IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 5, 2020, accepted May 10, 2020, date of publication May 18, 2020, date of current version June 2, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2995188

Blockchain and SDN Architecture for Spectrum Management in Cellular Networks

ASUQUO A. OKON[1], **IBRAHIM ELGENDI**[1], **(Member, IEEE)**, **OLUSEGUN S. SHOLIYI**[2], **JAAFAR M. H. ELMIRGHANI**[3], **(Senior Member, IEEE)**, **ABBAS JAMALIPOUR**[4], **(Fellow, IEEE)**, **AND KUMUDU MUNASINGHE**[1], **(Senior Member, IEEE)**
[1]School of IT and Systems, University of Canberra, Canberra, ACT 2601, Australia
[2]National Space Research and Development Agency, Obasanjo Space Centre, Umaru Musa Ydar'adua express way, Abuja, Nigeria
[3]School of Electronic and Electrical Engineering, University of Leeds, Leeds LS2 9JT, U.K.
[4]School of Electrical and Information Engineering, University of Sydney, Sydney, NSW 2006, Australia

Corresponding author: Asuquo A. Okon (Alex.Okon@canberra.edu.au)

This work was supported in part by the Engineering and Physical Sciences Research Council (EPSRC), in part by the Internet Project under Grant EP/H040536/1, in part by STAR Project under Grant EP/K016873/1, and in part by TOWS Project under Grant EP/S016570/1.

ABSTRACT Whereas 4G LTE networks have brought about an increase in data rates of mobile networks, they are unable to meet the capacity demands of future networks. Specifically, the centralized nature of the evolved packet core (EPC) makes the network non-scalable to match the exponential increase in number of wireless devices in addition to the complexities of diverse service requirements. The SDN concept has recently attracted a lot of research interest as a viable proposition for bringing about programmability and ease of network management while also offering flexibility for innovative network designs. However, current SDN implementations are not adapted to support business agreements that foster interoperability among mobile network operators (MNOs). This paper is an extended version of our earlier work and we intend to present a unified SDN and blockchain architecture with enhanced spectrum management features for enabling seamless user roaming capabilities between MNOs. Our simulation results show that users can experience no disruption in service with very minimal delay as they traverse between operators.

INDEX TERMS Blockchain, interoperability, LTE, MNO, SDN.

I. INTRODUCTION

The upsurge and exponential growth in the number of wireless devices owing to ubiquitous smartphones, tablets and other wireless devices has led to an unprecedented increase in mobile traffic with projected annual mobile traffic expected to hit 291.8 exabytes by 2019 [1]. While this trend is expected to increase year on year, studies have shown that about 80% – 90% of this traffic will be generated indoors [2]. Current 4G long term evolution (LTE) networks are being stretched to their theoretical limits as mobile network operators (MNOs) are faced with the challenge of meeting increasing demands for higher data rates, network capacity, spectral and energy efficiency [3].

Densification of the network has been adopted as a key technique for boosting the network capacity in a bid towards providing ubiquitous connectivity to these huge number of wireless devices. Network densification is characterized by huge concentration of base stations (BS) per unit area in order to exploit spatial reuse for higher spectral efficiency. Indeed the authors in [4] are of the view that contrary to BS densities of 8 – 10 BSs/km^2 in 4G cellular networks, the network density of future networks are anticipated to be in the region of 40 – 50 BSs/km^2, representing a fourfold increase over current 4G networks. However, while the densification of base stations seeks to address the spectrum scarcity problem and bring about higher system capacity, it invariably has its attendant challenges.

Firstly, the network complexity increases with increase in BS deployments [5]. Networks are becoming increasingly enormous in size and heterogenous in nature with different equipment, application and services provided by different manufacturers. Indeed one of the main drawbacks of current 4G deployments is the non-scalability of central devices such as the evolved packet core (EPC) [6], which introduces a single point of failure making configuration and management of these large-scale networks cumbersome. These complexities no doubt create a need for novel approaches in the design of

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

future networks that can guaranty flexibility, adaptability and agility to meet dynamic application requirements while also having the capability of simultaneously providing optimized support for the diverse use cases [5].

Secondly, the increased deployment of macro base stations (MBSs) may not be economically viable especially with meeting the coverage and capacity requirements in indoor environments owing to building penetration losses (BPL) [2]. This scenario creates coverage holes, which could result in severe performance degradation and disruption of services and applications. Specifically, the massive machine type communication (mMTC) use case of 5G, will witness large scale deployment of IoT devices which studies say will be in the region of 1,000,000 devices/km^2 [1], a good number of which will be deployed indoors. These devices are characterized by transmission of relatively low to relatively high volume of data with a requirement for adequate coverage to ensure long battery life operation.

In response to the above issues, current network deployments have witnessed increased deployments of small cells (such as femtocells and picocells) in indoor environments to fill the capacity and coverage gap. Through dense deployments of small cells, the average distance between transmitters and receivers is reduced, culminating in lower propagation losses, higher data rates and higher energy efficiency [7]. Small cells offer much higher processing and computational capabilities than Wi-Fi access points, thus providing support for mobile edge computing (MEC). By this approach, low latency (such as tactile internet) and real-time applications can be brought in closer proximity to end users, through the provision of IT and cloud computing capabilities within the radio access networks (RAN) [8].

Furthermore, the advances and success recorded with software defined networks (SDN) [6], [9] and blockchain [10], [11] have positioned them as key enabling technologies for 5G networks and beyond. Different from traditional networks where the control and data planes reside in the router and switching devices [12], SDN decouples the control plane from the data plane to allow for simpler programmable network elements while moving complex control logic to an external controller, which is a software platform running on a commodity server technology [13]. Blockchain is a distributed ledger technology (DLT), for recording a growing list of digital actions or transactions, chained to each other and distributed across nodes [11, 14]. Indeed there has been growing interests by several authors in employing the smart contract feature of blockchain for sharing spectrum assets among operators in a secure and trusted manner [10], [15].

In this paper, we present an extended version of our previous work [16], by proposing an enhanced platform for managing spectrum assets to enable interoperability between MNOs over small cells. Our solution leverages SDN and smart contracts to establish trust between operators in order to provide uninterrupted service to mobile subscribers as they switch from one mobile network to another. To this end, our major contributions are presented as follows:

- Our architecture incorporates an intelligent SDN controller design with the capability to dynamically switch subscribers between operators whenever an operator's service is unavailable. This switch is done in a seamless fashion to ensure that subscribers do not experience service disruption as they roam between networks.
- In addition, we employ the smart contract feature of blockchain to create trust between MNOs through which agreements and the complexities of service level agreements (SLAs) can be managed. The smart contract is used to simplify and automate interconnect billing processes as well as roaming settlements between operators.

The rest of this paper is structured as follows. Section II provides a literature review of related work, highlighting some of the research on small cell deployments done so far while also identifying gaps in current research. In section III, we present our proposed architecture and the concept behind it. Section IV describes the operation of our model in detail as well as the model implementation and tools to be used. Finally, in Section V, we summarize the work and give directions for future research.

II. RELATED WORK

Industry experts are of the view that 5G networks and beyond will not just be an incremental improvement over their predecessors but rather a revolutionary leap forward in terms of data rates, latency, massive connectivity, network reliability and energy efficiency [1]. In meeting with the extreme networking requirement especially in indoor scenarios, small cell network deployments have emerged as a very promising solution. Small cells are low cost and low power base stations that have shorter coverage area relative to macro base stations and are often employed for offloading macro traffic or to complement macro cells in dense networks [17].

While, it is well established that the majority of indoor mobile traffic today is carried by wireless local area networks (WLAN) or Wi-Fi, these networks are increasingly becoming saturated [17], [18], making them unable to deal with the exponential increase in the number of devices and data traffic which will characterize future networks. This has created the need for the deployments of small cells in indoor scenarios to meet the demands of 5G in terms of capacity and coverage requirements as well as providing Quality of Service (QoS) guarantees for vertical industries. Recently, the emergence of micro-operators (μO) [17] has received a lot of research interest, and has defined a concept whereby industry/business stakeholders can exploit their domain specific knowledge to establish local small cell networks where context related services and content can be offered with quality of service guarantees in high-demand areas such as shopping malls, hospitals, campuses, sport arenas and enterprises [17], [18]. Two good examples of successful commercial deployments of small cell networks include Cloudberry, the first small cell operator in the world [19], [20] and Denseair [21]. These μOs through their small cell deployments are responsible for providing the indoor radio access network (RAN) in collaboration with facility owners and service providers such as MNOs and vendors under a neutral host arrangement.

In essence, the micro-operator acts a carrier for carriers. Two main benefits of this approach to the MNOs are (i) massive cost savings (CAPEX and OPEX) in terms of reduction in the cost of rolling out and managing new base station deployments which in turn reduces time to market and (ii) extension of the MNOs geographic coverage and network footprint thus allowing their subscriber to access network services and applications over a neutral operator's network, which in turn provides additional revenue streams to the MNO and μO.

