

Blockchain Based Approach for Preserving Car Maintenance History

Master Project

Decentralized and Distributed Systems Lab

Iva Najdenova

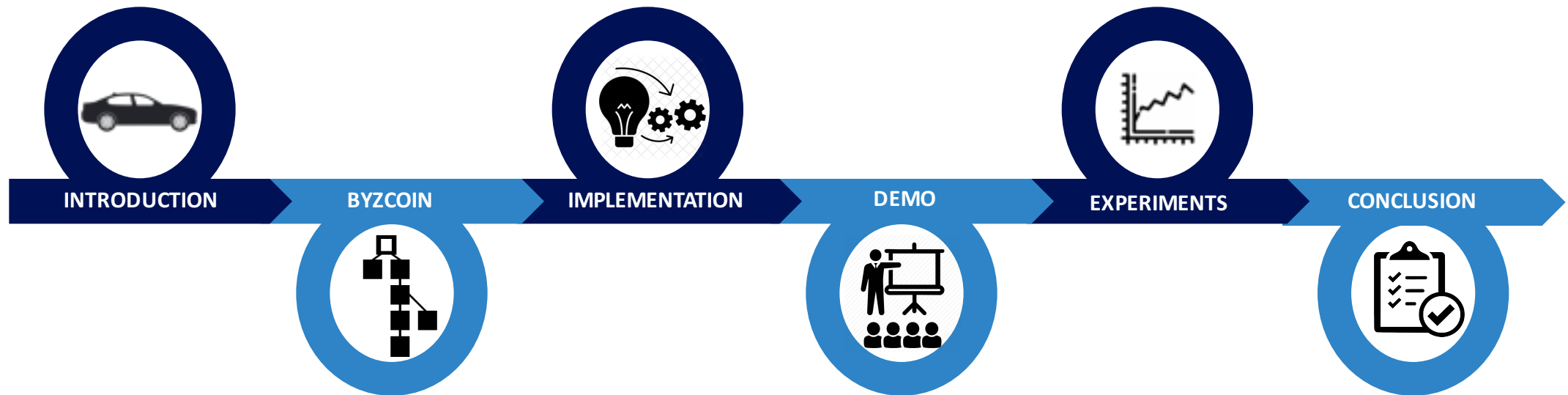


Professor: Bryan Ford

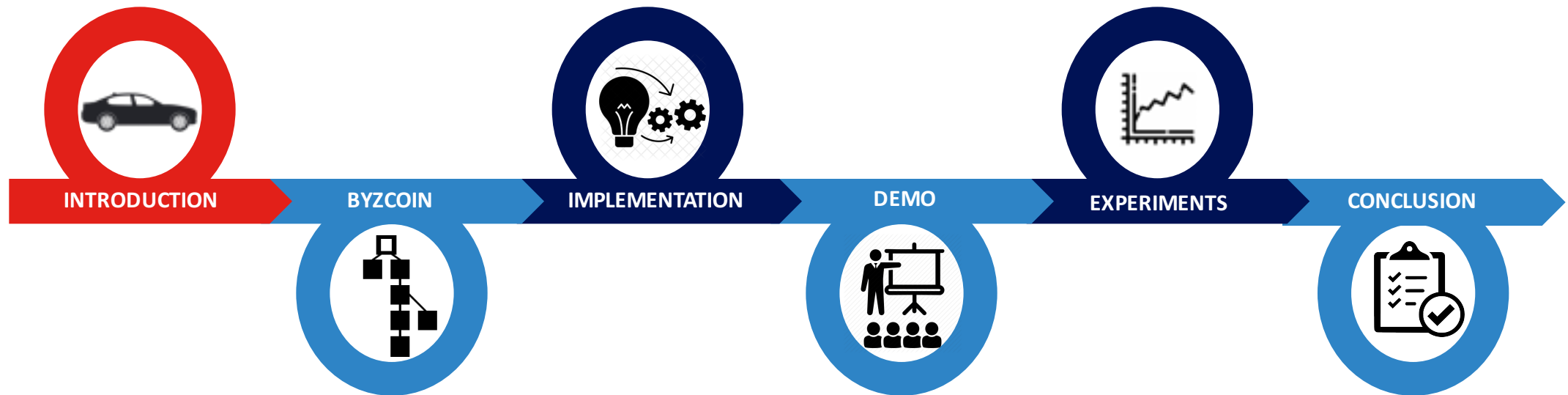
Supervisor: Linus Gasser

External Supervisor: Alexandru Rusu

Overview



Overview

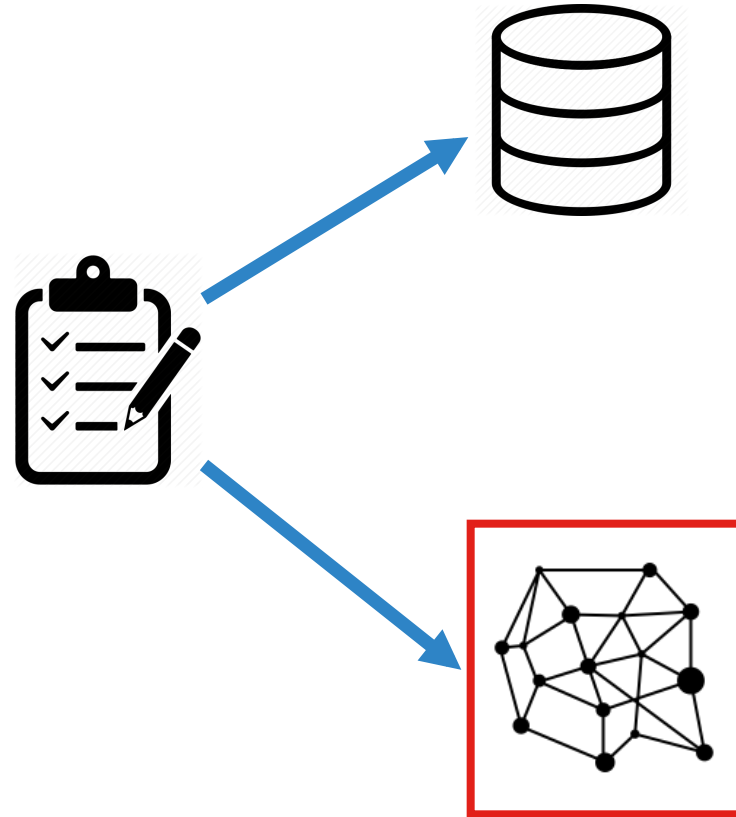


Motivation

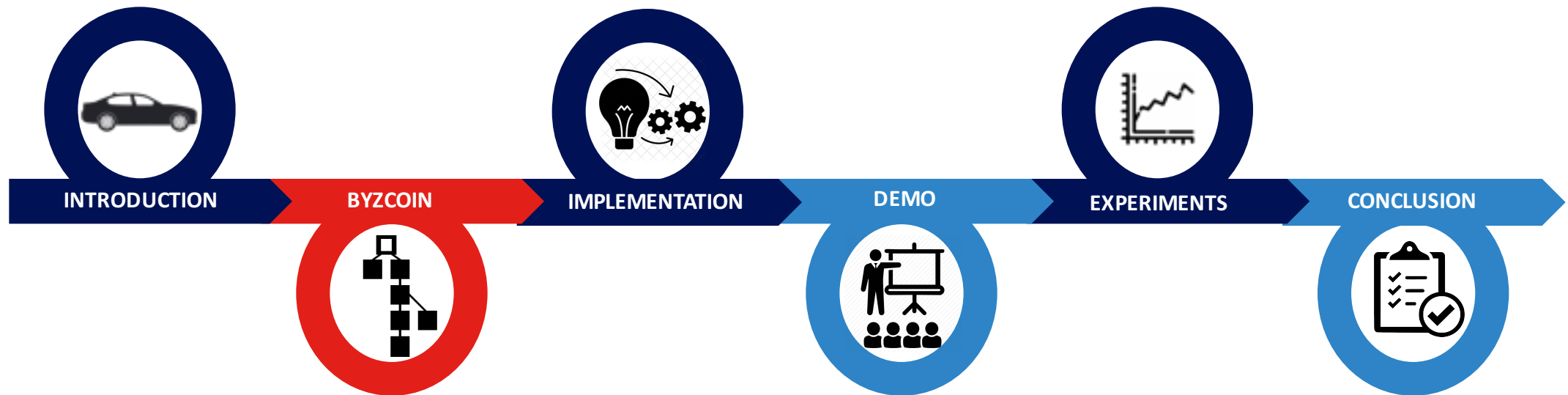
- Fighting frauds in the automotive industry
 - low quality repairs
 - tampering odometers (mileage)
 - hiding accidents

Goal

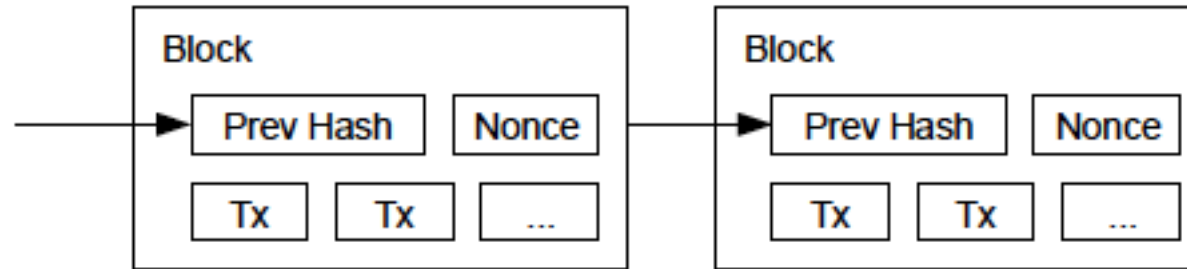
- Establish trust between:
 - Car buyers
 - Car owners
 - Car dealers
 - Insurance companies
 - ...



