

# ChargeltUp: On Blockchain-based technologies for Autonomous Vehicles

Alejandro Ranchal Pedrosa <sup>1,2</sup>    Giovanni Pau <sup>1,3</sup>

<sup>1</sup>LIP6 – Sorbonne Université, Paris, France

<sup>2</sup>CEA LIST, Gif-sur-Yvette, France  
EIT Digital, Stockholm, Sweden

<sup>3</sup>DISI — Università di Bologna, Bologna, Italy  
CS Dept — University of California, Los angeles, CA

June 15, 2018

# Blockchain for Autonomous Vehicles

## State Channels

- Motivations: trustless, reliable, decentralized system, etc.
- Challenges
  - latency

# Blockchain for Autonomous Vehicles

## State Channels

- Motivations: trustless, reliable, decentralized system, etc.
- Challenges
  - latency
- How is the judicial system not so bloated, with the amount of contracts that we all sign?

# Blockchain for Autonomous Vehicles

## State Channels

- Motivations: trustless, reliable, decentralized system, etc.
- Challenges
  - latency
- How is the judicial system not so bloated, with the amount of contracts that we all sign?
- We sign contracts everyday but. . .

# Blockchain for Autonomous Vehicles

## State Channels

- Motivations: trustless, reliable, decentralized system, etc.
- Challenges
  - latency
- How is the judicial system not so bloated, with the amount of contracts that we all sign?
- We sign contracts everyday but. . .
  - We (almost) never enforce them
    - Only if dispute
    - In that case, we go to court, and if we are right, we win.

# Blockchain for Autonomous Vehicles

## State Channels

- Motivations: trustless, reliable, decentralized system, etc.
- Challenges
  - latency
- How is the judicial system not so bloated, with the amount of contracts that we all sign?
- We sign contracts everyday but. . .
  - We (almost) never enforce them
    - Only if dispute
    - In that case, we go to court, and if we are right, we win.
  - the blockchain is the court

# Blockchain for Autonomous Vehicles

## State Channels

- Motivations: trustless, reliable, decentralized system, etc.
- Challenges
  - latency
- How is the judicial system not so bloated, with the amount of contracts that we all sign?
- We sign contracts everyday but. . .
  - We (almost) never enforce them
    - Only if dispute
    - In that case, we go to court, and if we are right, we win.
  - the blockchain is the court
    - We should look for a way to create a 2nd-layer where people can interact directly without going to "court" (the blockchain)
    - Only go to blockchain to finish the contract, or in the event of a dispute, to ascribe blame

# State Channels

- Suppose a car and a charging station are frequently trading
  - The station sells energy (electricity, gas, hydrogen, etc.)
  - The car purchases it



# State Channels

- Suppose a car and a charging station are frequently trading
  - The station sells energy (electricity, gas, hydrogen, etc.)
  - The car purchases it
- The car can lock-in some tokens with the station for future trades between the two → the car opens a channel

# State Channels

- Suppose a car and a charging station are frequently trading
  - The station sells energy (electricity, gas, hydrogen, etc.)
  - The car purchases it
- The car can lock-in some tokens with the station for future trades between the two → the car opens a channel
  - Inside this channel, they can:
  - sign and trade blockchain-enforceable information

# State Channels

- Suppose a car and a charging station are frequently trading
  - The station sells energy (electricity, gas, hydrogen, etc.)
  - The car purchases it
- The car can lock-in some tokens with the station for future trades between the two → the car opens a channel
  - Inside this channel, they can:
    - sign and trade blockchain-enforceable information
    - without publishing on the blockchain (off-chain), nor paying fees

# State Channels

- Suppose a car and a charging station are frequently trading
  - The station sells energy (electricity, gas, hydrogen, etc.)
  - The car purchases it
- The car can lock-in some tokens with the station for future trades between the two → the car opens a channel
  - Inside this channel, they can:
    - sign and trade blockchain-enforceable information
    - without publishing on the blockchain (off-chain), nor paying fees
    - **at the speed of their communication protocol (e.g. TCP).**

