Blockchain-based user profile and mobile number portability for beyond 5G mobile communication networks

Fariba Ghaffari, Emmanuel Bertin, Noel Crespi

Blockchain-based User Profile and Mobile Number Portability for Beyond 5G Mobile Communication Networks

[1, 2] Fariba Ghaffari, [1, 2] Emmanuel Bertin,*Senior Member, IEEE*, [1] Noel Crespi,*Senior Member, IEEE*
[1] *Orange Innovation, 14000 Caen, France*
[2] *IMT, Telecom SudParis, Institut Polytechnique de Paris, 91764 Palaiseau, France*
{Fariba.ghaffari, Emmanuel.bertin}@orange.com, and noel.crespi@it-sudparis.eu

***Abstract*—Mobile Number Portability (MNP) is a regulatory requirement for Mobile Network Operators (MNO) to enable users to switch MNO. Existing centralized structures in this regard suffer from single points of failure, imposed switching costs, data leakage, low availability, and high latency. In this paper, we propose a Blockchain-based system to allow switching between MNOs while keeping users' profiles and phone numbers. The experiments confirm that our solution can provide fast and scalable profile management and switching solutions.**

***Index Terms*—User profile management, switching MNOs, distributed systems, IPFS, Blockchain.**

I. Introduction

In 2021, there are more than 6B unique mobile subscribers in the world [1] that actively use the services and connections provided by Mobile Network Operators (MNO). On one hand, it is inevitable for the users to switch among MNOs based on their needs and preference. On the other hand, keeping a dedicated mobile number is a crucial requirement. Mobile Number Porting (MNP) is the process in which the subscriber can keep her mobile number in the process of porting from one MNO to another [2], [3]. Providing the capability of MNP can enhance the competitiveness of the cellular network market, decrease the imposed prices and services, and help to improve the innovation among MNOs [4].

Currently, the MNOs and users need to manage the switching procedure manually or in contact with MNP applications. Both procedures suffer from high delays and additional fees. Moreover, trust in the third party is a challenging issue [5]. From a technical point of view, the centralized architecture makes the system vulnerable to DoS attacks and threatens the availability of the system. Moreover, key management increases the processing load of the MNOs [6]. In this regard, an alternative solution would be a game-changer, if it can help the procedure to be executed faster, more transparent, and more secure.

Blockchain [7] is a distributed ledger of transactions fitted into blocks that are updatable only via a consensus among all participating nodes in the network. This technology and its extension, smart contracts [8], [9], can offer higher immutability and transparency in the system. Moreover, switching process management using smart contracts increases the trust and availability in the system. It means MNOs can outsource their porting procedure to a distributed system managed by all MNOs. As a result, the loading procedure of the MNOs would also decrease.

In this paper, we propose a new Blockchain-based system for MNP that aims to 1) remove the central authority to decrease the inherited threats and the complexity of the MNP procedure, and 2) provide a faster, more transparent, and secure method for switching MNOs. The main contributions of this paper are:

1) Porting the user's profile along with their number
2) Outsourcing the user profile management to a distributed environment without requiring any trusted third party.
3) Subscribers can change their MNO freely and promptly;
4) The system provides forward/backward secrecy.
5) The current MNO is not evolved in the switching procedure, resulting in faster switching.

Paper organization: Section II provides the state of the arts. In Section III we outline the problems of the existing methods and presents our proposed solution. The detailed design and construction of the proposed method are provided in Section IV, followed by the experiment in section V. Section VI provides our conclusions about the proposed method as well as some future research directions.

II. Related works

Due to the significance of mobile number portability, this concept is targeted in several recent studies. However, to the best of our knowledge, many limited methods focused on Blockchain-based MNP. In this section, we will provide a brief survey on the related works in this regard.

Shah et al. [5], proposed a Blockchain-based MNP scheme on top of Ethereum to provide transparency and immutability. This method is analyzed in the Remix platform. Moreover, Krishnaswamy et al. [10] proposed a Blockchain-based framework on top of a private Hyperledger Fabric. This method suffers from having a single point of failure and the non-availability of performance analysis. Apart from the Blockchain-based solutions, several studies provided MNP in a decentralized manner. For instance, Chen et al. [11] proposed a call routing mechanism to support enum-based mobile number porting. Moreover, Odii et al. [12] proposed a hybrid solution to support MNP and call routing.

