H2020 **IoT** Project

SOFIE

Secure Open Federation for Internet Everywhere

George C. Polyzos

Mobile Multimedia Laboratory

Department of Informatics
School of Information Sciences and Technology
Athens University of Economics and Business
Athens, Greece

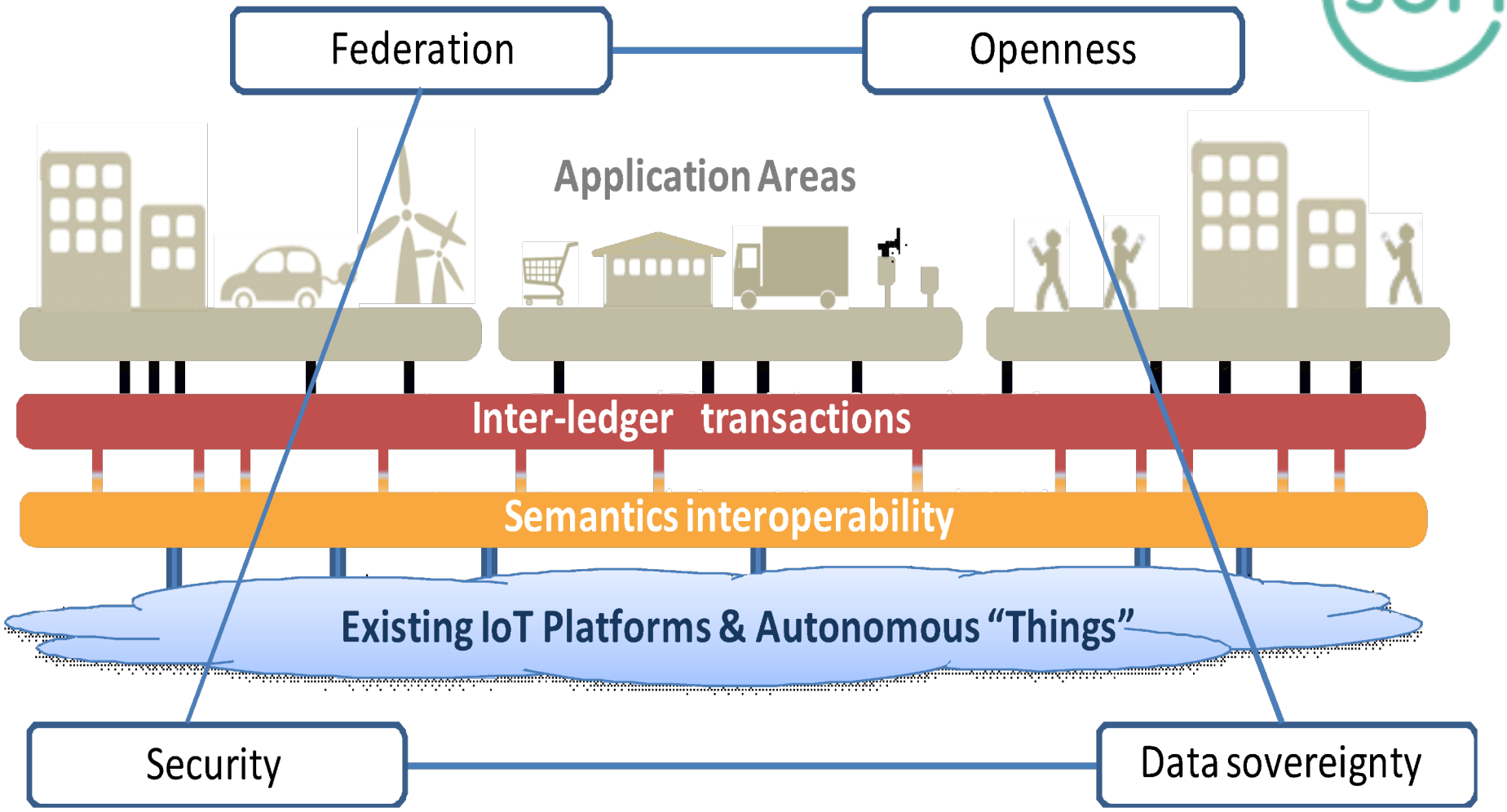
polyzos@aueb.gr, https://mm.aueb.gr/
Tel.: +30 210 8203 650, Fax: +30 210 8203 325

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

Motivation & Vision

- Key issues
  - IoT Fragmentation
  - Security & privacy
- Most of IoT: Vertically oriented, closed systems
  - Silos!
- Interoperability
  - well over 300 different IoT platforms
  - several dozens … standards
  - …
  - **business** counter-incentives
  - **privacy** constraints
- Vision: **4th Generation *Open* Business Platforms**
  - Exchanging data in an automatic and controlled way
    - Open public DLTs can contribute towards this goal
    - DLTs have various characteristics and properties
      - **Interledger**!

