ISSN 2712-0562
Sustainable Engineering and Innovation *Original Research*
Vol. 4, No. 1, February 2022, pp.8-21
https://doi.org/10.37868/sei.v4i1.id153

A blockchain-based trust management system for 5G network slicing enabled C-RAN

Asrar Ahmed Baktayan[1*], Ibrahim Ahmed Albaltah[1]
[1] Department of Information Technology, FCIT, Sana'a University, Sana'a, Yemen

*Corresponding author: asrar@yemenmobile.com.ye

Received Nov. 6, 2021
Revised Jan. 5, 2022
Accepted Jan. 27, 2022

Abstract
The mobility nature of the wireless networks and the time-sensitive tasks make it necessary for the system to transfer the messages with a minimum delay. The Cloud Radio Access Network (C-RAN) reduces the latency problem. However, due to the trustlessness of 5G networks resulting from the heterogeneity nature of devices. In this article, for the edge devices, there is a need to maintain a trust level in the C-RAN node by checking the rates of devices that are allowed to share data among other devices. The SDN controller is built into a macro-cell that plays the role of a cluster head. The blockchain-based automatically authenticates the edge devices by assigning a unique identification that is shared by the cluster head with all the C-RAN nodes connected to it. Simulation results demonstrate that compared with the benchmark, the proposed approach significantly advances the processing time of blocks, the detection accuracy of malicious nodes, and transaction transmission delay.

© The Author 2022.
Published by ARDA.

Keywords: Blockchain; C-RAN; MEC; Heterogeneous networks; SDN, Trust management

1. Introduction

Fifth-Generation (5G) networks will be very flexible, and they require sophisticated programmable software for cellular mobile users and other types of service networks. The 5G networks will serve many tenants depending on their characteristics and requirements. With the vast number of IoT and vehicles supplying improved communication capacity, lower transmission latency, and higher data rates, 5G mobile cellular networks are gradually taking over the 4G mobile network environment. Smaller cells, such as Micro, Femto, and Pico, can provide greater throughput and reduced latency in this environment. [1]. Besides, for the IoT and Intelligent Transportation System (ITS), Mobile Edge Computing (MEC) is presented to achieve similar goals [2].

5G cellular networks are likely to be dense, with each device requiring significant bandwidth to enable multimedia applications with stringent quality of service (QoS) expectations [3]. The excellent physical properties of mmWave (up to 60 GHz) can help with short-range, high-data-rate communication. Because of the limited coverage of 5G cells. Clustering, on the other hand, is one of the approaches for improving wireless network handover, offloading, and energy efficiency by balancing load and energy consumption among cells [4] [5]. Software-defined networks (SDN) and the Cloud Radio Access Network (C-RAN) are emerging as promising technological solutions for next-generation communication with a large number of heterogeneous devices and applications. These technologies make effective network resource sharing and flexible task scheduling possible across a wide range of cells. [6]. As shown in Fig.1, the separation of the control plane and the data plane, which can improve system resilience and scalability, is a key feature of SDN. As a result of this

This work is licensed under a Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/) that allows others to share and adapt the material for any purpose (even commercially), in any medium with an acknowledgement of the work's authorship and initial publication in this journal.

strategy, networks become programmable, centrally controlled, adaptive, and optimized for maximum efficiency [7]. It can communicate with the Open Flow-Switches and a pool of Base Band Units (BBUs) in real-time to obtain RAN state information. As a result, the SDN controller can intelligently distribute resources for BBUs depending on their load state, as well as adjust the connections between Remote Radio Heads (RRHs) and BBUs to generate logic cells based on the device's mobility. As a result, the SDN network becomes more intelligent and flexible, allowing it to fulfill resource demands in various locations covered by RAN cells [8].

