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

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

polyzos@aueb.gr
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
  - polyzos@aueb.gr

- **Partners**
  - Aalto University, Ericsson, Rovio (Finland)
  - Guardtime (Estonia)
  - AUEB, Synefexis, Optimum (Greece)
  - Eng, Asm Terni Spa, Emotion Srl (Italy)
SOFIE’s Federation Architecture

- Legacy IoT Application
- Hybrid IoT Application
- SOFIE IoT Application
- Hybrid IoT Application

- Services/API
- Abstraction
- Stored Data
- IoT Network

- Inter-ledger transactions Layer
- Guardtime KSI
- Ethereum
- Hyper-Ledger Fabric

- SOFIE Federation Framework
  - Semantic Representation
  - Secure Actuation

- Federation Adapter

- Existing “open” IoT Platforms (e.g. FIWARE)
- Existing DLT
- Existing IoT Platform

polyzos@aueb.gr
SOFIE’s Decentralized IoT Management System using Blockchains
Three types of ledgers with different functionality and features interconnected using interledger mechanisms.
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

1 TGF
2 TRA
3 SDC
4 TRB
5 SM

SynField*
Bridging the Cyber and Physical worlds using blockchains and smart contracts

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


polyzos@aueb.gr