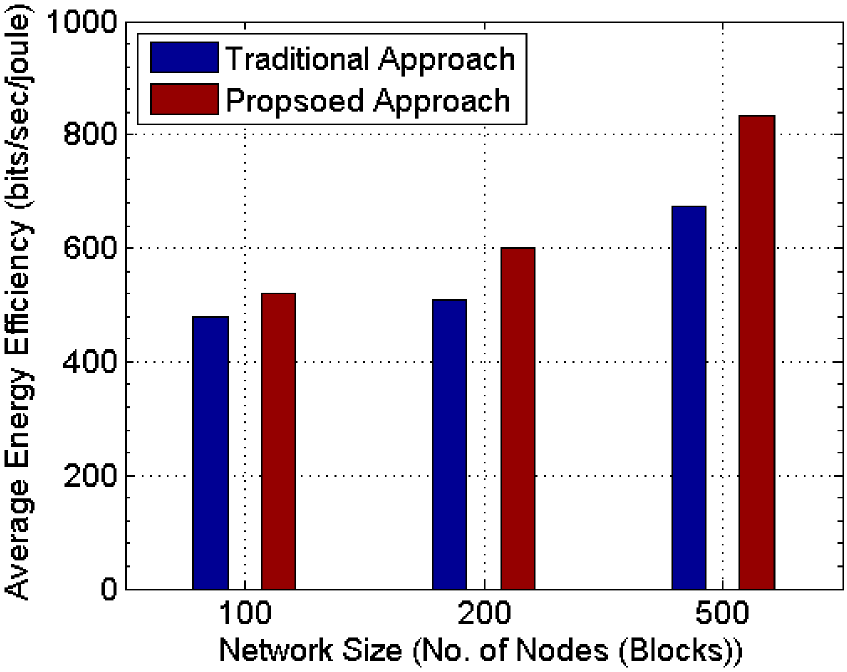


Figure 6. Comparison of average energy efficiency for the traditional approach and proposed approach.

5. Conclusions

In this paper, we discussed the working of a Blockchain, which has taken a very firm hold in e-healthcare in a very short span of time. We focus on how smart contracts over Blockchain can be used in the domain of Internet of Things and analyze what advantages and challenges it brings with itself. A comparison of the results of the proposed approach and the traditional approach shows that the proposed approach outperforms very well. The proposed approach shows that the average packet delivery ratio has an increase in delivery of the data packet because in the proposed approach no legitimate node is participating in the data transmission among the chains. Similarly, the same trend is being followed in the performance parameter of average latency and average energy efficiency. In the next section, future trends are discussed for more applications and other details.

6. Future Direction and Integration of Other Technologies

Various other cutting edge technologies can be implemented along with Blockchain, such as cloud computing [24,25], mobile edge computing [26], fog computing [27], big data analytics [28], artificial intelligence, and cyber physical systems [29]. The use of cloud computing can enable the extensive use of computation resources for additional processing. Various backend applications can be deployed on the cloud end as it scales very efficiently. Cloud storage can be used to store the Blockchain when its size increases and it becomes difficult for other nodes to handle it. Cyber physical systems provide a certain level of autonomous behavior where machines can interact with one another and behave accordingly. By using Blockchain-based smart contracts, this autonomous behavior can multiply as actions can be predefined. Such concepts can be easily integrated leading to manifold benefits. Big data analytics emerged in the last decade and has provided tremendous amount of business intelligence to people by analyzing large sets of data. Side by side analysis of the data being generated and stored in the cloud can provide the user with useful insights, which can help in increased efficiency and profits. Fog computing brings computation capability somewhat close to the end user by deploying nodes between the cloud end and user end. The managerial nodes proposed in the architecture also help in similar data processing before it is sent to the other end. Fog computing reduces latency, which can be a key factor for some use cases. Many other concepts are being introduced in the market now these days, such as use of software defined networking. Most of these can help in increasing service quality and data processing of user and devices respectively.

