Blockchain Based RAN Data Sharing

[*]Andreas Heider-Aviet, Danny Roswin Ollik
[**†]Stefano Berlato, [**§]Silvio Ranise, [**]Roberto Carbone
[***]Van Thanh Le, Nabil El Ioini, Claus Pahl, Hamid R. Barzegar
[*]*Deutsche Telekom, Berlin, Germany*
[**]*Fondazione Bruno Kessler, Trento, Italy*
[†]*DIBRIS, University of Genoa, Genoa, Italy*
[§]*Department of Mathematics, University of Trento, Trento, Italy*
[***]*Free University of Bozen-Bolzano, Bolzano, Italy*
name.surname@{@t-systems.com, @fbk.eu, @unibz.it}

***Abstract*—Providing seamless connectivity and services across national borders are intricate challenges with multifarious underlying aspects, ranging from the network management to business and political considerations. Since the cross-border inter-Public Land Mobile Network (PLMN) network handover is currently not available in European cellular networks, we present a complementary approach, diminishing the connectivity gap to a minimum. By leveraging Distributed Ledger Technology (DLT), we establish a dynamic, secure data exchange and management solution between several Mobile Network Operators (MNOs) of different countries. Systematically integrating foreign cell and base station parameter (i.e., Radio Access Network (RAN) data) of border regions into the internal network management systems permits their usage in standardized Mobility Management procedures. We demonstrate that this type of collaboration on the inter-MNO network governance considerably improves the network quality and customer experience when crossing national borders. Since foreign RAN data is also required for the inter-PLMN network handover (and can serve many additional purposes) and provided that our solution is not relying on any specific mobile network technology generation (e.g., 4G or 5G), we conclude that it is a fundamental step towards an inter-MNO ecosystem beyond 5G.**

***Index Terms*—Blockchain, RAN, DLT, 5G, Cross-border, Inter-PLMN network handover, Security, Access Control**

I. Introduction

In Europe a large number of Mobile Network Operators (MNOs) have to efficiently collaborate in order to provide digital services seamlessly. This is especially important when services have to be provided across several countries and “while crossing a national border”, which means across different Public Land Mobile Networks (PLMNs) of different MNOs. In the 5G context, the need for inter-MNO collaboration to ensure connectivity and service continuity across borders is emphasized in the European Union (EU) Horizon 2020 program, where several projects are currently researching and implementing 5G pilots for cross-border Cooperative, Connected and Automated Mobility (CCAM) services[1]. The call for ”cross-border corridors” has also been prioritized in a ”State of the Union” press release [1] and integrated into the European ”Connecting Europe Facility (CEF2)” Digital programme [2].

A practical example is the Multi-access Edge Computing (MEC)-based Cooperative Lane Merge service. This CCAM service aims at managing the gaps and maneuvers between vehicles safely and efficiently, although requiring a frequent exchange of information (e.g., speed, position, intents). Therefore, too much delay in communication may lead to inconsistencies, with a potential impact on users’ safety. As a result, the lack of service continuity slows down the overall (cross-border) adoption of new services and automated driving.

Although the cross-border inter-PLMN network handover is technically defined in Third Generation Partnership Project (3GPP) [3], for practical implementation and usage, further considerations are needed. This is foremost related to the fact that the network management and operations of MNOs are based on each country’s national territory and jurisdictions. As a consequence, it restricts the availability and sharing of network governance data among MNOs of different countries, which has already been highlighted in [4].

To better understand the situation, we need to point out that the inter-PLMN network handover requires inter-MNO Core Network Interfaces, which are normally implemented over Internetwork Packet Exchange (IPX) networks [3], [5]. However, specific challenges in the areas of security, latency, robustness, as well as respective processes and relations between MNOs and IPX-provider, and nevertheless indirectly related legal and political issues are known and in discussion[2] [3] [6]. Until now, to the best of our knowledge, there is no cross-border implementation of the additionally required interfaces (beyond basic interfaces for roaming) anywhere in Europe in public mobile networks.

Independently, all respective local radio cell (and base station) parameters of foreign MNOs near the border need to be taken into account in order to successfully hand over users, devices and services to another PLMN. Concerning the Ra-

Identify applicable funding agency here. If none, delete this.

[1] See https://5gcroco.eu/, https://www.5g-mobix.com/, and https://5gcarmen.eu/, respectively

[2] https://www.gsma.com/security/resources/ir-77-interoperator-ip-backbone-security-req-for-service-and-inter-operator-ip-backbone-providers-v5-0/

[3] https://interactive.itwglf.com/ITW-Global-Leaders-Forum/iot-1653ZN-152022V.html

dio Access Network (RAN), Automatic Neighbour Relations (ANR) [4] is often named as a solution, but in practice, it does not provide all information to entirely manage foreign cells - and thus inter-PLMN network handovers. This is mostly due to the missing cross-border inter-MNO Interfaces (e.g. X2 for 4G, Xn for 5G), different Radio Access Technologies (RATs) used by different MNOs on different sides of the border(s), and the proprietary network management (systems) of each MNO. These Operations Support Systems (OSS) have to manage several network generations and varying technological implementations (e.g., from different network equipment vendors) in parallel, and, above all, their historic focus is only one (national) cellular network. The optimization of cell neighbor relations has been addressed in scientific work—examples are [7], [8] and [9]—but, to the extent of our knowledge, not in a multi-PLMN, multi-country cross-border setup and/or they require the X2/Xn interface. Additionally, neighbor cells are usually detected via User Equipments (UEs) measurement reports, based on scans of predefined frequencies. However, foreign PLMNs are not considered because of limited measurement capacities and unknown foreign frequencies. The inevitable need is more data about foreign networks, e.g., including also the base stations and cell locations, antenna and radio signal threshold parameter, or other operational and business-related information, in order to assure a seamless handover.

Therefore, the requirement for a deeper inter-MNO collaboration concerning the network governance is the basis of our presented solution. We focus on new possibilities for a regulated, secure and dynamic (RAN) data management among multiple MNOs by leveraging recent advances in Distributed Ledger Technology (DLT). Our demonstration focuses on improving the current cross-border situation (speeding up the network re-selection), based only on RAN data sharing and standard 3GPP procedures.

The structure of the paper is as follows. Section II is about related worked in (national) RAN sharing and inter-MNO DLT activities. The reference scenario is described in the Section III with a brief description of the Ran Data Sharing model, its assumptions and requirements. Section IV presents the model architecture, while we illustrate our implementation in Section V. Based on quantitative and qualitative evaluations, we argue that the proposed approach is promising in terms of efficiency and security in Section VI. The conclusion and possible future work are described in section VII.

