Mobile Multimedia Laboratory

EU program Horizon 2020

SOFIE:
Secure Open Federation of 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

Outline

- Introduction
  - The Internet of Things: Vision & Status
  - IoT Challenges
    - Interoperability, Sustainability, Trust Model, Security, and Privacy
    - The role of Blockchains
- SOFIE: **S**ecure **O**pen **F**ederation for **I**nternet **E**verywhere
  - Motivation and Rationale
  - Use-cases and Trials
  - **4th Generation Platforms**
- Conclusion and Outlook

- Blockchain-assisted Information Distribution

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
    - refrigerators, scales, TVs, …
    - continuously decreasing manufacturing cost of sensors and actuators
    - new protocols for autonomous M2M communication
- Fragmentation & lack of security are the main issues today
- Most IoT: Vertically oriented, closed systems
  - Silos!

IoT Challenges

- Interoperability
- Sustainability
- Trust Model
- Security
- Privacy

The Interoperability Challenge

- well over 300 different Internet of Things (IoT) platforms
- several dozens … standards
- different basic IoT communication protocols will co-exist
  - Constrained Application Protocol (CoAP)
  - Message Queue Telemetry Transport (MQTT)
  - HTTP
- most of the deployed IoT systems are closed
  - largely incapable of communicating with other IoT systems

The Sustainability Challenge

- How often do we change/update…
  - smartphone?
  - laptop?
  - car?
  - refrigerator?
  - house electronic infrastructure (security system)?
- Danger of fragmented ecosystems
  - composed of old and new devices
- In many scenarios Things are “deployed and forgotten”
  - sensors installed during the construction of a building
  - bio-signal detection inside the body of a patient or of a wild animal

The Trust Model Challenge

- IoT's biggest breakthrough/vision:
  seamless, "unattended" interaction
  between the ***cyber*** and the ***physical*** worlds

- A new trust model is needed to enable the interaction of all devices ***with little human intervention***

- We need novel mechanisms for
  - transactions
  - compensation
  - accountability

The Security Challenge

- Existing security solutions cannot be directly applied to Things
  - Things are resource limited
    - no computational power for complex cryptographic operations
  - Things often (physically) exposed to malicious users.
  - Not always feasible to (remotely) connect to a Thing
- Things important/sensitive
  - can collect sensitive and personal information
  - may control critical aspects of our daily life

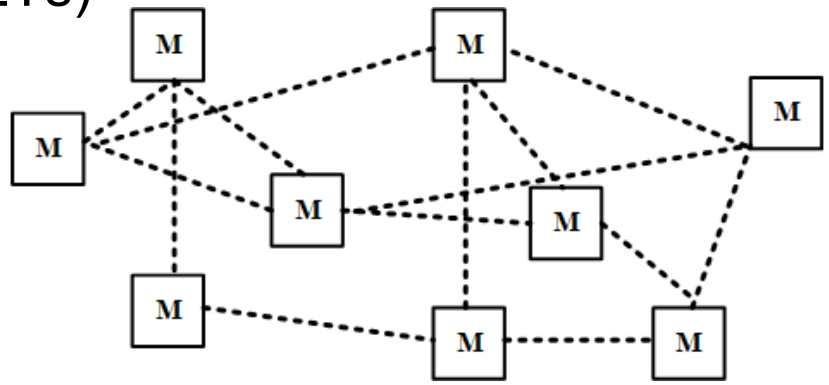
- **Actuators**, not only sensors
  - security even more critical… safety

The Privacy Challenge

- Things can collect personal and sensitive information
  - which may control critical aspects of our life
  - or the information obtained may impact our life
- Information from the IoT
  - can have significant context
  - be highly correlated…
- Because of the pervasive and invisible aspects of the IoT
  - information may be collected for a long time before it becomes known (and its impact felt)

Blockchains and Smart Contracts: part of the solution…

- Blockchain: "A ***distributed append-only*** ledger of transactions maintained by a number of (untrusted) **M**iners organized in a (distributed) network"
  - Distributed Ledger Technologies (DLTs)