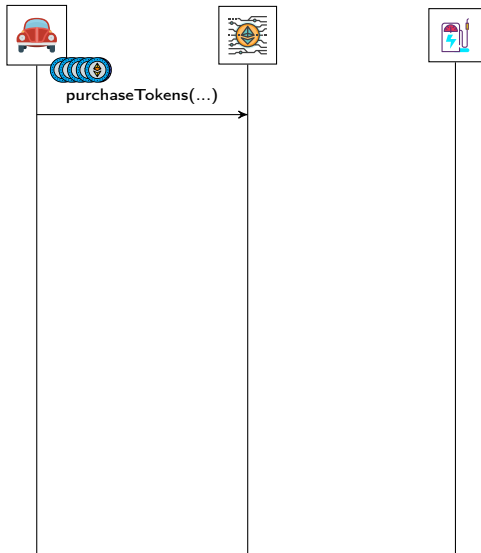
# State Channel

Phases: Opening a channel

Every channel has three main phases: setup, update and close.

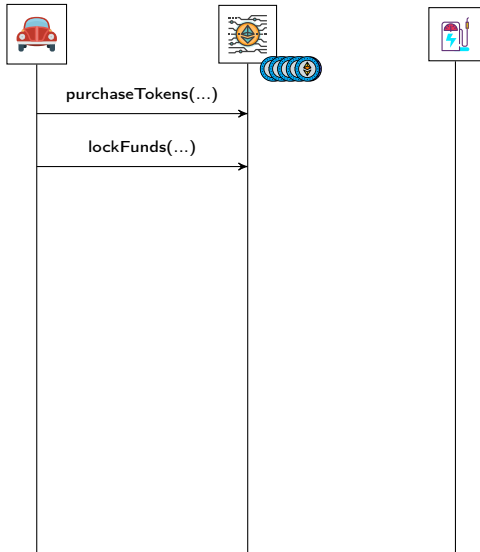
# State Channel

Phases: Opening a channel



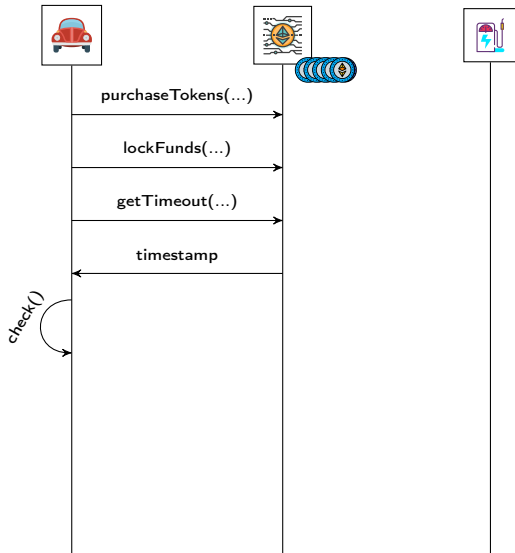
# State Channel

Phases: Opening a channel



# State Channel

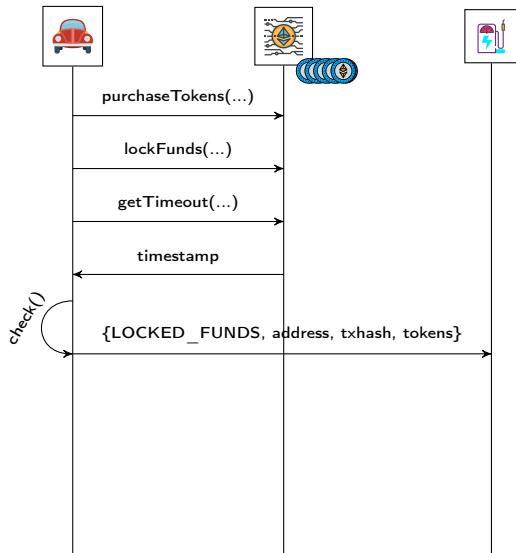
Phases: Opening a channel