II. Related work

Sharing the physical RAN infrastructure among MNOs and other (e.g. tower) companies operating in the same national perimeter is becoming convenient in several countries, mainly to optimize the network coverage (connectivity) in rural areas. However, the implied RAN data sharing at the national level has by far less non-technical constraints. Therefore, below we focus on a solution allowing dynamic and secure network data exchange (and management) internationally among several MNOs.

In this context, we highlight that centralized legacy systems already exist. For instance, the RAEX IR.21 Roaming Database[5] is operated by the Global System for Mobile Communications (GSMA) to share fixed network data (e.g. for IPX networks and international roaming). However, these kinds of solutions were designed for rather static and global network infrastructure data (not RAN parameter). As such, they are inappropriate for a dynamic cross-border scenario with complex relationships among multiple parties. RAN data sharing could also be carried out through independent bilateral confidential agreements among pairs of MNOs. However, the non-scalability of this approach would bring additional complexity for MNOs, as they would have to manage multiple relationships with different parties without the convenience of a common system. Moreover, we highlight that some RAN data should nevertheless be aligned among all MNOs in a given geographic area to avoid, e.g., radio interferences, which are a major cause of service degradation.

Distributed databases and DLT infrastructure are auspicious as technical frameworks for international collaboration. There are different consortium-based approaches, e.g., in the area of inter-MNO roaming charging reconciliation, which is closely linked to [10] where several MNOs propose an architecture integrating DLT for roaming agreements. The GSMA illustrates further opportunities for adoting blockchain technology in the telecommunication domain in [11].

Another application of DLT is the mitigation of roaming fraud, for example by SIM cloning. The authors in [12] propose a blockchain-based roaming management system for MNOs and mobile subscribers, automated via smart contracts. The authors choose a Proof-of-Stake (PoS) consensus mechanism to incentivize users to participate in the network. It is important to highlight that the authors operate in a different geographical context (i.e., Asia and Oceania) in which users are supposed to pay for roaming services. This is a fundamental assumption for their use case, as in the European Union users do not pay for roaming services. Furthermore, their system is open to both MNOs and users (i.e., public blockchain).

High-level operational roaming aspects are also made available in "Blockchain for Telecom Roaming" [6], whereas on the network infrastructure side DLT supports Software Defined Network (SDN) in [13] by building upon Blockchain as a security gate for Internet of Things (IoT) devices towards the cellular network and internet. Similarly in [14], a Blockchain is built on top of a SDN controller to manage request flows of users, and [15] proposed to upgrade the traditional Home Subscriber Server (HSS) to a distributed DLT-based version. At the application level in this scenario, Le et al [16] applied DLT to authenticate user when reconnecting to the network, whereas a smart contract decides which suitable services will

[4] https://www.etsi.org/deliver/etsi_ts/132500_132599/132511/15.00.00_60/ts_132511v150000p.pdf/

[5] https://www.gsma.com/security/resources/ir-21-gsm-association-roaming-database-structure-and-updating-procedures-v12-0/

[6] https://github.com/IBM/Blockchain_for_TelcoRoaming

be deployed for this user based on their historical requests. Barzegar el al. [17] provide a comprehensive view about this layer and include the possibility combine it with Artificial Intelligence (AI). We observe that blockchain technology can strengthen the network at different layers and has great potential to automate related telecommunication processes.

Complementary to our work, [18] also describes the shortcomings of the current situation and evokes the need for inter-MNO RAN data sharing. The 5G-ZORRO[7] European project focuses on the contracting and exchange of (information about) abstract resources, e.g., access, core-network, MEC, among MNOs, in a scenario where an MNO has to provide a service to a customer but does not possess all necessary resources. However, the non-technical cross-border aspects, as well as inherited security (e.g. lawful intercept) and data protection constraints in a complex cross-country, cross-industry context remain a challenge.

III. Reference Scenario

Our scenario considers geographical cross-border areas in which two or more MNOs in different countries operate at least one network cell; we refer to these regions as “interaction areas” (see Figure 1). In this context, we assume the presence of a UE, e.g., a vehicle connected to the cellular network, travelling from one country to the other (e.g., from Italy to Austria) passing through an interaction area (e.g., the Brenner highway between Italy and Austria). Crossing a national border naturally leads to a loss of connectivity (no inter-PLMN handover, as explained in Section I), where the UE is detached from the Home PLMN (HPLMN) (e.g., Telecom Italia, also known as TIM) and scans radio frequencies to re-select a suitable network (e.g., Magenta Austria, also known as Magenta). Currently, the network re-selection procedure often lasts several minutes[8] [19], an unacceptable delay in use cases with stringent latency requirements. For instance, a delay in communication may seriously affect the provision of services and the overall safety in CCAM use cases, such as the Cooperative Lane Merge service already mentioned in Section I.

Without the inter-PLMN handover, the most pragmatic way to minimize the connectivity loss and accelerate the network re-selection procedure is to identify in advance a foreign neighbor cell to which the UE can be redirected while using standard 3GPP RAN procedures [3]. We make use of the ”Release-with-Redirect” procedure, which indicates the (foreign) cell parameters directly to the UE. These configuration parameters are generally referred to as RAN data and need to be known beforehand. The RAN configuration is typically updated on a daily basis (depending on the MNOs and their respective OSS) and contains both non-critical (public) information as well as confidential (private) information, the latter being usually kept inside individual MNO perimeters. To allow cross-border cell neighbor relations, MNOs have to selectively share (part of) its cell configuration with foreign partners, which in turn have to configure their preferred cell neighbors accordingly (especially along a transportation corridor), and vice versa.

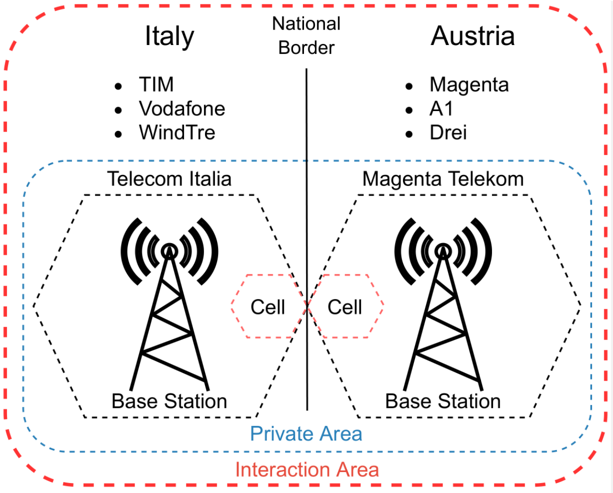


Fig. 1. RAN Data Sharing Example Scenario

We refer to the communication channel between these two (or more) MNOs as a “private area”. We point out that, while the private RAN data is *not* personal, it still is strategically important for providing a superior network coverage and quality. For this reason, the sharing of network-related information among competitors is regarded as a sensitive topic. Moreover, the choice of roaming partners may also be influenced by business strategies and commercial agreements among MNOs, which are out of the scope of this paper (however, these contractual and process aspects may also be integrated into our DLT framework).

