# Integrating Blockchain for Enhanced Subscription Management in B5G and 6G Networks

Nischal Aryal[1, 2], Fariba Ghaffari[2], Emmanuel Bertin[1, 2], Noel Crespi[2]
[1] *Orange Innovation, 14000 Caen, France*
[2] *SAMOVAR, Telecom SudParis, Institut Polytechnique de Paris, 91120 Palaiseau, France*
{nischal.aryal, emmanuel.bertin}@orange.com, fariba.ghaffari@telecom-sudparis.eu, and noel.crespi@it-sudparis.eu

***Abstract*—This paper demonstrates the feasibility of integrating Blockchain with existing cellular network architecture to handle the Subscription Management process. We deploy a LTE-based private cellular network testbed utilizing OpenAirInterface (OAI) and Magma core frameworks. Blockchain technology and the InterPlanetary File System (IPFS) are employed to manage subscription and initial registration processes. Our approach leverages Blockchain for secure access control and the InterPlanetary File System (IPFS) for decentralized storage of user-sensitive data. A hybrid cryptosystem is employed to safeguard this data when sharing through Blockchain to ensure both confidentiality and integrity. We evaluate our system by comparing its performance against a traditional LTE network. For comparison, we focus on latency during initial user registration. Our results show that the Blockchain-based approach maintains comparable latency while enhancing security and decentralization.**

***Index Terms*—Private cellular network, OAI, Magma core, Ethereum, Private Blockchain, Go-Ethereum, AAC.**

## I. Introduction

The evolving landscape of cellular networks is driving significant changes in their architecture to seamlessly integrate new technologies [1]. These advancements are crucial not only for enhancing user services but also for increasing revenue streams. A key component of this evolution is the collaboration between different Mobile Network Operators (MNOs) and service providers, which enables the introduction of a variety of user-centric services [2]. These services often require access to sensitive data that are managed by the MNO. To safeguard this information, MNOs currently rely on the Authentication and Key Agreement (AKA) process, a mutual authentication method that ensures both parties are verified before allowing data access. However, meeting the demands of novel and diverse services in Beyond 5G and 6G networks requires a flexible authentication process with enhanced collaboration features, which the current AKA process is unable to provide.

In our previous research [3], we addressed this challenge by proposing a Blockchain-based Authentication and Access Control (AAC) method inside the Core Network (CN). The main focus of this work was to present a novel *Initial Registration* process in cellular networks, leveraging Blockchain and smart contracts. Initial Registration is the authentication process that occurs when a user connects to the network for the first time or after powering on their smartphone. It consists of a series of message exchanges (see Figure 2) between the User Equipment (UE), the Radio Access Network (RAN), and the CN. We did not propose this method as a replacement for the existing AKA process but as an alternative solution for Beyond 5G and 6G networks to add flexibility for integrating new technologies, services, and providers. However, when we attempted to integrate this method with the current network architecture, we encountered numerous challenges (which are detailed in Section II). These obstacles led us to reconsider our architectural proposal to ensure compatibility with the existing network framework.

Driven by the search for introducing compatibility, this paper demonstrates how Blockchain and the InterPlanetary File System (IPFS) can be integrated with the existing cellular network architecture to handle subscription management process. For this integration, we develop scripts using *NodeJS* programming language to handle connections between Blockchain, IPFS, and the cellular network components. Additionally, we modify our Blockchain-based AAC method to support the existing AKA process. This integration serves as a guideline for future work aiming to provide a backward-compatible Blockchain-based solution for cellular networks. The video demonstration of this work is available in [4].

The rest of this paper is organized as follows: Section II discusses the challenges for integrating new AAC methods in existing cellular networks, followed by the description of demonstration setup in Section III. Section IV outlines the evaluation results, followed by conclusion in section V.

## II. Challenges for introducing new AKA procedure

To integrate our Blockchain-based AKA procedure [3] with the LTE private cellular network testbed [5], we needed major changes in the testbed components, especially the UE and MME. The challenges we faced during the integration process are as follows.

1) A cellular network AKA process is a mutual authentication process, meaning both the UE and the core network need to authenticate each other to establish a secure connection. This authentication protocol is implemented both in the core network (particularly in the Home Subscriber Server or HSS) and the UE (via the SIM card). However, in our scenario, the programmable SIM card could not be configured to support the Blockchain-based authentication process.
2) Our Blockchain-based proposal aimed to introduce decentralization into the existing centralized subscription

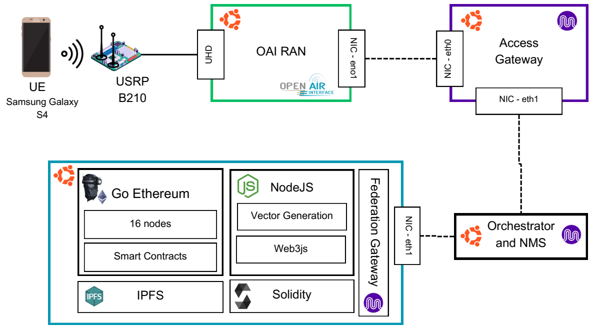


Figure 1. An overview of the testbed setup.

management process. In the LTE network, the Home Subscriber Server (HSS) handles subscription management functionality. All communication with the HSS occurs via the S6a interface using the Diameter protocol, which defines the framework for authentication, authorization, and accounting (AAA). Replacing the HSS with our Blockchain-based method was not feasible because our method did not conform to the Diameter protocol. Moreover, all LTE network functions relies on 3GPP-based standards for communication and messaging, which was incompatible with our new authentication process.