III. Problem statement and system overview

Assume that user u wants to switch its MNO form MNO_1 to MNO_2. Currently, this process is done in a centralized manner consisting of four steps as follows:

1) *Request:* u requests MNO_1 for start switching procedure; for the successful requests a verification code would be sent to u.
2) *Validation:* MNO_2 validates the user and the request by sending the validation request to MNO_1 through a centralized trusted party.
3) *Clearance:* MNO_1 manage the legal clearance from a legal authority.
4) *Activation:* Once, the trusted party receives the clearance notification, ask MNO_1 to delete the user and MNO_2 to insert the user into its list.

It is important to mention that, several mobile number portability applications manage this procedure on behalf of the user. Although these third-party entities can efficiently decrease the user side loads and facilitate the whole of this procedure, they introduce several new challenges as well. In any case, we have identified several drawbacks in the existing model (i.e., with/without MNP applications), as follows:

- The real-world switching process is highly time-consuming.
- User profile would not be ported to the new MNO, so, the user needs to repeat all subscription procedures.
- Centralized servers to manage the user's request, key management, and the centralized database for the user's identity can be a single point of failure.
- MNOs need to trust an MNP, which can pose a threat to user data protection.
- Users need to pay a porting fee (to MNO or third party).

Addressing these constraints, we propose a new Blockchain-based MNP system in telecommunication beyond 5G, which also makes the mobile number and profile switching procedure more secure, efficient, and faster. The proposed method relies on the Blockchain wallet, user's key pair in Blockchain, smart contracts, and distributed database to manage the switching MNOs. Moreover, the proposed method eliminates the single point of failure, removes the need to have any trusted third party, provides high immutability for user data, and delivers higher transparency and accountability.

Note that, we assume having a governance body that validated the identity of the MNOs before inserting them into the system (similar to the existing real-world scenario). It is important to mention that before this step we assume that the user's identity is stored in IPFS by MNO_1. The proposed procedures for subscribed users in this system are as follows:

1) u sends its request to the Blockchain.
2) Once receiving the user's request, the user is redirected to MNO_2 to submit the request.
3) MNO_2 verifies the request and fetched the hash of the user data.
4) MNO_2 requests the user to decrypt its data.
5) MNO_2 asks Blockchain to update user data ownership.
6) MNO_2 stores the user's encrypted data in a distributed database, and its access link in the user's smart contract.
7) Porting smart contract updates the contract of MNO_1 and MNO_2 to remove/add u from/to their user list.

IV. System design

In this section, we described the proposed method. It is important to mention that the general assumptions of the proposed method are as follows:

- Off-chain connections (i.e., the connections outside of the Blockchain) are secure.
- User equipment supports e-SIM in which the user's Blockchain address (Ad_u) and public/private key pair (Pub_u, Pr_u) are hard-coded.
- regulatory body is responsible to manage the list of validated MNOs, and registration/porting smart contracts.
- Regulatory body and MNOs participate in Blockchain's consensus procedure.

Firstly, we introduce the smart contracts used in the on-chain part of our system.

A. Designed smart contracts

The designed smart contracts are as follows:

1) *Address book (SC_{AB})* stores the addresses of the other single smart contacts (i.e., Registration, Port management, MNO list, and User list smart contracts), to make their collaboration secure. In this contract, the names of contracts are mapped to their addresses. Note that the purposes of designing this contract are 1) avoiding using hard-coded addresses to evade maintainability defects of smart contracts [13], 2) having a list of predefined addresses to limit the function execution to some smart contracts, and 3) avoiding data falsification by forged smart contracts.
2) *User smart contract (SC_U)* is a specific contract for the users which stores, at least, $Number_u, CID_{EN^M_{S_k}}, EN^{S_k}_{Pub_u}, EN^{S_k}_{Pub_{MNO}}, Hash(M)$, which represent user's phone number, access identifier of IPFS storage for user's data encrypted by S_k as master key, the S_k encrypted by user's and MNO's public key, and the hash of plain-text user data, respectively.
3) *User smart contract (SC_{UL})* stores the list of registered users by mapping Ad_u to the SC_U and the user's current MNO ($Code_{MNO}$).
4) MNO smart contract (SC_{MNO}) is a unique specific contract for each MNO, deployed by a regulatory body. This contract stores, at least, MNO's subscribers and the list of users' port requests.
5) MNO list smart contract (SC_{MNOL}) is a single smart contract, owned by the regulatory body, to keep the list of trusted and validated MNOs.
6) *Port management smart contract (SC_{port})* is a single smart contract dedicated to handling the switching process. To port the user, after validating the user's request, this contract removes the user from $SC_{MNO_{old}}$ and adds

