Blockchain Benefits for MAAS

Pascal Urien
Information Processing and Communication Laboratory (LTCI)
Telecom Paris
Saclay, France
Pascal.Urien@Telecom-Paris.fr

***Abstract*—This paper introduces blockchain services for Mobility As A Service (MAAS) infrastructures, allowing to use public or private modes of transport during a trip. The blockchain system interacts with three classes of blockchain accounts: User, MAAS, and transport operators. It details some possible scenari and associated transactions. It demonstrates that this concept is realistic with emerging and existing technologies.**

Keywords- Blockchain; Trust; Security; NFC

I. INTRODUCTION

The Mobility As A Service (MAAS, [1]) is an emerging concept, born in 2014 in Finland [2], allowing to use public or private modes of transport during a trip (see Figure 1). It involves the unification of mobility services, and a fusion of ticketing and multimodal information tools. According to [2] "*The ecosystem consists of the transport infrastructure, transportation services, transport information and payment services*".

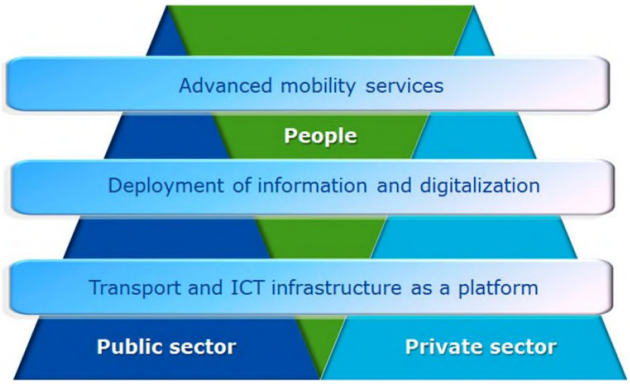

Figure 1. Mobility As A Service, MAAS

In this smart city context [10], many modes of transport are implemented such as bicycles, electric scooters, scooters, electric cars, buses, metro, and taxis. Some of them (generally private) rely on mobile applications associated with bank cards; others require tickets delivered by dedicated machines or subscription cards. In Helsinki, the WHIM app [9] offers several subscriptions; for example a monthly package of 499 Euros, including unlimited public transport, taxis (up to 5 km), car-sharing and cycling.

In this paper we introduce the concept of blockchain services for MAAS. The MAAS is a federation of transport operators, managing ticketing services and validators. The main idea is to store these tickets in blockchain interacting with several entities (transport operator, user, MASS operators) as illustrated by Figure 2.

The paper is constructed according to the following outline. Section 2 presents blockchain benefits for MAAS, and some existing concepts. Section 3 introduces our use case. Section 4 details the functional architecture. Finally section 5 concludes this paper.

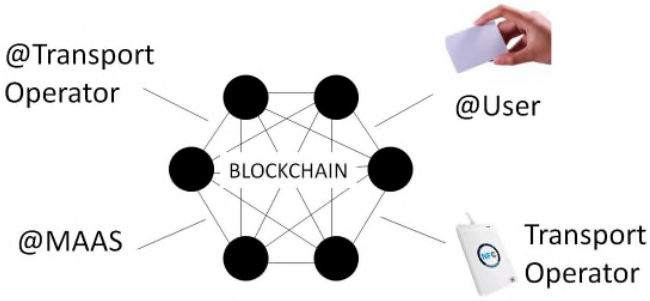

Figure 2. Actors involved in blockchain services for MAAS.

II. STATE OF ART

The first blockchain was deployed in 2009 by Satoshi Nakamoto [3], an anonymous creator (or group of creators). Bitcoin has had remarkable success, with a price reaching $20,000 at the end of 2017, for a valuation of $ 340 billion. Originally the blockchain carried out the transfer of crypto currency, but since 2015, several platforms appeared, such as Ethereum [4] or Hyperledger, which also allow the exchange of data or the execution of programs (smart contracts) charged in crypto currency.

The services delivered by a blockchain are as follows:

- Generation of signed transactions:
- Gathering of transactions by a P2P (*Peer To Peer*) network;

 ISBN: 978-1-61208-805-1

- Creation of transaction blocks by nodes of the P2P network.
- Chaining a new block to the existing block list (the blockchain), according to a consensus mechanism such as PoW (*Proof of Work*) or PoS (*Proof of Stake*).

The main contribution of blockchain is the creation of trust, based on consensus, i.e., there is no trusted third party. Transactions are authenticated by cryptographic signatures and are time-stamped, when they are mined (i.e., inserted in a block). The database storing these blocks is very widely duplicated in nodes of the P2P network; WEB APIs allow ubiquitous and secure access to data hosted by the blockchain infrastructure.

