The Technical Design of Blockchain Applications in Mobility

Sid Masih - *UC Berkeley MOBI Fellow*

This is a high level talk

Come talk to me later for the engineering

Who Am I?

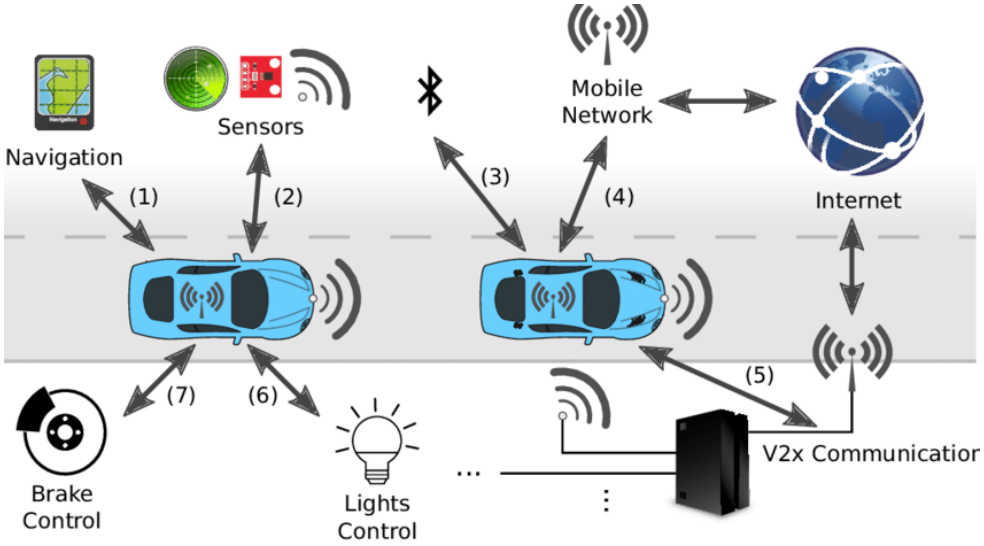
- I am Sid
- UC Berkeley Computer Science
- Systems Engineering
- Worked in big data systems, networking research, autonomous vehicles research, and blockchain systems
- Working at Facebook
- Currently working on the Vehicle Identity Standards Group

MOBI

Framing the Problem

The Mobile Environment

- Hyperconnectivity
- Moving actors
- Lossy connections
- Bandwidth



MOBI

Blockchain Constraints

Blockchain has important potential drawbacks

- Transaction speeds
- Expensive storage
- Liveness and Synchrony

MOBI

A good blockchain system must address these constraints

The Main Blockchain Design Verticals

Scalability

Privacy

Latency and Liveness

Crypto-Economics

MOBI

Blockchain Stack

Application Layer

Sybil Control Mechanism

Consensus

Network

Hardware/Infrastructure

MOBI

Importance of Scalability

- Cited as the biggest objection to blockchain technology
- Storage
- Throughput
- Duplication of data

MOBI

Scalability

Throughput Scalability

- Sharding
- Protocol Design
- State Channels
- Hardware
- Specific Use-Case Chains
- Fewer Nodes

Storage Scalability

- Polynomial Encoding
- State Channels
- Specific Use-Case Chains
- Fewer Nodes

MOBI

Importance of Privacy

- Example: Bitcoin
- Natively all information is stored on chain
- Forcing users to put more information of themselves online for public scrutiny
- GDPR
- Recent interest in privacy and online presence (Equifax, Google, Facebook, etc.)

MOBI

Privacy

Protocol Privacy

- ZK-Snarks (ZCash, Zexe, etc.)
- Secure Enclaves (SGX-Oasis)
- Usually slow and difficult to understand
- Problems related to proving entities within the system
- Still an active area of research (especially at UC Berkeley)

Other Privacy Techniques

- Private or Semi-Private chains
- Changing on-chain entities
- Token Tumblers

MOBI

Bottom Line: Privacy still is not fully solved

MOBI

Latency and Liveness

- Latency
- Liveness
- Real time applications
- Example: Access at physical gates
- Example: Payments
- Latency and liveness are critical for network usability

MOBI

Latency and Liveness

Content Distribution Networks

Cut through routing/caching

Network protocols like UDP

Fewer validators

MOBI

Networks must be active and available

Crypto-Economics

Validators

Privileges

Rewards

Cheating

Tokens ← (not always)

MOBI

Example: Vehicle Identity

Vehicle Identity (VID)