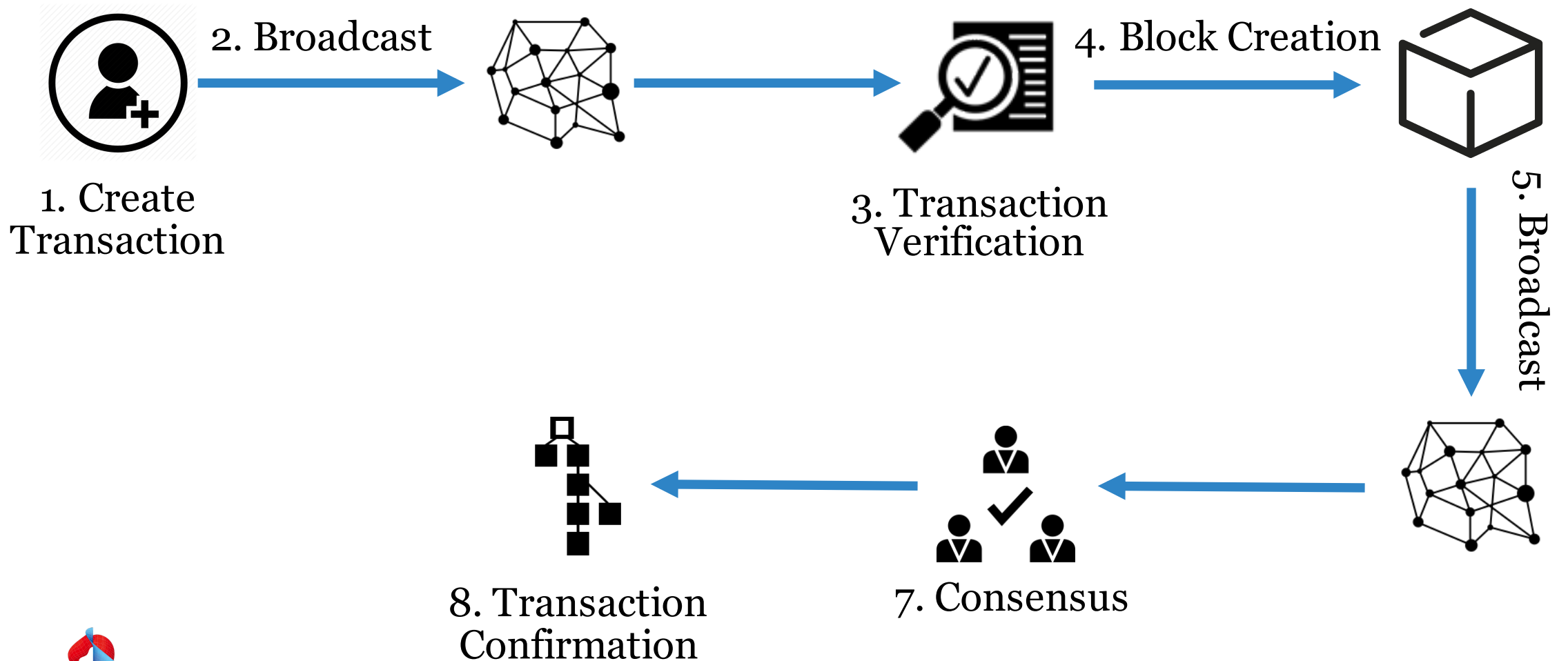
Overview



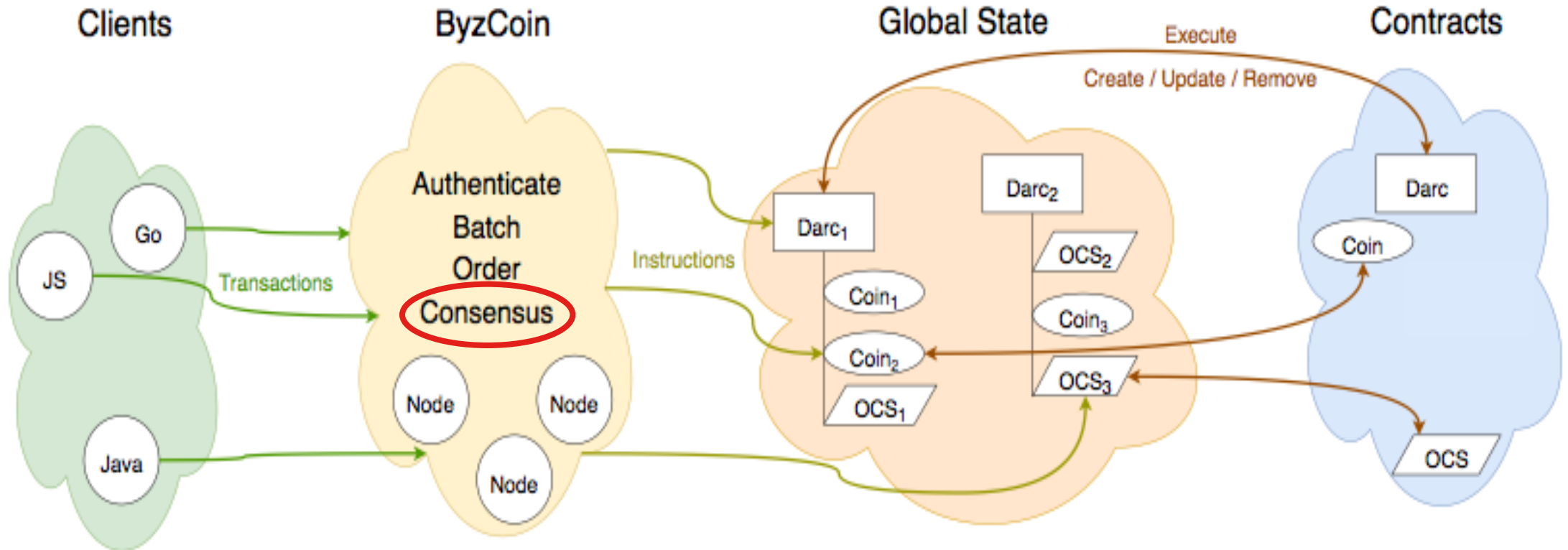
Blockchain Data Structure



Submitting a Transaction to a Blockchain

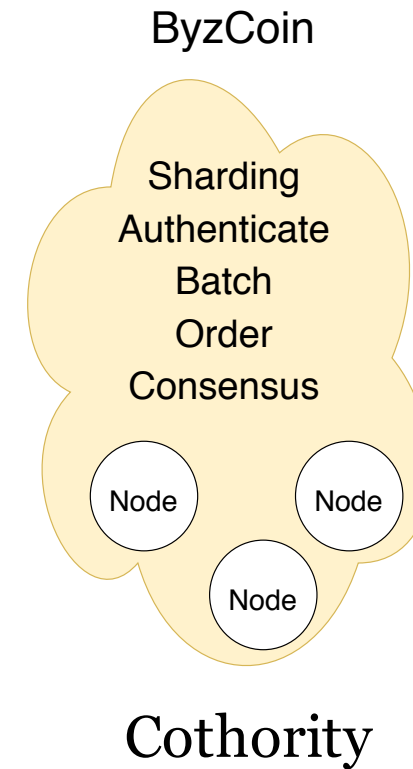


ByzCoin

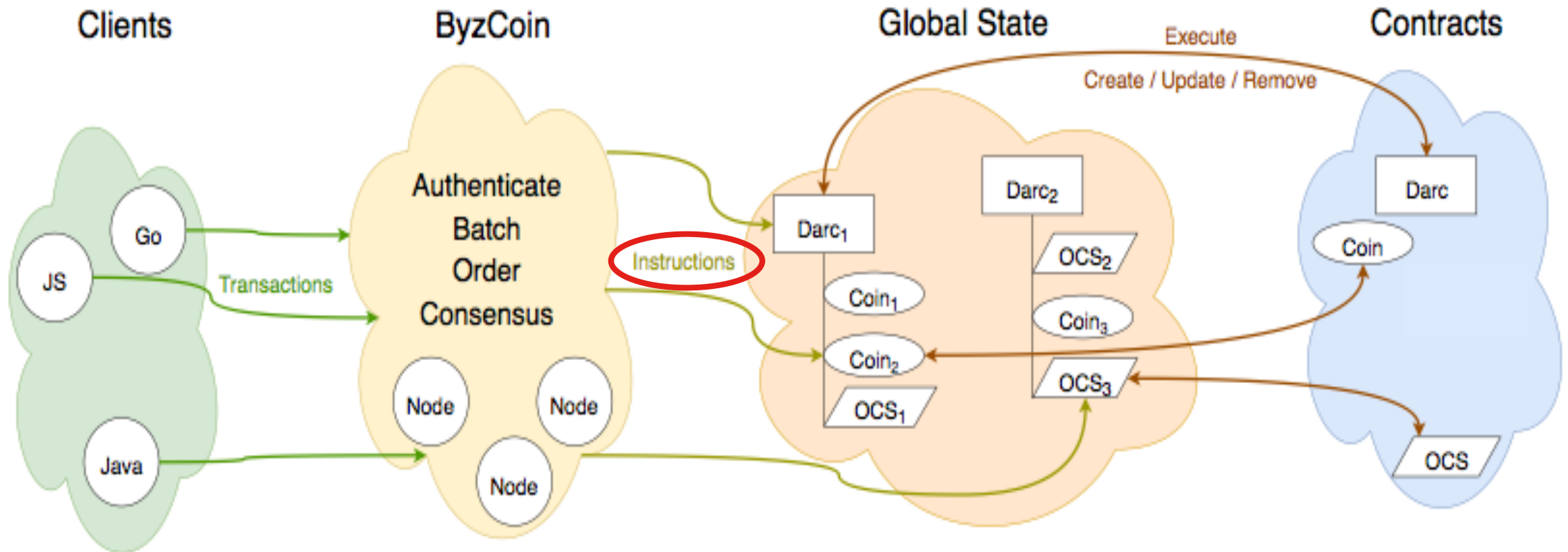


ByzCoinX Consensus Protocol

- Collective Signing
- Absolute Finality
- Open Membership
- Tree Structure for Communication