Author Contributions: All authors have equal contribution. Conceptualization, A.S. and S.; methodology, A.S. and R.T.; software, A.S., N.C. and B.-G.K.; validation, A.S., S. and R.T.; formal analysis, S., N.C. and B.-G.K.; investigation, A.S. and R.T.; resources, N.C. and B.-G.K.; data curation, A.S.; writing—original draft preparation, A.S., S. and R.T.; writing—review and editing, A.S., S., R.T., N.C. and B.-G.K.; visualization, S. and R.T.; supervision, N.C. and B.-G.K.; project administration, N.C. and B.-G.K.; funding acquisition, N.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Satoshi, N.; Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic cash system. *Bitcoin* **2008**, *9*. Available online: https://bitcoin.org/bitcoin (accessed on 24 February 2020).
2. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.
3. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.Y. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277. [CrossRef]
4. Restuccia, F.; Kanhere, S.D.; Melodia, T.; Das, S.K. Blockchain for the Internet of Things: Present and Future. *arXiv* **2019**, arXiv:1903.07448.
5. 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 6th International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
6. Schuh, F.; Larimer, D. Bitshares 2.0: General Overview. *Cryptonomex* **2017**, *3268*, 16. Available online: http://docs.bitshares.org/downloads/bitshares-general (accessed on 24 February 2020).

7. Szabo, N. Smart contracts: Building blocks for digital markets. *EXTROPY J. Transhumanist Thought* **1996**, *18*. Available online: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2 (accessed on 24 February 2020).
8. Salimitari, M.; Chatterjee, M. An Overview of Blockchain and Consensus Protocols for IoT Networks. *arXiv* **2018**, arXiv:1809.05613.
9. Alphand, O.; Amoretti, M.; Claeys, T.; Dall'Asta, S.; Duda, A.; Ferrari, G.; Rousseau, F.; Tourancheau, B.; Veltri, L.; Zanichelli, F. To cite this version: HAL Id: Hal-01705455. IoTChain: A Blockchain Security Architecture for the Internet of Things. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–7.
10. Umeh, J. Blockchain Double Bubble or Double Trouble? ITNOW. Available online: https://academic.oup.com/itnow/article/58/1/58/2392029 (accessed on 15 January 2020).
11. Huh, S.; Cho, S.; Kim, S. Managing IoT Devices using Blockchain Platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea, 19–22 February 2017; pp. 464–467.
12. Founder, G.W.; Gavin, E. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
13. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaría, V. Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet* **2018**, *10*, 20. [CrossRef]
14. Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Wills, G.B. Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. *Int. J. Intell. Syst. Appl.* **2018**, *10*, 40–48. [CrossRef]
15. 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]
16. Singh, D.; Jara, A.J. A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 287–292.
17. Internet of Things Forecast–Ericsson Mobility Report. Available online: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast (accessed on 2 April 2019).
18. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT Integration: A Systematic Survey. *Sensors* **2018**, *18*, 2575. [CrossRef] [PubMed]
19. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
20. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef]
21. Singhal, A.; Sarishma; Tomar, R. Intelligent accident management system using IoT and cloud computing. In Proceedings of the 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 14–16 October 2016; pp. 89–92.
22. Pustišek, M.; Kos, A. Approaches to Front-End IoT Application Development for the Ethereum Blockchain. *Procedia Comput. Sci.* **2018**, *129*, 410–419. [CrossRef]
23. 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 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 13–16 December 2017; pp. 1180–1184.
24. Park, J.H.; Park, J.H. SS symmetry Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. *Symmetry* **2017**, *9*, 164. [CrossRef]
25. Khanna, A.; Sarishma. RAS: A novel approach for dynamic resource allocation. In Proceedings of the 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 4–5 September 2015; pp. 25–29.
26. Yang, R.; Yu, F.R.; Si, P.; Yang, Z.; Zhang, Y. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1508–1532. [CrossRef]
27. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog Computing and Its Role in the Internet of Things Characterization of Fog Computing. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 17 August 2012; pp. 13–15. Available online: https://cse.buffalo.edu/faculty/tkosar/cse710_spring19/bonomi-bdiot14 (accessed on 2 April 2019).

