CoinCar : Système décentralisé de location de voitures entre particuliers fondé sur la blockchain BitCoin

----

IF-4-SERE

Use case

CoinCar allows individuals to rent out their cars (a sort of AirBnB for cars, or OuiCar) or other vehicles.

We assume that the cars are smart connected cars. Each car is equipped with a long range communication module (for example, 3G/4G) as well as a short range communication module (for example, Bluetooth, NFC). This implies that the car can communicate over the Internet as well as with user devices (such as smartphones) located in the vicinity.

Cars are electronically accessible by users through their smart phones. A car grants access only to a user who is authorized.

At any given time, a car has one owner, and can have one or no renter. The owner of the car can authorize one (and only one) renter at a time to access and use the car for a fixed duration. The owner of the car can also transfer ownership of the car, that is, sell the car to another user.

The owner of a car can publish the availability of the car for some chosen dates, as well as the rent/unit of time, address, and other details of the car (brand, model, etc.).

Renters can search for available cars that correspond to their preferred criteria. They can specify the desired location, rent, type, reputation (see below), etc.

When a renter discovers an available car that he wishes to rent, he sends a request to the owner for a specific duration along with mandatory credentials, which include national identity card (or equivalent document), driving license, and insurance. The owner can then approve the request by granting access to the renter for the requested duration.

The renter is able to access the car during the authorized duration. However, a condition for access is that the renter pays in advance for the entire duration. The car is locked down after the duration expires. Moreover, the car monitors its location and limits the mobility of the car as defined and published by the owner (e.g., no trip abroad).

The system also manages the reputation of the cars as well as the renters. After each car rental transaction, the renter can leave a rating and a comment about the car (for example, about its cleanliness, performance, etc.) and the owner of the car can do the same about the renter (for example, if he returned the car in a good condition). The feedback by the renter can be given in an open manner (that is, the owner knows the identity of the renter) or it can be given in a private ("anonymous") manner (that is, the owner does not learn the identity of the renter). The same applies for the feedback given by the owner. Note: we will not consider the inference of a feedback provider's identity in this TD.

The purpose of the TD is to study and design a solution for implementing the CoinCar service on top of the Bitcoin blockchain.

Exercise 1 (identity management) (Bitcoin address)

There is no central authority to issue or manage identities on the Bitcoin blockchain.

Describe how identities are generated for users (owners, renters, car manufacturers) such that they are uniquely identified on the blockchain.

Calculate the probability that two users will both generate the same identity (address collision) if there are 7 billion users in total (approximately the population of Earth). Note: There are 2^160 possible Bitcoin addresses.

Exercise 2 (car ownership) (smart property, asset management, colored coins)

Describe how cars can be represented on the blockchain. We assume that a car is assigned a universally unique serial number by the manufacturer.

Write a protocol for a car manufacturer to transfer the ownership of a new car to the first owner.

Write a protocol for an owner of the car to sell the car to another person.

Write a protocol for an owner to prove the ownership of a car to a renter.

Exercise 3 (advertisement)

Describe a scheme for an owner to publish the availability of a car on the blockchain.

Exercise 4 (credential exchange)

Write a protocol for the renter to send his credentials to the owner using another channel (such as email) while leaving a verifiable trace of the credentials on the blockchain. Authorities can indeed later demand the owner to disclose the credentials and verify their integrity. How can the renter also preserve the confidentiality of the credentials from the public ?

Exercise 5 (delegation of usage) (smart contracts)

Write a protocol for the owner of a car to delegate a temporally limited usage (renting of the car) to a user ?

The renter gets access to the car only if he pays the rent in full in advance.

Discuss how such a delegation of usage could be implemented using smart contracts[1] (like the ones available in Ethereum) ?

Exercise 6 (driver authentication)

Write a protocol for a car to authenticate a user in order to grant access ?

Exercise 7 (tax recovery)

Write an algorithm for a taxation authority to calculate the revenue earned by a car owner ?

Exercise 8 (alternative blockchain)

Discuss the pros and the cons of using the Bitcoin blockchain ?

Identify and discuss alternative solutions based on public blockchains ?

Identify issues to consider (…and propose solutions!) if one decides to implement the CoinCar service on top of a private blockchain ?

[1] Cf. for instance : Smart Contracts: The Blockchain Technology That Will Replace Lawyers http://blockgeeks.com/guides/smart-contracts/ and Smart Contracts Explained: http://www.blockchaintechnologies.com/blockchain-smart-contracts.