While facility owners do not want a single operator to dominate capacity provision on one hand, they are opposed to the deployment and management of multiple physical indoor networks by different actors on the other hand [20]. Therefore, in addition to providing the RAN for MNOs, μOs play a strategic role in managing business agreements between the various actors through the deployment of a single shared infrastructure. The potential benefits of employing blockchain technology, as a distributed digital ledger, in telecommunications has been suggested in literature. Some of these benefits include interoperability, traceability, reliability and capability to execute autonomous transactions [15]. Indeed, the authors in [10] proposed adopting blockchain technology as a facilitator for sharing network resources among operators in a secure and trusted manner. To this end, the main contribution of this paper is to present a framework for managing both the network operations and business agreements of multi-operator small cell deployments using blockchain. Specifically, we intend to employ the smart contract feature of blockchain to realize an autonomous, distributed, secure and reliable architecture for small cells networks.

Several studies have been conducted on small cell deployment for multi-operator support [10], [17], [18], [20]. In [17], the authors propose a framework for indoor small cell deployment managed by micro operators that leverages on network slicing to provide customized services. The authors identified insufficient coverage between local area networks (LAN) and wide area networks (WAN) as a motivation for the deployment of small cells. In their framework, the micro operator is responsible for virtualizing the small cell into network slices realized using SDN and NFV, and these slices can form part of the product/service offering of a micro operator to MNOs, service providers or end users. While it is envisaged that through this framework MNOs can improve their indoor coverage without much expenses, it also opens up additional revenue stream for the micro-operator as they can charge the MNOs for accessing its local network. The network slices to be used will depend on the end to end (E2E) requirements such as bandwidth, data rate, latency, number of users, etc. The assumption that network slicing should be operated by the MNO while 3^{rd} parties service providers buy the network slices from MNOs has been challenged [18]. In their view, new stakeholders such as micro operators could deploy ultra-dense small cell RAN for tailored service delivery to various infrastructure providers including MNOs by employing network slices and spectrum sharing techniques.

The different service models proposed include cloud-based Platform as a Service (PaaS), Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Network as a Service (NaaS) as an extension of all the afore-mentioned models. With network slicing, operators could meet the diverse use case requirements and exploit the benefits of a common network infrastructure by abstracting the slice functionality to expose the capabilities of 3^{rd} party service providers through open Application Programming Interfaces (APIs). However, network slices require radio resources for meeting agreed service quality, hence the authors are of the view that efficient deployment of ultra-dense small cell RAN calls for novel spectrum micro licensing models.

Two spectrum sharing models recently approved by regulators include licensed shared access (LSA) in Europe and the citizens broadband radio services (CBRS) in the U.S., where both models introduce mobile communications on bands shared with incumbent users. In their proposed high-level architecture, two entities are introduced – the spectrum manager and the co-existence manger whose roles are to control spectrum access according to spectrum availability information and to coordinate between different license holders including micro licensees with different levels of spectrum access rights respectively.

The problem of small cell network sharing with a focus on the business model implications for different multi-operator deployment solutions for indoor scenarios were discussed in [20]. Four business models were identified in their study and these include (i) distributed antenna systems (DAS) (ii) multi-operator smallcells using common frequencies (iii) multi-operator smallcells using dedicated frequencies and (iv) multi-operator access using roaming. The multi-operator small cells are femtocell networks comprising two types of nodes: femtocell access points (FAPs) and femtocell gateways (FeGW). The DAS solution are commonly used to improve indoor coverage for voice services and suffer capacity limitations in supporting the high demands of next generation networks. The small cell networks on the other hand can provide the very high capacity demands of future networks. From the business case perspective, the indoor deployment models can be further classified as shown in Fig.1.

In the multi-operator small cell network based on a common frequency, operators share the same frequency over the radio access network provided by the FAPs while the FeGW connects to and manages the access points over the internet and thereafter forwards operator traffic to their respective core network. In the dedicated frequency approach, each operator employs a different frequency and the FeGW located in the same premises as the FAPs is used to distinguish the various streams of traffic which are forwarded to different operators over the internet.

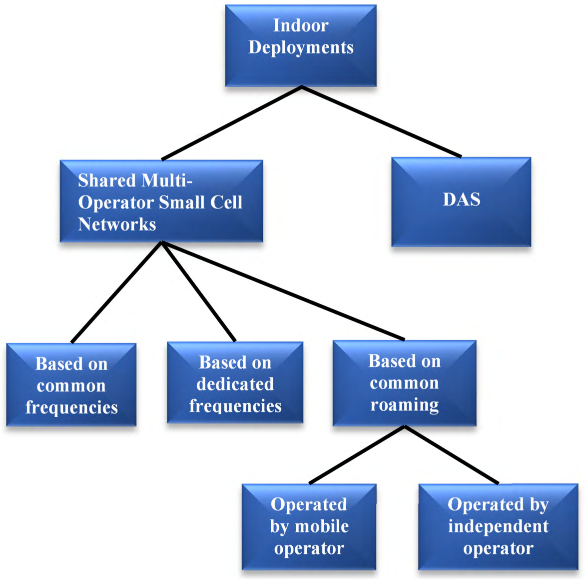

FIGURE 1. Classification of indoor network deployments based on the business model.

TABLE 1. Classification of cells.

Cells	Range	Number of Users
Femtocell	10 m - 50 m	A few users
Picocells	200 m	20 - 40
Microcell	2 km	> 100
Macrocell	35 - 35 km	Many

In the roaming-based approach, control of the spectrum is key to the business [20] for the independent operator, where the capacity to offload traffic and computationally intensive tasks is a vital service offering. There are different cellular implementations currently available. The transmission range varies from femtocells being the shortest to macrocells being the longest. A classification of cellular networks together with the number of devices they can support is presented in Table 1 [17], [22].

The concept of sharing network resources among operators in small cell networks is presented in [10]. Here the smart contract feature of blockchain is used to manage the attach and detach procedures of a user equipment (UE) to mobile networks, such that the user subscription information and authentication keys are stored in a distributed ledger instead of a centralized home subscriber server (HSS). The distributed ledger can thus be seen as a functional replacement of the HSS. Authentication and security procedures are performed by communicating with this ledger.

In the network sharing arrangement, multiple copies of the same ledger are distributed throughout the network and all nodes (core network elements) including the serving and guest network operators retain a copy of the entire blockchain. Here the MNO providing the service is the serving operator while the operator receiving the service is called the guest operator. This will facilitate the provision of services to subscribers from other operators based on successful network authentication. Hence, peer to peer transactions between the guest operator and the serving operator can be executed by the smart contract based on the user's consumption and smart contract contents which could be time variant depending on the geographical location of the small cells [10]. An interesting feature of the blockchain based approach to network management is that it enables autonomous transactions such that contract clauses embedded in the smart contracts are automatically executed once the triggering conditions are met (e.g., breach of SLAs) [15].

From the works reviewed so far, one thing that has clearly not been addressed is how business agreements can be created between operators that will enable subscribers from one MNO to use the services of another MNO in a shared network. Such a framework could enable MNOs to leverage on areas where each MNO has a comparative advantage to provide value added services to their subscribers in a cost-effective manner, for example in locations where an MNO may have poor network coverage. To the best of our knowledge, our solution is the first to come up with an architecture for enabling business agreements among MNOs. It will be interesting to develop an integrated framework that can efficiently manage network operations as well as the business agreements between the various actors in a multi-operator small cell network. This gap provides the motivation for this research work as we propose a blockchain-based approach implemented on top of an SDN infrastructure for supporting multi-operator small cell deployments.

III. PROPOSED INTEGRATED SDN AND BLOCKCHAIN ARCHITECTURE

We consider indoor scenarios such as shopping malls, hospitals and campuses, with high user traffic and where the radio signal from an MNO's macro base station may become severely attenuated, owing to BPL. The architecture is shown in Fig. 2. This architecture is central to our design as it integrates the SDN and blockchain platform to allow interoperability between MNOs. The μO is responsible for deploying the indoor small cell infrastructure following consultations with facility owners.

These indoor small cells are plug and play femtocells hereafter referred to as home eNBs (HeNBs) [23], [24], which have the capability to support much higher data rates, higher number of concurrent users, higher processing power and storage capacity than WiFi access points. The HeNBs provide the primary access technology based on the 3GPP standards and they are deployed extensively around the facility to provide adequate radio access network coverage.

A. SDN PLATFORM DESIGN

The role of SDN is to decouple the network operations into the control and data planes to allow for ease of network management and programmability via software programs.

