Blockchain for Transport (BC4T)

Simulations of a Blockchain Network for Emission Monitoring

Dermot O'Brien, Vasileios Christaras,
Ioannis Kounelis, Igor Nai-Fovino,
Georgios Fontaras,

KST-2022

JRC sites

Headquarters in **Brussels** and research facilities located in **5 Member States:**

Belgium (Geel)

Germany (Karlsruhe)

Italy (Ispra)

The Netherlands (Petten)

Spain (Seville)

European Commission

JRC role

Independent of private, commercial or national interests

Policy neutral: has no policy agenda of its own

Works for more than **20 EC policy departments**

JRC scientific excellence

40-50% of JRC publications belong to the **top 25% most cited publications**

Up to **23%** belong to the **top 10% most cited publications**

Up to **3%** belong to the **top 1% most cited publications**

Brief Overview of Blockchain Technology

Basics of BC and digital identity.

Definition of Blockchain Network

Working definition of a blockchain network:

"A system of electronic records that

(i) enables a network of independent participants to establish a consensus around

(ii) the authoritative ordering of cryptographically-validated ('signed') transactions. These records are made

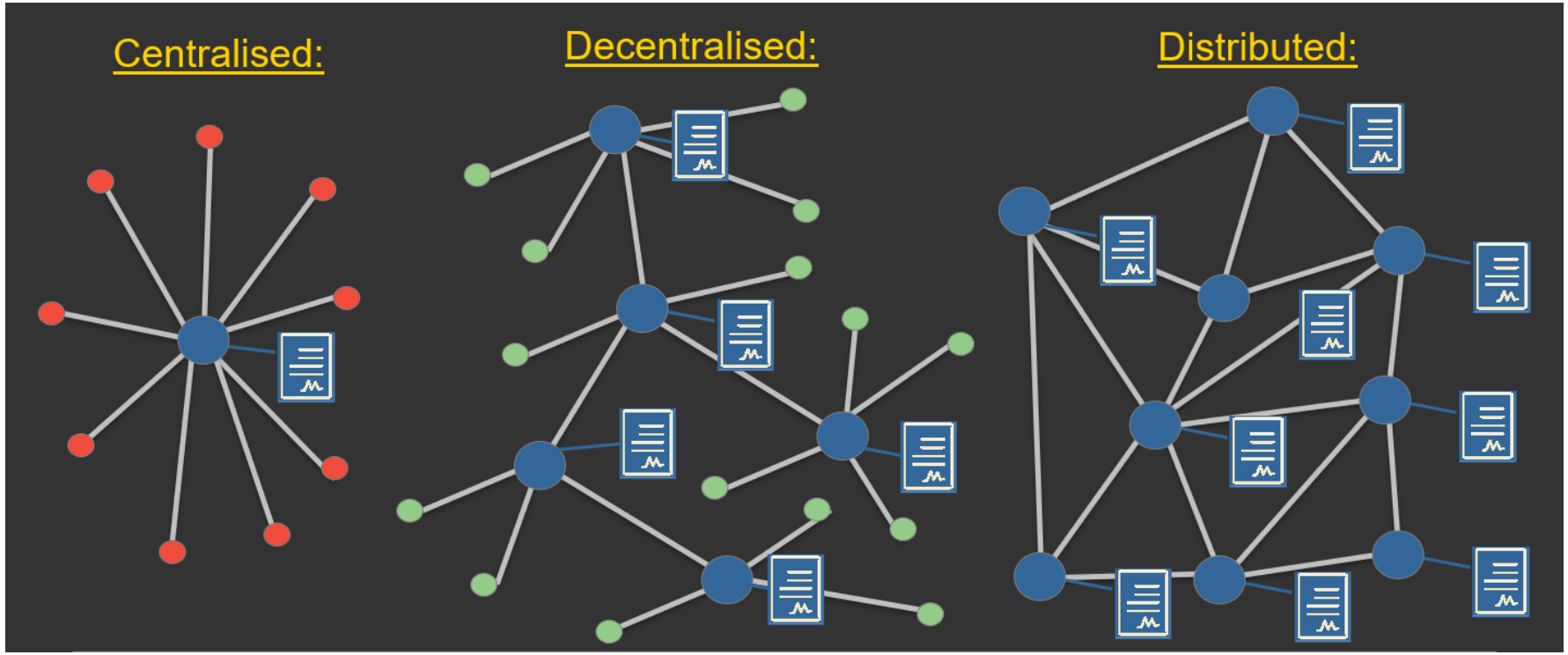
(iii) persistent by replicating the data across multiple nodes, and

(iv) tamper-evident by linking them by cryptographic hashes.

(v) The shared result of the reconciliation / consensus process - the 'ledger' - serves as the authoritative version for these records." (Rauchs et al., 2018)

Centralised vs Decentralised

In a **centralised system** which keeps one record of truth on it's database, there are **security concerns with a single point of failure and an element of trust required** for the party that holds these records.



European Commission

Types of Blockchain Networks

There are different types of BC network architectures, each with pros and cons. **Depending on the specific use-case one should choose a certain type of BC network.** The idea would **then** to also have the option of **interoperability between these networks** when required, preventing data silos.

Type	Read	Write	Commit Block	Example BC
Public Permissionless	Open to anyone.	Open to anyone.	Open to anyone.	Bitcoin, Ethereum.
Public Permssioned	Open to anyone.	Authorised participants only.	All or subset of authorised participants.	Sovrin, Ripple, EOS, Hyperledger Indy.
Private Permissioned	Fully private or restricted to a limited number of authorised nodes.	Network operator only.	Network operator only.	Hyperledger Fabric, Quorum, Enterprise Ethereum Alliance.
Consortium	Restricted to a set of authorised participants.	Authorised participants only.	All or subset of authorised participants.	Hyperledger Fabric, Quorum, Enterprise Ethereum Alliance.

Table 2: Types of Blockchain Networks. Source: Hileman & Rauchs (2017)

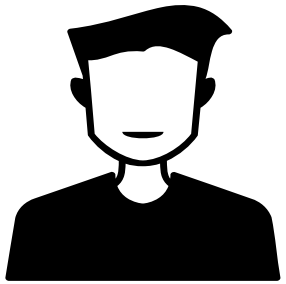
Why BC4T? Key Attributes of BC Technology

- **Immutability:** Very hard to change the history of hashes stored within a BC.
- **Decentralised Timestamping:** Clear record of when data has been transmitted which contains the lifetime data of a vehicle, without need to trust an single entity.
- **Non-Repudiation:** Due to the Immutability and Decentralised Timestamping of the hashed data records. It is very hard for an entity to dispute their validity or which vehicle recorded said data.
- **Security:** With a decentralised network there is increased security, due to no longer having a single point of failure.
- **Privacy:** With the utilisation of ZKPs an entity can have increased privacy while still providing a proof that a statement is true or a data value falls within a certain range.
- **Auditability:** Authorities that require a global view of all the transaction and associated data can be given access with ease, with the data in a format that is easily audited digitally.
- **Identity Management:** Identities can either be managed via a Member State authority or a decentralised identity solution could also be used, allowing for increased privacy and security.
- **Automation:** Smart Contracts can be written and often reused between different entities and a set of agreements that can automatically take effect after a time period or condition is met.

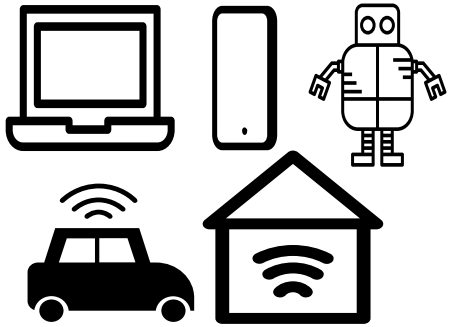
Digital Identity

Identity is defined by ISO 29115 as a set of attributes related to an entity.

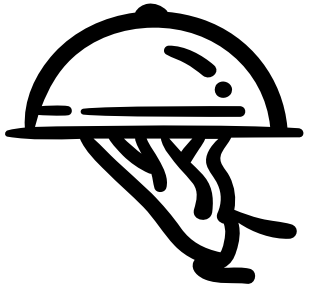
Where an **Entity** can be a:



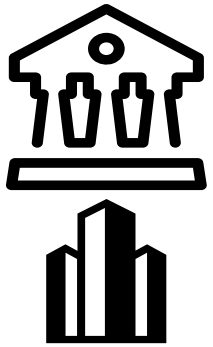
Person



Device, Machine, Property, etc.



