Blockchain-based Infrastructure Sharing in 5G Small Cell Networks

Babak Mafakheri[1], Tejas Subramanya[1], Leonardo Goratti[2], Roberto Riggio[1]
[1]Wireless and Networked Systems, FBK CREATE-NET, Trento, Italy
Email: {b.mafakheri, t.subramanya, rriggio}@fbk.eu
[2]Zodiac Inflight Innovations, Weßling, Germany
Email: Leonardo.Goratti@zii.aero

***Abstract*—Recently, the interest in using Blockchain as a secure and distributed ledger has increased dramatically. Although the main purpose of Blockchain by means of Bitcoin was about cryptocurrency and peer to peer transactions, its application to other systems has been widely used. One of the fields that has potential possibilities to benefit from BlockChain features is telecommunication. BlockChain can be applied in case of management of various networks to reduce some expenses. In this position paper, we apply a BlockChain network with smart contract in the cellular mobile networks. The Blockchain can provide a distributed HSS in a way that the core networks of different operators can use it in a secure manner. Moreover, the smart contract can act as a distributed Self Organizing Network features to handle self-transactions among mobile operators in return of sharing small cells' infrastructure.**

I. Introduction

There has been a continued increase in mobile traffic demand that is forecast to reach 49 exabytes per month by 2021 [1]. In order to accommodate such a dramatic increase, the fifth generation of mobile network (5G) is expected to deliver a 1000 times increase in the system capacity, reduced round-trip delays and enhanced performance for cell-edge users. To meet the aforementioned goals, Mobile Network Operators (MNOs) are predominantly considering network densification by deploying numerous small cells [2]. However, such a hyperdense network poses several deployment challenges, in turn, resulting in an increased total cost of ownership. In this regard, Self-Organizing Network (SON) plays a crucial role to adequately manage such dense heterogeneous network deployments in an autonomous fashion, through self-configuration, self-optimization, and self-healing, thereby cutting down the CAPital EXpenditure (CAPEX) and OPerating EXpenses (OPEX) of the network operator [3].

Although leveraging SON algorithms have allowed operators to reduce management and maintenance costs, its full potential is yet to be explored. One such use case for SON is to allow an operator to share their mobile network with other operators, thus reducing the operator investment costs on infrastructure. There are several technical solutions that make the sharing of network resources possible which includes site sharing, mast sharing, RAN sharing, and roaming. In site sharing, mast sharing, and RAN sharing, operators share their active network elements while in roaming, they do not share any network elements but carry user traffic from one carrier over to the other. In the current network sharing architectures, operators follow a well-known agreement model known as Service Level Agreements (SLA). However, in this paper, we propose adopting Blockchain technology as a facilitator to share network resources among operators in a sovereign, autonomous, secure and trusted manner. Moreover, we illustrate, by using a smart contract feature of the Blockchain, how operators can share their network resources through peer-to-peer self-executing transactions, resembling the characteristics of SON but in a rather distributed approach.

The remainder of this paper is organized as follows: Section II provides a literature review on SON and Blockchain. Section III describes the most important features of Blockchain technology. In section IV, we introduce the relevant functionalities of legacy LTE network architecture and then illustrate how Blockchain can renovate and optimize such an architecture. In the end, section V concludes this work.

II. State of the Art

Although both SON and Blockchain are fairly new, several literature works could be found with regard to these technologies. SON is introduced in 3GPP Release 8 and 9 with diminishing the operators' cost as being the main goal of automated network function. Authors in [4] focus on a self-booting mechanism of the SON while authors in [5] talk about the use of SON in the integration of inter-cell interference coordination and cognitive radio in 5G heterogeneous networks. There are many other works on SON to determine how it can reduce the network operation costs by adding self-ruling functionalities [3, 6, 7]. Blockchain and its practicality for various scenarios have seen a great interest in recent years such as its performance in 5G network. Authors in [8] remark spectrum sharing through a public Blockchain. A practical case can be found in the white paper of QLINK startup [9] which discusses the implementation of decentralized Wi-Fi sharing. Moreover, in [10] authors address different aspects of Blockchain in mobile networks such as in IOT, Smart Cities, and 5G service enablers. There are many other examples of research about the usage of Blockchain in telecommunications word such as as [11, 12].

To the best of our knowledge, this paper is the first of its kind to propose new techniques based on Blockchain to facilitate sharing of network resources amongst operators.

