Bridging the cyber and physical worlds using blockchains and smart contracts

Nikos Fotiou, Vasilios A. Siris, Spyros Voulgaris, **George C. Polyzos**

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Mobile Multimedia Laboratory

Dmitrij Lagutin

Aalto University
School of Electrical Engineering

Motivation

- IoT devices have limitations and cannot interact with blockchains/smart contracts
  – Limited computational power and storage
  – Limited network connectivity
  – Security and trust issues
- The output of an actuation operation cannot be easily verified using cyber means

Contributions

- realistic approach for paid IoT interactions:
  - ➢ limit loss in case of disruption of actuation
    - o micro-payments for micro-transactions
    - o make blochain related micro-transactions efficient/inexpensive
- blockchain-based micro-payments to constrained IoT devices
  - – incapable of
    - performing public-key encryption
    - (directly) participating in the blockchain
    - storing blockchain-related secrets.
- enable “payment delegation”
  - – allowing users without blockchain credentials to pay
    - up to a pre-configured amount
    - for a specific service
- support many-to-one payments
  - – enabling multiple users that share the same blockchain credentials to pay for a service
- a presently feasible solution
  - – that relies on existing, already deployed technologies

H2020 SOFIE: Secure Open Federation of Internet Everywhere

- Applying Distributed Ledger Technology to
  - ➢ **securely** and **openly**

  federate IoT platforms
- *interconnected* distributed ledgers
  - – decentralized business platforms
  - – interconnection of diverse IoT systems
  - – accessible metadata
  - – open business rules on how to connect to platforms
  - – securely record audit trails to be used to resolve disputes

http://www.sofie-iot.eu/

SOFIE

A solution

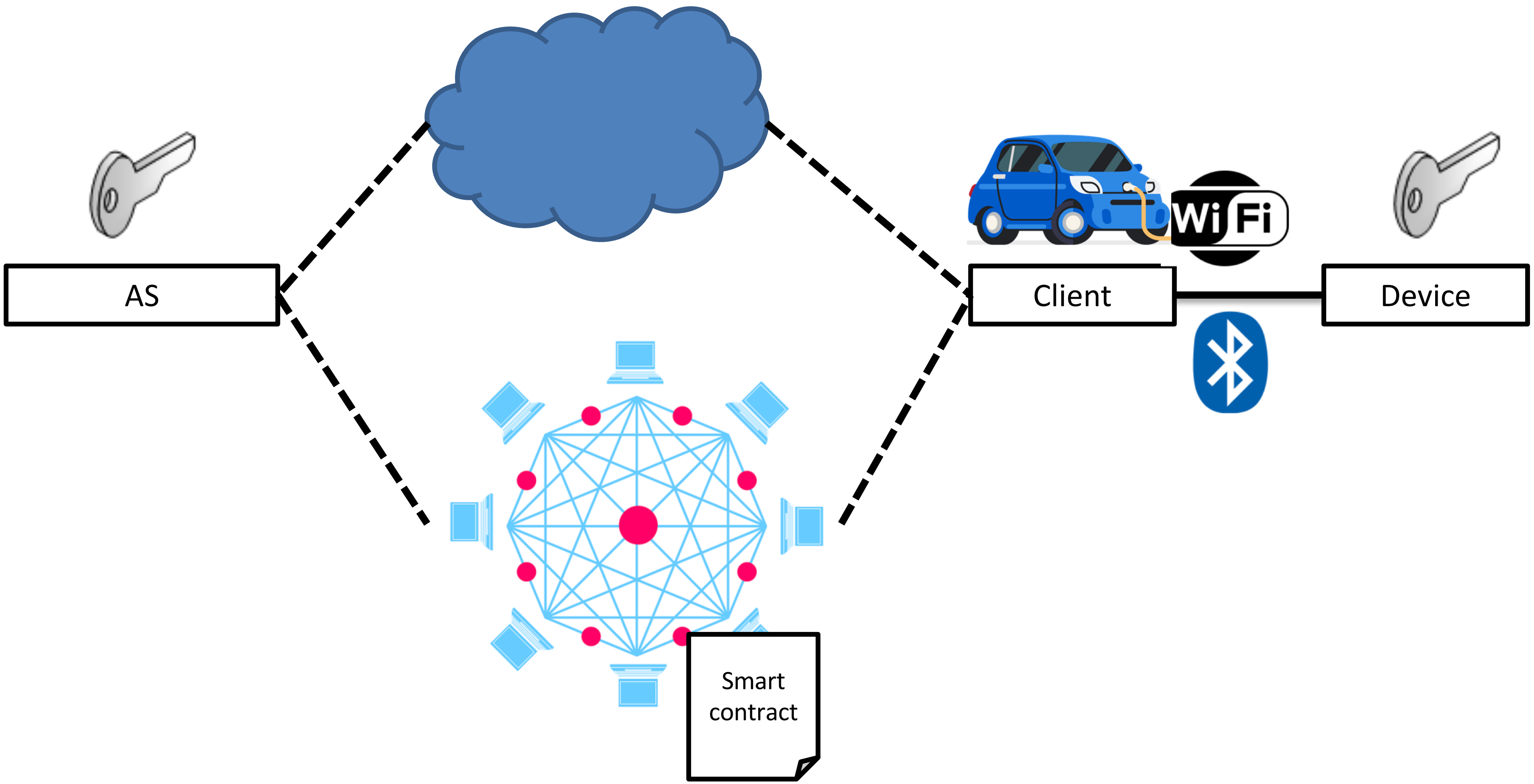
- We argue that the general cyber-real world interaction problem can not be easily solved

⇨ Damage control/limit potential loss

  – In case something goes wrong, the loss is a small pre-configured amount of money

- We leverage two existing solutions
  – Payment channels
  – Hash-based one time password (HOTP – RFC4226)

Setup



High-Level System Perspective

- A client (or his owner) makes a "deposit" to a smart contract
- The client requests from an AS an "one-time password"
  - for invoking the actuation process for 1 time slot
- The password is exchanged for a "payment receipt"
- The receipt can be used by the AS to claim, from the smart contract, (part of) the deposit
- If a client needs more passwords, it produces more receipts...