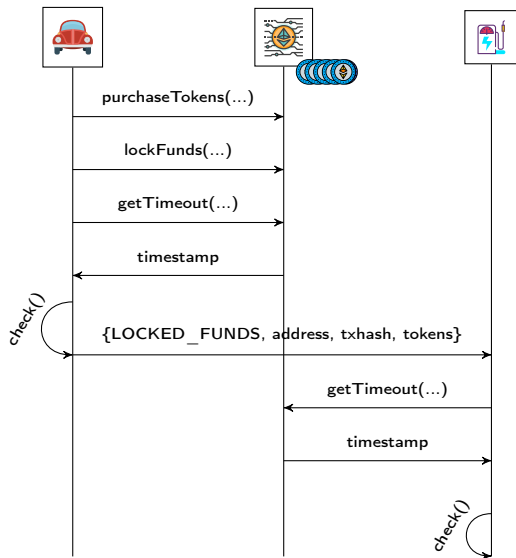
# State Channel

Phases: Opening a channel



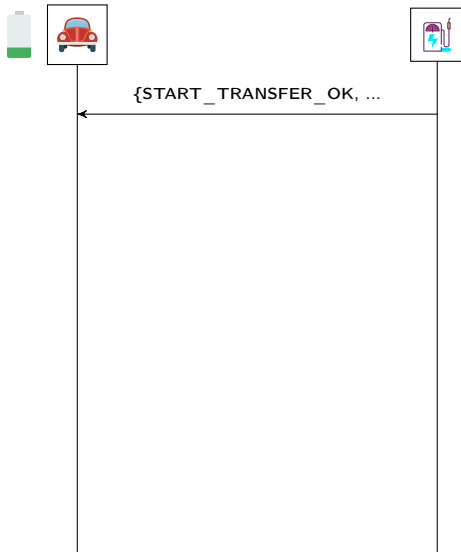
# State Channel

Phases: Opening a channel



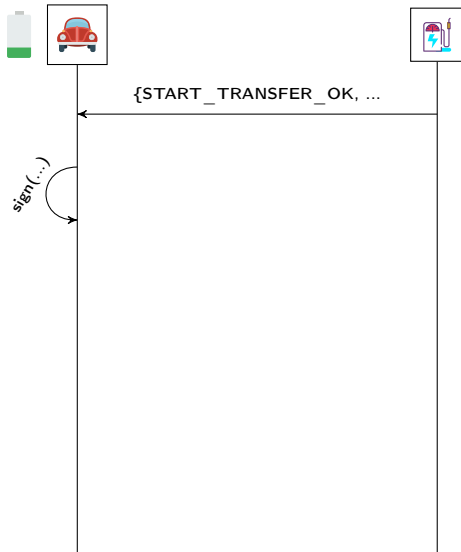
# State Channel

Phases: Updating a channel



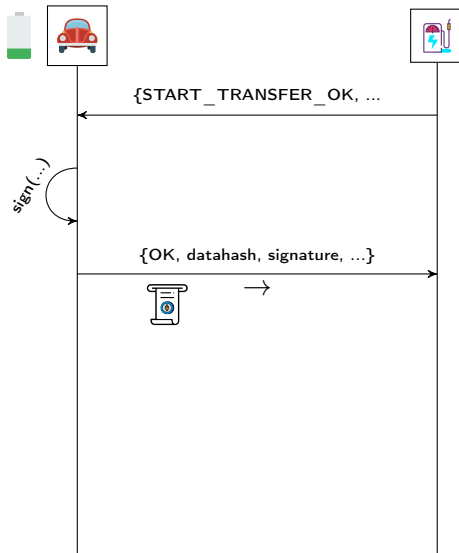
# State Channel

Phases: Updating a channel



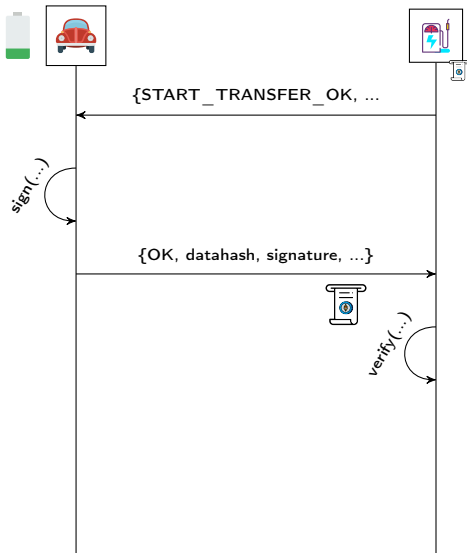
# State Channel

Phases: Updating a channel