In short, although our proposal addressed the challenges, it was not feasible to integrate with existing architecture. This highlighted the necessity of thorough planning, assessment, and ensuring compatibility with the current infrastructure to implement a novel solution effectively. Consequently, we modified our Blockchain-based proposal to first integrate with the existing network. We developed a script using the *NodeJS* programming language to manage connections based on the Diameter protocol and incorporated the existing authentication protocol to support current authentication and access control processes.

## III. Demonstration Setup and Scenario

Figure 1 gives an overview of our implemented Blockchain-based private cellular network testbed. We propose a novel approach to the registration and subscription process in cellular networks by replacing the HSS in LTE networks with two key components: 1) IPFS as a secure backend database and 2) Blockchain to access database access during the initial registration. The primary objective of this demonstration is to show the feasibility of integrating the proposed method into an end-to-end cellular network testbed. To achieve this, we simulate a real-world scenario where a user with a standard SIM card attempts to connect to their network provider after powering on their phone. During this initial registration process, the registration request is sent to the network and routed from the Mobility Management Entity (MME) to the Blockchain, replacing the traditional HSS, to perform the Authentication and Key Agreement (AKA) procedure. After completing this process, the user gains access to the internet via mobile data, indicating the feasibility of Blockchain-based authentication. Our earlier work [3] provides a detailed description of this procedure. Additionally, the communication messages between MME and Blockchain during the AKA and the initial registration processes are monitored and demonstrated using Wireshark.

The implementation of the testbed is done in two following phases.

### A. LTE Private Cellular Network

The detailed setup and configuration instructions for this testbed are present on our GitHub[1] page. The testbed has three main components: the UE, RAN, and CN.

The UE is implemented using a *Samsung Galaxy S4* smartphone paired with a programmable *Sysmocom* SIM card[2], which is configured using the *pySim* tool[3]. The RAN is deployed using the *OpenAirInterface5G (OAI)* software [6], running on an Ubuntu operating system with a low-latency kernel. For radio communication between the UE and the RAN, a *USRP B210* device is employed. The RAN is connected to the CN via an Ethernet cable. The configuration file named *enb.band7.tm1.50PRB.usrpb210.conf* in the *OAI* setup is used to store IP and Public Land Mobile Network (PLMN) data necessary for establishing the connection with CN. The CN is implemented using a combination of *OAI* and *Magma Core* frameworks [7] on an Ubuntu operating system. *Magma Core* provides several key components, including the Access Gateway (AGW), the Orchestrator (Orc8r), and the Federation Gateway (FeG). The *Mobility Management Entity (MME)* for LTE is implemented using the AGW, which handles all communication processes originating from the RAN. Additionally, the *OAI* software is utilized to configure the Home Subscriber Server (HSS), which stores all user-related information and plays a critical role in the authentication process. Finally, the *FeG* facilitates the connection between the MME and HSS. We modify the *FeG* configuration to connect the MME with our Blockchain-based method, which replaces the traditional HSS for managing user-related information and authentication processes.

### B. Blockchain Environment

We deploy a private Ethereum Blockchain using the Go Ethereum (Geth) framework [8], an implementation of Ethereum written in Go programming language. We first deployed 16 Ethereum nodes and assigned a unique `chainID` to the network. This `chainID` is the unique identifier of the network and ensures that nodes can only interact with other nodes with the same ID. Next, we use *Proof of Authority (PoA)* [9] as our network's consensus protocol. Finally, we save all this information along with other network information, such as gas limits, the initial allocation of `ether`, etc., in the `genesis block`. A genesis block is the very first block in the Blockchain and we configure this using the

[1] https://github.com/nischalaryal/cellular-network-testbed-setup
[2] https://sysmocom.de/products/discontinued/sysmousim/index.html
[3] https://github.com/osmocom/pysim

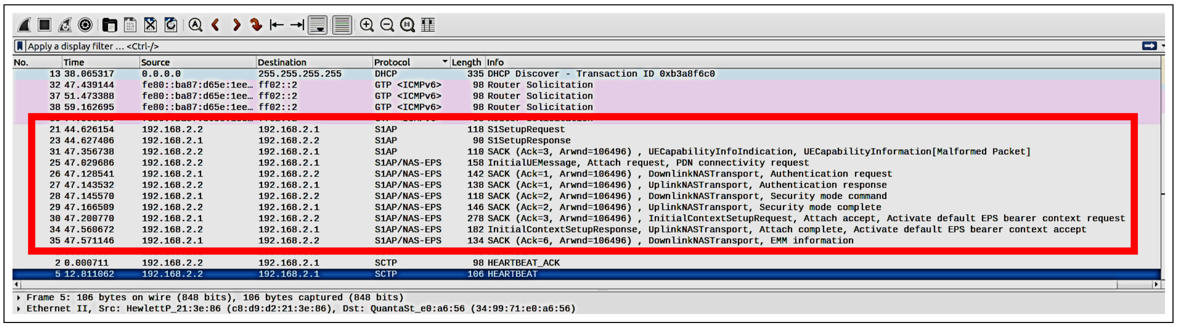


Figure 2. Wireshark packet capture showing the Initial Registration process (inside red box): the first three messages denote the connection between CN and RAN, with subsequent messages related to Initial Registration.