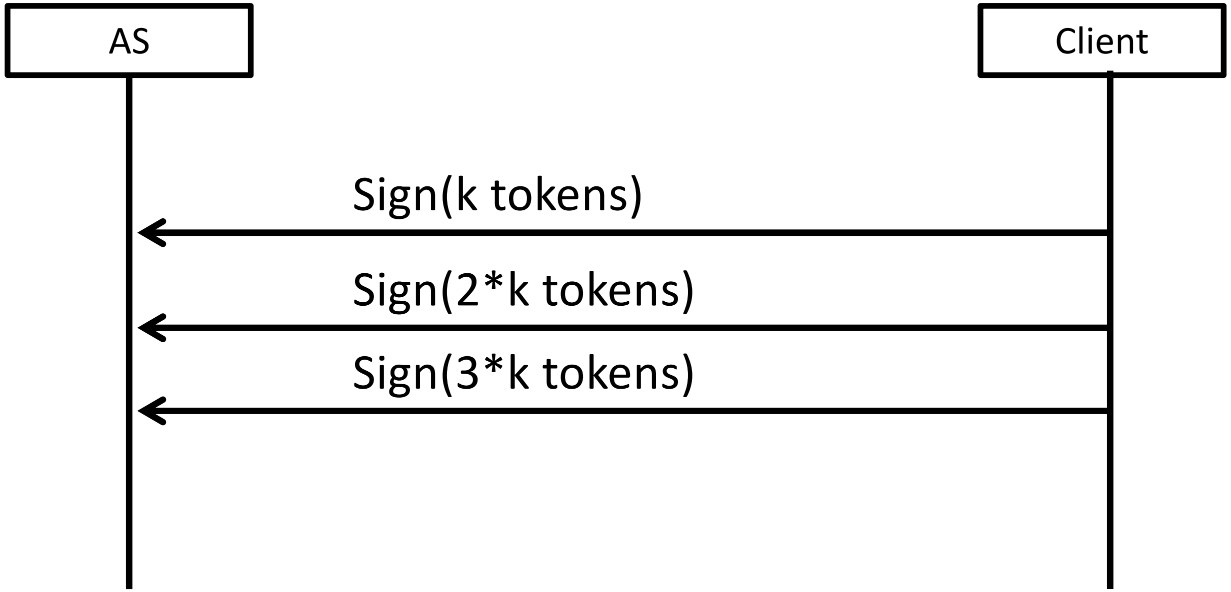
High-Level System Properties

- A deposit is claimed using only a single payment receipt
  - even in the case of many-to-one payments
  - minimizes the interactions with the smart contract and makes the smart contract implementation simpler
- Payment receipts are provided off-chain
  - generation & validation of receipts involves only digital signatures computation
  - generation & evaluation of an one-time password involves the computation of a keyed hash message authentication code (HMAC)
  - this process is fast -> small time slots can be used
    - minimizing the losses in case of service disruption
- A device and an AS have to be pre-configured with a shared secret key
  - no further interaction is required between these two entities
- The channel client-device does not have to be secure
  - as opposed to the channel between a client and an AS
- Except from the validation of an one-time password, a device does not have to perform any other operation