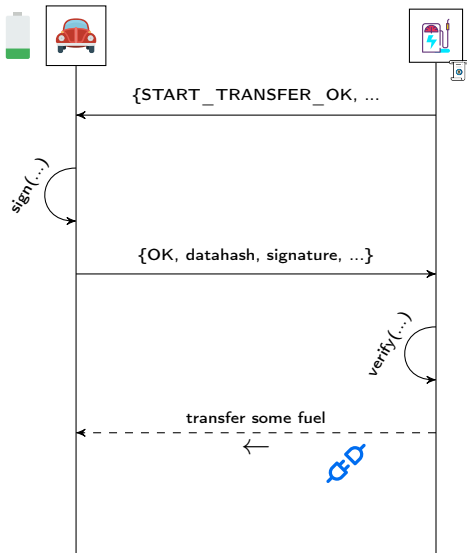
# State Channel

Phases: Updating a channel



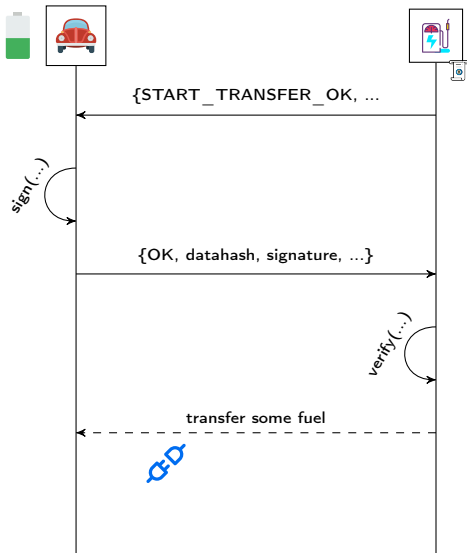
# State Channel

Phases: Updating a channel



# State Channel

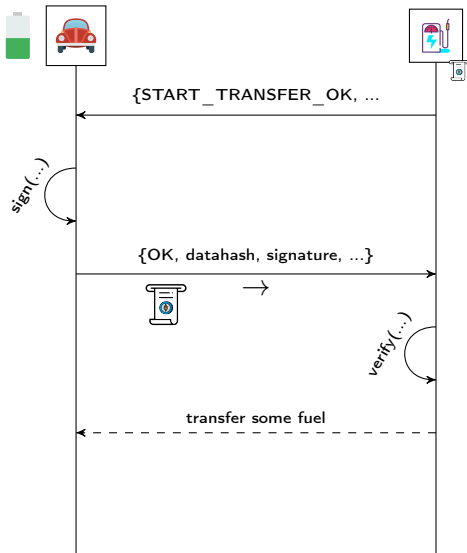
Phases: Updating a channel





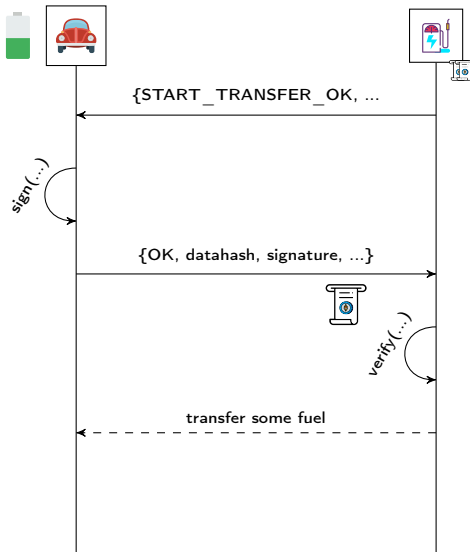
# State Channel

Phases: Updating a channel



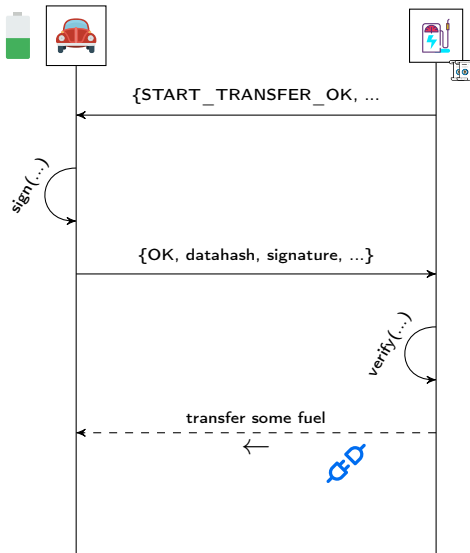