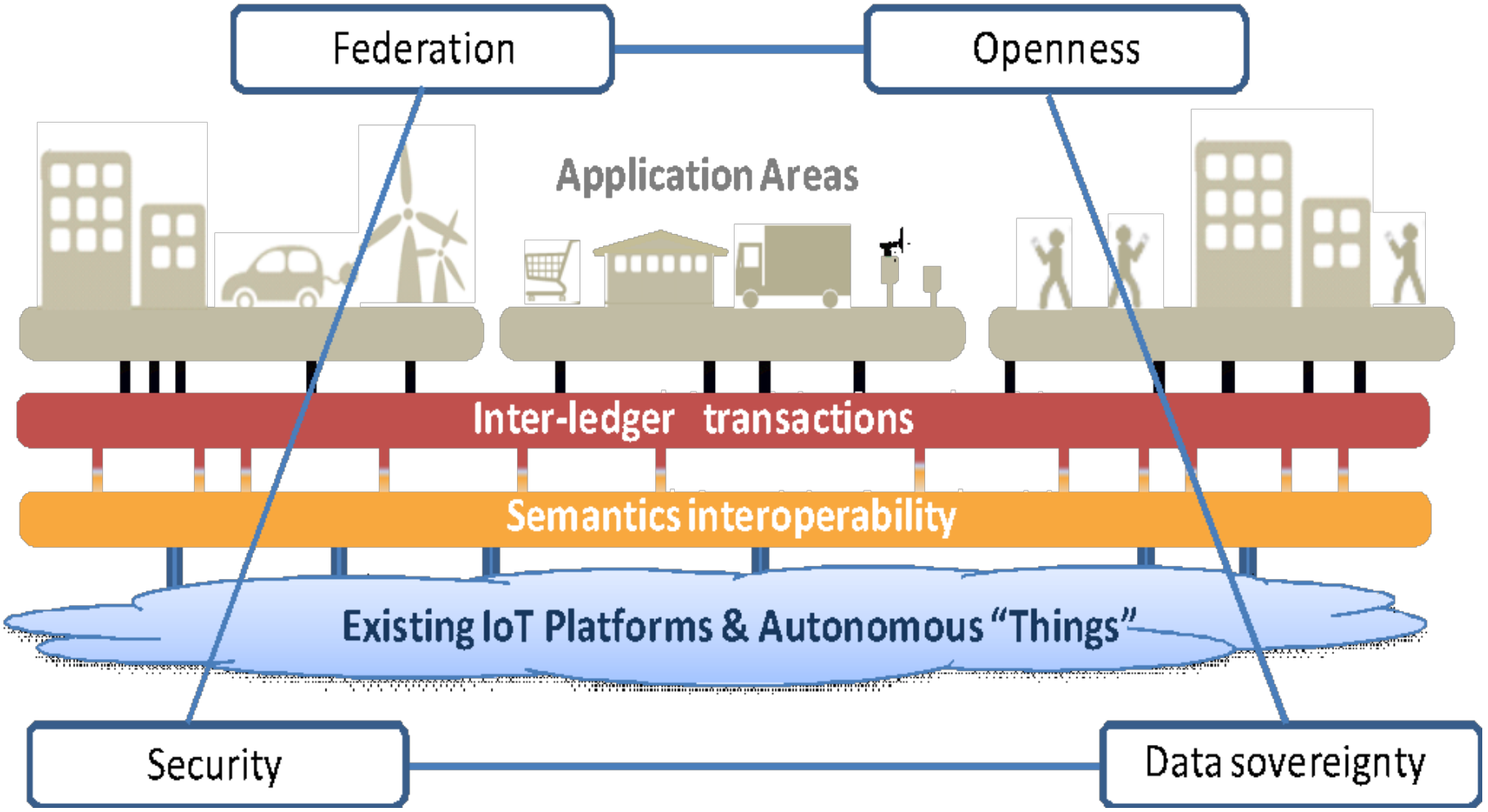


- Smart contracts
  - Built on DLTs
  - Autonomous applications with pre-defined inputs and outputs
    … that can be executed by a miner in a deterministic way
  - Any user can invoke a smart contract, the outcome of which is recorded as a transaction in the blockchain

SOFIE:
Secure **O**pen **F**ederation of **I**nternet **E**verywhere

- Applying Distributed Ledger Technology (DLT)
  - e.g. blockchains
- to securely and openly federate IoT platforms
- with *interconnected* distributed ledgers to
  - build decentralized business platforms
  - support the interconnection of diverse IoT systems
  - provide openly accessible metadata about platforms
  - define business rules on how to connect to platforms
  - securely record audit trails to be used to resolve disputes