Below we describe the model for RAN data sharing (Section III-A) and then formulate scenario assumptions along with functional and security requirements (Section III-B).

A. RAN Data Sharing Model

Although other parameters may be included, for the sake of simplicity we present in Figure 2 only the essential network re-selection parameters in the RAN data sharing model. A mobile network cell is uniquely denoted with a Cell Global Identifier (CGI) [20] and the general RAT, i.e., the underlying technology and connection method of the cell (e.g., 4G and 5G). Together, the CGI and the RAT of a cell represent the public RAN data to be shared between all MNOs in a given interaction area. Besides, a network cell is configured with technical parameters which constitute the private RAN data to share only with the chosen roaming partners within a private area:

- *Physical Cell Identifier (PCI)*: the MNO-defined identifier of a network cell in the physical layer. The number ranges from 0 to 504 and is defined per PLMN (i.e., the PCI is not a global identifier);

[7] https://www.5gzorro.eu/

[8] https://www.ericsson.com/en/blog/2019/5/connected-vehicle-cross-border-service-coverage

TABLE I
SCENARIO ASSUMPTIONS

Assumption	Description
$A1$	Only MNOs operating in European countries are involved
$A2$	RAN data are not personal, i.e., the European GDPR[10] is not applicable
$A3$	There are no significant latency requirements for the sharing of RAN data
$A4$	MNOs are curious of other MNOs' RAN data to which they (normally) do not have access to
$A5$	MNOs will faithfully notify each other about any updates and share them accordingly
$A6$	MNOs do not abuse the system (e.g., with useless requests or wrong RAN data)

TABLE II
SCENARIO FUNCTIONAL AND SECURITY REQUIREMENTS

Requirement	Description
$FR1$	The solution shall not allow outdated RAN data, but instead represent an always up-to-date inter-MNO reference system
$FR2$	The solution shall not interfere with any underlying standard procedure (e.g., 3GPP network handover [21]) or legacy system
$FR3$	The solution shall be able to accommodate future use cases (e.g., integration of roaming agreements, dynamic radio spectrum management, integration of 3rd parties)
$SR1$	The solution shall allow only previously authenticated and authorized parties to participate
$SR2$	The solution shall allow the public data of a cell deployed in a given interaction area to be visible to all MNOs operating in that interaction area only
$SR3$	The solution shall allow MNOs to selectively share private RAN data with MNOs in a private area to allow identifying neighbor cells
$SR4$	The solution shall guarantee the integrity and availability of RAN data, along with the accountability of updates to solve errors and potential disputes
$SR5$	The solution shall be able to differentiate AC rights (e.g., create, read, write, validate) depending on different roles (e.g., admin, technical, commercial, auditors)

- *DownLink Evolved-UTRA Absolute Radio Frequency Channel Number (DL_EARFCN)*: the identifier for the band and carrier frequency in 4G networks. We use this denomination since most current live networks are based on 4G; the identifier for 5G would be NR-ARFCN [9].

Moreover, we define a relationship (i.e., neighbor cell) identifying the (CGI of the) target cell for a given source cell to perform the fast network re-selection. A MNO is denoted with a name, an identifier and a PLMN-ID as public data, whereas the lists of cells and digital certificates (denote with "[]") are confidential. MNOs belonging to the same group may have similar names in different countries, but they are legally and operationally separated entities. Finally, an interaction area is defined by a name along with the list of involved countries and private areas (a more detailed geographical definition of the border zones is not relevant for our demonstration purposes. Logically, however, the interaction area(s) should correspond to real country borders and can be predefined). Similarly, a private area is characterized by a name, the interaction area to which it belongs and the list of involved MNOs.

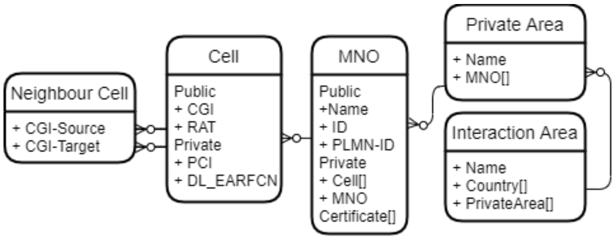


Fig. 2. Essential RAN Data Sharing Model

B. Scenario Assumptions

From the reference scenario, we can formulate six assumptions (A) which we report in Table I. $A1$ and $A2$ are directly inferred from the reference scenario. $A3$ is motivated by the fact that RAN data sharing happens independently and before any network re-selection procedure, which is instead the time-sensitive procedure and managed purely between the RAN, Core Network and the UE. Then, $A4$ is an elemental assumption derived from the strategic and practical importance of confidential RAN data. Finally, $A5$ and $A6$ are reasonable when considering that the best results are achieved when every MNO collaborates. We recall the example of the UE travelling from Italy to Austria via the Brenner cross-border highway. TIM can provide the fast network re-selection towards Magenta only if the latter previously shared its cells parameters with TIM. If Magenta does not provide its data, TIM has to choose another roaming partner, resulting in a financial impact for Magenta (depending on the contracts). The same would happen if Magenta provides—either willingly or by mistake—wrong data: the fast network re-selection procedure would fail. Since the overall success of the system is determined by the minimized network interruptions (at the respective borders, with the participating MNOs, and for each data session of each customer), analyzing network traces quickly reveals potentially dishonest participants. In our example, TIM would consequently adapt its own RAN configuration to use another roaming partner, or even apply a more fine-granular filtering (e.g. International Mobile Subscriber Identity (IMSI)-based) to provide the fast re-selection only to customers of fair playing MNOs. Nonetheless, we estimate there is only low interest/benefit for malicious actors in this use case context, it's rather a win-win situation for participating MNOs and their customers.