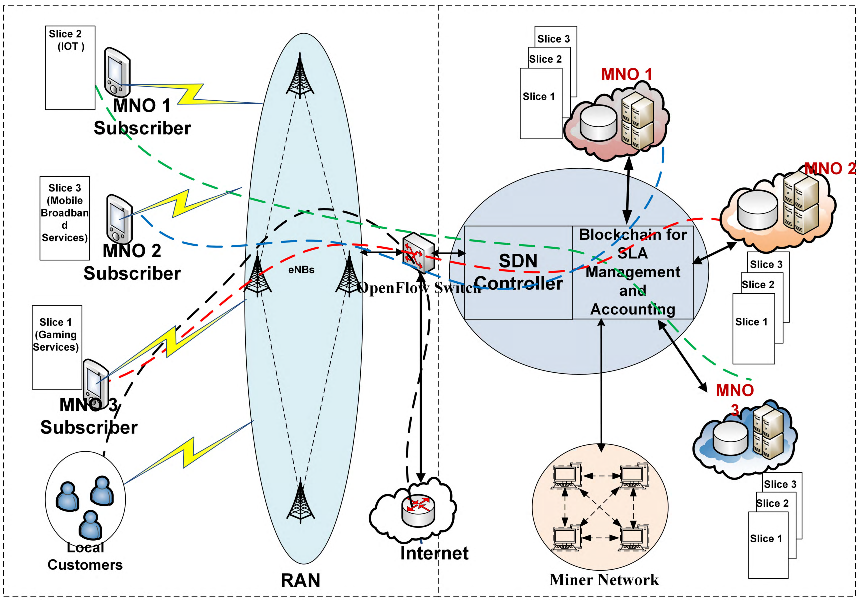

FIGURE 2. Proposed solution for supporting multi-operator small cell deployments.

Specifically, the control logic is migrated to SDN controllers which are implemented in software and are responsible for programming of forwarding devices as well as handling the allocation of traffic to the data plane.

In designing the SDN controller, we make reference to the recently developed OpenFlow switch (OF-Switch) 13 module developed by [25] and the architectural framework by [26]. The authors in these papers designed an SDN-based network using ns-3 simulator. The OF-Switch13 module provides support for OpenFlow protocol version 1.3 by incorporating both a switch device and controller in its design. However, unlike [26], where the GPRS tunneling protocol (GTP) is retained, our design eliminates the control signaling overhead incurred from maintenance of GTP tunnels by replacing the serving gateway (S-GW) and packet data network gateway (P-GW) with OF-Switches. The OF-Switch performs packet forwarding based on rules provided by the SDN controller. Thus, the data plane consists of a set eNodeBs (eNBs) connected to the switch ports of the OF-Switch through which UE traffic is forwarded to its destination. The SDN controller on the other hand handles the control plane functionalities of the mobility management entity (MME) and policy charging and rules function (PCRF). This makes it in charge of executing the control signal logic required for UE authentication, mobility management, network topology and flow table configuration. The controller communicates with the OF-Switch in the data plane using the OpenFlow protocol via the southbound interface [13], [27]. Packets arriving at the data plane are checked for a matching rule at the switch after which they are forwarded to their destination through the appropriate switch ports. If no matching rule is found, the OF-Switch forwards the packet to the SDN controller for further processing. Furthermore, flow modification messages from the SDN controller enable the OF-switch to maintain a mapping of port numbers to the media access control (MAC) address of eNBs. In this way, the controller has a global view of the network consisting of UEs, eNBs and OF-Switches.

A key advantage of this programmable platform is that it allows applications to adapt to the network based on real-time information [28]. Hence through SDN, the controllers in the control plane can more efficiently manage the underlying network with a view towards realizing a flexible and scalable architecture for implementing various network applications and services.

B. BLOCKCHAIN NETWORK LAYER IMPLEMENTATION

The blockchain network (BN) is deployed just above the SDN platform and enables verification of network operations via distributed network authorization. Every network operation such as attachment and detachment of the UE from the RAN, signaling request, data transfer etc. can be deemed to be a transaction and as such information from such transactions can be represented as a block and broadcast to all nodes on the network for verification. The blockchain network interfaces with the SDN controller via the northbound bound interface using APIs (Python or C++). When exchanging information (e.g., service request, service authorization, spectrum sharing policy, etc.) with the blockchain network, the SDN controller (sender) accomplishes this by using its private key to sign transactions their own transactions which are addressable on the network via the corresponding public key. The blockchain network (receiver) uses the same hash function as the sender to create the hash value of the transaction and compares this value with the hash obtained by decrypting the sender's digital signature with the corresponding public key in a bid to authenticate the sender's digital key. These transactions are written into the blockchain by means of smart contracts.

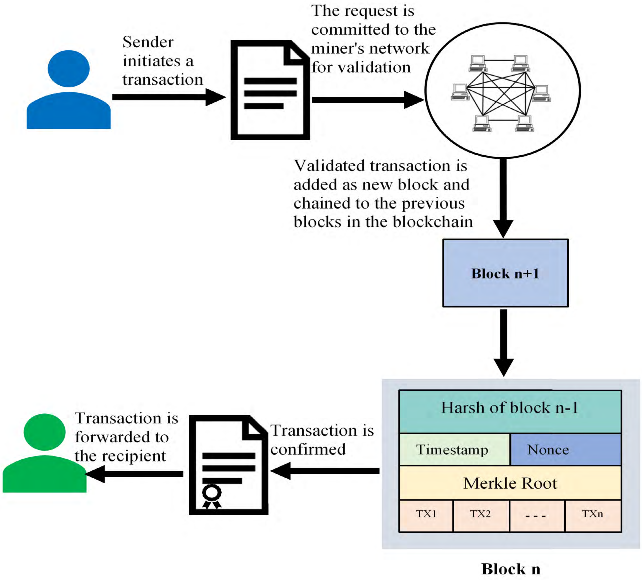

FIGURE 3. Formation of blockchain – each block carries a list of transactions and harsh functions of the previous block.

Smart contracts are computer programs with contractual clauses embedded in them which are automatically executed once the enforcing or triggering conditions are met. In addition, the smart contract takes over the functions of the HSS as it now stores user subscription information in a digital ledger. The MNOs communicate with the smart contract by writing transactions to the smart contract address and are made part of the private blockchain network to enable network interoperability. The choice of a private blockchain platform over a public version is justified by the fact that the large volume of traffic from external users in the public blockchain introduces extra delays in reaching consensus which ultimately impacts negatively on performance and scalability. In a private blockchain, all the nodes have to obey the rules of the network issued by a single monolithic body (e.g., spectrum regulator), in order to ensure efficient spectrum utilization while also enforcing penalties against MNOs who violate the transmission standard for the frequency band. Since the source code for the smart contract is publicly visible, the blockchain platform where the code resides guarantees immutability [29], in that way all parties to the smart contract are assured that all possible suspicious behaviors will be checked. Once the transactions have been verified as valid, it is appended to the chain as a block using a harsh value as shown in Fig. 3.

Thereafter, every node saves a copy of the updated blockchain. Fig. 4 depicts the type of information that could be contained in a typical smart contract. A brief description of elements in the smart contract is given as follows:

Device ID: This is the identification number assigned to devices which uniquely identifies the device (such as the UE, core network nodes, blockchain network etc.) in the network.The device ID is also used for authentication and authorization purposes.

Smart Contract Information

- Device ID
- Device location
- Subscription and billing information
- Participating MNOs
- Frequency band of operation
- QoS Parameters (Throughput, Delay, Packet loss rate, bandwidth, etc.)
- Breach of contract clause
- Payment intervals
- Transaction history

FIGURE 4. Typical information contained in a smart contract.

Device location: Gives the geographic location of nodes in the network. This is useful for mobility management in addition to providing targeted location-based services.

Subscription and billing information: Contains the service profile of users or subscribers on the network. Such information includes type and class of services subscribed to by the UE, the billing cycle, the charging rate as well as the validity period of those services.

Participating MNOs: Lists the MNOs participating in the contract and who have entered into agreements with their peers.

Operating frequency: Maintains information on the frequency bands currently used by each MNO to provide services to its subscribers for purposes of spectrum accountability.

QoS parameters: QoS parameters stipulate the performance metrics against which services provided by MNOs are monitored and evaluated. The services can be characterized in terms of priority, throughput, bandwidth to be provided, E2E packet delay, packet losses, availability etc. Failure to provide the prescribed levels of service amounts to a breach of contract and attracts a penalty (such as debit) which is automatically triggered by the corresponding clause.

Breach of contract clause: This contains clearly defined thresholds that must be met and the penalties that will be incurred if those thresholds are not exceeded. It contains explicit information on the deliverables by all parties involved, the triggering conditions and how the penalties will be enforced. In scenarios where the contract has been breached after several consecutive billing cycles, the offending party is automatically delisted from the smart contract.

Transaction history: All the information on the transaction history is stored in the blockchain and is accessible using smart contracts. The information contained therein can be used for account reconciliation and billing settlements. Over time the volume of transaction can become very huge and capable of creating storage bottlenecks in the blockchain. In such scenarios, the information is moved off-chain to ease the burden on the blockchain.

The centralization of SDN controllers, while enabling ease of management of the entire network has an inherent drawback in that it introduces a single-point of failure bottleneck in the network [15], [30]. In addition, the lack of consistent records of network data poses difficulties for network management given the heterogenous nature of the network. An integrated SDN and blockchain architecture using smart contracts would enable a distributed consistent record of SDN data among all nodes in the blockchain thus allowing for more efficient management of network resources. In addition, by eliminating total network control by any one node, the associated risks of single point failure and multi-vendor device isolation can be mitigated thereby enhancing fault recovery [31]. Also, in networks consisting of multiple SDN controller domains, the integration of blockchain and SDN makes it possible to provide network redundancy and faster recovery from network failure in the event any SDN controller fails [32]. This is possible since the network information stored in the blockchain is shared across all the other SDN controllers making it possible for another SDN controller to manage the affected domain.