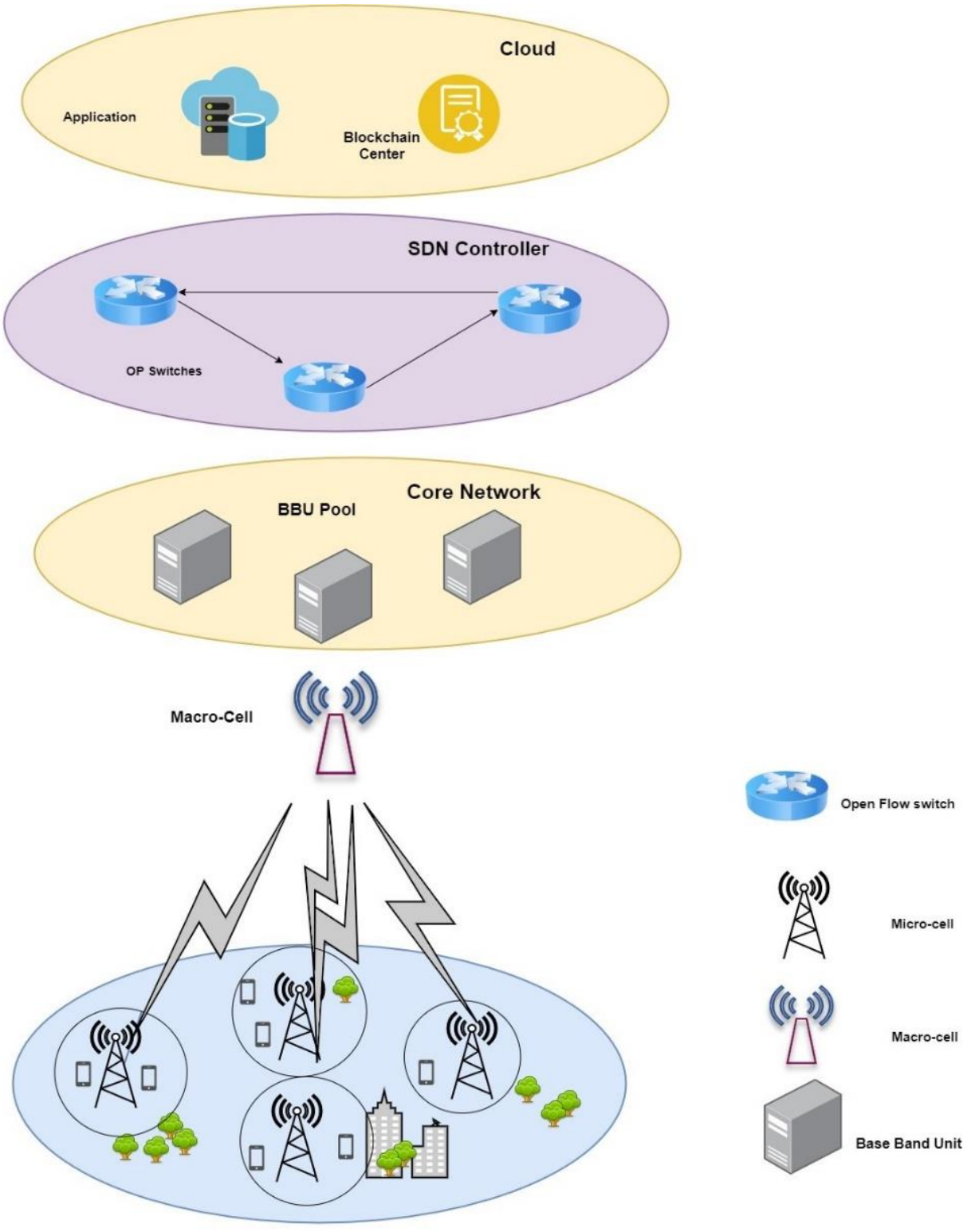

Figure 1. C-RAN enabled SDN architecture

5G devices are diverse, employing several different technologies for various purposes. As a result, maintaining their consistency and dependability is tough. On the other hand, using the clustering strategy can assist reduce base station (BS) overhead and delay. Each cluster has a single cluster head device; each BS cell's device serves as a cluster head or is served by a BS through the appropriate cluster head. Device-to-Device (D2D) transmissions are used for intra-cluster communication. In the uplink, the D2D connection is established from the cluster device to the cluster head. Consequently, the downlink traffic of a clustered device is first given downlink resources (from the BS to the cluster head) and then from the cluster head to the clustered device. Among all the clustered devices, the cluster head device should have the best link to the BS. As a result, downlink resources are conserved [9].

Using blockchain in wireless networks makes the exchange of information and the transfer of keys unnecessary [10]. To build public ledgers, the mined blocks are circulated around the network. Furthermore, depending on the sort of Artificial Intelligence (AI) algorithms employed, the transaction process could take a significant period of time [11]. To verify the authenticity of transactions, the blockchain employs asymmetric private/public key and hash cryptography algorithms. Each node's private key is used to sign transactions, while the public key is broadcast to all network nodes and serves as an identity. The network's mining nodes collect new transactions and attempt to resolve a consensus rule. When a node achieves mechanism consensus, it broadcasts the block to all other nodes.

As a result, every other node that receives the block will verify the transaction and acknowledge it by constructing the next block in the chain [12] [13]. In the same context, using edge computing with cellular networks improves the QoS of different industries and services for 5G application domains, which provide processing, computing, and storage capabilities near edge devices [14]. Besides, trust management is widely discussed, especially in wireless networks. Due to wireless and mobility nature, devices become open to many attacks throughout the communication. Blockchain's distributed nature makes it an intriguing piece of equipment for tackling many of the security and trust issues that arise in large-scale IoT networks with limited resources. Blockchain is used for decentralized applications that do not require interaction with a trusted third party [15]. Many authors focus on building trust in sensors and IoT with limited power and storage using blockchain technology to allow newly joined devices to set up trust instantly [16] as in Industrial IoT (IIot) [17], Wireless Sensor Network (WSN) [18] and wearable devices [19].

The development of a 5G communication system requires fast response, authorized power consumption, and secure communication between different devices connected to the heterogeneous networks. In this article, hierarchical architecture is proposed as a cluster to reduce energy consumption by building a trust zone for every cluster and connecting this zone with other clusters with the help of SDN and blockchain. The zone begins with a macro-cell Radio Access Technology (RAT) that contains the SDN controller; every macro-cell controls many C-RAN nodes. Therefore, the C-RAN node could use the blockchain's Delegated Proof of Stake algorithm (DPoS) to securely broadcast all devices' *IDs* automatically to every device in its coverage as used in [20]. As a result, the device can start D2D immediately without previous authentication. The contribution of this article can be summarized as: a) Macro-cell using the SDN controller to control all devices in its zone and working as a cluster head. b) Using public blockchain in C-RAN nodes is beneficial to dynamically distribute devices' *IDs* to the public ledger list to all devices under their control, so every device has a list of trusted entities. There is no need to reregister. c) C-RAN nodes perform automatic access control by assigning *IDs* to all connected devices via blockchain. d) Zones are connected to each other by using a private blockchain since the mobile operators verify the macro-cell.

The rest of this article is organized as Sec. 2 proposes a related work. Sec. 3 establishes blockchain-based trust for 5G networks.Sec.4 discusses the blockchain for trust and energy consumption. Sec. 4 provides the calculation of the proposed architecture. Sec. 5 provides the simulation results and evaluation. Sec.6 concludes this article.

1.1. Related work

The RAN is being developed to provide increased data speeds and capacity, as well as efficient spectrum utilization, low energy consumption, and widespread device connectivity [21]. Many new technologies are being merged to pave the way for 5G networks, including SDN, C-RAN, and NFV. The SDN controller, which is connected to a private blockchain [22] [23], administers and controls the entire C-RAN network.

In [24], the integration of the SDN controller with the blockchain was introduced. The network information and the blockchain ledger are stored using data from OF-Switches and the BBU pool. As shown in Fig.2 [25], this data includes the load on BBUs, resource allocation, device information, handover information between adjacent cells, information about every block in the blockchain, and the entire network topology information, which is used to choose the closest paths between Edge-RRHs and BBUs. The Blockchain operates between two end-to-end peer servers in a distributed or centralized controller. Thus, this idea has advantageous effects on end-to-end security management by reducing the complexity of the system deployment and latency taken for the end-to-end secure session setup [26]. In addition, SDN controllers are expected to handle the control traffic coming from C-RANs. As a result, the SDN controller is positioned in a macro-cell closer to the edge of the network. This design adds scalability to the control plane by directly handling wireless specific functions as a distributed control for the edge 5G network as provided in [27]. Therefore, SDN controllers can still be distributed and perform centralized control for each cluster to decrease management complexity while keeping part of the centralization benefits. There is also the possibility to pool resources, such as radio frequencies and processing power, under the control of SDN controllers in C-RAN, as in [28] [29]. The controllers in the C-RAN network are interconnected in a distributed private blockchain network, allowing each device to easily and efficiently transport data across the network without disclosing private information or requiring re-authentication. Many studies have been conducted in the area of optimizing SDN clusters and C-RAN, which is characterized by functional redistribution.