Moreover, we formulate 3 functional (FR) and 5 security (SR) requirements on the RAN data sharing solution which we report in Table II. $FR1$ is a basic functional requirement directly inferred from the reference scenario to ensure the effectiveness of the RAN data sharing solution. $FR2$ minimizes any additional complexity to make the solution

[9] https://www.etsi.org/deliver/etsi_ts/138100_138199/13810102/15.02.00_60/ts_13810102v150200p.pdf

seamlessly applicable, while *FR3* guarantees the possibility to extend the solution with regards to similar inter-MNO challenges. Regarding security requirements, *SR1* restricts the sharing of RAN data to authenticated and authorized MNOs (and potential 3rd parties like European supervisory agencies) only, thus blocking external parties from accessing sensitive data. *SR2* and *SR3* are directly inferred from the reference scenario, while *SR4* considers basic security properties which are desirable in any data sharing solution. Finally, *SR5* takes into account organizational and process aspects, allowing to differentiate AC rights depending on the (role of the) user of each MNO.

IV. RAN Data Sharing Architecture

In this section we propose a DLT-based RAN data sharing architecture, which permits to develop a distributed non-federated network among all participating MNOs. Figure 3 illustrates the general architecture of our solution. The RAN data sharing system is composed of three layers *i)* privacy preserving layer, *ii)* user access layer, and *iii)* platform layer.

A. Privacy Mechanism

Empowering MNOs with the capability of selectively sharing RAN data with each other at different levels of granularity is at the heart of our architecture. Based on the requirements in Table II, we have identified two potential mechanisms, namely i) full isolation, and ii) data isolation.

The first mechanism consists of providing a fully private subnet, where only the involved MNOs can interact. The advantage of this approach is the ability to create an independent overlay network on top of the existing network. Nevertheless, this adds a management overhead as the number of subnets increases (for example, with 100 organizations and each pair needs a private subnet, the governance becomes utterly complex to manage). Data isolation on the other hand refers to using one single network while the transactions are only visible to the participants with the corresponding access level. This dramatically reduces the overhead of the subsets and eases the application of the same business logic across the network.

B. User Access Right

User access rights layer is used to authenticate all the participants in the network and to manage the access to the shared data. In our architecture three roles have been set:

- MNO Admin: Has a full control over all data of one single MNO, including private data, private area(s), cell data and cell neighbor(s).
- MNO Users: Can not update or create private area(s), but can manage cells and cell neighbors of the MNO.
- MNO Guests: Can read MNO data if the access right has previously been attributed by an MNO Admin.

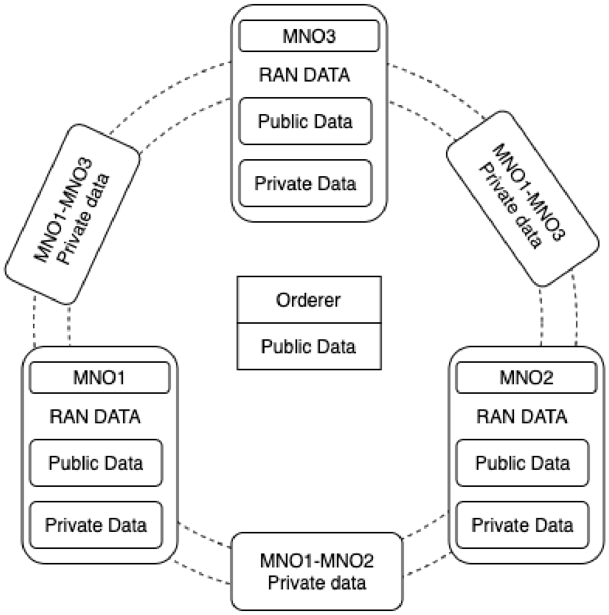


Fig. 3. RAN data sharing general architecture.

C. Platform

The above layers rely on a platform to manage the underlying network, transactions between MNOs, store the data, and execute the data sharing logic.

In the proposed architecture, we need a framework capable of satisfying the requirements in Table II under the assumptions in Table I to be able to implement the reference scenario described in Section III. In particular, the platform of choice needs to provide the ability to manage multiple organizations and provide different data access levels to all the participants. Since the context is domain specific, we consider a permissioned blockchain as a best fit. Although at the beginning our MNOs are known a priori, we need a flexible platform that allows the introduction of new MNOs as well as a configurable mechanism to define the adherence requirements (e.g., the number of existing MNOs who need to agree to add the new MNO).

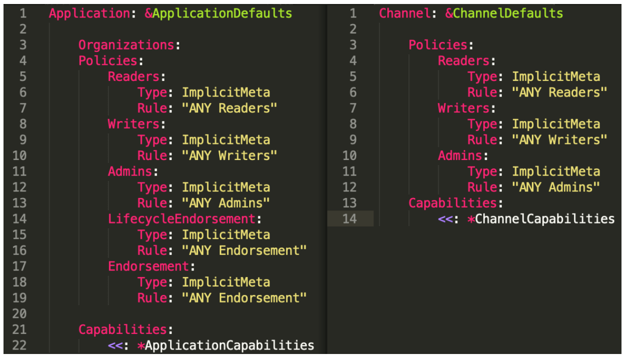
Additionally, since only part of the RAN data needs to be kept private, we opted for the data isolation option (see Figure 3). However, our solution can fully support the first option in the event of strict isolation requirements (e.g. for use cases where sensitive customer data or critical infrastructure is involved).

V. Implementation

Given all the properties in terms of performance, security and privacy, we developed a proof of concept implementation in Hyperledger Fabric, which also allows to evaluate the feasibility, robustness and resiliency of our architecture. Fabric is an open-source, permissioned blockchain platform featuring smart contracts (Chaincode) to implement business logic. Fabric provides channels, AC lists and private data collections to manage controlled access and enable privacy among the network participants. It supports a modular and extendable architecture which allows the integration of different components to perform specific tasks.

