SOFIE, Distributed Ledgers, and Decentralized Identifiers

Dmitrij Lagutin, dmitrij.lagutin@aalto.fi

Aalto University

COMNET Workshop, Espoo, Finland, 13.2.2020

SOFIE: Background

- Fragmentation is a major issue in IoT
  - Most of IoT systems are closed silos => difficult to exchange data, actions, etc. across IoT systems
  - Leads to high barriers of entry and reduces competition, worse privacy, etc.
- SOFIE provides secure open federation for existing (open and closed) IoT platforms through Distributed Ledger Technologies (DLTs)
  - Without requiring any changes to the existing IoT systems
  - Enables open business platforms and eventually open data markets

Distributed Ledger Technologies (DLTs)

- The main property of DLTs is immutability of data (once inserted, data can’t be changed afterwards)
  - DLTs enable distributed trust between entities that do not fully trust each other
  - Smart Contracts enable high degree of automation
- There exist different types of DLTs: open, semi-open, closed, etc.
  - In a real-life system, most of DLTs will be closed or semi-open, fully open DLT (such as public Ethereum or Bitcoin) is too expensive for most purposes
- Different DLTs have very different properties (throughput, latency, consensus model, etc.); therefore SOFIE utilizes multiple DLTs in parallel
  - Also necessary for privacy (data is not readable by everyone) and crypto agility (data can be moved to a new ledger)
  - Developing and applying technologies for *interledger* is one the main technical innovations of SOFIE

SOFIE Pilots

- Decentralized Energy Flexibility Marketplace (Italy)
  - Load balancing of the electricity grid through charging of electrical vehicles (EVs)
  - Grid operator and EVs participate in the Ethereum-based decentralized marketplace to offer and bid on flexibility requests
- Decentralized Energy Data Exchange (Estonia)
  - Exchanging customers' smart meter data in a secure, privacy-preserving, and GDPR-compliant manner
- Food Supply Chain (Greece)
  - Accurate data about growth and transportation conditions available to customers
  - Interactions between producers, distributors, retailers, and customers stored in DLT
- Mixed Reality Mobile Gaming (Finland)
  - Using DLT to store and trade in-game assets (enforcing scarcity, item ownership, etc.)
  - Interaction between the mobile game and real-world IoT devices (e.g. beacons, etc.)

Applications of Interledger

- Utilizing multiple DLTs gives several advantages, use cases include:
- Achieving lower costs by mostly using private ledgers:
  - Cheaper
  - Lower energy use
  - Lower latency and higher throughput
- Using more secure ledger as a trust anchor:
  - Storing data in private ledger, with the hash of data stored in public ledger
  - If necessary, data will be revealed and the publicly available hash guarantees that data has not been tampered with
- Better privacy
  - Personal data (e.g. data related to personal IoT devices) should not be stored to immutable ledger (right to be forgotten)