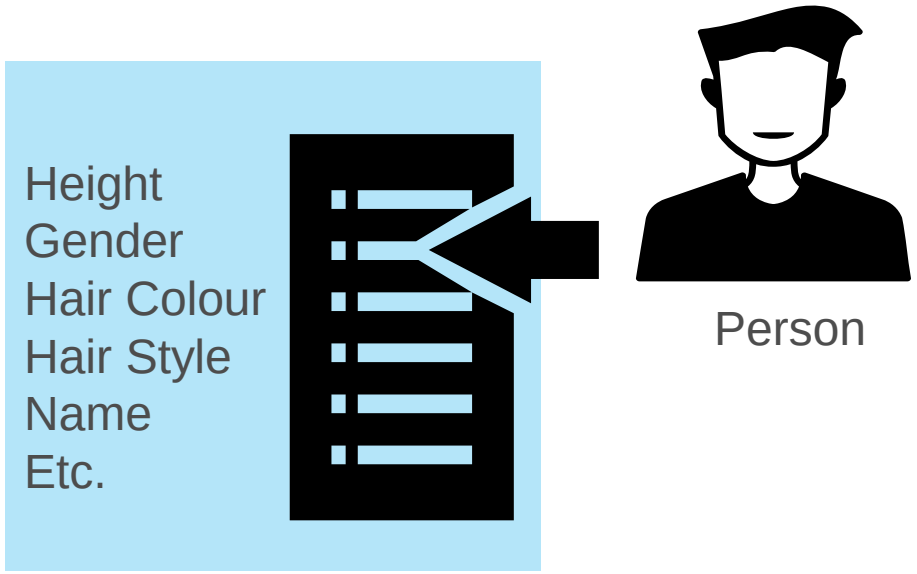
Service



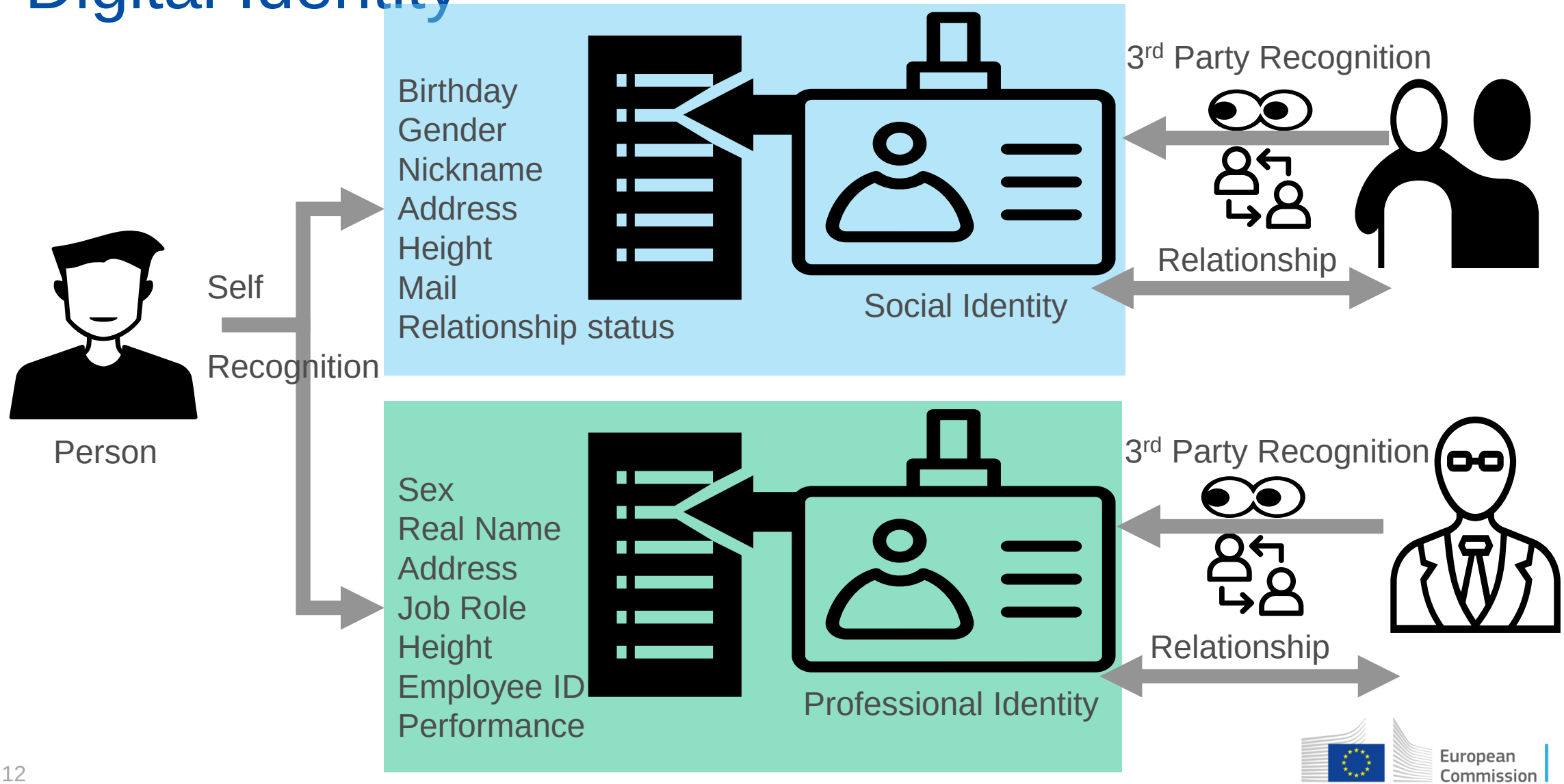
Institution, Government or Business

Digital Identity

Identity is perceived indirectly through attributes relating to an entity.

