ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

ARCHIVIO ISTITUZIONALE
DELLA RICERCA

Alma Mater Studiorum Università di Bologna
Archivio istituzionale della ricerca

Smart Contracts in the 5G Roaming Architecture: The Fusion of Blockchain with 5G Networks.

This is the final peer-reviewed author's accepted manuscript (postprint) of the following publication:

Published Version:
Babak Mafakheri, A.H. (2021). Smart Contracts in the 5G Roaming Architecture: The Fusion of Blockchain with 5G Networks. IEEE COMMUNICATIONS MAGAZINE, 59(3), 77-83 [10.1109/MCOM.001.2000857].

Availability:
This version is available at: https://hdl.handle.net/11585/812990 since: 2021-03-05

Published:
DOI: http://doi.org/10.1109/MCOM.001.2000857

Terms of use:

Some rights reserved. The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

This item was downloaded from IRIS Università di Bologna (https://cris.unibo.it/).
When citing, please refer to the published version.

(Article begins on next page)

12 October 2024

This is the final peer-reviewed accepted manuscript of:

B. Mafakheri, A. Heider-Aviet, R. Riggio and L. Goratti, "Smart Contracts in the 5G Roaming Architecture: The Fusion of Blockchain with 5G Networks," in *IEEE Communications Magazine*, vol. 59, no. 3, pp. 77-83, March 2021

The final published version is available online at:

https://doi.org/10.1109/MCOM.001.2000857

Terms of use:

Some rights reserved. The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

This item was downloaded from IRIS Università di Bologna (https://cris.unibo.it/)

When citing, please refer to the published version.

Smart Contracts in the 5G Roaming Architecture: The Fusion of Blockchain with 5G Networks

Babak Mafakheri*, Andreas Heider-Aviet†, Roberto Riggio‡§, Leonardo Goratti¶
*University of Bologna, Italy; Babak.Mafakheri2@unibo.it.
†T-Systems, Germany; Andreas.Heider-Aviet@t-systems.com.
‡i2CAT, Barcelona, Spain; Roberto.Riggio@i2cat.net.
§RISE Research Institutes of Sweden AB, Stockholm, Sweden; Roberto.Riggio@ri.se
¶Safran Passenger Innovations GmbH; Leonardo.Goratti@zii.aero

***Abstract*—The roll-out of the fifth generation of cellular network (5G) technology has generated a new surge of interest in the potential of blockchain to automate various use cases involving cellular networks. 5G is indeed expected to offer new market opportunities for small and large enterprises alike. In this article, we introduce a new roaming network architecture for 5G based on a permissioned blockchain platform with smart contracts. The proposed solution improves the visibility for mobile network operators of their subscribers' activities in the visited network, as well as enabling quick payment reconciliation and reducing fraudulent transactions. The paper further reports on the methodology and architecture of the proposed blockchain-based roaming solution using the Hyperledger platform.**

***Index Terms*—5G, Roaming, Blockchain, Distributed ledger, Hyperledger, Smart contracts**

I. Introduction

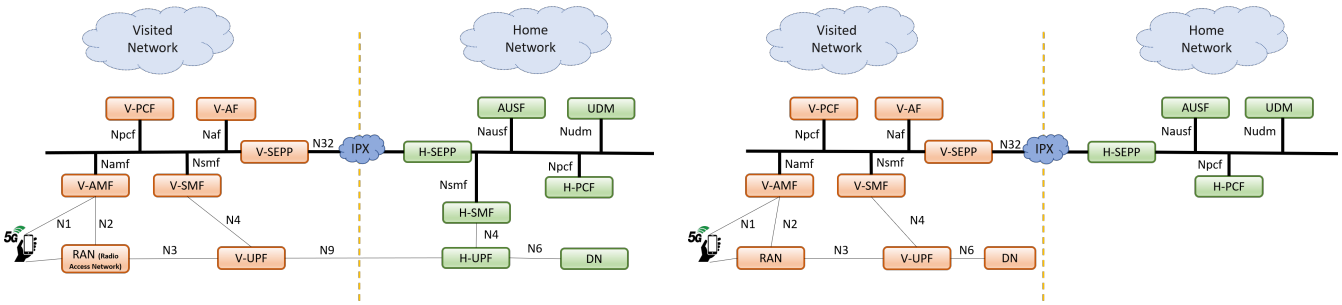
5G is made far more dense by the range of coverage of the cells (from macro- to pico-cells). Thus, it is predicted that cellular networks will shift toward complex systems with heterogeneous participants rather than uniquely owned single authority systems. Since these models require uninterrupted connectivity between all the cells, the availability of radio access and the core network remain a challenge due to the high mobility of the users. Roaming is implemented both nationally and internationally by mobile network operators (MNOs) as one of the technological solutions for sharing network resources. As a result of small cell implementation, roaming can happen more often in 5G networks [1]. With ever-increasing globalization and network densification, the need for reasonably priced roaming services becomes even greater, and to meet this need new advanced solutions are required. To this end, the decentralized nature may imposes novel challenges on service provision, and raises consistency, completeness and privacy concerns.

