IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received June 30, 2020, accepted July 19, 2020, date of publication July 28, 2020, date of current version August 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3012435

# DistBlockBuilding: A Distributed Blockchain-Based SDN-IoT Network for Smart Building Management

**ANICHUR RAHMAN[1], MOSTOFA KAMAL NASIR[1], ZIAUR RAHMAN[2], (Graduate Student Member, IEEE), AMIR MOSAVI[3,4,5], SHAHAB S[6], (Senior Member, IEEE), AND BEHROUZ MINAEI-BIDGOLI[7]**

[1]Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Tangail 1902, Bangladesh
[2]Department of Information and Communication Technology, Mawlana Bhashani Science and Technology University, Tangail 1902, Bangladesh
[3]Faculty of Civil Engineering, Technische Universität Dresden, 01069 Dresden, Germany
[4]Department of Mathematics and Informatics, J. Selye University, 94501 Komarno, Slovakia
[5]Kálmán Kandó Faculty of Electrical Engineering, Obuda University, 1034 Budapest, Hungary
[6]Institute of Research and Development, Duy Tan University, Da Nang 550000, Vietnam
[7]School of Computer Engineering, Iran University of Science and Technology, Tehran 13114-16846, Iran

Corresponding authors: Shahab S (shamshirbandshahaboddin@duytan.edu.vn) and Amir Mosavi (amir.mosavi@kvk.uni-obuda.hu)

**ABSTRACT** Security, privacy, and transparency aspects of the Internet of Things (IoT) sensors have recently raised significant concerns among the public and policymakers. The distributed ledger and Blockchain technologies had brought solutions through transparently bridging two or multiple untrusted parties. In this research, a novel architecture for a smart building system, including a control system and automatic approaches, is proposed. An efficient cluster head selection algorithm is proposed to select the desired cluster head with the consideration of low energy consumption and fast head selection. An enhanced combination of IoT forwarding devices and Software-Defined Networking (SDN) technology is further advanced. Furthermore, the proposed ''DistBlockBuilding'' architecture is implemented for managing a safe and secure data transfer from one surface to another surface. Besides, Blockchain technology is performed for transferring data within the smart building. Finally, the performance of IoT-SDN based secured networks is evaluated.

**INDEX TERMS** Internet of Things, Blockchain, software-defined networking, OpenFlow, smart buildings.

## I. INTRODUCTION

Nowadays, the rapid growth of IoT is accompanied by the rising number of physical objects connected to the internet. IoT realizes the ideology of interactions throughout the world via the internet [1]. It may sense or control surroundings through sensor networks and can recognize things by scanning an RFID tag [2]. IoT technologies now incorporate into home automation, industrial automation, health care, smart grid, smart cities, etc. Following the global health crisis COVID-19, enterprises are keen to deploy work-from-home capabilities at scale with high security and all intelligent facilities. Thus, we need remote access adoption more than ever. The enhancements of Information Technology (IT) services will further help IT leaders to quickly deliver secure remote access at scale to their employees at home across the globe, with the help of the nice combination of latest technologies if IoT, SDN, and Blockchain as the number of associated objects to the internet is growing these days, so the management and control of IoT become a very challenging job. Here SDN comes in to deliver the versatility and programmability of the IoT network without changing the architecture of existing implementations. Moreover, it can analyze the network impact the overall performance and efficiency of the network system, particularly in cases of real-time transactions. To minimize the reply time and safety issues, SDN is used in IoT applications. Recently, multiple controllers are used in SDN instead of using a centralized controller. The main goal of applying multiple controllers is to adjust the load among devices and controllers and reduce

The associate editor coordinating the review of this manuscript and approving it for publication was Kaitai Liang.

packet loss. Resources will be available instantly when they are required by the user utilizing the SDN-IoT network. Furthermore, using an SDN controller, a network can be configured dynamically. One of the most common protocols used by SDN is OpenFlow [3].

Another advanced technology is Blockchain, which is an emerging decentralized technology that can be consolidated with SDN based IoT applications. Various blocks are chained together by managing hash value, and each block of the transaction is permanently stored. Safety and privacy will be improved by combining this Blockchain technology [4]. Several researchers have been recommended many clarifications for enhancing network performance, but they cannot solve the problem completely.

Although IoT, SDN, Blockchain technologies are combined to provide a better solution for any smart technology such as intelligent building, smart homes, smart cities, and smart grids [5]. These technologies can also provide reliable data transmission as well as communication in the networks. But complexity is created when these technologies are applied. Several solvents proposals have been presented by many researchers. Some of these technologies provide a considerable security measure but are not a practical solution in terms of reliability. A Blockchain-based SDN-IoT enabled application has been presented, but the architectural view, analysis, and performance in different parameters are not decently asserted [6]–[8].

In this study, a distributed Blockchain-based SDN-IoT enabled architecture for the smart building has been proposed. In this consideration, smart building helps as a reliable domain to mechanically handle and control the temperature, security, lighting, and other building procedures. Moreover, SDN based smart building provides several significant elements such as objectives, method scope, target architecture (Centralized network controller), communication protocols, resource configuration (Homogeneous and Heterogeneous), etc. Highlighting objectives are security, energy efficiency, network management, Reliability, QoS, and Reduce latency. Further, the communication protocols are WiFi, LiFi, Zigbee, and Bluetooth for SDN established smart building [8]. The main contributions of the paper mentioned as follows:

- A cluster head selection algorithm proposed to select a cluster head (CHs) including the fastest head selection and low energy dissipation for IoT forwarding devices.
- SDN with multiple controllers from the data layer utilized to control layer that proportion the burden among devices, comptroller, and denigrate packet loss efficiently.
- ‘‘DistBlockBuilding’’ architecture, which provides more proficient security for a surface to surface and more important privacy for apartments to apartments in the smart building applications, is also proposed.
- Finally, the performance of the SDN-IoT enabled network environment in different parameters simulated, which includes a distributed Blockchain technology for increasing the overall network efficiency.

The rest of the paper is structured as follows: The related works and research background addressed in Section II. The ‘‘DistBlockBuilding’’ architecture for a smart building control system has been proposed in Section III, and it has also discoursed how the proposed architecture can function in. After that, evaluation and performance analysis are represented in Section IV. Further, the authors have concluded the article in Section V with the importance and succeeding research scope.