In [12], SDN controllers are distributed as a series of slave and master controllers. In remote locations, master controllers managed a set of macro-cells and acted as coordinators for slave controllers. Slave Controllers operated as a management unit for a set of small cells, providing a short-time scale. Furthermore, as demonstrated in [30] [31], combining blockchain with an SDN clustering design lowered the susceptibility and energy spent by IoT devices in the Mobile Edge Computing (MEC) structure while also providing a better. Authors in [32] focused on using blockchain for distributed trust and preventing malicious devices that disturb ordinary traffic by broadcasting a lot of false information. Those devices will be traced back to the system and temporarily banned. Consequently, the privacy of legitimate devices will be safe and their information will be protected. In work [33], the blockchain nodes must solve the nonce. The other nodes in the network verify the winning node's result. If at least 51 percent of the nodes agree with the transaction, the winning node adds it to the block and receives the reward. A blockchain is created and maintained as a result of this procedure. Hackers find it difficult to breach the Proof of Work (PoW)-based blockchain because they must compromise 51 percent of the network nodes, which takes time & expense. In addition, the SDN controller made use of a Genetic Algorithm (GA) to discover the most efficient data transmission paths. A lightweight trust model based on blockchain technology was developed by [34], and it produced the bare minimum requirements for supply chain actors to have confidence in the data they are receiving. A trust evaluation is carried out when a client node launches a transaction and requests endorsements from nearby nodes. In order for a transaction to be fully entered into the ledger, the client node needs to transmit transaction proposals to all accessible endorsing peers. Using a chain code, the endorsing peer nodes examine the trust score of the beginning node. The benchmark for this work is [35]. The authors focused on security and privacy issues in the transportation system and the vehicular IoT environment. Due to the decentralized and immutable properties of blockchain, a blockchain-based security framework is being created to support vehicular IoT services such as real-time cloud-

based video reports and trust management in vehicular messaging. The authors exhibited the SDN-enabled 5G-VANET paradigm as well as the scheduling algorithms of the blockchain-based architecture.

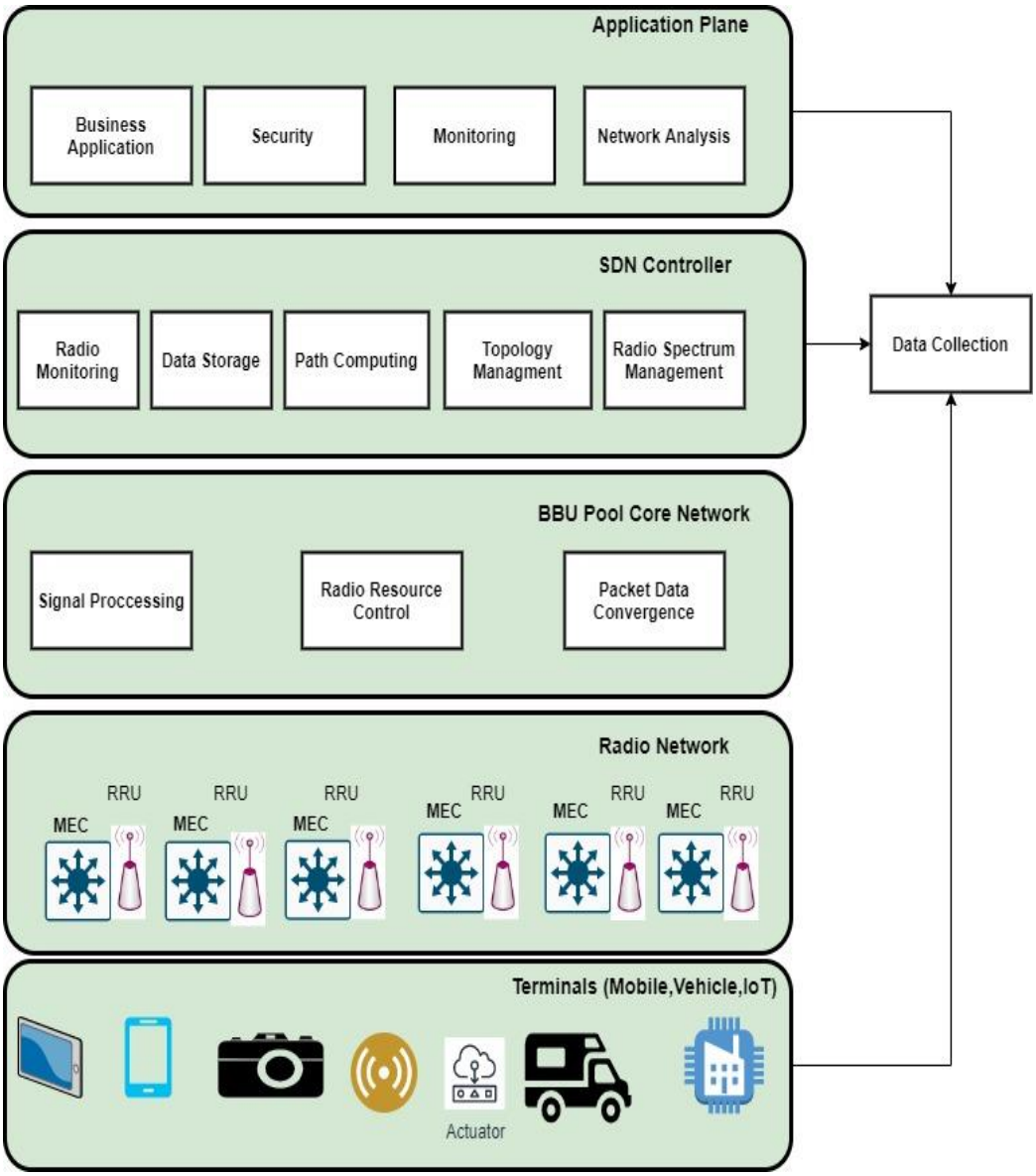

Figure 2. SDN Layer integrated with C-RAN

1.2. Trust in 5G networks powered by blockchain

All the edge devices are connected to C-RAN nodes, which are shared among macro-cell RATs in heterogeneous networks. The number of C-RAN nodes is much bigger than the number of macro-cell RATs in the proposed architecture, as shown in Fig.2. However, cryptographic techniques used in mining blocks prevent malicious devices from altering or deleting the blockchain [36]. The DPoS consensus is a mechanism to ensure trust in the wireless network, so C-RAN nodes in the network commonly agree on any block inserted into the chain. DPoS is the best well-known consensus algorithm that can be used in real-time voting to create a group of trusted delegate nodes that can verify the blocks. These C-RAN nodes have the authority to produce and contribute blocks to the blockchain network. Similarly, miner C-RAN nodes prevent rogue nodes from participating in block addition [37]. As a result, the number of nodes participating in voting will be reduced, resulting in a shorter creation block time and lower computing overhead in the PoW process, resulting in lower power consumption.