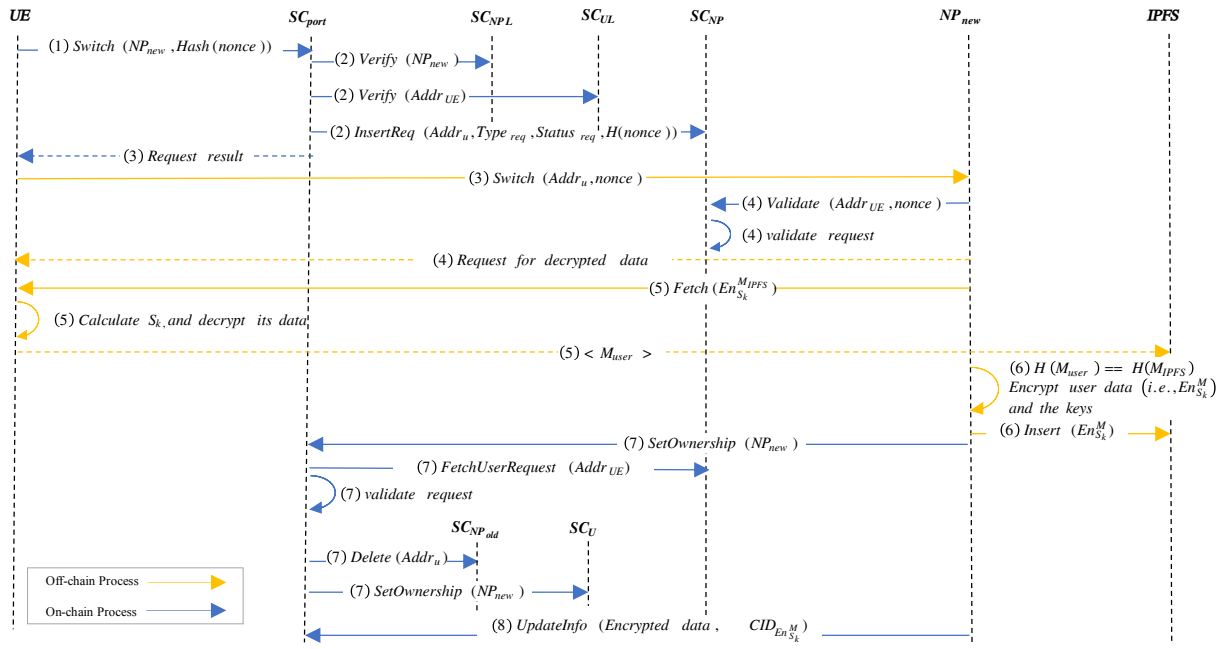

Fig. 1: MNO switching procedure

her into $SC_{MNO_{new}}$. Moreover, this contract switches the ownership of the user's data to MNO_{new}.

B. Switching MNOs

In this phase, we assume that 1) the user is subscribed in MNO_{old}, 2) her PII information is securely recorded in IPFS, and 3) her PII data is encrypted by a master key S_k (i.e., $EN^M_{S_k}$), 4) S_k is encrypted by user's and MNO's public key (i.e., $EN^{S_k}_{Pub_u}$, $EN^{S_k}_{Pub_{MNO}}$), and 5) the CID of encrypted keys are stored in the user's smart contract. Note that, after storing the data in IPFS, it would be indexed by a cryptographic hash function, which results in returning its unique content identifier (CID). The switching process is as follows (see Fig. 1):