## II. BACKGROUND AND RELATED WORKS

### A. BACKGROUND

#### 1) INTERNET OF THINGS (IoT)

The term ‘‘Internet of Things’’ first coined in 1999 considering a Radio Frequency Identification (RFID) concept [26]. The IoT is a tumultuous rising technology that permits physical devices to transmit across heterogeneous networks. The recent flourish in the IoT can be capable of allowing smart buildings, homes, and smart cities from plug to realism, where intelligent buildings should offer most of the IoT technologies. IoT provides several layers, such as the perception layer, network layer, and application layer. The perception layer incorporates wireless sensors, RFID, Cameras, and GPS, etc. Again, the network layer also allows the Gateways, Bluetooth, ZigBee, 2G, 3G, 4G, and WiFi, etc. [27]. The smart building, homes, cities, demand response, fault detection, and power lines are included by the application layer. The security aspects of IoT is privacy, trust, and data confidentiality. In the meantime, the main challenges of IoT are large scale, sensor networks, big data, reliability, security, legal and social aspects, and heterogeneity for smart technology.

Furthermore, IoT potential for smart cities includes smart communication, building, house, intelligent energy, and responsive customers. The IoT platform is used for utilizing the strength of smart buildings and homes as well. The state of the building is sensed incessantly by the IoT sensors to control the lighting and their intensities [28], [29].

### B. SOFTWARE-DEFINED NETWORKING (SDN)

SDN has been organized by two distinct layers, such as the data layer and control layer, which is shown in Fig. 2. The data layer maintains the IoT forwarding data, which is controlled by the SDN-enabled gateway. This gateway ensures the purity, confidentiality, and trusty of massive data in a proper way. The control plane of SDN is controlled by SDN controllers such as ONOS and ODL [4]. These SDN controllers include privacy, availability, security, confidentiality, configure the network [30], network services as well as increase the performance of the network accurately. SDN architecture provides some protocols such as OpenFlow, OpenStack, and OpenDaylight [31] for intercommunicating between the data layer and the control layer efficiently.

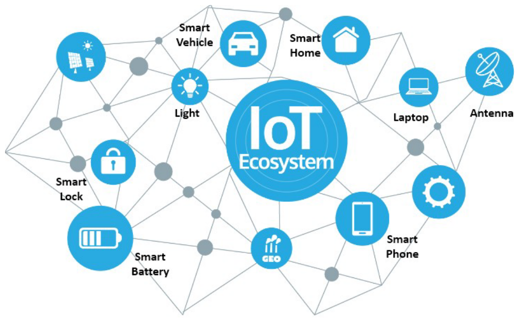


**FIGURE 1.** Internet of Things (IoT) architecture.

### 1) BLOCKCHAIN (BC) TECHNOLOGY

Blockchain is the integrated technology of Bitcoin, which was devised in 2008. It is called distributed ledger due to its nature. For example, ledger comprises of dissimilar blocks with different data-transactions that are enchained with each other applying cryptographic techniques such as hashing. Blockchain is the distributed and immutable list of elaborating blocks holding data as a transaction, which has shown in Fig. 3. Most notably, ledgers are evenly shared out a distributed network that guarantees transparency among Blockchain users. Once a block added to the ledger, it will be immutable. In case any participating node exchanged the transaction, chains in between collapse.

Besides, Blockchain can be classified into two categories, such as public and private Blockchain [33]. In a public Blockchain, anybody can connect after being consented.

Bitcoin and Etherum are public Blockchains. It turns slower due to excellent deal anonymity. This is another reason, and the public Blockchain cannot provide secure privacy and confidentiality in the desired system.

On the other hand, invitation or permission expected to link in the private Blockchain. As identity is already established, it has no anonymity that builds private Blockchain faster. Above all, privacy and confidentiality can be attained through particular protocols. Moreover, the conclusion is drawn as the concept of Blockchain as decentralized, open-source, transparent, autonomous, and immutable, etc. The application of Blockchain technologies [34] is the digital currency (Bitcoin), smart contract, hyper ledger, smart cities, grids, homes as well as smart building controlling system.

In summary, for our research perspective, the technical preliminaries IoT, SDN, and Blockchain technology are strongly dependent on each other. Firstly, IoT forwarding devices, as shown in Fig. 1 can be capable of forwarding it's all sensors information from the IoT concentered layer by using an efficient cluster head selection algorithm. Then SDN can control these sensors data in the data plane and control plane by utilizing the OpenFlow protocol. Besides, Blockchain provides automatic control security and confidentiality for surface wise as well as wise apartment management in the smart building application accurately.

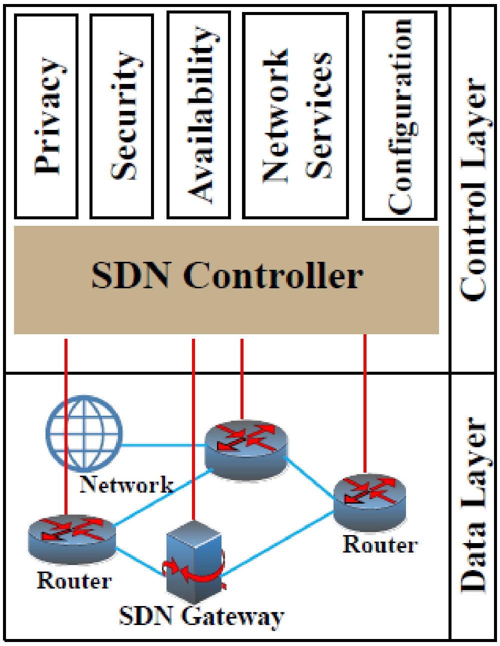


**FIGURE 2.** The architecture of SDN [32].

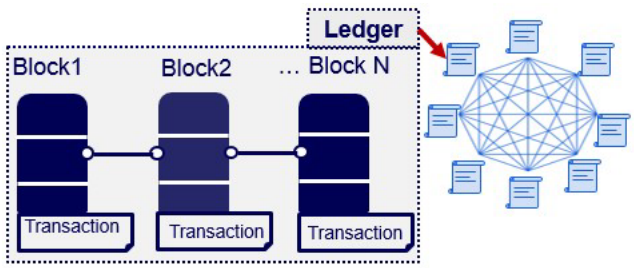


**FIGURE 3.** Distributed and Immutable Blockchain.

## C. RELATED WORKS

Several researchers have recently addressed emerging leading technology such as IoT, SDN, Blockchain, and other smart technologies in today's world. In this section, some literature reviews of recent works have been mentioned which are given below:

### 1) IoT NETWORKS IN SMART BUILDING

In [9], the authors defined the significant necessities for building a smart home. They mentioned seven unique requisite commendations for crating the specific quality of the smart home building blocks.