SOFIE: Overall Concept and Key Ideas



H2020 SOFIE: Secure Open Federation of Internet Everywhere

- 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 resolve disputes

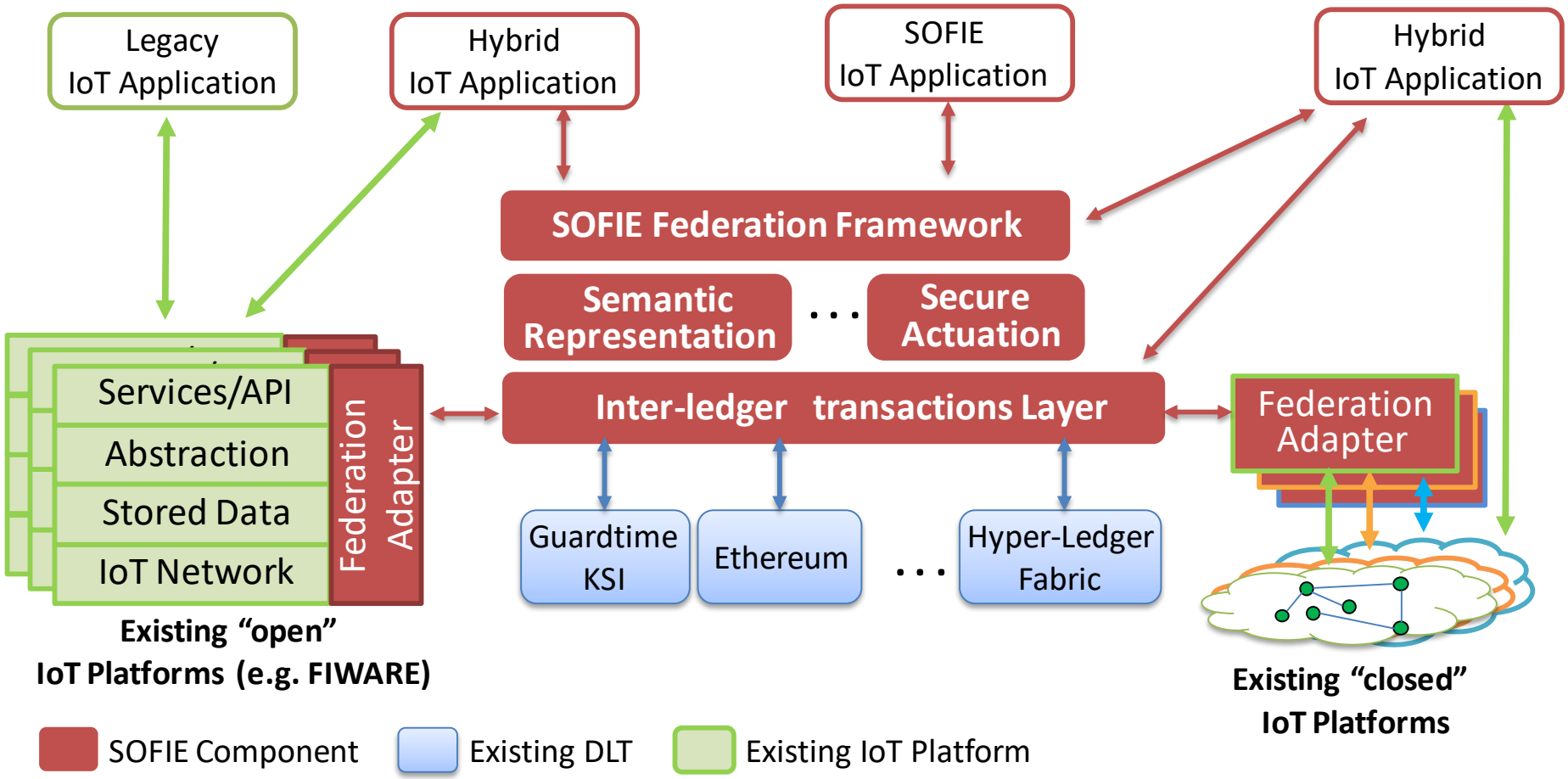
- Project
  - 1/1/2018 – 31/12/2020
  - €4.5M