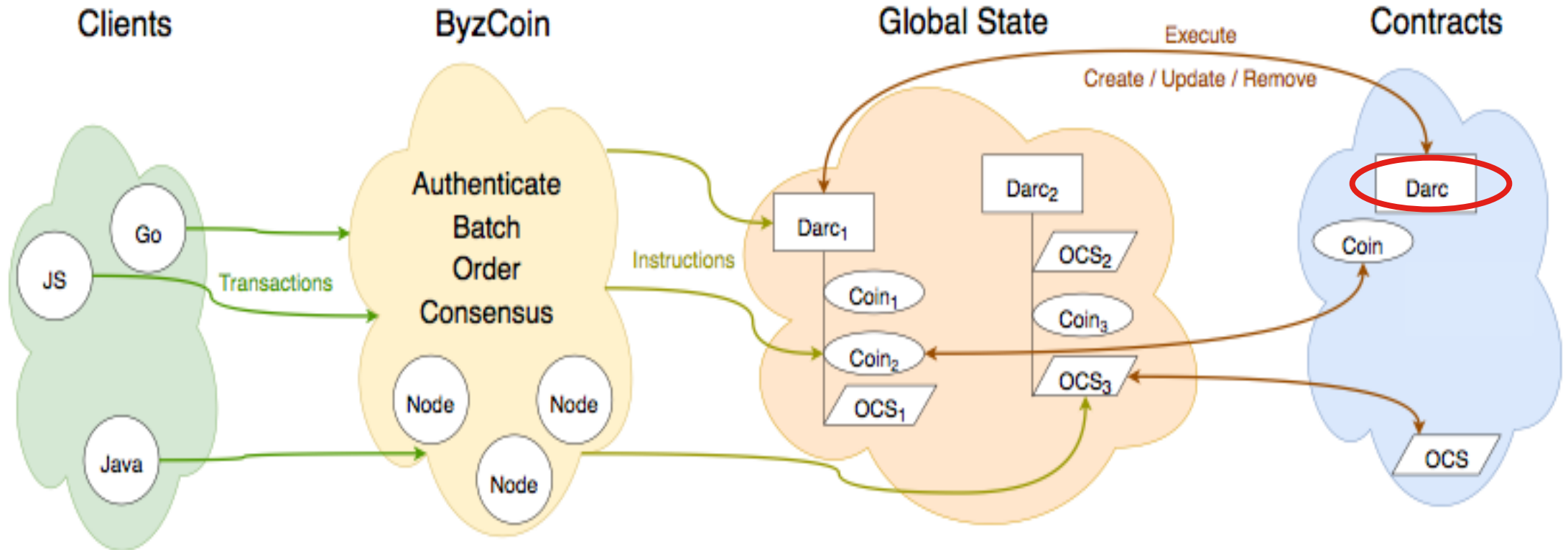
ByzCoin



Instructions

- Spawn
- Invoke
- Delete

ByzCoin

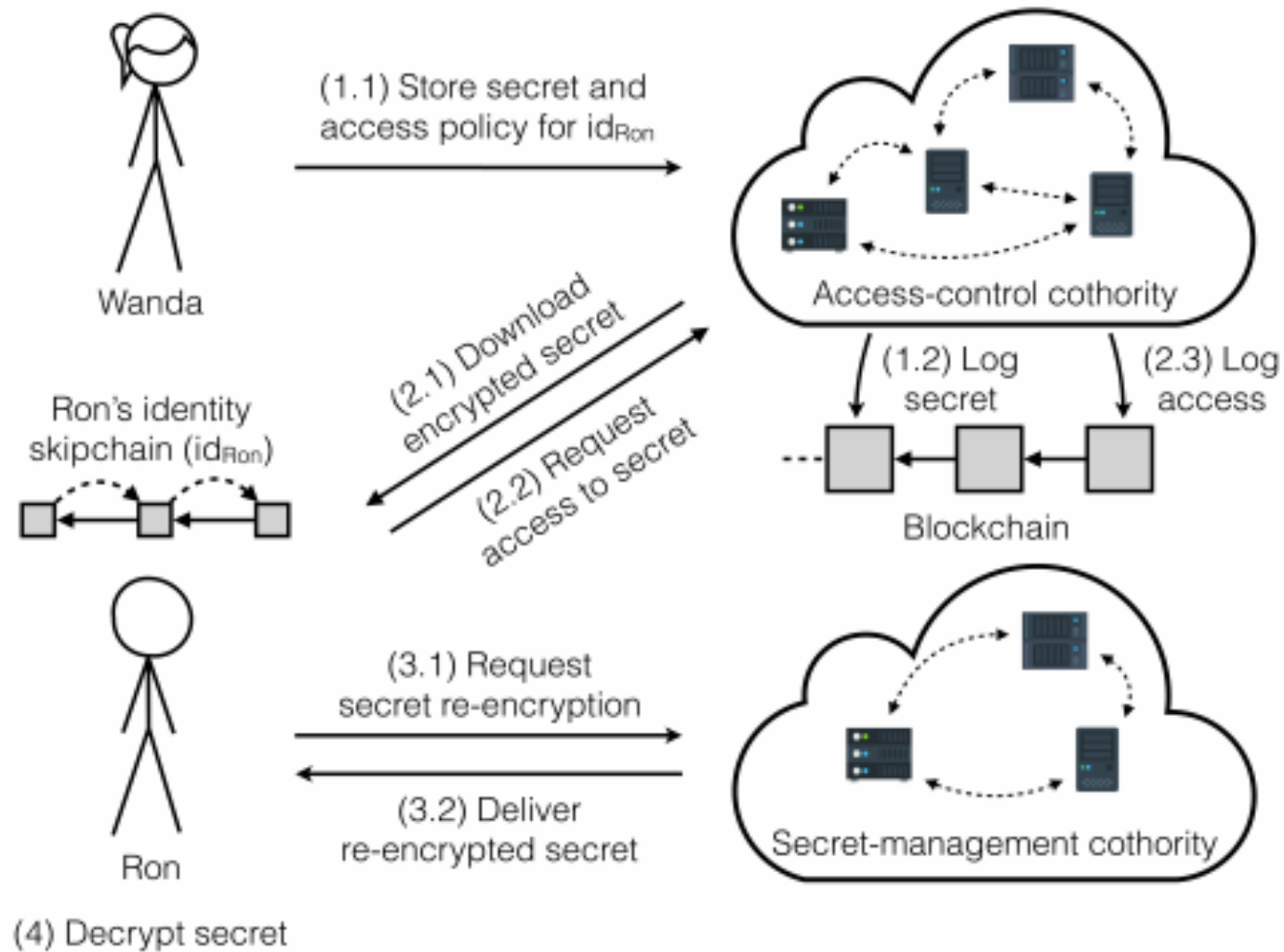


Distributed Access Right Controls

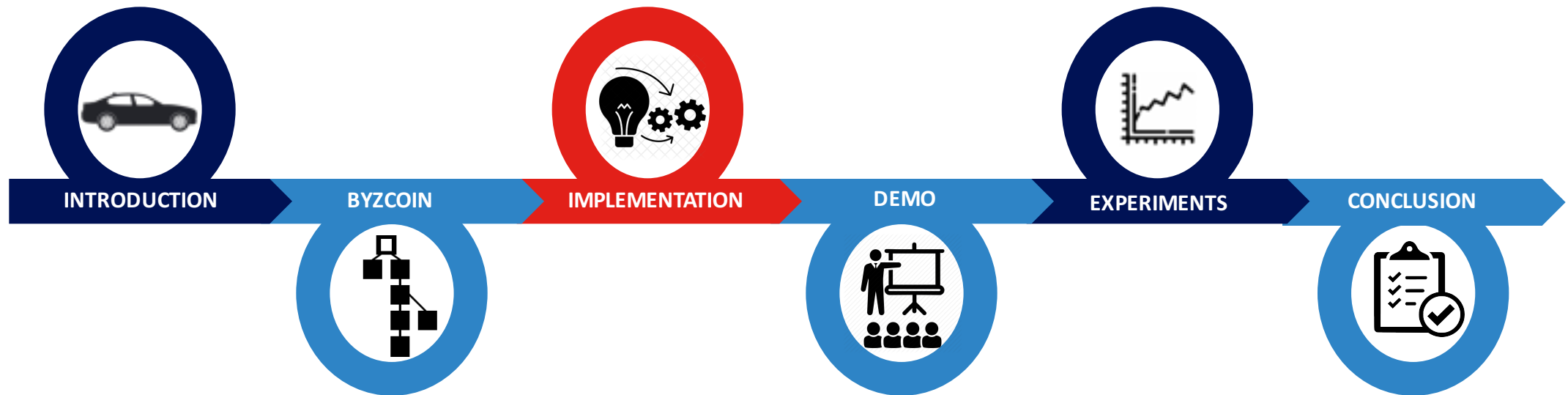
- Set of rules
- Rule – “action” : ”expression with allowed identities”
- Evolution of Rules
- Delegating the permissions to another DARC

