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
  - ...

[Diagram showing trust establishment between entities]
Blockchain Data Structure

Submitting a Transaction to a Blockchain

1. Create Transaction
2. Broadcast
3. Transaction Verification
4. Block Creation
5. Broadcast
6. Consensus
7. Transaction Confirmation
8. Transaction Confirmation
ByzCoin

Source: https://raw.githubusercontent.com/dedis/cothority/master/byzcoin/ByzCoin.png
ByzCoinX Consensus Protocol

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

Source: https://raw.githubusercontent.com/dedis/cothority/master/byzcoin/ByzCoin.png
ByzCoin

Source: https://raw.githubusercontent.com/dedis/cothority/master/byzcoin/ByzCoin.png
Instructions

- Spawn
- Invoke
- Delete
ByzCoin

Source: https://raw.githubusercontent.com/dedis/cothority/master/byzcoin/ByzCoin.png
Distributed Access Right Controls

• Set of rules

• Rule – “action” : ”expression with allowed identities”

• Evolution of Rules

• Delegating the permissions to another DARC

Source: https://raw.githubusercontent.com/dedis/cothority/master/byzcoin/ByzCoin.png
Private Data over a Blockchain
Calypso

Source: CALYPSO: Auditable Sharing of Private Data over Blockchains, 2018
Overview
Implementation

$3f + 2$

$f$ - faulty nodes

Users → Application → Nodes → Insurance Companies

3f + 2

f - faulty nodes
Business Case

• AutoSense IoT Devices

• Profit – customers of dongle devices

• AMAG – increased value of cars

• Insurance Companies – accidents detection in real time
DARCs

Access Control in the System
DARCs

Genesis DARC

spawn:darc

Admin DARC

- "_sign" : "PublicKeyAdmin"
- "invoke:evolve" : "PublicKeyAdmin"
- "spawn:darc" : "PublicKeyAdmin"
DARC

Admin DARC

User DARC

spawn:darc

Car Owner DARC

spawn:darc

Car Garage DARC

spawn:darc

Car Reader DARC

spawn:darc

Car DARC

spawn:darc
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:

<table>
<thead>
<tr>
<th>Car</th>
<th>Report</th>
<th>SecretData</th>
</tr>
</thead>
<tbody>
<tr>
<td>string VIN</td>
<td>string Date</td>
<td>string Mileage</td>
</tr>
<tr>
<td>[]Report Reports</td>
<td>string GarageID</td>
<td>boolean Warranty</td>
</tr>
<tr>
<td></td>
<td>[]byte WriteInstanceID</td>
<td>string RepairNote</td>
</tr>
<tr>
<td></td>
<td></td>
<td>string Score</td>
</tr>
</tbody>
</table>
Client Application

User-Friendly Way of Interaction
Client Application

- Car DARC
  - spawn:car

- Car Instance
  - Data: VIN
  - Reports[]
  - 1 GetProof (in order to get the car data)

- Add a Report
  - invoke:addReport
  - 2 spawn:calypsoWrite

- Write Instance
  - spawn:calypsoWrite

- Calypso Secret Management Cothority
  - Write Instance
  + Read Instance
  - 3 Reencryption Key

- Read Reports
  - spawn:calypsoRead
  - 2

- Read Instance
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