28. Koo, D.; Piratla, K.; Matthews, C.J. Towards Sustainable Water Supply: Schematic Development of Big Data Collection Using Internet of Things (IoT). *Procedia Eng.* **2015**, *118*, 489–497. [CrossRef]
29. Fotiou, N.; Siris, V.A.; Voulgaris, S.; Polyzos, G.C. Bridging the Cyber and Physical Worlds Using Blockchains and Smart Contracts. 2019. Available online: https://www.ndss-symposium.org/wp-content/uploads/diss2019_02_Fotiou_paper (accessed on 2 April 2019).
30. Giungato, P.; Rana, R.; Tarabella, A.; Tricase, C. Current Trends in Sustainability of Bitcoins and Related Blockchain Technology. *Sustainability* **2017**, *9*, 2214. [CrossRef]
31. Zhu, X.; Badr, Y. Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions. *Sensors* **2018**, *18*, 4215. [CrossRef]
32. Xu, R.; Chen, Y. BlendCAC: A Smart Contract Enabled Decentralized Capability-Based Access Control Mechanism for the IoT. *Computers* **2018**, *7*, 39. [CrossRef]
33. Chang, C.; Kuo, C.; Chen, J.; Wang, T. Design and Implementation of an IoT Access Point for Smart Home. *Appl. Sci.* **2015**, *5*, 1882–1903. [CrossRef]
34. Kshetri, N. Can blockchain strengthen the internet of things? *IT Prof.* **2017**, *19*, 68–72. [CrossRef]
35. Liu, B.; Yu, X.L.; Chen, S.; Xu, X.; Zhu, L. Blockchain based Data Integrity Service Framework for IoT data. In Proceedings of the 2017 IEEE International Conference on Web Services (ICWS), Honolulu, HI, USA, 25–30 June 2017.
36. Tzafestas, S.G.; Porter, J.; Coraggio, G. Ethics and Law in the Internet of Things World. *Smart Cities* **2018**, *1*, 6. [CrossRef]
37. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A. Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet Things J.* **2018**, *6*, 2188–2204. [CrossRef]
38. Lin, J.; Shen, Z.; Miao, C. Using Blockchain Technology to Build Trust in Sharing LoRaWAN IoT. In Proceedings of the 2nd International Conference on Crowd Science and Engineering, Beijing, China, 6–9 July 2017; pp. 1–6.
39. Rachkidi, E.; Agoulmine, N.; Taher, N.C.; Background, A. Towards Using Blockchain Technology for IoT data access protection. In Proceedings of the 2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB), Salamanca, Spain, 12–15 September 2017.
40. Ouaddah, A.; Elkalam, A.A.; Ouahman, A.A. Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT. In *Europe and MENA Cooperation Advances in Information and Communication Technologies*; Springer: Cham, Switzerland, 2017; pp. 523–533.
41. Sun, Y.; Zhang, L.; Member, S.; Feng, G.; Member, S.; Yang, B. Blockchain-enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment. *IEEE Internet Things J.* **2019**, *6*, 5791–5802. [CrossRef]
42. Polyzos, G.C.; Fotiou, N. Blockchain-assisted Information Distribution for the Internet of Things. In Proceedings of the 2017 IEEE International Conference on Information Reuse and Integration (IRI), San Diego, CA, USA, 4–6 August 2017; pp. 75–78.
43. Moin, S.; Karim, A.; Safdar, Z.; Safdar, K.; Ahmed, E.; Imran, M. Securing IoTs in distributed blockchain: Analysis, requirements and open issues Abstract. *Future Gener. Comput. Syst.* **2019**, *100*, 325–343. [CrossRef]
44. Swan, M. Blockchain Temporality: Smart Contract Time Speci fi ability with Blocktime. In *International Symposium on Rules and Rule Markup Languages for the Semantic Web*; Springer: Cham, Switzerland, 2016; pp. 184–196.
45. Atzori, M. Blockchain technology and decentralized governance: Is the state still necessary? *SSRN* **2017**, *6*, 45–62. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713 (accessed on 24 February 2020). [CrossRef]
46. Hsu, I.Y.Y.; Wódczak, M.; White, R.G.; Zhang, T.; Hsing, T.R. Challenges, approaches, and solutions in intelligent transportation systems. In Proceedings of the 2010 Second International Conference on Ubiquitous and Future Networks (ICUFN), Jeju, Korea, 16–18 June 2010; pp. 366–371.
47. Sharma, P.K.; Moon, S.Y.; Park, J.H. Block-VN: A distributed blockchain based vehicular network architecture in smart city. *J. Inf. Process. Syst.* **2017**, *13*, 184–195.
48. Lu, Z.; Wang, Q.; Qu, G.; Liu, Z. BARS: A Blockchain-Based Anonymous Reputation System for Trust Management in VANETs. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security And Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 98–103.