Private Data over a Blockchain

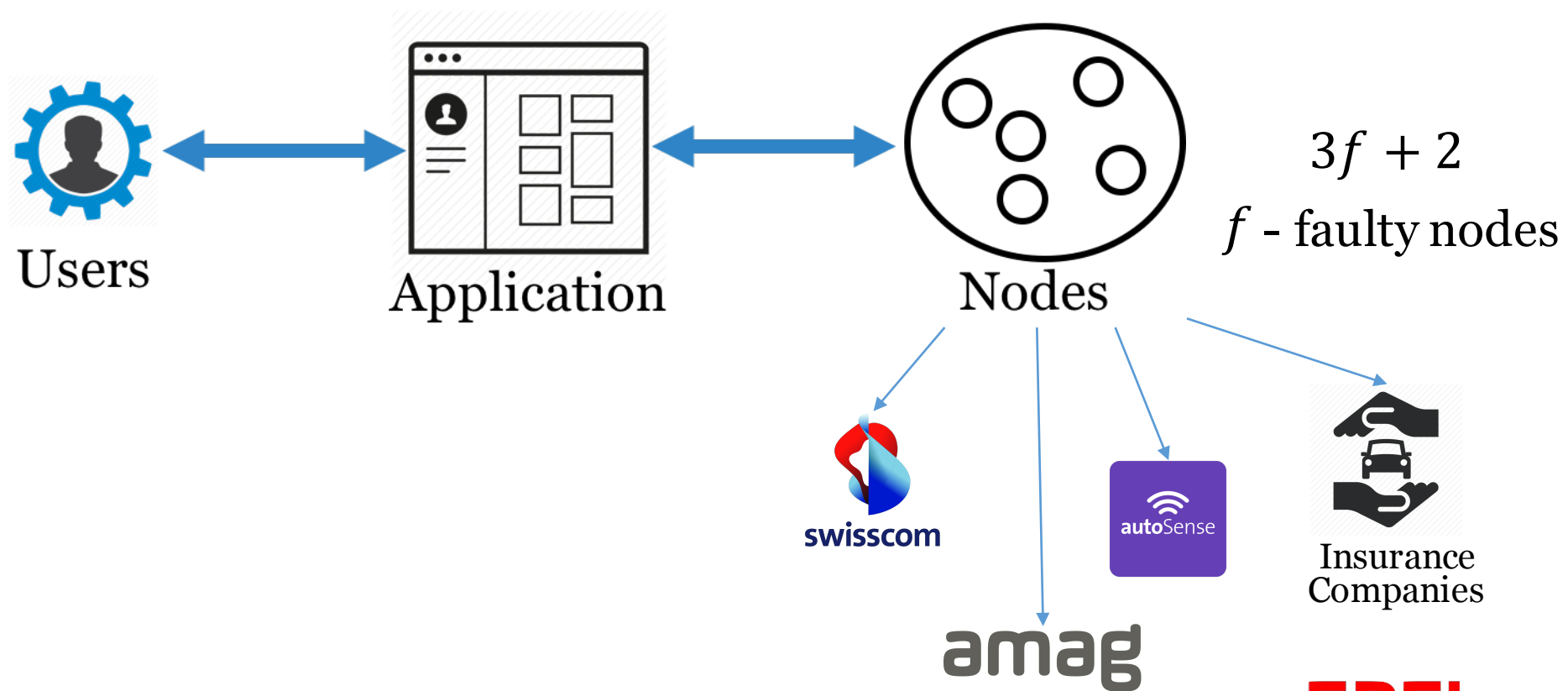
Calypso



Overview

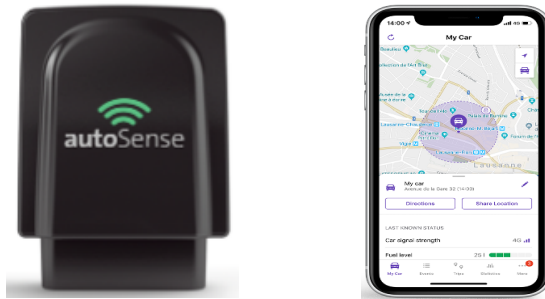


Implementation



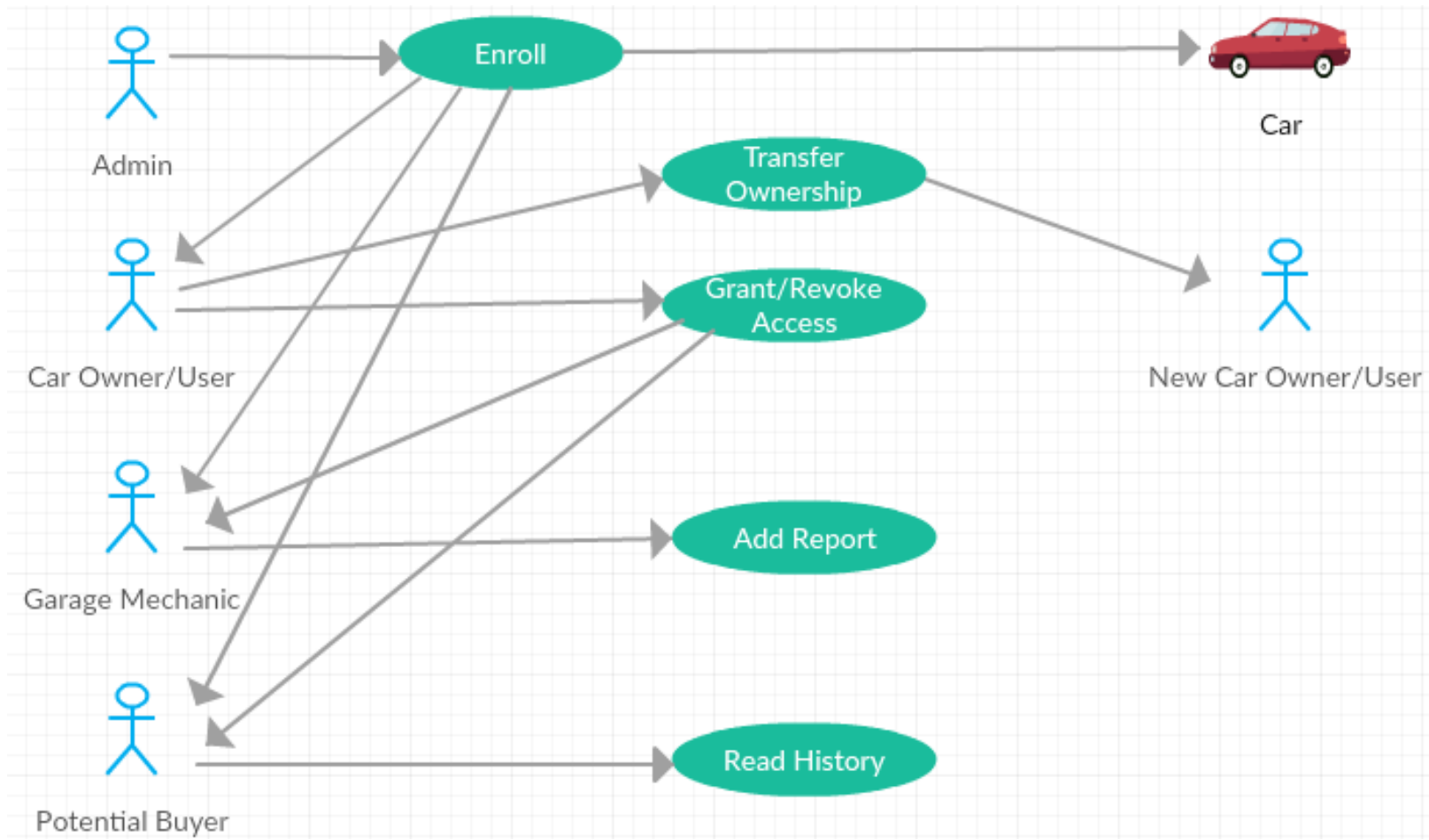
Business Case

- AutoSense IoT Devices



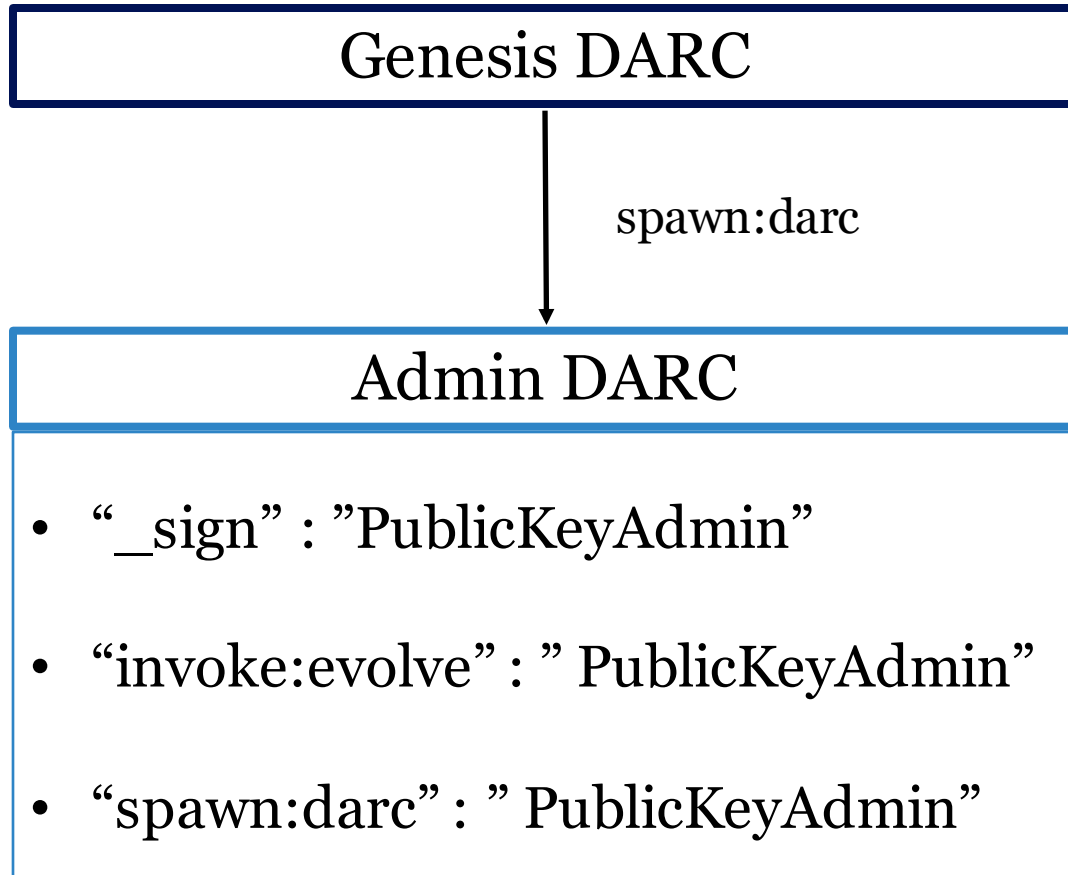
- Profit – customers of dongle devices
- AMAG – increased value of cars
- Insurance Companies – accidents detection in real time