By leveraging on its distributed nature, blockchain and distributed ledger technology (DLT) emerge as revolutionary approaches for decentralization with distributed consensus. Since blockchain technology permits the replacement of third-parties and enables new applications [2], it is predicted that it will play a disruptive role in the design of the next generations of cellular networks [3] and [4]. One interesting case of merging DLT with cellular networks is that of roaming scenarios, in which the blockchain can handle the charging systems between mobile operators to improve business processes, reduce costs, and enable new business opportunities. After introducing the possibility of using DLT in ultra-dense networks for cost effectiveness in [5], in this work, we propose to extend its use by demonstrating a new and comprehensive architecture for 5G core networks based on permissioned blockchain technologies in roaming scenarios. In [6] the authors illustrate a blockchain-based roaming system while comparing different platforms. It is, however, based on a permission-less platform (namely Ethereum), which can introduce significant security and, more importantly, privacy issues for the mobile operators since everyone can join the blockchain network. Moreover, as shown in [7], the Hyperledger permissioned blockchain outperforms the Ethereum platform in various performance metrics, such as transactions latency and network throughput in terms of transactions per second. Further, the global system for mobile communications association (GSMA) has already introduced blockchain in wholesale roaming and the interconnection of billing scenarios [8].

In this paper, we propose a new framework based on a permissioned blockchain that allows non-trusting mobile operators to perform peer-to-peer self-transactions adopting smart contract agreements to facilitate the charging system and accomplish billing settlements for roaming. The use of a permissioned blockchain, such as Hyperledger not only offers better performance in terms of network throughput and latency, but it will also guarantee security and privacy thanks to the possibility of making a consortium blockchain that prevents the presence of anonymous nodes. We begin with a brief description of current roaming architectures and the challenges they face, and then we continue with some background on DLT and the role of blockchain in roaming. After that, we describe the general architecture of our proposed blockchain-based roaming model that is focused on billing settlements. Finally, we summarize our work and outline some directions for future research.

II. Roaming in 5G Networks

Roaming is a very important feature developed by the third generation partnership project (3GPP) to provide mobile users with national and global cross-border service continuity. Thus, a user equipment (UE) camping in a visitor network



(a) *Home-routed* roaming architecture.

(b) *Local-breakout* roaming architecture.

Fig. 1: Roaming architectures in 5G networks (3GPP TS 23.501).

of another MNO can receive uninterrupted services as if it were camping in the network of the home MNO. According to 3GPP TS32.407 (V9.2.0), *national roaming* subscribers are the ones who are roaming in a public land mobile network (PLMN) than their own, with such a network, called visited-PLMN (V-PLMN), having the same mobile country code (MCC) as the home-PLMN (H-PLMN). *International roaming*, a subscriber roams in a V-PLMN network with a MCC that is different than that of the H-PLMN. The legal and business aspects contracted between the roaming parties for charging clients for the services used are specified in roaming agreements [9].

A. Roaming Architectures

Regardless of the type of interfaces used between the H-PLMN and the V-PLMN, according to 3GPP standards, international and national roaming services use the same architecture. In 5G, roaming always relies on a security edge protection proxy (SEPP), which acts as a service relay between the V-PLMN and the H-PLMN that provides a secure connection, as well as hiding the complexity of the network topology. In addition, the application function (AF) interacts with the 5G core to provide the required services, such as traffic routing or policy control. Moreover, the authentication server function (AUSF) in the H-PLMN is responsible for performing authentication between the UE and the 5G core.

As of today two types of roaming models are supported in 5G according to 3GPP TS 23.501, as summarized in [10]. In the first one, referred to as *home-routed*, the home network provides the IP address for the roaming users. The user plane traffic of the roaming UE is always served by the home-MNO (H-MNO), thus giving more control over the users' traffic (Fig. 1(a)). A UE uses the access mobility management function (AMF) and the session management function (SMF) of the visited-MNO (V-MNO), while the user plane function (UPF) of the home operator is used to connect to a data network (DN). The SMF in the H-MNO obtains the subscription data directly from the unified data management (UDM). The main drawback of this model is the high latency incurred, since user plane traffic must be tunneled toward the home network. Although latency is generally high, the model is recommended when the relationship between two operators is not of total trust.

