Mobile Multimedia Laboratory

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

SOFIE

# Bridging the Cyber and Physical worlds using Blockchains and Smart Contracts


**George C. Polyzos**

collaboration with

V. Siris, S. Voulgaris, G. Xylomenos, N. Fotiou,

D. Dimopoulos, I. Pittatras, M. Tsenos (AUEB/MMlab),

and Dmitrij Lagutin, Aalto University, and many other collaborators from the SOFIE project

polyzos@aueb.gr

# Outline

- Background
  - The Internet of Things
  - Blockchains/Distributed Ledger Technologies (DLTs)
  - H2020 Project SOFIE
- Motivation/Problem Statement
- Outline of Approach
- Contributions
  - Evaluation
- Conclusions

# Internet of Things (IoT): Vision & Status

- Blurred boundaries between the Cyber and Physical worlds!
  - 2010: # Internet connected devices > Earth's population
  - "Connected devices" now include everyday home appliances
    - TVs, lights, refrigerators, scales, …
  - continuously decreasing manufacturing cost of sensors and **actuators**
  - new protocols for autonomous M2M communication
- IoT Fragmentation & lack of security are the main issues
- Most IoT: Vertically oriented, closed systems
  - Silos!

# IoT Challenges


- Interoperability
  - well over 300 different Internet of Things (IoT) platforms; several dozens … standards
  - most of the deployed IoT systems are closed
- Sustainability
  - Danger of fragmented ecosystems: composed of old and new devices
  - in many scenarios Things are **"deployed and forgotten"**
- Trust Model
  - new trust model needed to enable the interaction of all devices with **little human intervention**
  - need novel mechanisms for
    - transactions
    - compensation
    - accountability
- Security
  - Existing security solutions often cannot be directly applied to Things
    - Things resource limited; no computational power for complex cryptography
  - Things often (physically) exposed to malicious users; not always feasible to (remotely) connect to them
  - Things can collect sensitive information; may control critical aspects of daily life
  - **actuators**: security even more critical… **safety**
- Privacy
  - Information from the IoT: can have significant context; be highly correlated…
  - pervasive and invisible aspects of the IoT: information collected for long before it becomes known

# Motivation & Vision

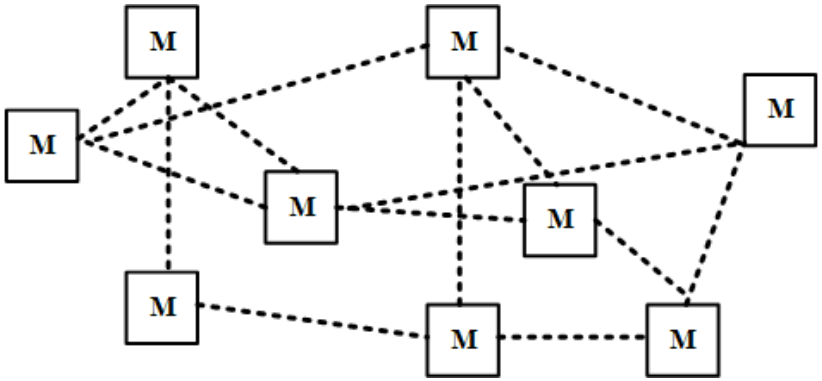
- Interoperability (addressing IoT fragmentation)
  - well over 300 different IoT platforms
  - several dozens … standards
  - …
  - mostly, not a technical issue…
  - **business** counter-incentives
  - **privacy** constraints

- Key IoT premise/goal: (mostly) ***unattended*** operation
  - Automation: Trust, Incentives, …
  - Unexpected interactions between/among unknown/untrusted parties
  - The issue: (prescribed) Control over Data

- Vision: **4th Generation *Open* Business Platforms**
  - Exchanging data (and value) in an ***automatic*** and ***controlled*** way
  - in an ***open***, ***decentralized*** ecosystem (with no controlling party)
    - Open public Blockchains can contribute towards this goal
    - Various Blockchains have various characteristics and properties
      - **Interledger**!