# State Channel

Phases: Updating a channel



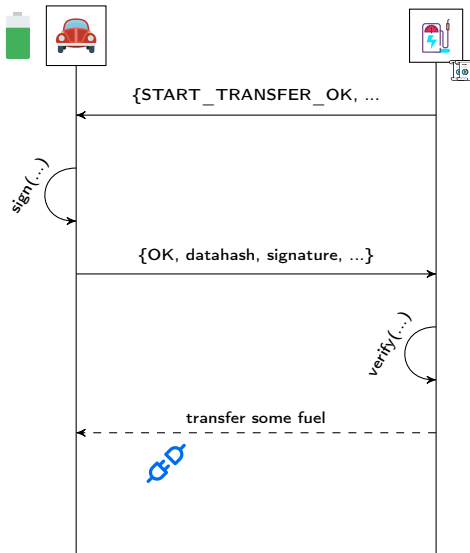
# State Channel

Phases: Updating a channel



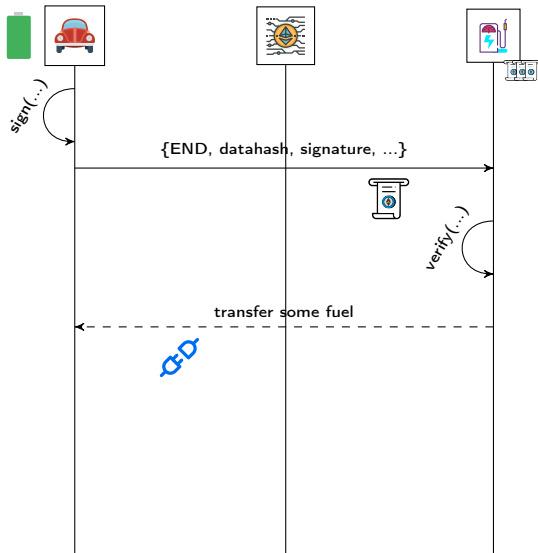
# State Channel

Phases: Updating a channel



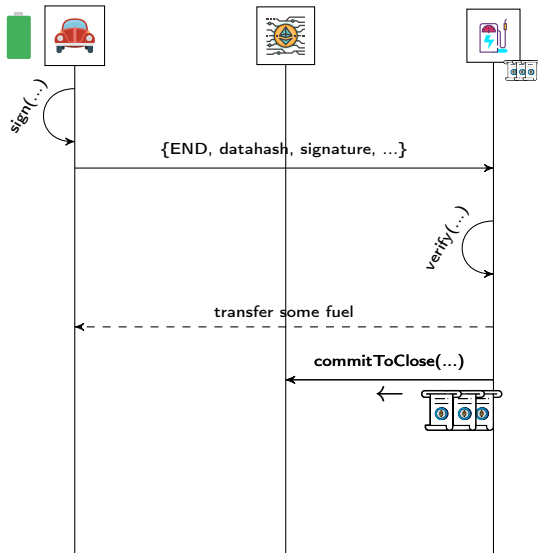
# State Channel

## Phases - Close



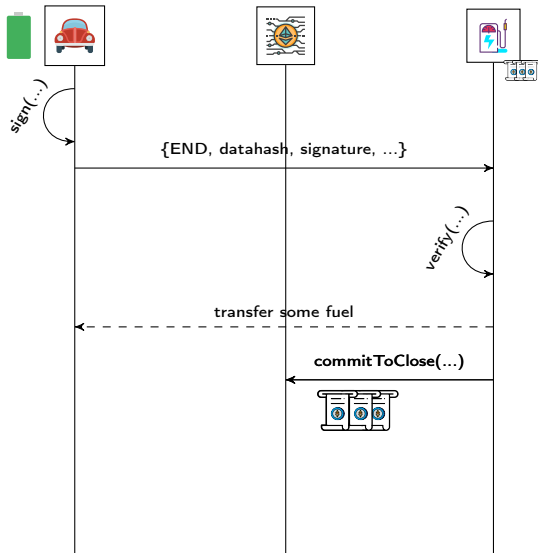
# State Channel

## Phases - Close



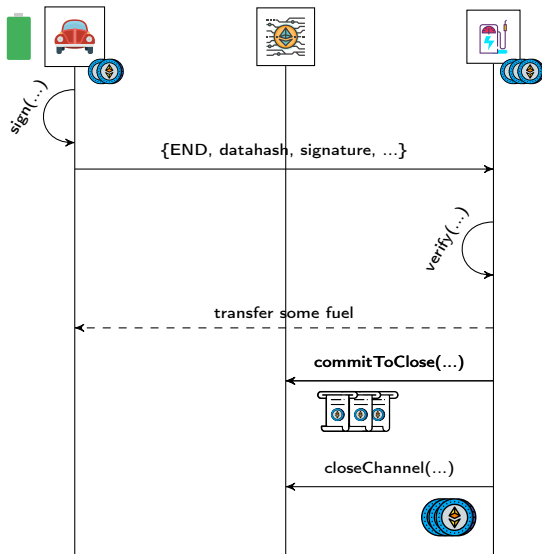