978-3-903176-14-0 © 2018 IFIP

III. Background

A. How Blockchain Works?

On a high level, the basic workflow of Blockchain can be described as follows: (i) say Operator A wants to send money to Operator B; (ii) This transaction data is represented as a block and it is broadcasted to every party in the network. (iii) Other nodes execute a consensus algorithm to approve that the transaction within the block is valid. (iv) at this point, the block is appended to the chain of blocks [13].

B. Consensus protocols and BlockChain types

The most important Blockchain consensus mechanisms are Proof of Work (PoW), Proof of Stake (PoS), and delegated Byzantine Fault Tolerance (dBFT), although several others exist. In PoW, miners compete against each other to confirm transactions on the network, in turn, to get rewarded. Thus, to operate a PoW system, the computational power required is very energy intensive. In PoS, there is no competition involved to mine blocks and hence there is no high electricity consumption. However, the validator holding more assets (coins/tokens) has a higher chance to mine blocks. Byzantine Fault Tolerance is an alternative energy efficient consensus mechanism that is able to defend against component failures in distributed systems that prevent other components of the system from reaching an agreement among themselves. The algorithm allows the distributed network to operate correctly in environments where certain nodes may be untrustworthy or outright malicious [14].

Apart from consensus mechanisms, we introduce three different types of Blockchain networks:

Public BlockChain. In this Blockchain, anyone can be part of the network and can have their own private and public keys. Moreover, all participant nodes can be involved in consensus mechanism and can also check and validate all transactions within the network.

Private BlockChain. In private or permissioned Blockchain not everyone in the network can engage in the consensus, but the nodes are selected by an administrator.

Consortium BlockChain. This type of Blockchain is considered to be a combination of two other Blockchain types. It is also a permissioned Blockchain but it has more than one administrator and the executives of the chain are in a partnership.

C. Decentralized applications and Smart Contracts

Decentralized Application (DApp) is a server-less peer to peer application that can run on a particular Blockchain written for a specific use case. Whereas, smart contract is a self-executing contract where the terms of agreement between the buyer and the seller are pre-agreed and are directly written into lines of code. A smart contract is a collection of functions and data that resides at a specific address on the Blockchain. The data can be queried or altered by calling functions of the smart contract or by making a transaction to it. The functions are executed automatically on every node in the network according to the data that was included in the triggering transaction [15].

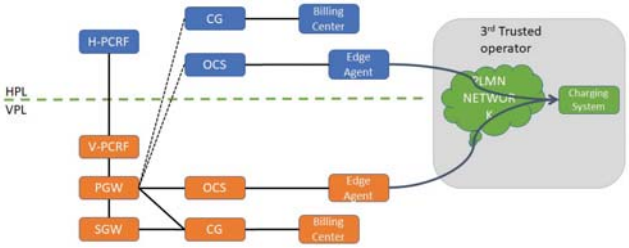

Fig. 1. LocalBreakOut Roaming with Charging System

IV. Sharing of network resources in Small Cells

A. Overview

In the conventional architecture of cellular networks, each operator covers the whole geographical area of interest such as a country, a province etc. Each operator can deploy its own access network or share their access network resources with other operators to reduce the infrastructure costs. However, satisfying the requirements of 5G by deploying dense small cells that has a very low coverage area (i.e., 10-100 m) would be very costly for operators to cover the whole geographical area within a country. So, in order to reduce both CAPEX and OPEX, operators can benefit from each other by splitting the coverage areas. The solution with Blockchain as a SON could be very efficient if used properly. With Blockchain technology, operators can cooperate with each other by splitting the entire geographical area to be covered among each of them and provide services to users from other operators. Thus, a peer to peer (Crypto-currency) transaction can be done among them in a secure environment without the need of any central third-party. This approach is very similar to Local-Break-Out roaming in LTE, [16]. Fig. 1 shows the architecture of Local Break-Out roaming in legacy roaming structure. In this scenario, for charging, roaming information must be associated with charging accounts. However, the visited network does not have subscriber charging information and the home network does not have subscriber roaming information. To solve this problem in legacy architecture, an intermediator needs to be introduced to coordinate and provide billing settlements [16]. However, having a third party entity does not solve the problem of trust amongst multiple operators. Moreover, implementation of this scenario for 5G small cells can be too complex; so by using Blockchain technology combined with legacy roaming scenario such as Local-Break-Out roaming, there would be no need for any trusted third party, or intermediate operator, to coordinate the billing procedure.

