AutoID

Self-Sovreign decentralized and distributed Vehicle Identification System

WANXIANG Hackaton Shanghai 2019

The International Team

Ted From Shenzen (memolabs.io)

Jack from Shanghai (Developer)

Enrico From Italy (commerc.io)

Johnny from Italy (commerc.io)

Background

- Enrico and Johnny last month had a meeting in Stuttgart, Germany with a **BIG** Automotive company senior top management (who ask us to remain nameless)
- We presented them our Documents Blockchain™ project and asked them to give us **A SUPER IDEA** for the Shanghai Hackaton…
- They told us that all Car manufaturers share one **BIG** problem
- Many car owners before selling their car, **HACK** the Milage counter gear (odometer) and reduce the number of Kilometers and car age, to sell it at higher price… This simple fraud actually has a lot of implications, like when you try a stone in a pond…
- In Shanghai We team up with Ted and Jack and realized that we need to expand the problem space…. We asked ourselves.. What we need to solve this problem and many many other problems?

Meet AutoID

- A Self-Sovreign, Decentralized and Distributed Vehicle Identity System based on WC3 DID

- Hackaton Goals:

  - Create the Specifications for a truly Decentralized Vehicle Identity System

  - Analyze the data from VIS (vehicle Information System)

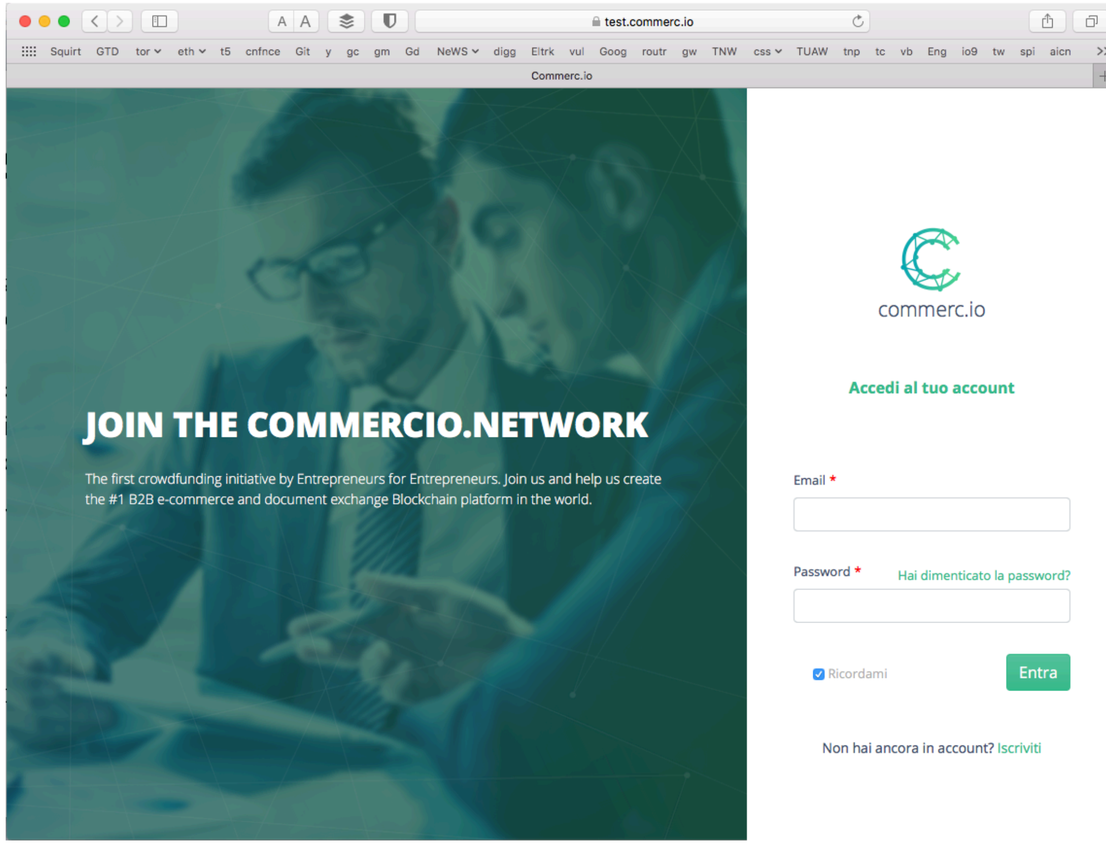
  - Code a way to Store the DDO and VC on IPFS