A. General configuration

In our implementation, we used Fabric version 2.2, with five organizations (MNOs), each with a Certification Authority (CA) and one ordering server to create and deliver the blocks. To manage access rights, Fabric uses AC lists and policies configurable at channel level, thus giving fine granular possibilities. To simplify the network model, we configured the AC list to allow all participating MNOs (admins) to update the smart contracts and the communication channel, which means that any new organization wanting to join into the channel only needs the acceptance from one organization inside the channel (see Figure 4).



```
Application: &ApplicationDefaults

    Organizations:
    Policies:
        Readers:
            Type: ImplicitMeta
            Rule: "ANY Readers"
        Writers:
            Type: ImplicitMeta
            Rule: "ANY Writers"
        Admins:
            Type: ImplicitMeta
            Rule: "ANY Admins"
        LifecycleEndorsement:
            Type: ImplicitMeta
            Rule: "ANY Endorsement"
        Endorsement:
            Type: ImplicitMeta
            Rule: "ANY Endorsement"

    Capabilities:
        <<: *ApplicationCapabilities
```

```
Channel: &ChannelDefaults

    Policies:
        Readers:
            Type: ImplicitMeta
            Rule: "ANY Readers"
        Writers:
            Type: ImplicitMeta
            Rule: "ANY Writers"
        Admins:
            Type: ImplicitMeta
            Rule: "ANY Admins"
    Capabilities:
        <<: *ChannelCapabilities
```

Fig. 4. ACL Configuration

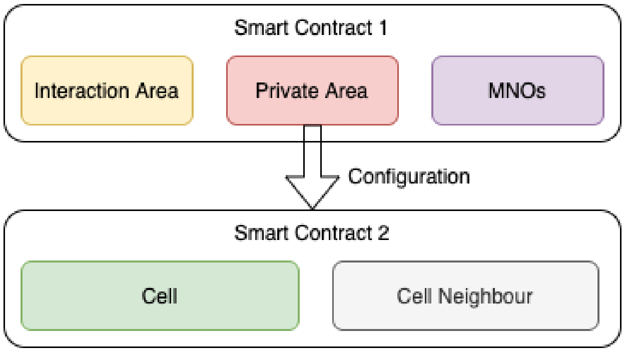
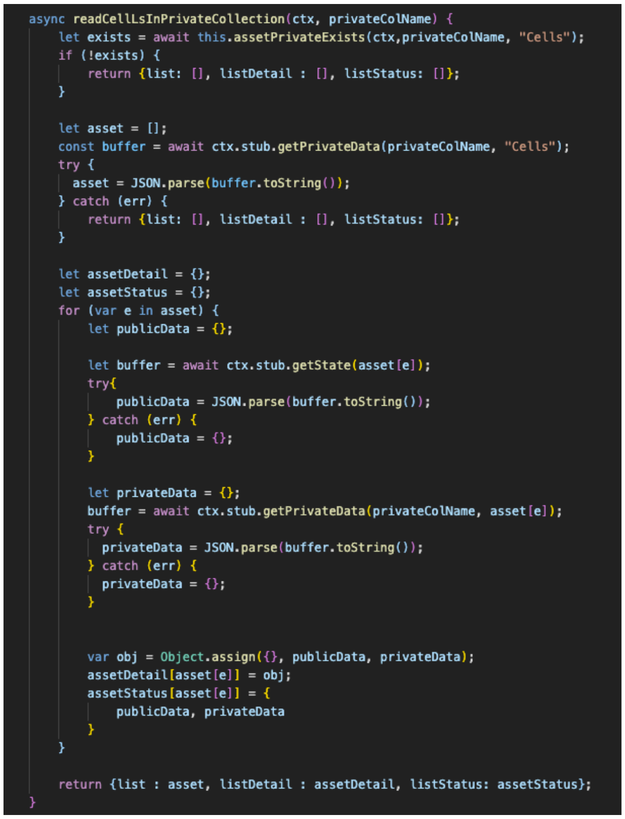


Fig. 5. Ran Sharing Model Configuration

B. Smart Contracts

Fabric handles RAN data validation, storage and sharing using dedicated smart contracts. A smart contract is composed of a set of data structures representing the data MNOs agree to share, as well as the sharing logic. Additionally, it contains a set of functions acting on the data, such as data validation (e.g., the data format), and a set of emitted events to trigger external business logic. Figure 6 depicts an example of a smart contract function for reading cell data from a private data collection. In our implementation the smart contracts manage the data sharing process among all the MNOs. The public data is distributed among all the nodes of the channel, while the private data is only stored in the involved MNO nodes.

To reduce the complexity of the smart contracts' logic, we have created two separate smart contracts, the first one for public entities such as Interaction Area, Private Area, and MNO public information (smart contract 1), and the second for the Cell and Cell Neighbors. The private collection configuration management can be taken from the Private Area data (smart contract 2). If the MNOs need to update their configuration of smart contract 2, they take the private collection configuration from the smart contract 1 and then send it to smart contract 2 (see Figure 5). When MNOs want to create a new private area, they need to update the database of both smart contracts. By separating it into independent smart contracts, we can be sure that all MNOs can read the latest private configuration from the public smart contract in order reconfigure their private one, thus preventing any out-of-date configuration problem in the private data sharing.



```
async readCellLsInPrivateCollection(ctx, privateColName) {
    let exists = await this.assetPrivateExists(ctx,privateColName, "Cells");
    if (!exists) {
        return {list: [], listDetail : [], listStatus: []};
    }

    let asset = [];
    const buffer = await ctx.stub.getPrivateData(privateColName, "Cells");
    try {
      asset = JSON.parse(buffer.toString());
    } catch (err) {
        return {list: [], listDetail : [], listStatus: []};
    }

    let assetDetail = {};
    let assetStatus = {};
    for (var e in asset) {
        let publicData = {};

        let buffer = await ctx.stub.getState(asset[e]);
        try{
            publicData = JSON.parse(buffer.toString());
        } catch (err) {
            publicData = {};
        }

        let privateData = {};
        buffer = await ctx.stub.getPrivateData(privateColName, asset[e]);
        try {
          privateData = JSON.parse(buffer.toString());
        } catch (err) {
          privateData = {};
        }


        var obj = Object.assign({}, publicData, privateData);
        assetDetail[asset[e]] = obj;
        assetStatus[asset[e]] = {
            publicData, privateData
        }
    }

    return {list : asset, listDetail : assetDetail, listStatus: assetStatus};
}
```

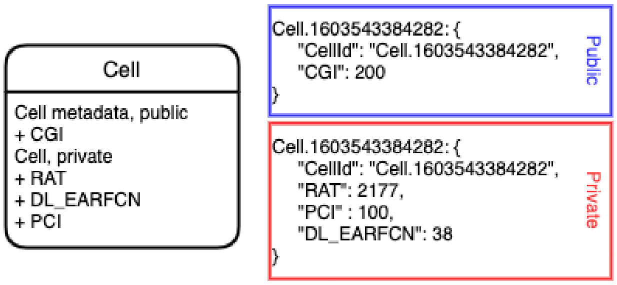
Fig. 6. Reading cell data in smart contract

C. Data modeling and Private Collection

Figure 2 shows a relational schema for RAN data sharing with a list of objects. The data provided by every single MNO is converted to the JSON format with key-value pairs and stored in CouchDB as a state database[11]. To integrate public

[11] https://hyperledger-fabric.readthedocs.io/en/release-2.2/couchdb_tutorial.html

and private data, using a cell as an example, the cell data will be broken down into two JSON objects, one stored inside a public storage and the other in a private storage. We deployed smart contract functions to work directly with JSON objects, including the verification process. The solution will facilitate flexible storage means, allowing all values to be set as public or private dynamically. More parameters for an object are also possible, without re-deploying the smart contract in the future (Figure 7 illustrates an example).