Furthermore, security concerns in SDN especially with respect to sharing network resources can be addressed using blockchain [32], as it ensures the privacy of network users by preventing untrusted members in the SDN network from viewing and modifying shared resources and records.

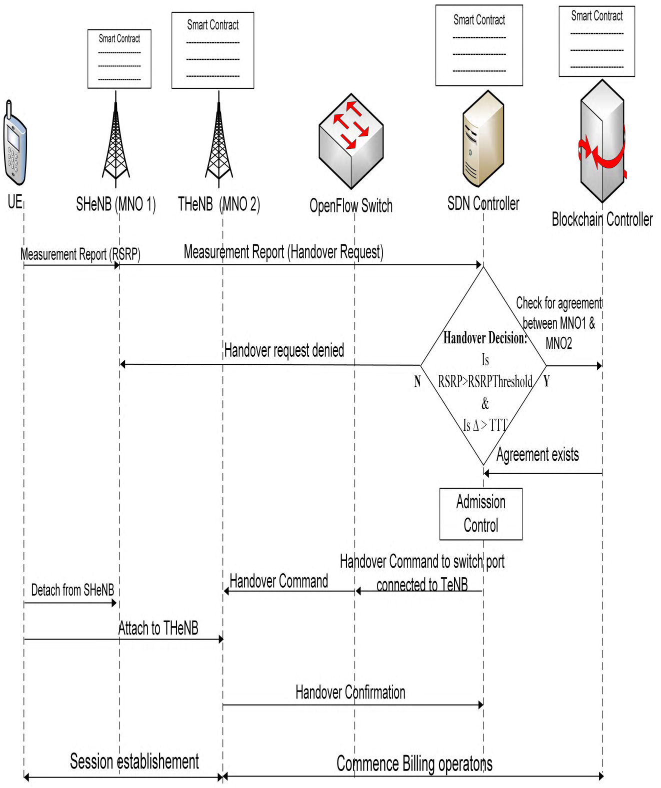

FIGURE 5. **Network management signaling diagram using smart contract.**

IV. NETWORK OPERATION AND MANAGEMENT

At the heart of the novelty of our design is the integrated SDN and blockchain architecture which serves to facilitate business agreements between MNOs while also managing radio access control in a shared network environment. Our framework seeks to answer a fundamental problem of network availability by facilitating the handover of mobile user traffic to the next mobile operator whenever the UE enters an area where the home operator has no coverage. Hence our solution is targeted at addressing the coverage hole problem experienced by mobile subscribers while maintaining their existing UEs.

To solve this problem, the SDN controller employs control logic to implement policies necessary for data flow control. This flow occurs in two directions. In the downward flow direction, the SDN controller generates packet forwarding rules and interacts with the data plane via the southbound interface based on network operation policies defined by SDN applications. In the upward direction, the controller collects network status and synchronization information from the underlying infrastructure which is used to build a global view of the network; this view is presented to SDN applications through the northbound interface. The BN on the other hand, handles user registration and maintains a shared billing system of both MNOs as well as an SLA manager which is implemented in the blockchain using a smart contract. With this configuration, the smart contract becomes responsible for coordinating and providing billing settlements and agreed levels of service to subscribers. Furthermore, service level authorization by blockchain ensures that only subscribers who have subscribed to a specific service have access to that service.

In terms of network operation, Fig. 5 illustrates the signaling sequence and transactions that occur between the different nodes and how the smart contract is used for access control and network management. First, the UE radio resource control (UE RRC) entity at the UE performs periodic channel state measurements and sends the report to the HeNB RRC entity at the HeNB. The HeNB as soon as it receives the measurement reports forwards only those related to handover events to the SDN controller which are employed in implementing handover decisions. The report includes such parameters as reference signal received power (RSRP) and reference signal received quality (RSRQ) which are used as event triggering conditions for handover. Currently ns-3 supports five (5) event-based triggering criteria: A1, A2, A3, A4 and A5 [33]. For the purposes of this study, we are interested in the event A3 triggering condition. The event A3 triggering condition is used for implementing the A3RsrpHandoverAlgorithm also known as the strongest cell algorithm. This is motivated by the fact that once the RSRP of the home MNO (MNO1) degrades significantly as may occur when a UE moves outside its coverage area, the next available MNO will have a higher RSRP. In current LTE standard, the UE performs handover as soon as the RSRP of the target HeNB (THeNB) exceeds the RSRP of its serving HeNB (SHeNB) by a threshold value called the hysteresis [33] or handover margin [26]. The condition for handover is given by:

$$\mathrm{RSRP}_{\mathrm{THeNB}} > \mathrm{RSRP}_{\mathrm{SHeNB}} + \beta \tag{1}$$

where β is the handover margin. In our model, the SHeNB represents the HenB of the home MNO while THeNB represents the HeNB of the next available MNO.

A further condition known as the time to trigger (TTT) is required prior to commencing handover procedures and it indicates the time duration over which the THeNB's RSRP must be continuously higher than the RSRP in order to trigger handover. The RSRP threshold values and TTT are implemented at the SDN controller as matching conditions. Note that it is critically important that these two conditions are met before handover can be initiated in order to mitigate the "ping-pong handover problem" [34] – a phenomenon characterized by back and forth signaling storm which results in too frequent handovers. Unlike current LTE implementation where handover is either initiated from the UE or HeNBs, we argue that it will be better if the handover decision is made by the SDN controller since it has a global view of the network and hence has a greater potential of realizing efficient resource allocation. The optimum placement of the SDN controller therefore presents a very interesting and important research problem which has been earmarked for future work.

Upon receiving the handover request, the SDN controller compares the received values with the matching conditions given by (1) and TTT values. Once the conditions are met, the controller exchanges messages with the smart contract which checks if there are any pre-existing agreements between MNO 1 and MNO 2 for that UE. If such agreements exist, the controller performs admission control procedures to ascertain that MNO 2 core network can provide the agreed QoS guarantees as stipulated in the SLA and implements the A3RsrpHandoverAlgorithm by forwarding the handover request to the OF-Switch port connected to the THeNB. At the same time, the UE detaches from SHeNB and attaches to the THeNB. The THeNB thereafter replies with a handover confirmation packet to the controller. Finally, the subscriber establishes a session with MNO 2 over the THeNB and billing procedures are automatically initiated. The pseudocode for this implementation is illustrated in Algorithm 1. Line 6 of the algorithm is crucial as it stipulates the criteria necessary for commencing handover procedures. If this first condition is not met, no handover occurs.

Algorithm 1 Spectrum Access Mangement Between Operators

```
 1: Initialization: Enter (UE ID, $MNO_1$, $MNO_2$, SHeNB, THeNB, smart contract, BN, SDN controller, $RSRP_{threshold}$)
 2: UE performs RF measurements and obtains RSRP values
 3: UE sends RSRP values to the SHeNB
 4: The SHeNB sends RSRP values to the SDN controller
 5: SDN controller receives RSRP values:
 6: if $RSRP_{THeNB} > RSRP_{SHeNB} + \beta$ then
 7:     if $\Delta > TTT$ then
 8:         SDN controller sends service request to BN
 9:         BN checks smart contract for verification of pre-existing agreement between $MNO_1$ and $MNO_2$:
10:         if contract exists between $MNO_1$ and $MNO_2$ then
11:             SDN controller $\rightarrow$ Send UE Service Request to $MNO_2$
12:             $MNO_2$ checks SLA provisioning requirement
13:             if $MNO_2$ meets SLA provisions then
14:                 $MNO_2$ $\rightarrow$ SDN controller //service request notification
15:             else
16:                 $MNO_2$ refuses service request and handover fails
17:             end if
18:         end if
19:     end if
20:     SDN controller $\rightarrow$ SHeNB $\rightarrow$ UE //service grant notification
21:     Session establishment: UE $\rightarrow$ THeNB $\rightarrow$ $MNO_2$
22:     Smart contract initiates billing procedures
23: end if
```

The logical centralized control provided by the SDN controller enables it to maintain a global view of the network allowing for efficient monitoring of spectrum usage, proper coordination of spectrum mobility and effective implementation of spectrum sharing strategies among MNOs. The blockchain network advertises the service profile of the devices on the network to the SDN controller and enforcement of the terms of the contract which is translated into flow rules and made available to the SDN switches. These flow rules determine which devices should be granted access to the network and what type/class of service these devices can access. Thus, access to the network is controlled at two levels – service level using blockchain and device level using SDN. Furthermore, the blockchain layer facilitates a distributed peer-to-peer network where non-trusting members (MNOs) can interact with each other without a trusted intermediary, thus creating a framework for trusted interaction in a trustless environment. From the mobile subscriber perspective, a digital transaction is carried out when a phone call is made, text messages are sent or data is used on the network, leading to large amount of transactional information that has to be verified to ensure customers are billed correctly. In heterogenous networks consisting of diverse devices with different service profiles and service requirements, the lack of consistent billing records of network data could pose serious difficulties for network management and billing settlement. Our integrated SDN and blockchain architecture using smart contracts enables a distributed consistent record of network management data which ensures accurate billing and effective network management. Specifically, the smart contract helps maintain a record of which devices have access to what resources. Fig.6 shows how the smart contract in the

