IOTWeek

3rd IEEE Global IoT Summit
June 17-21 2019 Aarhus (Denmark)

Blockchain Applications to Industrial IoT

Privacy-preserving solutions for Blockchain

Antonio Skarmeta

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 779852

Department of Communications and Information Engineering

University of Murcia (Spain)

Index

- Blockchain
- Identity Mixer
- Hyperledger Fabric
- IoT Scenarios
- On-going work
- Conclusions

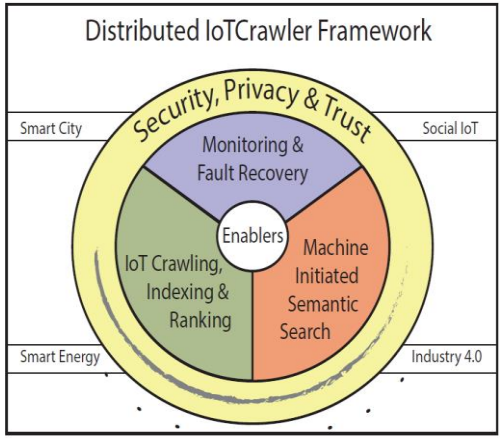
IoTCrawler Partners

IOTWeek

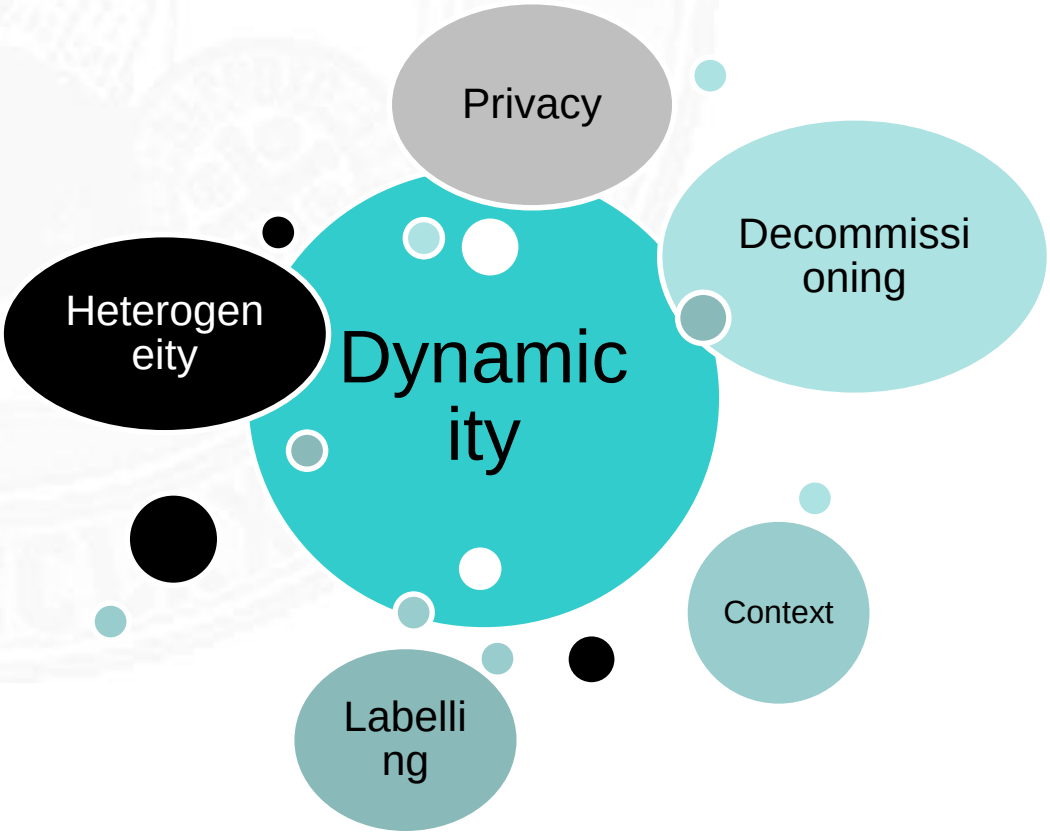
Participant No	Participant organisation name	Short name	Country
1	Universidad de Murcia	UMU	Spain
2	University of Surrey	UniS	United Kingdom
3	University of Applied Sciences Osnabrück	UASO	Germany
4	Aarhus University	AU	Denmark
5	Siemens AG Österreich	SIEMENS	Austria
6	NEC Corporation	NEC	Germany
7	AGT Group (R&D) GmbH	AGT	Germany
8	digital worx	DW	Germany
9	Odin Solutions S.L.	OdinS	Spain
10	City of Aarhus	AAR	Denmark

