Decentralized Operation and Security in the IoT Space

The IoT space and where SOFIE fits in

What kind of results are produced

A broader sense overview

George C. Polyzos

Mobile Multimedia Laboratory

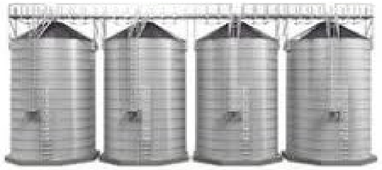
Department of Informatics
School of Information Sciences and Technology
Athens University of Economics and Business
Athens, Greece

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

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

Motivation & Vision

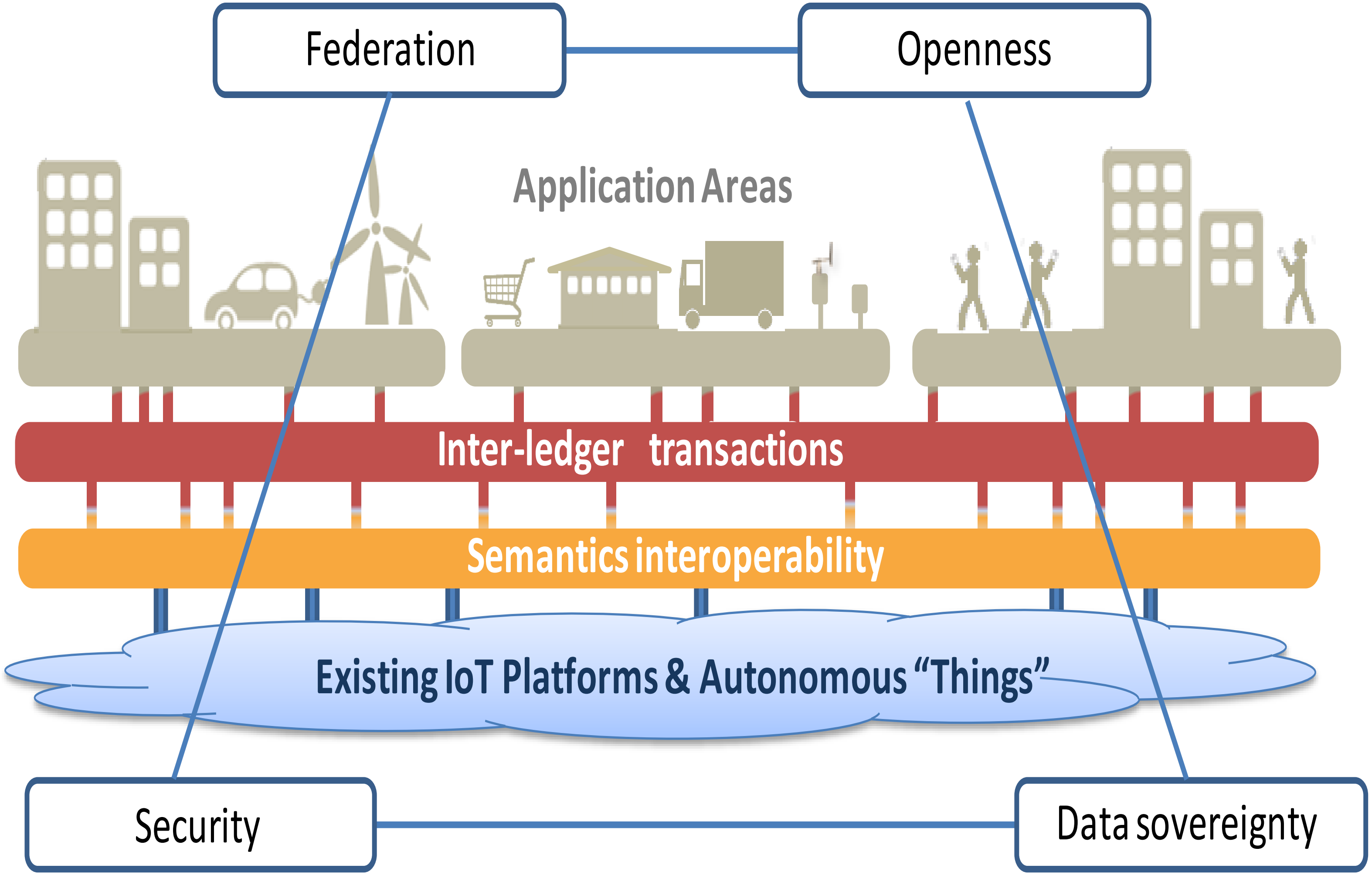
- The Internet-of-Things (IoT): vision
  - unattended operation
- Key IoT issues
  - IoT Fragmentation
  - security & privacy
- Most of IoT: Vertically oriented, *closed* systems