Use Case Diagram

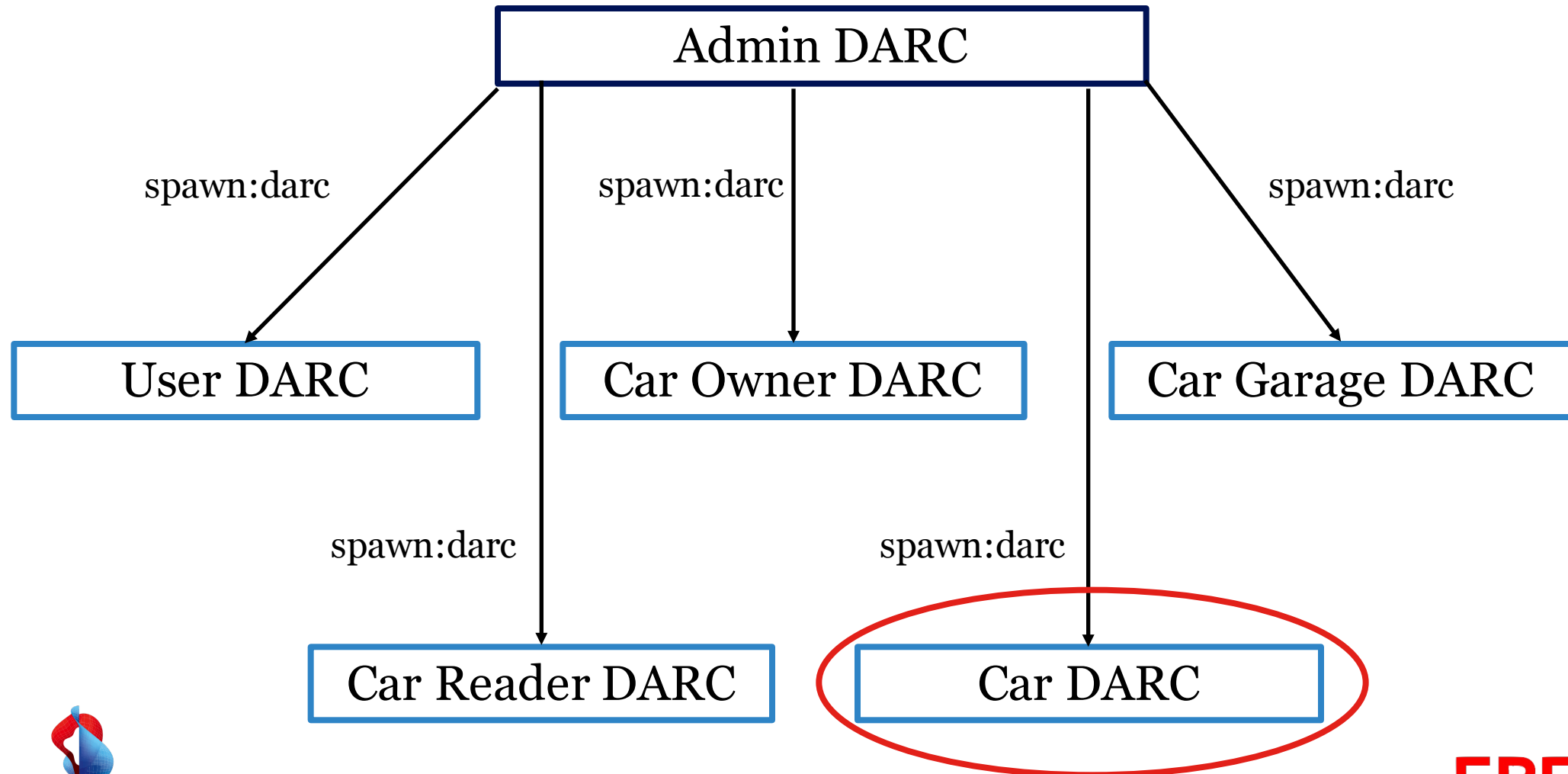


Access Control in the System

DARCs



DARCs



DARCs

Car DARC

- “spawn:car” : ”adminDARC”
- “invoke:car.addReport” : ” carGarageDARC”
- “spawn:calypsoWrite” : “carGarageDARC”
- “spawn:calypsoRead” : “carReaderDARC”

Car Contract

- Instructions:
 - spawn : car
 - invoke : car.addReport
- Data Structures:

Car
string VIN
[]Report Reports

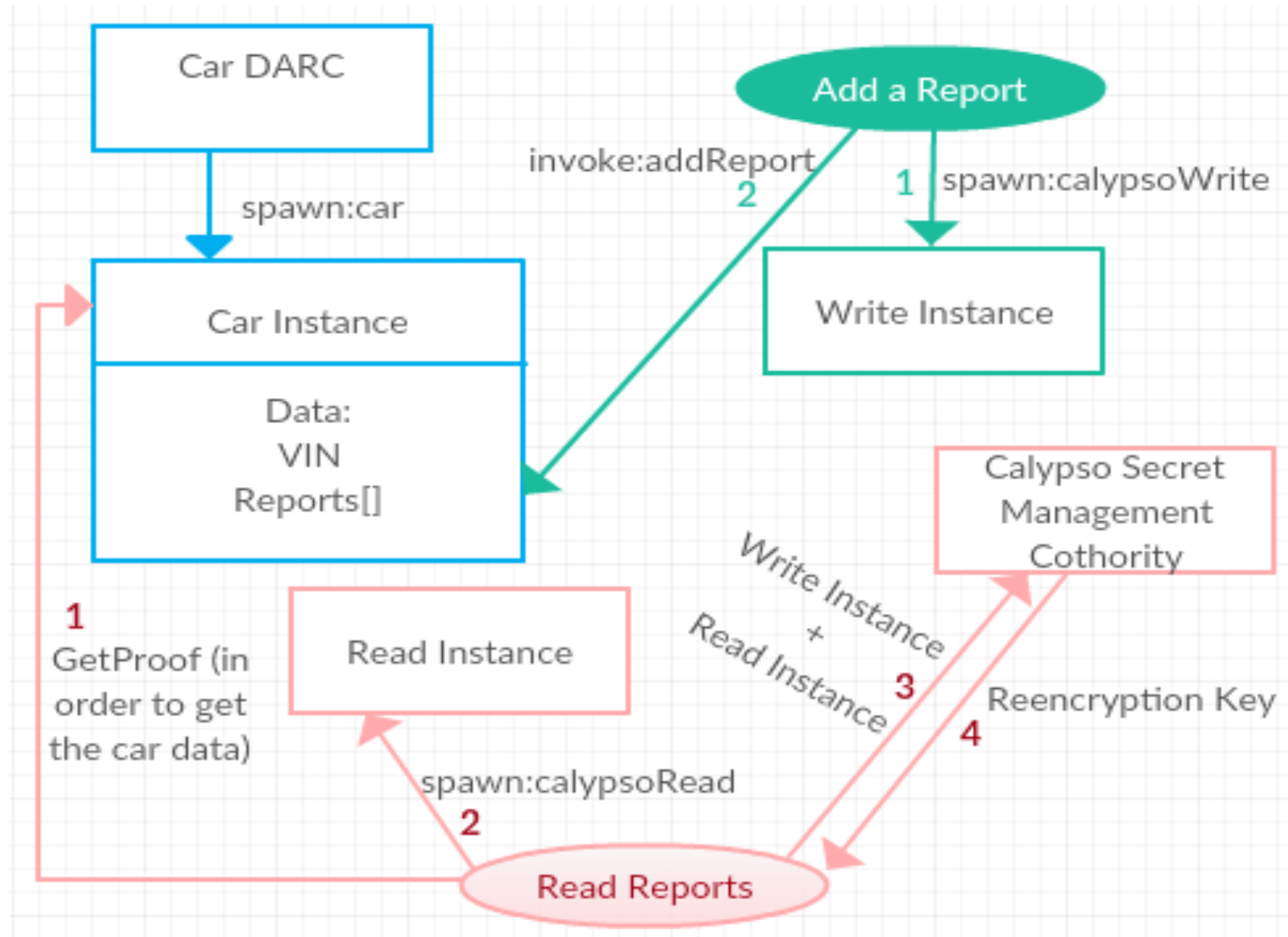
Report
string Date
string GarageID
[]byte WriteInstanceID

SecretData
string Mileage
boolean Warranty
string RepairNote
string Score

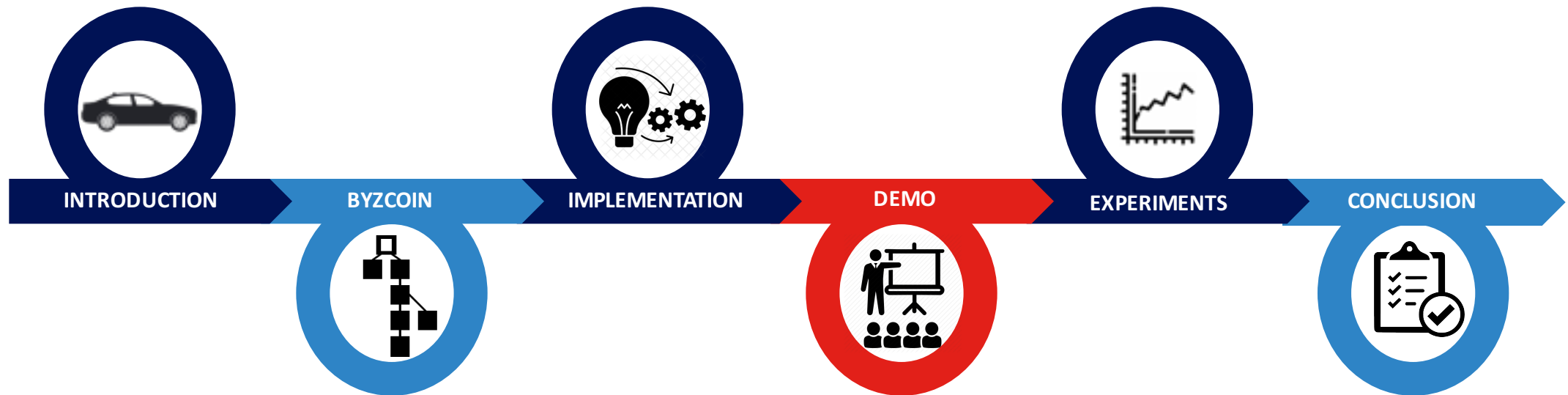
Client Application

User-Friendly Way of Interaction

Client Application



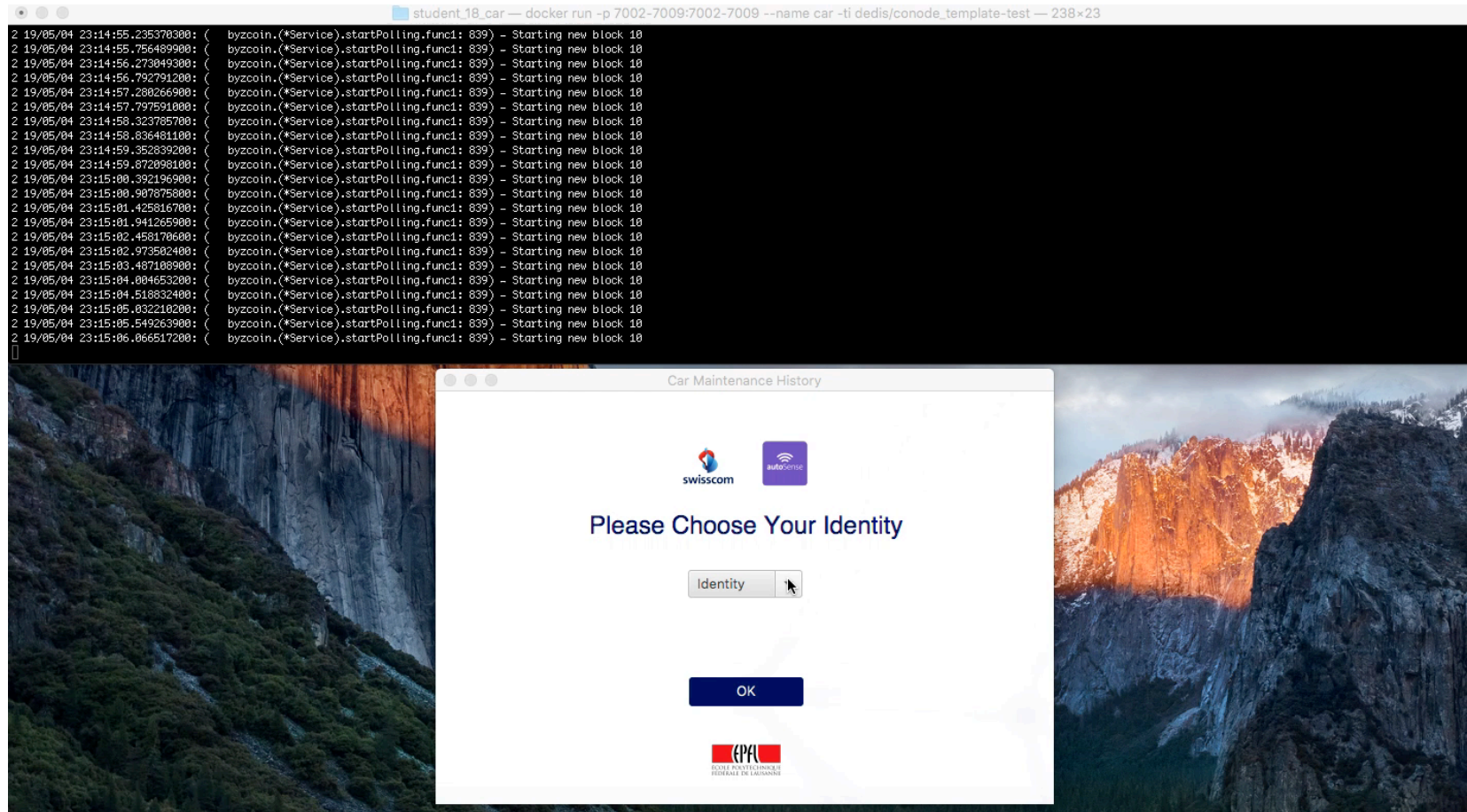
Overview



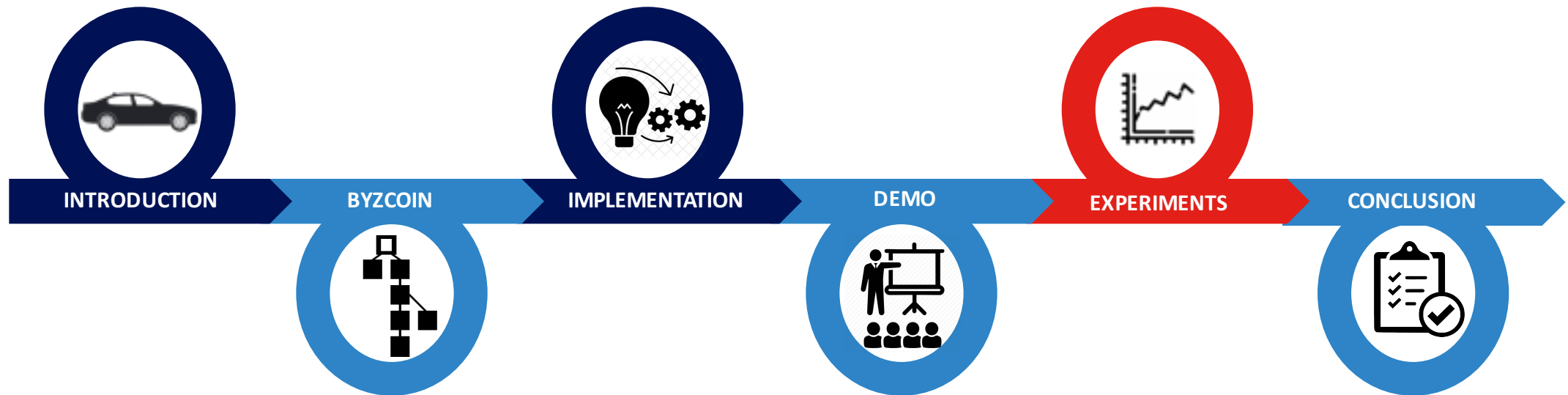
DEMO

- Logs of Conodes
- User Interface (Desktop Application)

