LESSON SC 1 – Smart Car Renting Service

University of West Attica

Department of Electrical and Electronics Engineering
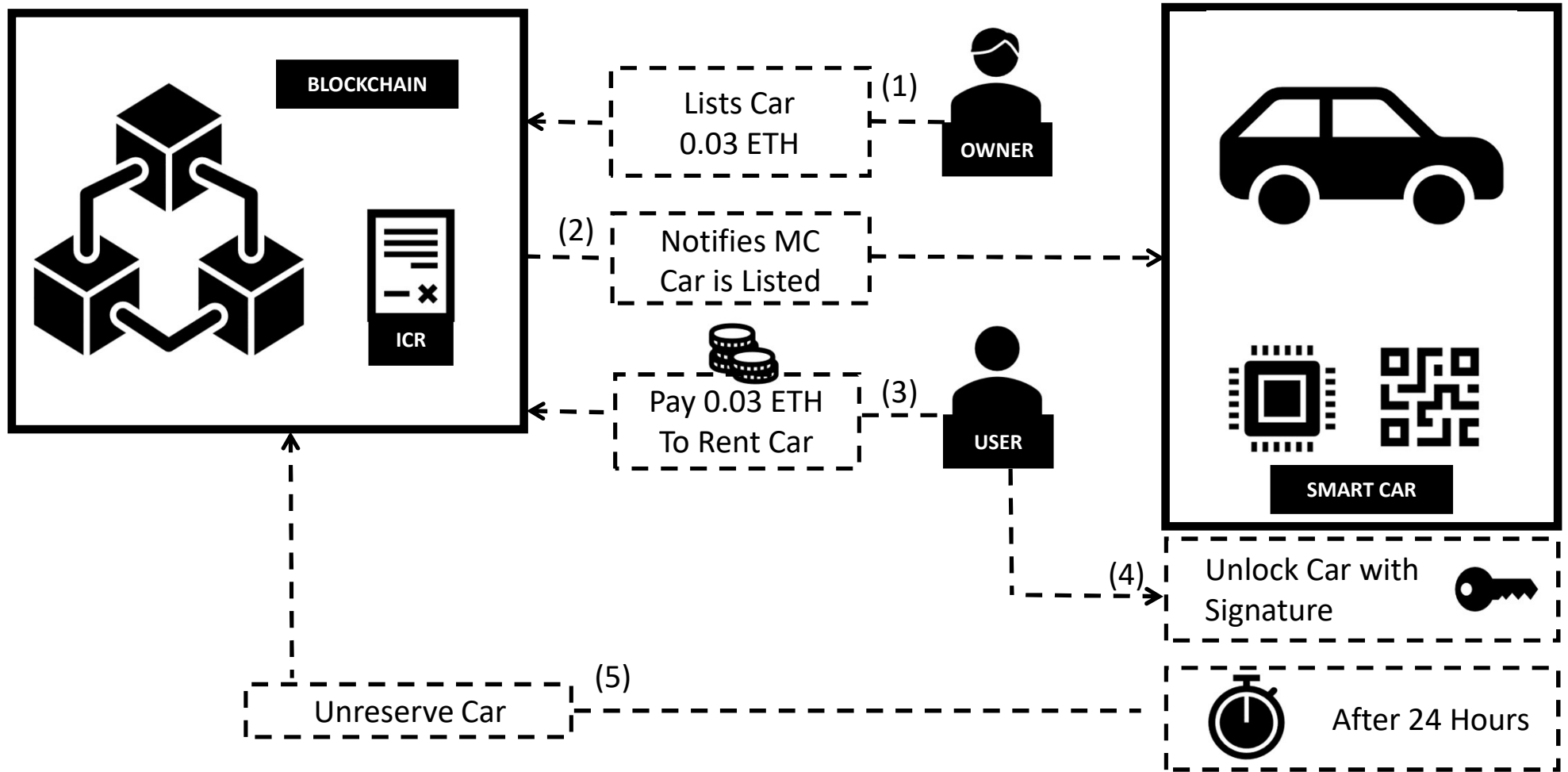
Ioannis Christidis

Christoforos Kachris

Concept

We are building the smart contracts for a **Decentralized Instant Smart Car Renting Service (ICR)**.

We assume that an ***Innovative IoT Company (IIoTC)*** provides the service of installing *Smart Devices* in cars, allowing them to be rented using an ICR Decentralized Application (DApp).

Smart Car Fleet Owners list their cars for rent to the ICR DApp.

Users of ICR DApp are able to find cars and rent them for a day by paying the renting-cost in ETH.

Smart Devices control who has access to the cars they are installed on.

BLOCKCHAIN

ICR

Lists Car
0.03 ETH

(1)

OWNER

(2) Notifies MC
Car is Listed

Pay 0.03 ETH
To Rent Car

(3)

USER

SMART CAR

(4) Unlock Car with
Signature

Unreserve Car **(5)**

After 24 Hours

Scenario

IIoTC has installed a **Smart Device (microcontroller - MC)** on a car.

1. The **owner** of the car _lists_ it in the ICR for `0.3` ETH.

2. **ICR SC** _notifies_ the **MC** installed on the car that it is listed.

3. **User** _pays_ `0.3` ETH to rent the car on the **ICR SC**. The car is now _reserved_ for the **User**.

4. **User** tries to _unlock_ the car with their **signature** (explained on the next slide).

5. After 24 hours the **MC** _unreserves_ the car.

What is a **Signature**?

An _Ethereum Signature_ is a _cryptographic proof generated by signing a message (e.g. "Hello World") or transaction with the private key_ of an Ethereum account. It is _a way to prove ownership of an account without revealing the private key_. Messages can be signed, using a blockchain wallet like MetaMask. (We will not dive deeper into this concept in this course, but we will use the signatures later.)

Key takeaways for the course: If we have the **signature of an account** and the **message it signed,** we can **retrieve the address of the account without exposing their private key**. We will see an example of that later.

In our project, we will use the signature to ensure that the entity that tries to unlock the car is the user that rented the car in our ICR SC.

Outro

In the next lesson we will start building our Smart Contract.