UNIVERSITY of NICOSIA

Session 10

Self-sovereign Identities and Data Markets

BLOC 514: Emerging Topics in Blockchain and Digital Currency

Session Objectives

- Provide an overview of the online identity models
- Present the principles of self-sovereign identities
- Introduce data markets
- Compare centralized vs. decentralized architectures of data markets

The key idea that underlies self-sovereign identities is to enable users to have full control over their digital identities. In this session, we will discuss how the decentralized architectures (including blockchains) can be utilized towards the self-sovereign paradigm.

Agenda

- Self-sovereign identity: introduction
- Principles of online and self-sovereign identity
- Self-sovereign identity: use cases
- Digital identities on metaverse(s)
- Data markets: introduction
- Data markets: centralized vs. decentralized design
- Conclusions
- Resources

Self-sovereign Identities

Introduction

- Self-sovereign identity: users should have full control over their identity and respective data
- This is not the case for today's internet

"The Internet was created without an identity layer"

- Kim Cameron, Chief Architect of Identity for Microsoft

  - Primary design aspect of Internet's addressing system: identification of physical endpoints, i.e., machines
  - People not considered as endpoints
- Management of digital identities is done at ad-hoc basis
  - Websites, applications
  - Popular scheme: <username, password> pair
- As a result:
  - Centralization of credentials
  - Lack of portability

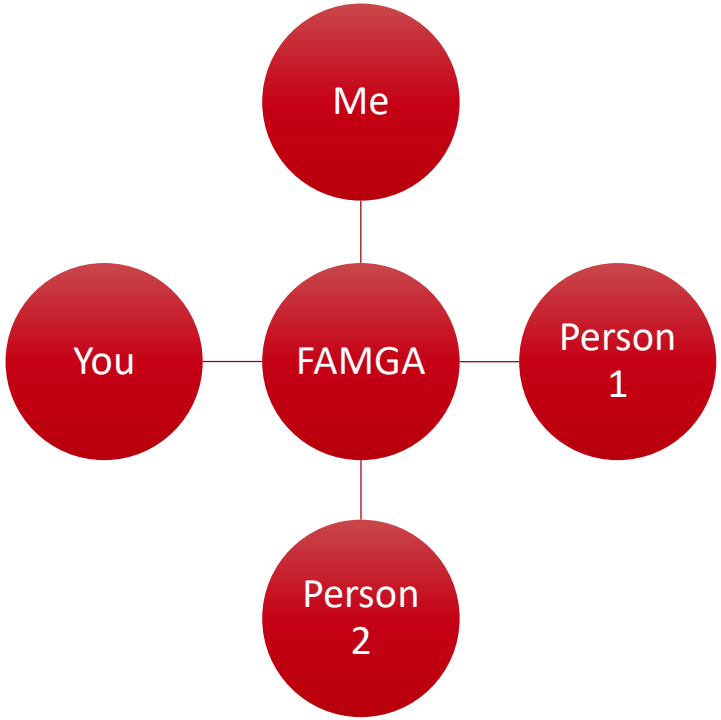
Impact

- The lack of a true digital identity layer in the online ecosystem has a significant impact
- Examples:
  - Cost of identity assurance in the UK: > £3.3 Bn
  - Average retailer cost of stolen data related to digital identities: $165
  - 30-40% of call centers traffic deal with account recoveries
  - In the USA, every 60 secs 25 cases of identity theft occur
  - Issues related to <username, password> prevent 18% of online shoppers from completing their purchases
  - 82% of business face fake digital identities
- Currently: silos of digital identities
- Bad user experience – Assume a user
  - Different digital identities scattered across different services/applications
  - Reduced ability to control his/her identity holistically

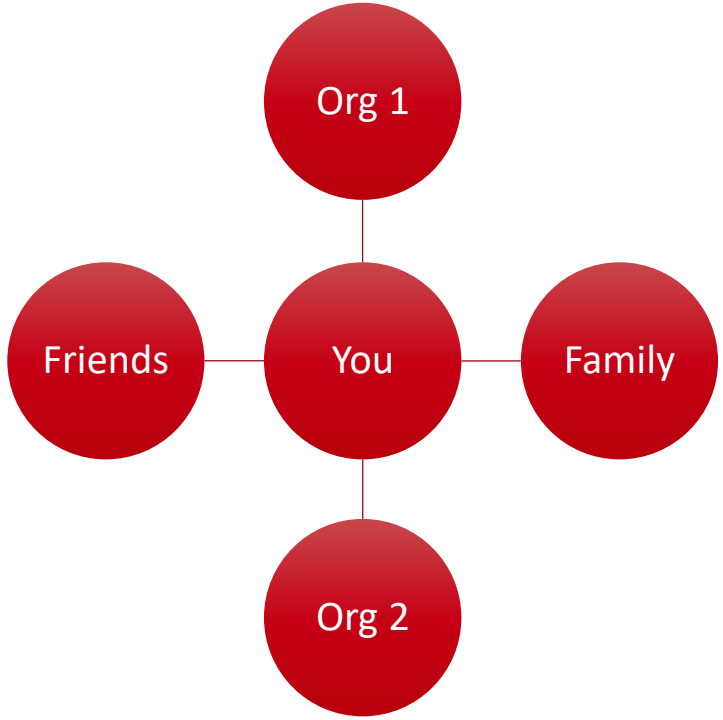
Source: "The Inevitable Rise of Self-Sovereign Identity", A white paper from the Sovrin Foundation