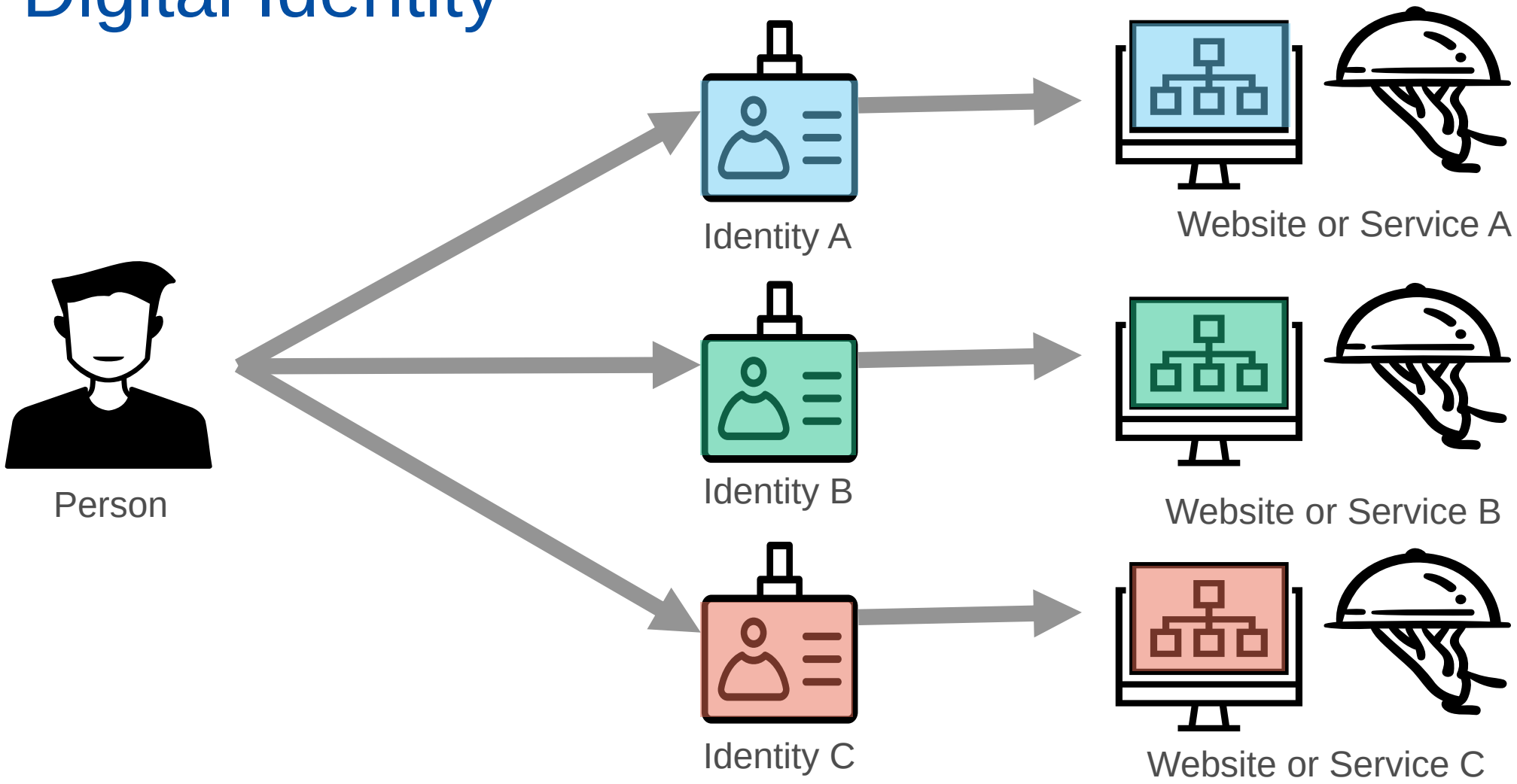


Digital Identity



European Commission

Digital Identity

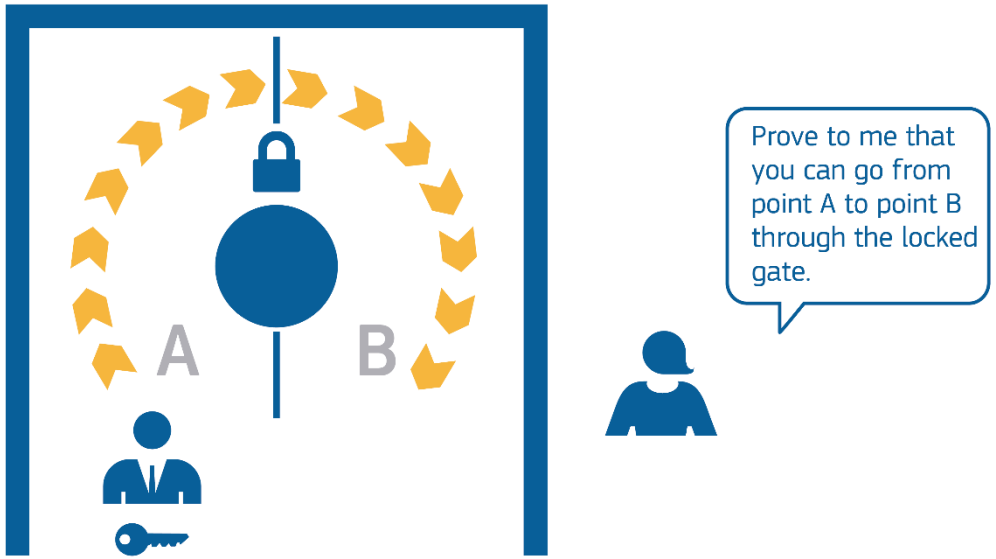


Zero-Knowledge Proofs

Zero-Knowledge Proofs (ZKPs) is a cryptographic method in which the prover can show the verifier that a claim is true without providing any additional information to the verifier or leaking information about the claim.

- This reduces disclosure of sensitive data to verifiers and increases privacy while allowing for a proof that certain parameters of a claim are met or that they fall within a required range, as when using Zero-Knowledge Range Proofs (ZKRPs).

Over simplified illustration:



European Commission

Digital Identity

X.509 Certificates are a particular format of Public Key Certificates (PKCs) that links public keys to an entities name. Signed by a Certificate Authority (CA) who is a trusted network administrator.

- **Enables secure communications between entities or authorises transactions or validates data or documents via digital signatures with the corresponding private key.**

Self-Sovereign Identities utilises data identifiers that are kept offline and are carried by the owner (vehicle), this increases the security with respect to centralised digital certificate solutions and when used in combination with ZKPs allows for increased privacy.

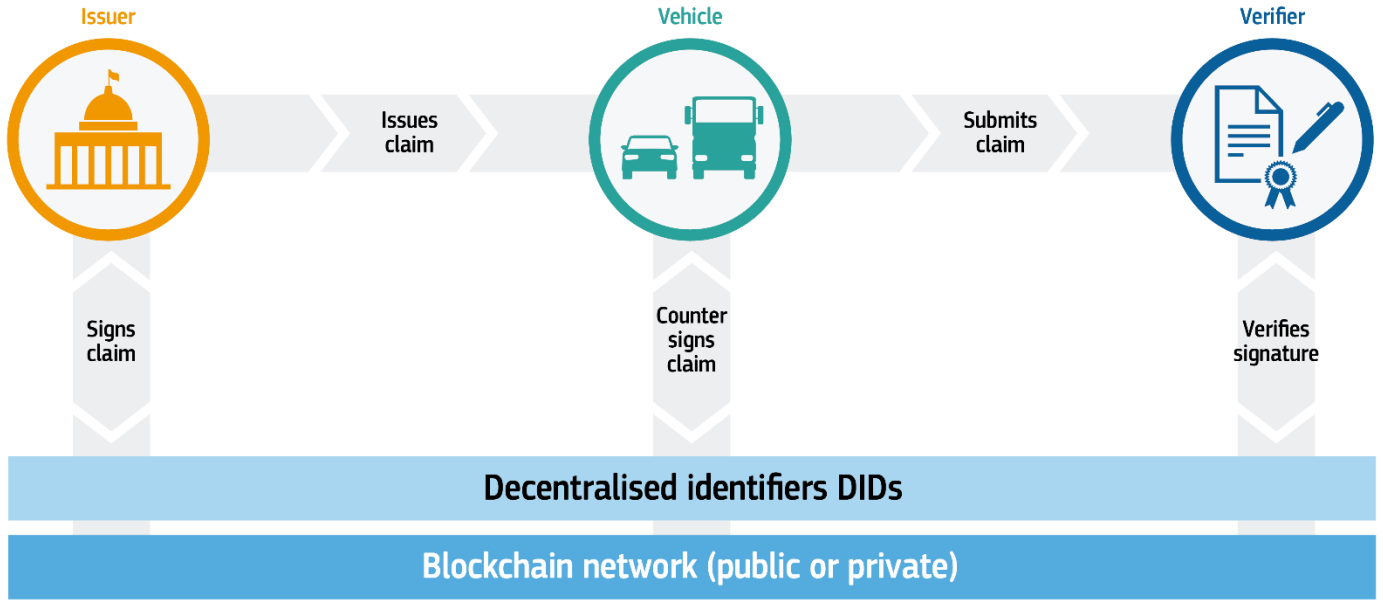
- **Allowing to prove your identity on the internet or a network, in a secure way that helps your credentials and information remain private.**

Self-Sovereign Identities

SSIs incorporate two main standards, that of Decentralised Identifiers (DIDs) and Verifiable Credentials/Claims (VCs).

I. **DIDs** utilise cryptographic methods for identification of an entity (Vehicle).

II. **VCs** enable authentication of a credential/claim often with a focus on privacy, with the use of ZKPs.



European Commission

BC4T Scenarios

European Commission

Explored Scenarios.

The three pilots explored within the BC4T project:

- **SSI Management System in collaboration with MOBI** solution for digital identity management forwarding data to either a centralized or decentralized database.
- **Provenance and Integrity of Data at the JRC:** Achieved deploying a Hyperledger Fabric network on JRC infrastructure.
- **SSI Management System combined with Data provenance and Integrity in collaboration with CERTH** using OpenID Connect standards for their SSI tool that communicates between Hyperledger Ares and Indy in order to add a more robust identity layer to the Hyperledger Fabric Network of our previous work to enable data provenance and integrity.

Pilot 1: Self-Sovereign Identity Management System

BC-based identity management; operation, requirements and integration.