Vision

- To develop the next generation of Internet search engines that support crawling, discovery, search and integration of IoT data.
- To provide tools and mechanisms to respond to machine initiated search, offer adaptive and dynamic solutions for resource ranking and selection,
- To develop distributed crawling and indexing mechanisms to enable real-time (or near real-time) discovery and search of massive real world (IoT) data streams in a secure and privacy- and trust-aware framework.
- To integrate the security and privacy properties of smart object within the registry and lookup procedure
- To change the way that the data (especially new forms such as IoT data) can be published, discovered and accessed in large-scale distributed networks.
- Providing enablers for security-, privacy and trust-aware discovery and access to IoT resources in constrained IoT environments
- To pave the way for creating new applications and services that rely on ad-hoc and dynamic data/service query and access.



Challenges for the security IoT lifecycle management



IoTCrawler and IoT Data

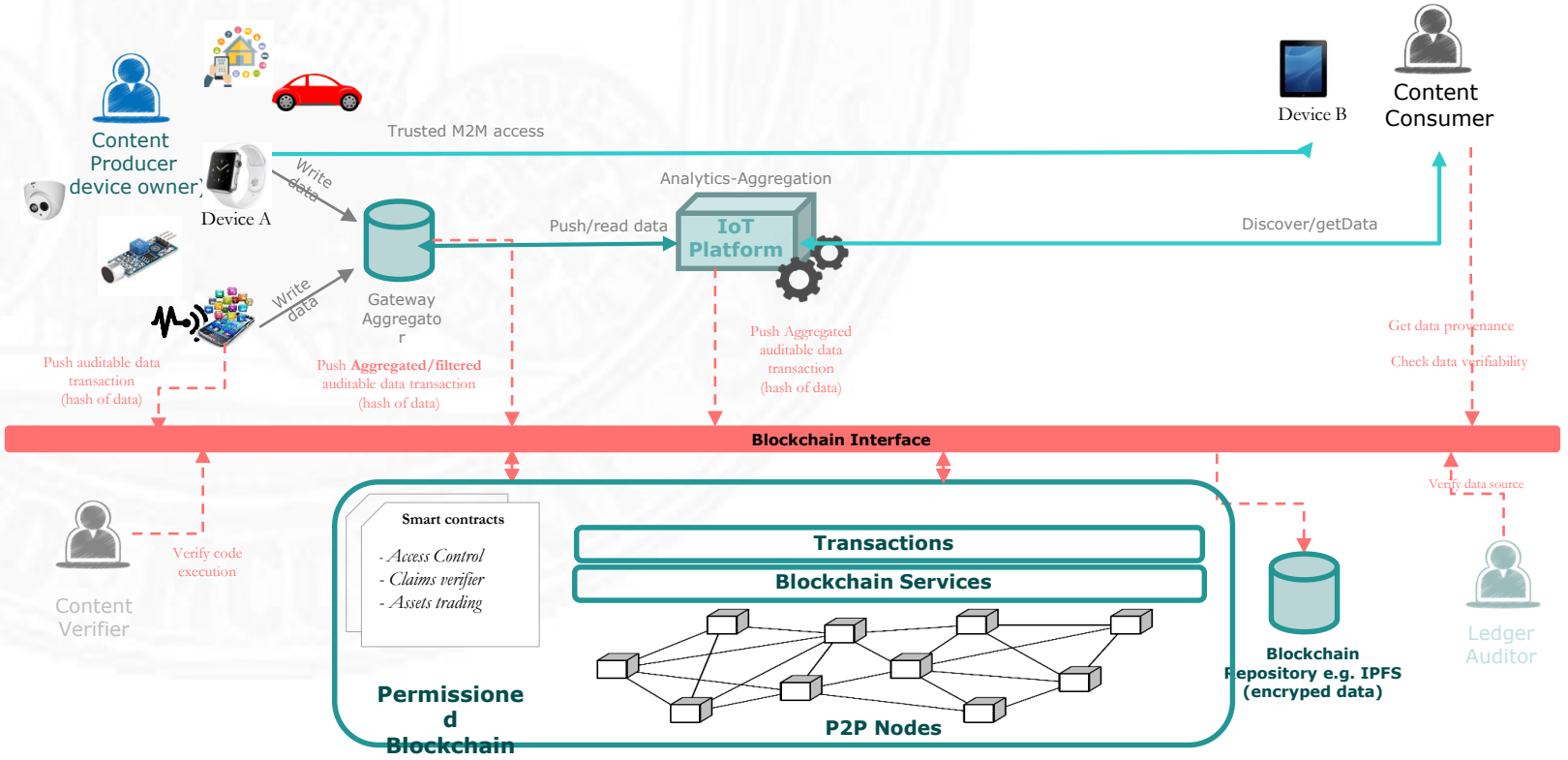
- It is important to control particularly **sensitive information** is foreseen to be provided for IoT end-devices
- To be able to control who Access to the data but also if I am interested to be discover and by whom
- To decide how I can disclosure my data
- Trust with central entity/data repositories must be properly managed
- Authorizations decisions need to be based on contextual information
- More distributed access control and accesible to constrained devices
- Provide a trust on the origin of data, confidence on the processing by others and in general on a quite distributed architecture