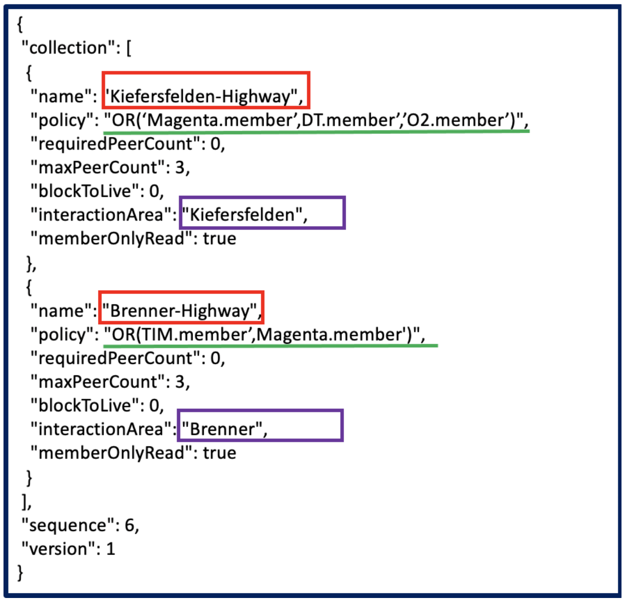


```
Cell.1603543384282: {
    "CellId": "Cell.1603543384282",
    "CGI": 200
}
```

```
Cell.1603543384282: {
    "CellId": "Cell.1603543384282",
    "RAT": 2177,
    "PCI" : 100,
    "DL_EARFCN": 38
}
```

Fig. 7. Data Storage Example

The private collection configuration example is presented in Figure 8, where all objects of smart contract 1 can be built with a single JSON object of the configuration. The purple rectangle is the interaction area, the red one is the private area and the green lines show a list of the participants MNOs .



```
{
 "collection": [
  {
   "name": 'Kiefersfelden-Highway",
   "policy": "OR(‘Magenta.member’,DT.member’,’O2.member’)",
   "requiredPeerCount": 0,
   "maxPeerCount": 3,
   "blockToLive": 0,
   "interactionArea":"Kiefersfelden",
   "memberOnlyRead": true
  },
  {
   "name":"Brenner-Highway",
   "policy": "OR(TIM.member’,Magenta.member’)",
   "requiredPeerCount": 0,
   "maxPeerCount": 3,
   "blockToLive": 0,
   "interactionArea":"Brenner",
   "memberOnlyRead": true
  }
 ],
 "sequence": 6,
 "version": 1
}
```

Fig. 8. Private Configuration Example

D. *Experimental Setting*

The entire system is deployed into five Virtual Machines (VMs) in a cloud cluster. Each VM represents one MNO, with 4GB RAM, 16G disk space and 1 CPU core. Two VMs are respectively connected to a test telecommunication network environment for the inter-PLMN network re-selection. They contain two independent 4G mobile networks where both Core Networks are connected respectively to independent 4G cells of different frequencies. The HPLMN has DL_EARFCN 3750 and PCI 360. The Visited PLMN (VPLMN) has DL_EARFCN 1300 and PCI 147. The test device (UE) is a Samsung Galaxy S9, configured to use all Radio Access Technologies to reflect live network scenarios. Both networks only have the basic interfaces for roaming. The SIM card has the VPLMN defined as equivalent PLMN. We must note that otherwise - as long as the HPLMN is still detectable - the redirection won't be accepted.

The radio signals are emitted inside a shielded box, whereas a USB interface connects the devices inside to the outside world. During the test, the UE is first connected to the HPLMN while the VPLMN cell is also available. The mobility procedure is started by continuously degrading the signal strength of the HPLMN cell until predefined thresholds automatically initiate a ”Release-with-Redirect” procedure (pointing to the target cell and frequency): The UE starts to pick the indicated alternative cell (first measure point), upon selection of the suitable cell a tracking area update is sent to the network (second measure point), and rejected (due to missing inter-MNO Core Network interfaces), but the following attach to the VPLMN message is accepted.

VI. Evaluation

Concerning the overall network setup, all measured durations are related to the synthetic setup with a limited number of Radio Access Technologies and frequencies. In reality, with more MNOs operating in parallel at the concerned locations, more PLMNs and frequencies are in use. Beyond this, the physical topology and especially location-specific obstacles have a considerable impact on the network coverage and received cell signal strength - despite best possible cell locations and antenna configurations. The following paragraph describes the cellular network related test proceeding and results. Afterwards we discuss the requirements and finally we consider the wider European context.

A. *Cellular network laboratory results*

In a setup without RAN data sharing, the HPLMN does not have any information about potential target cell. The UE scans all frequencies, and picks the VPLMN cell after 60s. An essential part of the improvement is the equivalent PLMN configuration, which requires the knowledge of (all potential) target PLMNs and their configuration in the HPLMN. The network outage can be reduced to 6 seconds on average. With additionally a connection to the DLT platform and the configuration of cell neighbor relations, the UE reconnects to the new PLMN within 0,5s on average, a gap which can easily be coped with on the application levels.

B. *Requirement evaluations*

The core mechanism of Fabric (and of DLTs frameworks in general) guarantees up-to-date transactions among participant nodes. Moreover, as described in Section V-A, we split the

TABLE III
INFORMATION FROM REAL ENVIRONMENT.

Name	Value
Number of Countries	25 (except Malta, Cyprus) [12]
Number of MNOs	47 [13]
Interior borders (only Shengen area)	34 [14]
Number of MNOs per country (average)	3
Number of borders per country (average)	4
Avg network update propagation (impacting other MNOs) per hour	(3 x 4 x 25)/24h = 12.5
Avg num of base stations per MNOs/a border area	200 (estimated/confidential conversations with MNOs involved in 5G-Carmen)
Avg num of cells impacted by daily updates	60 (estimated/confidential conversations with MNOs involved in 5G-Carmen)
Total updates per hour	60 x 12.5 = 750 updates

RAN data model (Figure 2) into two smart contracts for public and private data, respectively. This approach solves the out-of-date blockchain problem for private data sharing even in the presence of multiple RAN data update sources (*FR1*). Moreover, the RAN data sharing solution complements the 3GPP network handover [21] by providing means to identify in advance a suitable neighbor cell while being agnostic in respect to the underlying network infrastructure (*FR2*). Besides, the use of smart contracts allows building further functionalities on top for other relevant scenarios (e.g., roaming billing, service migration) by simply creating new smart contracts (*FR3*).