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

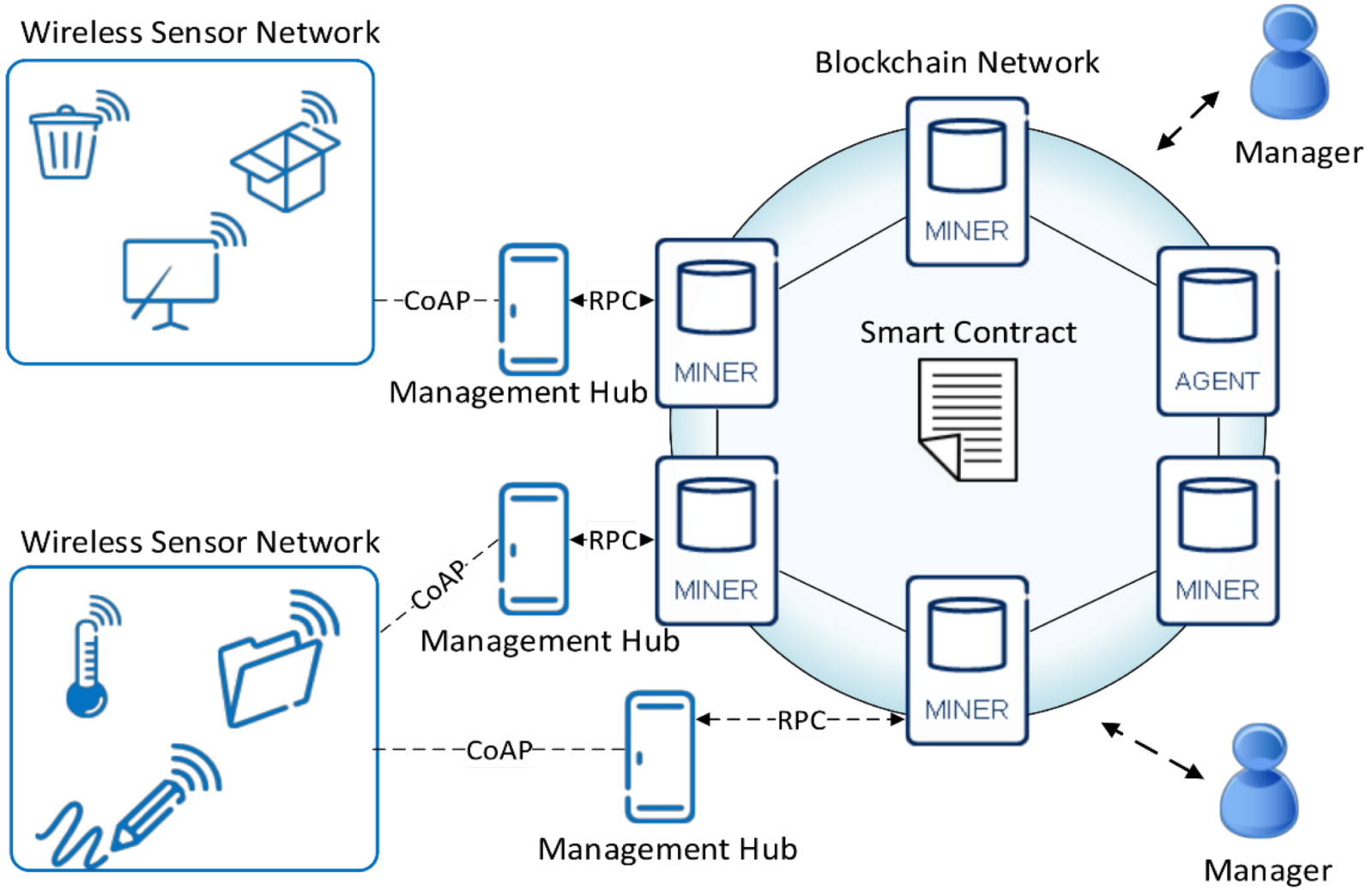
polyzos@aueb.gr

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

SOFIE's Federation Architecture

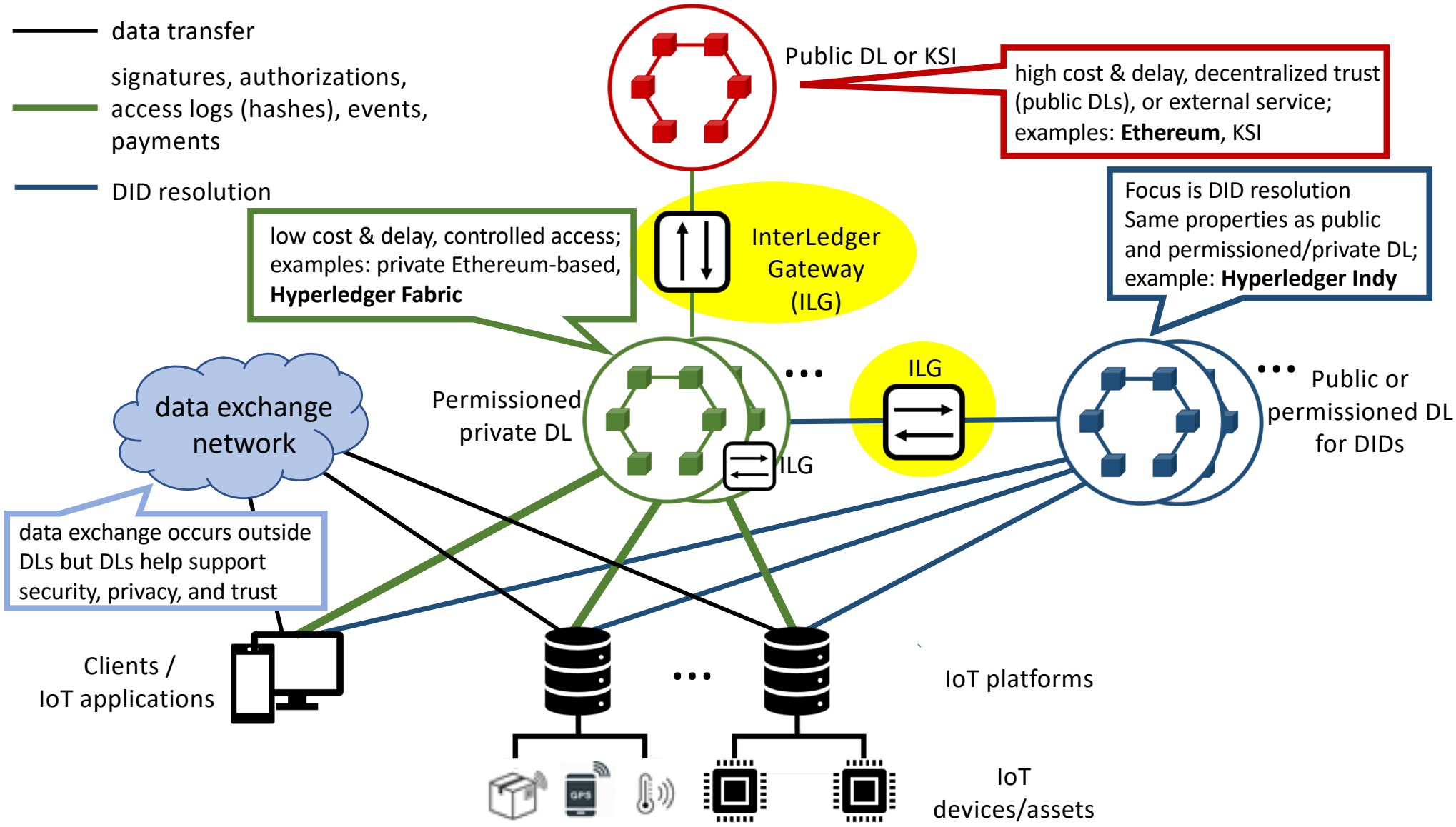


SOFIE's Decentralized IoT Management System using Blockchains



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

Interledger

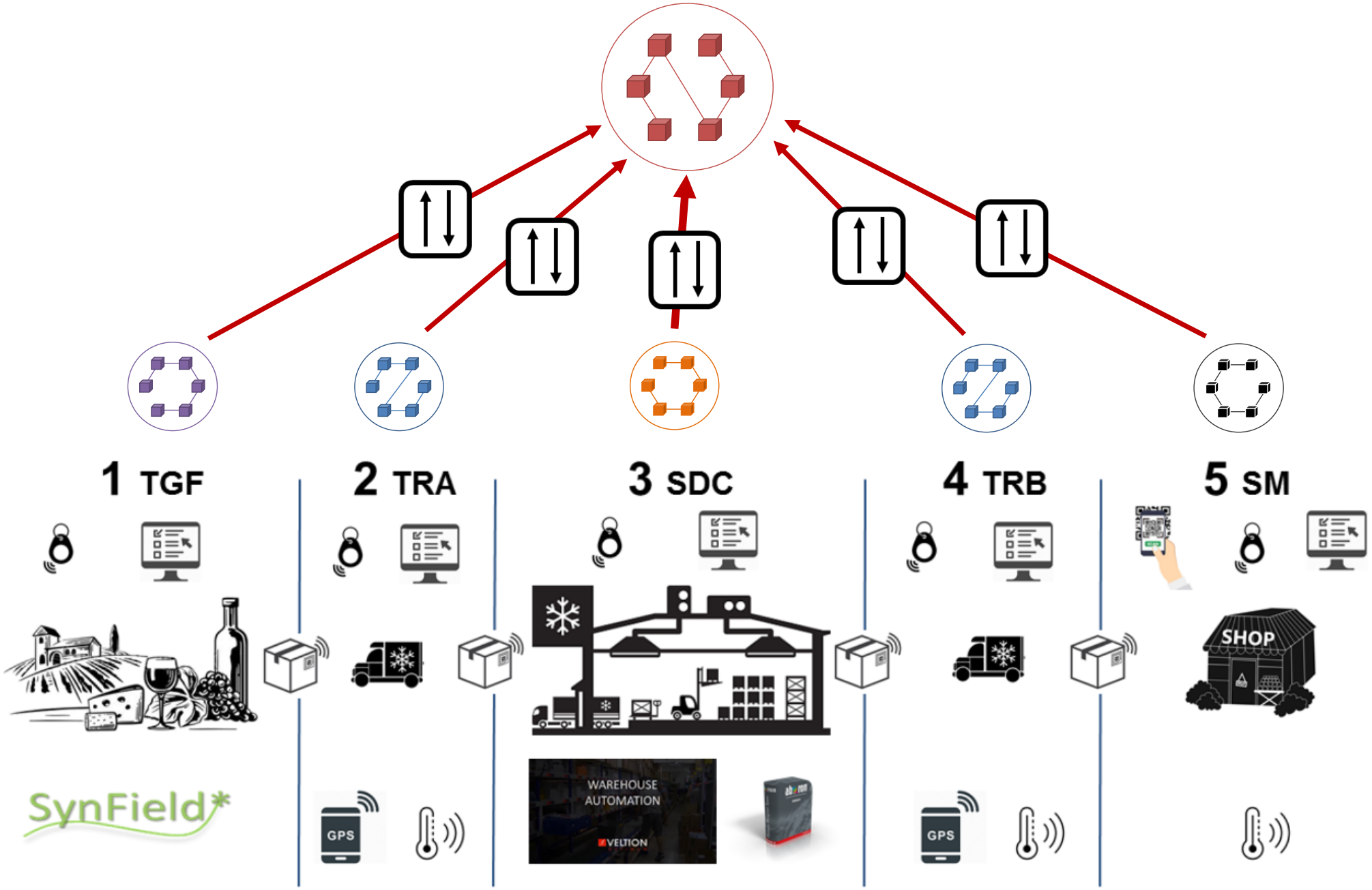


ILG

Interledger: Why, What, Who, and How

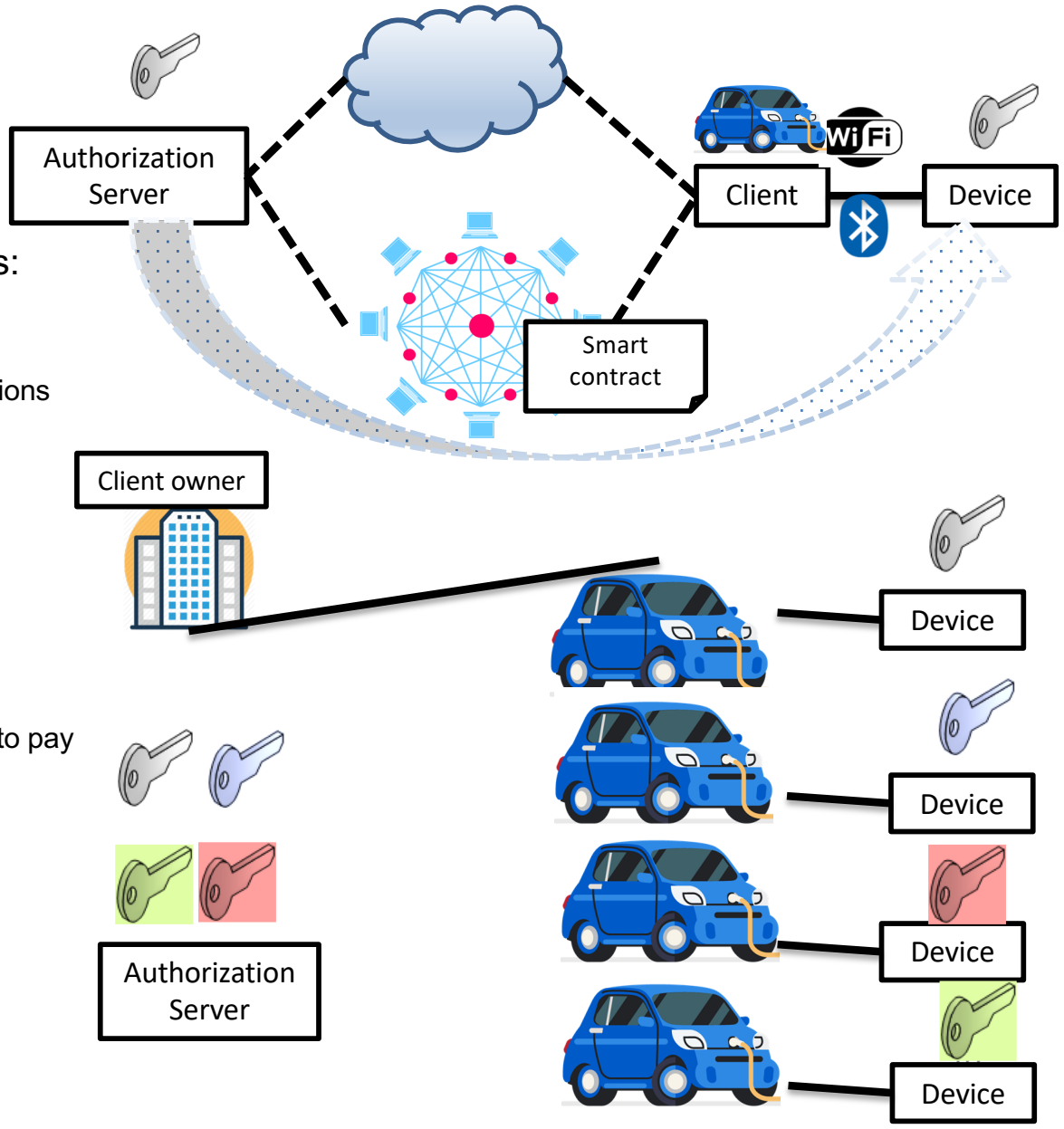
- **Why** an interledger function (or operation)
  - Interconnection of otherwise existing/operating ledgers
  - Exploitation of different properties (performance, cost, privacy etc.)
  - Long-term evolution/robustness (smooth transfer of functionality across DLTs)
- **What** is an interledger function (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

SOFIE's Food Chain Pilot



Bridging the Cyber and Physical worlds using blockchains and smart contracts

- We leverage two existing solutions
  - Payment channels
  - Hash-based one time password (HOTP)
- 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 for a service
- a feasible solution now
  - relies on existing, deployed technologies



polyzos@aueb.gr

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

- 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 SOFIE Publications

- 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.
- A.S. Ahmed, T. Aura, "**Turning Trust Around: Smart Contract-Assisted Public Key Infrastructure**," Proc. 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, Aug. 2018.
- S. Paavolainen, T. Elo and P. Nikander, "**Risks from Spam Attacks on Blockchains for Intemet-of-Things Devices**," Proc. 9th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, Nov. 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 (SPIoT) with the 11th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS), 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.