Law, Science and Technology
MSCA ITN EJD n. 814177

RI☰E
Rights of Internet of Everything

Mirko Zichichi[1,2], Stefano Ferretti[3],
Gabriele D'Angelo[2]

[1]Universidad Politécnica de Madrid
[2]University of Bologna
[3]University of Urbino "Carlo Bo"

MOVO: a dApp for DLT-based
Smart Mobility

Overview

Introduction

Smart Mobility Systems (SMS)

Smart Mobility Systems have emerged as way to efficiently improve mobility, travel security and increase the options for travellers

Smart Mobility Systems (SMS)

Smart Mobility Systems have emerged as way to efficiently improve mobility, travel security and increase the options for travellers

- Vehicles and infrastructures are becoming increasingly "smarter" → equipped with sensors that track a huge amount of different types of information

Smart Mobility Systems (SMS)

Smart Mobility Systems have emerged as way to efficiently improve mobility, travel security and increase the options for travellers

- Vehicles and infrastructures are becoming increasingly "smarter" $\rightarrow$ equipped with sensors that track a huge amount of different types of information
- Smartphones and IoT devices enables individuals' ubiquitous connectivity and the ability to collect personal information and/or crowdsensing data

Smart Mobility Systems (SMS)

Smart Mobility Systems have emerged as way to efficiently improve mobility, travel security and increase the options for travellers

- Vehicles and infrastructures are becoming increasingly **"smarter"** $\rightarrow$ equipped with sensors that track a huge amount of different types of information
- Smartphones and IoT devices enables individuals' ubiquitous connectivity and the ability to collect personal information and/or crowdsensing data

Our aim
$\rightarrow$ transparent and self-managed system for SMS users to exchange **data and services**

Smart Mobility Systems (SMS)

Smart Mobility Systems have emerged as way to efficiently improve mobility, travel security and increase the options for travellers

- Vehicles and infrastructures are becoming increasingly **"smarter"** $\rightarrow$ equipped with sensors that track a huge amount of different types of information
- Smartphones and IoT devices enables individuals' ubiquitous connectivity and the ability to collect personal information and/or crowdsensing data

Our aim
$\rightarrow$ transparent and self-managed system for SMS users to exchange **data and services**

MOVO
app acting within the SMS framework and exploiting the combination of several decentralized technologies

Technologies

Veicular Ad-hoc NETwork

· Wireless communication network between moving vehicles

Veicular Ad-hoc NETwork

- Wireless communication network between moving vehicles
- **Application Unit (AU)** ← device inside the vehicle that communicates with the vehicle's **On-Board Unit (OBU)**. They communicate with RSUs:

Veicular Ad-hoc NETwork

- Wireless communication network between moving vehicles
- **Application Unit (AU)** ← device inside the vehicle that communicates with the vehicle's **On-Board Unit (OBU)**. They communicate with RSUs:
- **Road Side Units (RSUs)** ← devices that are usually fixed along the side of the road to provide services to drivers.

Distributed Ledger Technologies (DLT)

Data ledger distributed among a network of peer nodes, where data are written in the form of transactions.

Distributed Ledger Technologies (DLT)

Data ledger distributed among a network of peer nodes, where data are written in the form of transactions.
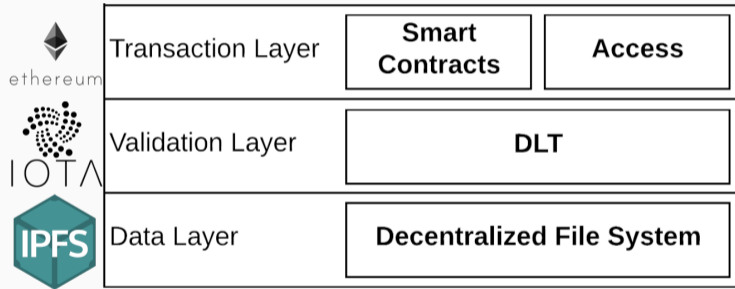
Shift trust from a third party intermediary to a consensus mechanism;
Guarantee **data validation** through transparency and immutability;
Enable **direct interactions and agreements** between users.

Smart Contracts

- **Ethereum** → blockchain that integrates a (quasi-)Turing-complete language in the form of smart contracts.

Smart Contracts

- **Ethereum** $\rightarrow$ blockchain that integrates a (quasi-)Turing-complete language in the form of smart contracts.
- Once a smart contract is issued in the blockchain, its **instructions** are **immutable** and will be executed **deterministically**.

Smart Contracts

- **Ethereum** → blockchain that integrates a (quasi-)Turing-complete language in the form of smart contracts.
- Once a smart contract is issued in the blockchain, its **instructions** are **immutable** and will be executed **deterministically**.
- Business logic execution → semi-autonomously move **assets** (i.e. tokens and cryptocurrencies) as the result of an **agreement between two parties**.