In general, network partners in DPoS are unpredictable when it comes to making negative judgments for the network. Through a distributed ledger that contains all of the transactions on the blockchain, the blockchain enables reliable and secure services. The transaction ledger is settled by multiple trusted C-RAN nodes in various places. The legitimacy of transactions can be monitored by all C-RAN nodes. The asymmetric encryption and certification technology stored on the blockchain is public, but it is deeply encrypted and can only be accessed with the permission of the data owner, unlike the public device identification (device *ID*). Furthermore, the effectiveness of a blockchain transaction is determined by the usage of a consensus method, which precludes tampering [38]. In heterogeneous cellular networks, DPoS is preferable because mobile network operators (MNOs) choose C-RAN nodes, which are employed as miners and validated by a public blockchain. In a DPoS blockchain, for example, a certified node (C-RAN node) verifies the transaction and the block without incurring the high computational costs of mining, as shown in Fig.3. The time it takes to add a new block to the blockchain is reduced because of this mining process. This C-RAN validator node needs to authenticate on the blockchain, which is difficult to come by. Even if there is a malicious C-RAN node, it will be stopped out by other C-RAN nodes' votes similar to [39]. On the other hand, cluster heads (macro-cells) connect with one another via a private blockchain maintained by a central SDN controller. The blockchain network's distributed nature ensures greater resilience in the event of a system failure. To reduce energy consumption, message transfer between wireless heterogeneous devices should have low latency and as few steps as possible [11]. To solve this problem, the blockchain in the proposed architecture might be distributed, i.e., many blockchains handling different tasks, one blockchain to serve only one task. It is better to have a separate blockchain for access control, another for D2D, and one for connecting clusters so that every process is faster and independent of others.

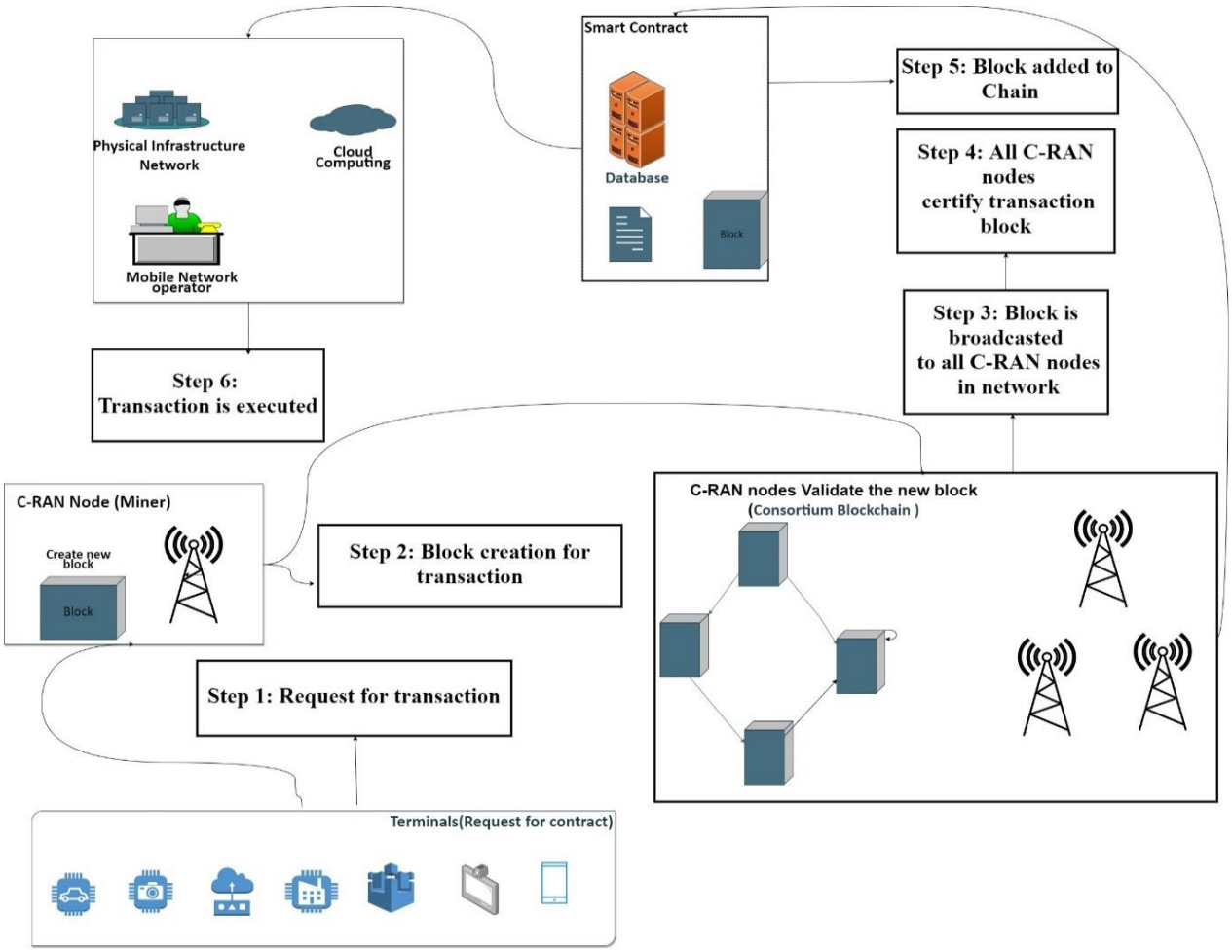

Figure 3. Consortium blockchain for the C-RAN network

The network's quality of service (QoS) is determined by the data received from edge devices. To overcome this challenge, Edge computing is used, which is closer to the edge device [40] [41] and can be shared among many MNOs. These C-RAN nodes can be designed as a trusted point that uses the public blockchain to permit any new device to connect. The message exchange in the wireless networks could be facilitated by using the blockchain mining process since the blockchain structure releases decentralized authentication. C-RAN nodes communicate with one another by mining blocks and broadcasting the results to all network cells. Transaction signatures are checked to see if the information in the transactions is reliable. Furthermore, ciphertext in transactions is secured from decryption until it reaches the destination because it is encrypted with the destination's public key [11], which is the device's *ID* in the proposed trusted system, and decrypted using the edge device's private key.