Online identity models

Typical centralized model



Self-sovereign identity model: decentralized



Fundamental properties of online identity

- Security
  - The identity-related data must be efficiently protected making the disclosure of them non feasible
    - Disclosure: unintentional, intentional
- Individual control
  - The owner (i.e., the person who is being identified through the data) must fully control who access and why
    - "Who": physical/legal entities as well as software services
    - "Access": different types of access rights, e.g., partial/full, view-only/edit, etc.
    - "Why": internal vs. external usage, types of processing
- Portability
  - The identify data must be portable
    - Use across different websites
    - Provider-agnostic

The evolution of online identity

Proposed by Christopher Allen

- Centralized: An identity is owned and controlled by a single entity
- Federated: Introduces a weak degree of decentralization
  - Credentials from service A are used in service B
  - Used in large corporations
- User-centric: The user controls the data as well as the release of the data to third parties
  - However, the user needs to select an identity provider
- Self-sovereign: Ensures all 3 fundamental properties (control, security, portability)
  - DLT constitute the technological cornerstone towards this vision

The 10 principles of self-sovereign identity

Security	Control	Portability
Protection	Existence	Interoperability
Persistence	Persistence	Transparency
Minimalizasation	Control	Access
	Consent	

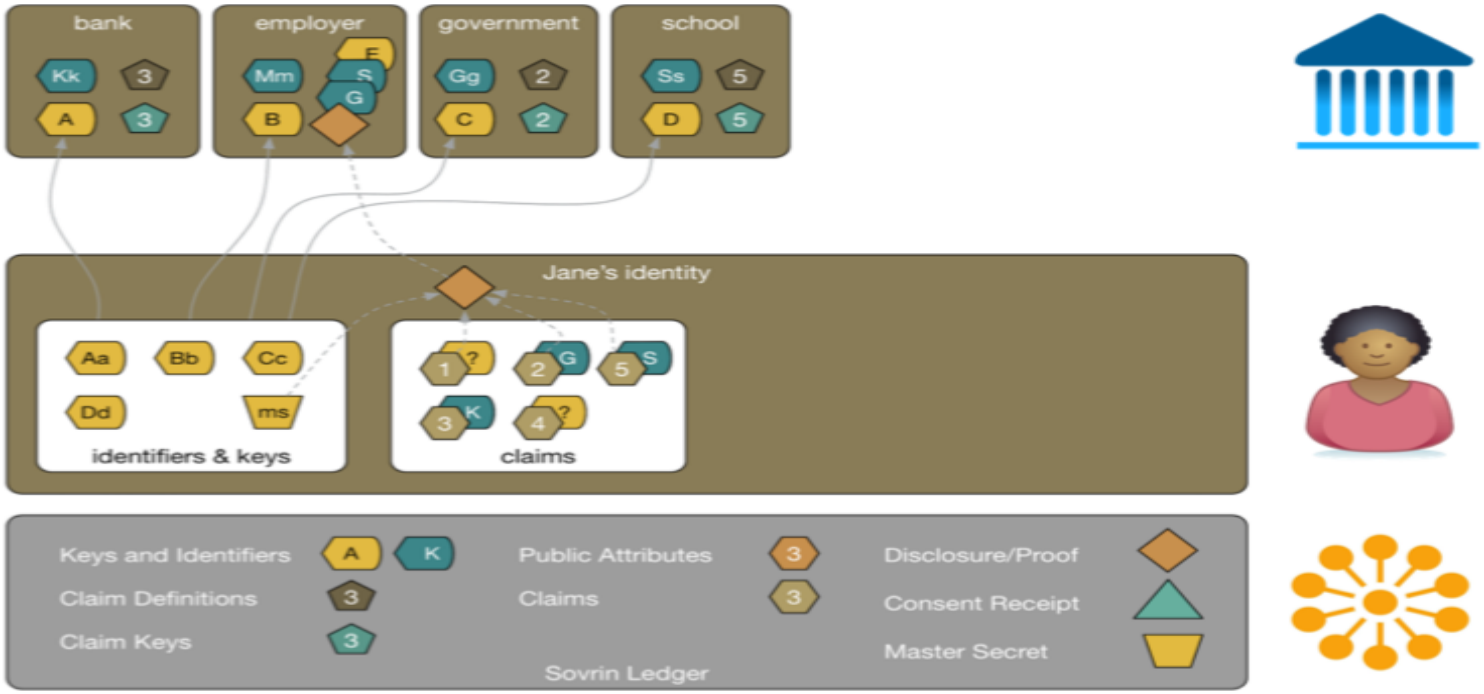
- Protection: Users' rights must be preserved
- Persistence: Digital identities should last for a long period of time
- Minimalization: Minimize the amount of disclosed data as much as possible
- Existence: A digital identity must correspond to an independent existence
- Control: Users must have the full control of their identities
- Consent: Users must provide their consent regarding the use of identities
- Interoperability: Identities must exhibit wide usability
- Transparency: The functionality of involved systems/algorithms should be open
- Portability: Digital identities must be transportable
- Access: Easy access to identity-related data