Applications of Interledger

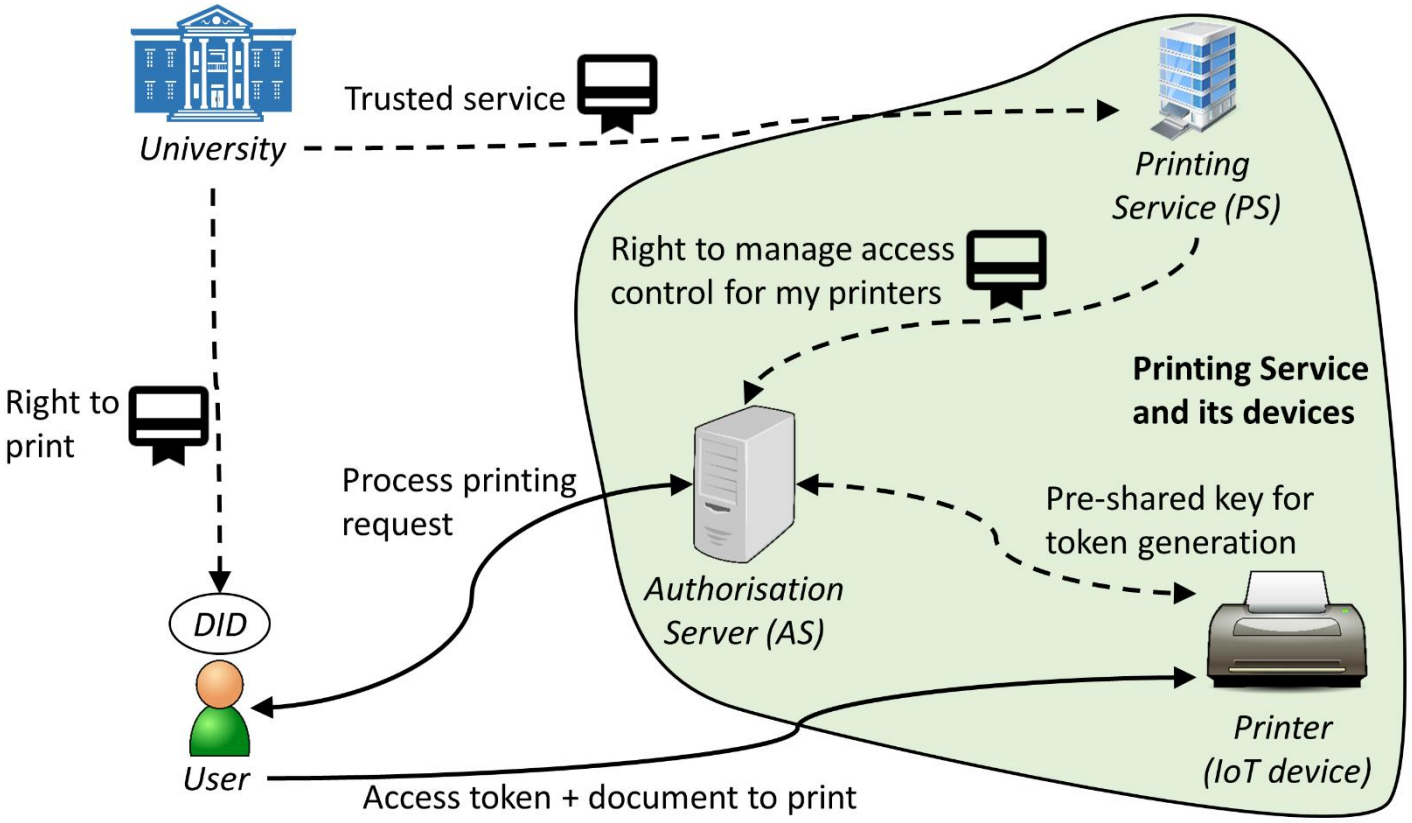
- Atomic operations:
  - E.g., providing access token for the service after the payment has been made in a secure manner
  - Transferring assets/state between ledgers
  - Can be implemented using Hash Time Locked Contracts (HTLC)
- Triggering transactions in ledger *X* based on activity in ledger *Y*
- Crypto-agility: in long term it is necessary to be able to move data to new, more secure, ledger

Decentralized Identifiers (DIDs)

- Current identifier solutions have multiple problems:
  - Different identifier for each service, lack of interoperability
  - Lack of privacy in case of social logins
  - Very complicated to provide privacy-preserving proofs online
- Decentralised Identifiers (DIDs) aim to provide *self-sovereignty*
  - Can be created by the user without dependence on any third party, hence a large number of DIDs can be used (even different one for each transaction)
  - Often derived from public/private key pair
- With verifiable credentials (VCs), owner of identifier can prove something (e.g. date of birth, degree) about themselves
  - Selective disclosure: disclose only part of the information present in credential
  - Zero-knowledge Proofs (ZKP) allow one to prove of, e.g., being over certain age without revealing their real age listed in credential. ZKPs are not supported by all solutions.

Decentralized Identifiers (DIDs) with IoT

- Example: DIDs with OAuth2
  - Better privacy, flexibility, etc.
- Visiting lecturer wants to use printer without university's user account
- Printer is a constrained device supporting OAuth2
- Printing service can not correlate lecturer's activities
- University can not see which printer lecturer is using



Decentralized Identifiers and Ledgers

- Notable DID solutions include: Sovrin (Hyperledger Indy), uPort, Veres One
- Many DIDs were supposed to be stored in DLTs
  - Problems with: performance, cost, privacy, GDPR, etc.
  - Current practice: only DIDs of public entities should be stored in ledgers
  - DIDs are clearly useful even without ledgers
  - Research question: how useful are the ledgers for storing DIDs and related information compared to alternatives?

Questions / Comments?

References

- Vasilios Siris, Pekka Nikander, Spyros Voulgaris, Nikos Fotiou, Dmitrij Lagutin, and George Polyzos. Interledger Approaches. IEEE Access, July 2019. https://doi.org/10.1109/ACCESS.2019.2926880.
- Yki Kortesniemi, Dmitrij Lagutin, Tommi Elo, and Nikos Fotiou. Improving the Privacy of Internet of Things with Decentralised Identifiers (DIDs). Journal of Computer Networks and Communications. 2019. https://doi.org/10.1155/2019/8706760.
- Dmitrij Lagutin, Yki Kortesniemi, Nikos Fotiou, and Vasilios Siris. Enabling Decentralised Identifiers and Verifiable Credentials for Constrained IoT Devices using OAuth-based Delegation. In Proceedings of Workshop on “Decentralized IoT Security and Standards” (DISS) in conjunction with the 26th “Network and Distributed System Security Symposium” (NDSS 2019). San Diego, USA, 2019. https://dx.doi.org/10.14722/diss.2019.23005.
- SOFIE Website (with much more publications): https://www.sofie-iot.eu
- SOFIE Github: https://github.com/SOFIE-project