- **Security and privacy** as the main barriers for a broad scale IoT deployment

Operational challenges in Security

- **Standard** security and access control mechanisms are used over the Internet today
  - These proposals often based on heavy primitives, difficult application on resource-constrained devices
  - Unlike current Internet, smart objects are working in harsh and uncontrolled environments, prone to attacks and misuse and being controlled by non-expert users
  - Control on information sharing in IoT requires advanced privacy-preserving IdM techniques
- Requirements from **Management**
  - Scenarios with millions of heterogeneous devices can not be managed by centralized and out-of-band approaches → self-management techniques should be supported
  - It includes the application of scalable mechanisms for bootstrapping, configuration, upgrading and key management

IoT/Identity and data provenance in Blockchain



Blockchain

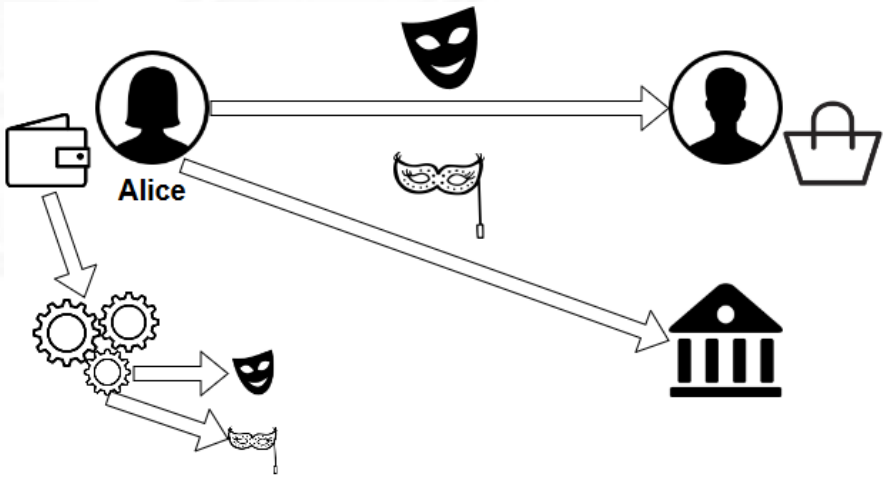
- Blockchain for Identity Management (IdM).
- Enhancing privacy features.
- Enabling a decentralized identity management by:
  - Removing legacy login methods.
  - Removing central entities that holds too much power in our organizations.
  - Storing personal data/identifiers in the blockchain.
- Protecting the identity infrastructure.