  - Silos!
  - mostly for non-purely-technical reasons
- Interoperability and interconnection
  - well over 300 different IoT platforms
  - several dozens … standards
  - …
  - **business** counter-incentives
  - **privacy** concerns and constraints

- Vision: **4th Generation *Open* Business Platforms**
  - across IoT systems and business platforms
    - exchange data in an automatic and controlled way
    - ... & perform actions
  - Smart Contracts on open public blockchains can contribute towards this goal
  - Distributed Ledger Technologies (DLTs)
    - … blockchains
    - decentralized trust, automation (Smart Contracts)
    - various types, various characteristics & properties
      - permissionless/open, permissioned…
    - combine different DLTs for various trade-offs
  - **Interledger**!

SOFIE: Overall Concept and Key Ideas



Federation
Openness
Application Areas
Inter-ledger transactions
Semantics interoperability
Existing IoT Platforms & Autonomous "Things"
Security
Data sovereignty

- Openness
  - inclussiviness
  - system expansion
- Federation
  - loose interconnection
  - diverse systems interoperability
- Security
  - increases trust
  - proper operation
- Data Sovereignty
  - key principle
  - incentive for cooperation/interoperation

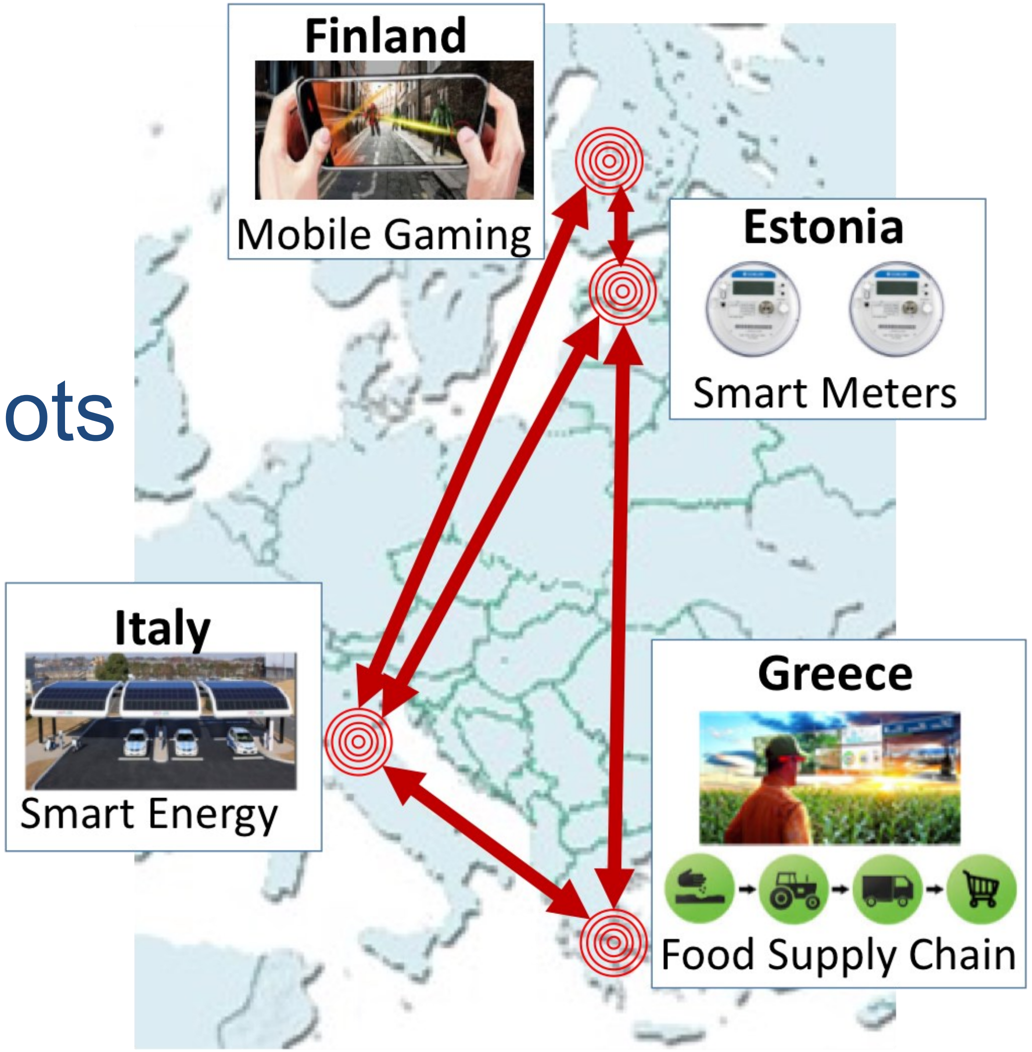
H2020 **SOFIE**:
Secure Open Federation for Internet Everywhere