Biljana *et al.* highlighted several critical points for IoT-Enabled smart homes in [10]. They are:

- Smart home defining for a holistic framework with key features and parameters.
- An excellent explanation of a smart home management model based on the Holistic framework.
- Analyzing the current and future challenges for the Internet of Things based Results.

Authors discussed the IoT Necessities and smart architectures for smart buildings in [11]. They are also given the direction for energy optimization and the next propagation building management systems. Furthermore, they addressed some technical chances proffered and the technical disputes confronted by the IoT in the smart building field. Mehmood *et al.* [12] presented the IoT-enabled model for smart cities and also integrated with ICT, network categories, possible prospects, and significant desires. Again, they used several wireless technologies such as IEEE 802.11p, SIGFOX, 6LoWPAN, and LTE/LTE-A. Also, they highlighted some challenges and future research directions for smart technology. In [13], they tried to overcome several constraints in Bluetooth Low Energy (BLE) core building blocks by creating three contributions:

- They have been presented the design of a new open hardware platform for BLE.
- A Contiki O.S. port for the new platform is provided. - Identifying the research disputes and opportunities in 6LoWPAN connected Bluetooth Smart.

The authors also highlighted the many challenging parameters that could hypothetically progress the performance in the IoT scope.

### 2) SDN WITH IoT

A reliable SDN oriented IoT formation has evolved in [14]. The authors recommended a security-based structure for the IoT ecosystem utilizing the SDN. They considered the various security issues in IoT are examined.

Another related research [15] discussed two significant issues, such as security and privacy. Moreover, the authors presented an architecture for coupling SDN with IoT as well as particular networks. Further, they performed as a model for software based on the Software-Defined Network (DTN).

Similarly, the article [16] presented the structure of the model network, which is created based on the Laboratory of the IoT in the State University of Telecommunication. By using the model, the network enables network operators as well as service providers to make the network for the IoT real-time application services. Secure mechanisms are projected to handle different attacks [17]. The authors introduced the Middlebox placement and flow table capacity constraints for SDN. Again, they also demonstrated the experimental results that the proposed M-G model and can improve the overall IoT network safety and constancy.

### 3) BLOCKCHAIN INTEGRATING WITH SDN

Authors in [18] proposed the "DistBlockNet" model for IoT architecture. This architecture provides two significant advantages for networking technology, such as SDN and Blockchain technology. Then, they introduced a design for renewing a flow rule table utilizing a Blockchain method as well as validating the flow rule table. In addition, they also evaluated the performance in various metrics where their work represented a better result compare with the current work. Another similar research [19] proposed a permission Blockchain-based consensus imminent in distributed SDIIoT. The authors also used a new dueling in-depth Q-learning approach for better simulations process in the proposed scheme effectively. The authors [20] provided several overviews of the application domains of Blockchains in IoT, e.g., Internet of Vehicles, Internet of Energy, Internet of Cloud, Edge computing, etc. Furthermore, they also mentioned the five major attacks in the IoT networks, such as identity-based attacks, cryptanalytic attacks, reputation-based attacks, manipulation based attacks, and service-based attacks. Authors in [21] demonstrated the combination of Blockchains, SDN, and OpenStack. They tried to focus the Blockchain-based security over the software-defined technology (SDN). For file sharing purposes, they also used a distributed peer-to-peer basis using OpenStack as a cloud storage platform.

### 4) BLOCKCHAIN FOR SMART BUILDING

Xu *et al.* [22] presented a Blockchain-based DApp for smart building system with isolated Ethereum Blockchain, including Raspberry Pi (RPi), Blynk platform, and sensors. They provided some benefits for Blockchain technology in Uranus:

- tamper-resistant based.
- there is no single point of failure it has. - trusted and auditable.

Also, they built a proof-of-concept (POC) to simulate smart building applications as well as to validate its achievability and demonstrate its performance based on simulated work.

In the research [23], the authors presented an excellent integration between Blockchain technology (BCT) and Building Information Modeling (BIM) for a potential application. Moreover, they mentioned some aspects such as Hyper Ledger Fabric (HLF), distributed ledger technology (DLT), and reinforcing network security for more reliable data storage and management. In addition, the authors proposed the BCT and BIM framework to enhance the permitting process, security, trust, and positively impact post-disaster recovery efforts as well.

The authors discussed the excellent combination of ICT, IoT, and Blockchain for smart urban in [24]. Also, they mentioned some intelligent parameters, such as energy, safety, security, information management, and communication.

Moreover, they concluded that interoperability is a big challenge for smart city management or smart building.

The research [25] performed on how the Blockchain technology could be more beneficial in the building industry. Further, it used comprehensive enterprise solutions to manage building information as records using Blockchain. The authors addressed some lacking such as to estimate and respond to the case of the Blockchain, action of performance, and the design assignment to a particular level of detail - cannot be performed. In summary, several works are developed shown in TABLE 1. based on the above highlighted SDN-IoT and Blockchain, but no architecture and

**TABLE 1.** State of the art.

| Research Works | Used Technology | | | | Summary Contributions and Features |
|---|---|---|---|---|---|
| | Blockchain | Software Defined Networking | Internet of Things | Smart Building | |
| Minoli et al. [11] | × | × | √ | √ | Directed the energy optimization way and presented the future extension of building management systems |
| Sharma et al. [18] | √ | √ | √ | × | Proposed an excellent combination between Blockchain and SDN for IoT networks and presented flow rule table for validation of blocks as well |
| Qiu et al. [19] | √ | √ | √ | × | Proposed an imminent permitted blockchain-based consensus in distributed SDIoT and also efficiently used a novel dueling deep Q-learning approach |
| Ferrag et al. [20] | √ | × | √ | × | Provided several overviews of the Blockchains application domains in IoT, e.g., Vehicle Internet, Energy Internet, Cloud Internet, Edge Computing, etc. |
| Xu et al. [22] | √ | × | √ | √ | The intelligent building system with Ethereum Blockchain included Raspberry Pi (RPi), Blynk platform as well as sensors |
| Turk et al. [25] | √ | × | × | √ | Blockchain technology proposed to be more beneficial in the smart building sector |
| J. Islam et al. [4] | × | √ | √ | × | Presented a distributed black net with SDN-IoT architecture for smart cities and addressed the cluster head selection scenario |

management procedures are depicted. Thus this study provided a distributed architecture and processes based on Blockchain to manage the Smart Building. Besides, a cluster head selection algorithm for efficient clustering among the sensors and for exchanging data with low power is depicted.