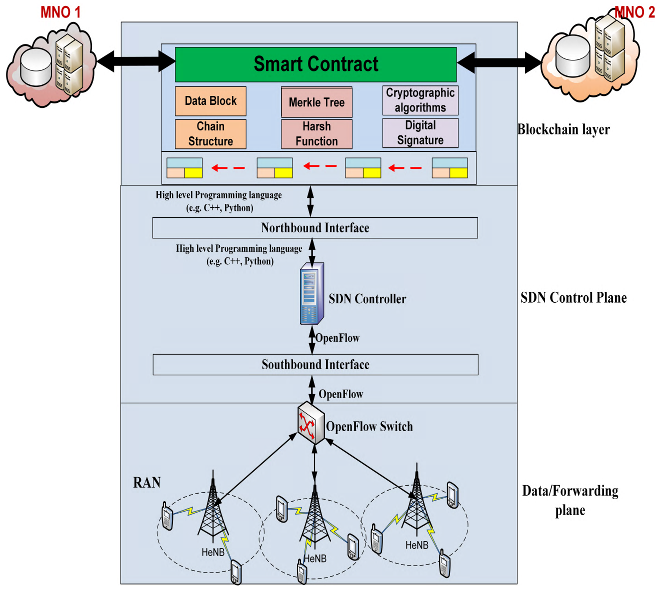

FIGURE 6. Smart contract implemented in blockchain layer as an overlay on SDN.

blockchain layer can be implemented on top of the SDN layer while Fig 7. shows the logical flow of information between blockchain and SDN.

V. EXPERIMENTAL SETUP

The architecture is modeled using network simulator 3 (ns-3) and a blockchain platform. The ns-3 simulator is integrated with an SDN platform realized using the OpenFlow switch (OFSwitch) 1.3 module while the blockchain platform consists of an off-chain smart contract, Ethereum private blockchain and the simulation module. The consensus mechanism employed is the Proof of Work (PoW). The smart contract enables management of access rights needed to facilitate interoperability between multiple operators. The contracts are designed based on the different vertical services users subscribe to and serves as an interface between multiple operators. The private blockchain is initialized on a test-net using Geth (go-ethereum) software and thereafter the genesis file is set up. The genesis file is used to define the genesis block which is the first block of the blockchain [15], and provides information about specifications of the block including such variables as gas limit, difficulty level, coinbase, timestamp and transaction fee.

In this paper, our focus is on how the SDN controller and blockchain platform can be used to manage spectrum resources through access control of UEs to spectrum assets (RAN) as well as output from the blockchain. In studying the impact of SDN and blockchain platform in radio access management, we assume that a contractual agreement between the different MNOs is already in place. The SDN controller is designed using the OFSwitch13InternalHelpler function which is included in the new OFSwitch13 module in ns-3. The parameters used in the simulation are presented in Table 2 and the RAN simulation scenario is illustrated in Fig. 8.

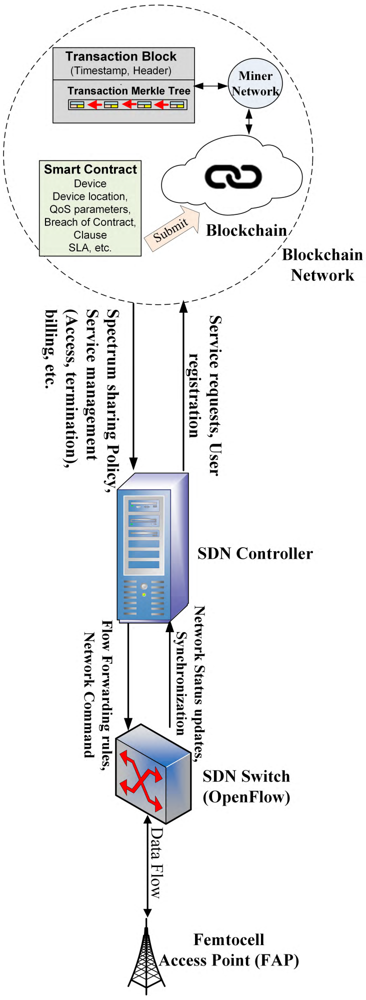

FIGURE 7. Logical flow of information between blockchain and SDN.

Any UE from a given MNO (e.g., MNO 1 subscriber) seeking to access services on different MNO (e.g., Host on MNO 2), conducts regular measurement reports to confirm spectrum availability of the intended MNO (by virtue of a higher RSRP) and notifies the SDN controller via the SHeNB. The UEs and HeNBs have a transmit power of 100 mW with the HeNB having a coverage radius of 30 m. The above scenario is modelled in NS3 simulator, to study the performance of the network when users move between 3 HeNBs as shown in Fig. 8. The duration of the simulation takes into consideration the length of time required to transfer the control signal from a UE moving at a velocity of 2 m/s, between 3 MNOs beginning from the cell edge of MNO 1 to the edge of MNO 3, while also allowing extra time for the simulation to settle into a steady state. Based on the above considerations, a simulation duration of 150 seconds is chosen.

Once access has been granted by the SDN controller to the RAN, the UE makes a transaction to the smart contract address to initialize and trigger the services specified in the contract. It is important to note that the time it takes for the BN to change the contract from one operator to the next one

TABLE 2. Simulation paramters.

Paramter	Value
Network Configuration	
Simulation grid	180 m x 100 m
Number of UEs	10
Number of HeNBs	3
Number of MNOs	3
Number of SDN controllers	1
SDN controller type	OFSwitch13InternalHelper
Number of OFSwitches	3
UE speed	2 m/s
UE Tx power	100 mW (20 dBm)
eNB Tx power	100 mW (20 dBm)
Carrier frequency	3.6 GHz
Pathloss model	Friis
Mobility model (eNB)	ConstantPosition
Mobility model (UE)	ConstantVelocity
Type of traffic	UDP
Handover algorithm	A3RsrpHandoverAlgorithm
Handover margin (Hysterisis)	3 dB
TTT	256 ms
Blockchain Configuration	
Blockchain platform	Geth (go-Ethereum)
Consensus mechanism	Proof of Work (PoW)
Total gas limit	3,000,000
Cost per transaction	21,000
Number of transactions per block	142
Block time	10 s
Transactions/sec	14.2
Number of users	Variable

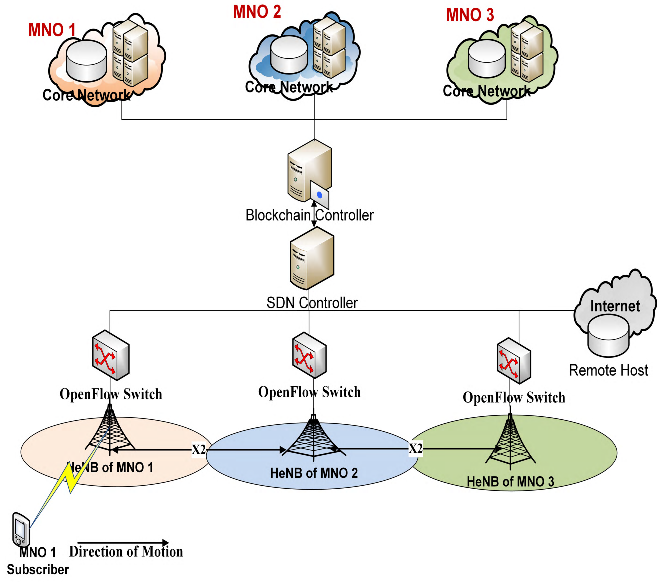

FIGURE 8. RAN simulation scenario in ns-3 simulator.

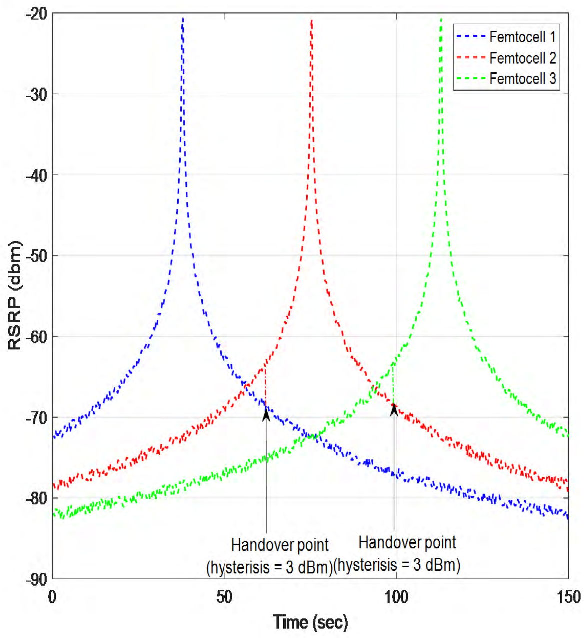

FIGURE 9. RSRP measurements received by the SDN controller as the UE moves across femtocells.

will affect the network availability for the user. Hence it is a critical requirement that this contract switching delay be kept to a minimum.