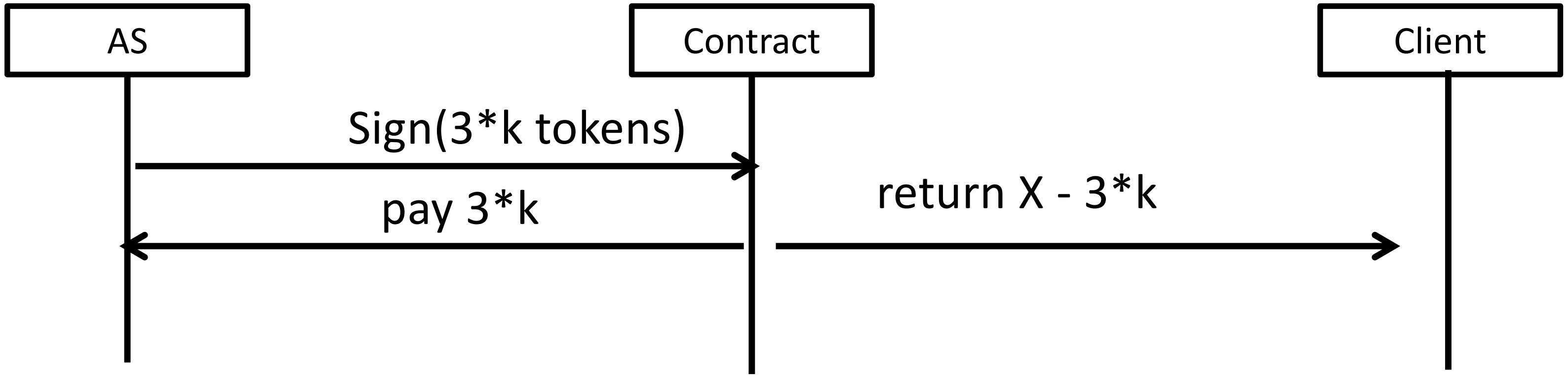
BUILDING BLOCKS

Payment channel: setup

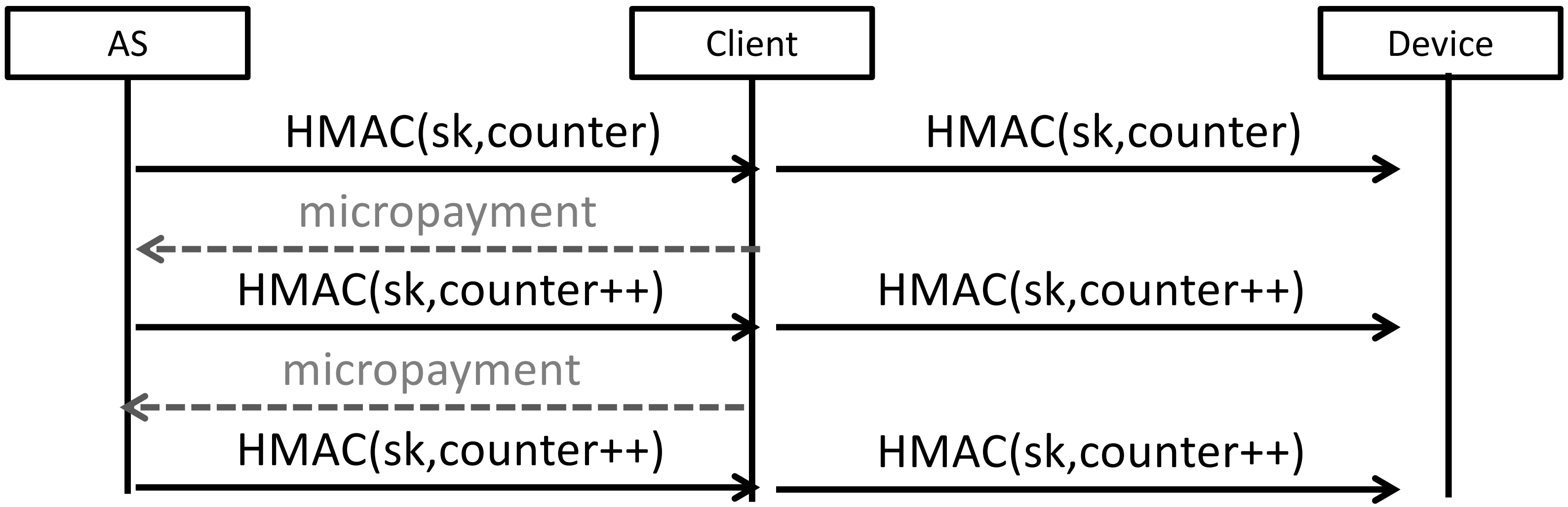
Payment channel: Micropayments



Payment channel: closing the channel

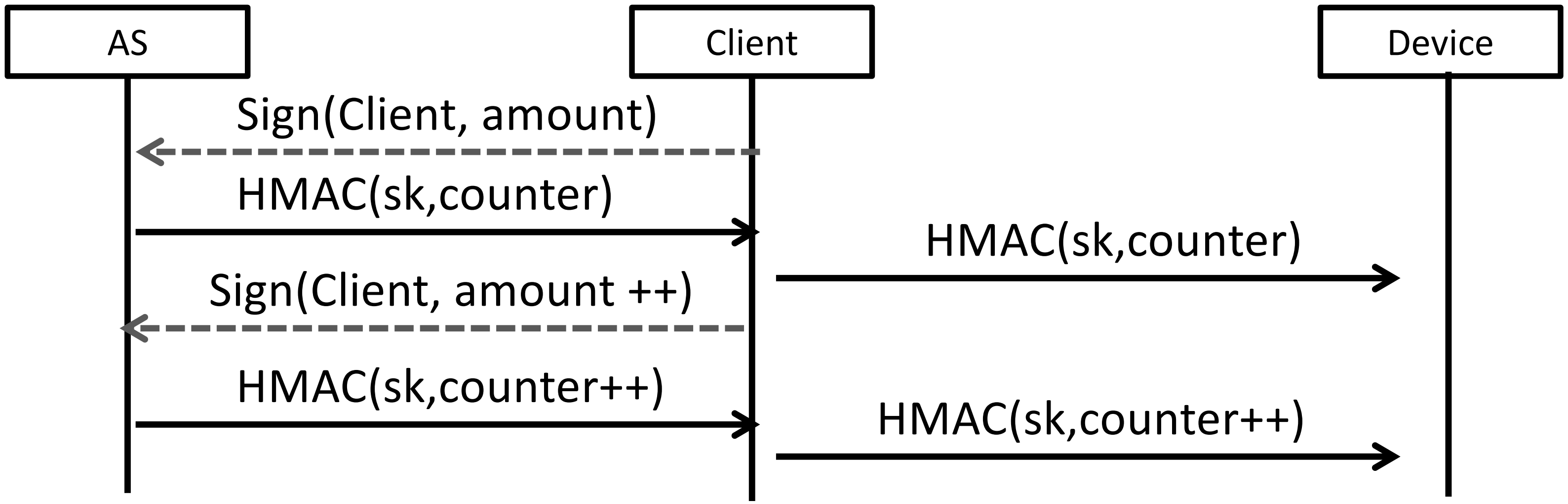


keyed **H**ash Message Authentication Code (HMAC)
One-**T**ime **P**assword (HOTP)