# State Channel

## Phases - Close



# State Channel

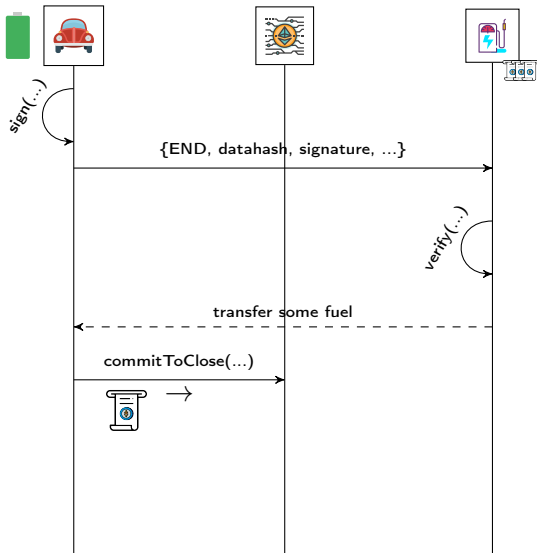
## Phases - Close





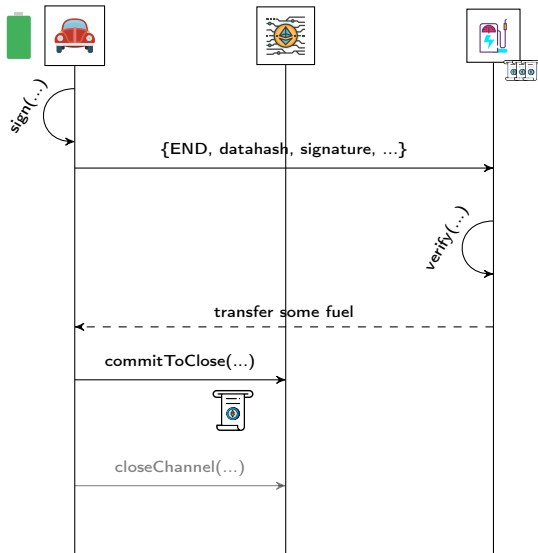
# State Channel

## Phases - Close



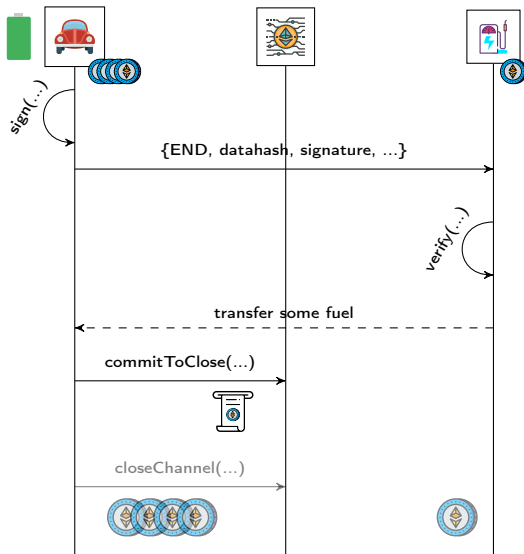
# State Channel

## Phases - Close



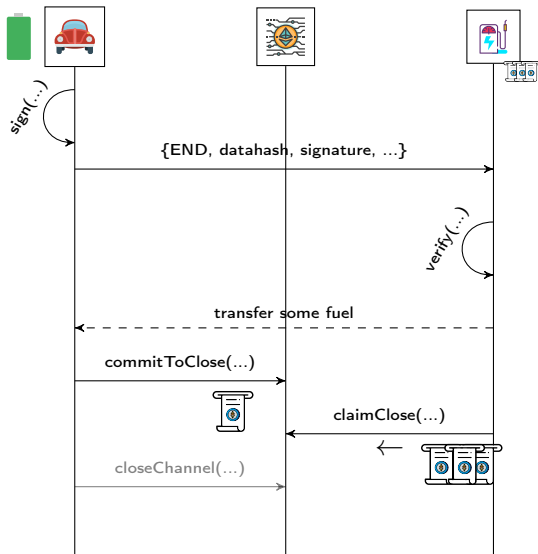
# State Channel

## Phases - Close



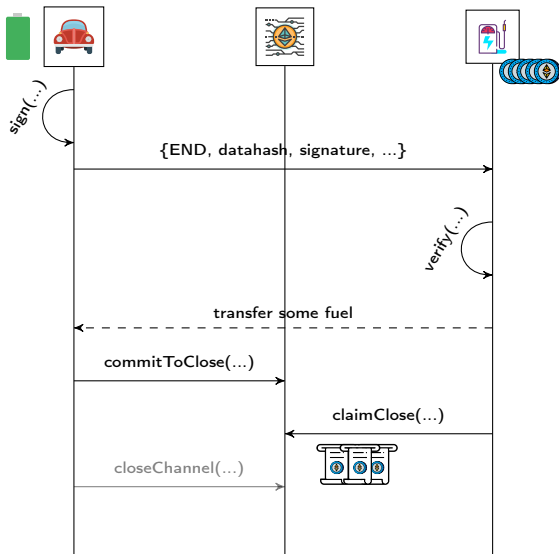