1) u sends the switching request to SC_{port} by creating a transaction in the Blockchain, and sending:
$$< Code_{MNO_{new}}, Hash(nonce) >,$$
2) SC_{port} receives the user request, verifies her existence in the network from SC_{UL}, and verifies $Code_{MNO}$ to ensure that the MNO_{new} exists in SC_{MNOL}. If all conditions passed, SC_{port} inserts the summery of the user's request in $SC_{MNO_{new}}$), using the following data:
$$< Ad_u, St_{req} = 1, Hash(nonce) >$$
in which St_{req} shows the progress of the request; It can be 1 to indicate the request is demanded, 2 to show the request is validated, and 3 to determine that the request is terminated. It is important to mention that inserting the switching requests to SC_{MNO} are restricted to SC_{port}.
3) The request result would be sent to u, that redirects her to the page of porting request of MNO_{new}. User sends $< Ad_u, nonce >$ to MNO_{new}.
4) To validate the user request, MNO_{new} asks $SC_{MNO_{new}}$ to confirm the correctness of the $nonce$ (i.e., $Hash'(nonce) == Hash(nonce)$ stored by SC_{port}), and verify $St_{req} == 1$. If the validations are successful, $SC_{MNO_{new}}$ changes the St_{req} to 2.
5) Since the user's data exists in IPFS and only MNO_{old} and the user have access on that, MNO_{new} asks the user to send the plain-text data. User retrieves $EN^{M_{IPFS}}_{S_k}$ from IPFS, using $CID_{EN^M_{S_k}}$. To decrypt M_{IPFS}, she executes the following steps:
   - Retrieves $EN^{S_k}_{Pub_u}$ from SC_U;
   - Decrypts it with Pr_u and retrieves S_k;
   - Decrypts $EN^{M_{IPFS}}_{S_k}$ using S_k and retrieves M_{IPFS}

   Then, user sends M_{user} to MNO_{new}. Note that we call the new version of user data as M_{user}, because the user may change the data without validation. The aim is to make this modification impossible in the next step.
6) MNO receives M_{user} and needs to validate its integrity with the previous version which is validated by MNO_{old}. To do so, $SC_{MNO_{new}}$ retrieves $Hash(M_{IPFS})$ from SC_U that is stored by MNO_{old}. Then validates that $Hash(M_{IPFS}) == Hash(M_{user})$.After successful validation, MNO_{new} generates new symmetric key, S_{k2}, and calculates $EN^M_{S_{k2}}$, $EN^{S_{k2}}_{Pub_u}$ and $EN^{S_{k2}}_{Pub_{MNO}}$. MNO stores $EN^M_{S_{k2}}$ in IPFS and gets $CID_{EN^M_{S_{k2}}}$).
7) MNO requests SC_{port} to delegate the ownership of update function of SC_U to MNO_{new}. SC_{port} gets the record of user request and verifies that $St_{req} == 2$. If the validation is successful, the ownership will be delegated to MNO_{new}. Moreover, SC_{port} sends a transaction to $SC_{MNO_{old}}$ to remove the $Number_u$ from the list of its active users.
8) MNO stores $Attr_u$ into SC_U.

TABLE I: System throughput (BT (s), Throughput (tps))

P	***Switching***							
BS	*30*		*60*			*100*		
BT C	5	10	5	10	15	5	10	15
50	0.79	0.46	0.78	0.79	0.78	0.79	0.79	0.79
100	1.04	0.59	1.52	0.91	0.79	1.51	1.48	1.45
200	1.06	0.61	1.97	0.99	0.78	**2.65**	1.7	1.24
300	1.19	0.64	1.85	1.12	0.84	**2.59**	1.8	1.28
500	1.22	0.73	2.01	1.13	0.85	**2.86**	1.84	1.31
700	1.23	1.01	2.03	1.22	0.99	**2.99**	1.79	1.34

V. Evaluation

To evaluate the proposed method, we simulated the whole procedure in a private Ethereum Blockchain. The smart contracts are written in Solidity language [14]. Following, we provided the performance analysis of the proposed method by evaluating the scalability of the system in terms of the increasing number of concurrent requests. Scalability can be defined as changes in throughput when altering a parameter [15]. We assess the throughput [16]–[18] as:

$$Throughput = \frac{|Tx|}{t}$$

where Tx is the set of transactions, $|Tx|$ is the number of transactions, t is the total time of execution.

We adjusted the Block size (BS), Block time (BT), and Concurrent requests (C) which are the number of transactions fitting into one block, the required time period of extraction of blocks, and the number of users sending concurrent requests, respectively.