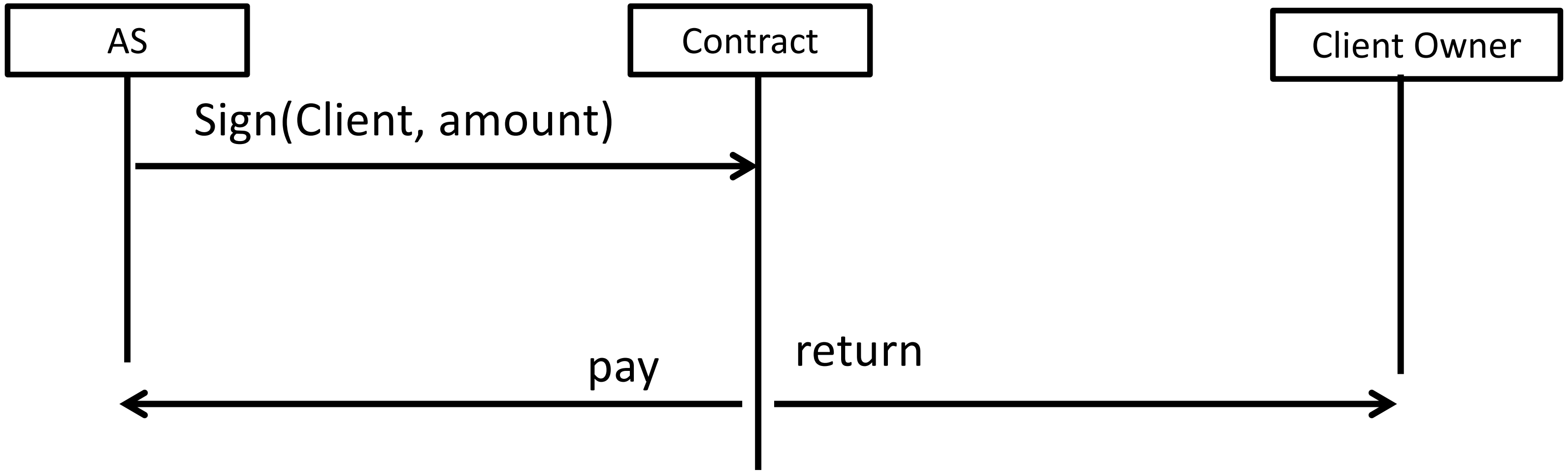


TRIVIAL CONSTRUCTION

Device access

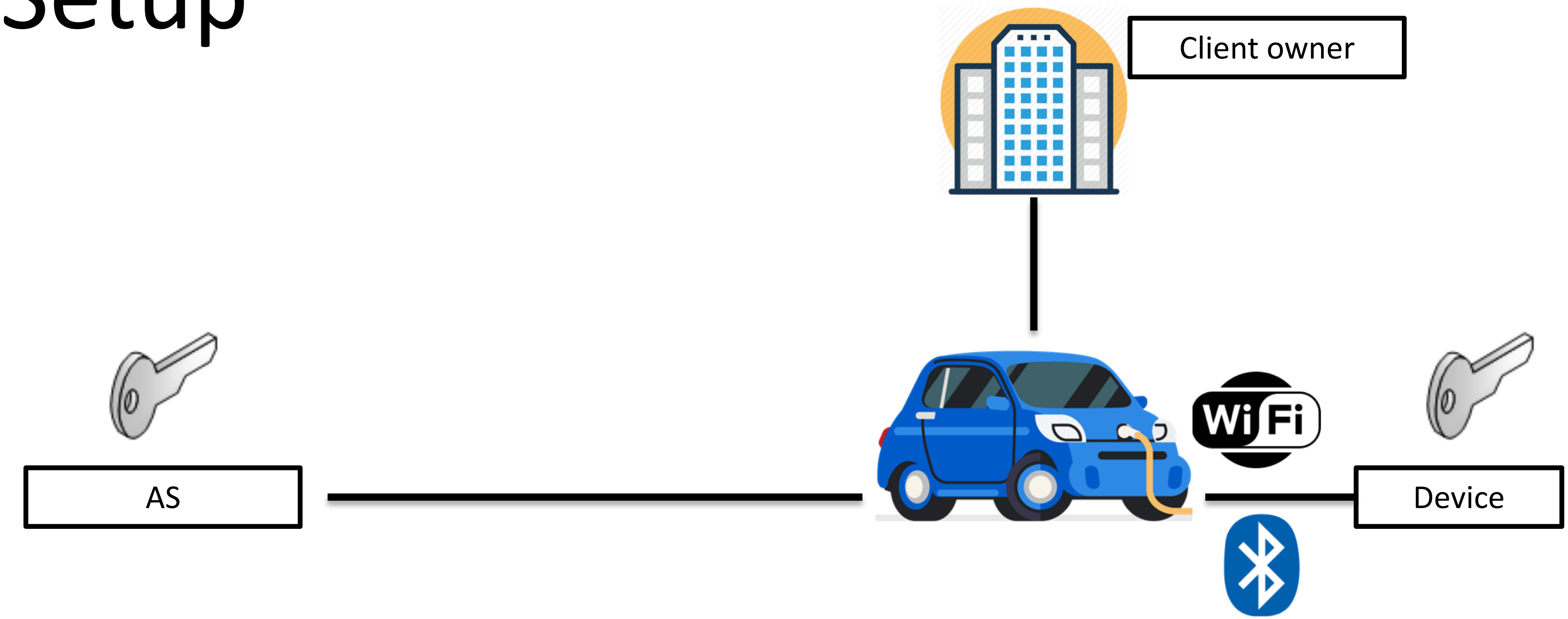


Channel close

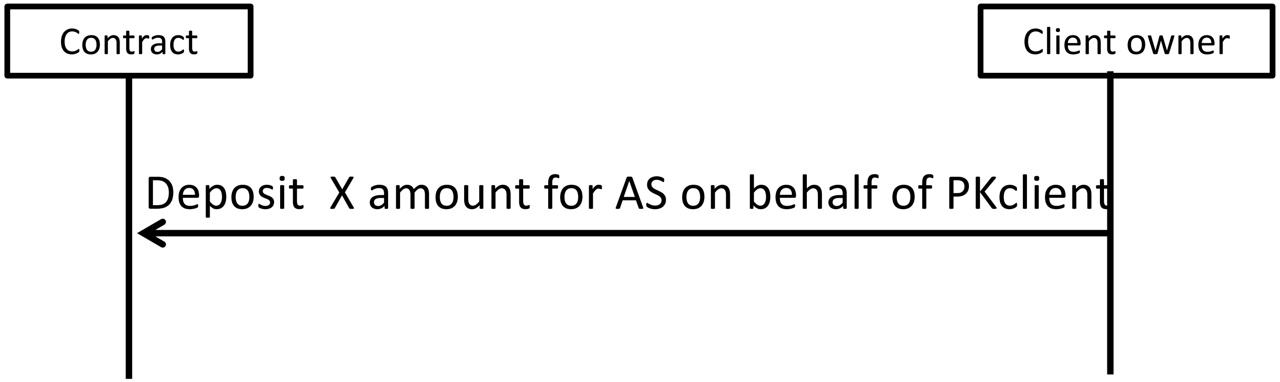


CLIENTS WITHOUT ACCESS TO THE BLOCKCHAIN

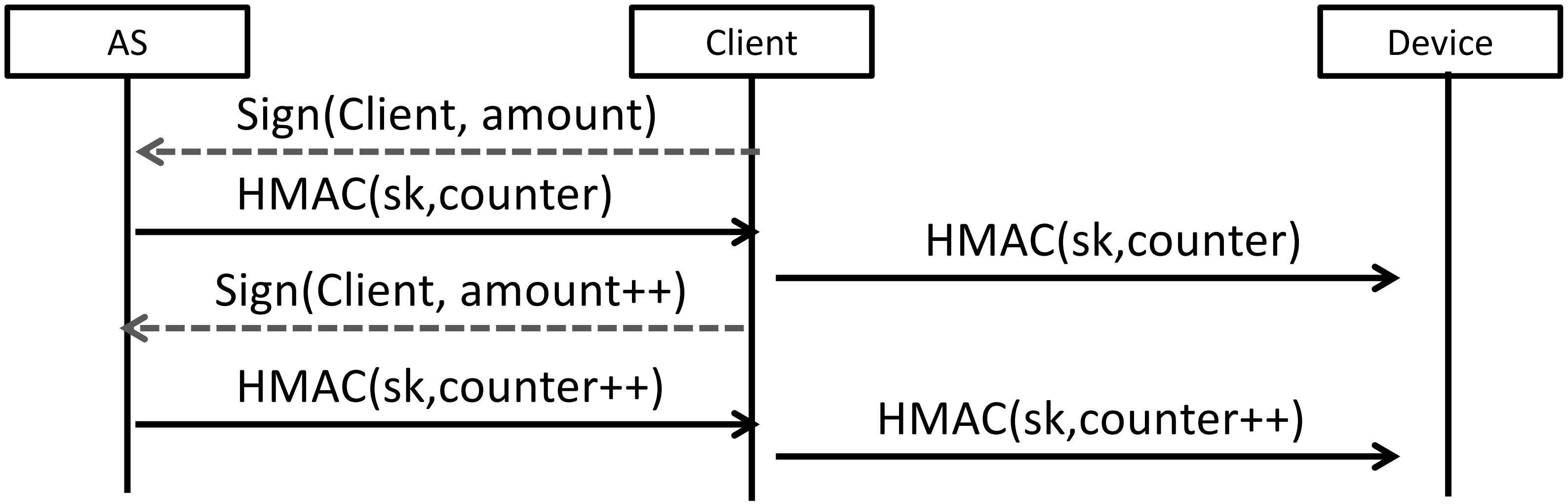
Setup



Payment channel setup