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

  federate IoT platforms

- ***interconnected*** distributed ledgers
  - to interconnect diverse IoT systems
  - decentralized business platforms
    - open business rules on how to join platforms
  - accessible metadata
    - & semantic interoperability
  - securely record **audit trails**
    - to resolve disputes

4 Pilots



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

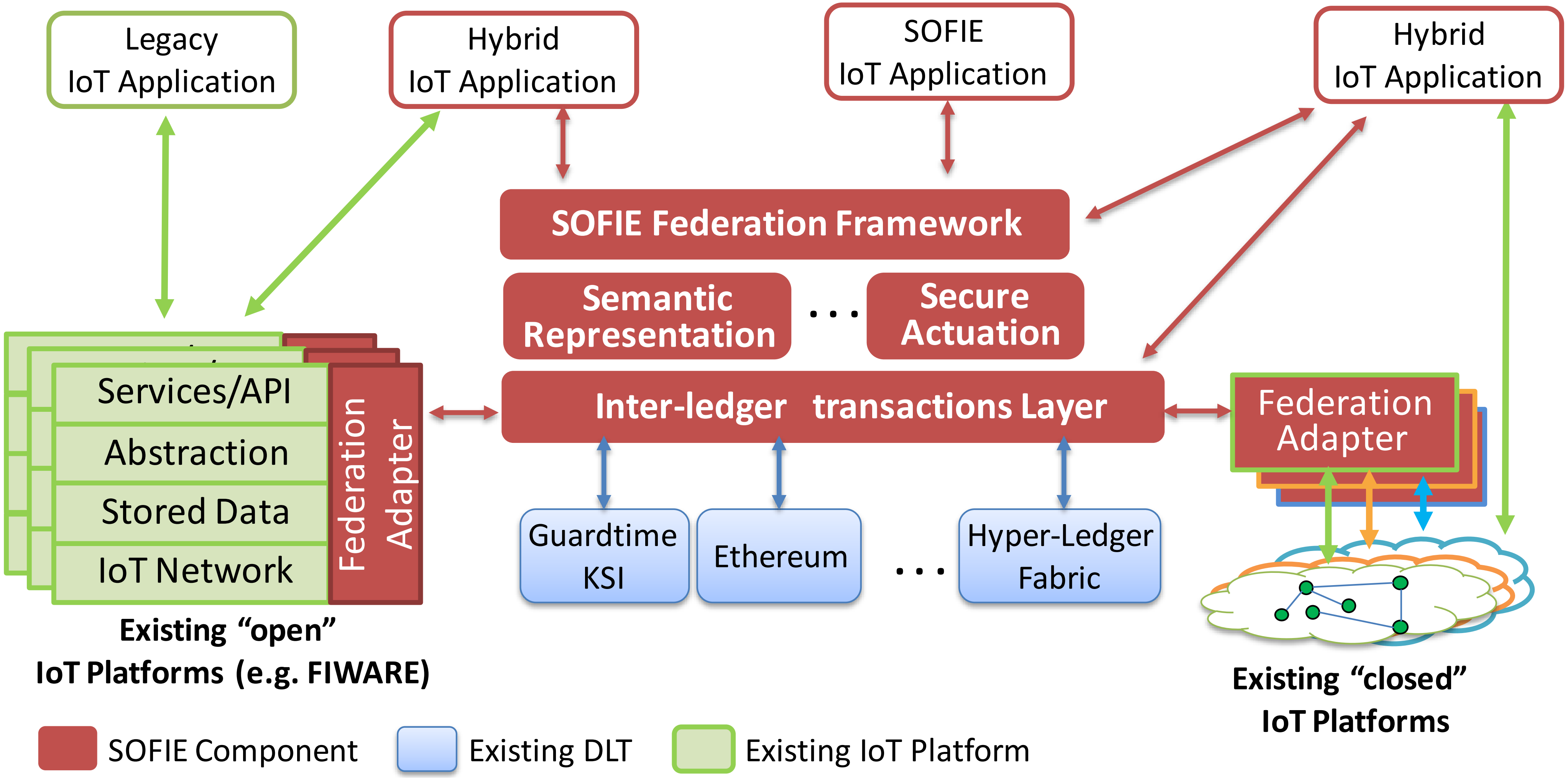
- Partners
  - Aalto University, Ericsson, Rovio (Finland)
  - Guardtime (Estonia)
  - AUEB, Synelixis, Optimum (Greece)
  - Eng, Asm Terni Spa, Emotion Srl (Italy)