SOFIE: Overall Concept and Key Ideas

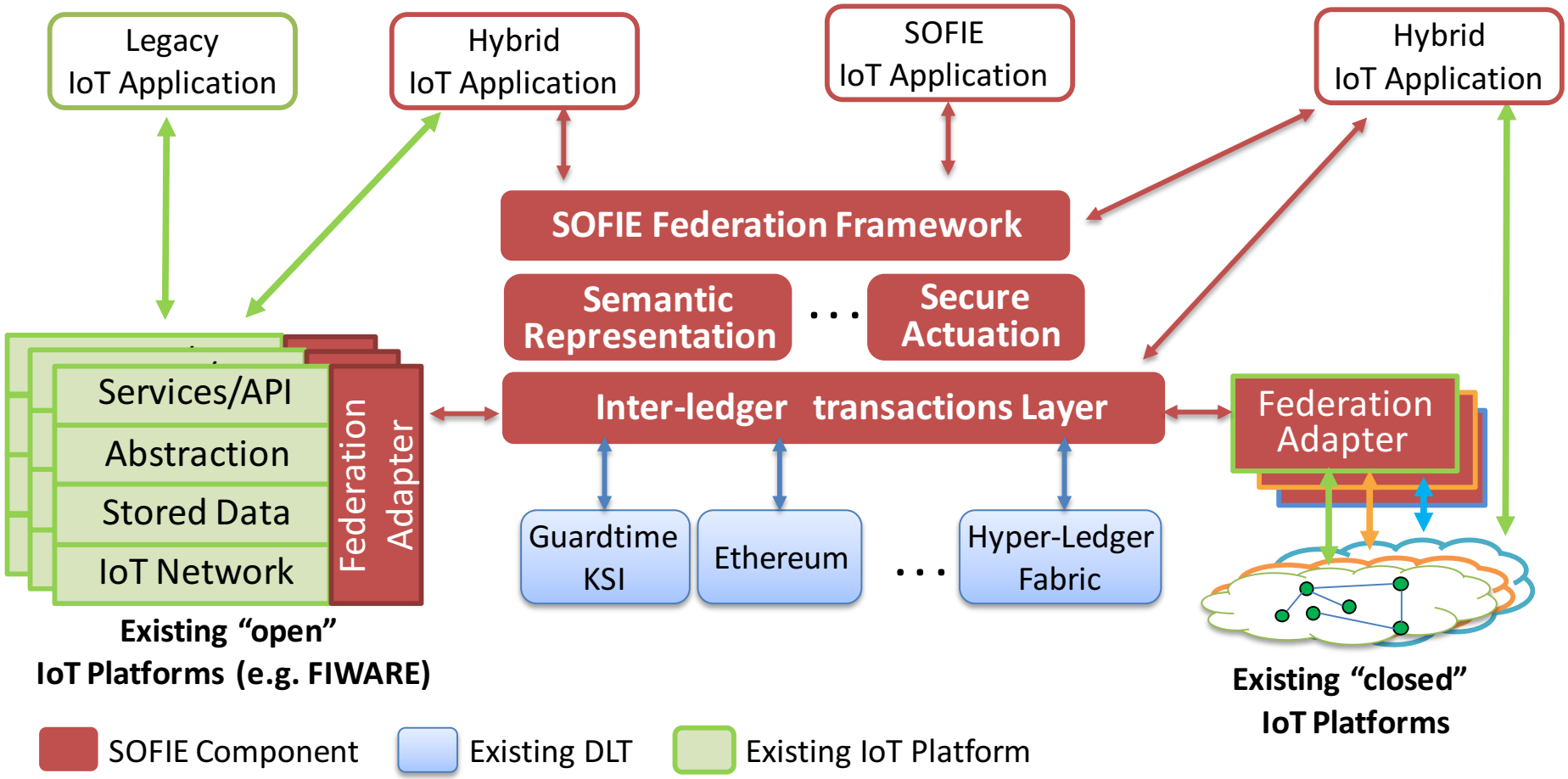


SOFIE

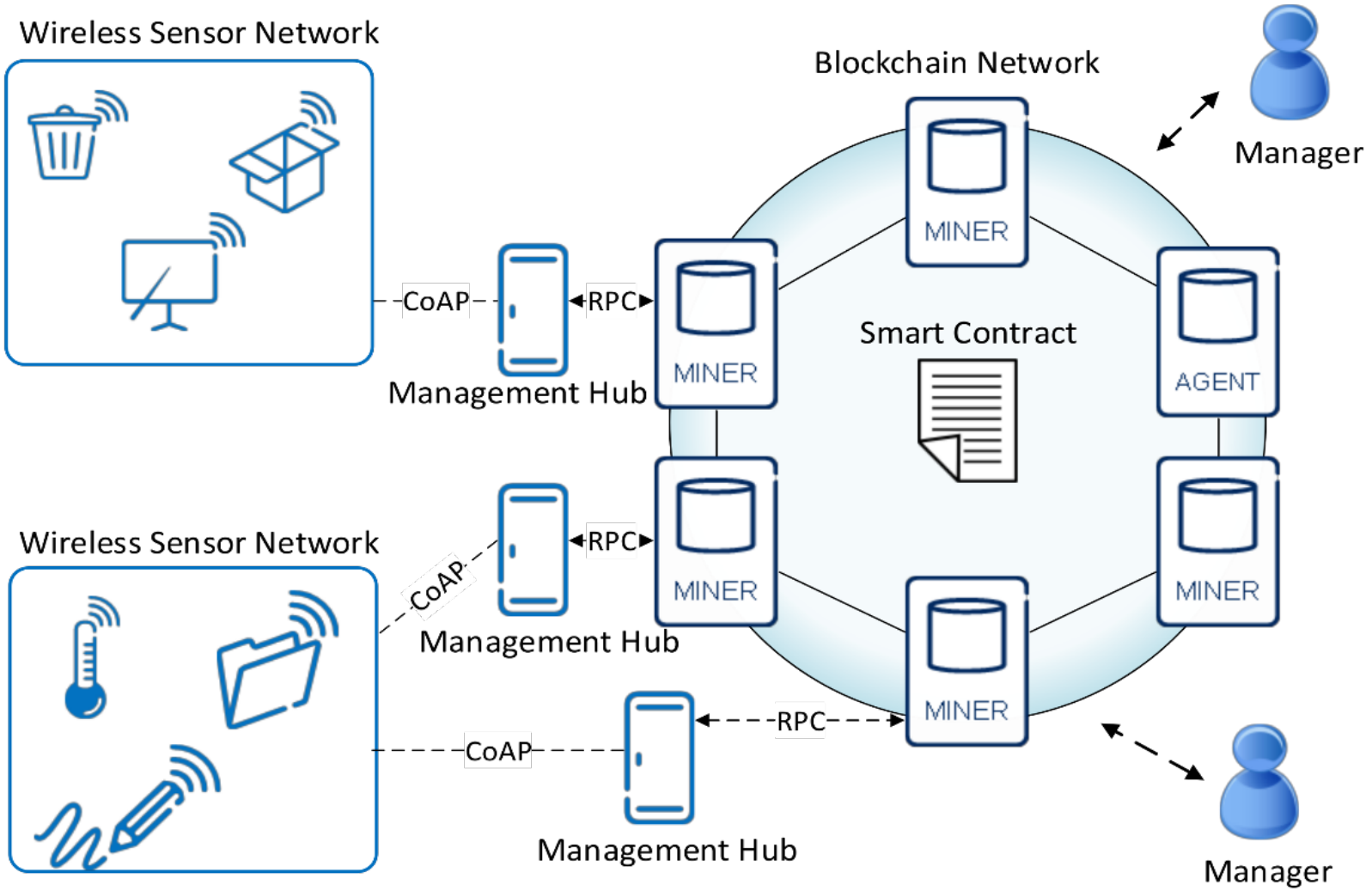
- The concept will be prototyped and studied in an EU Horizon 2020 funded project
  - 1/1/2018 – 31/12/2020
  - €4.5M