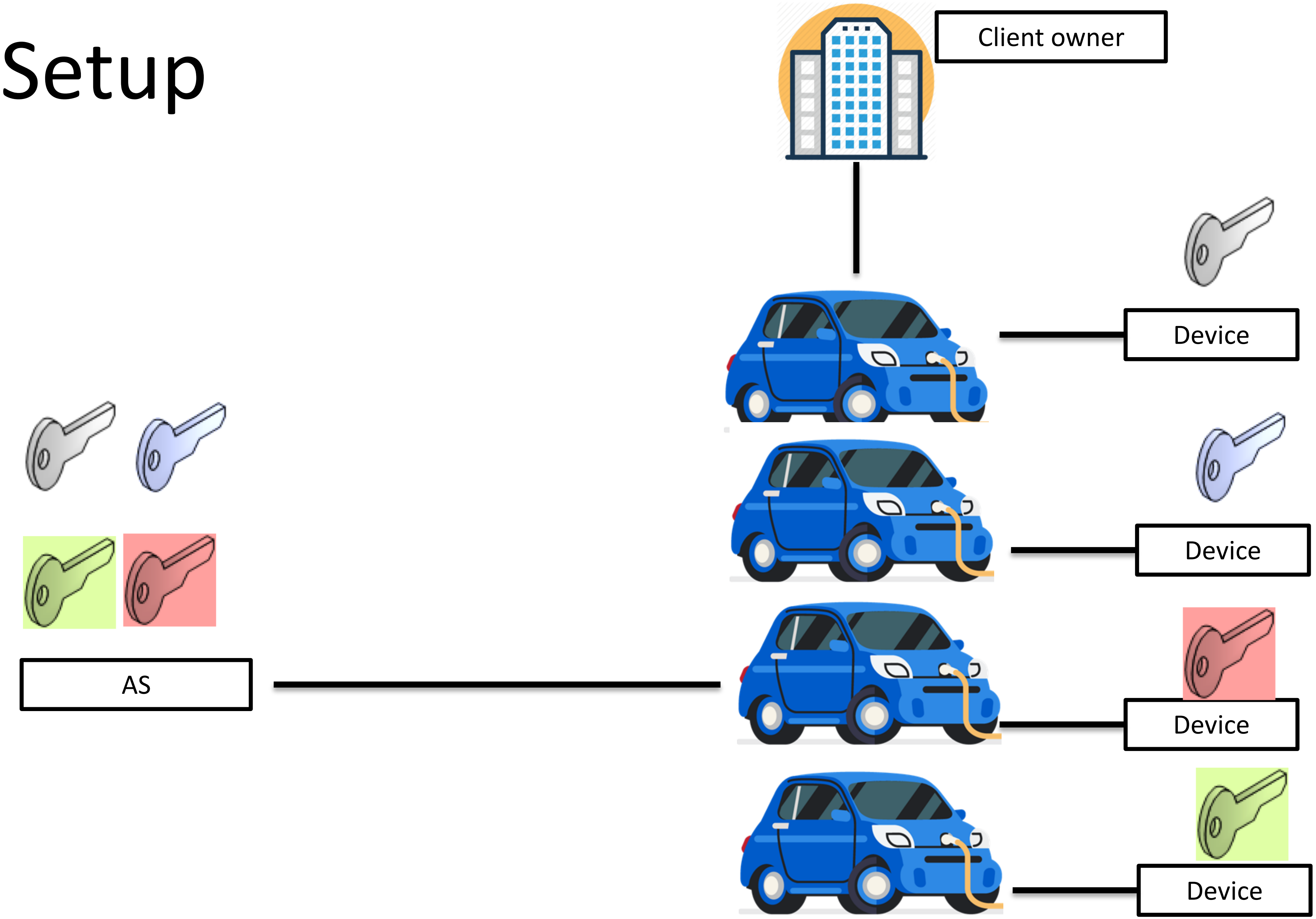


Device access



ONE CLIENT OWNER
MULTIPLE CLIENTS

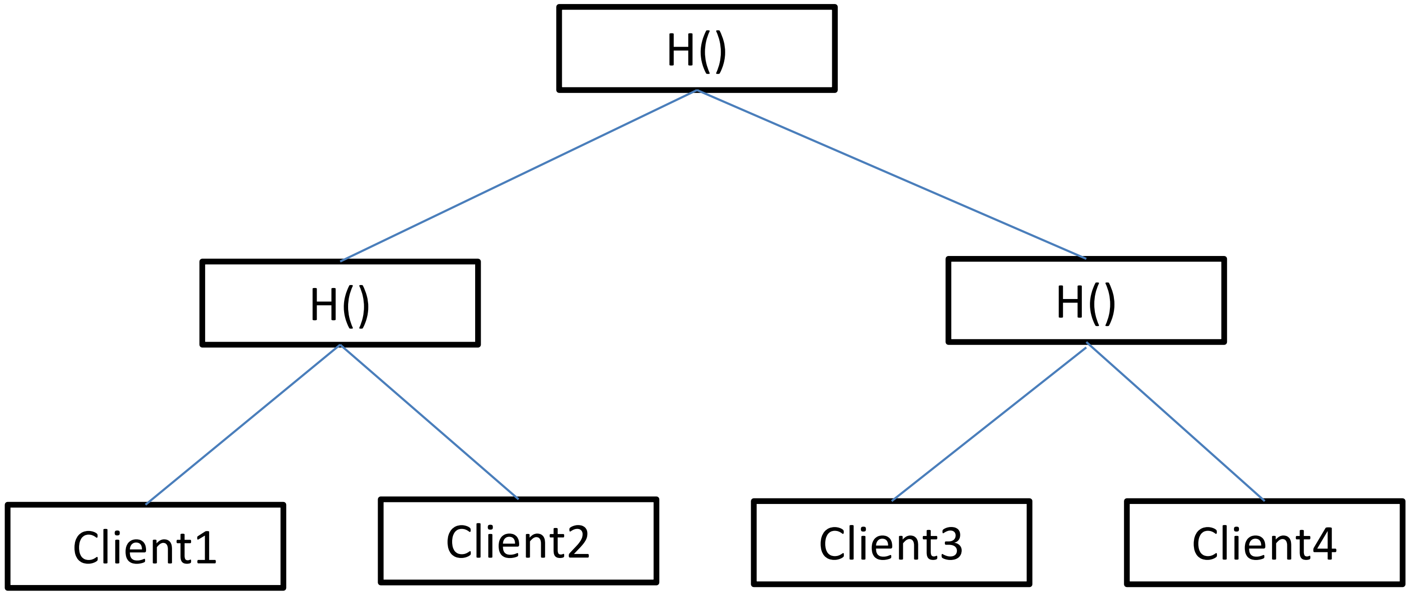
Setup



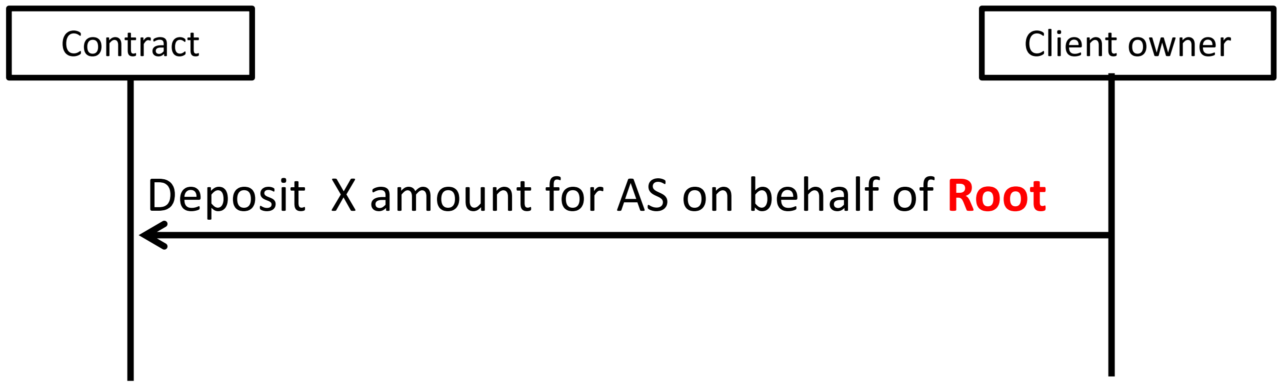
Challenges

- 1. Store all legitimate public keys
- 2. Close the channel with a single transaction