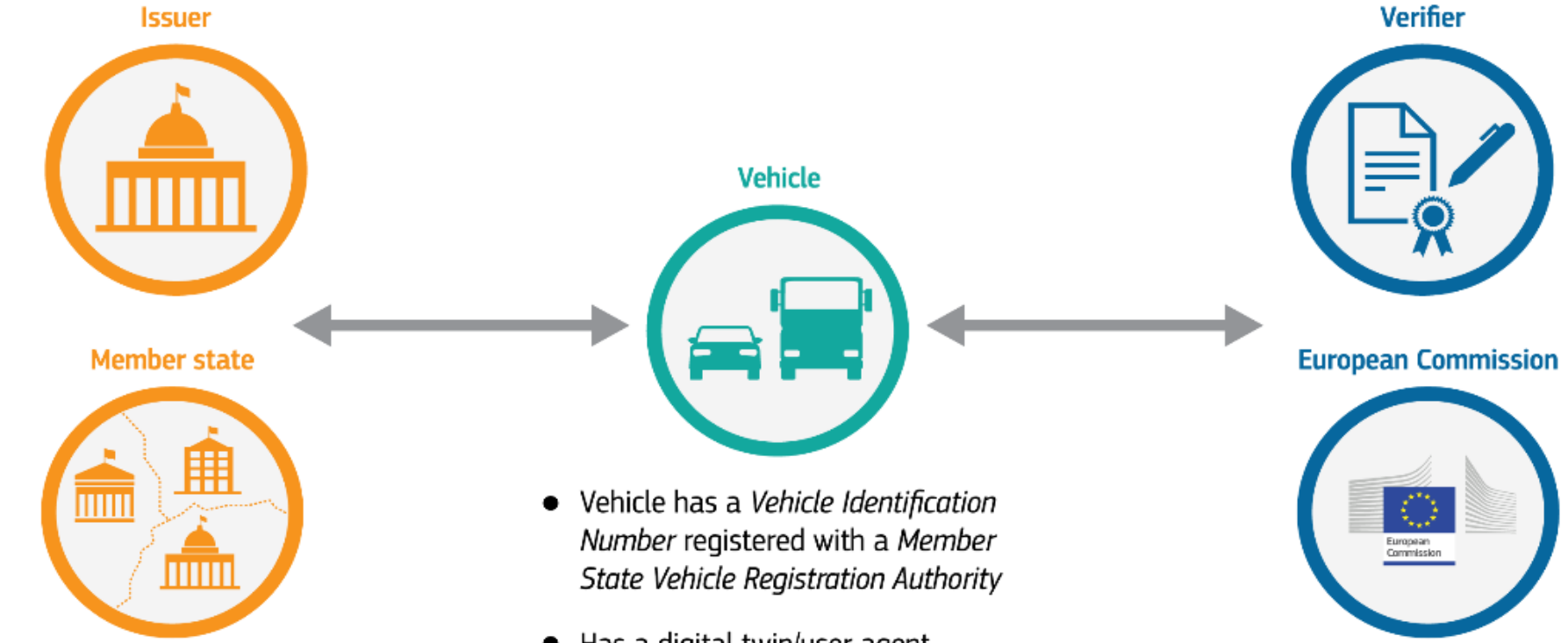
European Commission

About MOBI

Mobility Open Blockchain Initiative (MOBI) is a global non-profit smart mobility consortium. MOBI and its members are creating blockchain-based standards to identify vehicles, people, businesses, to make transportation more efficient, equitable, decentralised, and sustainable. MOBI officially launched in May 2018 and released its first standard, Vehicle Identity (MOBI VID), which leverages internationally accepted vehicle identification number (VIN) to define a vehicle's digital twin. Since its launch, MOBI has formed seven working groups, released 13 standards, and launched several initiatives surrounding the MOBI Web3 Technology Stack (MTS).

European Commission

MOBI: Roles and Assumptions

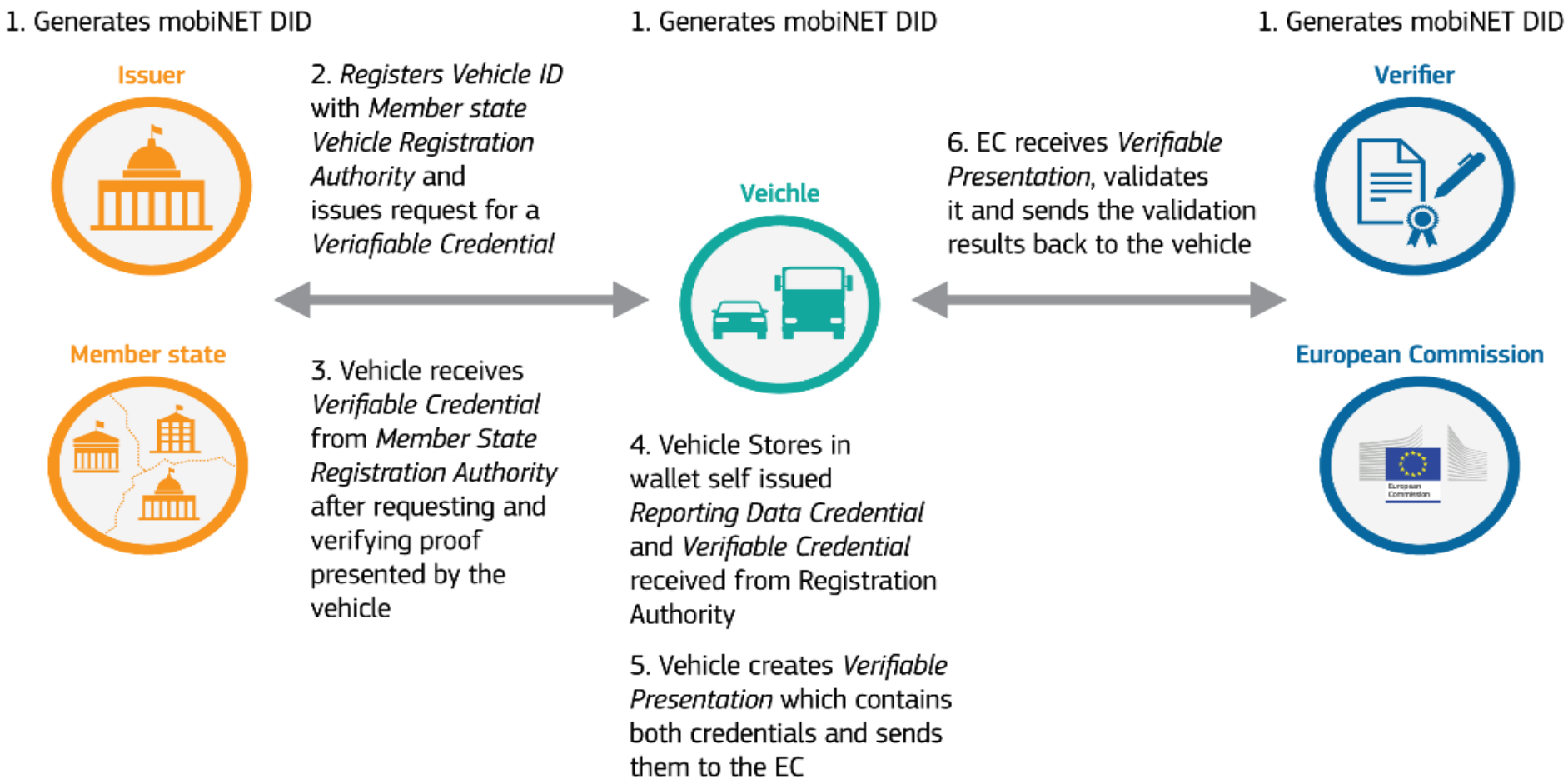


- 27 Independent organisation
- Issues registrations
- Has digital twin/user agent

- Vehicle has a *Vehicle Identification Number* registered with a *Member State Vehicle Registration Authority*
- Has a digital twin/user agent

- Has digital twin/user agent
- Verifies *Verifiable Presentation* and *Verifiable Credential* from vehicle

Emissions Reporting Process Flow



MOBI Detailed Process Flows

- **Issue Vehicle Registration Credential flow:** A vehicle asks the Member State Vehicle Registration Authority to issue a credential. This flow consists of following operations:

1. Establishing a secure connection between two parties (Vehicle and RA.)
2. Vehicle sends an issue credential request to the RA.
3. RA receives issue credential request and asks Vehicle to prove mobiNET membership.
4. Vehicle receives a “request proof” message from the RA and presents the proof back to the RA.
5. The RA receives the proof, verifies it, issues a "VehicleCredential" credential and sends it to the Vehicle.
6. Vehicle receives the issued credential and stores it in its wallet.

- **Self-Issue CO2-emission Credential flow:** A vehicle self-issues a CO2-emission credential. This flow consists of following operations:

1. Vehicle self-issues "ReportingDataCredential" and stores it in its wallet.

- **Verify CO2-emission Credential flow:** A vehicle sends two credentials from its wallet and sends as a Verifiable Presentation to EC for validation. This flow consists of following operations:

1. Establishing a secure connection between two parties (Vehicle and EC.)
2. Vehicle takes two credentials from its wallet:
3. "VehicleCredential" issued by the RA.
4. "ReportingDataCredential" self-issued by Vehicle.
5. Vehicle creates a Verifiable Presentation including both credentials and sends it to the EC.
6. EC receives the Verifiable Presentation, validates it (validate proofs, diddocs, contexts) and sends the validation result back to Vehicle.
7. Vehicle receives validation results from the EC.

Results

Flow name	Time to complete 1 million flow executions	# of flow executions per second
Issue credential (IC)	9 minutes (average)	1851
Self-issue (SI)	1 minute 40 seconds (average)	10000
Verify credential (VC)	7 minutes (average)	2380

Test results for 1 million* flow executions:

Hardware used in Performance Tests

75 c6i.xlarge AWS instances (4 vCPU, 8GB RAM each) 1 db.m6g.8xlarge AWS instance for RDS (32 vCPU, 128 GB RAM)

Pilot 2: Data Provenance and Integrity of CO2 Emissions, Monitoring Scenario

Simple Scenario Currently being Simulated

Emission Monitoring Regulations

Regulation (EU) 2018/1832 of November 2018 decreed, starting from January 2021, On-board Fuel and/or Energy Consumption Monitoring Devices (OBFCM devices) as compulsory devices in all newly produced commercial and light passenger vehicles.