In the absence of a trusted third party, participants generate their keys. A private key is usually a 32 bytes (256 bits) random number, from which a public key and the blockchain account identifier are calculated. Blockchain is by nature based on a consensus of players, and therefore could be the technological cornerstone of the new MAAS mobility, bringing together multiple players.

An example of this concept is the "planar networks" project [5], which uses Ethereum smart contracts (see Figure 3), for implementation of universal ticketing system.

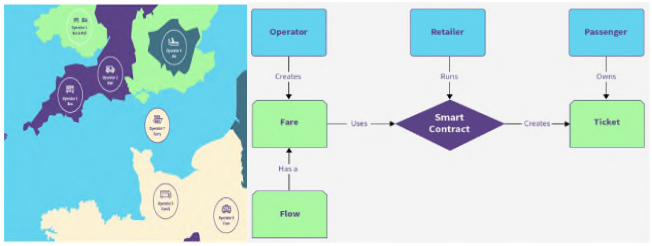

Figure 3. The planar networks project uses Smart Contracts for implementation of universal ticketing system.

The creation of crypto currencies dedicated to MAAS is also an opportunity. The DOVU project [6] deploys a crypto currency (see Figure 4) dedicated to multimodal mobility services.

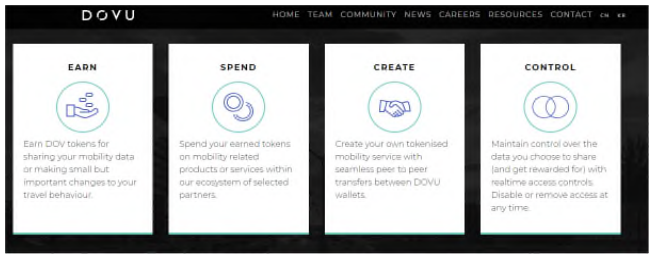

Figure 4. The DOVU project

III. USE CASE

This section details an experimental implementation of the concept of "Blockchain for MAAS". The latter uses the ROPSTEN (Ethereum) test blockchain, a Near Field Communication (NFC) chip card performing transaction signature, and free software (BTOOLS [7]).

A. *Blockchain Ticket*

Figure 5. A French SNCF ticket

In order to clarify our approach, we consider the e-ticket illustrated in Figure 5. Reading the QR-Code (located at the top right) by a dedicated validator allows access to the mobility service. The ticket (content of the QR code) is a series of ASCII characters illustrated by the left part of Figure 6.

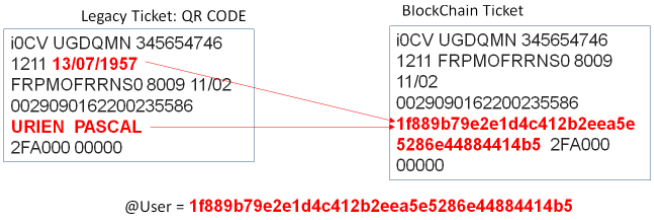

Figure 6. Legacy Ticket (left) and blockchain ticket (right)

B. *Blockchain MASS entiies*

Three types of blockchain accounts are involved in MAAS:

- User accounts, using addresses, deduced from previously generated private keys.
- MAAS entities, identified by their addresses.
- Transport operators, identified by their addresses.

Figure 7 lists the MAAS actors (MASS entity, user, transport operator), and their associated addresses in the ROPSTEN blockchain. Transactions can be retrieved at [11].

Entity	**Ropsten Blockchain Address**
User account	1f889b79e2e1d4c412b2eea5e5286e44884414b5
MAAS	266abe4b01ce1899100c36c3d33e872b52cb12d8
Transport operator	11baa7742ff512acc35b86d2c1b02391d533a4b2

Figure 7. MAAS actors and their ROPSTEN adresses.

IV. FUNCTIONNAL ARCHITECTURE

The functional architecture of MAAS is illustrated in Figure 8. Three types of services are supported, the ticket generation, the ticket transfer to user, and the ticket use in a transport network.