To resolve the latency issue in *home-routed* roaming, mobile network operators can use the second type of roaming via the *local breakout* (LBO) architecture shown in Fig. 1(b). In this model, the user plane traffic of a roaming UE is served directly by the V-MNO, while authentication and handling of subscription data is managed by the home network. The basic roaming policy and charging is applied by the visiting policy charging function (PCF) as per the roaming agreements. In this case, only signaling data is routed to the home network, which allows more efficient routing in terms of latency, although the home MNO loses control over its subscribers. In this case, the IP address of a roaming user is obtained from the visited network. Therefore, a roaming UE uses a radio bearer and 5G core resources of the visiting network. From a quality of service viewpoint, this is considered the best architecture option. However, intermediaries may be required to handle the billing settlements between independent mobile operators, thus raising concerns regarding security, trust and complexity.

B. Challenges and Operational Requirements

In the LBO architecture, the roaming information must be associated with the subscribers' accounts. This configuration gives rise to the problem that the H-MNO lacks the subscriber's roaming information and the V-MNO lacks the subscriber's charging information. Therefore, the MNOs have to manage multiple relationships, interconnect globally, and handle complicated financial exchanges [11]. The relationships between MNOs can be classified as direct or indirect. In the direct case, MNOs maintain point-to-point relationships with each other, which requires a separate contract for each relationship. The disadvantages of this are high costs, overheads and the requirement of direct communication, which is not always possible (e.g. in the case of political impediments). In the indirect case, a clearinghouse is used to connect the MNOs, as shown in Fig. 2. This model also presents several drawbacks. First, the presence of an intermediary implies significant extra costs for the network but, more importantly, it raises concerns about security and trust by introducing a third-party.

Currently, among almost all MNOs the *home-routed* approach is the most widely adopted. Although the LBO offers better performance in theory, MNOs prefer to keep control over their user identities, security, billing, etc. Moreover,

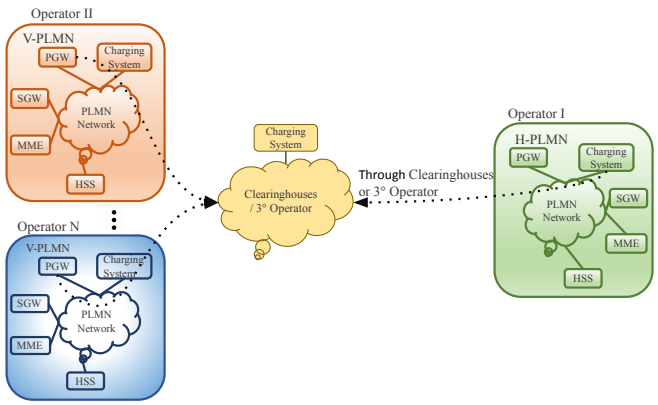


Fig. 2: Roaming with a third-party clearing-house.

neither the long term evolution (LTE) nor the 5G standard incorporates shared and distributed database approaches, which could facilitate, optimize and harmonize data management. Since it has been realized that from a technical point of view it is highly inefficient to tunnel back all the IP data packets of roamers (i.e. the *home-routed* approach), it is worth investigating new models for establishing billing settlements for roaming cellular users.

III. Why Blockchain for Roaming?

While discussing the pros and cons of the current roaming architecture in both LBO and *home-routed*, we found it crucial to study the way to redesign the billing mechanism in roaming scenarios. Hence, we propose a new model to exploits the possibilities of DLT to remove the role of clearinghouses in LBO while avoiding the latency issues in the *home-routed*. In this model the home network is not fully bypassed as the ledger provides the chance to monitor the users' activities in a secure and transparent manner.

A. Blockchain Topology

As can be seen in Fig. 3, four implementation layers are abstracted for a blockchain network [12]. To establish a chain of blocks, the data and network organization layer is responsible for shaping cryptographic data and organizing blocks of data in chronological order to provide security and privacy for the blockchain network.

The consensus layer guarantees reliable data synchronization (e.g. transactions) in peer to peer connections and different algorithms are used to achieve consensus such as proof of work (PoW), proof of concept (PoC), delegated byzantine fault tolerance (dBFT) [12]. In our roaming use-case, we rely on a permissioned scheme that provides the network participants with the advantage of information sharing and peer-to-peer transactions between inter-authorized organizations by forming a consortium blockchain. Moreover, since in this scheme the consensus mechanism is semi-centralized, it provides a high processing throughput. One important aspect that limits the deployment of public blockchains in many use cases is the scalability issue that by increasing the number of users, the number of transactions and validations increases which leads to communication overheads. Although there are proposals for solving the issue (e.g. lighting or sharding), they are still under development. Since private or consortium blockchains limit the number of users, they do not normally address the scalability issues. However, some consortium blockchains such as Hyperledger are equipped with channels that are like a subnet of communication between two or more members of the network. These channels could increase the scalability of the network when the number of (authorized)-users increases.