Smart Contracts

- **Ethereum** → blockchain that integrates a (quasi-)Turing-complete language in the form of smart contracts.
- Once a smart contract is issued in the blockchain, its **instructions** are **immutable** and will be executed **deterministically**.
- Business logic execution → semi-autonomously move **assets** (i.e. tokens and cryptocurrencies) as the result of an **agreement between two parties**.
- **Data Access Control**
  Access to the data can be **purchased** or **allowed by the owner** through dedicated smart contract methods

IOTA Masked Authentication Messaging Channels

- **IOTA** $\rightarrow$ network of nodes that holds a distributed ledger where transactions are validated without fees
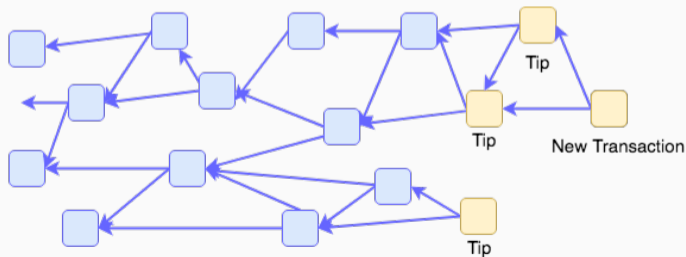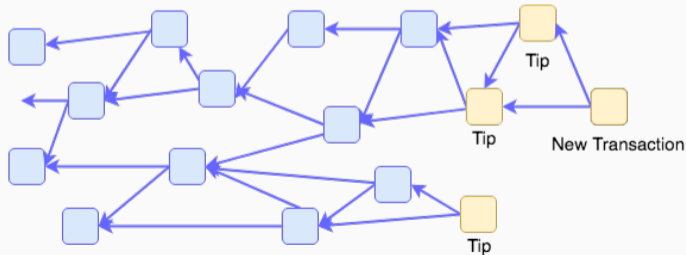
IOTA Masked Authentication Messaging Channels

- **IOTA** → network of nodes that holds a distributed ledger where transactions are validated without fees
- **Masked Authenticated Messaging (MAM)** → communication protocol that adds the functionality to emit and access an encrypted data channels over IOTA

IPFS

- **Decentralized File Storages (DFS)** → overcome typical scalability and privacy issues of DLTs and cloud services, while maintaining the benefits of decentralization

IPFS

- **Decentralized File Storages (DFS)** → overcome typical scalability and privacy issues of DLTs and cloud services, while maintaining the benefits of decentralization
- **InterPlanetary File System (IPFS)** → A DFS that builds a file system over a peer-to-peer network.

IPFS

- **Decentralized File Storages (DFS)** $\rightarrow$ overcome typical scalability and privacy issues of DLTs and cloud services, while maintaining the benefits of decentralization
- **InterPlanetary File System (IPFS)** $\rightarrow$ A DFS that builds a file system over a peer-to-peer network.
- Uses **data digest** as identifier, i.e. CID $\leftarrow$ hash pointer

Affdex

- Emotion measurement technology able to recognize human emotions based on facial cues or physiological responses.

Affdex

- Emotion measurement technology able to recognize human emotions based on facial cues or physiological responses.
- **Facial Action Coding System (FACS)** → face and facial landmark detection, face texture feature extraction, facial action classification and emotion expression modelling.

Affdex

- Emotion measurement technology able to recognize human emotions based on facial cues or physiological responses.
- **Facial Action Coding System (FACS)** $\rightarrow$ face and facial landmark detection, face texture feature extraction, facial action classification and emotion expression modelling.
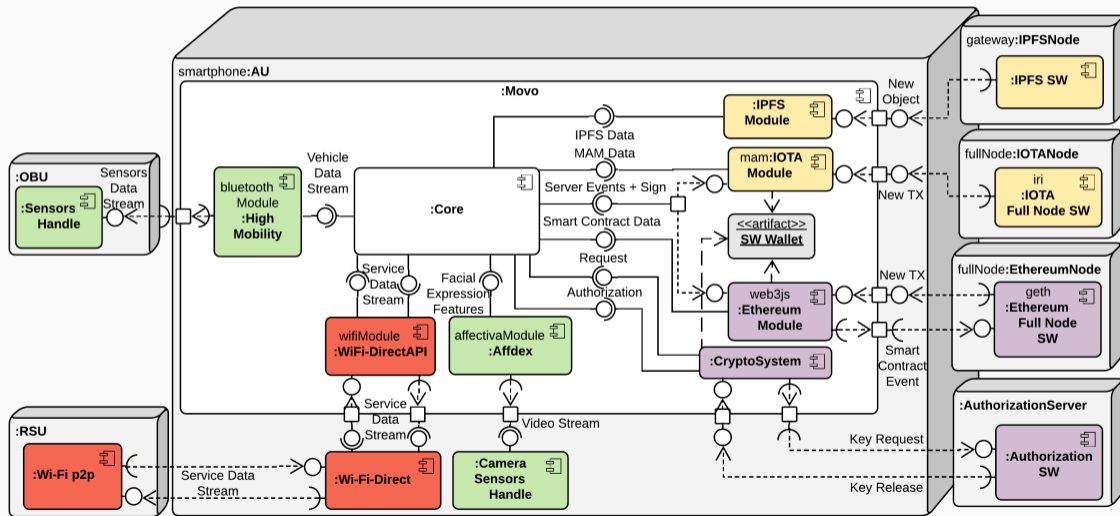- Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN)