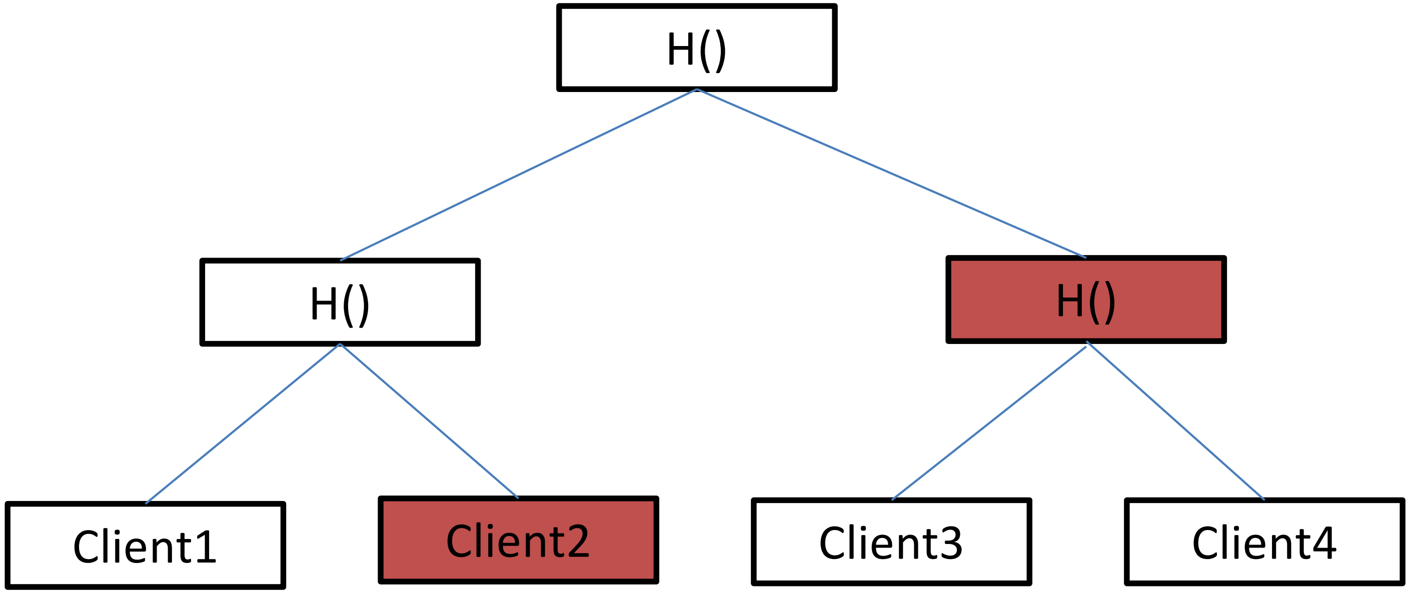
Store all client keys in a Merkle tree



Payment channel setup



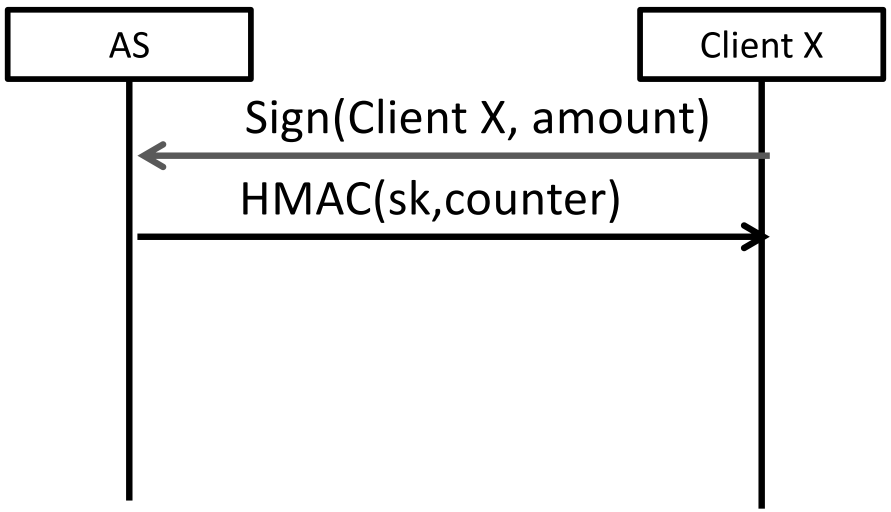
Prove membership



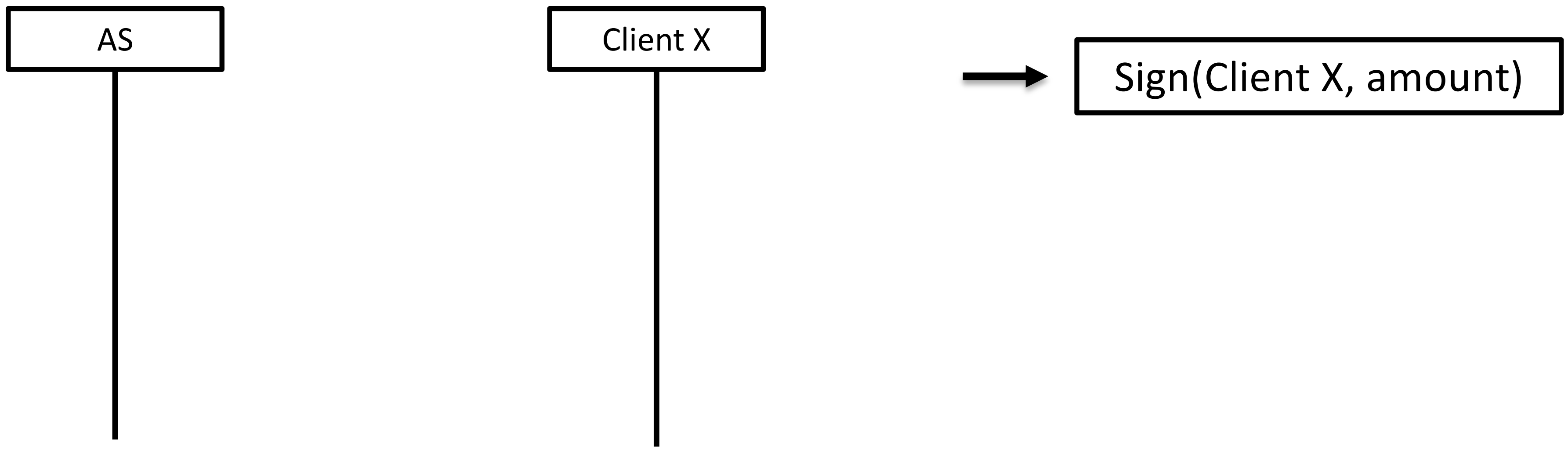
Challenges

- 1st Store all legitimate public keys
- 2nd Close the channel with a single transaction