## III. PROPOSED "DistBlockBuilding" FOR SMART BUILDING MANAGEMENT

For smart building, utilizing SDN implementation, a disseminated block building (DistBlockBuilding) SDN-IoT oriented architecture has been introduced. Fig. 4. illustrates the concept representing a dynamic environment for IoT network SDN technology is utilized. Furthermore, to analyze the architecture of physical networks and at the same time to improve the safety and privacy of the smart building purposes, authors have also performed Blockchain technology in these proposed network architecture.

The authors have been classified as the full application scenario into four distinct levels, as shown in Figure 4. They are-

- IoT Forwarding Devices
- SDN-IoT Enabled Gateway
- Secure and Distributed Blockchain Networking Approach
- Smart Building Management

### A. IoT FORWARDING DEVICES

IoT forwarding devices such as smart lighting, routers, switches, firewalls, smart TV, storage devices, etc. can be capable of forwarding data through the SDN standard gateways controller.

SDN dynamic gateway comptroller can filter the IoT devices data, and this process is helped by OpenFlow protocol. Further, DistBlockBuilding offers the security of data that assists in reaching these data to the application surface layer in the smart building blocks efficiently. But this discussion will be executed their different functions expeditiously if the IoT devices can be able to create a cluster head accurately. In this section, we introduced the cluster head selection procedure in Fig. 5.

After that, the significance of the cluster head selection algorithm, this algorithm allows selecting the cluster heads

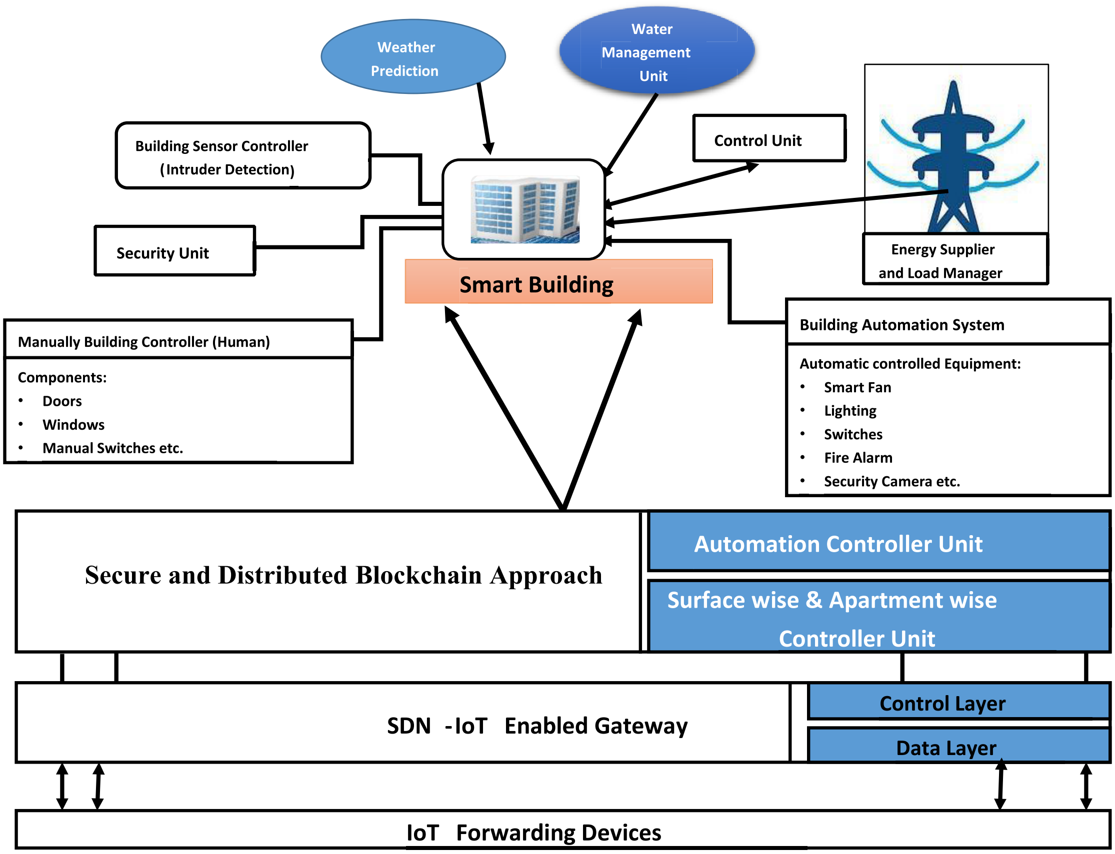


**FIGURE 4.** Proposed "DistBlockBuilding" architecture.

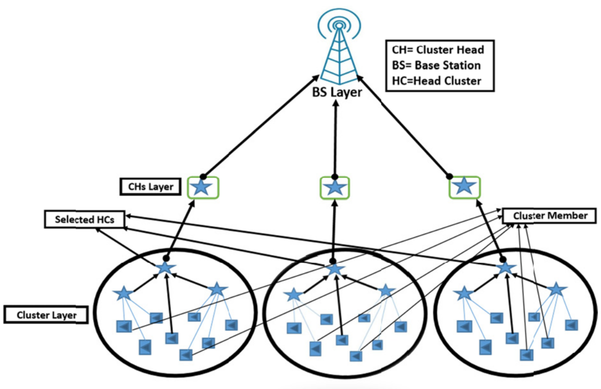


**FIGURE 5.** Cluster head selection scenario of IoT networks [5].

through the fastest process among the clusters that have been proposed. These CHs can be capable of forwarding the sensor's data to the trusted base station. This algorithm is designed to lower energy consumption and to enhance the lifetime of the network expeditiously.