The third layer of the network involves smart contracts that are deployed on a distributed virtual system. It provides a user-defined business logic aimed at automatically executing the content of the smart contract (e.g. the costs of roaming users) across inter-authorized organizations according their agreements that define the smart contracts' rules. Afterwards, the contracts are installed in the blockchain network while their self-executable nature can apply a new transaction as soon as new data is uploaded to the distributed ledger. These transactions, which are processed by the smart contract, are added to the chain of blocks when they are confirmed through a consensus mechanism.

Finally, the top layer is called the application layer, and this acts as a sand-boxed run-time environment (e.g. Hyperledger Fabric) and defines a programming language implementation and user interface for the smart contracts by means of a decentralized application (DApp).

B. Role of Blockchain in Roaming

In order to provide support for mobile networks, a blockchain-based roaming solution must support three basic functions: discovery, identity management, and billing settlement. The rest of this section will describe these functions in detail.

1) Discovery: When a roaming UE attempts to attach to a visited network, this network first tries to discover whether the UE is a visitor coming from another MNO. In this design, the exchange of user information between the H-MNO and the V-MNO is necessary to perform this operation, which takes place on the blockchain and effectively results in the generation of a new block. This block specifies the new location of the user, the identifiers of the home- and V-MNOs, and a discovery timestamp.

2) Identity management: Immediately after the discovery phase is performed, the identity of the user must be verified and the user must be registered in the visited network as a roaming user. The authentication of the user is performed using the rules of the smart contract. The end result is that the user is either accepted or declined by the V-MNO. Once registration is successfully completed, the visiting user is able to access the authorized services in the visited network, e.g. voice calls, data, etc.

3) Billing settlements: The blockchain network is also used to record all the billing-related activities performed by the visiting user. For example, when a roaming user starts a voice call or uses data traffic, such events are logged in the blockchain. Similarly, when the call finishes, the duration of the call or the amount of data consumed is also stored. The

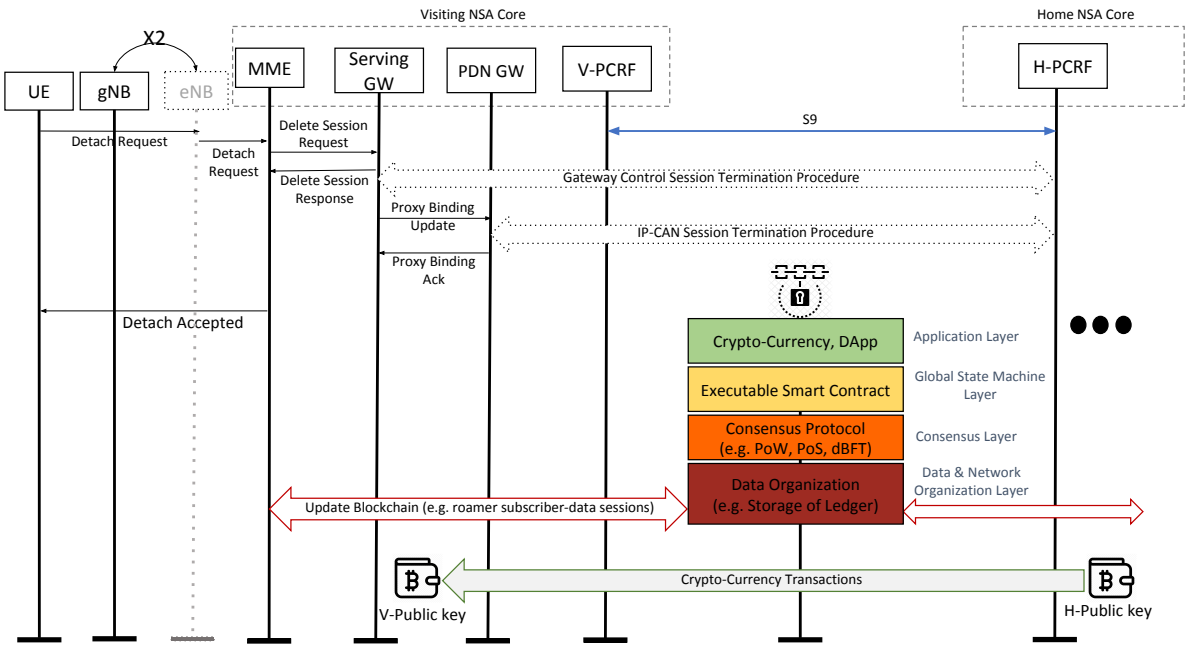


Fig. 3: Blockchain-enabled billing settlement for roaming in NSA core.

smart contract is responsible for specifying the charging rules and for triggering a payment from the H-MNO to the V-MNO according to the specific consensus mechanism used by the blockchain network. Such an approach completely removes the reliance on third parties (e.g. clearinghouses).