  - Try a simple transaction on the Commercio.network test-net

  - Create a Simple UX Demo app to show anyone how this actually might actually work for the end user

About Commercio.network

- The Documents Blockchain™
- Based on Cosmos SDK Technology
- Tendermint Consensus Algorithm
- Proof of Stake 10K TPS
- Stable fee Chain €0.01
- Stable (coins) Credits 1€



Stakeholders

C




Supply Chain Companies
Components Manufacturers and Sub-Suppliers

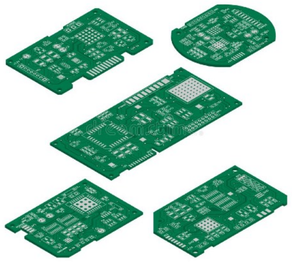
A

Manufacturer creates AutoID
`did:com:14zk9u8894eg7fhgw0dsesnqzmlrx85ga9rvnjc`

B

Companies
Banks - Financial - Insurance

People
Owner - User - Driver - Renter - Mechanic - Buyer



IOTs
VIS - Blackboxes - GPS

DID and DDO

- DID: Decentralized Identifier (ref: https://w3c-ccg.github.io/did-spec/)
  - Identifies a person, object, entity etc. Has a method (i.e. reference to «how interpreting the DID). It's is decentralized on a blockchain.
- DDO: Did Document (ref: https://w3c-ccg.github.io/did-spec/)
  - It is univocally associated to the DID. It contains, at least, cryptographic material and – possibly – endpoint to check revocation or to gather VCs. It should be «resolvable», i.e. given a DID, via the DID method, i can retrieve the associated DDO. It is recommended to store it on the blockchain

- Neither the DID, nor the DDO give any information about the DID subject.
- One person, object or entity, can control any number of DIDs and DDOs
- DIDs and DDOs can be public (i.e. written on the blockchain) or private / pairwise, and live locally.

Verifiable Credential (VC)

- VC: Verifiable Credential (ref: https://www.w3.org/TR/vc-data-model/)
  - A Verifiable credential is a set of attributes, that a subject issue for itself or for another subject. It may include cryptographic proof (i.e. signature) of these attributes.
  - It should NOT be public, in order to avoid privacy issues

DID in Commercio.network

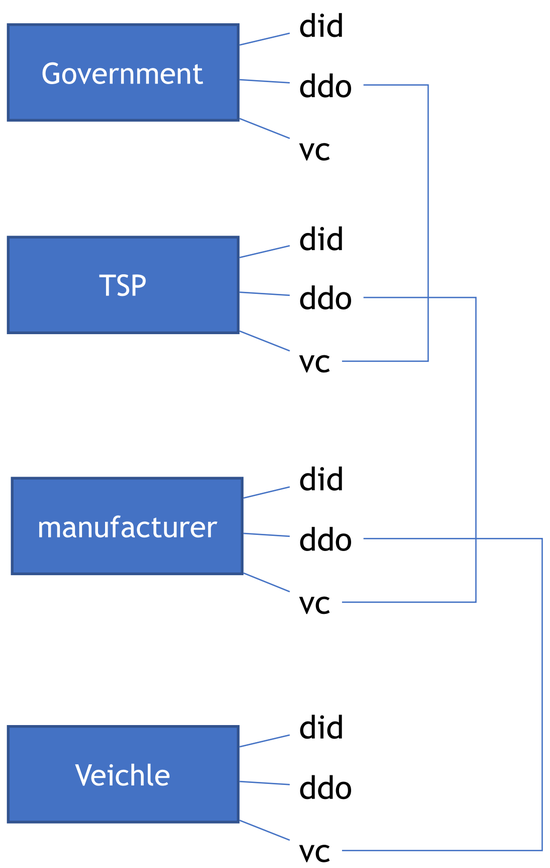
- Commercio.network DID scheme consists of the following parts:
  - url scheme identifier: `did`
  - identifier for the DID method: `com`
  - Method-specific identifier: `<commercio**.**network address>`, which conforms to the cosmos.network address scheme
- An example of commercio.network DID is the following:

```
did:com:14zk9u8894eg7fhgw0dsesnqzmlrx85ga9rvnjc
```