2. Research method

2.1. Proposed approach and calculation

Blockchain allows devices to communicate with each other and with C-RAN nodes without sharing personal information [42] [43]. The C-RAN node is used as a gateway to allow new devices to access the system and monitor its trustworthiness. The central trust point (cluster head) is used for authenticating devices and having *ID*s as registered numbers. These *ID*s are provided to build trust and communicate safely with C-RAN nodes and between devices themselves. In this way, any device that asks for a service for the first time will be authenticated by a public blockchain. This authentication will be accomplished through the use of a smart contract and several blockchain transactions.

Similar to [44], as a first step, edge devices have to be registered, then the edge device will be able to request any service. When the edge device with no *ID* forwards the request to the C-RAN node, the MNO immediately accesses the server data of the related tenant to get the data requested. When the C-RAN node gives the response to the edge device, it will legitimize the service first with the help of smart contracts to ensure whether this service is secure or not. Then, the device will be registered on the public blockchain with the lowest possible trust value. After that, whenever a device sends a request to the C-RAN node for the services, it will be in an encrypted form. While some devices will always misuse information or offer false information to the network, the blockchain method can assess the trustworthiness of data and alert the relevant device several times. The blockchain restricts the device if it continues to submit misleading data [45]. However, when the edge devices communicate with each other (like in D2D communication), they validate messages received from the neighboring devices. Through this validation, the edge device generates a trust rate for the device that sends the correct information. The rate is then uploaded to the C-RAN node, which calculates the trust value of that device from all other devices that are communicated with it. Then the C-RAN node sends the device's trust value to the macro-cell, which stores this rate in the private blockchain that connects all macro-cell RAT in heterogeneous networks.

For the establishment of trust throughout many layers in clustering architecture, the C-RAN nodes act as mediators. When a service transaction starts, the devices and MNO agree on the service contents and keep the service parameters in the C-RAN node [46]. The edge device is identified by a unique *ID* provided by the public blockchain in the same cluster controlled by its SDN controller. This *ID* is unique universally as a MAC address In simple words, an edge device starts a connection with the C-RAN node to get a unique identification for trust evaluation from the blockchain. After authentication is done between the edge device and the cluster head (macro-cell) by validating the data received from the edge device. The edge device collects its data and forwards it to the MEC with its public key (device *ID*) which in this case is assumed as N_{id} (node identification) with its $RV_{Nid}s$ (Reputation Values given by a specific device to rate other devices that have a previous interaction with). On the other hand, $RD_{Nid}s$ is the list of devices' reputations in the C-RAN node database that is collected from the devices, which had communicated with the device N_{id}. The trust rate of any device can be expressed

as a real number between -1 (showing untrusted) and 1 (fully trusted) [48]. When a device receives an invite from another device (row 2 in algorithm 1), it determines whether that device has a trust value stored (row 6) or not. Since the C-RAN nodes send the list of trusted devices periodically, all devices have a list of legitimate devices to avoid any connection with a malicious device and reduce the energy consumed in validating the connection with any other device. If the new device is not in the list of this C-RAN node, it will search for it in surrounding C-RAN nodes (rows 8 to 13).

Algorithm 1 Trust among devices

Input: Received Req ≠ ∅
output: RD_{Nid} ≠∅ // reputation database for specific device
1: while true do
2: req ⇐ receive();
3: req id ⇐ req.id;
4: if trust RD_{Nid}s list.find(req id) ≠ ∅ then // the requested id is stored in device's list
5: {trust} ⇐ if trust RD_{Nid}s list.take(req id);
6: req id ⇐ req.id;
7: end if
8: if trust RD_{Nid}s list.find(req id) = ∅ then // the requested id is not stored in the device's trust RD_{Nid}s list, so the device will ask C-RAN node
9: send ⇐ {TRUST REQ, req new id}; // C-RAN node investigates a new device in surrounding C-RAN nodes
10: trust RD_{Nid}s list.put(req id, trust); // put the new RD_{Nid} in trust RD_{Nid}s list
11:msg ⇐ {UPDATE trust RD_{Nid}s list} // C-RAN node sends the updated list to device
12: else
13: send(ERROR, req reject); // trusted device rejects request from suspicious device
14: end if
15: end while

On the other hand, when the new device communicates with the C-RAN node for the first time, i.e., it is not registered anywhere. In this way, the pre-registration is used as proactive access control to permit or restrict interaction with new devices. For the new device, the C-RAN node gives it a value depending on both provided service and device feedback, but this value should not be more than zero.

Algorithm 2 register a new device

input: Received Req ≠ ∅
output: new RD_{Nid}≠ ∅
1: while true do
2: req ⇐ receive();
3: req id ⇐ req.id;
4: if Block Chain.find(req id) == ∅ then // the device is not registered anywhere

```
5: observation ⇐ do & monitor(req); //C-RAN node monitoring
services for the new device
6:msg ⇐ {approved service &req new id} // new device sends
feedback to C-RAN node
7: new id ⇐ compute new RD_Nid (observation);
8: if new RD_Nid  > -1 then
9: block ⇐ create block(req id, observation);
10: msg ⇐ { req id, new block};// C-RAN node add new block to
blockchain
11: trust RV_Nids list.put(req id, new RD_Nid);
12: send(OK, updated trust RV_Nids list ); // send new id and updated
trust RV_Nids list to new device
13: else
14: send(ERROR, req.reject); // C-RAN node restricts suspicious
device
15: end if
16: end while
```

The C-RAN node broadcasts the list of *IDs* of all connected devices only. When a device requests contact with the C-RAN cell, the C-RAN cell will verify its own database for the current trust status. If C-RAN discovers a previous (trusted value), otherwise it will use Eq.1 to generate the new trust value for a specific device based on the experiences of other devices.

$$TV_{Did} = \omega 1 * TV_{N_{id}(Historical)} + \omega 2 * \sum_{i=0}^{n} \frac{TV_{N_{id}}{}^{RVi}}{i} \qquad (1)$$

In the equation.1 TV_{Did} is the trust value on the Edge server database for a device N_{id}. RVi is a Reputed device (N_{id}) value from other devices, whereas i is the number of devices controlled by a specific C-RAN node. The ω1 and ω2 are the weight factors where ω1+ω2 =1. After providing, the new $TV_{N_{id}}$, a new block will be added to the blockchain, which will be sent to all C-RAN cells for verification.