Concerning security aspects, since the solution is built on top of Fabric, it inherits all the advantages of a permissioned blockchain architecture. In particular, all participants must be authenticated via a CA with an X.509 digital certificate and authorized by participating nodes before interacting with the system. This effectively prevents external parties from accessing sensitive data (*SR1*). Beyond this, the certificate based security is also key for the 5G roaming architecture [6]. The use of the Peer-to-Peer (P2P) gossip mechanism and private collections described in Section V-C allows MNOs to share public RAN data within their interaction areas (*SR2*) and to selectively share private RAN data with selected partners in dedicated private areas (*SR3*). Similar to other DLT-based models, the integrity and availability of all data exchanged in Fabric is guaranteed by the orderer service, and the same applies for the accountability of RAN data updates (*SR4*). Nevertheless we highlight that the orderer, as well as unauthorized nodes, see only the hash values of private data exchanged among MNOs [22]. Finally, since the purpose of access rights is only in the scope of the MNOs, when different roles inside the MNOs are taken into account, the concept of Attribute-based Access Control (ABAC) [23] would be able to categorize access rights for each MNO respectively (*SR5*). This concept is already discussed in [24], [25]. With ABAC, AC lists are configured directly inside smart contracts.

To conclude, we highlight that external threats in our solution are the same as those in any generic scenario employing permissioned blockchains. For instance, the lack of a cohesive key management scheme by Hyperledger Fabric could allow a malicious external entity to obtain an MNO's cryptographic private key, thus opening the possibility for further attacks (e.g., replay and message tampering attacks). Another significant issue is the difficulty to detect and mitigate a distributed Denial-of-Service attack because of the decentralized nature of the blockchain. For a detailed survey of attacks on permissioned blockchain and Hyperledger Fabric, we refer the interested reader to [26].

C. European Union-wide Scalability

Investigating on a European-wide setup and live network pilots are the focus of our future work. We stress the fact that, on the cellular network side (RAN and Core), our solution is build upon standardized procedures, available from 4G onwards, which signifies very low integration efforts. In addition, network infrastructure data sharing in the inter-MNO ecosystem is gaining more and more importance, and any solution for the complex cellular network governance between neighboring countries need political, legal and industry contemplations. In here, we sketch a high-level estimation for a real-life application. Our assumptions are explained in Table III, all references are reported at the current time of this paper (April 2021).

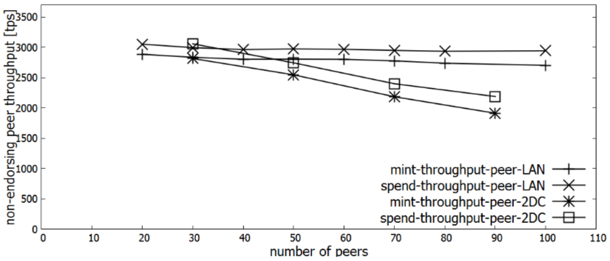


Fig. 9. Scalability Performance [27]

Following [27], the authors examined the performance of Fabric with different numbers of nodes, starting with 10 (the assumption is that each MNO operates one node) and then scaling up to 100 nodes (see Figure 9). *mint* and *spend* are two testing functions, 2DC stands for two data centers (10 peers each) and LAN means all peers run in the same network. This benchmark already covers 47 nodes, representing the number of MNOs operating an own mobile network infrastructure in Europe. We also observed that in the worse case, the throughput still reaches over 2000 transactions per second, which is higher than our requirement with 750 transactions per hour for the RAN sharing application.

VII. Conclusions

We propose a generic solution for the inter-MNO RAN data exchange and management. This cross-carrier collaboration is essential for the provision of seamless coverage and connectivity across national borders: Mobile networks enable the mobility of all users and (automated) devices such as drones, vehicles and trains. The specific use case of RAN data sharing with the evaluated benefit of an accelerated network re-selection at country borders is a pragmatic solution which considerably improves the continuity of service in cross-border scenarios. Apart from being based on standardized cellular network procedures, it yields the advantage of circumventing many associated issues of the inter-PLMN network handover and its inter-MNO Core Network interfaces.

Leveraging DLT for the data governance enables a secure, trusted and transparent system for all MNOs, where public data can be shared in parallel to dynamic individual private alignments. The main mechanism of permissioned blockchains facilitates the access management since each MNO is protected by a CA, and it assures the overall integrity and consistency by cooperatively maintaining the blocks and transactions (data). Future work will provide an additional level of security and further fine-grained AC on the RAN data. Indeed, the proposed solution can also be integrated with cryptographic access control techniques traditionally used in the cloud to protect the confidentiality of sensitive data shared in partially trusted environments [28]. Further uses cases with similar secure cross-border data sharing needs are an improved network planning and radio optimization (both to consider also foreign networks), or a dynamic frequency allocation and coordination (which is currently only statically assigned per country for long periods).

Cross-border scenarios will remain challenge for the near future, especially in Europe with a large number of countries, MNOs and a high cross-border mobility. Despite the advancements e.g. in the GSMA 5G Mobile Roaming Revisited (5GMRR) task force, or with the CCAM mobility corridors, elevated costs and risks for MNOs—including cyber-attack possibilities towards critical telecommunication infrastructure—make it a topic on the political agenda. Nevertheless, the current ecosystem needs a redesign of the traditional cellular network management to lay the ground for future networks. The global network management relies on the collaboration, trust and well-organized data governance between different organizations and countries - a key requirement also for 6G.

Acknowledgment

This work has been performed in the framework of the EU Horizon 2020 project 5G-CARMEN co-funded by the EU under grant agreement No. 825012. The views expressed are those of the authors and do not necessarily represent the project. The Commission is not liable for any use that may be made of any of the information contained therein.

References

[1] Johannes Bahrke and Marietta Grammenou, “State of the Union: Commission calls on Member States to boost fast network connectivity and develop joint approach to 5G rollout),” 2020, URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1603 [accessed: 2021-21-04].

[2] European Commission, “Connecting Europe Facility (CEF2) Digital programme),” 2021, URL: https://ec.europa.eu/digital-single-market/en/connecting-europe-facility-cef2-digital [accessed: 2021-07-02].