Table I depicts the throughput of the system for aforementioned configurations of BS and BT. If the throughput stays almost stable regarding the alteration of parameters, we can claim that the system is scalable [18], [19]. As shown in I, system throughput is almost stable for $C \geq 200$. Therefore, we can claim that **the system is scalable** and can maintain adjustable and low latency in a large-scale request environment for switching procedure. Moreover, Table I provides the throughput of the system in different Blocklchaion configuration. As shown in the table, increasing the BS and decreasing the BT can positively affect the performance by increasing the overall throughput.

VI. Discussion and Future direction

We introduced a novel method for user profile and mobile number portability in MNOs using Blockchain technology. This method can bring high availability, integrity, scalability, and transparency. Moreover, it decreases the IT complexity on the MNO side, reduces imposed switching fees on the user side, enhances the user's control of her data, and delivers better security. The assessments show that the system can provide agile low-cost profile switching between MNOs.

As the proposed method is an ongoing work, some future directions are as follows: 1) to implement the user/MNO subscription procedure and the user subscription termination phases to support the whole procedure of user profile creation, porting, and termination, 2) provide the opportunity for the users to participate in the Blockchain's consensus procedure and propose an incentivization method to encourage them, and 2) provide more assessments about the feasibility of the method, For instance, by evaluating the method on different Blockchain implementations such as Hyperledger Fabric, Quorum, etc., and several consensus models.

References

[1] "Mobile subscriptions forecast – Mobility Report," Nov. 2021, last Modified: 2021-11-30T06:30:56+00:00. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/mobile-subscriptions-outlook

[2] S. Bühler and J. Haucap, "Mobile number portability," *Journal of Industry, Competition and Trade*, vol. 4, no. 3, pp. 223–238, 2004.

[3] Y.-B. Lin, I. Chlamtac, and H.-C. Yu, "Mobile number portability," *IEEE network*, vol. 17, no. 5, pp. 8–16, 2003.

[4] Dong Hee Shin, "A study of mobile number portability effects in the united states," *Telematics and Informatics*, vol. 24, no. 1, pp. 1–14, 2007. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0736585305000626

[5] J. Shah, S. Agarwal, A. Shukla, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain-based scheme for the mobile number portability," *Journal of Information Security and Applications*, vol. 58, p. 102764, 2021.

[6] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5g and beyond networks: A state of the art survey," *Journal of Network and Computer Applications*, vol. 166, p. 102693, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804520301673

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[8] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[9] N. Szabo, "Secure property titles with owner authority," *Online at http://szabo. best. vwh. net/securetitle. html*, 1998.

[10] D. Krishnaswamy, K. Chauhan, A. Bhatnagar, S. Jha, S. Srivastava, D. Bhamrah, and M. Prasad, "The design of a mobile number portability system on a permissioned private blockchain platform," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2019, pp. 90–94.

[11] W.-E. Chen and Y.-L. Ciou, "Enum-based number portability for mobile communication networks," *Journal of Internet Technology*, vol. 20, no. 1, pp. 135–145, 2019.

[12] J. Odii, M. Onyesolu, and C. Onukwugha, "A hybrid call routing framework for mobile number portability in nigeria," *Int Res J Comput Sci (IRJCS)*, vol. 3, pp. 9–17, 2014.

[13] J. Chen, X. Xia, D. Lo, J. Grundy, X. Luo, and T. Chen, "Defining smart contract defects on ethereum," *IEEE Transactions on Software Engineering*, 2020.

[14] C. Dannen, *Introducing Ethereum and solidity*. Springer, 2017, vol. 1.

[15] M. Schäffer, M. d. Angelo, and G. Salzer, "Performance and scalability of private ethereum blockchains," in *International Conference on Business Process Management*. Springer, 2019, pp. 103–118.

[16] F. Ghaffari, E. Bertin, N. Crespi, S. Behrad, and J. Hatin, "A novel access control method via smart contracts for internet-based service provisioning," *IEEE Access*, vol. 9, pp. 81 253–81 273, 2021.

[17] F. Ghaffari, E. Bertin, and N. Crespi, *A Novel Approach for Network Resource Sharing via Blockchain*. New York, NY, USA: Association for Computing Machinery, 2021, p. 50–52. [Online]. Available: https://doi.org/10.1145/3472716.3472867

[18] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," *IEEE Network*, vol. 33, no. 5, pp. 166–173, 2019.

[19] P. W. Eklund and R. Beck, "Factors that impact blockchain scalability," in *Proceedings of the 11th international conference on management of digital ecosystems*, 2019, pp. 126–133.