# State Channel

## Phases - Close



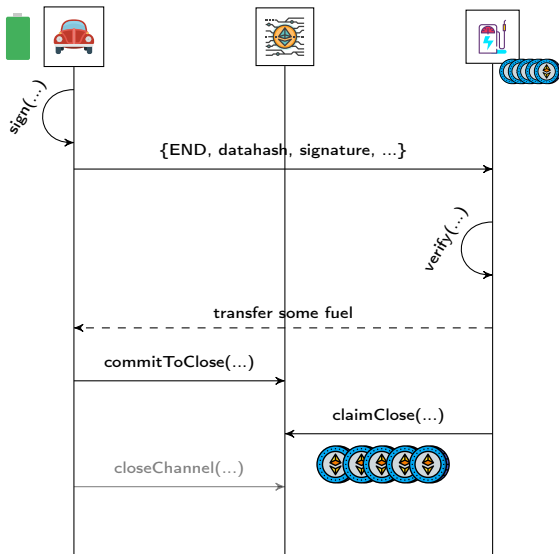
# State Channel

## Phases - Close



# State Channel

## Phases - Close



# Results & Improvements

- Latency
  - Open channel  $\rightarrow$  that of blockchain + that of communication protocol

# Results & Improvements

- Latency
  - Open channel  $\rightarrow$  that of blockchain + that of communication protocol
    - Can be opened beforehand, or for multiple charges