49. Misbahuddin, S.; Zubairi, J.A.; Saggaf, A.; Basuni, J.; Sulaiman, A.; Al-Sofi, A. IoT Based Dynamic Road Traffic Management for Smart Cities. In Proceedings of the 2015 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET), Islamabad, Pakistan, 21–23 December 2015; pp. 142–146.
50. Li, Y. An Integrated Platform for the Internet of Things Based on an Open Source Ecosystem. *Future Internet* **2018**, *10*, 105. [CrossRef]
51. Lin, Y.; Petway, J.R.; Anthony, J.; Mukhtar, H.; Liao, S. Blockchain: The Evolutionary Next Step for ICT e-agriculture. *Environments* **2017**, *4*, 50. [CrossRef]
52. Zhou, J.; Leppänen, T.; Harjula, E.; Yu, C.; Jin, H.; Yang, L.T. CloudThings: A Common Architecture for Integrating the Internet of Things with Cloud Computing. In Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Whistler, BC, Canada, 27–29 June 2013; pp. 651–6573.
53. Ren, Q.; Man, K.L.; Li, M.; Gao, B. Using Blockchain to Enhance and Optimize IoT-based Intelligent Traffic System. In Proceedings of the 2019 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea, 28–30 January 2019; pp. 1–4.
54. Talari, S.; Shafie-Khah, M.; Siano, P.; Loia, V.; Tommasetti, A.; Catalão, J.P. A Review of Smart Cities Based on the Internet of things concept. *Energies* **2017**, *10*, 421. [CrossRef]
55. Ganchev, I.; Ji, Z. A Generic IoT Architecture for Smart Cities. 2014. Available online: https://www.semanticscholar.org/paper/A- generic-IoT-architecture-for-smart-cities-Ganchev-Ji/b720fb72af9b729de523a5db36d1e915db339741 (accessed on 24 February 2020).
56. Fernández-Caramés, T.M.; Fraga-Lamas, P. Towards The Internet of Smart Clothing: A Review on IoT Wearables and Garments for Creating Intelligent Connected e-Textiles. *Electronics* **2018**, *7*, 405. [CrossRef]
57. Singh, S.; Ra, I.; Meng, W.; Kaur, M. SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719844159. [CrossRef]
58. Qi, R.; Feng, C.; Liu, Z.; Mrad, N. *Blockchain-Powered Internet of Things e-Governance and e-Democracy*; Springer: Singapore, 2017; pp. 509–520.
59. Wang, B.; Sun, J.; He, Y.; Pang, D.; Lu, N. Large-scale Election Based On Blockchain. *Procedia Comput. Sci.* **2018**, *129*, 234–237. [CrossRef]
60. Laplante, P.A.; Amaba, B. Blockchain and the Internet of Things in the Industrial Sector. *IT Prof.* **2018**, *20*, 15–18. [CrossRef]
61. Dobrovnik, M.; Herold, D.M.; Kummer, S. Blockchain for and in Logistics: What to Adopt and Where to Start. *Logistics* **2018**, *2*, 18. [CrossRef]
62. Betti, Q.; Khoury, R.; Hallé, S.; Montreuil, B. Improving Hyperconnected Logistics with Blockchains and Smart Contracts. *IT Prof.* **2019**, *21*, 25–32. [CrossRef]
63. Sharma, A.; Rathee, G.; Kumar, R.; Saini, H.; Varadarajan, V.; Nam, Y.; Chilamkurti, N. A Secure, Energy-and SLA-Efficient (SESE) E-Healthcare Framework for Quickest Data Transmission Using Cyber-Physical System. *Sensors* **2019**, *19*, 2119. [CrossRef]