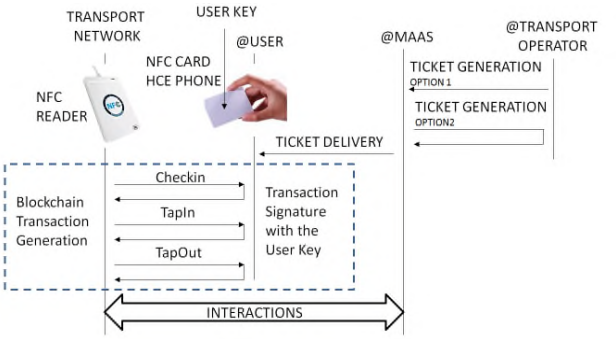

Figure 8. Functionnal Architecture

A. *Ticket Generation*

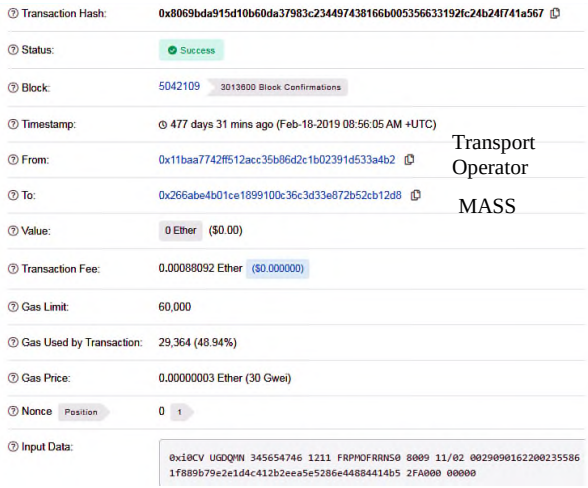

Figure 9. Ticket generation from the transport operator to the MASS.

The basic idea is to store the ticket in the blockchain account of the MAAS entity. Two modes of ticket generation are possible:

- Option 1: the transport operator generates the ticket in a transaction, whose recipient is the MAAS entity. This option is illustrated in Figure 9. This transaction can be retrieved at [12].
- Option 2: MAAS generates the ticket in a self addressed transaction. This transaction is illustrated in Figure 10; it can be retrieved from [13].

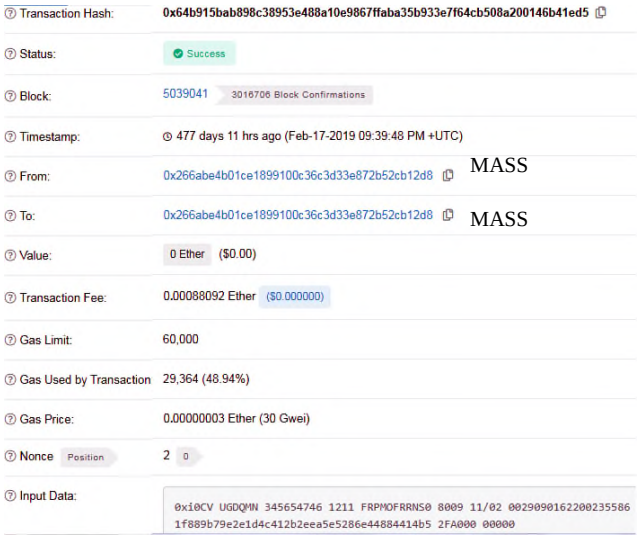

Figure 10. Ticket generation from the MASS to MASS.

B. *Ticket Transfer to User*

The MAAS transfers the ticket to the client in a transaction, as illustrated in Figure 11. The ticket is thereafter stored in the client's blockchain account. This transaction can be retrieved at [14].

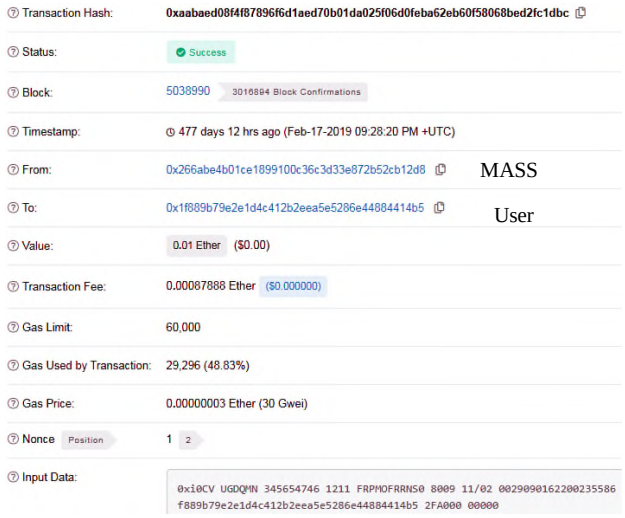

Figure 11. Ticket Transfer from MAAS to user

C. *Ticket Use*

The user is equipped with a Near Field Communication (NFC) card or a Host Card Emulation (HCE) smartphone. The NFC card (possibly virtual) hosts the private key associated to the blockchain account, and is able of carrying out the transaction signature.