3. Results and discussion

In this section, we analyze the proposed blockchain-enabled trust for 5G networks in terms of three metrics: processing time of blocks, detection accuracy of malicious nodes, and transaction transmission delay. Moreover, we also compare our results with those of benchmark (Blockchain-Based Secure and Trustworthy-SDN5G) BBST-SDN5G [35], which offers the SDN-enabled 5G-VANET model. We accomplish the simulation of our proposed method through the OMNeT ++ 5.4.1 framework within the INET 4.1.2. The function of blockchain during simulation is implemented in the INET framework as in [49]. The proposed method offers a blockchain in the 5G network, which applies the consensus-updated DPOS algorithm to all C-RAN nodes in each SDN cluster. To assess the comparability of the proposed architecture, the size of the 5G network is considered 1000m x 1000m. The bandwidth is set at 10Mbps, and the number of edge devices is between 200 and 500. We want to see how well the network performs at different network densities. Table 1 shows the details of the simulation parameters.

Table 1. Stimulation parameters

Parameters	Values
Simulator	OMNeT++ 5.4.1 with INET 4.1.2
Area	1000m * 1000m
Total number of edge devices	200-500
numbers of C-RAN	30

Number of Transactions	2500

Processing time: The time is taken to produce the block in the proposed architecture. In other words, it is the time that the C-RAN node needs to generate the block. Moreover, we also implement an efficient method, which provides low overhead during the simulation. All edge devices are automatically registered in the proposed architecture and join the network with no need to identify each other. As it has been illustrated in Fig.4, our proposed architecture has a lower processing time for generating blocks in comparison with the BBST-SDN5G [35], owing to the fact that the C-RAN node could apply a DPoS algorithm that has a direct effect on reducing the time during generating blocks.

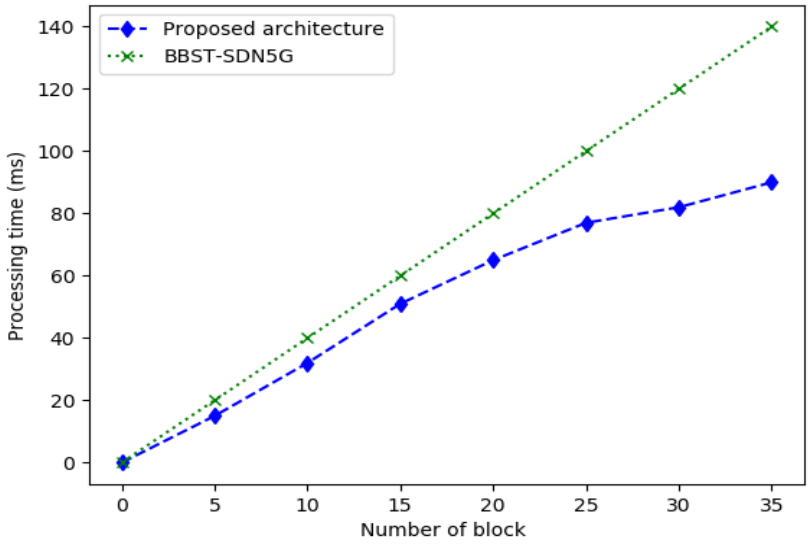

Figure 4. Impact of the number of blocks on process time

Detection accuracy: We want to see how accurate it is to detect hostile nodes that want to connect to the network using a fake or stolen *ID*. When a few malicious nodes are present, as shown in fig.5, the network's message transmissions can be trusted. In comparison to BBST-SDN5G [35]. The suggested architecture has a higher detection rate because it is C-RAN enabled, and all nodes have lower speeds. Indeed, our approach is capable of detecting all rogue nodes with ease.

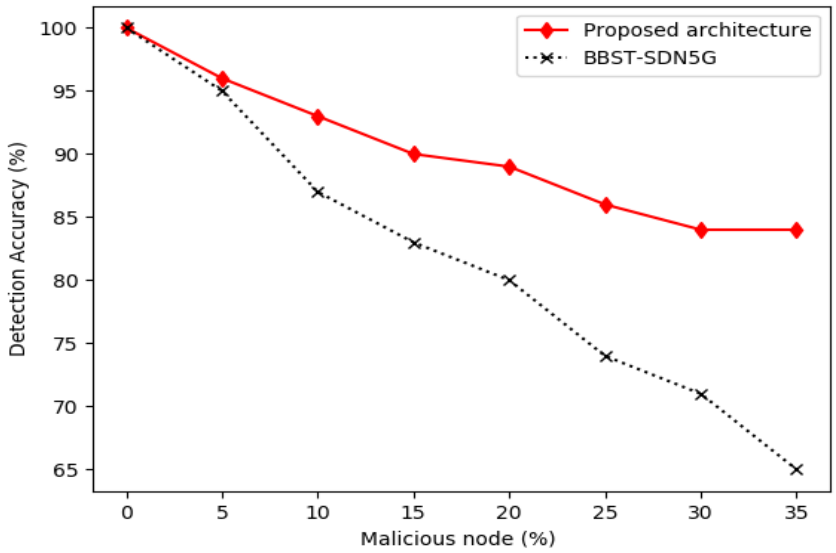

Figure 5. Detection accuracy of malicious nodes.

Transaction transmission delay: To demonstrate the scalability and utility of blockchain for trust management in 5G SDN network-enabled C-RAN, we examine the transmission delay of blockchain transactions with a variety of message flows and different numbers of edge devices. Usually, when the device has to communicate with others, the message rate is increased to build trust, then agreed upon to secure messages between nodes. As a result, the whole 5G network will suffer from a heavy load. However, the proposed architecture has less transmission delay in comparison with the BBST-SDN5G [35] because, as shown in Fig.6, the proposed architecture verifies and prepares all connected nodes to interact without any prior agreement. Furthermore, the proposed architecture verifies transaction authentication using asymmetric private/public key and hash cryptography algorithms. Each node's private key is used to sign transactions, while the public key is broadcast to all network nodes and serves as an identity.