DDO in Commercio.network


```
{
          "@context": "https://www.w3.org/2019/did/v1",
          "id": "did:com:14zk9u8894eg7fhgw0dsesnqzmlrx85ga9rvnjc",
          "publicKey": [{
                    "id":"did:com:14zk9u8894eg7fhgw0dsesnqzmlrx85ga9rvnjc#keys-1",
                    "type": "RsaVerificationKey2018",
                    "controller": "did:com:14zk9u8894eg7fhgw0dsesnqzmlrx85ga9rvnjc ",
                    "publicKeyPem": "-----BEGIN PUBLIC KEY---
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDMr3V+Auyc+zvt2qX+jpwk3wM+m2DbfLjimByzQDIfrzSH
Q8erL0kg69YsXHYXVX9mIZKRzk6VNwOBOQJSsIDf2jGbuEgI8EB4c3q1XykakCTvO3Ku3PJgZ9PO4qRw7QVvTkCbc91rT93/pD3/
Ar8wqd4pNXtgbfbwJGviZ6kQIDAQAB-----END PUBLIC KEY-----r"
                    },{
                    "id": "did:com:14zk9u8894eg7fhgw0dsesnqzmlrx85ga9rvnjc#keys-2", +
                    "type": "Secp256k1VerificationKey2018",
                    "controller": "did:com:14zk9u8894eg7fhgw0dsesnqzmlrx85ga9rvnjc ",
                    "publicKeyHex":"02b97c30de767f084ce3080168ee293053ba33b235d7116a3263d29f1450936b71"
          }],
          "authentication": "did:com:14zk9u8894eg7fhgw0dsesnqzmlrx85ga9rvnjc#keys-1",
          "proof": {
                    "type": "LinkedDataSignature2015",
                    "created": "2016-02-08T16:02:20Z",
                    "creator": "did:com:14zk9u8894eg7fhgw0dsesnqzmlrx85ga9rvnjc#keys-1",
                    "signatureValue": "QNB13Y7Q9...1tzjn4w=="
          }
}
```

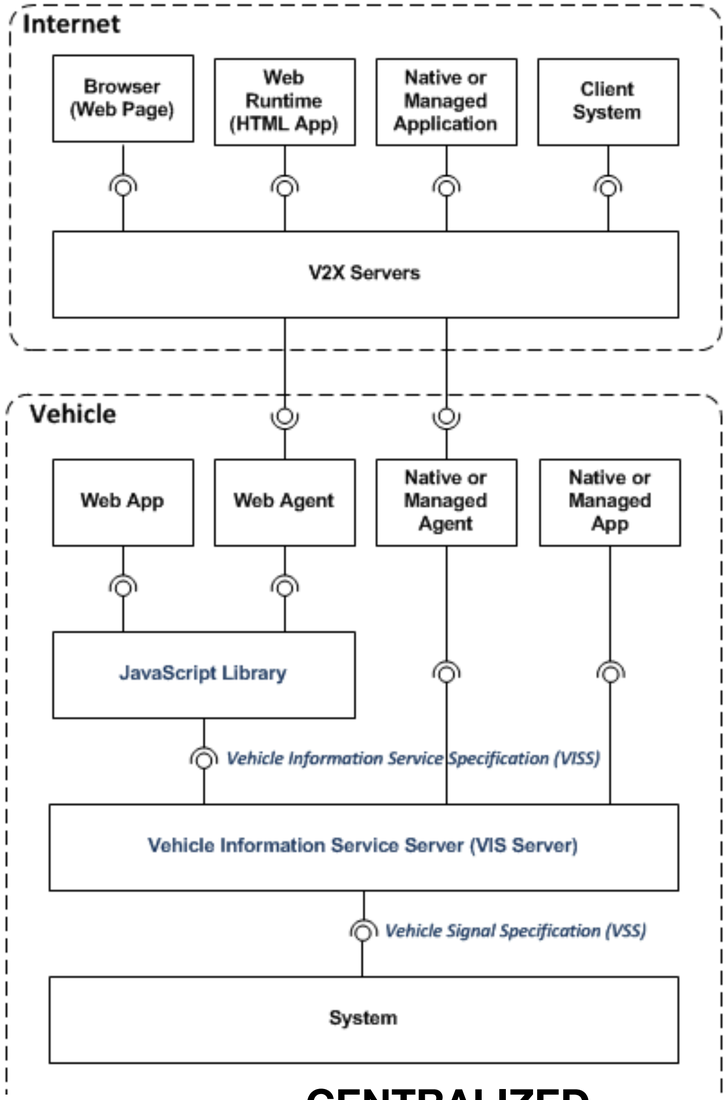
AutoID Trust Scheme



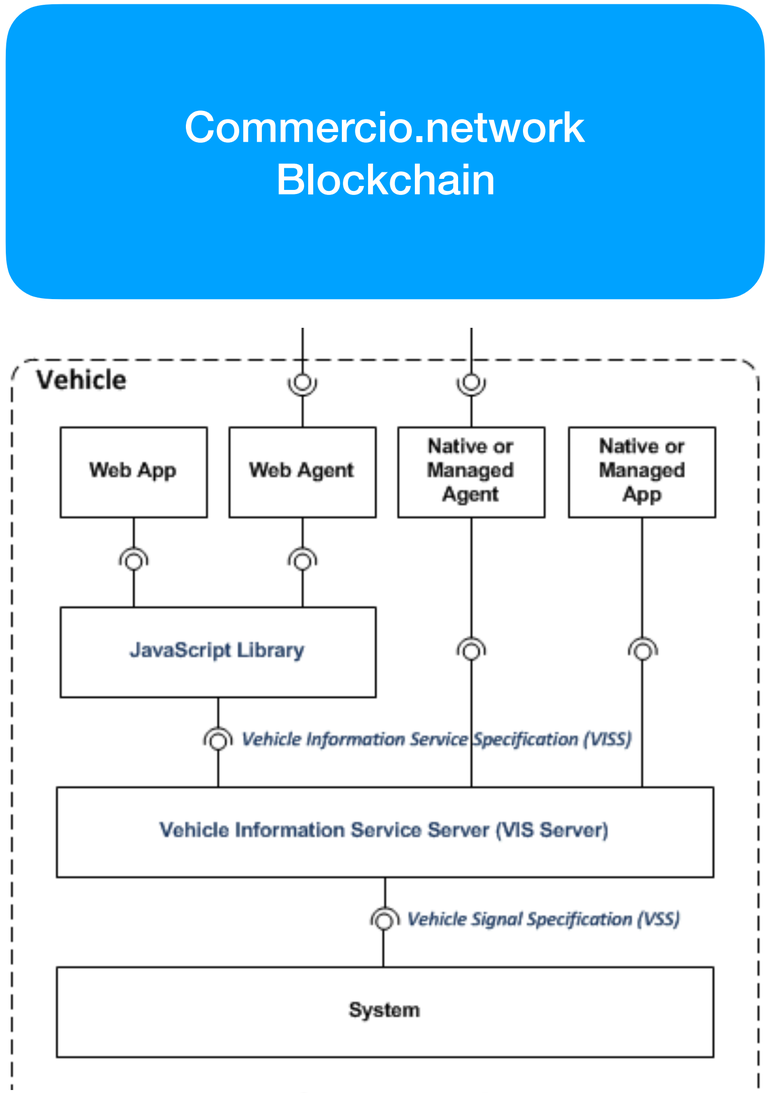
- AutoID, implemented on Commercio.network, provide the following trust scheme:
  - **Government**: it is the Root of truth in commercio.network, and it has it's DID, DDO and VC public on the Genesis Block. Government issue VC credential for TSP
  - **TSP**: are the entities (Companies or Persons) that provide trust services, i.e. verifies identity of persons and companies and issues VCs for them.
  - **Manufacturer**: its is the company that produce the vehicle. It generates DID, DDO and issues a VC for it, that includes all the relevant data.
  - **Vehicle**, thanks to the Identity issued by the manufacturer, the vehicle can pull data from the VIS, Sign transaction with its own verification key (included in the DDO), satisfying a chain of trust that goes up until the government DID and provide, if required, all the properties included in its verifiable credential, including the proof signed by the manufacturer

Vehicle Information Service WC3 standard

Ref link https://w3c.github.io/automotive/vehicle_data/vehicle_information_service.html)



CENTRALIZED



DECENTRALIZED

DEMO TIME

My Vehicles

Karma

SUV

Jeep

Bike

My Vehicles

Karma

SUV

1

Jeep

Bike

Jeep Events

X

☐		Information Sharing Request 3/12/2019	55550 Miles
√		Scheduled Maintenance 3/12/2018	45550 Miles
√		Bank Loan Paid 3/5/2018	35550 Miles
√		Scheduled Maintenance 3/4/2019	5550 Miles
√		Insurance Premium Paid 31/12/2018	0 Miles

Share information

Enrico

Owner

Jeep

Potential Buyer

Ted

- [x] Vehicle registration Disclosure
- [ ] Financial Disclosure
- [ ] Insurance Disclosure
- [x] Maintenance Disclosure

Share information with TED

Thanks!

github.com/commercionetwork/AutoID