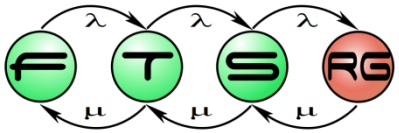
Blockchain-Based Control of Device Access in Cyber-Physical Systems

Péter Garamvölgyi

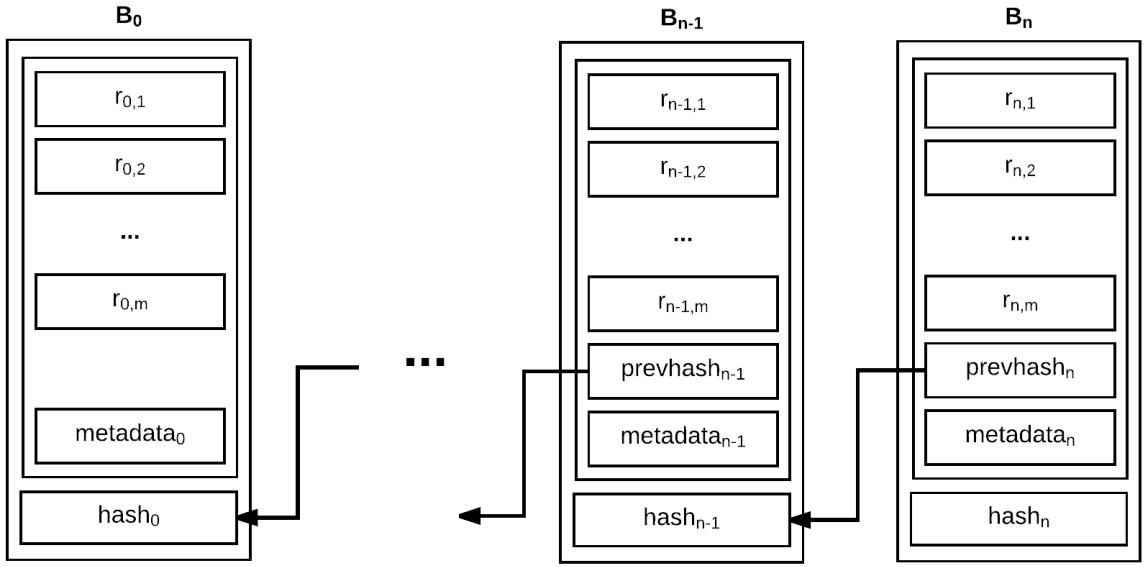
Advisor: Imre Kocsis

Budapesti Műszaki és Gazdaságtudományi Egyetem
Hibatűrő Rendszerek Kutatócsoport



Blockchain: Overview

- Shared ledger with distributed consensus
  - E.g. Proof-of-Work
- Key enabler for cryptocurrencies
- Transparent, immutable
- Bitcoin, Ethereum



Blockchain: Smart Contracts

- Bitcoin: basic scripting
- Ethereum: Turing complete
  - Ethereum Virtual Machine, EVM bytecode
  - Deterministic, redundantly parallel execution
  - High-level languages: Solidity, Serpent, etc.
- Smart contract programming is hard

Cyber-Physical Systems

- Seamless intergration of algorithms and physical components
- Numerous applications for the blockchain
  - Security, immutability
  - Digital micropayments
  - Smart contracts

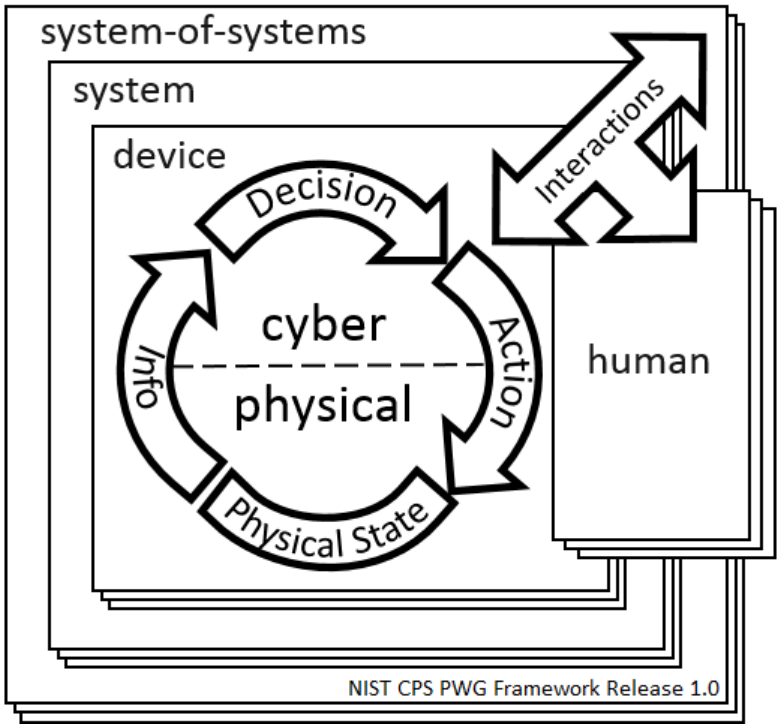
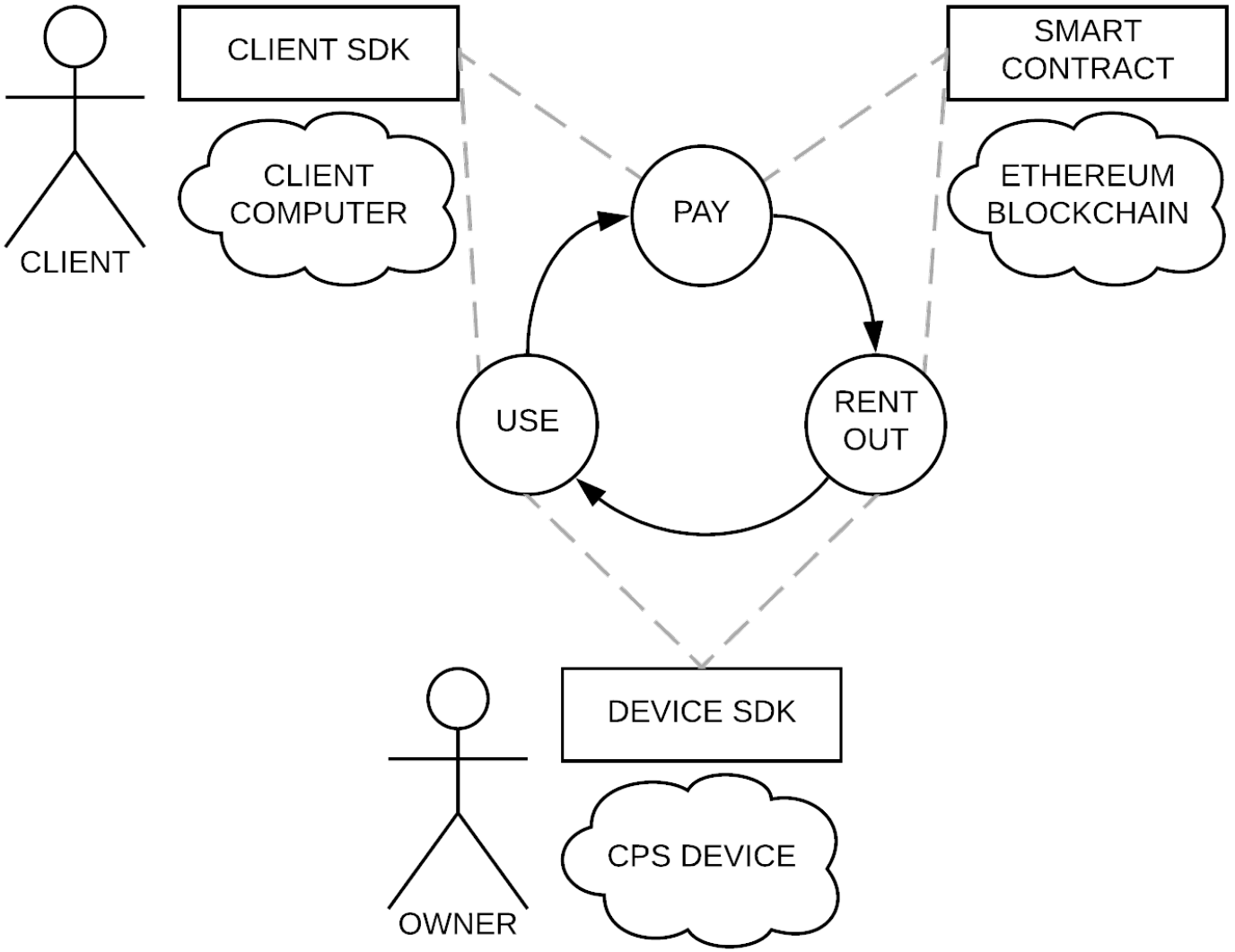
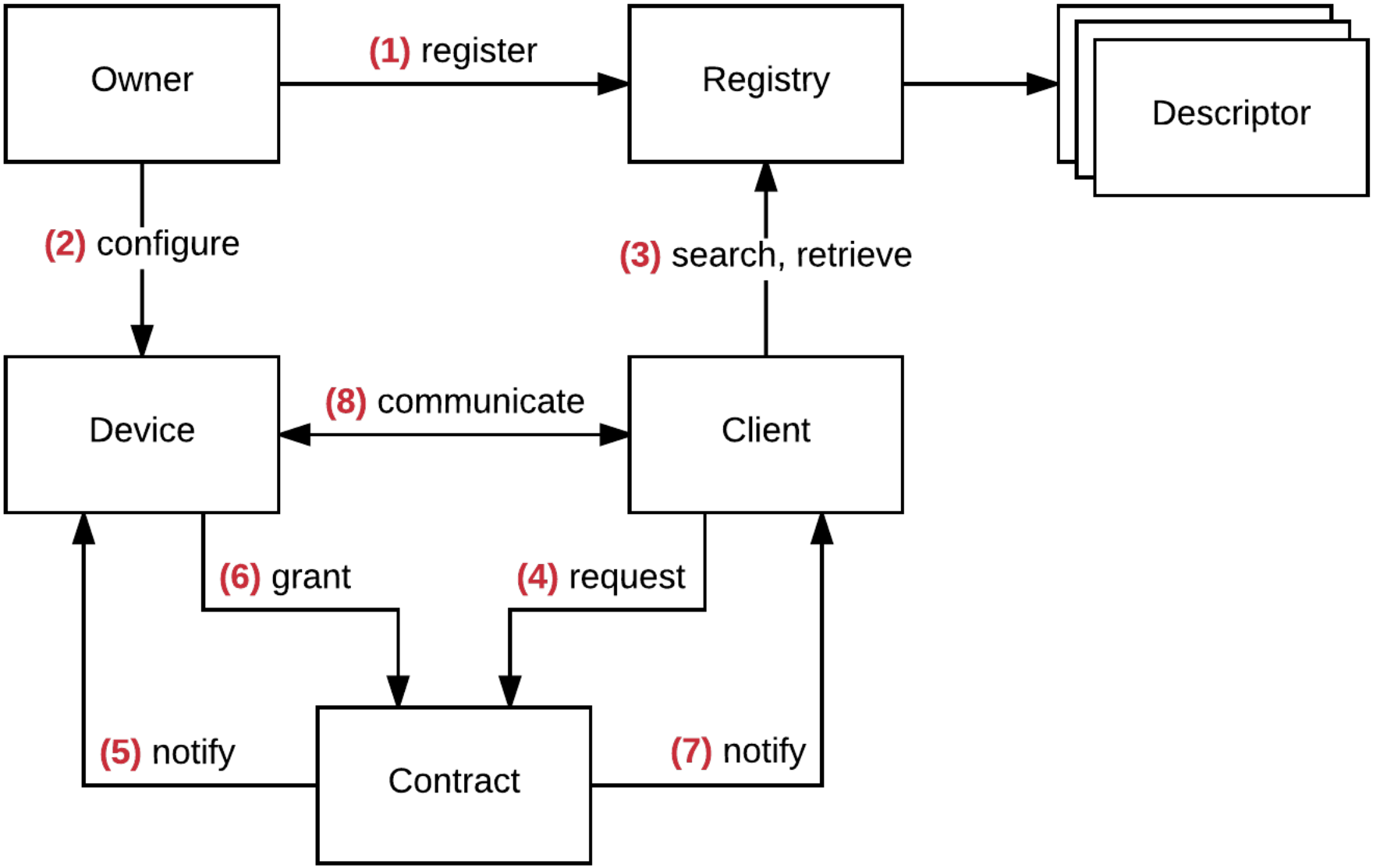


Image source: NIST. Cyber-Physical Systems Public Working Group, 2017. https://pages.nist.gov/cpspwg

Device Rental Platform: Overview



Device Rental Platform: Components



Device Rental Platform: Access Control

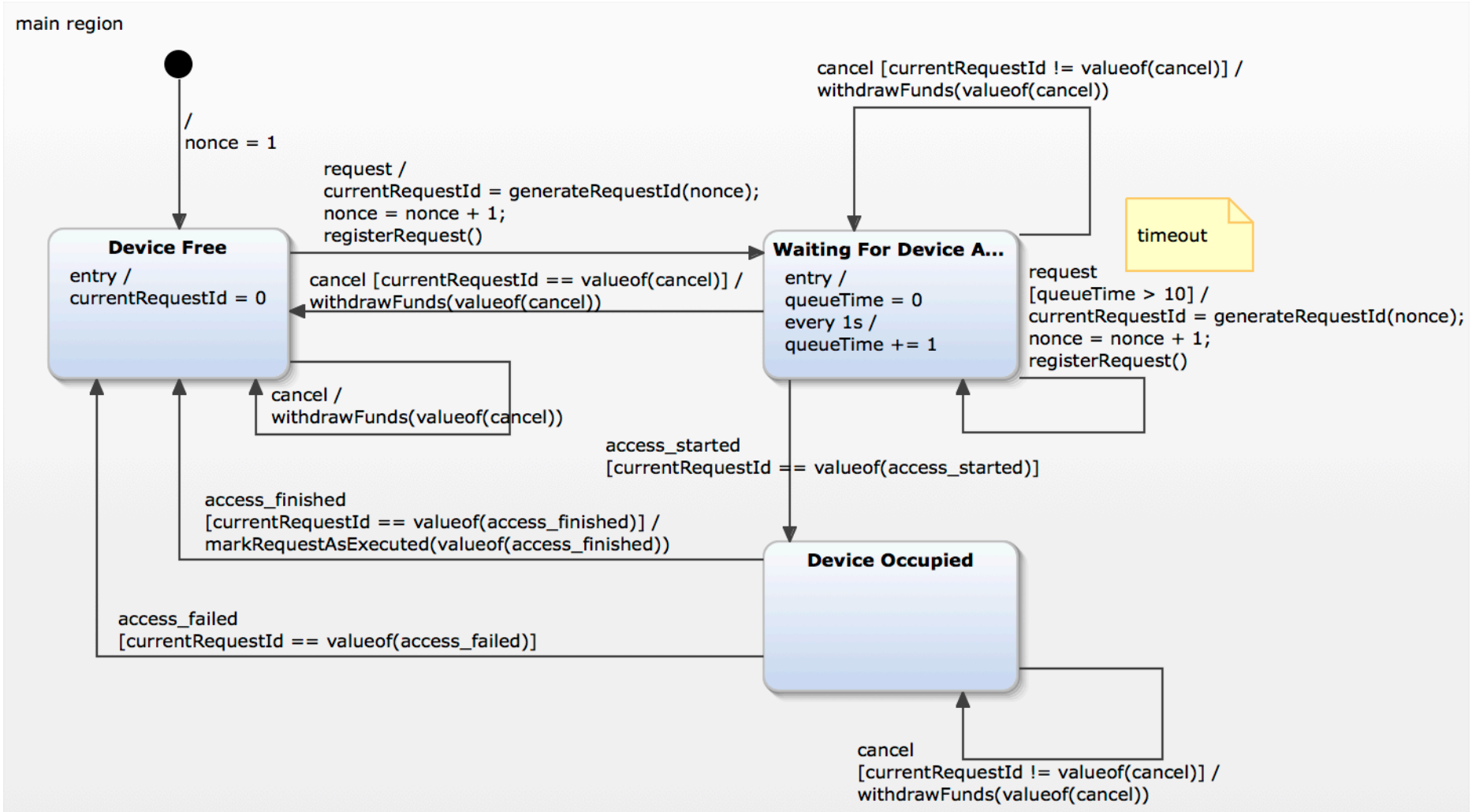
- Request and grant access through smart contract
  - New Request
  - Request Started
  - Request Finished
  - Request Failed
  - Cancel

- Key-exchange over blockchain
  - Diffie-Hellman

Device Rental Platform: Formal Modelling (1)

- Advantages of formal modelling
  - Formal verification
  - Automatic code generation
- Few applications to smart contracts
- Limitations
  - Limited expressive power of UML state charts
  - Extra execution and deployment costs

Device Rental Platform: Formal Modelling (2)



Device Rental Platform: Evaluation

- Local testing with Raspberry Pi
- Public test network

Transaction	C_T	C_E	$C_\$$
request	153,992	132,016	\$0.671
access_started	35,055	12,119	\$0.111
access_finished	36,041	50,617	\$0.203
withdrawProfit	19,643	13,371	\$0.077

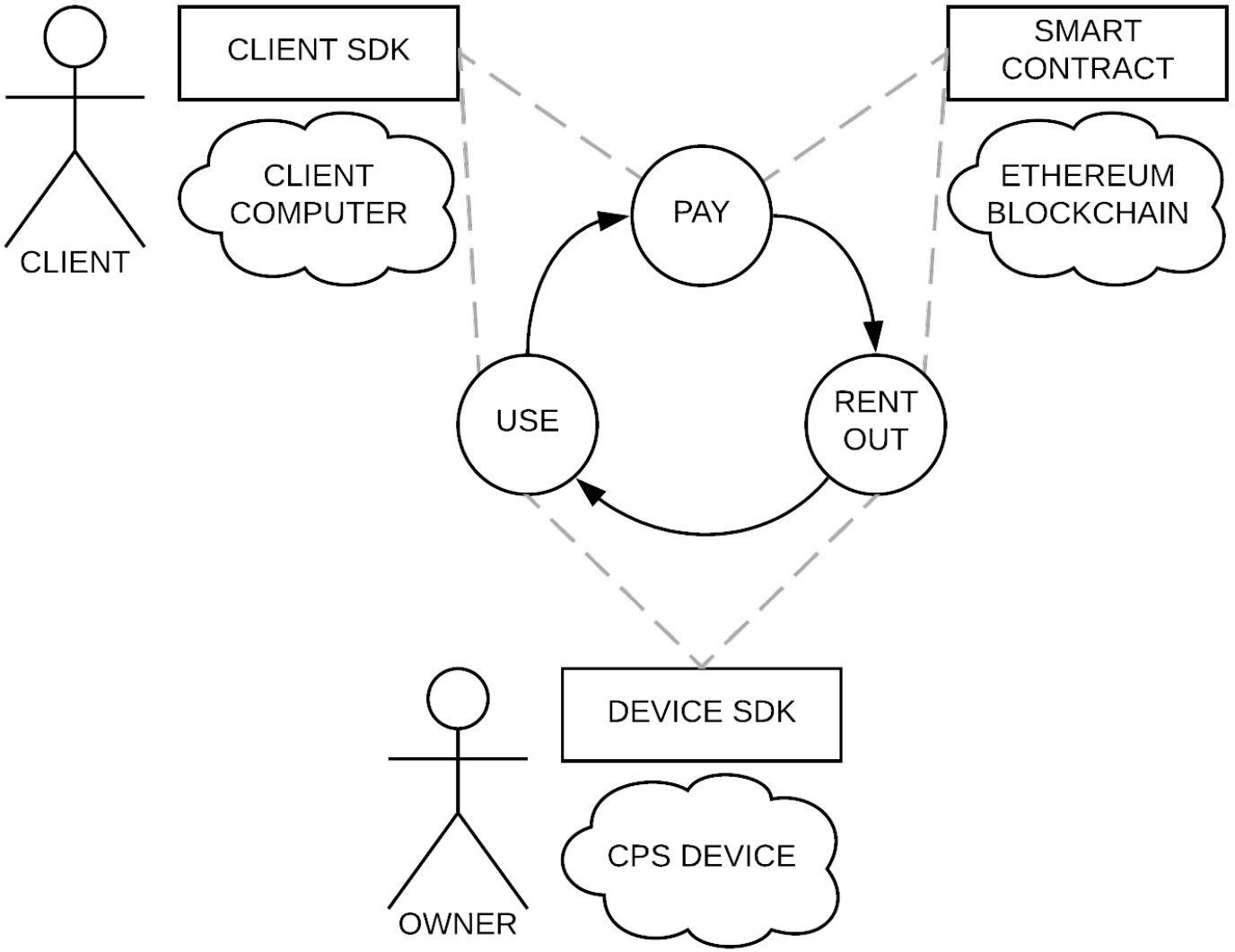
Table 5.1: Simple Cost Benchmarks (Remix)

- Cost/time overhead
  - Uncertainty of the Ethereum blockchain (e.g. ICOs)

Future work

- Device Rental Platform
  - Device Registry
  - Usability (UI)
- State modelling
  - Automatic code generation
  - Formal verification

Device Rental Platform



Question #1: Contracting external services

In principle, contracting external services can be problematic. Ethereum-based contracts are not exception. What are the best ways to overcome this issue?

Question #2: Hiding confidential data

With the coming GDPR regulation, any idea on compliance?

Question #3: Ethereum scalability and CPS real-time control

Does the proposed solution meet the real-time requirement challenges? In what scenarios?

Question #4: Enforcing on-chain payments

What could be the challenges with regard to enforcing on-chain payments?

Question #5: Comparison with existing solutions

What are the challenges and proposed solutions for access control methods in CPS?

What are the benefits of a blockchain-based approach compared to more lightweight solutions such as RSVP?