MOVO

MOVO Communication
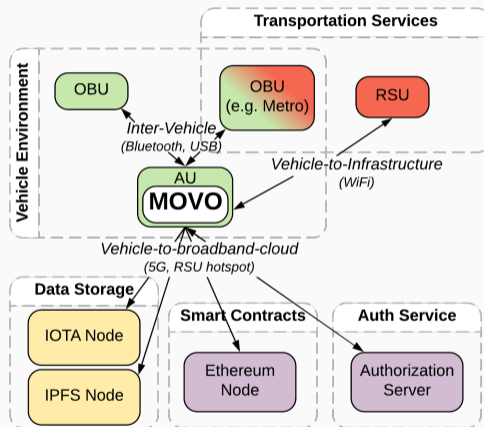
Movo dApp is at the heart of a DLT-based Middleware system built for mobility in SMS

MOVO Implementation

Collection and Sharing of Sensors' Data

- **Vehicle Environment.** Movo dApp is designed to work **inside a vehicle**, connected to the OBU and directly accessible by the driver.

Collection and Sharing of Sensors' Data

- **Vehicle Environment.** Movo dApp is designed to work **inside a vehicle**, connected to the OBU and directly accessible by the driver.
- **Data Storage.** Encrypted sensors data are stored directly in IPFS and then indexed through the use of MAM Channels. **Off-chain storage** $\rightarrow$ (i) higher availability for data reads, (ii) better performances for data writes, (iii) compatible with data protection requirements.

Collection and Sharing of Sensors' Data

- **Vehicle Environment.** Movo dApp is designed to work **inside a vehicle**, connected to the OBU and directly accessible by the driver.
- **Data Storage.** Encrypted sensors data are stored directly in IPFS and then indexed through the use of MAM Channels. **Off-chain storage** $\rightarrow$ (i) higher availability for data reads, (ii) better performances for data writes, (iii) compatible with data protection requirements.
- **Smart Contracts for Data Sharing.** Access to the data through specifying an entitled Ethereum address in a **smart contract**. The release of keys for accessing the encrypted data is executed by an **authorization service** that check on the smart contract.

Fruition of DLT-based Services

- **Transportation Services.** RSUs can offer various services to drivers and Movo makes use of those through a direct communication, e.g. issuing of location certificates by 'trusted' RSUs.

Fruition of DLT-based Services

- **Transportation Services.** RSUs can offer various services to drivers and Movo makes use of those through a direct communication,e.g. issuing of location certificates by 'trusted' RSUs.
- **Smart Contracts for Services.** Users and service providers can create ad-hoc smart contracts for the provision of services in SMS. Ethereum ERC20 Token for the payment of smart contract based services.

Fruition of DLT-based Services

- **Transportation Services.** RSUs can offer various services to drivers and Movo makes use of those through a direct communication,e.g. issuing of location certificates by 'trusted' RSUs.

- **Smart Contracts for Services.** Users and service providers can create ad-hoc smart contracts for the provision of services in SMS. Ethereum ERC20 Token for the payment of smart contract based services.