# Blockchains and Smart Contracts: part of the solution…

- Blockchain: "A ***distributed append-only*** ledger (db) of transactions maintained (as a chain of blocks) by a number of (untrusted, independent) nodes (**M**iners) on a (distributed) network"
  - Distributed Ledger Technologies (DLTs)




- **Smart Contracts**
  - Built on DLTs
  - Autonomous applications with pre-defined inputs and outputs… that can be executed by a miner in a deterministic way
  - often Turing-complete (but with issues…)
  - Any user can invoke a smart contract, the outcome of which is recorded as a transaction in the blockchain

open/permissionless ➪ ❍ Ethereum: Smart Contracts (Solidity)

permissioned ➪ ❍ Hyperledger Fabric: chaincode

# Smart Contract
# Security and Privacy Considerations

- (open/public) Smart Contracts are … open/public
  - all can view the (immutable) “source code” of a Smart Contract
    - **Trust**…
  - similarly..., data on Blockchains, unless they are encrypted
    - often tricky to achieve…
- Smart Contract data is always available
  - all users of a blockchain are able to view the values that contract variables hold, historical data, as well as, all transactions related to that contract
- Smart contracts are **immutable**
  - Once deployed, smart contracts cannot be modified
    - errors can be costly/damning!

# H2020 SOFIE: Secure Open Federation for Internet Everywhere

- Distributed Ledger Technology (DLT) to
  - ➢ **securely** and ***openly***

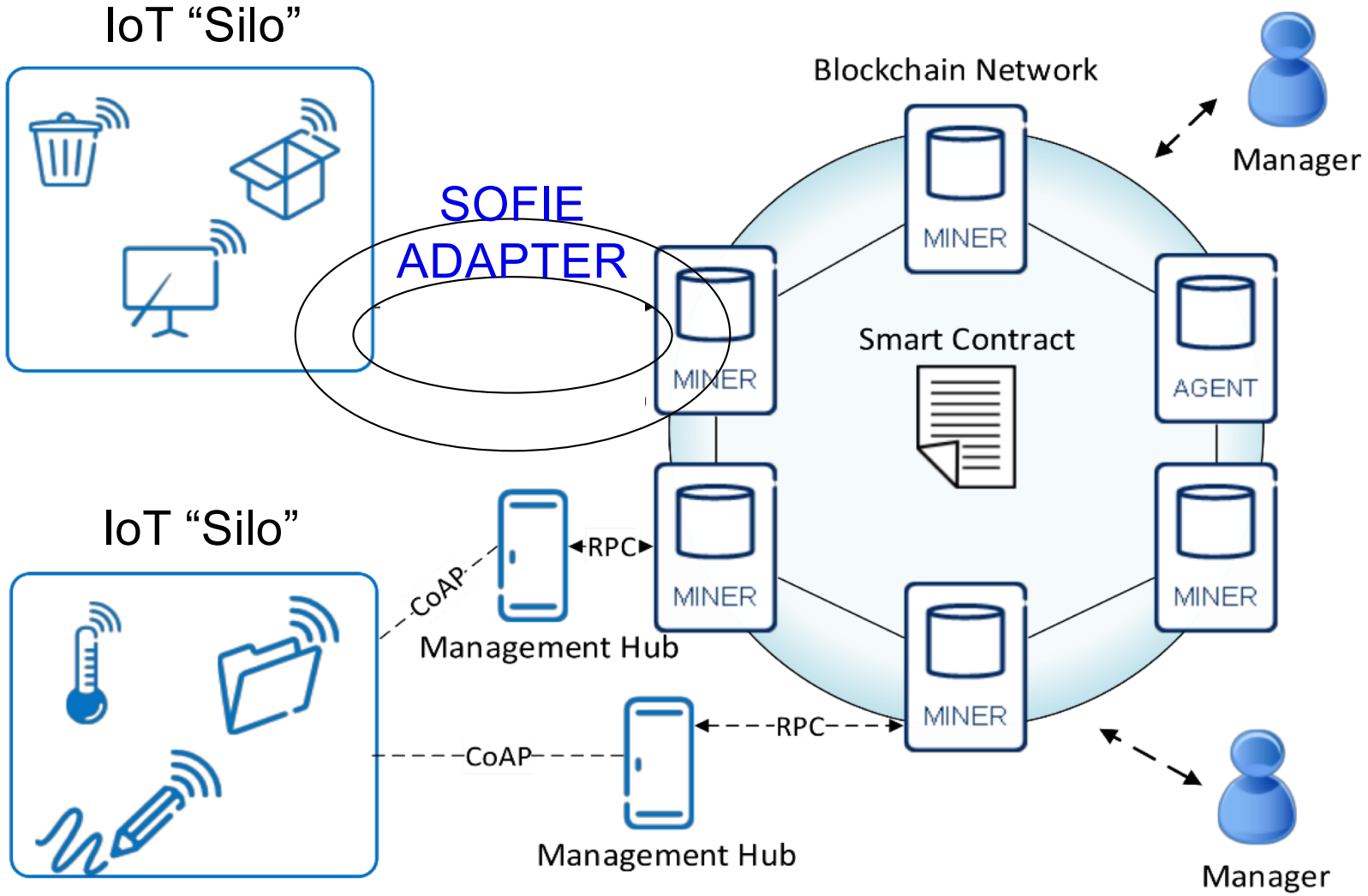
  federate IoT platforms
- ***interconnected*** distributed ledgers
  - decentralized business platforms
  - interconnection of diverse IoT systems
  - accessible metadata
  - open business rules on how to connect to platforms
  - Securely, immutably, record **audit trails** to resolve disputes