DEMO



Overview



Experiments

- Larger Networks and Concurrent Transactions
- IC Cluster with Mininet Platform:
 - Each Server: 24 cores, 256GB of RAM, 2.5GHz processor
- Measure:
 - Wall Time
 - System Cost

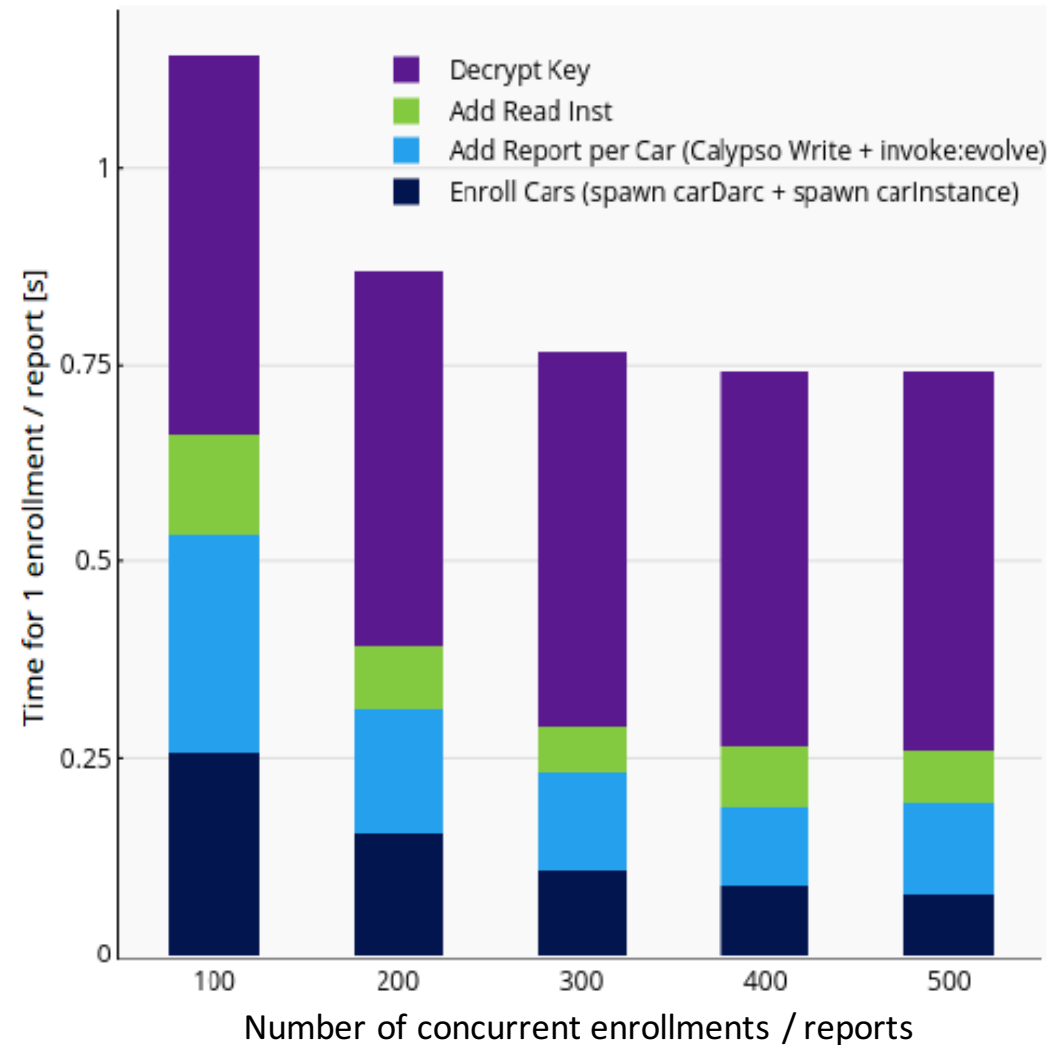
Experiments

Constant Number of Nodes

Variable Number of Concurrent Car Enrollments

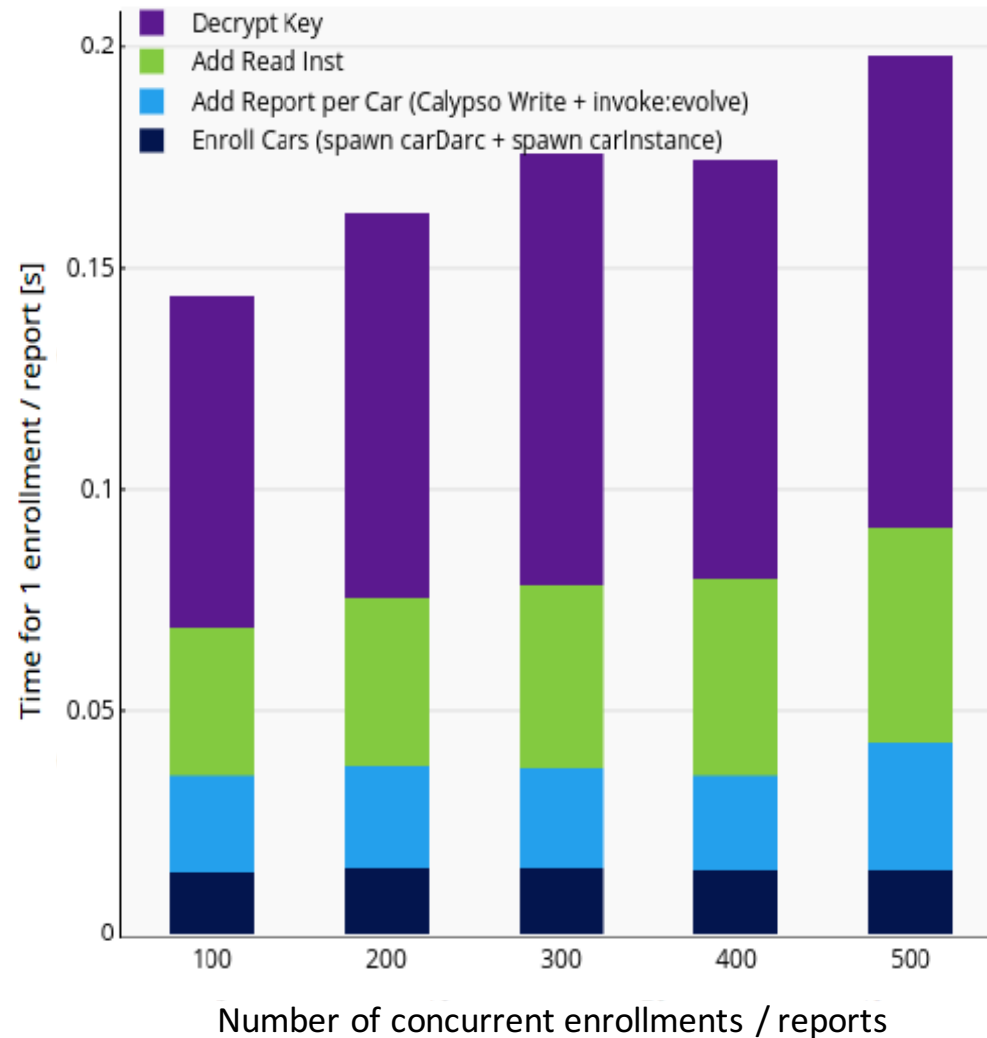
Experiments

- Wall Time
 - 5 Nodes, 2 servers
 - Bandwidth = 100Mbps
 - Delay = 100ms
 - Block Interval = 5s



Experiments

- System Cost
 - 5 Nodes, 2 servers
 - Bandwidth = 100Mbps
 - Delay = 100ms
 - Block Interval = 5s