Identity Mixer - Idemix

- It’s a privacy preserving crypto-protocol-suite.
  - Strong authentication.
    - Idemix allows proving of attributes without revealing directly.
    - Certified attributes.
  - Anonymity.
    - Unless user disclosing, real identity remains hidden.
  - Unlinkability.
    - Multiple public identities.

Identity Mixer - Idemix

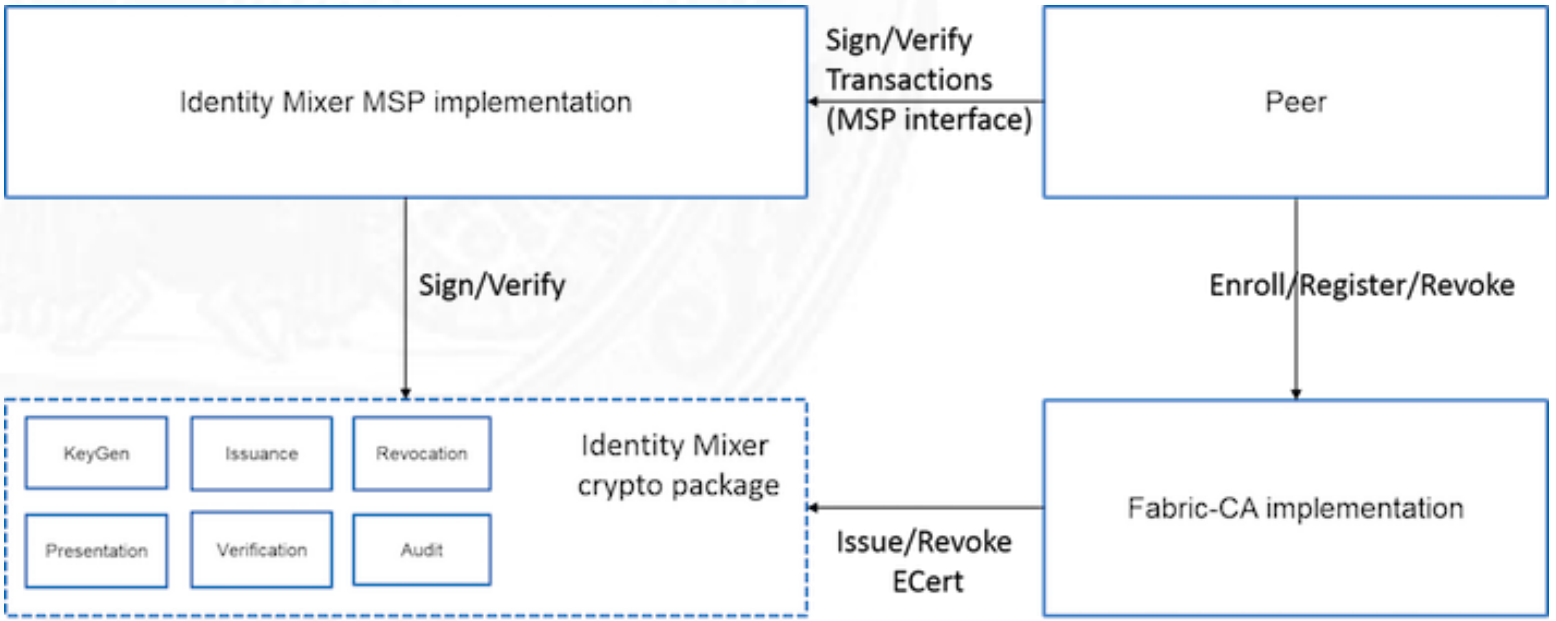
- Idemix vs attribute-credential systems.
  - Each user has a single private key buy can have multiple public keys.
  - The private key is the user secret identity.
  - Users can derive, from the secret, as many public identities as they wish.
    - i.e. Alice can use an identity for buying goods in an online shop and another, for paying her taxes. Both belong to Alice but without leaving any trace.