- Project
  - 1/1/2018 – 31/12/2020
  - €4.5M

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

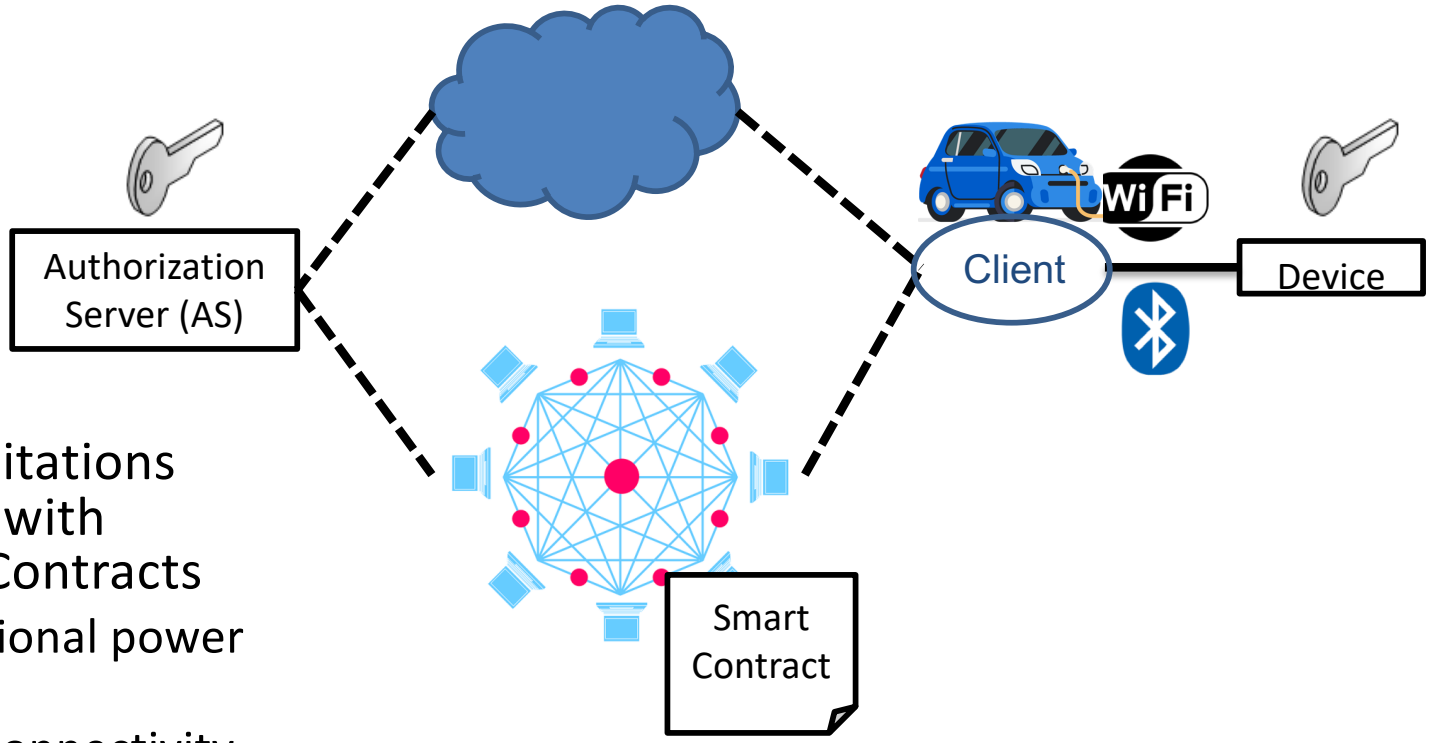
- Partners
  - Aalto University, Ericsson, Rovio (Finland)
  - Guardtime (Estonia)
  - AUEB, Synelixis, Optimum (Greece)
  - Eng, Asm Terni Spa, Emotion Srl (Italy)