- **State channels and Micropayments.** design pattern for instant DLT transactions made off-chain, where only the first and the last payment transactions are stored into the ledger.
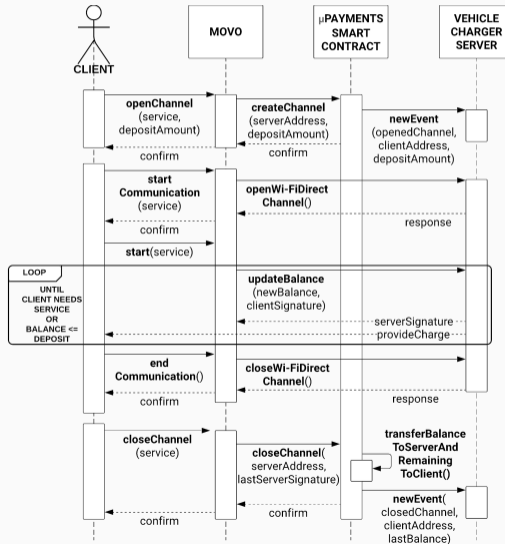
Use cases

Vehicle Insurance Monitoring Scenario
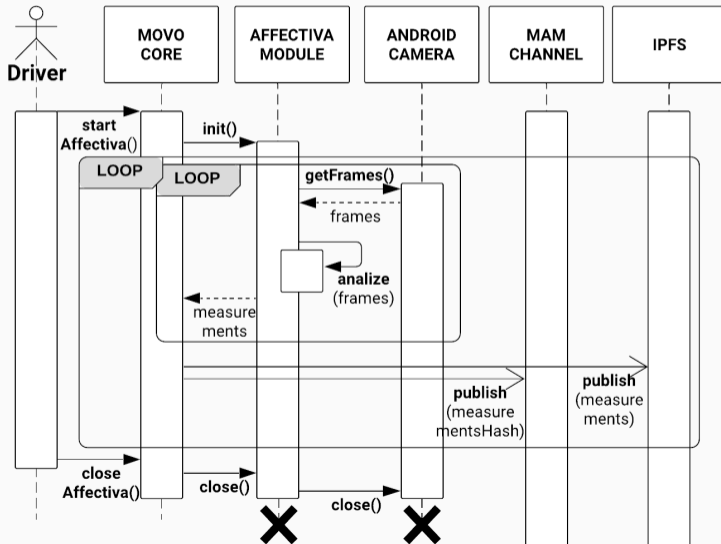
Vehicle Insurance Monitoring Scenario
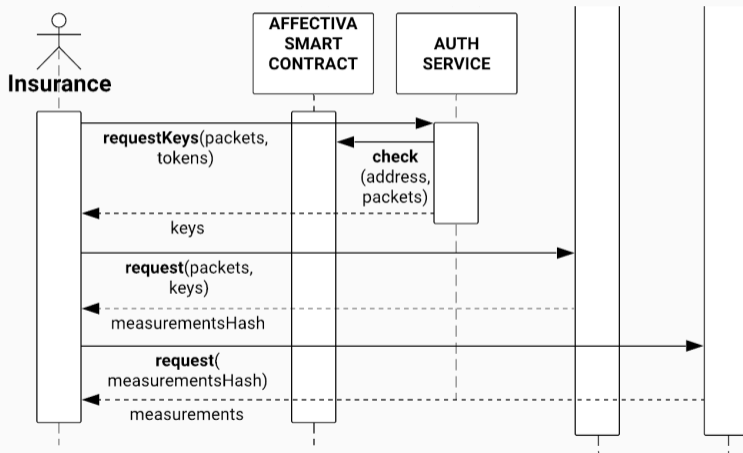
Electric Car Charging Service Scenario

Data sizes and frequencies in the use-case scenarios

Scenario	Sensor Data	Size	Frequency	TOT
Insurance Monitoring	Camera frame	~100KB (640x480px)	10/sec	~60MB/min (IPFS)
Insurance Monitoring	Camera frames hashes	1 MAM message (3 TXs)	1/20sec	3/min (IOTA)
MyMovoMechanic Service	Vehicle data point	~300Bytes (256 chars + JSON + timestamp)	90/sec	~1.62MB/min (IPFS)
MyMovoMechanic Service	Vehicle data point hashes	1 MAM message (3 TXs)	1/20sec	3/min (IOTA)
Charging Service	Open/Close payment channel	1 Ethereum TX	2 per service	2 TXs (Ethereum)
Charging Service	Off-chain balance update msgs	1 Wi-Fi Direct msg	Several per session	Several (off-chain)

Conclusion

Conclusion

- **Movo**, a DLT-based mobile dApp that allows drivers to manage and distribute **data** produced by vehicles and users, while on the move, and to use DLT-based **services**

Conclusion

- **Movo**, a DLT-based mobile dApp that allows drivers to manage and distribute **data** produced by vehicles and users, while on the move, and to use DLT-based **services**
- Movo can interact with the vehicle, uses the **IOTA Tangle and IPFS** to store data in a decentralized way

Conclusion

- **Movo**, a DLT-based mobile dApp that allows drivers to manage and distribute **data** produced by vehicles and users, while on the move, and to use DLT-based **services**
- Movo can interact with the vehicle, uses the **IOTA Tangle and IPFS** to store data in a decentralized way
- **Ethereum smart contracts** allows authorized users to get access to data and services