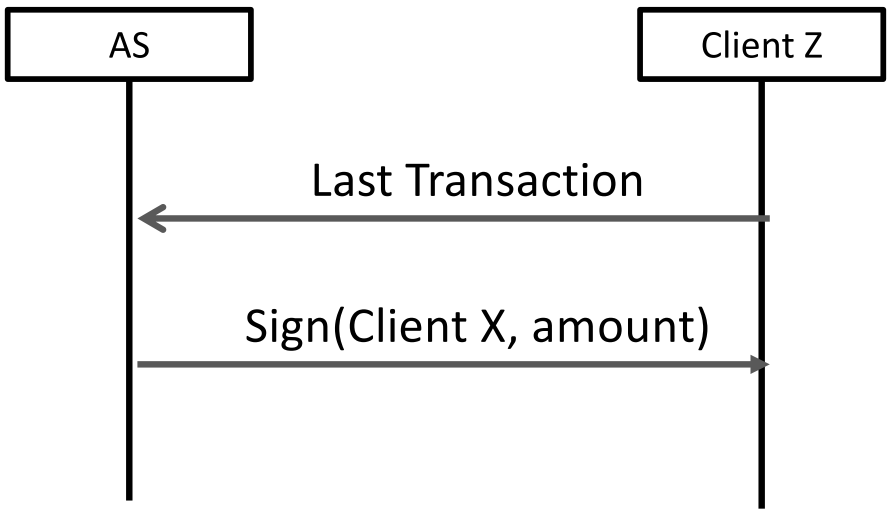
The straw man ledger



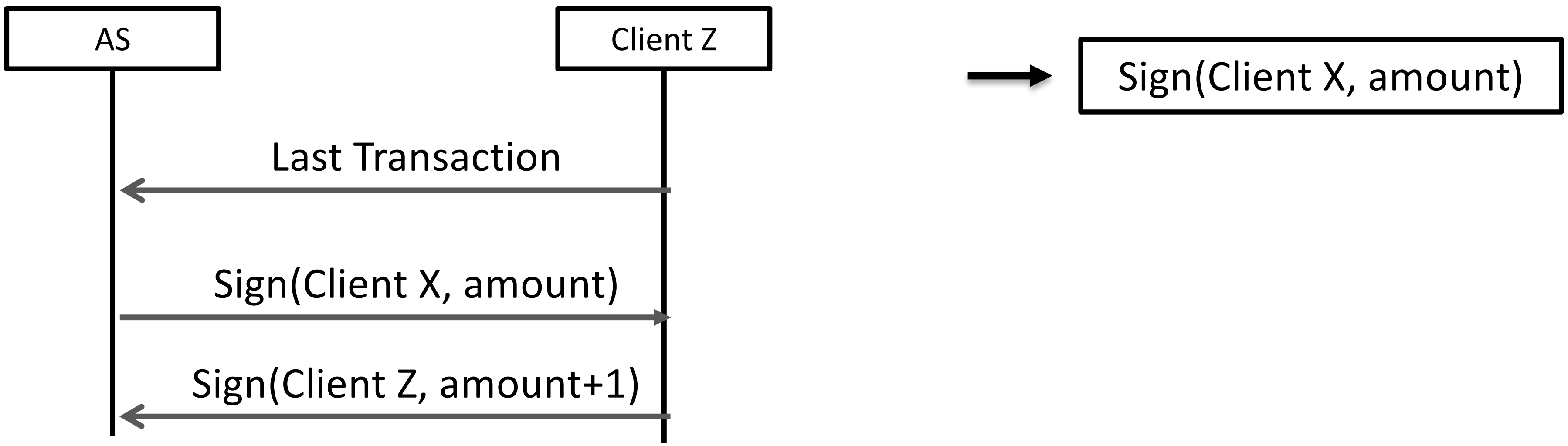
The straw man ledger



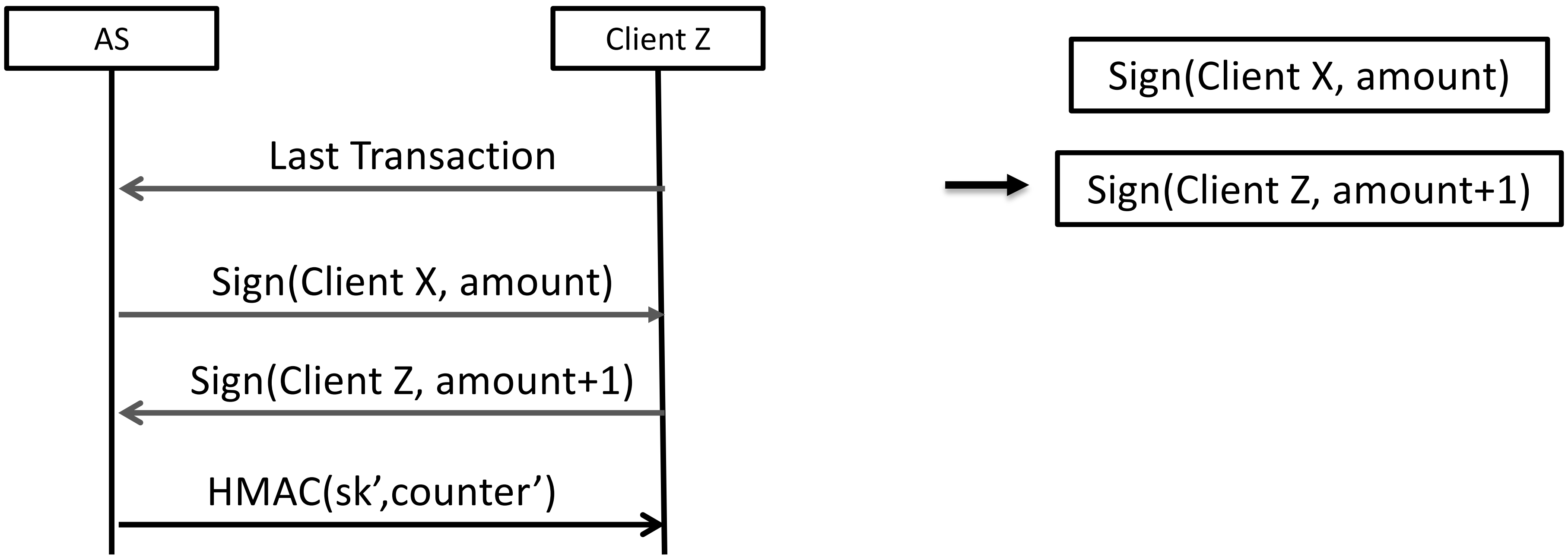
The straw man ledger



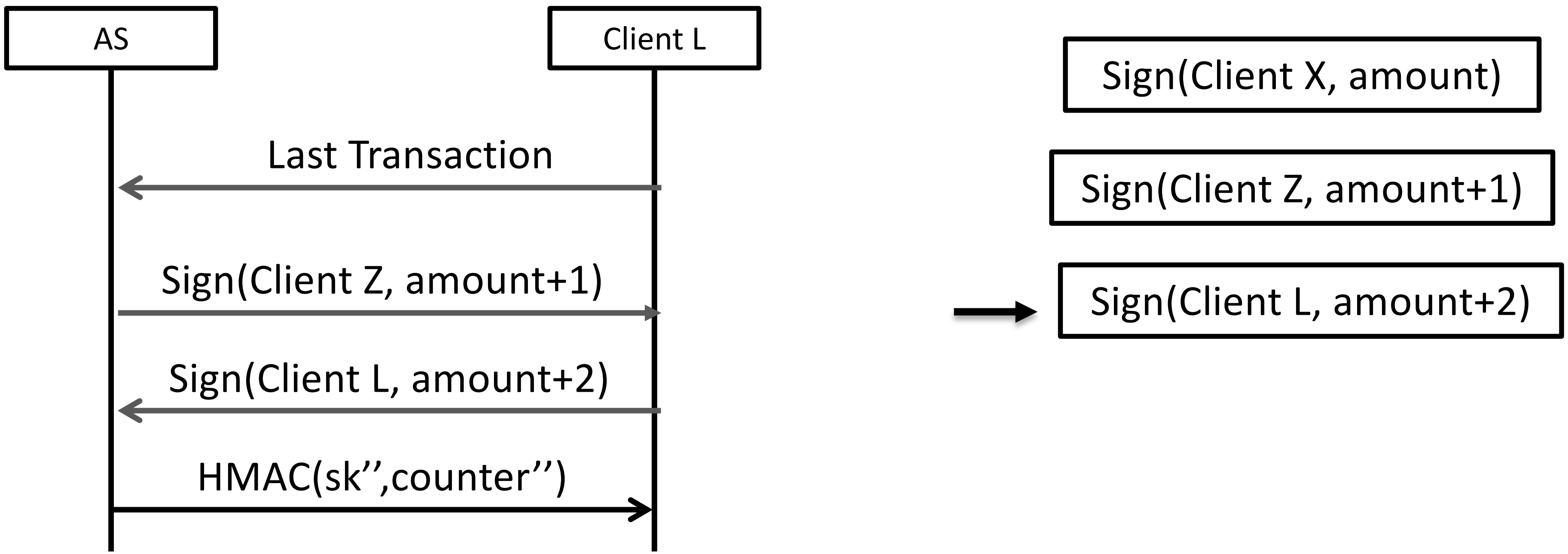
The straw man ledger



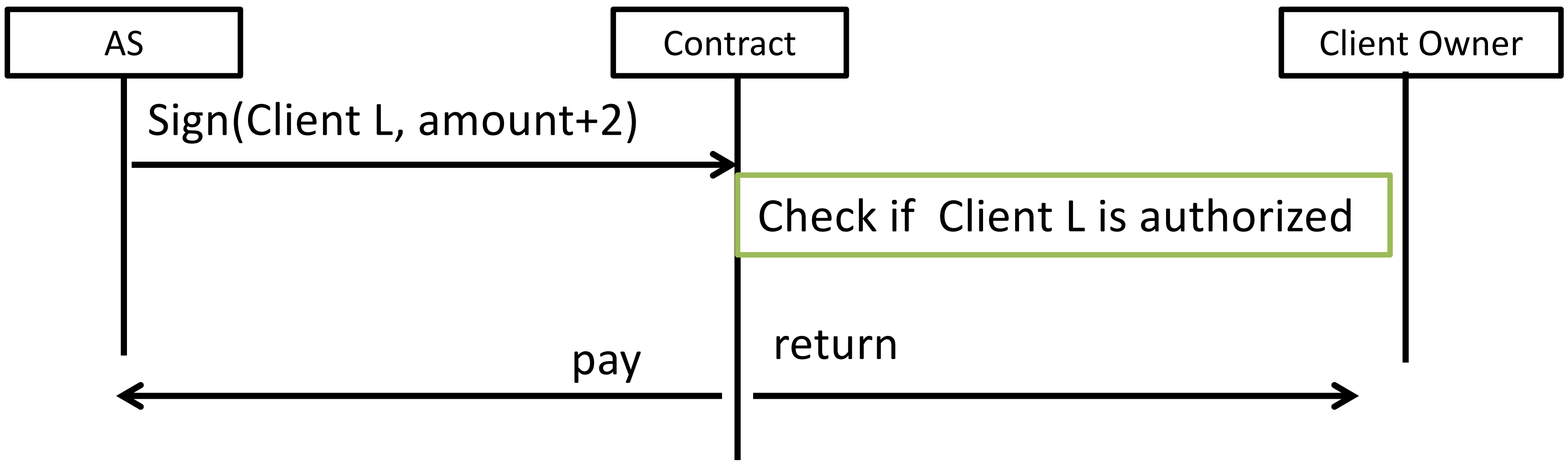
The straw man ledger



The straw man ledger



Channel close



Implementation and Evaluation

- Implementation with Ethereum smart contracts
- Public-private key pairs with secp256k1
- HMAC with SHA256
- Merkle tree with keccak256
  - Hash function recommended for Ethereum Smart Contracts
- Cost of Open and Close:
  - 3rd construction: 4 cars
- Opening deposit: 14.5 sec

First construction		
Operation	**Cost measured in gas**	
open channel	43700	€0,05
close channel	36258	€0,04
Second construction		
Operation	**Cost measured in gas**	
open channel	50388	€0,06
close channel	36258	€0,04
Third construction		
Operation	**Cost measured in gas**	
open channel	50388	€0,06
close channel	36330	€0,04

Conclusions

- realistic approach for paid IoT interactions:
- blockchain-based micro-payments to constrained IoT device owners
  - payment delegation
- efficiently support groups of clients (1 owner)
- a presently feasible solution

Future Work

- Advanced Ledger and ILP
- Key revocation

Thanks!

polyzos@aueb.gr

SOFIE

Bridging the cyber and physical worlds using blockchains and smart contracts

Nikos Fotiou, Vasilios A. Siris,
Spyros Voulgaris, **George C. Polyzos**

Dmitrij Lagutin

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Aalto University
School of Electrical Engineering

Mobile Multimedia Laboratory