### B. PROPOSED CLUSTER HEAD SELECTION ALGORITHM

By using this algorithm 1, the cluster heads among the sensors or nodes are selected. Further, the notation and symbols

**TABLE 2.** Symbol and their description.

| Symbol | Description |
|---|---|
| n | no. of devices in the list |
| SList | List of the IoT devices |
| cluster_no | sequence no. of the cluster |
| E_dist | Euclidean Distance |
| dist | Distance |
| CHList | Cluster Head List |

used in the algorithm given in Table-2. A set is provided to the algorithm, including all the nodes or sensors with some attributes like energy, radius to define the coverage area, position in the XYZ plan. In the algorithm, SList contains the sensors with a particular data structure containing the attributes. The variable cluster no returns the number of cluster heads at the end of the algorithm.

First of all, the variables are initialized for different purposes such as SList[i].ch is assigned to -1 to indicate the cluster head no. under which the ith sensor is allocated. The negative 1 means that the sensor is not allocated yet to any cluster head for data transmission. The list addressed as SList concerning the energy of the sensors has been sorted. Then the first sensor as a cluster head that has the highest energy was chosen as the list was sorted. Now the rest of

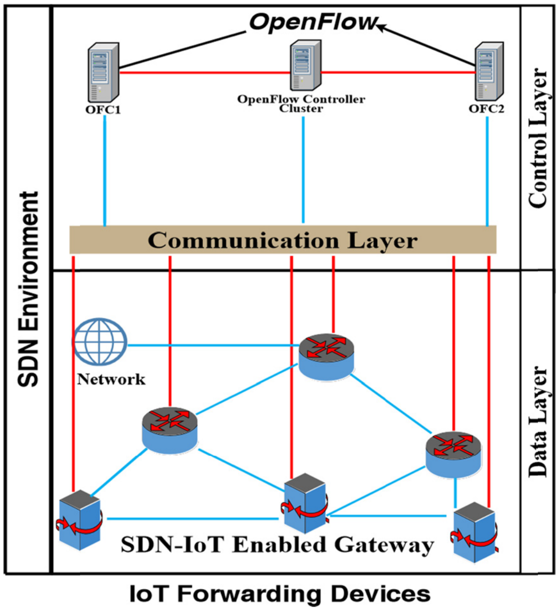


**FIGURE 6.** SDN-IoT enabled architecture.

the list is scanned, and the distance between two sensors is calculated shown as E_dist. The sensors that fall into the area of the cluster head selected earlier is added to another array named as SList[i].sensors shown in the algorithm, which also has the same data structure as the IoT sensors defined earlier in this section. Euclidean distance to measure the distance between two sensors has been selected. Here is the equation,

$$d(p,q) = \sqrt{(p_x - q_x)^2 + \left(p_y - q_y\right)^2 + (p_z - q_z)^2} \quad (1)$$

Every sensor contains the coordinates in the 3 dimension space (x,y,z), which is used to get the distance. SList[i].isHead indicates whether the ith sensor is a cluster head or not. This field is assigned by 1 when the sensor became a cluster head; otherwise, it is 0. After getting the cluster heads, the leaders are stored into the list named CHList, and each cluster head contains a list of sensors which are under the cluster head as seen in the SList[i].sensors is the list of sensors under the cluster head with the sensor which is a cluster head. This procedure is repeated until all the sensors are allocated under a cluster head.

### C. SDN-IoT ENABLED GATEWAY

SDN has separated the data plane to the control plane, as depicted in Fig. 6. The Software-Defined Networking (SDN) denotes a recent technology of network scheme, which serves to establish, measure, and establish the network [30]. The central benefits of SDN indicate to promote the execution of the network and construct the common efficient usage regarding the resourcefulness about the network. Data plan arrangements are also controlled automatically [35]. This environment [12] has adjusted with IoT network architecture, where SDN acts as a significant role in wireless network safety. In [36] and [37] adjustments on SDN architecture with the IoT networks for the wireless network has introduced. In this segment, the combination of SDN with the IoT environment into the present context, as shown in Fig. 6. The primary component is the Internet of Things (IoT) forwarding device level, which spirits, compiles, examines the data from the perception layer. Every IoT device forwards the data into SDN standard gateway, and this gateway is known as SDN-IoT enabled gateway. IoT controller produces the forwarding patterns, and each pattern grounded on the relating network communications protocol and communicates every rule of the SDN controller. SDN controller makes a network path within the objectives utilizing a routing algorithm. This controller not only defeating the heterogeneousness of materials but supervising the entering and outgoing transportation. Furthermore, by decoupling the data level from the control layer, the SDN controller can handle virtual machines, and for dissociating the accessible API is OpenFlow protocol [3]. Besides, by aggregating these technologies, networking environs are getting massive robust in terms of power expenditure, confidentiality, security, integrity, and execution optimization. Instead of applying a traditional gateway scheme, an SDN-IoT based gateway in our proposed application for efficient controlling has been utilized.

### D. SECURE AND DISTRIBUTED BLOCKCHAIN NETWORKING APPROACH

Blockchain is a P2P disseminated ledger technology that can monitor confidential proceedings, arrangements, contracts, and gross sales [38]. The main goal of Blockchain technology, it can ignore the third party interferer in smart communication and transaction systems. In this section, the Blockchain approach for a smart building has been is shown in Fig. 7.

Basically, the Blockchain process for securely and distributed communication purposes like surfaces to surfaces and apartments to apartments in the building blocks in a proper way has been used. The primary objectives of applying Blockchain technology in our proposed architecture named ''DistBlockBuilding'' are building automation control, including smart lighting, fan, switches, fire alarm, and security camera, etc. Another reason is surface wise as well as apartments wise security controlling of the building blocks by using this technology. Moreover, A Blockchain-based IoT scheme allows security, trust, confidentiality, unity, availability, authentication, authority, non-repudiation, and access control for the network appropriately [39]. A distributed Blockchain-based building has been presented, as shown in Fig. 7., which plies the deconcentrated controller. These controllers are affiliated efficiently and allow a vast number of insured data to entertain the desire for smart building control systems.