B. Attach and Detach procedure in LTE

In this section, we will briefly introduce the overall LTE network architecture and describe the UE attach and detach procedure in detail. As shown in Fig. 2, the LTE network is composed of two main elements: Radio Access Network (RAN) and Evolved Packet Core (EPC). The RAN is composed of a number of interconnected small cells and macro eNodeBs using a standard x2 interface, to which the terminals

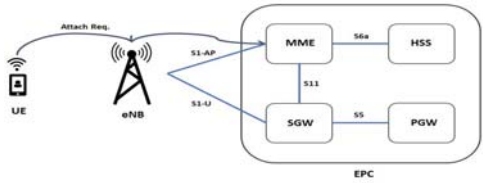

Fig. 2. Architecture of LTE Network

can connect. The EPC is composed of the Mobility Management Entity (MME), the Serving Gateway (SGW), the Packet Gateway (PGW), and the Home Subscriber Server (HSS) [17]. All of these elements are interconnected to each other using standardized LTE interfaces.

The UE attach procedure mainly consists of five steps, that are discussed here in briefly.

At first, the UE ID acquisition will be done when UE tries to attach to the network. Second, MME checks the users International Mobile Subscriber Identity (IMSI) with HSS. After this and upon accepting the IMSI, the UE and MME perform mutual authentication using Non-Access Stratum (NAS) protocol to complete the security setup. At the next step, MME registers the subscriber to the network and sends an update location request towards HSS. The HSS then responds with a message containing all the subscriber information (Access Point Name, PGW-ID, QoS profile) necessary for establishing the EPS sessions. Finally, MME based on the user subscription information creates an EPS session and a default EPS bearer for the user by establishing the GPRS Tunnelling Protocol (GTP) among eNodeB, SGW, and PGW.

The UE detach procedure can be classified into three types:

1) UE-initiated Detach, is when the UE is turned off or if the SIM card is removed from the UE,

2) MME-initiated Detach, is when it cannot provide services to the user because of the poor radio link quality or if the re-authentication fails.

3) HSS-initiated Detach, is when the subscriber profile available in HSS is changed.

Once UE is done using its services, it will initiate a 'Detach Request' message towards MME for releasing its bearers. MME in coordination with SGW and PGW removes all the networks or radio resources allocated to the EPS session of the user and notifies HSS to update its database accordingly. MME now responds with 'Detach Accept' message towards UE to complete the detach process.

C. Blockchain as a solution

In the previous section, we described how a UE can attach and detach to the mobile network based on the subscription information maintained by the HSS of EPC. Here, we illustrate how the user subscription information and authentication keys can be stored in a distributed ledger instead of a centralized HSS and perform authentication and security procedures by communicating with this ledger.

We propose a new architecture for the core network of LTE i.e., instead of having a centralized database for maintaining all the subscriber information in a single place, a distributed database is considered. There are different options to store data in a Blockchain-based distributed data base. There is possibility of storing all the information in Blockchain itself. Although this approach is the simplest way of data storage, very slow transaction speed is a known drawback. This drawback can cause significant problems with regards to retrieving user information by core network especially in handover scenarios among small cells. Therefore, there is a need to have a distributed, fast-transaction database. One such option is Interplanetary File System (IPFS), a technology based on BitTorrent with enormous data capacity and very fast transaction speed [18]. The details of such distributed databases are out of the scope of this paper. However, the core network of all mobile operators need to have access to such distributed database, enabling operators to provide services to even subscribers from other operators based on successful network authentication as will be discussed below.

In our scenario, we recommend using Consortium Blockchain to facilitate collaboration among different operators. This would allow having multiple operators as administrators who can decide, select and approve the associated nodes within the chain in a permissioned fashion. Moreover, Consortium Blockchain is highly secure compared to a public chain thereby avoiding any risk of Sybil attack [15]. Furthermore, in a cellular network, using a power-hungry consensus mechanism is not practical due to the huge operational costs involved. Therefore, among the discussed consensus mechanisms, PoS and dBFT could be the best possible options. We consider that all core networks of various operators are part of the Consortium Blockchain. Hence, each one of them is able to communicate with a smart contract by means of a transaction to the smart contract address. Since each core network (node) is authenticated by the administrator to be part of the chain, all nodes have a copy of the entire Blockchain.