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

SOFIE's Federation Architecture

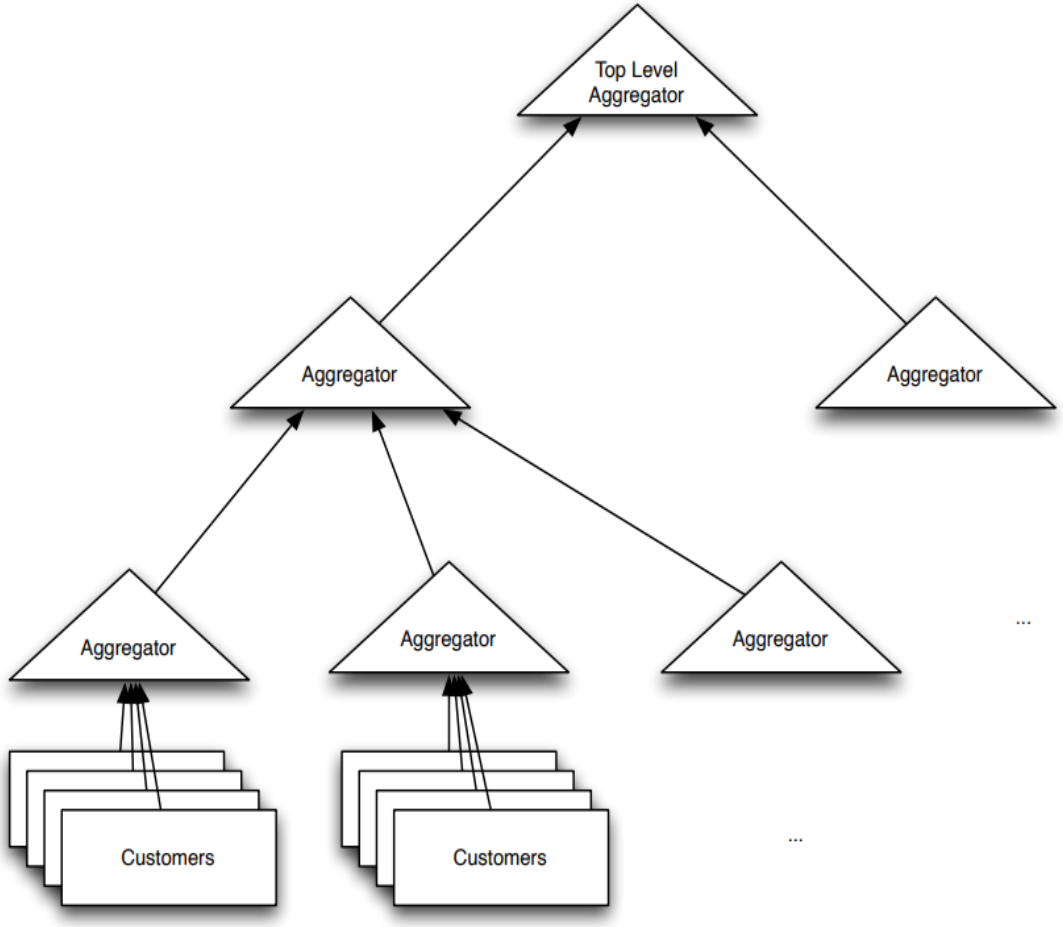


SOFIE's Decentralized Management System using Blockchains



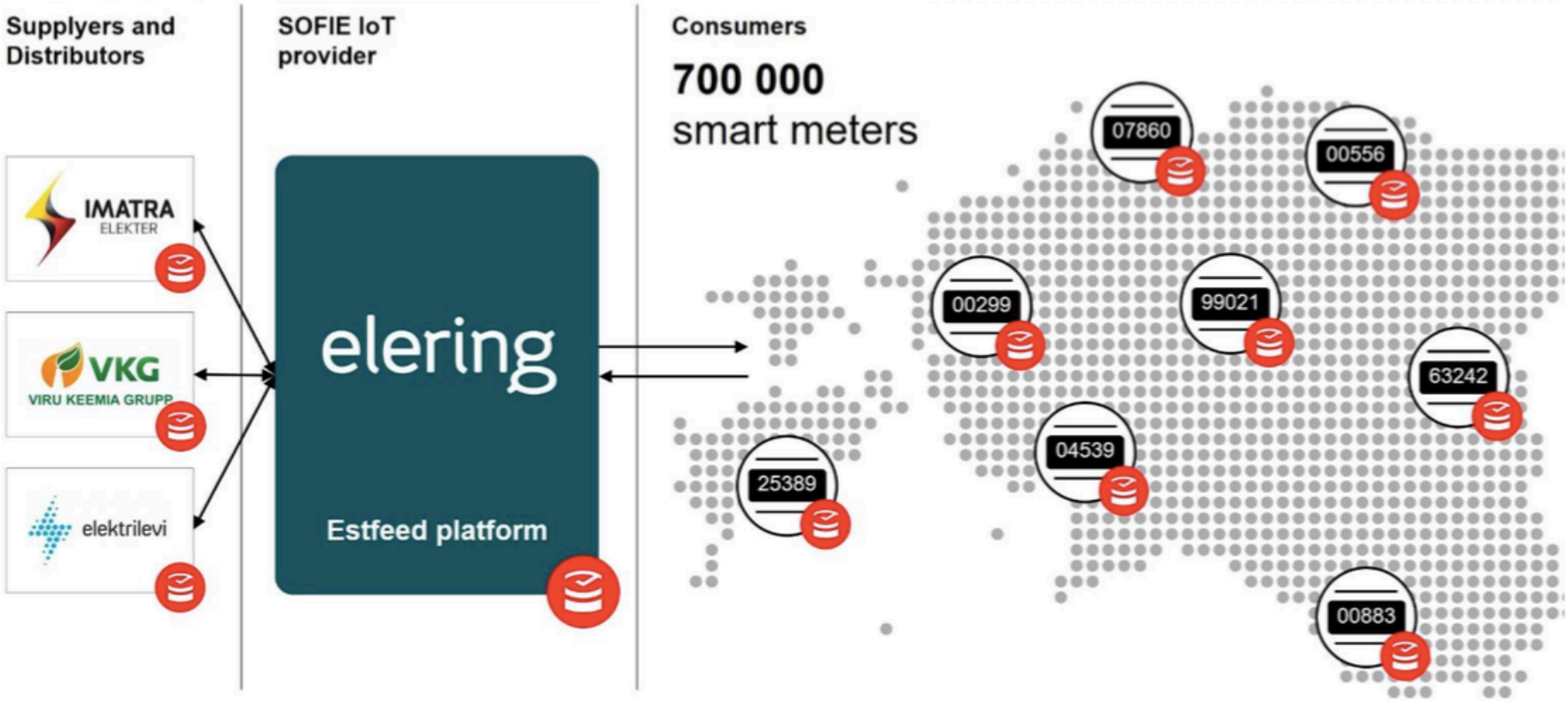
Guardtime's Keyless Signatures' Infrastructure (KSI)

- Permissioned ledger
- In production since April 2008
- Each block is the root of a Merkle tree
- The leafs of the tree are hashes of documents
- Formally verified
- Once per month: current block is published in the FT

