A novel approach for network resource sharing via blockchain

Fariba Ghaffari, Emmanuel Bertin, Noel Crespi

A Novel Approach for Network Resource Sharing via Blockchain

Fariba Ghaffari, Emmanuel Bertin
Orange Labs, France
{fariba.ghaffari,emmanuel.bertin}@orange.com

Noel Crespi
Institut Telecom, Telecom SudParis,
CNRS 5157, France
noel.crespi@it-sudparis.eu

ABSTRACT

Authentication and access control are among the vital procedures to build efficient networks. Existing centralized solutions suffer from vulnerabilities to DoS attacks, high maintenance costs, and high computational load. Emerge of Blockchain technology provides unprecedented opportunities to improve existing methods. In this paper, we propose a Blockchain-based access control mechanism for providing access to network resources. Removing the single point of failure, decreasing the computational cost and load, high scalability and immutability, and trustful payment are some of the main advantages of the proposed model.

CCS CONCEPTS

• **Security and privacy** → **Access control**; **Mobile and wireless security**; • **Networks** → **Network management**.

ACM Reference Format:
Fariba Ghaffari, Emmanuel Bertin and Noel Crespi. 2021. A Novel Approach for Network Resource Sharing via Blockchain. In *ACM SIGCOMM 2021 Conference (SIGCOMM '21 Demos and Posters), August 23–27, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3472716.3472867

1 INTRODUCTION

Authentication and access control play a key role in the security of cellular networks. Authentication and Key Agreement (AKA) solutions in cellular networks suffer from a variety of vulnerabilities that may weaken the user confidentiality or facilitate attacks [1]. Moreover, the Service Providers (*SP*) authenticate the users and manage their access in a centralized process, leads to having a single point of failure and bottleneck for performance and scalability. Blockchain-based decentralized applications (i.e., smart contracts)[2, 5, 6, 8] can help addressing these issues. This paper focuses on a Blockchain-based access control solution that aims to replace the AKA-based method. We propose a prototype where AKA-based authentication is completed by a Blockchain-based authorization to access given services without additional cost. The proposed approach is scalable and not vulnerable to DoS attacks. It also decreases the processing load and maintenance cost in the *SP* and Network Provider (*NP*).

One of the recent studies related to our work, is proposed by Ling et al. [3, 4] to reach an agreement between the user and *NP* to access the network through a smart contract. The main constraint of this model is its single point of failure.

2 SYSTEM DESIGN

We propose a solution for *NPs* to outsource their authentication and access control procedure. In this method, the access control is done via immutable and fault-tolerant smart contracts without a central authority. Moreover, providing a trustful payment procedure eliminates for *NP* the need of billing the users for accessing specific services. To do so, the *SP* pays the *NP* on behalf of the user. Registration and access control, are the two main steps of the proposed model.

In the registration step (Fig. 1(a)), users and *SPs* are registered in the system via a smart contract (*Reg_contract*), through the following steps: 1) *NP* and *SP* reach an agreement on the price of media (e.g., based on service time). 2) *SP* deploys a contract according to the agreement (*Net_contract*). 3) The user subscribes to the *NP* for the connections. 4) User reaches an agreement for the service plan and price with the *SP*. 5) The user deploys a smart contract in the system based on the agreed parameters (*Ser_contract*).

The access control procedure for registered users is as follows (Fig. 1 (b)): 1) The *NP* assures that the user is one of its customers. So, the user sends a request for network connection. 2) *NP* authenticates the user by AKA-based method. 3) The authentication gateway redirects the request to the access control contract (*AC_contract*) which is responsible for controling the user's access to the network and provide secure payment to the *NP*. 4) *AC_contract* makes the access decision based on the policies and the attributes stored in the *Net_contract* and *Ser_contract*. 5) For eligible users, the network cost is deducted from the balance of the *SP* and deposited in the *AC_contract*. Then the user can use the service

SIGCOMM '21 Demos and Posters, August 23–27, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8629-6/21/08.
https://doi.org/10.1145/3472716.3472867

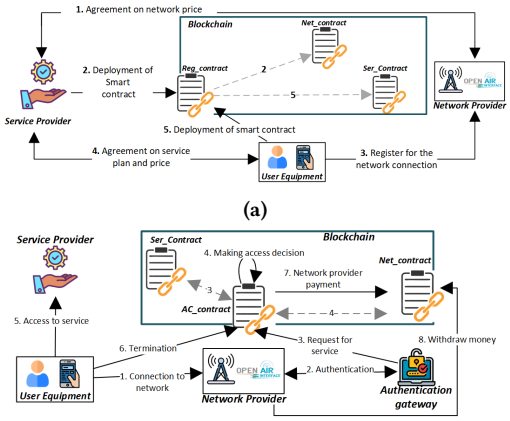

Figure 1: The registration (a), and access control (b) steps of the proposed system

exempted from network billing. 6) After using the service, the user sends a termination trigger to the *AC_contract*. 7) The *AC_contract* fetches the connection information from the Blockchain and pays the *NP* accordingly. So, the *NP* can be assured that after providing the network connection, it will be paid by the *SP*. 8) The *NP* can withdraw the money from *Net_contract*.