IV. Blockchain-based Roaming

This section focuses on 5G networks operating in non-standalone (NSA) mode. The reason behind such a choice lies in the fact that standalone (SA) operations are not expected to be deployed in the short to medium term due to their significantly higher capital and operational expenditures. We can expect that the 4G core network will co-exist alongside new 5G deployments for quite some time [13]. Billing information for roaming users is exchanged over the S9 interface interconnecting the policy and charging rules function (PCRF) of the home and visited MNOs. The UE attach procedure is initiated by the roaming user towards the mobility management entity (MME) of the visited operator and then the following procedures are executed: UE ID acquisition, authentication, location update, non-access stratum (NAS) security setup, and finally session establishment.

It is worth noting that the home subscriber server (HSS) of the home operator takes care of the authentication procedure, and that in LBO all the roaming services reside in the visited network which thus handles service control and data packet forwarding via the packet data network gateway (PGW) and serving gateway (SGW), respectively. When the attach procedure is completed, the visited operator offers the roaming user the services requested. As shown in Fig. 3, the control plane is passed between gNodeB (gNB) and evolved node-B (eNB) through the X2 interface in NSA architecture. This figure represents the detach procedure initiated by the UE. Upon receiving the detach request, the established packet data network (PDN) sessions are terminated and an accept message is sent to the UE. At this moment, the visited evolved packet core (EPC) pushes the session activities of the roaming user into the distributed ledger to activate and execute the smart contract. The content of a smart contract, with its predefined set of rules, is defined in advance by the mobile operators and provides them with the possibility of using token/cryptocurrency among them. Note how each and every transaction in the blockchain is validated by the other nodes of the blockchain network using the network consensus mechanism. The next section explains this procedure in detail.

V. Distributed billing settlements

The permissioned blockchain for roaming consists of several organizations that are, in fact, different MNOs. The 5G-cores (5GCs) that shape the participant nodes of the network are identified by their corresponding mobile network. All the cores have an internal copy of the ledger and are able to read and update it through an application. Furthermore, the contents of the smart contracts are defined and agreed by the consortium of the MNOs. [14].

A. System Model

At the system level, the system model of our blockchain network is composed of three layers with the top layer including different mobile operators which are communicating with the distributed ledger. The peers in the blockchain are the core networks of each of the service providers that have already agreed to have a common smart contract and a consensus on the content of the contract. Hence, all their cores have an instance of this mutual contract and will be able to read or

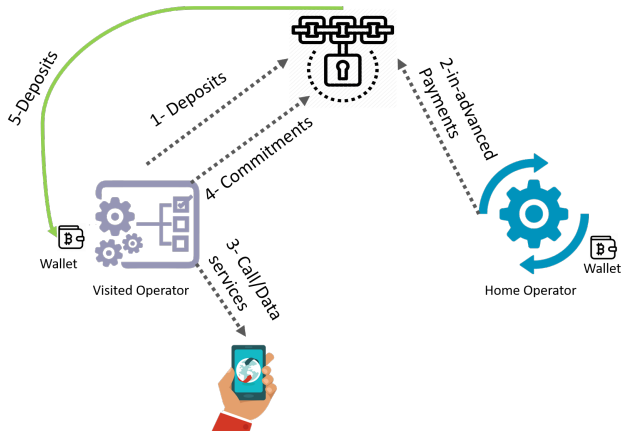


Fig. 4: Blockchain-based cellular service trading.

update the distributed ledger. The second layer includes any user or device that needs to be connected to the network and use roaming services because of their movements to areas not covered by their home network. These users can be connected vehicles, connected drones, or normal roaming users willing to use network services. Finally, the bottom layer of the model correspond to the transactions within the blockchain network that are performed when a new operator provides services to the users of other operators. We define the visited operator as a seller of service, and the home operator as a payer. As depicted in Fig. 4, when a roaming user connects to one of the core networks of the visited network, the latter will deposit a certain amount of crypto-currency in accordance with the content of the smart contract. The deposit is to assure the home operator that the required services will be provided to the user. In the second step, the home operator will pay the amount due in advance. Thirdly, the required services will be provided to the user and the roamer can be connected to the network and be able to make a new call or use data. When the user is disconnected, a commitment message will be sent to the blockchain informing all the peers and the smart contract about the consumption of the user and confirming the service fee, in the form of cryptocurrency. Finally, the smart contract will release the deposit paid and send it back to the wallet address of the visited operator.