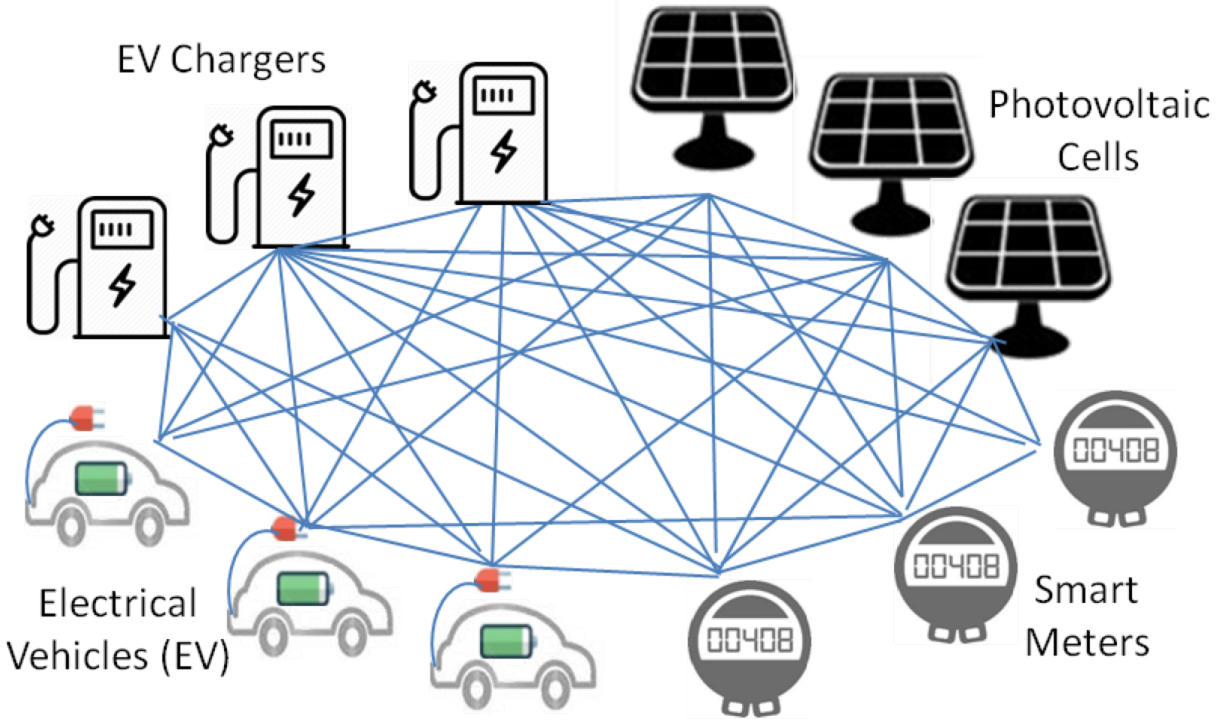


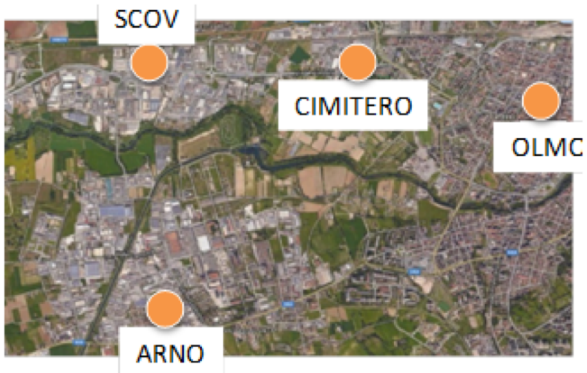
Ahto Buldas and Andres Kroonmaa and Risto Laanoja, Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees, Cryptology ePrint Archive: Report 2013/834

SOFIE's Energy I Pilot: Smart Meters (Estonia)

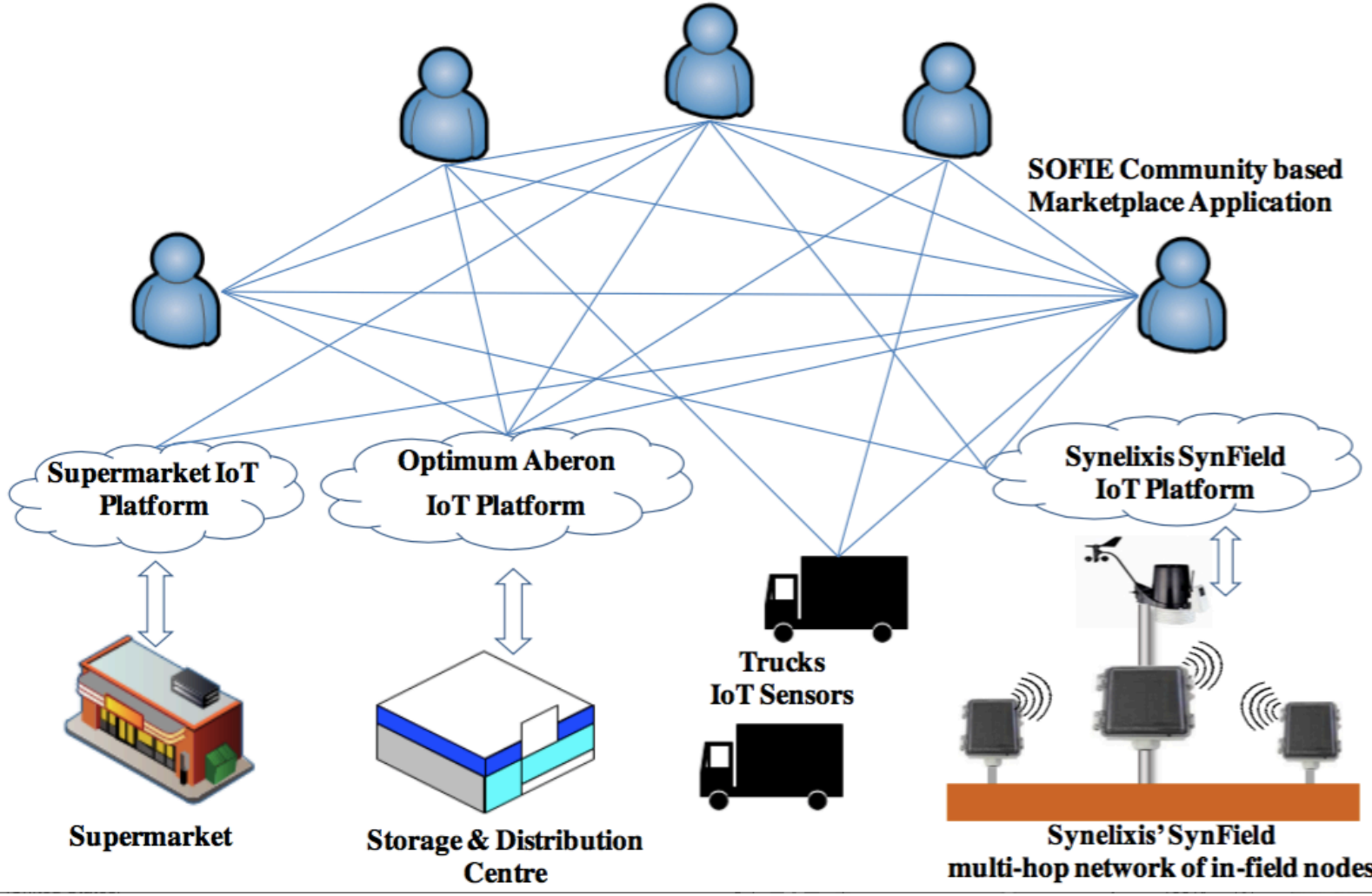


SOFIE's Energy II Pilot: Electricity Marketplace (Italy)





SOFIE's Food-Chain Pilot



SOFIE's Mixed-Reality Gaming Pilot

Gamers

Games

Blockchain-based marketplace for in-game assets

SOFIE Federated IoT Platform

Physical World

NFC

Shopping Mall

Warehouse

Park

IoT Platforms (movement sensors, passage control, lighting, etc.)

Conclusions

- Blockchains will be critical enablers for the IoT
  - they will enable
    - unattended operation – the heart of the IoT

  through
    - automatic contract enforcement
    - trust between devices with unplanned interactions
    - decentralized payments
- Major challenges remain
  - performance issues
  - real-world events not directly verifiable for 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?
    - …

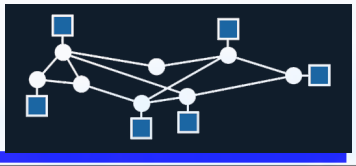
Thank you!

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

Workshop on Decentralized IoT Security



- **Network and Distributed System Security Symposium**
  - San Diego, CA, USA
  - February 18-21, 2018

  https://www.ndss-symposium.org/

- Workshop: **18/02/2018**
  - Abstract: **01/12/2017**
  - Paper: **08/12/2017**

http://www.ndss-symposium.org/ndss2018/cfp-ndss2018-diss/

- Organizers
  - Carsten Bormann, Universität Bremen
  - Dirk Kutscher, Huawei German Research Center
  - Michael McCool, Intel
  - Pekka Nikander, Aalto University
  - George C. Polyzos, AUEB
  - Thomas C. Schmidt, Hamburg U. of A.Sc.
  - Matthias Wählisch, Freie Universität Berlin

- **Enabling secure interoperability across IoT ecosystems**
  - Applying blockchains and Distributed Ledger Technology to IoT infrastructure
  - Security and availability in multi-tiered IoT edge networks (“fog computing”)
  - Peer-to-Peer security and privacy (P2P) in IoT
  - Decentralized trust and rights management, including access control
  - Decentralized authentication and access management at the IoT edge
- **Security and privacy in ongoing IoT standardisation work**
- **Other topics**
  - Security and privacy trade-offs related to IoT scalability and decentralization
  - Secure Service provisioning and migration in IoT
  - Sensor and Actuator Key Management and other Security Protocols
  - Smart Contracts for IoT, including formal verification of smart contracts
  - Usable security for decentralized IoT

Selected Publications

- Nikos Fotiou *et al*., "**ICN enabling CoAP Extensions for IP based IoT devices**," Proc. ACM ICN, Berlin, Germany, September 2017 (Best Demo Award).
- G.C. Polyzos & N. Fotiou, "**Blockchain-assisted Information Distribution for the Internet of Things**," Proc. Workshop on Information Integration in Cyber Physical Systems w/ IEEE International Conference on Information Reuse and Integration, San Diego, CA, USA, August 2017.
- N. Fotiou, *et al*., "**Edge-ICN and its application to the Internet of Things**," Proc. Workshop on Information-Centric Fog Computing w/ IFIP TC6 Networking Conference, Stockholm, Sweden, June 2017.
- N. Fotiou & G.C. Polyzos, "**Decentralized Name-based Security for Content Distribution using Blockchains**," Proc. IEEE INFOCOM Workshops, San Francisco, CA, USA, April 2016.
- G.C. Polyzos & N. Fotiou, "**Building a Reliable Internet of Things using Information-Centric Networking**," *Journal of Reliable Intelligent Environments*, Springer, vol. 1, no. 1, July 2015.
- N. Fotiou & G.C. Polyzos, "**Enabling NAME-based security and trust**," Proc. IFIP International Conference on Trust Management, Hamburg, Germany, May 2015.

Horizon 2020

INTER-IoT/ACHILLES: Access Control and autHenticatIon deLegation for interoperabLE IoT applicationS

interiot

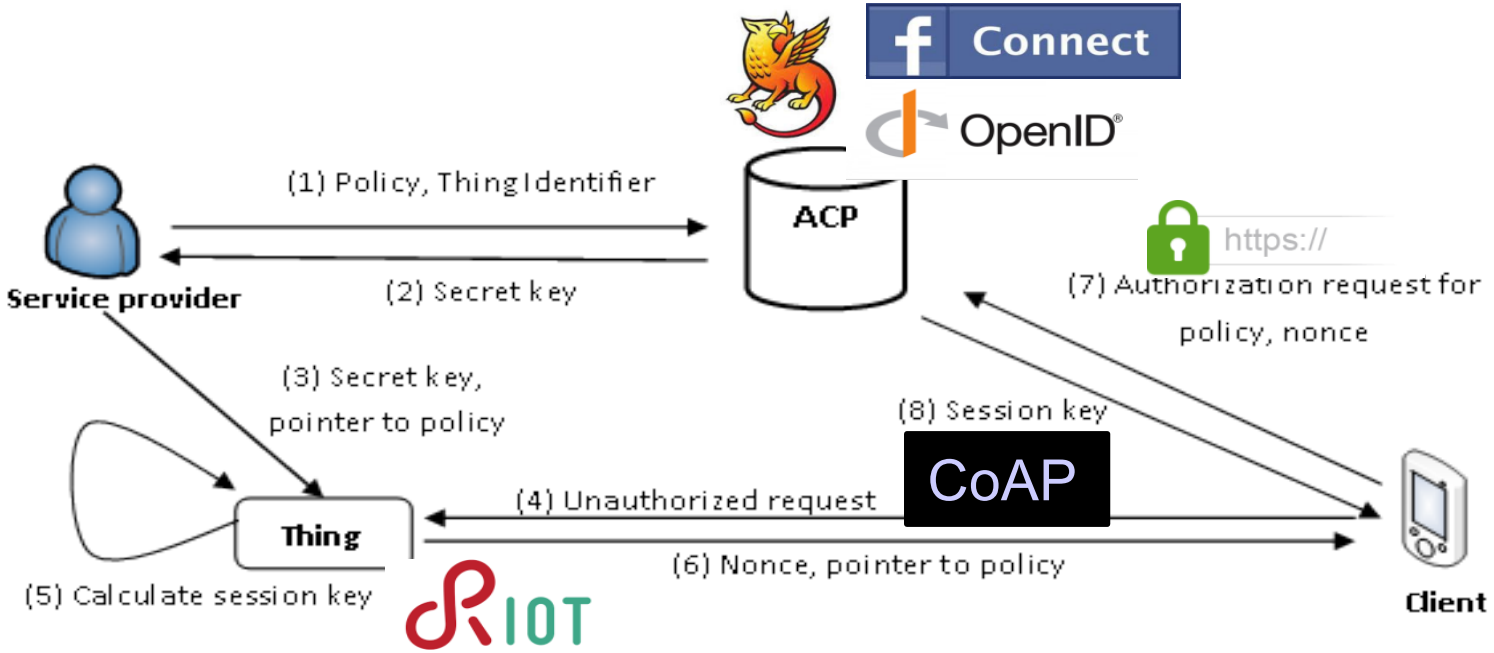
- Interoperability
- API
- Link-layer
- IoT Platforms

ACHILLES

- Access control
- Authentication
- Encryption
- Privacy

Key features

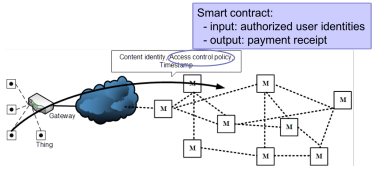
- ✓Lightweight
- ✓Business oriented
- ✓Integratable
- ✓Open source



Blockchains contribute to system sustainability

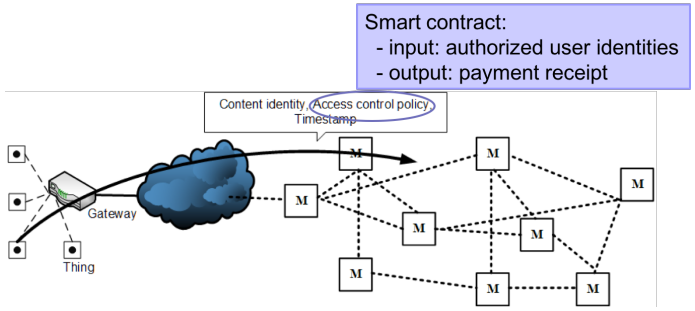
- resistant against cyber attacks, secure
- many critical operations of an IoT system can be delegated to or realized with blockchains
  - using smart contracts
- end-points can be “dumb”

- inter-ledger technology can provide long-term sustainability across DLTs



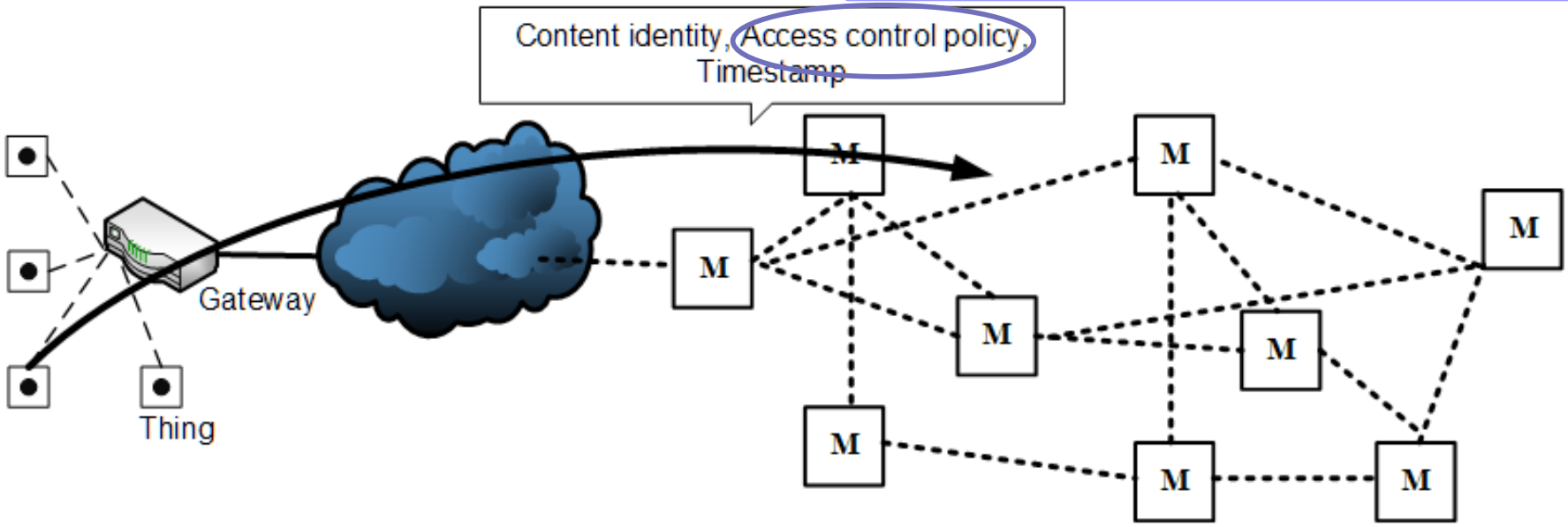
Blockchains enable new Trust Models

- Blockchains are built around transactions
- The mapping of blockchain's digital *coin* to the physical world is application specific:
  - Real money
  - Domain name
  - Actuation
  - Transfer of electricity
  - …

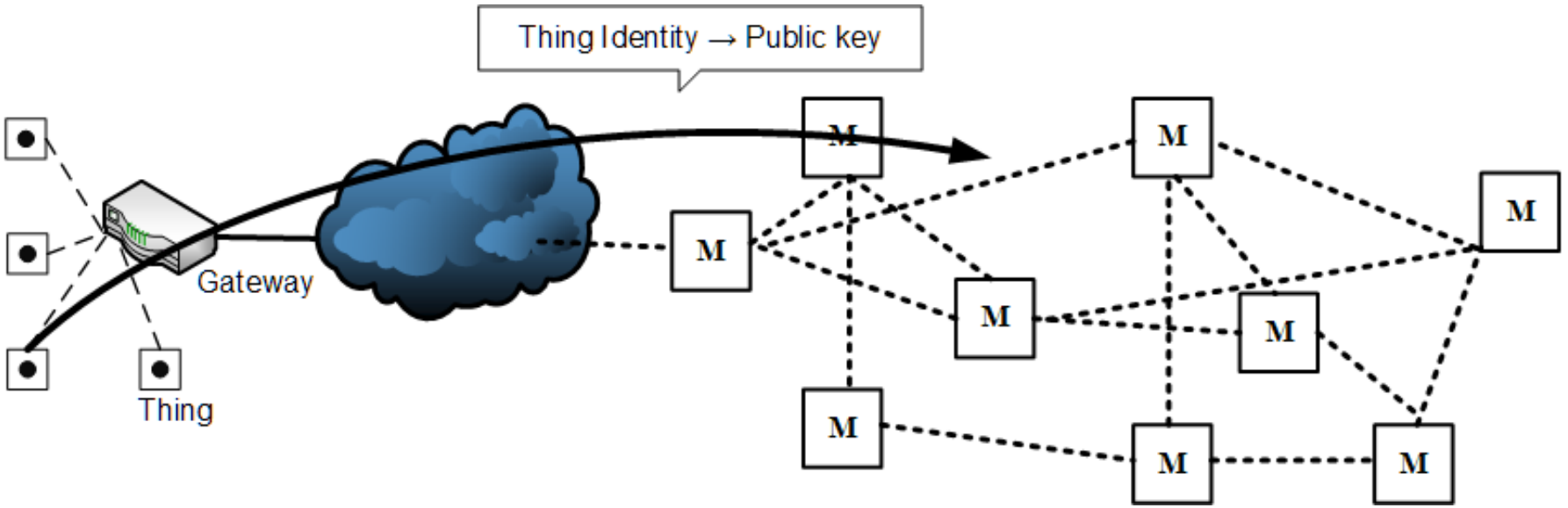


Provenance Verification & Information Tracking

Smart contract:
- input: authorized user identities
- output: payment receipt

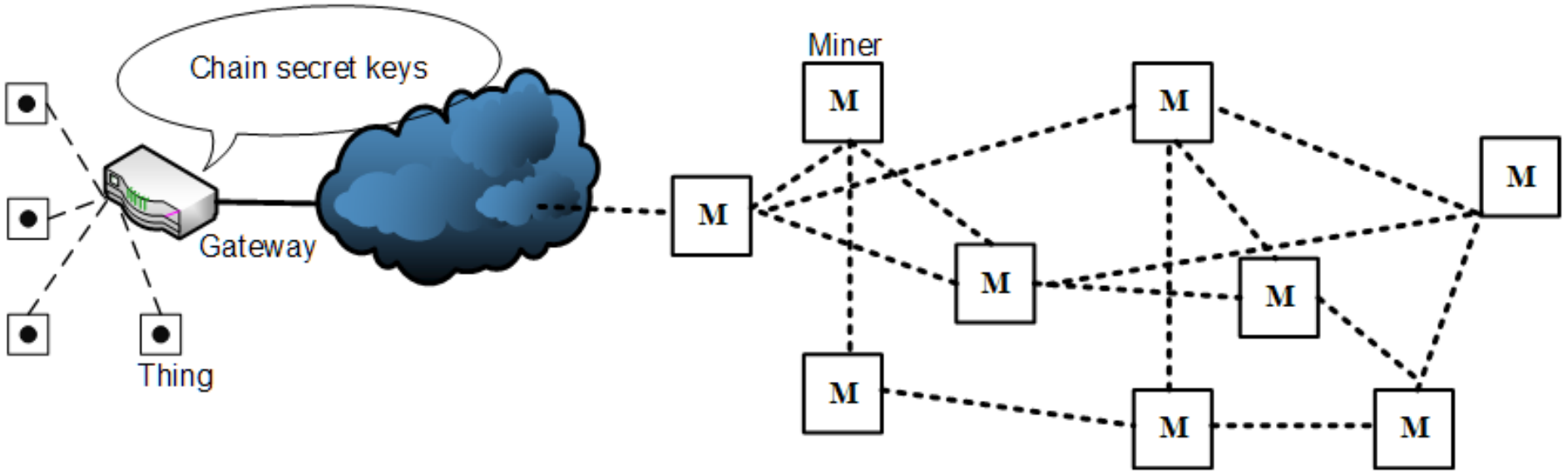


Identification and Trust Management



N. Fotiou and G.C. Polyzos, "**Decentralized name-based security for content distribution using blockchains**," Proc. IEEE INFOCOM Workshops, San Francisco, CA, April 2016.

Blockchain-assisted Information Distribution



- The getaway can sign information on behalf of the thing
  - and perhaps store it in the blockchain
- The corresponding public key can also be on the blockchain