3 EVALUATION

We simulated the scenario of Fig. 1 in 5G network using OAI (Open Air Interface) consisting of a Radio Access Network (RAN) and Core Network (CN). OAI implements cellular network functions of the RAN and the core network. We add a function to CN for authentication and sending the user's request to the Blockchain. For OAI-RAN, master branch release v1.1.0 is used. USRP B210 board is utilized for radio communications. It supports 2*2 MIMO and connects to the PC through the USB3 interface. For the Blockchain, we used the Ethereum network simulated on ganache-cli v6.12.2. The smart contracts are deployed by Solidity (Solc v0.8.2). We evaluate the performance and scalability of the proposed method based on latency and storage complexity [9].

If the latency experience low deviation by altering parameters, it means the system is scalable [7]. We evaluate the latency for different Block-Time (*BT*) and Block-Sizes (*BS*). *BT* is an interval between consecutive blocks, and *BS* is the number of transactions fit into one block. As shown in Fig. 2 (a) and (b), increasing number of concurrent requests, the latency stays stable (i.e., suitable for a large number of users). Also, an increasing number of users in the system increases the number of validators. So, we can claim that the system latency is not highly dependent on the number of users.

Blockchain stores all transactions. So, its size is always growing. Creating many transactions for validation of a request results in a sharp increase in the required space. This

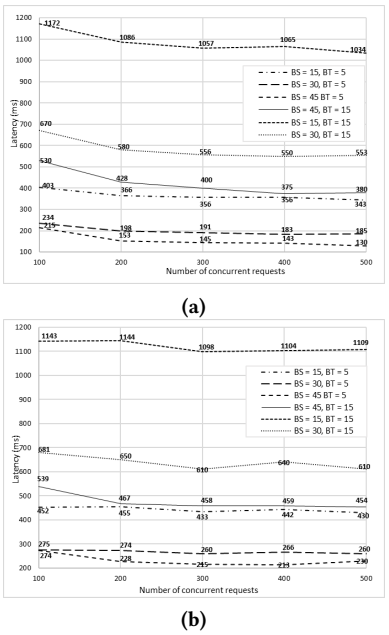

Figure 2: The evaluation results. the latency for (a) registration, and (b) access control procedure

problem decreases the possibility of real-world implementation. For our proposed method, the *SP* registration generates three transactions per request, so its complexity is $n \times 3$. This parameter is $n \times 4$, and $n \times 5$ for user registration and access control, respectively. Decreasing the storage complexity of the method is suggested as future work.

4 DISCUSSION AND FUTURE DIRECTION

The proposed method brings high scalability in terms of the number of users, high integrity, and immutability regarding the access policies and the agreement among parties. It also provides the capability of trustful payment for the *NP*.

Although having the first step AKA-based authentication can increase the security in the whole method, having an authentication gateway may cause to high load of request processing and make it a single point of failure in authentication step. So, as a suggestion for future direction, this method can be introduced as the first step to replace the AKA-based access control mechanism with a Blockchain-based approach. This can result to enable the network provider to provide an internet connection for any user (regardless of being a customer) if there is a service provider who pays the connection through the Blockchain. Also, it can provide an idea and vision about how to implement more software-based and loosely-coupled network authentication and access control, by outsourcing these process and decoupling it from the network. Decreasing the storage consumption and latency are other proposed future direction, to make the method suitable for storage constraint devices and time-dependent use-cases.

REFERENCES

[1] Shanay Behrad, Emmanuel Bertin, Stéphane Tuffin, and Noel Crespi. 2020. A new scalable authentication and access control mechanism for 5G-based IoT. *Future Generation Computer Systems* 108 (2020), 46–61.

[2] Julien Hatin, Emmanuel Bertin, Baptiste Hemery, and Nour El Madhoun. 2020. Welcome to the jungle: A Reference Model for Blockchain, DLT and Smart-Contracts. In *Tokenomics 2020 on Blockchain Economics, Security & Protocols (2nd International Conference)*.

[3] Xintong Ling, Yuwei Le, Jiaheng Wang, Zhi Ding, and Xiqi Gao. 2020. Practical modeling and analysis of blockchain radio access network. *IEEE Transactions on Communications* (2020).

[4] Xintong Ling, Jiaheng Wang, Taha Bouchoucha, Bernard C Levy, and Zhi Ding. 2019. Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm. *IEEE Access* 7 (2019), 9714–9723.

[5] Ahmed Afif Monrat, Olov Schelén, and Karl Andersson. 2019. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* 7 (2019), 117134–117151.

[6] Satoshi Nakamoto. 2019. *Bitcoin: A peer-to-peer electronic cash system*. Technical Report. Manubot.

[7] Markus Schäffer, Monika Di Angelo, and Gernot Salzer. 2019. Performance and scalability of private Ethereum blockchains. In *International Conference on Business Process Management*. Springer, 103–118.

[8] Nick Szabo. 1998. Secure property titles with owner authority. *Online at http://szabo. best. vwh. net/securetitle. html* (1998).

[9] Junfeng Xie, F Richard Yu, Tao Huang, Renchao Xie, Jiang Liu, and Yunjie Liu. 2019. A survey on the scalability of blockchain systems. *IEEE Network* 33, 5 (2019), 166–173.