The ensuing Regulation (EU) 2019/631 of April 2019 “setting CO2 emission performance standards for new passenger cars and for new light commercial vehicles”, further detailed that the EC are required to store a record of the data reported by Member States. Parameters that need to be shared from OBFCM devices with the EC, starting from the 1st of January 2021 include:

— Vehicle Identification Number (VIN);
— “fuel and/or electric energy consumed;”
— “total distance travelled;”
— “for externally chargeable hybrid electric vehicles, the fuel and electric energy consumed and the distance travelled distributed over the different driving modes;”

Or any other parameters required to ensure the obligation of the EC to monitor and asses the real-world representativeness of CO2 emissions and fuel or energy consumption values determined pursuant to Regulation (EC)

No 715/2007 . In addition Regulation (EU) 2019/631 states the three modes of data collection, consisting of data derived from: manufacturers, national authorities or directly transferred from the vehicles themselves. Regulation (EU) 2021/392 put into legislation an obligation for the Member States and manufacturers to compile data from OBFCM devices and transmit it once a year to the EC via data exchange platforms provisioned by the European Environmental Agency (EEA)

Proposal to Amend eIDAS Regulation

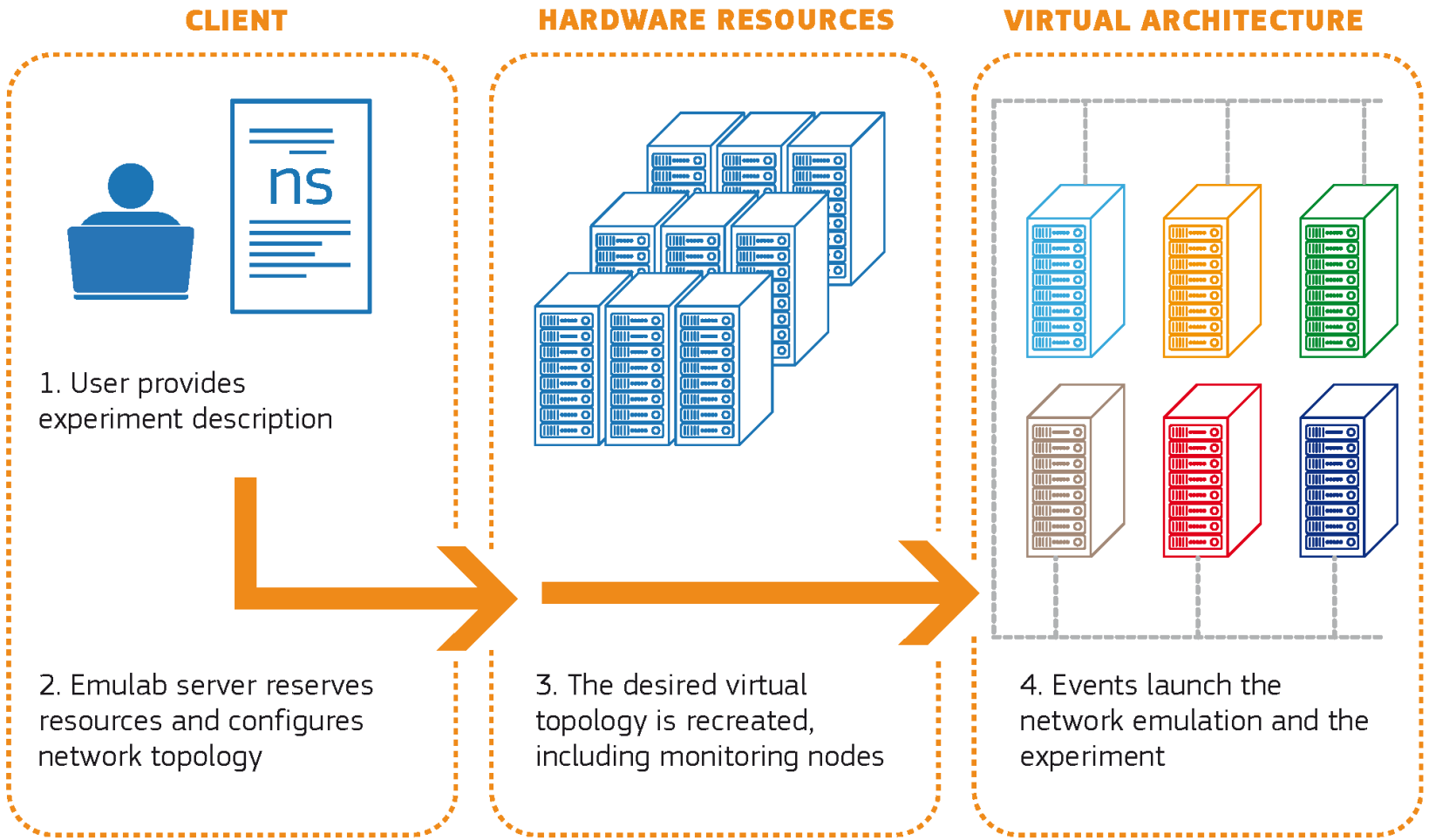
https://eur-lex.europa.eu/resource.html?uri=cellar:5d88943a-c458-11eb-a925-01aa75ed71a1.0001.02/DOC_1&format=PDF

Increasing demand for means to authenticate and identify online, including the need to exchange information relating to one's identity digitally: certificates, attributes and qualifications one holds (could include ID number, residence address, age, qualifications, driving licence and other permits or payment information). This has sparked off a new paradigm, with the adoption of "advanced and convenient solutions that can integrate different verifiable data and certificates of the user." Users expect a self-determined environment where various credentials and attributes can be carried and shared, such as your national eID, professional certificates, and public transport passes. These are so-called self-sovereign app-based wallets managed through the mobile device of the user allowing for secure and easy access to different services, both public and private, under their full control."

The European Digital Identity Proposal echoes the need for a more harmonized approach to digital identification to that of divergent national methods and the vitality this will give to the EU digital Market by enabling citizens, businesses and public services to identify online conveniently and uniformly while facilitating data subjects control over what personal data is shared and when. All EU citizens should benefit from secure access to public and private services provisioned by an ecosystem at the EU level that enables trust between participants relying on verified proofs of identity and attestations of attributes and verifiable claims. The reliability of digital identity solutions will support competition within the EU, by benefiting "from a harmonized European approach to trust, security and interoperability. " It is, therefore, necessary to in addition lay out the conditions to be included in a harmonized framework for European Digital Identity Wallets:

- Enable users to access a large scope of cross-border private and public services through electronic identification and authentication, both online and offline.
- Benefit from the potential delivered by tamperproof solutions to provide a high level of assurance.
- Permit the issuance and handling of trustworthy digital attributes and support the decline in administrative strain, enabling citizens to use the verifiable credentials and claims in their private and public interactions. For example, EU citizens should be capable of proofing digitally, ownership of a valid driving licence issued by a Member State Vehicle Registration Authority, which can be verified and relied upon by the authorities in the other Member States.
- "Qualified electronic ledgers record data in a manner that ensures the uniqueness, authenticity, and correct sequencing of data entries in a tamper-proof manner. An electronic ledger combines the effect of time stamping of data with certainty about the data originator similar to e-signing and has the additional benefit of enabling more decentralised governance models that are suitable for multi-party co-operations. For example, it creates a reliable audit trail for the provenance of commodities in cross border trade, supports the protection of intellectual property rights, enables flexibility markets in electricity, provides the basis for advanced solutions for self-sovereign identity and supports more efficient and transformative public services. To prevent fragmentation of the internal market, it is important to define a pan-European legal framework that allows for the cross-border recognition of trust services for the recording of data in electronic ledgers"
- "The certification as qualified trust service providers should provide legal certainty for use cases that are built on electronic ledgers."

The EPIC Cluster, Emulation not just Simulation



The EPIC JRC Data Centre

Simple Scenario for CO2 Emissions Monitoring

Registration of new vehicle

UUID	Total distance traveled (Lifetime)	Total fuel consumed (Lifetime)
32Fas D03	0 Kilometers	0 Litres

Periodic **transmission** of CO_2 emission data:

UUID	Total distance traveled (Lifetime)	Total fuel consumed (Lifetime)
32Fas D03	24 Kilometers	3 Litres