After that, every Blockchain command is controlled by request/respond signal into the building blocks suitably. This signal refers to a specialized database for the desired system. Then the whole information of smart building man-

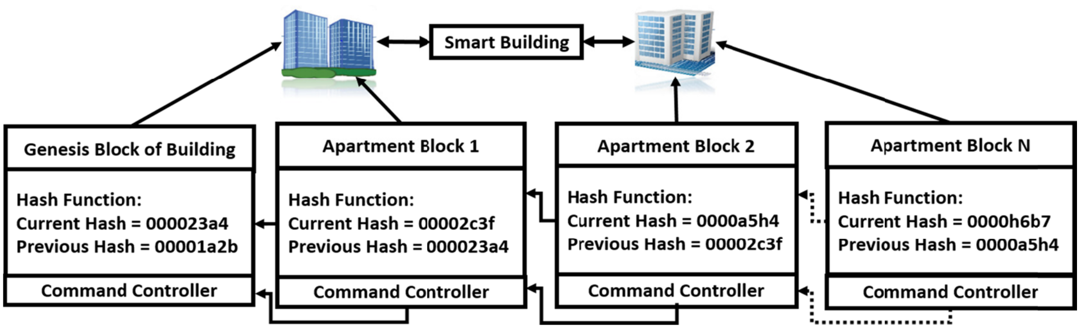


**FIGURE 7.** Distributed Blockchain approaches for smart building.

**Algorithm 1** Proposed Cluster Head Selection Algorithm

```
Input: Total Number of Nodes (N), Energy, Radius,
       Position in xyz plan for each node.
Output: No. of clusters and their members as arrays
Initialize the Variables
while (1) do
  SList.sort()
  cluster_no ← 0
  for i ← 1 to n do
    if SList[i].ch = -1 then
      SList[i].isHead ← 1
      for j ← 1 to n do
        if SList[j].isHead = 0 and SList[j].ch = −1
        then
          dist ← E_dist( SList[i], SList[j] )
          if dist <= SList[i].radius then
            SList[j].ch ← cluster_no
            SList[i].sensors.append(j)
          end
        end
      end
      CHList.append(SList[i])
      cluster_no ← cluster_no + 1
  end
end
```

agement is stored by its database [18]. Finally, a DistBlockBuilding controller for the Blockchain network, which provides more confidentiality, security, trust, availability, excellent privacy, and enhances the scalability, as well as improve the lifetime of the desired application, has been applied.

### E. SMART BUILDING MANAGEMENT

An intelligent smart building includes the security unit, control unit, weather predictor, water management unit, energy provider and load manager unit, building sensor controlling unit, etc. Where the control unit maintains an automatic and manual system of the desired building management. The security unit provides the auto secured process for detecting a third party or intruder of the smart building control. Then one of the essential units of an intelligent building is power and energy supplier unit, which can be capable of handling the whole energy load of the building for each service activation efficiently.

Also, intelligent buildings aid in producing and keep a safer and more insure, generative, and comfortable environment as cost-effectively as potential. Moreover, the automation unit of a smart building can give us huge benefits such as fire detection systems, CCTV, access control systems, and smart lighting, etc. Finally, an intelligent building can capable of establishing automation and highly protected services which can be able to guide our lives as well as to conduct our life very vigorously.

**TABLE 3.** Simulation environment.

| Evaluated Parameters Name | Parameter Values |
|---|---|
| Emulator | Mininet 2.2.1 |
| Simulation Area | 3000m X 3000m |
| Number of nodes | 1-100 |
| Simulation Times | 700s |
| Data Rate | 11Mbps |
| Packet Size | 100-512 bytes |
| Routing Protocol | OpenFlow |
| Measured parameters | Throughput and Round Trip Time (RTT) |

## IV. EVALUATION AND PERFORMANCE ANALYSIS

### A. ENVIRONMENT SETUP

To the Environment setup of our proposed methodology, Emulator (Mininet), Mininet-Wifi, OpenFlow protocol in the SDN environment for producing the goal outcomes has been deployed. Ubuntu (GNU/Linux) operating system, x86

Processor (2.20GHz), 6GB Primary Memory, and other external memory for evaluating our desired outputs have been used. Moreover, for visualizing the performance of the SDN-IoT network, the Wireshark platform was appropriately utilized. Simulation parameters, as shown in Table 3.

**TABLE 4.** Comparison of results.

| Study → / Issues ↓ | A. Rahman et al. [5] | Z. Qin et al.[40] | Y. Wang et al. [41] | A. Rahman et al. [proposed] |
|---|---|---|---|---|
| **Environment** | Mininet 2.2.1 | Qualnet Simulation platform | Modified Mininet 2.1.0 | Mininet-wifi |
| **Protocol** | OpenFlow | Opneflow like protocol in IP layer | Network Layer-3 protocol | OpenFlow protocol |
| **Throughput** | Almost similar for less no. of nodes but increases with the numbers of nodes | Suddenly falls after 5 sec of simulation | - | Progresses identically through the simulation |
| **Round Trip Time** | - | - | RTT increases over 20 ms for 100 nodes | RTT remains under 10 ms for 100 nodes |

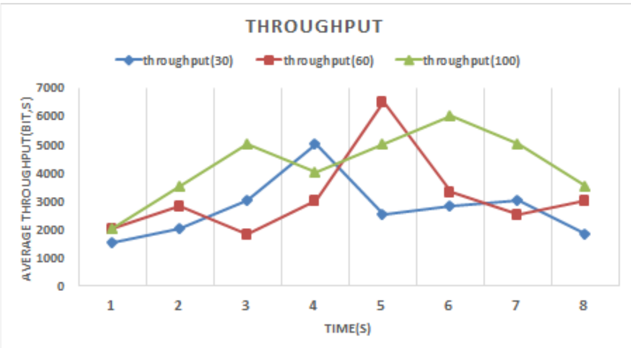


**FIGURE 8.** Average Throughput comparison (30 vs. 60 vs. 100 Nodes).

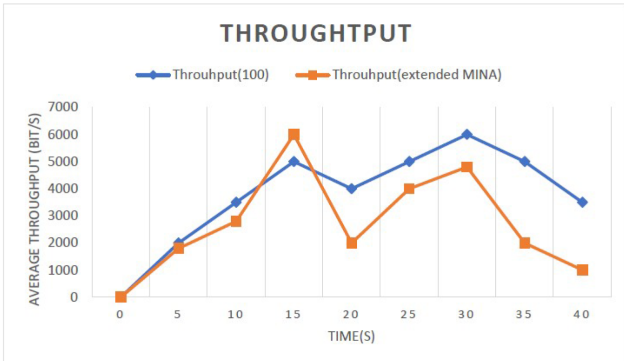


**FIGURE 9.** Average Throughput comparison (100 Nodes vs. Extended MINA).

## *B. SIMULATION AND PERFORMANCE MEASUREMENT OF SDN-IoT ENVIRONMENT*

Two parameters, such as Throughput, Round Trip Time (RTT), to measure the execution of the proposed methodology, has been used. The throughput is obtained by the equation Eq. (2).

$$\text{Throughput} = \frac{\sum_{n=i}^{n} CBRrece}{Simulation\ Time} \tag{2}$$

where CBR = Constant Bit Rate.