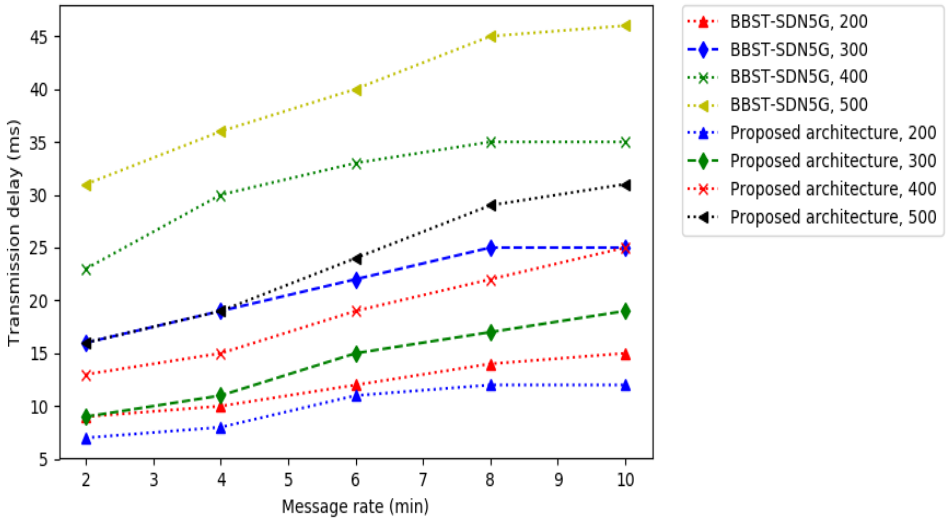

Figure 6. Transaction transmission delay

4. Conclusion

Blockchain is a technology used to share the registry concepts for a distributed system over a wireless network. Different types of application domains exist in 5G heterogeneous networks, ranging from broadband mobile applications to potentially any industrial system requiring decentralized, trusted, and automated decision making in multi-tenant companies. Due to the heterogeneity of edge devices and service requirements, trust management is critical for 5G networks. Indeed, trust management enables dynamic access restrictions, which is essential to resist internal attacks carried out by malicious nodes. It cuts down on the amount of time spent communicating between the device and the MNO, which is something that is likely to happen in the real world. The suggested trust management reduces the number of messages exchanged to establish trust with other devices and the MNO, resulting in lower network latency. The result is an improvement in the detection of malicious devices and a reduced time to create a block, which leads to improved network latency. For future work, trust management is required to focus on how the cloud calculates the trust degree of every MNO and how the devices in 5G heterogeneous networks can appropriately choose the optimal MNO to handle their requests depending on the operator's reputation.

Declaration of competing interest

The authors declare that they have no any known financial or non-financial competing interests in any material discussed in this paper.

References

[1] Q. Zhao and M. Gerla, "Energy efficiency enhancement in 5G mobile wireless networks," 2019, doi: 10.1109/WoWMoM.2019.8792998.

[2] H. El-sayed and M. Chaqfeh, "Exploiting mobile edge computing for enhancing vehicular applications in smart cities," *Sensors (Switzerland)*, 2019, doi: 10.3390/s19051073.
[3] G. Mesbahi and A. Ghaffarpour Rahbar, "Cluster-Based Architecture Capable for Device-to-Device Millimeter-Wave Communications in 5G Cellular Networks," *Arab. J. Sci. Eng.*, 2019, doi: 10.1007/s13369-019-03830-w.
[4] H. Zhang, L. Zhu, K. Long, and X. Li, "Energy Efficient Resource Allocation in Millimeter-Wave-Based Fog Radio Access Networks," Sep. 2018, doi: 10.23919/URSI-AT-RASC.2018.8471411.
[5] P. Shantharama, A. S. Thyagaturu, N. Karakoc, L. Ferrari, M. Reisslein, and A. Scaglione, "LayBack: SDN management of multi-access edge computing (MEC) for network access services and radio resource sharing," *IEEE Access*, 2018, doi: 10.1109/ACCESS.2018.2873984.
[6] A. A. A. Ari, A. Gueroui, C. Titouna, O. Thiare, and Z. Aliouat, "Resource allocation scheme for 5G C-RAN: a Swarm Intelligence based approach," *Comput. Networks*, 2019, doi: 10.1016/j.comnet.2019.106957.
[7] E. J. Kitindi, S. Fu, Y. Jia, A. Kabir, and Y. Wang, "Wireless Network Virtualization with SDN and C-RAN for 5G Networks: Requirements, Opportunities, and Challenges," *IEEE Access*, 2017, doi: 10.1109/ACCESS.2017.2744672.
[8] W. He, J. Gong, X. Su, J. Zeng, X. Xu, and L. Xiao, "SDN-enabled C-RAN: An intelligent radio access network architecture," 2016, doi: 10.1007/978-3-319-31307-8_32.
[9] G. Kollias, F. Adelantado, C. Verikoukis, and N. I. Jun, "Spectral Efficient and Energy Aware Clustering in Cellular Networks," pp. 1–13.
[10] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari, "Decentralized Authentication of Distributed Patients in Hospital Networks using Blockchain," *IEEE J. Biomed. Heal. Informatics*, 2020, doi: 10.1109/jbhi.2020.2969648.
[11] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems," *IEEE Internet Things J.*, 2017, doi: 10.1109/JIOT.2017.2740569.
[12] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, "An Energy-efficient SDN Controller Architecture for IoT Networks with Blockchain-based Security," *IEEE Trans. Serv. Comput.*, pp. 1–1, Jan. 2020, doi: 10.1109/tsc.2020.2966970.
[13] S. Kim, "Blockchain for a Trust Network Among Intelligent Vehicles," *Advances in Computers*, vol. 111. Academic Press Inc., pp. 43–68, 2018, doi: 10.1016/bs.adcom.2018.03.010.
[14] H. Zhang, Y. Qiu, X. Chu, K. Long, and V. C. M. Leung, "Fog radio access networks: Mobility management, interference mitigation, and resource optimization," *IEEE Wirel. Commun.*, vol. 24, no. 6, pp. 120–127, Dec. 2017, doi: 10.1109/MWC.2017.1700007.
[15] G. Wang, Z. J. Shi, M. Nixon, and S. Han, "ChainSplitter: Towards Blockchain-based Industrial IoT Architecture for Supporting Hierarchical Storage," 2019, doi: 10.1109/Blockchain.2019.00030.
[16] B. Tang, H. Kang, J. Fan, Q. Li, and R. Sandhu, "IoT passport: A blockchain-based trust framework for collaborative internet-of-things," 2019, doi: 10.1145/3322431.3326327.
[17] S. K. Dwivedi, P. Roy, C. Karda, S. Agrawal, and R. Amin, "Blockchain-Based Internet of Things and Industrial IoT: A Comprehensive Survey," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/7142048.
[18] D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. Shen, "Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain," *IEEE Trans. Ind. Informatics*, 2019, doi: 10.1109/TII.2019.2898900.
[19] Y. Dai, X. Wang, P. Zhang, and W. Zhang, "Wearable biosensor network enabled multimodal daily-life emotion recognition employing reputation-driven imbalanced fuzzy classification," *Meas. J. Int. Meas. Confed.*, 2017, doi: 10.1016/j.measurement.2017.06.006.
[20] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Blockchain-enabled Authentication Handover with Efficient Privacy Protection in SDN-based 5G Networks," *IEEE Trans. Netw. Sci. Eng.*, 2019, doi: 10.1109/tnse.2019.2937481.
[21] M. R. Camana, C. E. Garcia, and I. Koo, "Cluster-Head Selection for Energy-Harvesting IoT Devices in Multi-tier 5G Cellular Networks," 2019, doi: 10.1007/978-3-030-26763-6_61.
[22] A. A. Barakabitze, A. Ahmad, A. Hines, and R. Mijumbi, "5G Network Slicing using SDN and NFV: A Survey of Taxonomy, Architectures and Future Challenges," *Comput. Networks*, 2019, doi: https://doi.org/10.1016/j.comnet.2019.106984.
[23] M. F. Hossain, A. U. Mahin, T. Debnath, F. B. Mosharrof, and K. Z. Islam, "Recent research in cloud