European Commission

EU Regulations 2018/1832 – OBFCM data availability 2019/631/EU - Data reporting

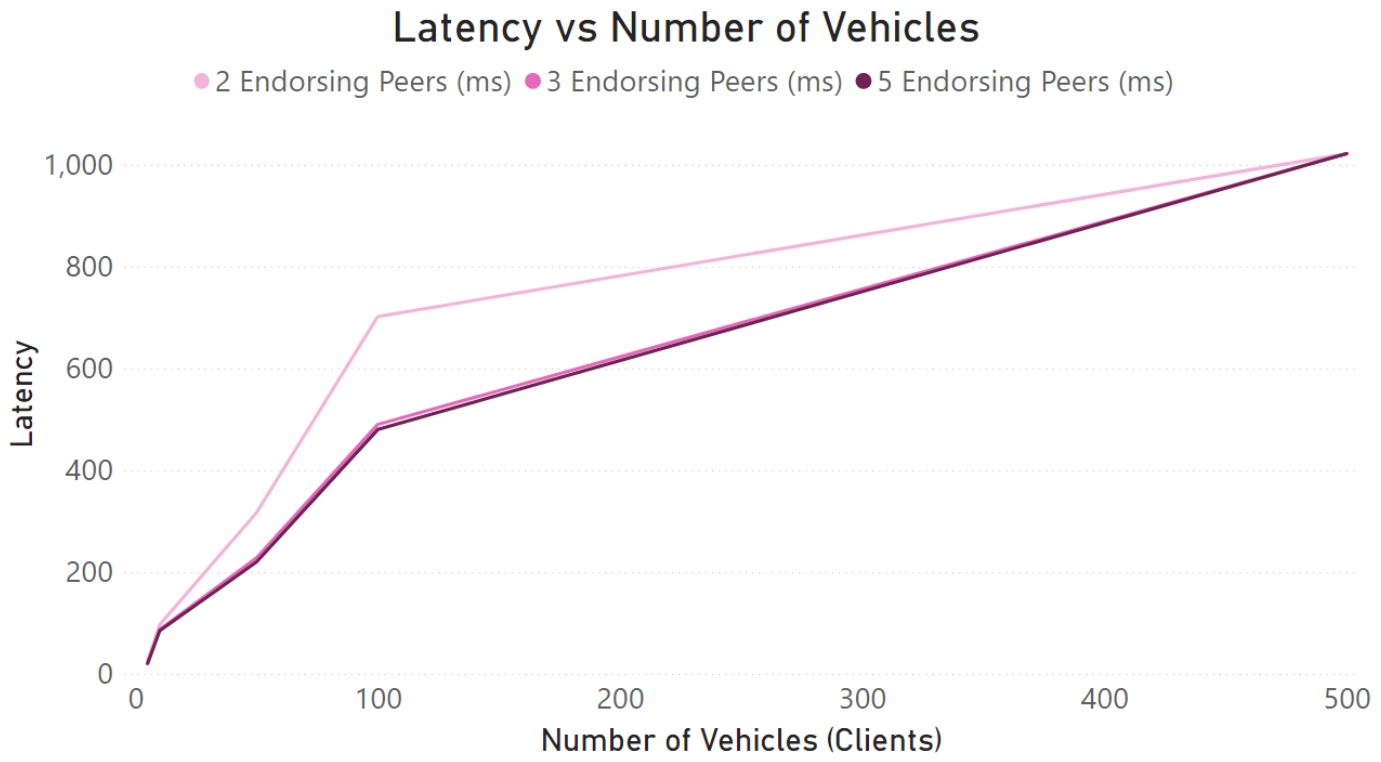
- **Standard Fuel Vehicles** data reporting requirements:
  - Total distance travelled (lifetime).
  - Total fuel consumed (lifetime).
- **Hybrid Vehicles** data reporting requirements:
  - Total distance travelled (lifetime).
  - Total fuel consumed (lifetime).
  - Total distance travelled in charge depleting operation with engine off (lifetime).
  - Total distance travelled in driver-selectable increasing operation (lifetime).
  - Total fuel consumed in charge depleting operation (lifetime).
  - Total fuel consumed in driver-selectable charge increasing operation (lifetime).
  - Total grid energy consumed in charge depleting operation with engine off (lifetime).
  - Total grid energy consumed in charge depleting operation with engine running (lifetime).

Simulation Parameters

- **Number of Vehicles on the Road** (Currently ~280M), pre-registered with CA.
- **Number of Vehicles bought and resold each day,** requiring registration with CA.
- **Number of Nodes** for Member States and for the European Commission (EC).
- **Number of transactions** per time period required for :
  - Emission Monitoring (once every 6 months to 1 month time period).
  - Tolling and Trading (few times a week to every day).
  - Traffic Management (10K+ per second).
- **Size of Data** requiring transmitting (from OBFCM regulation)
  - Standard Fuel Vehicle: Total Distance Traveled (Lifetime), Total Fuel Consumed (Lifetime), UUID.
  - Hybrid Vehicle: Total Distance Traveled (Lifetime), Total Fuel Consumed (Lifetime), UUID, + 7 other data points (see previous slide).

Latency of Transactions

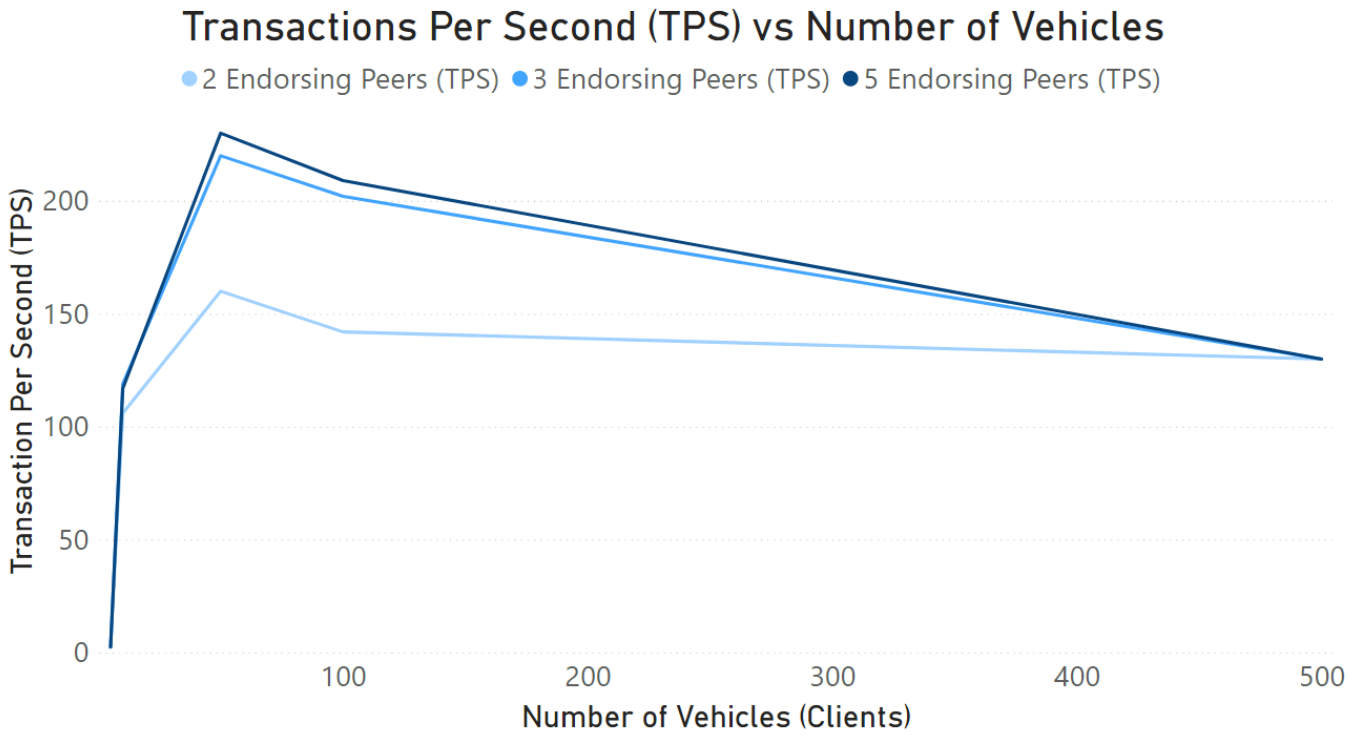
- For the application of emissions monitoring, due to the data only requiring transmission once a month, the relatively large latency when compared to 5G (24ms) interacting with a centralised database is not an issue. Although could be a limiting factor on certain blockchain for transport use-cases.



European Commission

Transactions Per Second (TPS)

- With 280M vehicles on the road currently, requiring to send CO2 emissions data once a month, roughly 108 Transactions Per Second (TPS) is needed for the emissions monitoring use-case.



European Commission

Limitations of Initial BC Network Setup

- **Disk usage**
  - Incremental increase of storage due to consensus strategy. HLF stores signatures of every endorsing peer for each transaction.
- **Network connectivity**
  - Maintaining open connections from a few clients to each peer does not represent real world usage.
  - Requiring signatures from each endorsing peer increases network usage and limits the number of organisations in network.
- **For more details on subsequent experiments** performed, please see the Science for Policy Report for BC4T that will be published and released to the public shortly.

Pilot 3: SSI Management with Data Provenance and Integrity in Collaboration with CERTH.

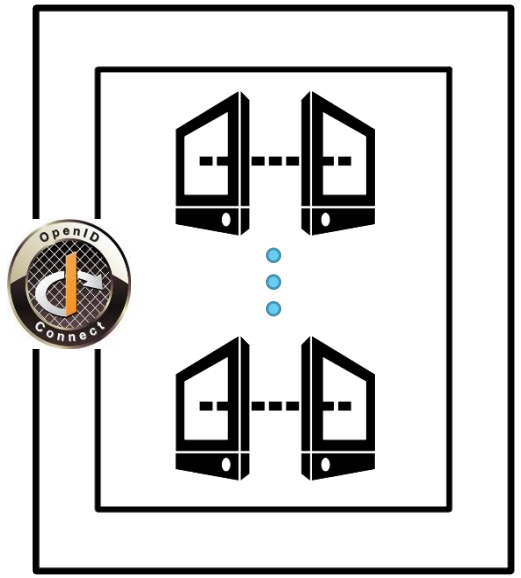
BC-based identity management; operation, requirements and integration.

European Commission

Operation Transaction Flow

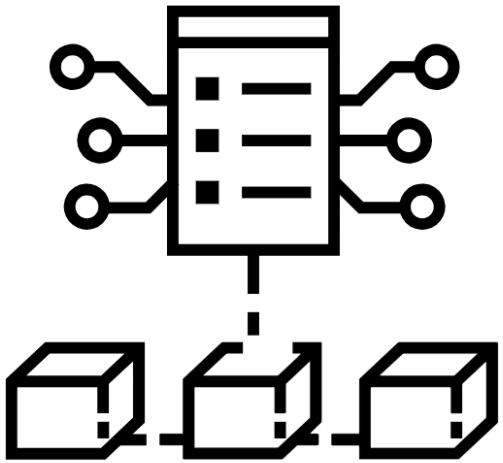
1. Request ID token

Gateways



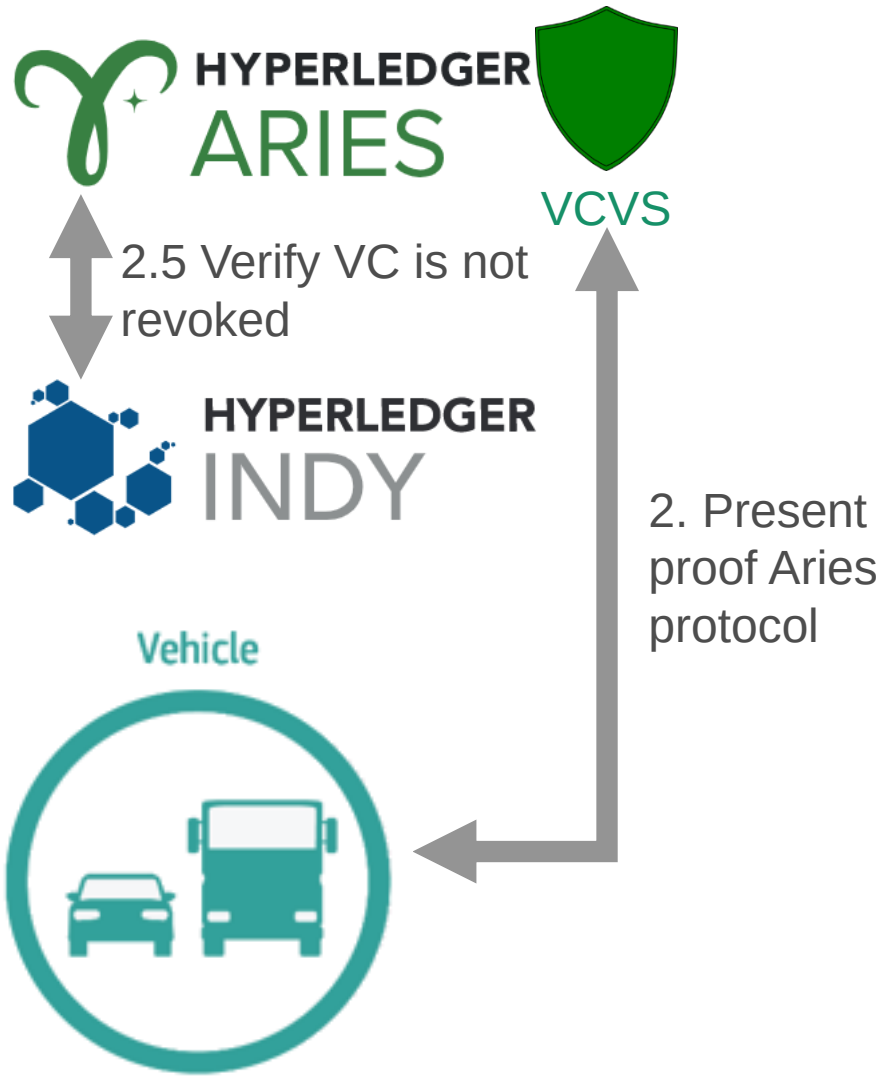
HYPERLEDGER
FABRIC

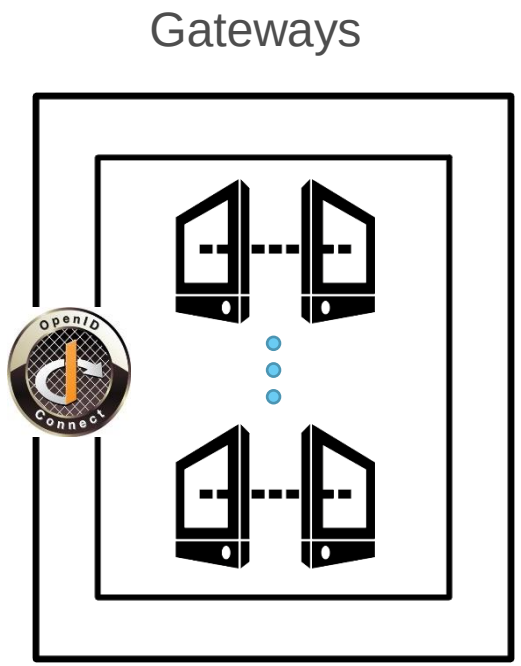
& Smart Contract

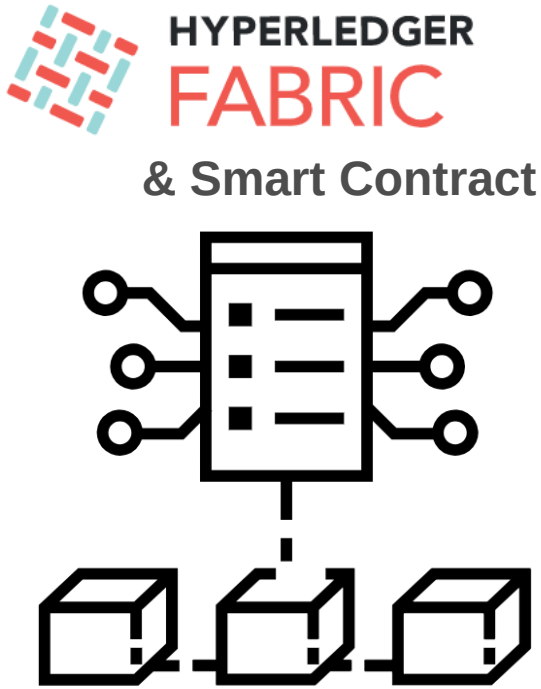


European Commission

Operation Transaction Flow





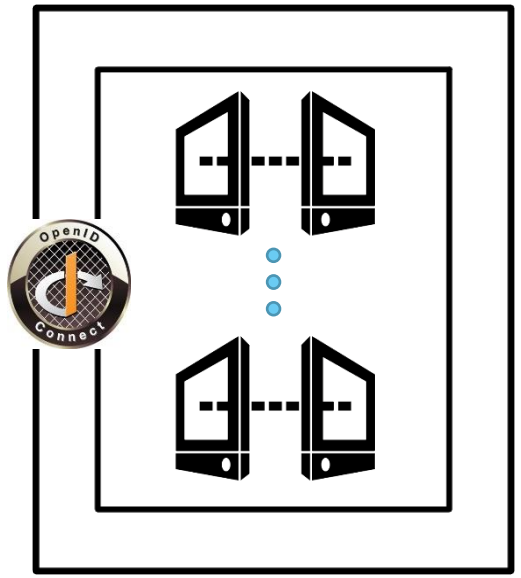


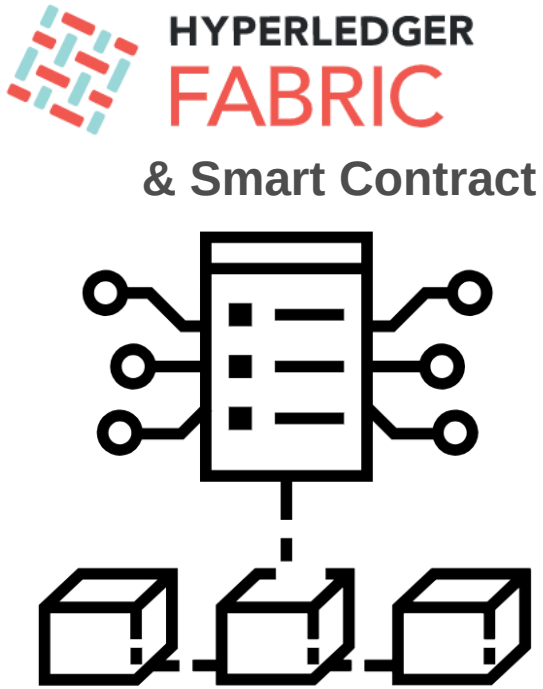
Operation Transaction Flow

3. Issue ID token

Vehicle

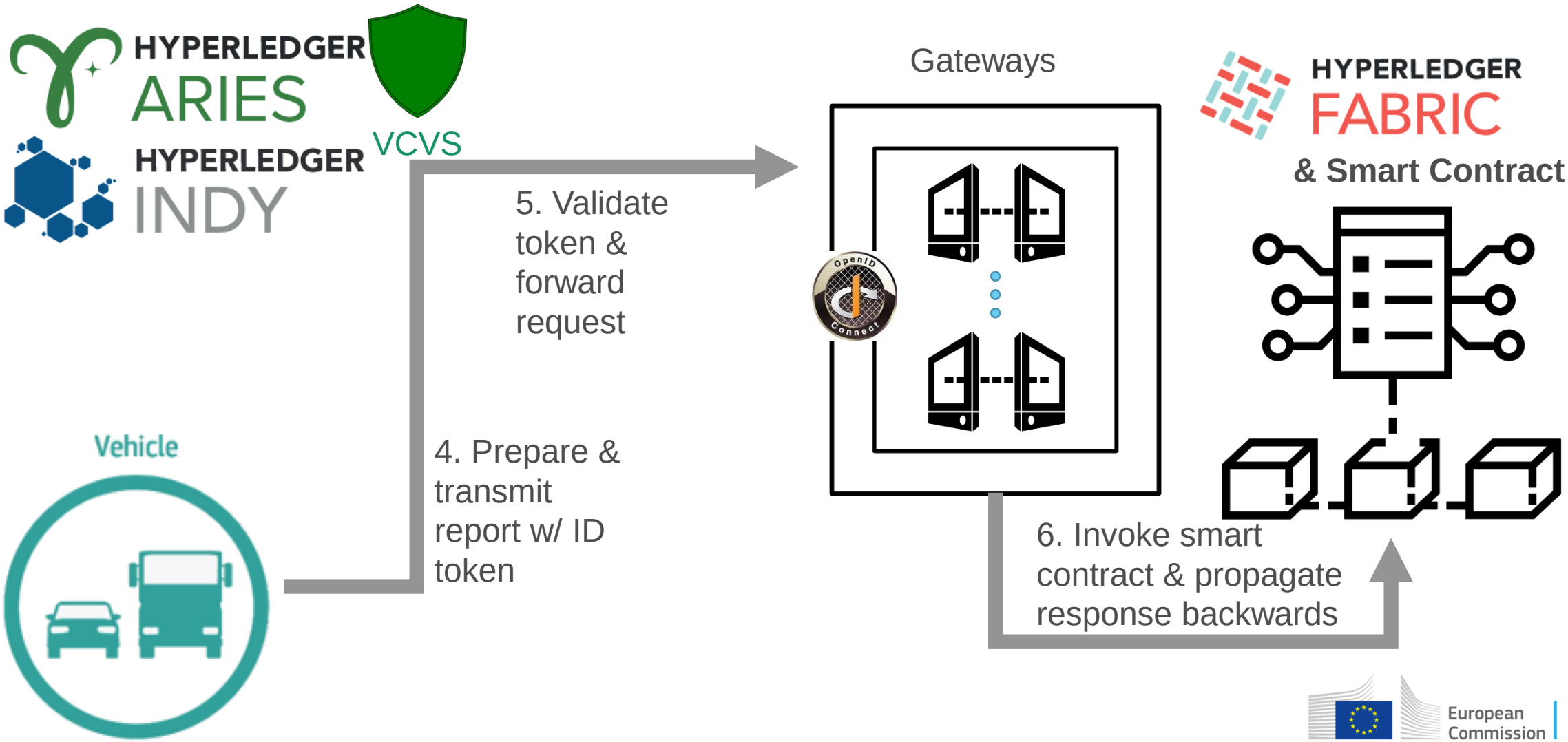
Gateways





European Commission

Operation Transaction Flow



BC4T: Conclusion

Next steps and closing remarks.

Conclusions

- In pilot one, the initial experiment achieved the TPS required for the emissions monitoring use-case. Subsequent experiments improved the results and changes where made to more closely approximate real world conditions
- Pilot two, achieved a magnitude of order higher number of process flow executions needed for 280M vehicles, for the tested use-case
- Pilot three: System successfully deployed on JRC infrastructure, with performance results to be published in journals at a later date.
- The results and details of these pilots will be published soon in a Science for Policy Report that will be available to the public.

Next Steps for BC4T ER Project

- **Finishing study for the combination of SSI standards for vehicle digital identity management on Hyperledger Ares and Indy and data provenance for emissions data on Hyperledger Fabric:** benefits, including increased privacy when combining with Zero-Knowledge Proofs.

- **Extend simulations to other blockchain for road transport use-cases:** Providing evidence for the feasibility of other applications, such as trading and tolling, additionally what the requirements and cost for these applications would be.

Future Research Opportunities

- Identity layer for IoT devices and users is a key implementation for almost all mobility applications. For a digital society you need a digital identity.
- EU has objective to digitalize different sectors as much as possible including transport, need identity for most applications. Need to be secure (trust the data is verified, and history of that data is true and private).
- European Self-sovereign Identity Framework (ESSIF) from EBSI platform, built with a focus on standards and compliance to regulation.
- Applications to electric vehicles (optimal charging station locations, green electricity consumed, etc..)
- Supply Chain applications such as:
  - Goods/Sensitive Materials track and trace
  - ETS applied to transport fuels accounting for how much carbon is inside.

Keep in touch

EU Science Hub: ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub – Joint Research Centre

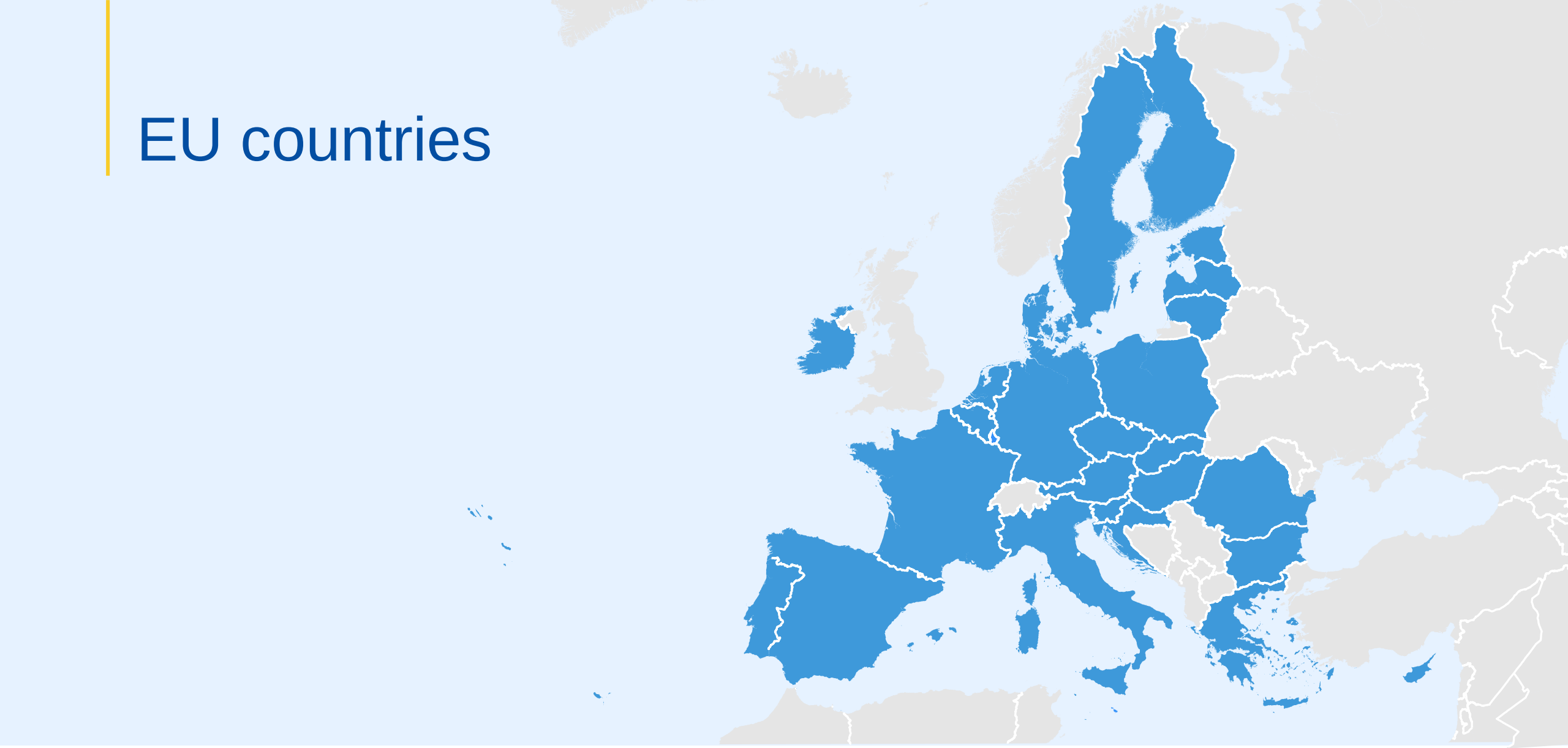
EU Science, Research and Innovation

EU Science Hub

Thank you

European Commission

EU countries



0 250 500 1,000 Km

European Commission