Hyperledger + Identity Mixer

- Introducing Identity Mixer in Hyperledger Membership Service Providers (MSP).
- Provide protection to users when:
  - Signing.
  - Authentication.
  - Attribute transfer.
- Trust model like X509 but with advanced privacy features such us unlinkability and minimal attribute disclosure.

Hyperledger + Identity Mixer



IoT Scenarios - Challenges

- Technology
  - Security.
  - Scalability.
  - Privacy.
  - Resilience.
- Operational challenges
  - Business model.
  - Data definition.
- Legal and compliance issues
  - Final responsibility.
  - Jurisdiction to apply.

IoT Scenarios

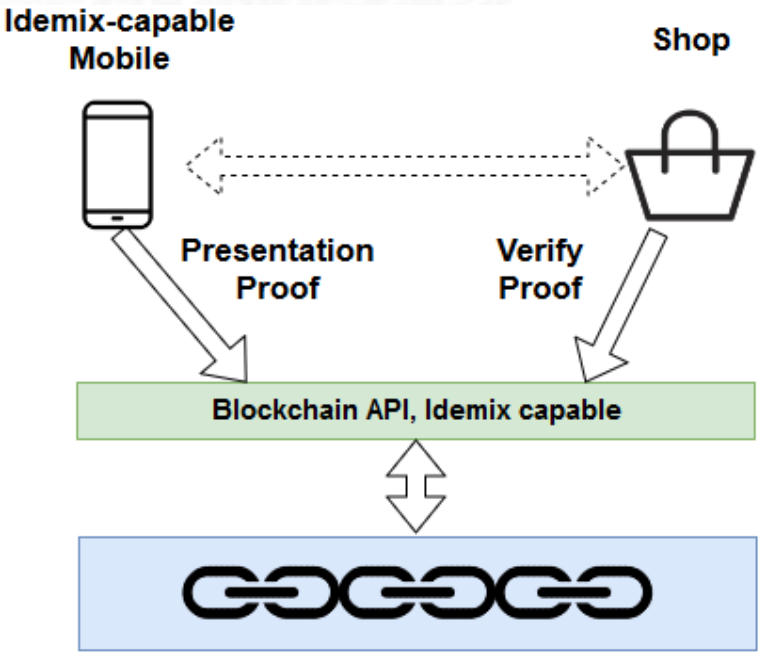
- Combination between IoT and blockchain is currently a reality.
  - IBM Integrate Watson IoT Platform with Blockchain.
  - Microsoft Azure, IoT and blockchain.
  - Atonomi.
  - Chain of things.
  - And more…
- Adding Blockchain to an IoT peer-to-peer network provides a contractual behavior without any third party to “certify” transactions.
- Also adding ZKP provide privacy empowerment

On-going work

- Interaction between mobile devices (i.e. Smartphones) and blockchain networks.
- The interaction must be privacy-preserving.
- Integration of the Identity Mixer API in mobile devices.
- Deploy Membership Service Providers (MSP) based on Identity Mixer.

On-going work

- By enabling the previous interaction:
  - The IoT device will be able to act as Idemix prover.
  - The IoT device will be able to perform proof presentations against the blockchain.



Conclusions

- Blockchain is a disrupting technology that can be applied in many scenarios.
- Privacy by-design is a desired feature.
- Combining blockchain with privacy-preserving protocols is feasible and is being carried out.
- Combining IoT scenarios with blockchain is possible and should follow privacy-preserving principles for a good adoption.

IOTWeek

3rd IEEE Global IoT Summit
June 17-21 2019 Aarhus (Denmark)

Blockchain Applications to Industrial IoT

Privacy-preserving solutions for Blockchain

Antonio Skarmeta

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 779852

Department of Communications and Information Engineering

University of Murcia (Spain)