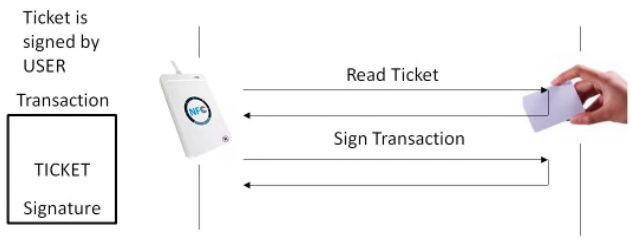

Figure 12. Illustration of the *CheckIn scenario*.

In an off-line approach (*Checkin* scenario, see Figure 12), the NFC card stores a ticket linked to an address, whose authenticity is proven by a signature, calculated using the private key. The user's blockchain address can be associated with a certificate issued by the MAAS, if a static authentication mechanism (off-line) is required.

In an on-line approach (*TapIn, TapOut* scenario), similar to payment by contactless bank card in the London Underground, proof of customer identity is required at the start and end of the mobility service. The ticket (or contract) can be stored in the MAAS account, or paid by using a dedicated crypto currency.

Figure 13. Illustration of the *TapIn, TapOut scenario*

1) *Checkin Transaction.*

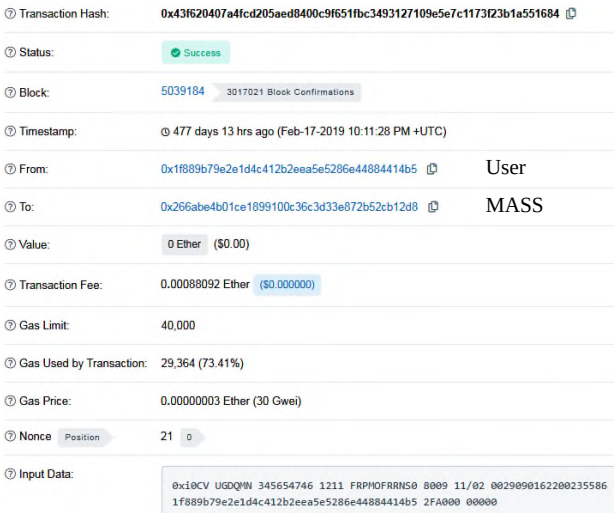

Figure 14. Illustration of a Checkin Transaction

Figure 14 illustrates a transaction between user and MAAS entity which contains the ticket. It can be retrieved at [15]. This latter is authenticated by the signature generated using the private key bound to the user account.

2) *TapIn, TapOut Transactions.*

Figures 15 and 16 illustrate respectively the *TapIn* and *TapOut* procedures. These transactions can be respectively retrieved at [15] and [16]. A self transaction, addressed to the user, proves its identity, and is thereafter time stamped by the blockchain infrastructure

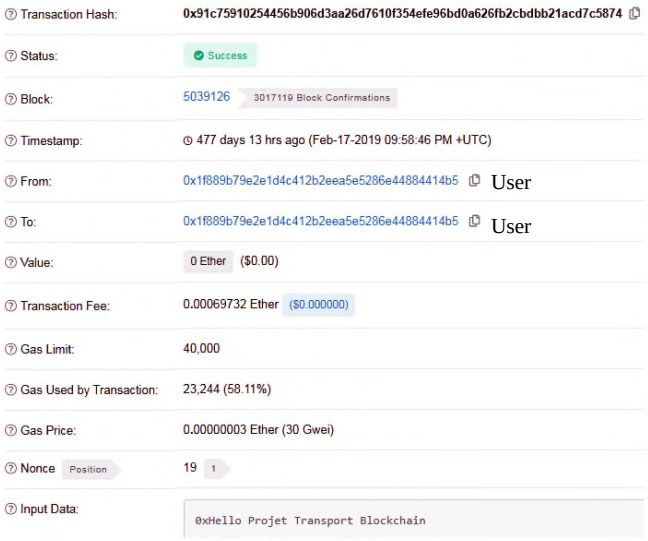

Figure 15. A TapIn transaction, proving the user identity, recorded and time stamped by the blockchain.