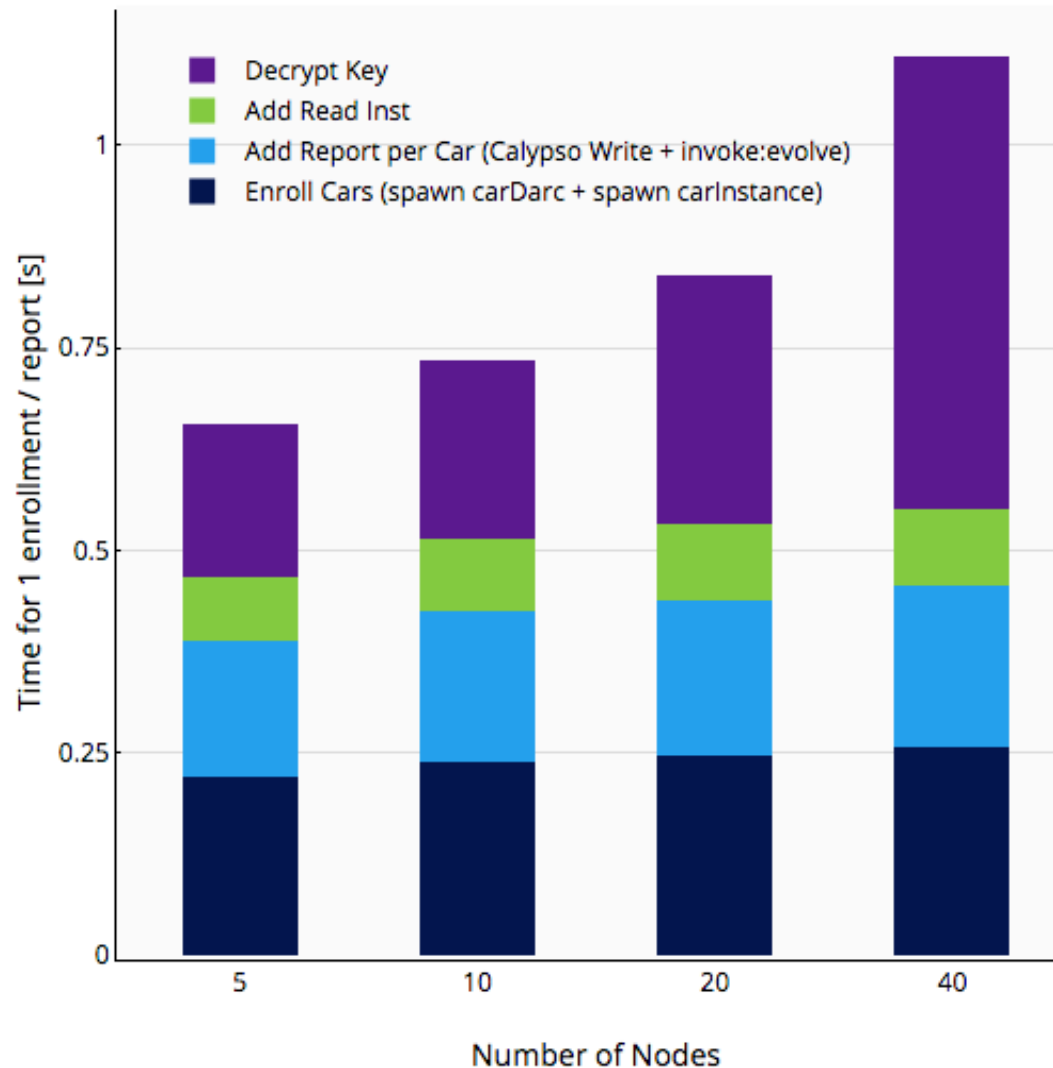
Experiments

**Constant Number of Concurrent Car
Enrollments**

Variable Number of Nodes

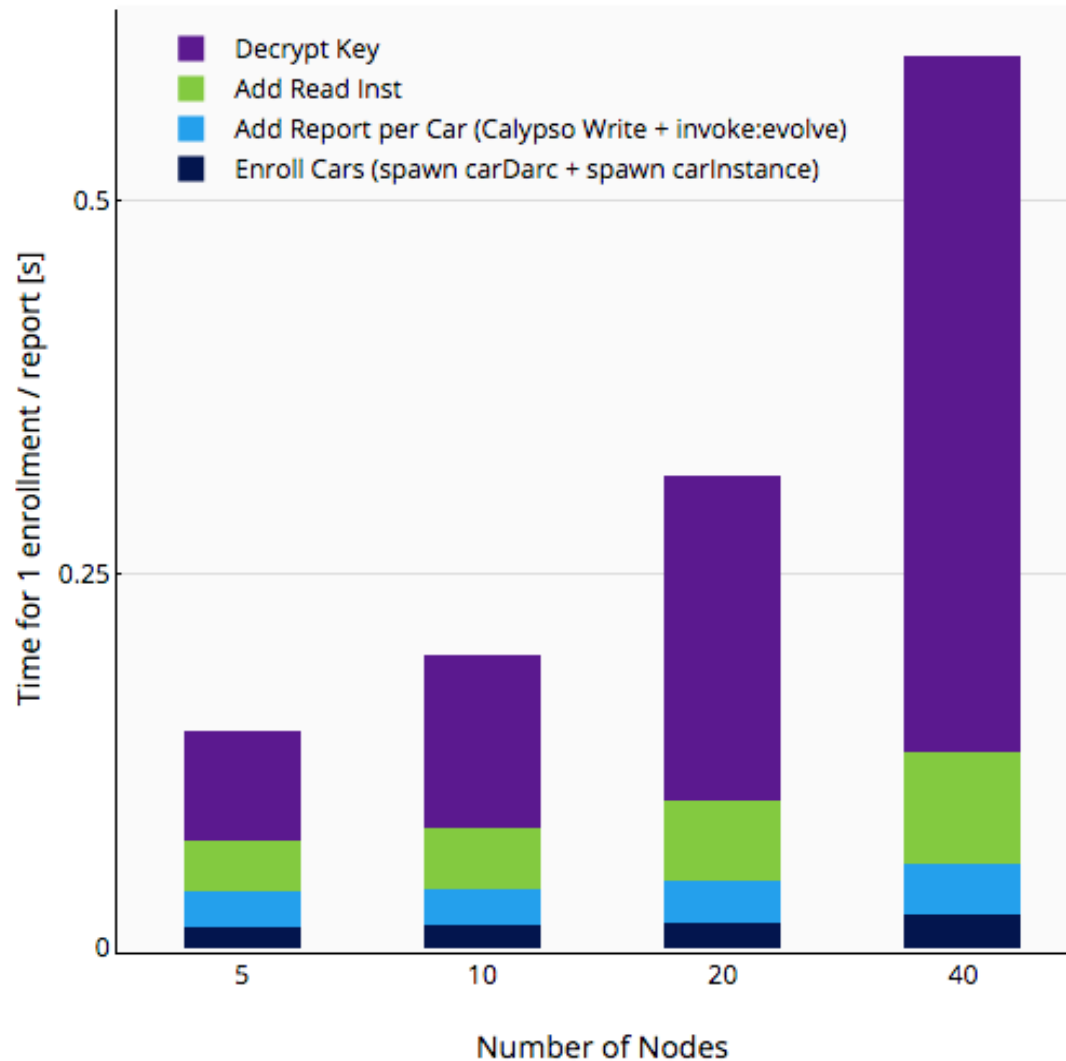
Experiments

- Wall Time
 - 2 servers
 - Bandwidth = 100Mbps
 - Delay = 30ms
 - Block Interval = 5s

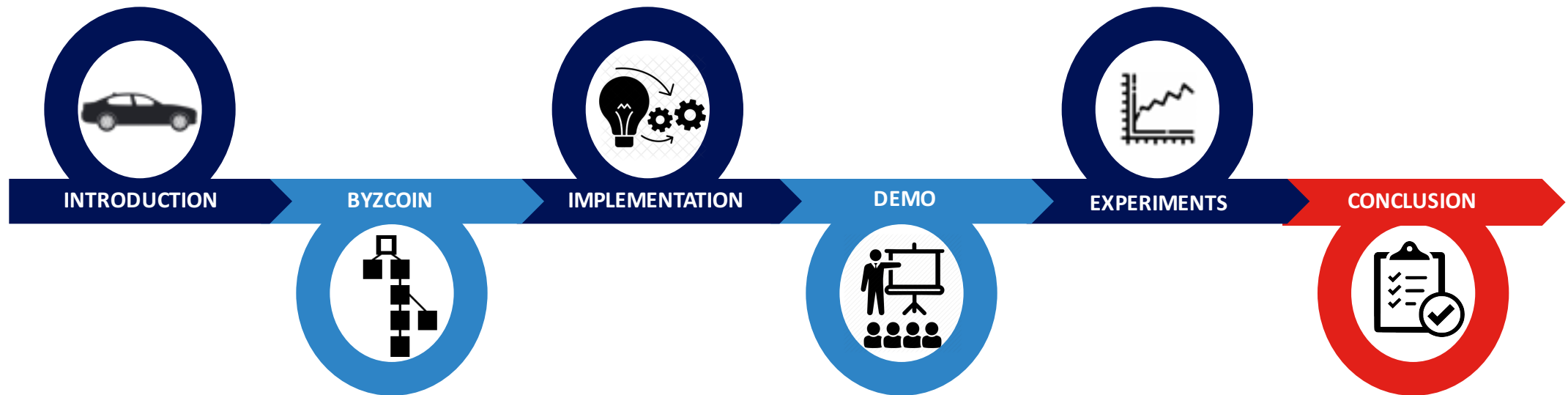


Experiments

- System Cost
 - 2 servers
 - Bandwidth = 100Mbps
 - Delay = 30ms
 - Block Interval = 5s



Overview



Conclusion

- Proof of Concept
- Implementation
 - Car Contract
 - Access Control
 - Calypso Interaction
 - Java Desktop Application
- Experiments
- Future Work



Thank You for Your Attention!

Overview