# Results & Improvements

- Latency
  - Open channel  $\rightarrow$  that of blockchain + that of communication protocol
    - Can be opened beforehand, or for multiple charges
  - Update and close channel  $\rightarrow$  that of communication protocol (e.g. TCP)

# Results & Improvements

- Latency
  - Open channel → that of blockchain + that of communication protocol
    - Can be opened beforehand, or for multiple charges
  - Update and close channel → that of communication protocol (e.g. TCP)
- Private vs trustless-based system

# Results & Improvements

- Latency
  - Open channel → that of blockchain + that of communication protocol
    - Can be opened beforehand, or for multiple charges
  - Update and close channel → that of communication protocol (e.g. TCP)
- Private vs trustless-based system
  - For fully trustless system, both parties must have:
    - Contract address and Application Binary Interface ABI
    - Contract code

# Results & Improvements

- Latency
  - Open channel → that of blockchain + that of communication protocol
    - Can be opened beforehand, or for multiple charges
  - Update and close channel → that of communication protocol (e.g. TCP)
- Private vs trustless-based system
  - For fully trustless system, both parties must have:
    - Contract address and Application Binary Interface ABI
    - Contract code
  - Scanning the blockchain, it is possible to know all interactions

# Results & Improvements

- Latency
  - Open channel → that of blockchain + that of communication protocol
    - Can be opened beforehand, or for multiple charges
  - Update and close channel → that of communication protocol (e.g. TCP)
- Private vs trustless-based system
  - For fully trustless system, both parties must have:
    - Contract address and Application Binary Interface ABI
    - Contract code
  - Scanning the blockchain, it is possible to know all interactions
  - With ethereum, the trustless property comes at a cost in privacy

# Results & Improvements

- Latency
  - Open channel → that of blockchain + that of communication protocol
    - Can be opened beforehand, or for multiple charges
  - Update and close channel → that of communication protocol (e.g. TCP)
- Private vs trustless-based system
  - For fully trustless system, both parties must have:
    - Contract address and Application Binary Interface ABI
    - Contract code
  - Scanning the blockchain, it is possible to know all interactions
  - With ethereum, the trustless property comes at a cost in privacy
  - State channels increase privacy (updates off-chain)

# Results & Improvements

- Latency
  - Open channel → that of blockchain + that of communication protocol
    - Can be opened beforehand, or for multiple charges
  - Update and close channel → that of communication protocol (e.g. TCP)
- Private vs trustless-based system
  - For fully trustless system, both parties must have:
    - Contract address and Application Binary Interface ABI
    - Contract code
  - Scanning the blockchain, it is possible to know all interactions
  - With ethereum, the trustless property comes at a cost in privacy
  - State channels increase privacy (updates off-chain)
  - Fragmentable good

# Risks, Future Work & Applications

- Risks



# Risks, Future Work & Applications

- Risks
  - Forced expiration spam

# Risks, Future Work & Applications

- Risks
  - Forced expiration spam
  - Colluding miner

# Risks, Future Work & Applications

- Risks
  - Forced expiration spam
  - Colluding miner
  - Stale channel

# Risks, Future Work & Applications

- Risks
  - Forced expiration spam
  - Colluding miner
  - Stale channel
- Future Work & Applications
  - SMS control logs

# Risks, Future Work & Applications

- Risks
  - Forced expiration spam
  - Colluding miner
  - Stale channel
- Future Work & Applications
  - SMS control logs
  - SMSs connectivity

# Risks, Future Work & Applications

- Risks
  - Forced expiration spam
  - Colluding miner
  - Stale channel
- Future Work & Applications
  - SMS control logs
  - SMSs connectivity
  - Logs on the road

# Risks, Future Work & Applications

- Risks
  - Forced expiration spam
  - Colluding miner
  - Stale channel
- Future Work & Applications
  - SMS control logs
  - SMSs connectivity
  - Logs on the road
  - Carpooling

# Conclusion

- Blockchains can bring many applications for Autonomous Vehicles
- State channels can help cope with the latency constraints



# Conclusion

- Blockchains can bring many applications for Autonomous Vehicles
- State channels can help cope with the latency constraints
- We show here an actual implementation of a charging station
  - Evaluation
  - Improvements
  - Risks
  - Other applications

Q/A