VI. RESULTS

The simulation performance of the SDN controller in handling the handover decisions across the 3 HeNBs is shown in Fig. 9.

In our simulation, the SDN controller is responsible for making the handover decisions since it maintains a global view of the network. The graph shows the periodic RSRP measurements (in dBm) provided by the UE to the SDN controller as it moves from one HeNB to another.

At the beginning of the simulation, the UE is connected to HeNB 1 (the Home MNO) since it has the highest RSRP (strongest cell). This is indicated by the dotted blue line. As the UE moves from the edge of HeNB 1 along the positive x-axis (UE, 0, 0), the RSRP values increase accordingly and reaches its peak when the UE is at the centre of the HeNB 1. Further movement of the UE away from the centre towards the other edge of HeNB 1 sees a decline in the RSRP values reported to the SDN controller. At the same time, it is observed that there is a gradual increase in the RSRP value of HeNB 2, which represents the next available MNO (dotted red line), due to the movement of the UE away from HeNB 1 towards the vicinity of HeNB 2.

It should be noted at this point the UE is still connected to HeNB 1, albeit its RSRP value continues to decrease until the RSRP value of HeNB 2 exceeds that of HeNB 1 by a threshold value and persists in that condition for a certain

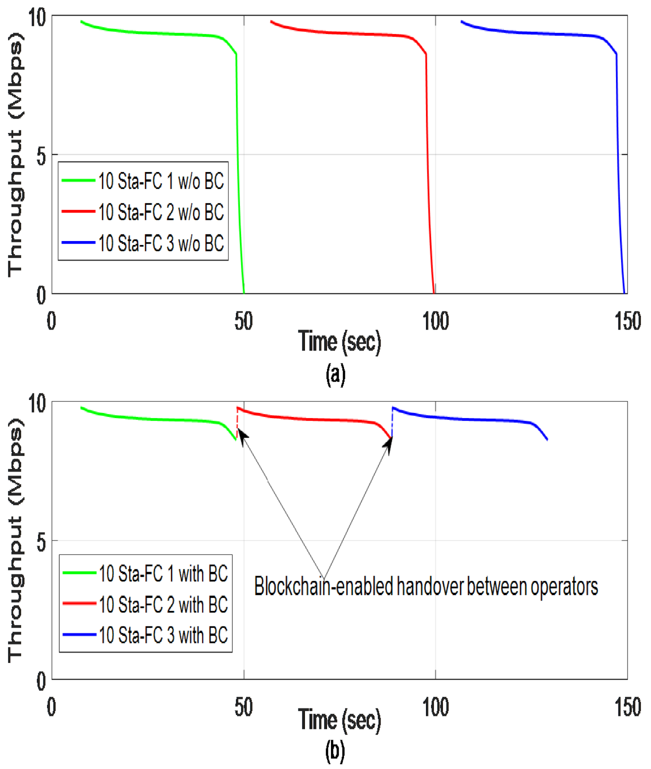

FIGURE 10. Average throughput from UEs (a) Without blockchain (b) With blockchain.

duration - we have set these values in our simulation as 3 dB and 256 ms respectively. These values which represent our matching conditions are chosen because a 3 dB difference represents a 50 percent drop in signal power level, which is very significant, while a delay of 256 ms is just about adequate to accommodate handover procedures and transactions to the blockchain while also ensuring session continuity for real time applications such as voice and video. Upon receiving these matching conditions, the SDN controller writes to the smart contract to confirm the presence of a contract between both MNOs and thereafter automatically initiates the handover procedure for transferring the UE from HeNB 1 to HeNB 2 (since it is now the cell with the strongest RSRP) by invoking the A3RsrspHandoverAlgorithm. The handover point is indicated by the dotted vertical red line. The same procedure is executed when the UE moves away from the coverage area of HeNB 2 into the vicinity of HeNB 3. The second handover point is indicated by the dotted vertical green line.

Fig. 10 shows a comparison of the network performance in terms of the average throughput measured across ten (10) UEs with and without blockchain implementation. It can be seen in Fig. 10 (a) that in the absence of a smart contract agreement, users experience a total break in network connectivity and hence a disruption in services as they move between HeNBs. The absence of a smart contract agreement between MNOs means that there is no control signal available from the next operator to facilitate handover and session transfer between MNOs when users move between operators.

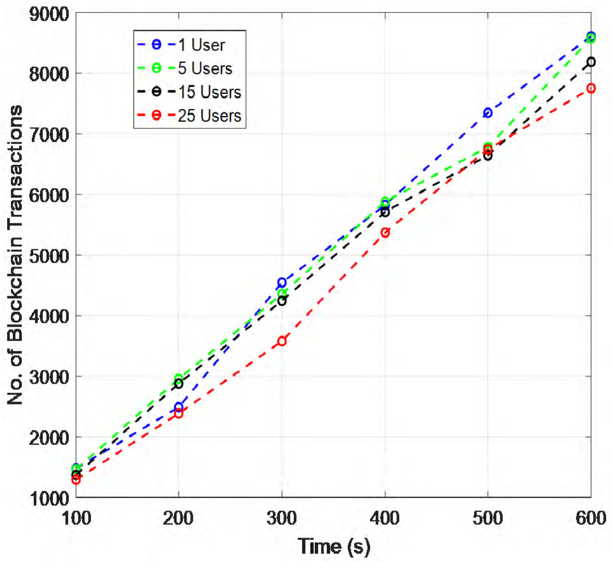

FIGURE 11. Number of transactions across different users on MNO2.

In contrast however, Fig. 10 (b) shows the performance of the network when a smart contract agreement is in place. In this scenario, the throughput is maintained at near optimum levels (10 Mbps) with very minimal disruption as the user moves between different MNOs due to the enforcement of the smart contract. The is because the smart contract makes a control signal available to serve as mobility anchor point from other operators who are co-parties to the agreement in order to enable the handover between MNOs as soon as users move outside the coverage area of any MNO. Furthermore, the execution of the smart contract ensures that operators provide the prescribed levels of service stipulated in the SLA, to enable seamless continuity of sessions as illustrated in the graph. The handover delay in moving from one HeNB to the next available HeNB is equivalent to the roundtrip time in writing a transaction to the smart contract address, which from our simulation is approximately 70 ms. This delay figure is enough to meet the stringent delay requirements required for real-time applications such voice and video (150 - 200 ms) [35].

The blockchain transaction simulation is carried out on fifteen (15) Ethereum virtual machines (VM) in order to provide insight on the frequency of transactions between multiple users and the number of times users access services from the MNOs. The virtual machines run on a Dell Latitude 7400 with Intel(R) Core (TM) i7-8665U CPU @ 2.11 GHz, 16 GB of RAM, and 1 Gbps ethernet connection. The difficulty level is set to 1 for every block and the approximate block processing time is set to about 10 seconds using the PoW consensus algorithm. The blockchain performance is evaluated across different instances with 1, 5, 15 and 25 users actively interacting with the smart contract, each instance was simulated for 600 seconds as shown in Fig. 11.

It is observed that the number of transactions increases over time across the different categories of users, however,

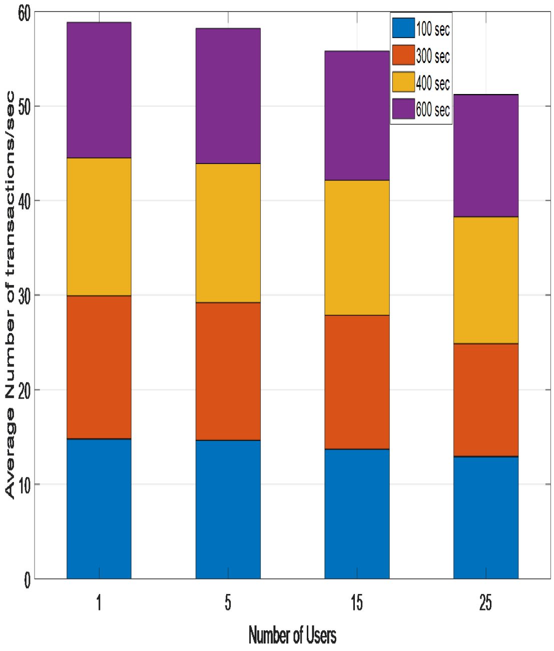

FIGURE 12. **Average number of transactions per second at different instances during the simulation with increasing number of users.**

the number of transactions mined decreases with increase in users. This is due to the increased number of blocks that have to be processed by miners which in turn increases the difficulty level culminating in a slow consensus. The recording of every single transaction in the blockchain results in a very huge amount of data to be stored in the blockchain which comes with severe penalties such as increased latency (i.e. time to execute a transaction) and reduced scalability. To cope with latency and scalability issues which constitute a major challenge in blockchain implementations, our solution adopts the strategy of moving most of the transactional data off-chain, leaving only the most recent transaction on the blockchain. To facilitate this without breaking the block's harsh, all transactions are hashed in a Merkle tree with only the root included in the block's hash. This is supported by our results in Fig.12, which shows an analysis of the number of transactions per second at different instances of the simulation with increasing number of users. It is observed that the number of transactions executed at each instance of the simulation (100 s, 300 s, 400 s, 600 s) are relatively consistent for each set of users and decreases just marginally with an increasing number of users. From the simulation results, the huge number of successful transactions recorded notwithstanding the increase in number of users clearly demonstrates the scalability of our solution and how smart contracts can enable interoperability across network operators.

Our proposed multi-operator small cell solution very much aligns with provisions of the latest 3GPP Release 15 and beyond which allow support for multi-operator core network (MOCN), whereby the RAN can be shared by multiple core networks [24], [36]. This blockchain agreement executed via smart contracts enables spectrum sharing through the shared use of the RAN by multiple core networks. The serving MNO provides the radio access elements e.g., eNBs/HeNBs which are shared to provide access to both home and visiting subscribers. The MOCN used in our scenario is justified because the MNOs each maintain their core networks and shared access is provided over the RAN. However, our approach uses smart contracts to enable RAN sharing so that subscribers from other operators can have access to the shared radio elements provided by the serving MNO (sharing operator). It is important to note that the approach we have introduced here is generic and can apply to any part of the spectrum that is currently in use by cellular systems or other parts that may be included by 3GPP in future.

VII. CONCLUSION AND FUTURE WORKS

This paper presents a model for multi-operator small cell deployment for 5G systems and beyond. The most important contribution of this work is the development of a framework that enables business agreements between MNOs for managing access to the radio network and network services using the smart contract feature of blockchains. Simulation results show that our platform enables users to access network service across operators.

Future research work includes consideration of additional decision metrics such as minimizing additional latency due to the blockchain, maximizing energy efficiency and maximizing resilience. Furthermore, the resource allocation problem will be extended into a mixed integer linear programming (MILP) optimization problem. The objective here is to find the optimum number of UEs from MNOs with limited resources that can be matched to MNOs with adequate resources based on some metrics (such as latency, power consumption, resilience). Finally, the effect of the SDN controller and blockchain operation on network performance indices such as E2E delay and packet loss will also be investigated.

REFERENCES

[1] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, and G. Wunder, "5G: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1201–1221, Jun. 2017.

[2] F. Hu, *Opportunities in 5G Networks: A Research and Development Perspective*, 1st ed. Boca Raton, FL, USA: CRC Press, 2016, ch. 5, pp. 71–95.

[3] Z. S. Bojkovic, M. R. Bakmaz, and B. M. Bakmaz, "Research challenges for 5G cellular architecture," in *Proc. 12th Int. Conf. Telecommun. Modern Satell., Cable Broadcast. Services (TELSIKS)*, Oct. 2015, pp. 215–222.

[4] X. Ge, S. Tu, G. Mao, C.-X. Wang, and T. Han, "5G ultra-dense cellular networks," *IEEE Wireless Commun.*, vol. 23, no. 1, pp. 72–79, Feb. 2016.

[5] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A survey on software-defined networking," *Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 27–51, 1st Quart., 2014.

[6] P. Ameigeiras, J. J. Ramos-munoz, L. Schumacher, J. Prados-Garzon, J. Navarro-Ortiz, and J. M. Lopez-soler, "Link-level access cloud architecture design based on SDN for 5G networks," *IEEE Netw.*, vol. 29, no. 2, pp. 24–31, Mar. 2015.

[7] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5G cellular: It will work!," *IEEE Access*, vol. 1, pp. 335–349, 2013.

[8] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017, doi: 10.1109/COMST.2017.2745201.

[9] I. Elgendi, K. S. Munasinghe, and A. Jamalipour, "A three-tier SDN based distributed mobility management architecture for DenseNets," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6, doi: 10.1109/ICC.2016.7511020.

[10] B. Mafakheri, T. Subramanya, L. Goratti, and R. Riggio, "Blockchain-based infrastructure sharing in 5G small cell networks," presented at the 14th Int. Conf. Netw. Service Manage. (CNSM), 2018, pp. 313–317.

[11] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, "Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. 7, pp. 9714–9723, 2019.

[12] P. Goransson and C. Black, *Software Defined Networks: A Comprehensive Approach*. Amsterdam, The Netherlands: Elsevier, 2014, ch. 4, pp. 59–79.

[13] H. Venkatarman and R. Trestian, *5G Radio Access Networks: Centralized RAN, Cloud-RAN, and Virtualization of Small Cells*. New York, NY, USA: Taylor & Francis, 2017, ch. 6, pp. 117–133.

[14] M. Saravanan, S. Behera, and V. Iyer, "Smart contracts in mobile telecom networks," in *Proc. 23RD Annu. Int. Conf. Adv. Comput. Commun. (ADCOM)*, Sep. 2017, pp. 27–33.

[15] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," 2019, *arXiv:1906.00245*. [Online]. Available: http://arxiv.org/abs/1906.00245

[16] A. Okon, N. Jagannath, I. Elgendi, J. M. H. Elmirghani, A. Jamalipour, and K. S. Munasinghe, "Blockchain-enabled multi-operator small cell network for beyond 5G systems," *IEEE Netw.*, to be published.

[17] J. S. Walia, H. Hammainen, and M. Matinmikko, "5G micro-operators for the future campus: A techno-economic study," in *Proc. Internet Things Bus. Models, Users, Netw.*, Nov. 2017, pp. 1–8, doi: 10.1109/CTTE.2017.8260985.

[18] M. Matinmikko-Blue, S. Yrjoelae, and M. Latva-aho, "Micro operators for ultra-dense network deployment with network slicing and spectrum micro licensing," in *Proc. IEEE 87th Veh. Technol. Conf. (VTC Spring)*, Jun. 2018, pp. 1–6, doi: 10.1109/VTCSpring.2018.8417554.

[19] Cloudberry. *Cloudberry Mobile*. Accessed: Aug. 9, 2019. [Online]. Available: http://www.cloudberrymobile.com

[20] J. Markendahl and A. Ghanbari, "Shared smallcell networks multi-operator or third party solutions-or both?" in *Proc. 11th Int. Symp. Workshops Modeling Optim. Mobile, Ad Hoc Wireless Netw. (WiOpt)*, Tsukuba Science City, Japan, May 2013, pp. 41–48.

[21] Denseair. *Dense Air*. Accessed: Aug. 9, 2019. [Online]. Available: http://denseair.net/

[22] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Phys. Commun.*, vol. 18, pp. 64–84, Mar. 2016.

[23] T. D. Assefa, R. Hoque, E. Tragos, and X. Dimitropoulos, "SDN-based local mobility management with X2-interface in femtocell networks," in *Proc. IEEE 22nd Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Jun. 2017, pp. 1–6, doi: 10.1109/CAMAD.2017.8031628.

[24] *(3GPP) Evolved Universal Terrestial Radio Access X2 Application Protocol (X2AP) (Rel 14), Version. 14.1.0*, document 3GPP TS 36.423, (E-UTRA), 3GPP, 2017.

[25] L. J. Chaves, I. C. Garcia, and E. R. M. Madeira, "OFSwitch13: Enhancing ns-3 with OpenFlow 1.3 support," in *Proc. Workshop ns-3-WNS3*, Seattle, WA, USA, 2016, pp. 33–40.

[26] F. H. Khan and M. Portmann, "A system-level architecture for software-defined LTE networks," in *Proc. 10th Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Gold Coast, QLD, Australia, Dec. 2016, pp. 1–10, doi: 10.1109/ICSPCS.2016.7843360.

[27] V.-G. Nguyen, A. Brunstrom, K.-J. Grinnemo, and J. Taheri, "SDN/NFV-based mobile packet core network architectures: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1567–1602, 3rd Quart., 2017, doi: 10.1109/COMST.2017.2690823.

[28] 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.

[29] E. Di Pascale, J. McMenamy, I. Macaluso, and L. Doyle, "Smart contract SLAs for dense small-cell-as-a-service," 2017, *arXiv:1703.04502*. [Online]. Available: http://arxiv.org/abs/1703.04502

[30] W. Jiasi, W. Jian, L. Jia-Nan, and Z. Yue, "Secure software-defined networking based on blockchain," 2019, pp. 1–19, *arXiv:1906.04342*. [Online]. Available: http://arxiv.org/abs/1906.04342

[31] C. Xue, N. Xu, and Y. Bo, "Research on key technologies of software-defined network based on blockchain," in *Proc. IEEE Int. Conf. Service-Oriented Syst. Eng. (SOSE)*, Apr. 2019, pp. 239–243.

[32] 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," 2019, *arXiv:1905.03193*. [Online]. Available: http://arxiv.org/abs/1905.03193

[33] *ns-3 Model Library Release ns-3.30*, document, NS3, NS-3 Project, Aug. 2019, pp. 1–549. [Online]. Available: https://www.nsnam.org/docs/release/3.30/models/ns-3-model-library.pdf

[34] T. Bilen, B. Canberk, and K. R. Chowdhury, "Handover management in software-defined ultra-dense 5G networks," *IEEE Netw.*, vol. 31, no. 4, pp. 49–55, Jul. 2017.

[35] Y. Chen, T. Farley, and N. Ye, "QoS requirements of network applications on the Internet," *Inf. Knowl. Syst. Manage.*, vol. 4, no. 1, pp. 55–76, Mar. 2004.

[36] *5G; System Architecture for the 5G System (Rel 15), Version. 15.3.0*, document 3GPP TS 23.501, ETSI, 2018.

ASUQUO A. OKON received the B.E. degree in electrical and computer engineering from the Federal University of Technology, Minna, Nigeria, in 2006, and the M.Sc. degree (Hons.) in telecommunications electronics from the University of Glasgow, U.K., in 2012. He is currently pursuing the Ph.D. degree with the School of IT and Systems, University of Canberra, Australia. From 2012 to 2017, he was a Senior Research Engineer at National Space Research and Development Agency, Nigeria. His research interests include software-defined networks, blockchain, the Internet of Things, and resource allocation and optimization techniques in beyond 5G networks.

IBRAHIM ELGENDI (Member, IEEE) received the Ph.D. degree in information technology from the University of Canberra, Australia. He is currently a Lecturer in networking and cybersecurity. He is a member of the Institution of Engineers Australia, His researches focus on mobile and wireless networks, the Internet-of-Things, machine learning, and cyber-physical-security. He has over 14 refereed publications with over 63 citations (H-index 5) in highly prestigious journals, and conference proceedings. He has served as a Reviewer for a number of journals, such as the *IEEE Wireless Communications Magazine*, the IEEE TRANSACTIONS ON MOBILE COMPUTING, and the IEEE/ACM TRANSACTIONS ON NETWORKING. He has 17 years' experience from industry in the field of automation and AI.

OLUSEGUN S. SHOLIYI was born in Ifo, Ogun, Nigeria, in 1970. He received the B.E. degree in electrical engineering from the University of Ilorin, Kwara, Nigeria, in 1992, the M.Sc. degree in microwave engineering and wireless subsystems design from the University of Surrey, U.K., in 2008, and the M.Sc. and Ph.D. degrees in electrical engineering from The University of Alabama in Huntsville, USA, in 2013 and 2014, respectively. His research interests include antenna propagation, numerical methods in electromagnetics, characterization of electromagnetic properties of materials, and microwave devices. In 2015, he started developing interest in guidance, navigation and control (GNC) of aerospace vehicles. He is currently the Director/Chief Executive at the National Space Research and Development Agency, Nigeria. He is also a Facilitator and a Project Supervisor with the National Open University of Nigeria.

JAAFAR M. H. ELMIRGHANI (Senior Member, IEEE) received the Ph.D. degree in the synchronization of optical systems and optical receiver design from the University of Huddersfield, U.K., in 1994, and the D.Sc. degree in communication systems and networks from the University of Leeds, U.K., in 2012. He is the Director of the Institute of Communication and Power Networks, School of Electronic and Electrical Engineering, University of Leeds. He joined Leeds in 2007 and prior to that (2000–2007) as the Chair of Optical Communications at the University of Wales Swansea, he founded, developed, and directed the Institute of Advanced Telecommunications and the Technium Digital (TD), a technology incubator/spin-off hub. He has provided outstanding leadership in a number of large research projects at the IAT and TD. He has coauthored *Photonic Switching Technology: Systems and Networks* (Wiley) and has published over 500 articles. He has research interests in optical systems and networks. He is a Fellow of the IET and the Institute of Physics. He was the Chairman of the IEEE Comsoc Transmission Access and Optical Systems Technical Committee and IEEE Comsoc Signal Processing and Communications Electronics Technical Committee, and an Editor of the *IEEE Communications Magazine*. He was the Founding Chair of the Advanced Signal Processing for Communication Symposium which started at IEEE GLOBECOM’99 and has continued since at every ICC and GLOBECOM. He was also the Founding Chair of the first IEEE ICC/GLOBECOM Optical Symposium at GLOBECOM’00, and the Future Photonic Network Technologies, Architectures, and Protocols Symposium. He chaired this Symposium, which continues to date under different names. He was the Founding Chair of the first Green Track at ICC/GLOBECOM at GLOBECOM 2011, and is the Chair of the IEEE Sustainable ICT Initiative within the IEEE Technical Activities Board (TAB) Future Directions Committee (FDC) and within the IEEE Communications Society, a Pan IEEE Societies Initiative responsible for Green and Sustainable ICT activities across IEEE, 2012–present. He was on the Technical Program Committee of 39 IEEE ICC/GLOBECOM Conferences, from 1995 to 2020, including 19 times as the Symposium Chair. He received the IEEE Communications Society Hal Sobol Award, the IEEE Comsoc Chapter Achievement Award for excellence in chapter activities (both in 2005), the University of Wales Swansea Outstanding Research Achievement Award, in 2006, the IEEE Communications Society Signal Processing and Communication Electronics Outstanding Service Award, in 2009, the Best Paper Award at IEEE ICC’2013, the IEEE Comsoc Transmission Access and Optical Systems Outstanding Service Award 2015 in recognition of “Leadership and Contributions to the Area of Green Communications,” received the GreenTouch 1000x Award, in 2015, for pioneering research contributions to the field of energy efficiency in telecommunications, the 2016 IET Optoelectronics Premium Award and shared with 6 GreenTouch Innovators the 2016 Edison Award in the collective disruption category for their work on the GreenMeter, an international competition, clear evidence of his seminal contributions to Green Communications which have a lasting impact on the environment (green) and society. He was Co-Chair of the GreenTouch Wired, Core and Access Networks Working Group, an Adviser to the Commonwealth Scholarship Commission, a member of the Royal Society International Joint Projects Panel, and a member of the Engineering and Physical Sciences Research Council (EPSRC) College. He was the Principal Investigator (PI) of the £6m EPSRC INTelligent Energy awaRe NETworks (INTERNET) Programme Grant, 2010–2016 and is currently PI of the £6.6m EPSRC Terabit Bidirectional Multi-User Optical Wireless System (TOWS) for 6G LiFi Programme Grant, 2019–2024. He has been awarded in excess of £30 million in grants to date from EPSRC, the EU, and industry and has held prestigious fellowships funded by the Royal Society and by BT. He was an IEEE Comsoc Distinguished Lecturer, from 2013 to 2016. He was an Editor of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS and the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS series on green communications and networking. He is currently an Editor of *IET Optoelectronics*, the *Journal of Optical Communications*.

ABBAS JAMALIPOUR (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Nagoya University, Japan. He is a Professor of ubiquitous mobile networking with the University of Sydney, Australia. He has authored nine technical books, 11 book chapters, over 450 technical articles, and five patents, all in the area of wireless communications. He is a Fellow of the Institute of Electrical, Information, and Communication Engineers (IEICE) and the Institution of Engineers Australia, an ACM Professional Member, and an IEEE Distinguished Lecturer. He is the President and an Elected Member of the Board of Governors of the IEEE Vehicular Technology Society. He has been a General Chair or a Technical Program Chair for a number of conferences, including IEEE ICC, GLOBECOM, WCNC, and PIMRC. He was a recipient of a number of prestigious awards, such as the 2019 IEEE ComSoc Distinguished Technical Achievement Award in Green Communications, the 2016 IEEE ComSoc Distinguished Technical Achievement Award in Communications Switching and Routing, the 2010 IEEE ComSoc Harold Sobol Award, the 2006 IEEE ComSoc Best Tutorial Paper Award, and 15 best paper awards. He was the Editor-in-Chief of the IEEE WIRELESS COMMUNICATIONS, the Vice President-Conferences, and a member of the Board of Governors of the IEEE Communications Society. He serves as an Editor of IEEE ACCESS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and several other journals.

KUMUDU MUNASINGHE (Senior Member, IEEE) received the Ph.D. degree in telecommunications engineering from the University of Sydney. He is currently an Associate Professor in network engineering and the Leader of the IoT Research Group, Human Centred Research Centre, University of Canberra. His researches focus on next generation mobile and wireless networks, the Internet-of-Things, green communication, smart grid communications, and cyber-physical-security. He has over 100 refereed publications with over 900 citations (H-index 17) in highly prestigious journals, conference proceedings and two books to his credit. He has secured over $ 1.6 million dollars in competitive research funding by winning grants from the Australian Research Council (ARC), the Commonwealth and State Governments, Department of Defense, and the industry. He has also won the highly prestigious ARC Australian Postdoctoral Fellowship, served as a co-chair for many international conferences, served as an editorial board member for a number of journals. His research has been highly commended through many research awards, including two VC’s research awards and three IEEE best paper awards. He is currently a Charted Professional Engineer, an Engineering Executive, and a Companion (Fellow Status) of Engineers Australia.

• • •