radio access network (C-RAN) for 5G cellular systems - A survey," *Journal of Network and Computer Applications*. 2019, doi: 10.1016/j.jnca.2019.04.019.
[24] T. Alharbi, "Deployment of blockchain technology in software defined networks: A survey," *IEEE Access*, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 9146–9156, 2020, doi: 10.1109/ACCESS.2020.2964751.
[25] X. Duan, X. Wang, Y. Liu, and K. Zheng, "SDN enabled dual cluster head selection and adaptive clustering in 5G-VANET," 2016, doi: 10.1109/VTCFall.2016.7881214.
[26] Y. Jung, M. Peradilla, and R. Agulto, "Packet key-based end-to-end security management on a blockchain control plane," *Sensors (Switzerland)*, 2019, doi: 10.3390/s19102310.
[27] M. A. Marotta, M. Kist, J. A. Wickboldt, L. Z. Granville, J. Rochol, and C. B. Both, "Design considerations for software-defined wireless networking in heterogeneous cloud radio access networks," *J. Internet Serv. Appl.*, 2017, doi: 10.1186/s13174-017-0068-x.
[28] S. Basloom, N. Akkari, and G. Aldabbagh, "Reducing Handoff Delay in SDN-based 5G Networks Using AP Clustering," *Procedia Comput. Sci.*, 2019, doi: 10.1016/j.procs.2019.12.101.
[29] G. C. Valastro, D. Panno, and S. Riolo, "A SDN/NFV based C-RAN architecture for 5G mobile networks," Aug. 2018, doi: 10.1109/MoWNet.2018.8428882.
[30] P. K. Sharma, S. Singh, Y. Jeong, and J. H. Park, "DistBlockNet : A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," no. September, pp. 78–85, 2017.
[31] A. Muthanna *et al.*, "Secure and reliable IoT networks using fog computing with software-defined networking and blockchain," *J. Sens. Actuator Networks*, vol. 8, no. 1, pp. 1–20, 2019, doi: 10.3390/jsan8010015.
[32] H. Yang, Y. Liang, J. Yuan, Q. Yao, A. Yu, and J. Zhang, "Distributed Blockchain-based Trusted Multi-domain Collaboration for Mobile Edge Computing in 5G and beyond," *IEEE Trans. Ind. Informatics*, 2020, doi: 10.1109/tii.2020.2964563.
[33] S. Abbas, N. Javaid, A. Almogren, S. M. Gulfam, A. Ahmed, and A. Radwan, "Securing Genetic Algorithm enabled SDN Routing for Blockchain based Internet of Things," *IEEE Access*, no. October, pp. 1–1, 2021, doi: 10.1109/access.2021.3118948.
[34] M. S. Al-Rakhami and M. Al-Mashari, "A blockchain-based trust model for the internet of things supply chain management," *Sensors*, vol. 21, no. 5, pp. 1–15, 2021, doi: 10.3390/s21051759.
[35] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019, doi: 10.1109/ACCESS.2019.2913682.
[36] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, 2018, doi: 10.1109/MCOM.2018.1701095.
[37] N. Elisa, L. Yang, F. Chao, and Y. Cao, "A framework of blockchain-based secure and privacy-preserving E-government system," *Wirel. Networks*, 2018, doi: 10.1007/s11276-018-1883-0.
[38] M. Fan and X. Zhang, "Consortium Blockchain Based Data Aggregation and Regulation Mechanism for Smart Grid," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2905298.
[39] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," *Sensors (Switzerland)*, 2019, doi: 10.3390/s19040970.
[40] A. Yazdinejad, R. M. Parizi, A. Bohlooli, A. Dehghantanha, and K. K. R. Choo, "A high-performance framework for a network programmable packet processor using P4 and FPGA," *J. Netw. Comput. Appl.*, 2020, doi: 10.1016/j.jnca.2020.102564.
[41] T. Wang *et al.*, "Data collection from WSNs to the cloud based on mobile Fog elements," *Future Generation Computer Systems*. 2017, doi: 10.1016/j.future.2017.07.031.
[42] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K. K. R. Choo, "P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking," *Comput. Secur.*, 2020, doi: 10.1016/j.cose.2019.101629.
[43] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, "Trust management in social Internet of vehicles : Factors , challenges , blockchain , and fog solutions," vol. 15, no. 1, 2019, doi: 10.1177/1550147719825820.
[44] L. Hang and D. H. Kim, "Design and implementation of an integrated iot blockchain platform for sensing data integrity," *Sensors (Switzerland)*, 2019, doi: 10.3390/s19102228.
[45] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019,

doi: 10.1109/JIOT.2018.2836144.
[46] T. Wang, G. Zhang, M. D. Z. A. Bhuiyan, A. Liu, W. Jia, and M. Xie, "A novel trust mechanism based on Fog Computing in Sensor–Cloud System," *Future Generation Computer Systems*. 2018, doi: 10.1016/j.future.2018.05.049.
[47] Y. Hussain and Z. Huang, "TRFIoT: Trust and reputation model for fog-based IoT," 2018, doi: 10.1007/978-3-030-00021-9_18.
[48] C. E. and S. R. Marcello Cinque, "Trust Management in Fog/Edge Computing by Means of Blockchain Technologies. 2018 IEEE International 2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Infor.".
[49] Y. Gupta, R. Shorey, D. Kulkarni, and J. Tew, "The applicability of blockchain in the Internet of Things," 2018, doi: 10.1109/COMSNETS.2018.8328273.