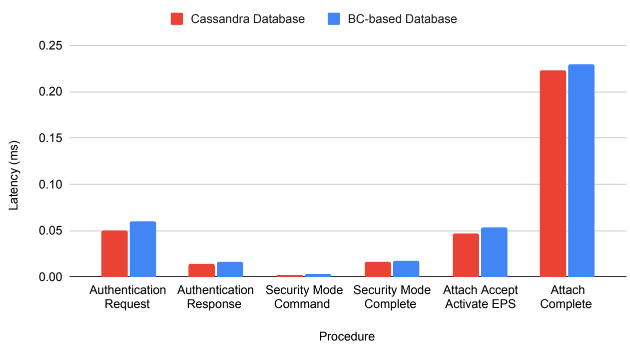


Figure 3. Latency measurement during different message passing for initial registration procedure. Red bars represent the existing testbed using a Cassandra database for HSS, while blue bars depict our Blockchain-based testbed.

`genesis.json` file. We develop the smart contracts using the Solidity programming language and utilize the `web3js` framework to communicate with our private Ethereum network.

## IV. Evaluation

To evaluate the method, we investigate the time taken by Blockchain-based end-to-end network testbed to complete the initial registration procedure. We used Wireshark to capture detailed information during each message exchange (see Figure 2). Subsequently, we compared the latency results of the registration procedure between our Blockchain-based testbed and an existing LTE network testbed. We repeated this procedure 15 times for each testbed, and chose the optimal result which is demonstrated in Fig. 3. As shown in the figure, the Blockchain-based testbed shows comparable performance to the existing testbed, with slightly increased latency. This could be attributed to the additional step of message requests passing through the Blockchain layer.

## V. Conclusion

This study demonstrates the integration of a Blockchain-based AAC method into the existing cellular network architecture. We utilize the IPFS as a decentralized, distributed database for storing user information. To protect data privacy, we employ a hybrid cryptosystem for encrypting the data before storage and ensuring that only authorized personnel can decrypt and access the data. Blockchain and smart contracts manage all authorization and access control requests to this data.

To integrate this DLT solution into a LTE private cellular network, we developed scripts using the NodeJS programming language to facilitate communication with the Mobility Management Entity (MME). We evaluated our method by comparing it with an existing LTE private cellular network testbed, focusing on the latency required to complete the registration procedure. The results indicate that our method exhibits comparable performance to existing solutions with slight increase in latency which can be attributed to the additional step of data passing through the Blockchain layer.

For future works, we plan to study the feasiblity of implementing a software-based UE which can store different authentication methods. Blockchain community could also explore the development and optimization of Blockchain components, such as consensus mechanisms, to better suit the cellular network ecosystem.

## References


[1] N. Aryal, F. Ghaffari, E. Bertin, and N. Crespi, "Distributed ledger technology for next-generation cellular networks: A swot analysis," in *Blockchain and Smart-Contract Technologies for Innovative Applications*. Springer, 2024, pp. 281–304.

[2] Z. Luo, S. Fu, M. Theis, S. Hasan, S. Ratnasamy, and S. Shenker, "Democratizing cellular access with cellbricks," in *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*, 2021, pp. 626–640.

[3] N. Aryal, F. Ghaffari, E. Bertin, and N. Crespi, "Subscription management for beyond 5g and 6g cellular networks using blockchain technology," in *2023 19th International Conference on Network and Service Management (CNSM)*. IEEE, 2023, pp. 1–7.

[4] N. Aryal, "Demonstration on integrating blockchain and ipfs with private cellular network," accessed on 1 Sept 2024. [Online]. Available: https://youtu.be/gtJ_VLv8wu4

[5] N. Aryal, F. Ghaffari, S. Rezaei, E. Bertin, and N. Crespi, "Private cellular network deployment: Comparison of openairinterface with magma core," in *2022 18th International Conference on Network and Service Management (CNSM)*. IEEE, 2022, pp. 364–366.

[6] "OpenAirInterface – 5G software alliance for democratising wireless innovation." [Online]. Available: https://openairinterface.org/

[7] "Magma – Linux Foundation Project." [Online]. Available: https://magmacore.org/

[8] G. Ethereum, "Go-Ethereum," https://geth.ethereum.org/, accessed: 2024-04-07.

[9] "Proof of Authority." [Online]. Available: https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains