POSTER: Using Blockchain for Enhanced Inter-MNO Authentication in B5G and 6G Networks

Nischal Aryal
Fariba Ghaffari
SAMOVAR, Télécom SudParis,
Institut Polytechnique de Paris
Palaiseau, France

Emmanuel Bertin
Orange Innovation
Caen, France

Noel Crespi
SAMOVAR, Télécom SudParis,
Institut Polytechnique de Paris
Palaiseau, France

Abstract

This paper introduces a Blockchain-based overlay network that allows users to authenticate and access services across different MNOs without requiring prior agreements. The overlay leverages smart contracts for decentralized access control and IPFS for secure, shared storage of encrypted subscription data. A hybrid testbed using OpenAirInterface, Magma Core, Go Ethereum, and IPFS validates the system, demonstrating comparable latency, secure, and scalable cross-operator authentication—supporting flexible inter-operator collaboration in future B5G/6G networks.

CCS Concepts

• **Networks** → **Network architectures**.

Keywords

Cellular Networks, AKA procedure, Blockchain, Smart Contracts

ACM Reference Format:
Nischal Aryal, Fariba Ghaffari, Emmanuel Bertin, and Noel Crespi. 2025. POSTER: Using Blockchain for Enhanced Inter-MNO Authentication in B5G and 6G Networks. In *ACM SIGCOMM 2025 Posters and Demos (SIGCOMM Posters and Demos '25), September 8–11, 2025, Coimbra, Portugal.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3744969.3748426

1 Introduction

As mobile networks evolve toward Beyond 5G and 6G, existing 3GPP-standardized architectures face limitations in supporting emerging use cases like private networks, cross-border mobility, and multi-tenant infrastructure sharing. These scenarios require dynamic and secure collaboration among multiple Mobile Network Operators (MNOs). However, current mechanisms, such as the Authentication and Key Agreement (AKA) protocol, rely on static trust relationships and bilateral agreements, making them inadequate for the flexible and scalable requirements of future networks [4].

Building on previous work [1], which uses Blockchain and IPFS for subscription management within a single MNO, this document extends the architecture to enable inter-MNO collaboration which is crucial for Beyond 5G and 6G networks. It proposes a Blockchain-based overlay network that provides decentralized access control and authentication across different MNOs without relying on static trust or bilateral agreements. In this method, subscription data is securely stored off-chain in IPFS using a hybrid cryptosystem. Unlike traditional 3GPP AKA protocols, which rely on fixed trust relationships, the proposed solution uses smart contracts to handle more dynamic situations involving external providers. This allows for a more scalable and flexible system that doesn't require pre-established trust between all parties.

We developed a Blockchain-based cellular network testbed to validate our approach, using OpenAirInterface for the radio access network, Magma Core for core network functionalities, and Go Ethereum as the Blockchain platform. To enable seamless interaction between the Blockchain, IPFS (for decentralized storage), and the cellular core components, we created a module written in *Node* programming language that handles data exchange and coordination across these systems. This setup allowed us to test the integration and performance of our proposed solution in a controlled environment.

Note: This study focuses specifically on the authentication function in the context of inter-MNO roaming agreements. While other essential functions, such as billing and routing, are acknowledged, they fall outside the scope of this work.

2 System Design

In this paper, we propose a blockchain-based system designed to securely manage user identities, access attributes, and service agreements across mobile networks. When a user connects to an external provider, their registration and access control data are handled through smart contracts, enabling decentralized and verifiable interactions. The user's public key and service plan are securely stored and referenced during the AKA procedure, ensuring mutual authentication while maintaining compatibility with standard cellular protocols. All sensitive data are stored off-chain for enhanced performance, and a hybrid cryptographic approach is used for privacy and security of these data.

The proposed architecture assumes secure off-chain communication, next-generation eSIMs capable of storing Blockchain credentials, and the proper authorization and certification of all participating entities. When a user attempts to connect to an external connectivity provider, their device shares its Blockchain address along with the identifier of its home MNO. The external provider then uses smart contracts to verify the user's identity, validate access permissions, and ensure the integrity of the request. To complete mutual authentication, the provider coordinates with the home MNO, which verifies the provider's legitimacy and permission to serve the user, then assists in validating the user's credentials.

SIGCOMM Posters and Demos '25, Coimbra, Portugal

ACM ISBN 979-8-4007-2026-0/25/09
https://doi.org/10.1145/3744969.3748426

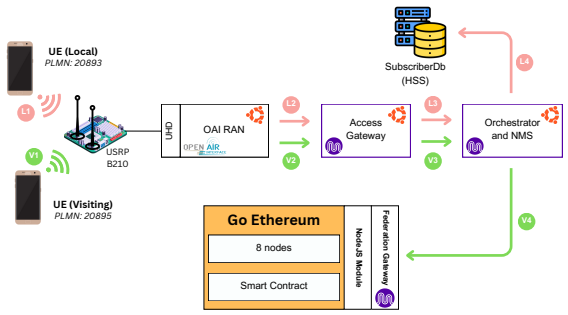

Figure 1: An overview of the Blockchain-based end-to-end testbed for authentication processes of a local user (L1-L4) and a visiting user (V1-V4).

Overall, the proposed overlay network enhances flexibility and scalability in Beyond 5G networks by enabling decentralized collaboration between operators while maintaining security, accountability, and compatibility with existing mobile network standards.

3 Evaluation

To validate our Blockchain-based authentication framework, we developed an end-to-end testbed, illustrated in Figure 1. The testbed integrates a private LTE network with a private Ethereum Blockchain. The LTE network is built using OpenAirInterface and Magma Core, and includes a UE (Samsung Galaxy S4 with a programmable SIM), a radio access network (RAN) based on a USRP B210 software-defined radio, and a core network using Magma with containerized components such as the MME and subscriber database. The Blockchain component is implemented using Geth (Go Ethereum), running eight nodes configured with the Clique proof-of-authority (PoA) consensus mechanism. Smart contracts are written in Solidity, and all blockchain interactions are managed through the web3.js library.

The testbed supports two scenarios: local users are authenticated through the standard LTE procedure, while visiting users are verified through the Blockchain overlay.

The integration of Blockchain in the LTE authentication workflow introduced several challenges. In a typical LTE setup, the MME communicates with the subscriber database (HSS) over the S6a interface using the Diameter protocol. However, this protocol is not compatible with Blockchain-based logic. To overcome this, we developed a module written in Node programming language that can parse Diameter messages and forward the necessary data to the Blockchain for processing.

Another significant challenge involved SIM card limitations. The programmable SIMs we used could not be reconfigured to store Blockchain-related cryptographic keys. Moreover, the Milenage algorithm, commonly used for LTE authentication, is tightly integrated with both the SIM, MME, and HSS. To resolve this, we adapted the vector generation module to retrieve data from the Blockchain and compute Milenage vectors, maintaining compatibility with LTE authentication while enabling evaluation of the Blockchain mechanism.

The evaluation process is divided into two distinct phases, outlined below. 1) We assess 3GPP-based authentication by measuring message-level latency using Wireshark. Our prototype shows slightly higher latency compared to the conventional testbed, primarily due to the Blockchain layer and its non-optimized configuration, although overall performance remains comparable (Figure 2); 2) We evaluate the scalability of the proposed authentication process (Figure 3). The system handles up to 1000 concurrent requests with minimal latency increase, even with multiple validator nodes, demonstrating its scalability and suitability for high-demand networks.

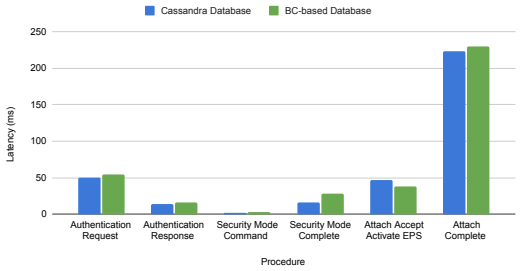

Figure 2: Latency measurement for different steps in AKA procedure.

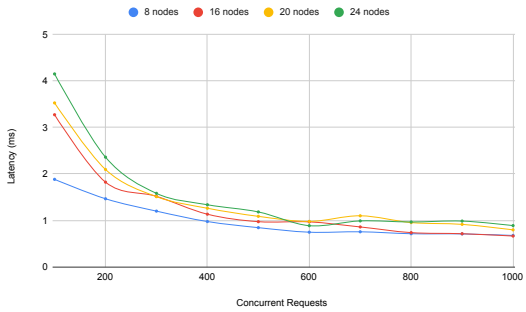

Figure 3: Scalability assessment with varying number of validator nodes.

4 Discussion and Future Directions

This work proposes a Blockchain-based overlay network to enable secure, decentralized authentication and billing in collaborative cellular networks, while remaining compatible with existing systems. Key challenges include managing ownership, ensuring node diversity, and addressing scalability trade-offs. Techniques like Layer 2 solutions, chain sharding [2, 3], and custom Blockchain designs can improve performance. Data privacy is preserved through restricted access and minimal data use.

Future research can focus on enhancing network scalability and latency, extending support to additional procedures (billing and routing), and expanding the testbed for broader validation. Exploring Blockchain models specifically tailored for cellular networks could further optimize performance and support real-world deployment at scale.

References

[1] Nischal Aryal, Fariba Ghaffari, Emmanuel Bertin, and Noel Crespi. 2023. Subscription Management for Beyond 5G and 6G Cellular Networks Using Blockchain Technology. In *2023 19th International Conference on Network and Service Management (CNSM)*. 1–7. doi:10.23919/CNSM59352.2023.10327810

[2] Gagandeep Kaur and Charu Gandhi. 2020. Scalability in Blockchain: Challenges and Solutions. In *Handbook of Research on Blockchain Technology*, Saravanan Krishnan, Valentina E. Balas, E. Golden Julie, Y. Harold Robinson, S. Balaji, and Raghvendra Kumar (Eds.). Academic Press, 373–406. doi:10.1016/B978-0-12-819816-2.00015-0

[3] Yi Li, Jinsong Wang, and Hongwei Zhang. 2023. A survey of state-of-the-art sharding blockchains: Models, components, and attack surfaces. *Journal of Network and Computer Applications* 217 (2023), 103686. doi:10.1016/j.jnca.2023.103686

[4] Dinh C. Nguyen, Pubudu N. Pathirana, Ming Ding, and Aruna Seneviratne. 2020. Blockchain for 5G and beyond networks: A state of the art survey. *Journal of Network and Computer Applications* 166 (2020), 102693. doi:10.1016/j.jnca.2020.102693