B. Components

Our blockchain-based roaming architecture is designed using the permissioned blockchain framework Hyperledger Fabric [15]. As shown in [7], Hyperledger outperforms Ethereum in almost all evaluation metrics, including execution time, latency and throughput. It uses virtualized containers to host smart contracts and provides the functionality of confidential transactions in a trust-less environment without any central authority. This takes place via private channels between different actors (organizations) in the network, who privately agree on the terms of their interaction without going through a central authority.

The essential 5GC networks host replicas of the ledger and respectively allow their own or other applications to access the ledger (to query, read or update) via smart contracts. In addition, the applications connect to the 5GC and invoke smart contracts, which in turn create and submit transactions to the distributed ledger, when needed, and return events to the applications in question. Within a blockchain network, the presence of private channels allow a series of 5GCs and applications to communicate with each other. Moreover, these channels provide the possibility for different actors of the network to agree on the terms of their interaction privately and in a trust-less environment. Each of the members is identified by a unique certificate issued by a certificate authority (CA), which can be their own MNO. This also corresponds to the 5G roaming security model as defined in [10]. The channel membership service provider (MSP) validates the corresponding MNOs via this certificate when a 5GC connects to a channel, as shown in Fig. 5 (e.g. 5GC I-A and 5GC I-B with identities from CA-I). On the basis of this roaming blockchain network setup, the next section examines the initiation of transactions, the generation of blocks and consensus finalization.

C. Transactions and Consensus

When the procedure for detaching from the visited MNO is completed, the application generates a transaction proposal and pushes it to the cores in a channel. This is referred to as the detach transaction proposal (DTP) (see Fig. 5), which also contains the identity of the V-MNO (via the 5GC ID), the identity of the user and the H-MNO (via the authentication procedure), as well as the call duration/data usage, time and location of the service provided, and the value of the roamer's consumption. Following that, all of the 5GCs receiving the DTP run the smart contract independently and provide a response. After the 5GCs have checked these values, individual responses (DTP-Rs), including their digital signature and a signed payload (using their respective private keys), are created and sent back to the application. This "endorsement" step is typical of many blockchain frameworks and indicates the validation of a particular response from each operator's 5GC. The number of 5GCs having to endorse the new ledger entry is configurable via (predefined) policies. In our case, the two service providers, the V-MNO and the H-MNO, are sufficient for justification and consensus. Once confirmed, the smart contract activates a token/cryptocurrency transfer from the H-MNO to the V-MNO. All the transactions are lastly packaged in a block by the "Orderer" service and dispatched to all the nodes, which add it to the ledger.

D. Privacy Issues

Distributed ledger technology already combines several known functionalities from domains such as cryptography and distributed state machines. Different frameworks, flavors, and implementations additionally enhance the technology for specific needs. For example, using (different) channels from Hyperledger already establishes (different) distinct private groups to which other MNOs do not have access. This feature allows two or more operators to implement new smart contracts with different policies among themselves while still being in the same blockchain network with all the other operators. Additionally, since the preservation of privacy is

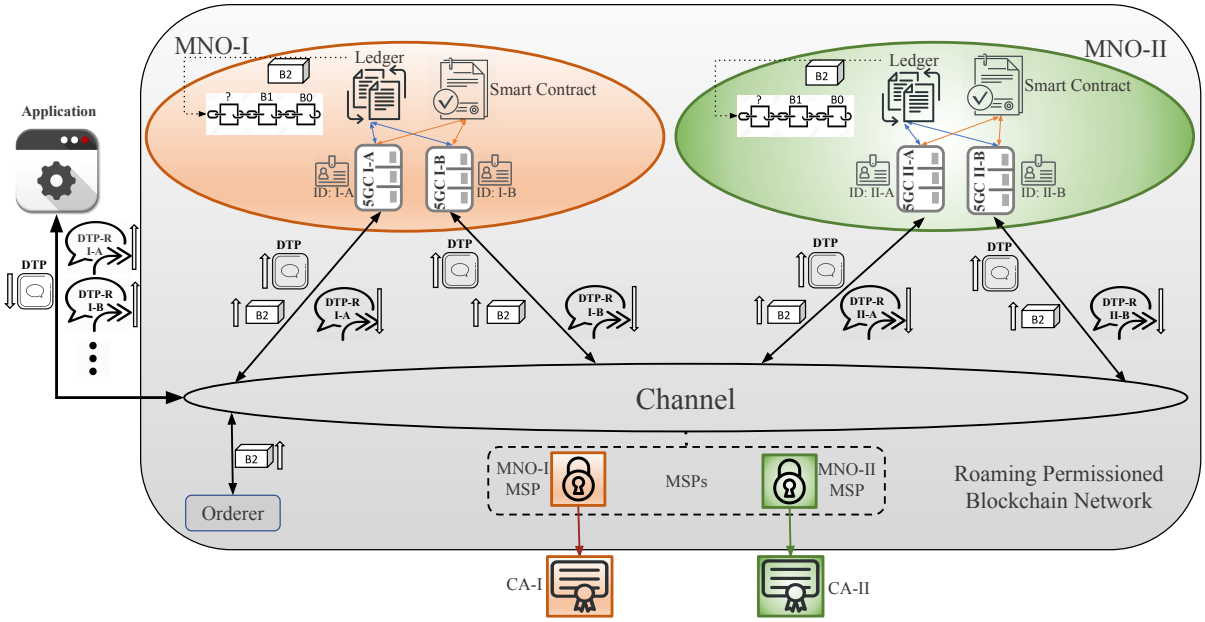


Fig. 5: Configuration of blockchain-based roaming.

a basic right and highly important, in our approach this can be hardened by leveraging the asymmetric key encryption scheme: confidential (e.g. personal) data can be encrypted with the public key of the home MNO (which also must be made available for other purposes anyway), and only the home MNO can decrypt it. With regards to additional parties such as the visited MNOs, several options are possible: a) the data can be encrypted (separately) with other public keys of the MNO(s), e.g. the public key of the currently visited MNO, so that the respective MNO(s) can decrypt it; b) multi-party private/public key scenarios also exist, for example a shared private key can be generated via the Diffie–Hellman key exchange for several MNOs, e.g. together with a roaming agreement; and c) additional mechanism directly between the visited and home MNOs to obtain the confidential data, e.g. additional transactions via the same blockchain (which may also be combined with further transactions), or this may be carried over already established inter-carrier collaboration systems (e.g. the interfaces via the IPX network and/or related GSMA databases).

Alternatively or additionally, with zero-knowledge proofs (ZKPs), yet another functionality of some DLT-frameworks can be used. According to the common simplified definition, ZKP is a method by which one party (the prover) can prove to another party (the verifier) that they know a value ”x”, without conveying any information apart from the fact that they know the value ”x”. Applied to privacy, this means that personal data does not have to be revealed directly to a third MNO, but the proof (that the personal data-set is known) is sufficient. Any third MNO can thus verify by itself whether this proof is valid or not, without having to know the real personal data. More substantial measures might totally exclude private data (completely, or at least unencrypted personal data) from being stored on the blockchain. Typically, a separate secure database can be used, and only the metadata, data hashes, ZKPs and/or pointers to the real data can be stored within the blockchain. This paradigm might be practical especially when larger amounts of data do not have to be on-chain. However, the questions of governance and access control of the off-chain database must then be addressed (e.g. such as mechanisms like rotating leaders and temporary access tokens).

VI. Conclusion and Discussions

Most mobile network operators are in the midst of technological transformation due to the introduction of heterogeneous and ultra-dense networks. Moreover, many enterprises have shown interest in using blockchain-based services due to the promise of cost reduction and higher efficiency. They cannot, however, use the public blockchain because of a lack of privacy, poor scalability, and low transaction throughput. In this regard, adding permissioned blockchain-based services to handle billing settlement in roaming offers mobile operators the chance to have an efficient system while decreasing the extra expenses in current roaming architecture.

In this article, we describe how MNOs, despite many benefits that LBO offers them, still prefer using the *home-routed* architecture to control and monitor their users even beyond their geographical coverage. Therefore, we propose a permissioned and smart-contract-based blockchain network to target the problem of a lack of trust between MNOs. By using the proposed architecture, the billing settlement is performed automatically via smart contracts. Moreover, thanks to the transparent nature of blockchain, mobile operators can ensure the accuracy of charging. This novel model uses the standard 3GPP interfaces that are used in roaming when a user attaches and detaches from a network, and has a minimum impact on

the core and radio access network of LTE/5G. Thus, it can be easily integrated with mobile operators.

Further applications beyond roaming can be enabled relying on the recently revealed concepts of DLT. For example, the network services offered by mobile operators can be synchronized and aligned, an approach already in dispute in the area of network slicing. Also, different service providers must guarantee a certain network quality and service level agreement (SLA), which are of crucial importance for autonomous and connected vehicles crossing national borders. Here, DLT can be applied as a slice broker, for cross-charging, and as a service management tool, which is thus the missing trust link between MNOs. Finally, mobile operators should investigate the potentials of blockchain in the long-term for revenue growth and new business opportunities. In future work, we intend to evaluate the performance of blockchain in roaming with multiple channels, and the presence of the overhead that is introduced by adding smart contracts to the 5G cores.

Acknowledgements

This work has been performed within the EU's H2020 projects 5G-CARMEN (825012), and 5G-ZORRO (871533) and funded through a collaborative program between the University of Bologna and the Fondazione Bruno Kessler.

References

[1] W. Yu, H. Xu, H. Zhang, D. Griffith, and N. Golmie, "Ultra-Dense Networks: Survey of State of the Art and Future Directions," in *proc. of ICCCN. Hawaii, USA*. IEEE, 2016.

[2] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "Distblocknet: A Distributed Blockchains-based Secure SDN architecture for IOT networks," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78–85, 2017.

[3] V. Sharma, I. You, F. Palmieri, D. N. K. Jayakody, and J. Li, "Secure and Energy-Efficient Handover in Fog Networks Using Blockchain-based DMM," *IEEE Communications Magazine*, vol. 56, pp. 22–31, 2018.

[4] A. Chaer, K. Salah, C. Lima, P. Ray, and T. Sheltami, "Blockchain for 5G: Opportunities and Challenges," in *Proc. of GLOBECOM. Waikoloa, HI, USA*. IEEE, 2019.

[5] B. Mafakheri, T. Subramanya, L. Goratti, and R. Riggio, "Blockchain-based Infrastructure Sharing in 5G Small Cell Networks," in *Proc. of IEEE CNSM. Rome, Italy*. IEEE, 2018.

[6] A. Refaey, K. Hammad, S. Magierowski, and E. Hossain, "A Blockchain Policy and Charging Control Framework for Roaming in Cellular Networks," *IEEE Network*, vol. 34, no. 3, pp. 170–177, 2019.

[7] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance Analysis of Private Blockchain Platforms in Varying Workloads," in *Proc. of ICCCN*. IEEE, 2017.

[8] P. A. Vanleeuwen and D. van de Ruit, "Blockchain-–Operator Opportunities. GSMA, Version1.0," Tech. Rep., 2018.

[9] "GSM Association Roaming Database, Structure and Updating Procedures. Version 9.1," Tech. Rep., 2013.

[10] "GSMA 5GS Roaming Guidelines. Version 2.0," Tech. Rep., May, 2020.

[11] LTE International Roaming Whitepaper. Access on August, 2020. [Online]. Available: http://carrier.huawei.com/en/technical-topics/core-network/lte-roaming-whitepaper

[12] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, pp. 22 328–22 370, 2019.

[13] 3GPP Release 15 Overview. Access on May, 2019. [Online]. Available: https://spectrum.ieee.org/telecom/wireless/3gpp-release-15-overview

[14] B. MAFAKHERI, "Centralized and Distributed Self-x Features in Heterogeneous 5G Networks," Ph.D. dissertation, Fondazione Bruno Kessler and University of Bologna, 2020.

[15] Y. Manevich, A. Barger, and Y. Tock, "Endorsement in Hyperledger Fabric via Service Discovery," *IBM Journal of Research and Development*, vol. 63, no. 2/3, pp. 2–1, 2019.

Babak Mafakhei received his Ph.D. degree from the University of Bologna in collaboration with the Fondazione Bruno Kessler (FBK) Research Center in Trento, Italy. Currently, he has been doing a Postdoc with the University of Bologna that is done with collaboration of the FEV Italia Srl. His research interests include coexistence in unlicensed bands, connected vehicles and blockchain technologies. He has served as a reviewer for journals such as IEEE TWC and IEEE Access.

Andreas Heider-Aviet has a leading role in the Deutsche Telekom 5G Program, with a focus on Traffic Infrastructure, Mobility and Autonomous Driving. He has filed several 5G DLT patents and initiated blockchain research and several DLT projects in cooperation with the Telekom Innovation Laboratories. Apart from this, he works on inter-MNO collaboration improvements in accordance with 5G-PPP and the EU. His interests comprise Multi-access Edge Computing, Multi-Operator scenarios and Identity Management. Prior to this, he held different technical and management positions in France in the Telecommunications domain.

Roberto Riggio is Senior Researcher in the Connected Intelligence Group at RISE AB in Stockholm, Sweden. He received his PhD from the University of Trento (Italy), after that he was postdoc at University of Florida, Researcher/Chief Scientist at CREATE-NET in Trento (Italy), Head of Unit at FBK in Trento (Italy), and Senior 5G Researcher at the i2CAT Foundation in Barcelona (Spain). Roberto Riggio has published more than 130 papers in internationally refereed journals and conferences. He has received several awards including the IEEE INFOCOM Best Demo Award (2013 and 2019) and the IEEE CNSM Best Paper Award (2015). He is a member of the ACM and a Senior Member of the IEEE.

Leonardo Goratti received his Ph.D. degree from the University of Oulu and his MSc from the University of Firenze (Italy). He is currently a Senior System Engineer at Safran Passenger Innovations, Germany. His interests include SDN and NFV for 5G, LTE-Advanced and millimeter wave communications. He has authored more than 70 research papers in journals and conferences. He is a TPC member in international conferences, and serves as reviewer for journals such as IEEE JSAC and IEEE Communications Magazine.