# SOFIE's Decentralized IoT Management System using Blockchains



# Bridging the Cyber and Physical worlds using Blockchains and Smart Contracts

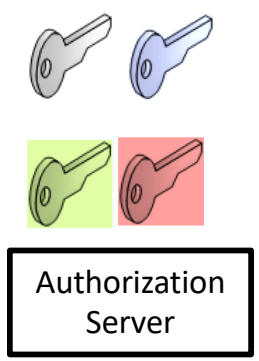
## Setup

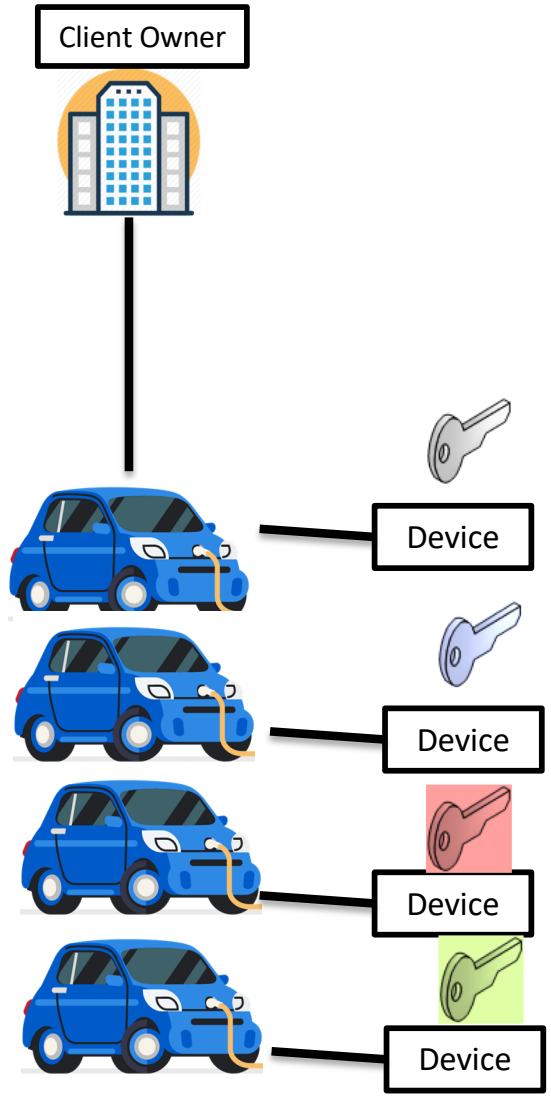



- IoT devices have limitations and cannot interact with Blockchains/Smart Contracts
  - Limited computational power and storage
  - Limited network connectivity
  - Security and trust issues
- The output of an actuation operation cannot be verified using cyber means

# Bridging the Cyber and Physical worlds using Blockchains and Smart Contracts

- realistic approach for paid IoT interactions:
  - **limit loss in case of disruption**
    - **micro-payments for micro-transactions**
    - make blockchain 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
- a feasible solution, now!
  - relies on existing, deployed technologies
- we leverage two existing solutions
  - Payment channels
  - Hash-based one time password (HOTP)