When a new sim card is configured by an operator, the information of the sim will be distributed within the Consortium Blockchain through a new block. Thus, this block will be available to all the nodes (core networks) among the chain. Furthermore, new blocks can be made and the whole Blockchain will be updated upon new user subscriptions and data consumption. Whenever a user does any activity such as charging the sim card or subscribing to a new offer, this information will be stored in another block and after validation by other nodes, it will be published to all the other nodes within the chain as a copy in the distributed ledger. This ledger can have the same role to that of HSS which stores user subscription information. In contradiction to classical architecture, it will remain shared among all operators.

For the remainder of this paper, the operator who is providing any service to the users is called the serving operator while other operators are named as the guest operator.

To begin, when a SIM card is first sold to the client, the serving operator validates the client and sends an encrypted digital proof of the clients validity into the Blockchain. As shown in Fig. 3, when the EPC of the serving network receives an attach request from a user, it retrieves IMSI information

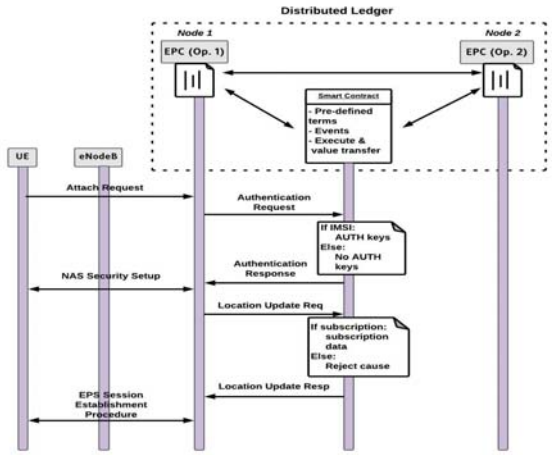

Fig. 3. Attach procedure using Blockchain approach

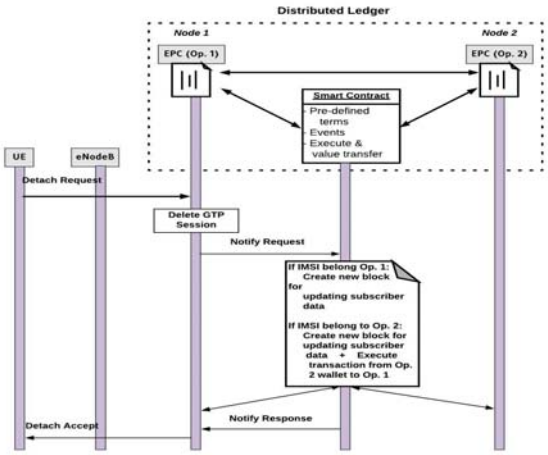

Fig. 4. Detach procedure using Blockchain approach

from the message and performs a null transaction to the smart contract. The smart contract will then check if the user belongs to one of the operators who are already in an agreement with Consortium Blockchain. If that's the case, the smart contract sends user's authentication keys to the MME. The MME then performs authentication and security mechanisms towards the UE. Once they are complete, MME requests and receives subscriber information from the distributed ledger. At this stage, the MME with the help of SGW and PGW of the core network establishes necessary radio bearers to provide services to the user. Once the user detaches from the network (Fig. 4), the MME sends the charging information about the user along with its IMSI to the smart contract. From now on, the smart contract will check if the user belongs to the serving operator or if it belongs to the guest operator. In the former, a new block will be created with the updated information on the user's subscription; In the latter case, beside updating the user's information in a new block, peer to peer transaction between the guest operator wallet and the serving operator wallet will be executed by the smart contract based on the user's consumption and the smart contract contents. The contents of smart contract can also vary from time to time and based on the geographical location of small cells. For example, small cells that are deployed in a crowded area (i.e., city centers) can ask for more crypto-currency than small cells that are deployed in remote areas. These information can be agreed among operators in advance.

D. Possible existing platform

To create a DApp and to implement a smart contract for our use case, we need to rely on one of the existing platforms. Currently there are several Blockchain platforms that provide the possibility for writing smart contracts such as Ethereum, NEO, and Qtum. Ethereum is one of the most popular platform upon which many smart contacts are implemented. It provides a chain based, turing-complete, smart contract system that can be used to create a variety of decentralized Blockchain applications. However, Ethereum is based on PoW consensus mechanism. As already discussed in subsection IV-C, PoW is not suitable for our use case. NEO is another popular Blockchain platform with the aim of digitizing assets. The Consensus mechanism of NEO Blockchain is based on dBFT. The Byzantine fault-tolerant consensus mechanism enables large scale participation in consensus through proxy voting [19]. Due to its consensus mechanism, this platform does not consume too much energy which can be an ideal for our DApp. The smart contract will generate some tokens specifically for the operators to make transactions. Each operator can get the tokens by sending NEO crypto-currency to the smart contract address. The ratio of the generated token and the crypto-currency can be defined by operators and programmed to the smart contract. Due to the nature of private or consortium Blockchain, this ratio will remain stable.

V. Conclusion

This study aims to use Blockchain as a distributed database to add new functionalities to SON using smart contracts. It also demonstrates how operators can collaborate and define the contents of a smart contract to reduce many expenses. Having a decentralized network of nodes to maintain the distributed ledger allows operators to offset and offload hosting, security, and maintenance costs. It removes many expenses for IT staffing and infrastructural overhead. Moreover, the decentralized network provides a secure and trusted mechanism than any other third-party brokers since all transactions are executed using smart contracts in a transparent and traceable way. In this manner, Blockchain is not only a distributed database, but a technology that enables to share database among different operators. This new database equipped with an executable smart contract enables high availability of data and transparent transaction among different nodes of the chain.

Acknowledgments

Research leading to these results received funding from the European Union's H2020 RIA Action under Grant Agreement H2020-ICT-644843 (5G-ESSENCE Project).

REFERENCES

[1] Cisco White Paper, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021," 2017.

[2] "MBiT Index," Nokia, Tech. Rep., 2017.

[3] H. Klessig, D. Öhmann, A. I. Reppas, H. Hatzikirou, M. Abedi, M. Simsek, and G. P. Fettweis, "From immune cells to self-organizing ultra-dense small cell networks," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 4, pp. 800–811, 2016.

[4] H. Hu, J. Zhang, X. Zheng, Y. Yang, and P. Wu, "Self-configuration and self-optimization for lte networks," *IEEE Communications Magazine*, vol. 48, no. 2, 2010.

[5] S. Sun, M. Kadoch, and T. Ran, "Adaptive son and cognitive smart lpn for 5g heterogeneous networks," *Mobile Networks and Applications*, vol. 20, no. 6, pp. 745–755, 2015.

[6] O. K. Tonguz and W. Viriyasitavat, "A self-organizing network approach to priority management at intersections," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 119–127, 2016.

[7] C. Ramirez-Perez and V. Ramos, "Sdn meets sdr in self-organizing networks: fitting the pieces of network management," *IEEE Communications Magazine*, vol. 54, no. 1, pp. 48–57, 2016.

[8] K. Kotobi and S. G. Bilén, "Blockchain-enabled spectrum access in cognitive radio networks," in *Wireless Telecommunications Symposium (WTS), 2017*, Chicago, USA, 2017.

[9] A. L. Susan Zhou. Qlink White Paper. [Online]. Available: https://qlink.mobi/qlink2/res/WhitePaper.pdf

[10] E. Langberg. Blockchain in Mobile Networks. [Online]. Available: http://e.huawei.com/us/publications/global/ict_insights/201703141505/core-competency/201703150928

[11] T. Sanda and H. Inaba, "Proposal of new authentication method in wi-fi access using bitcoin 2.0," in *Consumer Electronics, 2016 IEEE 5th Global Conference on*. IEEE, 2016.

[12] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing: Challenges and applications," *arXiv preprint arXiv:1711.05938*, 2017.

[13] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges." *IJ Network Security*, vol. 19, no. 5, pp. 653–659, 2017.

[14] J. Charles, "Byzantine fault tolerance: Prime vs the bitcoin blockchain."

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

[16] LTE International Roaming Whitepaper. [Online]. Available: http://carrier.huawei.com/en/technical-topics/core-network/lte-roaming-whitepaper

[17] T. Subramanya, L. Goratti, S. N. Khan, E. Kafetzakis, I. Giannoulakis, and R. Riggio, "A practical architecture for mobile edge computing," in *Network Function Virtualization and Software Defined Networks (NFV-SDN), 2017 IEEE Conference on*, Berlin, Germany, 2017.

[18] T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, R. Henderson, S. Bellemare, and A. Granzotto, "Bigchaindb: a scalable blockchain database," *white paper, BigChainDB*, 2016.

[19] NEO White Paper, A distributed network for the Smart Economy . [Online]. Available: http://docs.neo.org/en-us/whitepaper.html