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

DLTs: Properties, Guarantees, and Trade-offs

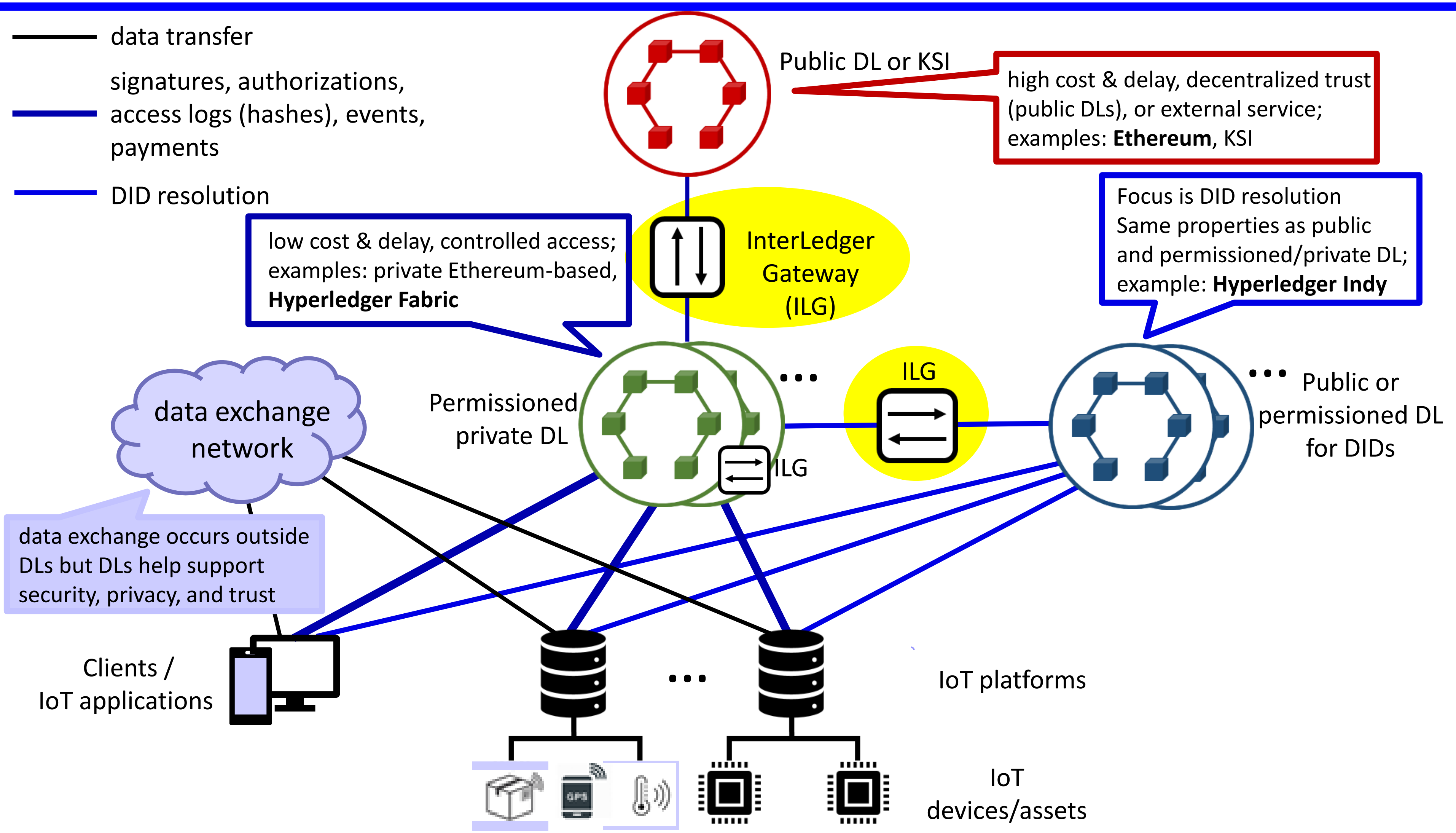
- DLTs (Distributed Ledger Technologies) / blockchains
  - **Decentralized trust**: no dependence on a single trusted (“third”) party
  - **Immutability**: signatures & majority of nodes need to agree on state changes
  - **Availability**: decentralized storage and execution – robust against multiple node failures
  - **Transparency**: not only a feature, but a requirement for decentralized trust
    - could conflict with **privacy** requirements & **business** logic ➔ permissioned DLTs
  - Off-chain transactions … starting and ending on the blockchain…
    - Scope of trust between two parties (e.g., funds set aside…) ➔ fast direct transactions with limited overhead (& signed receipts)
- Interledger: interconnection of multiple DLTs
  - Tradeoffs: permissionless/public/open ledgers vs. permissioned/private ledgers
    - wide-scale decentralized trust vs. consortium trust
    - full transparency vs. privacy
    - monetary cost, overhead, performance/latency, scalability trade-offs
- Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs)
  - Improved privacy, availability

SOFIE’s Federation Architecture



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

Interledger



data transfer

signatures, authorizations, access logs (hashes), events, payments

DID resolution

high cost & delay, decentralized trust (public DLs), or external service; examples: **Ethereum**, KSI

low cost & delay, controlled access; examples: private Ethereum-based, **Hyperledger Fabric**

Focus is DID resolution
Same properties as public and permissioned/private DL;
example: **Hyperledger Indy**

data exchange occurs outside DLs but DLs help support security, privacy, and trust