Here, figure 8 shows that the average throughput of 30, 60, and 100 nodes is approximately similar during 0-5s. Finishing the 5s, the average throughput for 30 and 60 nodes drops while throughput for 100 nodes grows identically.

Further, the authors take the best performer in throughput comparison (100 nodes) and compare it with Qin *et al.* [40], an extended version of the Multinetwork Information Architecture (MINA). Figure 9 shows the average throughput of both networks increase identically until they reach 6000bits/s but after 5s, the throughput of extended MINA suddenly falls down meanwhile the throughput of 100 nodes progresses similarly.

Again RTT has been shown for the different number of nodes. RTT is the time required to send a signal plus the time it takes to receive an acknowledgment of that signal. Initially, the authors compare to each other with their three (3) build topology. From Figure 10 it's clear that when the number of nodes increases, the round trip time decreases. As a result, the lowest time required for a round trip is for 100 nodes. Furthermore, the authors compare the 100-node RTT to another Wang *et al.* OpenFlow-based protocol [41]. The result of this is shown in Figure 11. It is notified that with increasing the time RTT of 100 nodes reaches in a stable

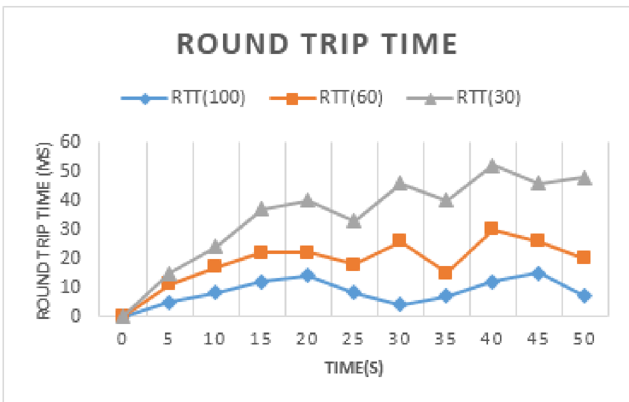


**FIGURE 10.** RTT comparison (100 vs. 60 vs. 30 Nodes).

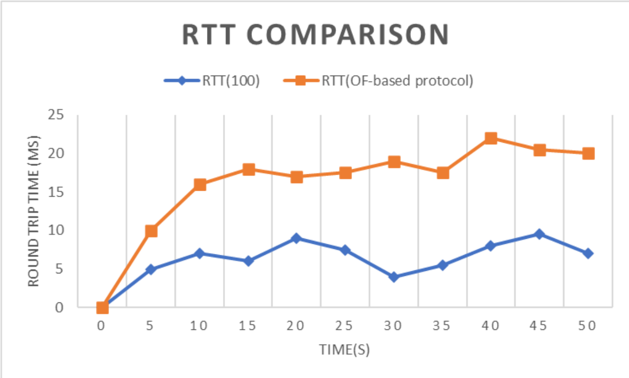


**FIGURE 11.** RTT comparison (100 Nodes vs. OF-based Protocol).

state. On the other hand with the increase, the time OF-based protocol is also rising according to Table 4.

## V. CONCLUSION

Nowadays, IoT, Blockchain, SDN, and smart building technologies services and facilities are known as immure as well as imprison technologies to the researchers. But these technologies demand and scope to the researchers very increasingly. There is a considerable threat to growing SDN based IoT networks in good order. Further, only several numbers of research workers are equating successful in these threats. By this presumption, a distributed Blockchain-based SDN with IoT enabled gateway for a smart building control system and a modern cluster head selection algorithm has been proposed. In an SDN-based network that has been multiple dynamical controllers, these controllers can be capable of improving more privacy, excellent security, accessibility, integrity, and overall security. Furthermore, distributed secure Blockchain building (DistBlockBuilding) in IoT network that provides the smart lighting, firewalls, switches, and secured camera services for the intelligent building control system has been offered. In the Implementation and result Analysis environment, the performance measurement in the SDN-IoT networking platform for smart building management has been utilized. It can provide energy preservation and load management tools for SDN-IoT architecture in the distributed Blockchain-based networks.

In the future, the efficient performance evaluation of Blockchain architecture will be added in different parameters for our proposed model in a proper way.

## REFERENCES

[1] K. Kalkan and S. Zeadally, "Securing Internet of Things with software defined networking," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 186–192, Sep. 2018.

[2] S. Chakrabarty and D. W. Engels, "A secure IoT architecture for smart cities," in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2016, pp. 812–813.

[3] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Mar. 2008.

[4] M. J. Islam, M. Mahin, S. Roy, B. C. Debnath, and A. Khatun, "DistBlackNet: A distributed secure black SDN-IoT architecture with NFV implementation for smart cities," in *Proc. Int. Conf. Electr., Comput. Commun. Eng. (ECCE)*, Feb. 2019, pp. 1–6.

[5] A. Rahman, M. J. Islam, F. A. Sunny, and M. K. Nasir, "DistBlockSDN: A distributed secure blockchain based SDN-IoT architecture with NFV implementation for smart cities," in *Proc. ICIET*, 2019, pp. 1–6.

[6] K. Akkaya, I. Guvenc, R. Aygun, N. Pala, and A. Kadri, "IoT-based occupancy monitoring techniques for energy-efficient smart buildings," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Mar. 2015, pp. 58–63.

[7] T. M. Lawrence, M.-C. Boudreau, L. Helsen, G. Henze, J. Mohammadpour, D. Noonan, D. Patteeuw, S. Pless, and R. T. Watson, "Ten questions concerning integrating smart buildings into the smart grid," *Building Environ.*, vol. 108, pp. 273–283, Nov. 2016.