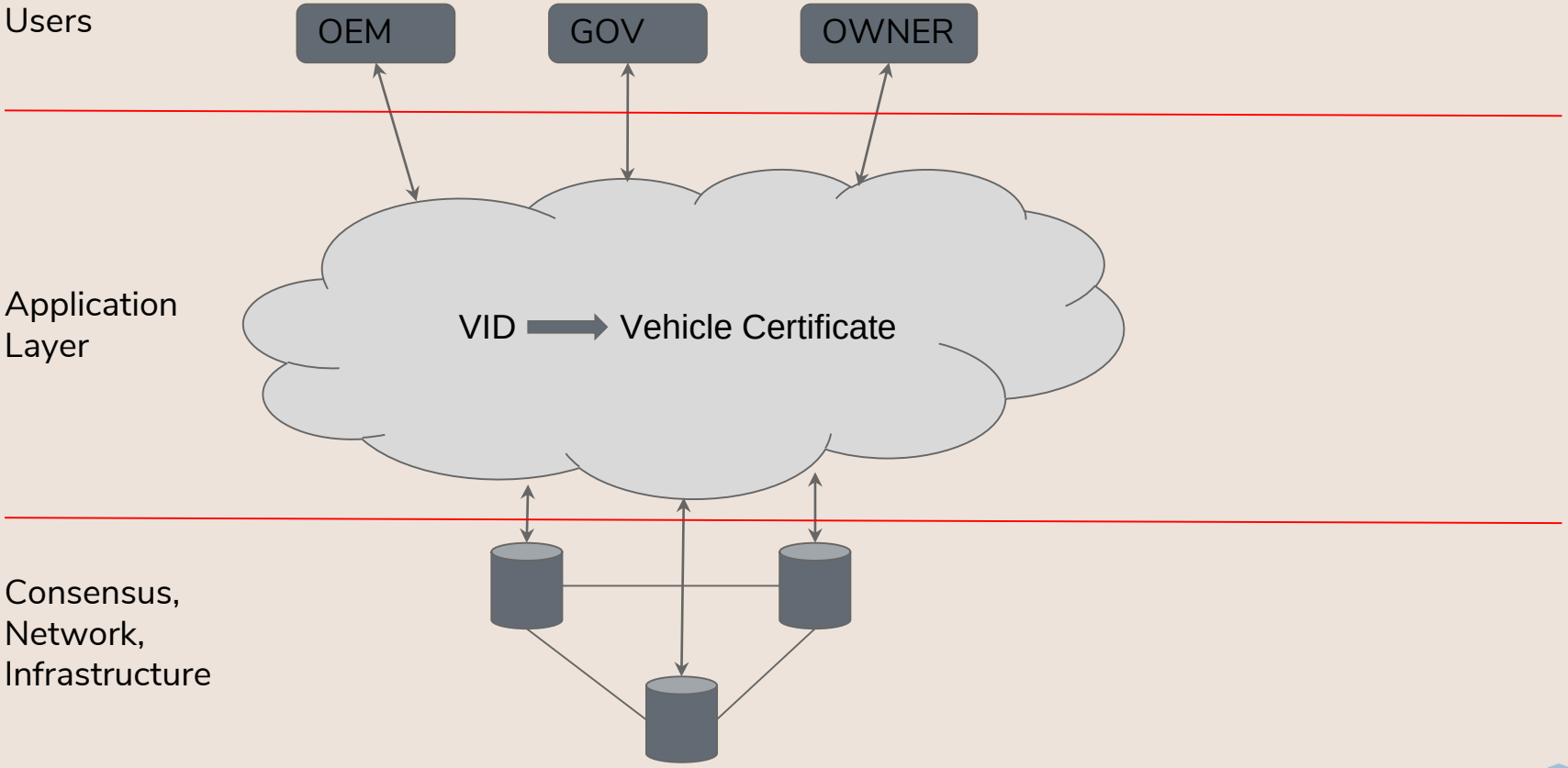
We want a unique number that identifies a car

We want that number to map to a certificate

We want to have entities

We want those entities to have permissioned access

MOBI


Users
OEM
GOV
OWNER
Application Layer
VID
Vehicle Certificate
Consensus, Network, Infrastructure

Vehicle Identity (VID)

Scalability

Privacy

Latency and Liveness

Crypto-Economics

MOBI

We just examined a real project with respect to the four design verticals

Questions?

MOBI