# High-Level …

**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...

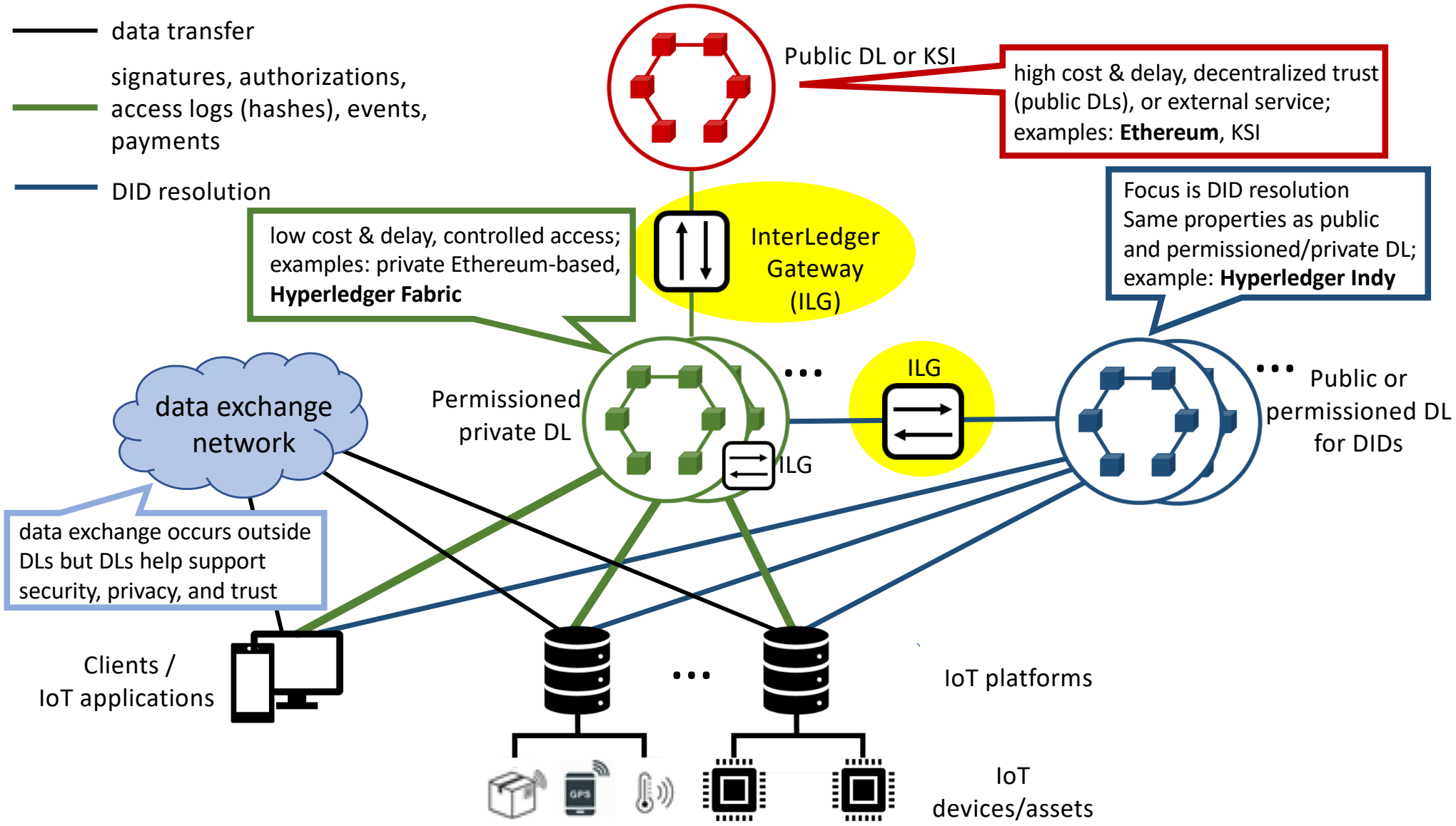
**System Properties**

- 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

✓ N. Fotiou, V.A. Siris, , S. Voulgrais, G.C. Polyzos, D. Lagutin, “Bridging the Cyber and Physical Worlds using Blockchains and Smart Contracts,” Proc. Workshop on **Decentralized IoT Systems and Security** (DISS) with the **Network and Distributed System Security Symposium** (NDSS), San Diego, CA, USA, February 2019.