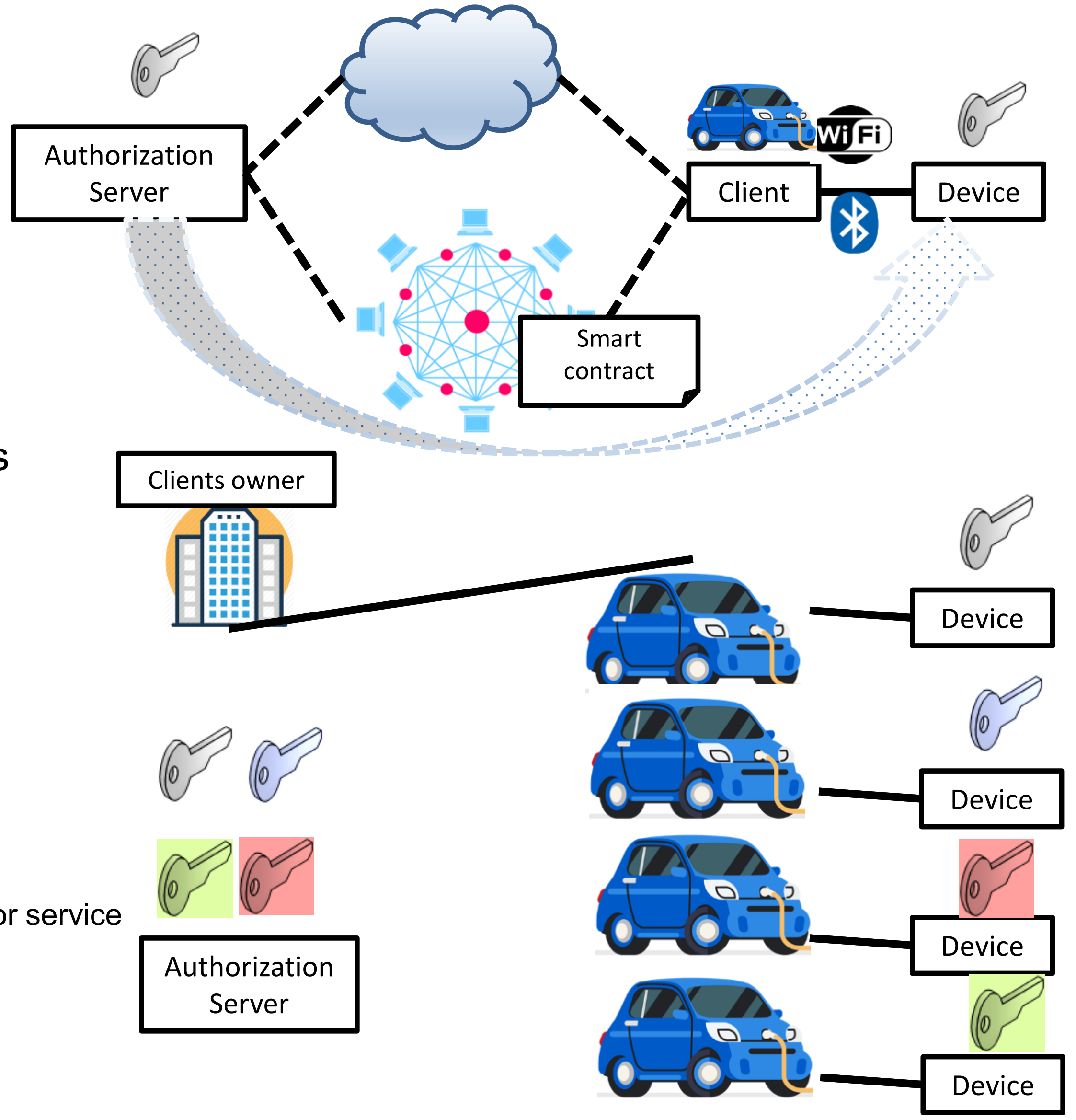
Interledger: Why, What, Who, and How

ILG

- **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
    - 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

Bridging the Cyber & Physical worlds using DLTs and smart contracts
Electric Vehicle fleet management: charging at 3rd-party stations

- we leverage two existing solutions
  - Payment channels
  - Hash-based one-time passwords (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 service
- a feasible solution now
  - relies on existing, deployed technologies