[3] ETSI, “ETSI TR 121 900 V16.4.0, [Third Generation Partnership Project (3Gpp)] ,” 2021, URL: https://www.etsi.org/deliver/etsi_tr/121900_121999/121900/16.04.00_60/tr_121900v160400p.pdf [accessed: 2021-21-04].

[4] 5GPPP, “5g trials for cooperative, connected and automated mobility along european 5g cross-border corridors - challenges and opportunities,” 2018, URL: https://5g-ppp.eu/wp-content/uploads/2020/10/5G-for-CCAM-in-Cross-Border-Corridors_5G-PPP-White-Paper-Final2.pdf [accessed: 2021-21-04].

[5] GSMA, “5GS Roaming Guidelines v3.0 ,” 2020, URL: https://www.gsma.com/aboutus/workinggroups/networks-group [accessed: 2021-21-04].

[6] GSMA, “Guidelines for ipx provider networks,” 2020, URL: https://www.gsma.com/newsroom/wp-content/uploads//IR.34-v16.0-3.pdf [accessed: 2021-21-04].

[7] M. Amirijoo, P. Frenger, F. Gunnarsson, H. Kallin, J. Moe, and K. Zetterberg, “Neighbor cell relation list and physical cell identity self-organization in lte,” in *ICC Workshops - 2008 IEEE International Conference on Communications Workshops*, 2008, pp. 37–41.

[8] D. Duarte, P. Vieira, A. Rodrigues, A. Martins, N. Oliveira, and L. Varela, “Neighbour list optimization for real lte radio networks,” in *2014 IEEE Asia Pacific Conference on Wireless and Mobile*, 2014, pp. 183–187.

[9] A. Gorcin and N. Cotanis, “Hybrid automatic neighbor relations for 5g wireless networks,” 07 2017.

[10] DeutscheTelekom, “Deutsche Telekom links into carrier blockchain gang,” 2020, URL: https://www.telcotitans.com/deutsche-telekomwatch/deutsche-telekom-links-into-carrier-blockchain-gang/1373.article [accessed: 2021-21-04].

[11] GSMA, “Blockchain – operator opportunities,” 2018, URL: https://www.gsma.com/newsroom/wp-content/uploads/IG.03-v1.0_Whitepaper.pdf [accessed: 2021-21-04].

[12] C. Nguyen, D. Nguyen, H. T. Dinh, A. H. Pham, N. T. Huynh, Y. Xiao, and E. Dutkiewicz, “Blockroam: Blockchain-based roaming management system for future mobile networks,” *IEEE Transactions on Mobile Computing*, pp. 1–1, 2021.

[13] C. Tselios, I. Politis, and S. Kotsopoulos, “Enhancing sdn security for iot-related deployments through blockchain,” in *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, 2017, pp. 303–308.

[14] A. Okon, N. Jagannath, I. Elgendi, J. M. H. Elmirghani, A. Jamalipour, and K. Munasinghe, “Blockchain-enabled multi-operator small cell network for beyond 5g systems,” *IEEE Network*, vol. 34, no. 5, pp. 171–177, 2020.

[15] R. P. Jover and J. Lackey, “dhss - distributed peer-to-peer implementation of the lte hss based on the bitcoin/namecoin architecture,” in *2016 IEEE International Conference on Communications Workshops (ICC)*, 2016, pp. 354–359.

[16] V. T. Le, C. Pahl, and N. E. Ioini, “Blockchain based service continuity in mobile edge computing,” in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 2019, pp. 136–141.

[17] H. R. Barzegar, N. E. Ioini, V. T. Le, , and C. Pahl, “Cross border service continuity with 5g mobile edge,” in *Mobile Edge Computing*. Springer, 2021, inproceeding.

[18] Geerd Kakes, Pieter Nooren, Maciej Muehleisen, “Seamless roaming with 5G SA deployments scaling across europe,” 2021, to appear in Proceedings of the 30th European Conference on Networks and Communications (EuCNC).

[19] J. Hillebrand, M. Gerosa, D. Garcia-Roger, S. Inca, J. F. Monserrat, G. Avdikos, F. Poli, B. Denis, A. Heider-Aviet, “Current-4G-Networks-Limitations-Pleading-for-5G-for-Cross-border-CAM-Services,” 2021, URL: https://5g-mobix.com/assets/files/Current-4G-Networks-Limitations-Pleading-for-5G-for-Cross-border-CAM-Services-5G-CARMEN.pdf [accessed: 2021-07-07].

[20] ETSI, “Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003 version 10.1.0 Release 10),” 2011, URL: https://www.etsi.org/deliver/etsi_ts/123000_123099/123003/10.01.00_60/ts_123003v100100p.pdf [accessed: 2021-23-03].

[21] Konstantinos Dimou and Min Wang and Yu Yang and Muhammmad Kazmi and Anna Larmo and etc , “ Handover within 3GPP LTE: Design Principles and Performance ,” 2009, URL: https://www.ericsson.com/en/reports-and-papers/research-papers/handover-within-3gpp-lte-design-principles-and-performance [accessed: 2021-21-04].

[22] F. Benhamouda, S. Halevi, and T. Halevi, “Supporting private data on hyperledger fabric with secure multiparty computation,” *IBM Journal of Research and Development*, vol. 63, no. 2/3, pp. 3–1, 2019.

[23] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, “Guide to attribute based access control (ABAC) definition and considerations,” pp. NIST SP 800–162. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf

[24] U. Ann, P. Horea, J. Sowmya, and I. Kaleen, “Use access control in your blockchain smart contracts to streamline supply chain operations,” 2020, URL: https://developer.ibm.com/technologies/blockchain/patterns/fabric-contract-attribute-based-access-control/ [accessed: 2021-08-04].

[25] S. Rouhani, R. Belchior, R. S. Cruz, and R. Deters, “Distributed attribute-based access control system using a permissioned blockchain,” *arXiv preprint arXiv:2006.04384*, 2020.

[26] A. Davenport, S. Shetty, and X. Liang, “Attack surface analysis of permissioned blockchain platforms for smart cities,” in *2018 IEEE International Smart Cities Conference (ISC2)*, 2018, pp. 1–6.

[27] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, “Hyperledger fabric: a distributed operating system for permissioned blockchains,” in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.

[28] S. Berlato, R. Carbone, A. J. Lee, and S. Ranise, “Exploring architectures for cryptographic access control enforcement in the cloud for fun and optimization,” in *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, ser. ASIA CCS ’20. New York, NY, USA: Association for Computing Machinery, 2020, p. 208–221. [Online]. Available: https://doi.org/10.1145/3320269.3384767