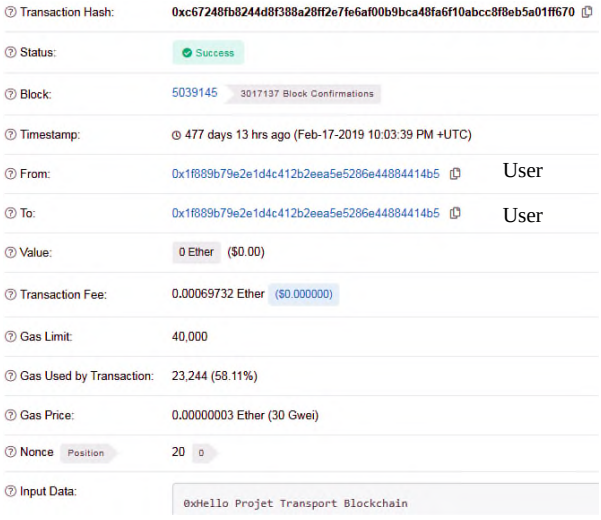

Figure 16. A TapOut transaction, proving the user identity, recoreded and time stamped by the blockchain.

V. CONCLUSION

In this paper we presented a blockchain infrastructure dedicated to MAAS services, which comprises three actors, MAAS entity, transport operator and user. A ticket can be generated in MAAS to MASS transaction or in transport

operator to MAAS transaction. The MAAS transfers this ticket to user account. Validators of the transportation system check ticket according to two operating modes *CheckhIn* and *TapIn-TapOut*. In the first mode the user generates a transaction to the MAAS entity in which the ticket in inserted; the ticket is bound to user's identity and its use is time stamped by the blockchain. In the second mode the user proves its blockchain identity by self-addressed transaction; thereafter the transport system checks its subscription.

In summary blockchain could create very attractive technological platform for MAAS services, due to the lack of third trusted party. Nevertheless such infrastructures should provide the required level of performances.

REFERENCES

[1] https://en.wikipedia.org/wiki/Mobility_as_a_service, accessed September 2020

[2] "Mobility as a Service - the new transport paradigm". June 2014, https://www.lvm.fi/, accesed September 2020

[3] S. Nakamoto, S., "Bitcoin: A peer-to-peer electronic cash system", 2008

[4] W. Gavin, Ethereum Yellow Paper, "Ethereum : a Secure Decentralised Generalised Transaction Ledger", EIP-150, 2015, http://yellowpaper.io, seen september 2020.

[5] The Planar Network Blockchain Transport, https://planar.network/assets/docs/whitepaper.pdf, retrieved September 2020.

[6] DOVU: a unified token, wallet and marketplace for earning and spending mobility related rewards, https://dovu.io/, retrieved September 2020.

[7] P. Urien et al., "BTOOLS: Trusted Transaction Generation for Bitcoin and Ethereum Blockchain Based on Crypto Currency SmartCard", ICDT 2018, The Thirteenth International Conference on Digital Telecommunications

[8] P. Urien, "Towards secure elements for trusted transactions in blockchain and blockchain IoT (BIoT) Platforms", Fourth International Conference on Mobile and Secure Services (MobiSecServ), 2018.

[9] WHIM application, https:// https://whimapp.com/, retrieved September 2020.

[10] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for Smart Cities," in IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22-32, Feb. 2014.

[11] Ropsten Testnet Explorer, https://ropsten.etherscan.io, retrieved September 2020.

[12] Ticket generation from the transport operator to the MASS. https://ropsten.etherscan.io/tx/0x8069bda915d10b60da37983c234497438166b005356633192fc24b24f741a567, retrieved September 2020

[13] Ticket generation from the MASS to MASS, https://ropsten.etherscan.io/tx/0x64b915bab898c38953e488a10e9867ffaba35b933e7f64cb508a200146b41ed5, retrieved Sseptember 2020

[14] Ticket Transfert from MAAS to user, https://ropsten.etherscan.io/tx/0xaabaed08f4f87896f6d1aed70b01da025f06d0feba62eb60f58068bed2fc1dbc, retrieved September 2020.

[15] Checkin Transaction, https://ropsten.etherscan.io/tx/0x43f620407a4fcd205aed8400c9f651fbc3493127109e5e7c1173f23b1a551684, retrieved September 2020

[16] TapIn transaction, https://ropsten.etherscan.io/tx/0x91c75910254456b906d3aa26d7610f354efe96bd0a626fb2cbdbb21acd7c5874, retrieved September 2020

[17] TapOut transaction, https://ropsten.etherscan.io/tx/0xc67248fb8244d8f388a28ff2e7fe6af00b9bca48fa6f10abcc8f8eb5a01ff670, retrieved September 2020

 ISBN: 978-1-61208-805-1