[8] M. U. Younus, S. U. Islam, I. Ali, S. Khan, and M. K. Khan, "A survey on software defined networking enabled smart buildings: Architecture, challenges and use cases," *J. Netw. Comput. Appl.*, vol. 137, pp. 62–77, Jul. 2019.

[9] T. K. L. Hui, R. S. Sherratt, and D. D. Sánchez, "Major requirements for building smart homes in smart cities based on Internet of Things technologies," *Future Gener. Comput. Syst.*, vol. 76, pp. 358–369, Nov. 2017.

[10] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *J. Cleaner Prod.*, vol. 140, pp. 1454–1464, Jan. 2017.

[11] D. Minoli, K. Sohraby, and B. Occhiogrosso, "IoT considerations, requirements, and architectures for smart buildings—Energy optimization and next-generation building management systems," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 269–283, Feb. 2017.

[12] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things-based smart cities: Recent advances and challenges," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 16–24, Sep. 2017.

[13] S. Raza, P. Misra, Z. He, and T. Voigt, "Building the Internet of Things with Bluetooth smart," *Ad Hoc Netw.*, vol. 57, pp. 19–31, Mar. 2017.

[14] C. Vandana, "Security improvement in IoT based on software defined networking (SDN)," *Int. J. Sci., Eng. Technol. Res.*, vol. 5, no. 1, pp. 2327–4662, 2016.

[15] F. Al Shuhaimi, M. Jose, and A. V. Singh, "Software defined network as solution to overcome security challenges in IoT," in *Proc. 5th Int. Conf. Rel., Infocom Technol. Optim. (Trends Future Directions) (ICRITO)*, Sep. 2016, pp. 491–496.

[16] R. Kirichek, A. Vladyko, M. Zakharov, and A. Koucheryavy, "Model networks for Internet of Things and SDN," in *Proc. 18th Int. Conf. Adv. Commun. Technol. (ICACT)*, Jan. 2016, pp. 76–79.

[17] Y. Liu, Y. Kuang, Y. Xiao, and G. Xu, "SDN-based data transfer security for Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 257–268, Feb. 2018.

[18] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.

[19] C. Qiu, F. R. Yu, F. Xu, H. Yao, and C. Zhao, "Permissioned blockchain-based distributed software-defined industrial Internet of Things," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–7.

[20] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[21] S. R. Basnet and S. Shakya, "BSS: Blockchain security over software defined network," in *Proc. Int. Conf. Comput., Commun. Automat. (ICCCA)*, May 2017, pp. 720–725.

[22] Q. Xu, Z. He, Z. Li, M. Xiao, R. S. M. Goh, and Y. Li, "An effective blockchain-based, decentralized application for smart building system management," in *Real-Time Data Analytics for Large Scale Sensor Data*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 157–181.

[23] N. O. Nawari and S. Ravindran, "Blockchain and building information modeling (BIM): Review and applications in post-disaster recovery," *Buildings*, vol. 9, no. 6, p. 149, Jun. 2019.

[24] C. Lazaroiu and M. Roscia, "Smart district through IoT and blockchain," in *Proc. IEEE 6th Int. Conf. Renew. Energy Res. Appl. (ICRERA)*, Nov. 2017, pp. 454–461.

[25] Ž. Turk and R. Klinc, "Potentials of blockchain technology for construction management," *Procedia Eng.*, vol. 196, pp. 638–645, Jan. 2017.

[26] K. Ashton, "That 'Internet of Things' thing," *RFID J.*, vol. 22, no. 7, pp. 97–114, 2009.

[27] M. Jaradat, M. Jarrah, A. Bousselham, Y. Jararweh, and M. Al-Ayyoub, "The Internet of energy: Smart sensor networks and big data management for smart grid," *Procedia Comput. Sci.*, vol. 56, pp. 592–597, Jan. 2015.

[28] X. Ye and J. Huang, "A framework for cloud-based smart home," in *Proc. Int. Conf. Comput. Sci. Netw. Technol.*, vol. 2, Dec. 2011, pp. 894–897.

[29] L. Martirano, "A smart lighting control to save energy," in *Proc. 6th IEEE Int. Conf. Intell. Data Acquisition Adv. Comput. Syst.*, vol. 1, Sep. 2011, pp. 132–138.

[30] D. Kreutz, F. M. V. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," 2014, *arXiv:1406.0440*. [Online]. Available: http://arxiv.org/abs/1406.0440

[31] D. Chourishi, A. Miri, M. Milic, and S. Ismaeel, "Role-based multiple controllers for load balancing and security in SDN," in *Proc. IEEE Canada Int. Humanitarian Technol. Conf. (IHTC)*, May 2015, pp. 1–4.

[32] M. Ojo, D. Adami, and S. Giordano, "A SDN-IoT architecture with NFV implementation," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2016, pp. 1–6.

[33] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[34] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.

[35] H. Kim and N. Feamster, "Improving network management with software defined networking," *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 114–119, Feb. 2013.

[36] S. Costanzo, L. Galluccio, G. Morabito, and S. Palazzo, "Software defined wireless networks: Unbridling SDNs," in *Proc. Eur. Workshop Softw. Defined Netw.*, Oct. 2012, pp. 1–6.

[37] Á. L. V. Caraguay, A. B. Peral, L. I. B. López, and L. J. G. Villalba, "SDN: Evolution and opportunities in the development IoT applications," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 5, May 2014, Art. no. 735142.

[38] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[39] S. Roy, M. Ashaduzzaman, M. Hassan, and A. R. Chowdhury, "BlockChain for IoT security and management: Current prospects, challenges and future directions," in *Proc. 5th Int. Conf. Netw., Syst. Secur. (NSysS)*, Dec. 2018, pp. 1–9.

[40] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian, "A software defined networking architecture for the Internet-of-Things," in *Proc. IEEE Netw. Oper. Manage. Symp. (NOMS)*, May 2014, pp. 1–9.

[41] Y. Wang and J. Bi, "A solution for IP mobility support in software defined networks," in *Proc. 23rd Int. Conf. Comput. Commun. Netw. (ICCCN)*, 2014, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6911783/, doi: 10.1109/ICCCN.2014.6911783.