Three ***types of ledgers*** with ***different functionality*** and ***features*** interconnected using interledger mechanisms

# *Interledger*



ILG

# Interledger: Why, What, Who, and How

- **Why** an interledger function (or operation)
  - Interconnection of otherwise existing/operating ledgers
  - Exploitation of different properties (performance, cost, privacy etc.)
  - Long-term evolution/robustness (smooth transfer of functionality across DLTs)
- **What** is an interledger function (or operation)
  - Transfer of information or value between ledgers
  - Basic operations: listen to events and submit transactions
  - Events & transactions on multiple ledgers can be cryptographically linked and can satisfy timing relations
- **Who** performs interledger functions: Three alternatives …
  - Interledger service provider (third party)
  - Existing entity, e.g. client or IoT platform
  - Private/permissioned or public decentralized system of interledger gateways; distributed execution and trust similar to blockchains but with specific function
- **How** is an interledger function performed
  - Listen to events or verify transactions on one ledger and perform transactions on another
  - Hash-locks cryptographically link events and transactions on multiple ledgers
  - Dependency of events or transactions on different ledgers can be one-to-one, one-to-many, many-to-one, or many-to-many
  - Time-locks ensure timing relations of events and transactions
  - Hash-locks and time-locks enforced automatically and transparently by smart contracts

# Conclusions

- Blockchains will be critical enablers
  for the IoT & 4th Generation Business Platforms
  - they will enable
    - unattended operation – the heart of the IoT & 4GBP

  through
    - automatic (smart) contract enforcement
    - creating trust between devices/systems with unplanned interactions
    - decentralized payments (also widely used as internal system incentives)

- **Interledger** technologies critical to exploit
  - widely varying properties of various DLTs
  - future proof solutions… by smoothly moving across DLTs

- Major challenges remain
  - performance issues
  - real-world events not directly verifiable by smart contracts
  - sustainability & business issues
  - … blockchains record transactions “in the open”
    - privacy issues
      - some data can be recorded encrypted
        - what?
        - how to pass on keys to unplanned future parties?

# Thank you!

***George C. Polyzos***

**Mobile Multimedia Laboratory**
Department of Informatics
School of Information Sciences and Technology
Athens University of Economics and Business
Athens, Greece

http://mm.aueb.gr/
polyzos@aueb.gr

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 779984

# Selected AUEB/MMlab Publications on DLTs for the IoT


- G.C. Polyzos and N. Fotiou, "**Blockchain-assisted Information Distribution for the Internet of Things**," Proc. 4th International Workshop on Information Integration in Cyber Physical Systems (IICPS) in conjunction with the 18th IEEE International Conference on Information Reuse and Integration, San Diego, CA, USA, Aug. 2017.
- A. Karila et al., "**Secure Open Federation for Internet Everywhere**," Proc. Workshop on Decentralized IoT Security and Standards (DISS) with the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, Feb. 2018.
- N. Fotiou, G.C. Polyzos, "**Smart Contracts for the Internet of Things: Opportunities and Challenges**," Proc. European Conference on Networks and Communications (EuCNC), Ljubljana, Slovenia, June 2018.
- N. Fotiou, V.A. Siris, G.C. Polyzos, "**Interacting with the Internet of Things using Smart Contracts and Blockchain Technologies**," Proc. 7th International Symposium on Security and Privacy on Internet of Things, with the 11th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Melbourne, Australia, Dec. 2018.
- N. Fotiou, V.A. Siris, S. Voulgaris, G.C. Polyzos, D. Lagutin, "**Bridging the Cyber and Physical Worlds using Blockchains and Smart Contracts**," Proc. Workshop on Decentralized IoT Systems and Security (DISS) in conjunction with the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, Feb. 2019.
- D. Lagutin, Y. Kortesniemi, N. Fotiou, V.A. Siris, "**Enabling Decentralised Identifiers and Verifiable Credentials for Constrained Internet-of-Things Devices using OAuth-based Delegation**," Proc. Workshop on Decentralized IoT Systems and Security (DISS) in conjunction with NDSS, San Diego, CA, USA, Feb. 2019.
- Y. Kortesniemi, D. Lagutin, T. Elo, N. Fotiou, "**Improving the Privacy of IoT with Decentralised Identifiers (DIDs)**," *Journal of Computer Networks and Communications*, Vol. 2019, March 2019.
- V.A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, G.C. Polyzos, "**OAuth 2.0 Meets Blockchain for Authorization in Constrained IoT Environments**," Proc. 5th IEEE World Forum on Internet of Things, Limerick, Ireland, April 2019.
- V.A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, G.C. Polyzos, "**Interledger Smart Contracts for Decentralized Authorization to Constrained Things**," Proc. 2nd Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock 2019), in conjunction with IEEE INFOCOM 2019, Paris, France, April–May 2019.