Agenda

- **Combining multiple ledgers for better control – Interledger approaches in IoT**
  - Santeri Paavolainen, Aalto University (Finland)
- **Enabling Decentralised Identifiers and Verifiable Credentials for Constrained IoT Devices**
  - Prof. Vasilios A. Siris, Professor, AUEB (Greece)
- **Enabling next generation secure energy services through data exchange liberation**
  - Priit Anton, Guardtime OÜ (Estonia)
- **A marketplace for flexibility: improving power network efficiency using electric vehicles**
  - Giuseppe Raveduto, Engineering Ingegneria Informatica (Italy)
- **Exploring DLT & IoT use-cases in mobile gaming**
  - Max Samarin, ROVIO (Finland)
- **Blockchain-based Architectures for Food Supply-Chain Management**
  - Prof. Spyros Voulgaris, AUEB (Greece)

- **Conclusion**: George C. Polyzos, AUEB (Greece)
- **Closing Remarks**: Nicholas Ferguson, Cyberwatching.eu Project Coordinator (Italy)

Summary & Conclusions

- Blockchains/DLTs as enablers for
        - the IoT &
        - 4th Generation Business Platforms
    - support unattended operation
        - the heart of the IoT & 4GBP

  through
    - automatic (smart) contract enforcement
    - trust between devices/systems with unplanned interactions
    - decentralized payments
    - audit trails

- Interledger & multiple DLTs improve
    - privacy
    - cost
    - scalability
    - efficiency
    - performance
    - longevity

- SOFIE is driven by 4 pilots
    - grounded in real applications
    - direct impact in diverse industries
    - indirect impact in
        - IoT architecture
        - business platforms
        - identification, privacy…
        - …

- Major challenges remain
    - sustainability & business issues
    - real-world events not directly verifiable by smart contracts
        - oracles... (decentralized oracles…)
    - performance issues
    - … blockchains record transactions “in the open”
        - privacy issues
            - some data can be recorded encrypted on public ledgers
                - what?
                - how to pass on keys to unplanned future parties?
        - **interledger**… (with private ledger)
        - …

Selected SOFIE Publications

Journal Publications

- V.A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, G.C. Polyzos, “Interledger Approaches,” ***IEEE Access***, vol. 7, 2019.
- S. Voulgaris, N. Fotiou, V.A. Siris, G.C. Polyzos, M. Jaatinen, Y. Oikonomidis, “Blockchain Technology for Intelligent Environments,” ***Future Internet***, vol. 11, 2019.
- Y. Kortesniemi, D. Lagutin, T. Elo, N. Fotiou, “Improving the Privacy of IoT with Decentralised Identifiers (DIDs),” ***Journal of Computer Networks and Communications***, March 2019.
- V.A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, G.C. Polyzos, “Decentralized authorization in constrained IoT environments exploiting interledger mechanisms,” ***Computer Communications***, Elsevier, vol. 152, February 2020.

Conference and Workshop Publications

- 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), August 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 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) 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.
- D. Lagutin et al., “**Secure Open Federation of IoT Platforms through Interledger Technologies – The SOFIE Approach**,” Proc. European Conference on Networks and Communications (EuCNC), Valencia, Spain, June 2019.
- N. Fotiou, I. Pittaras, V.A. Siris, S. Voulgaris, G.C. Polyzos, “**OAuth 2.0 Authorization using Blockchain-based Tokens**,” Proc. Workshop on Decentralized IoT Systems and Security (DISS) in conjunction with the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, February 2020.
- S. Voulgaris, N. Fotiou, V.A. Siris, G.C. Polyzos, A. Tomaras, S. Karachontzitis, “**Hierarchical Blockchain Topologies for Quality Control in Food Supply Chains**,” Proc. European Conference on Networks and Communications (EuCNC), June 2020.

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

Let’s discuss cooperation!

We welcome discussions
&
we are open to various types of collaboration

Each SOFIE pilot has a **dissemination** and **exploitation** agenda – contact each pilot lead directly!

www.sofie-iot.eu
twitter.com/EU_Sofie
linkedin.com/company/sofie

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