Sovrin

- Sovrin (https://sovrin.org): open-source identity network being public and permissioned
  - Public: Everyone can use the network
  - Permissioned: The consensus of transactions is governed by a subset of nodes
    - Those nodes are selected by the Sovrin Foundation (non-profit organization)
- Main concepts
  - Identifiers: cryptonyms encoded encoded as Ed25519 digital signature
    - Each identifier is also associated with a Ed25519-encoded verification key
    - A user can share his/her verification
  - Claims: Verifiable assertions or attestations; Two types of claims:
    - Made by the user
    - Made by others
  - Disclosures: A mechanism that enables the (re-)use of claims according to the needs of the particular use case
    - Multiple claims can be combined
    - Meant the serve the minimalization principle

Sovrin

- Assume that the user is sending an application the a candidate employer along with his/her verification key. The user can combine claims from government and school as well as self-asserted claims. Note that the user can select which attributes to share, e.g., address, grades, and age.



Digital Identities on Metaverse(s)

Digital identities and metaverse(s)

Question for discussion:

(First of all)

Metaverse

or

Metaverses

Digital identities and metaverse(s)

(Extended) question for discussion:

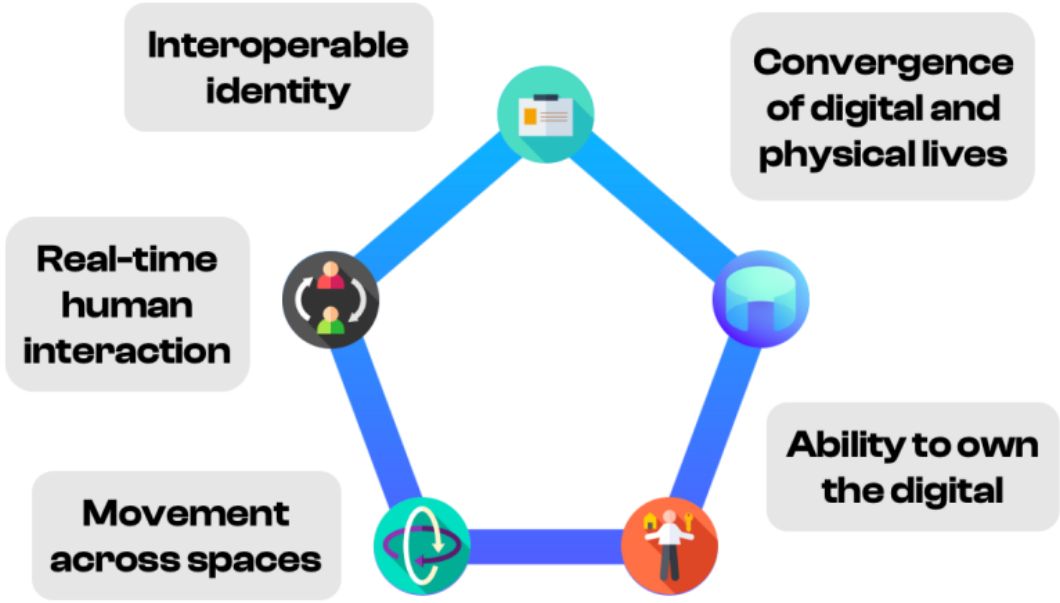
If metaverses,

then

what's the role of interoperability?

(also consider previous session)

Metaverse pentagon



Source https://www.web3-studios.com/research ("Digital Identities - Who will we be in the Metaverse?" Market Report)

From physical to metaverse identities

Physical Identity

Where you **live**
Where you **went to school**
How you **physically look**

Online Identity

What you **searched**
What you **bought**
What you **say online**

Metaverse Identity

What you **like to share**
(in an ideal state)

Source https://www.web3-studios.com/research ("Digital Identities - Who will we be in the Metaverse?" Market Report)

Punk6529 on digital identities

"It's fairly clear that in an increasingly digital world people will switch between digital identities - you are not going to always have to use the same persona across different applications and in various use cases over the next 50 years."

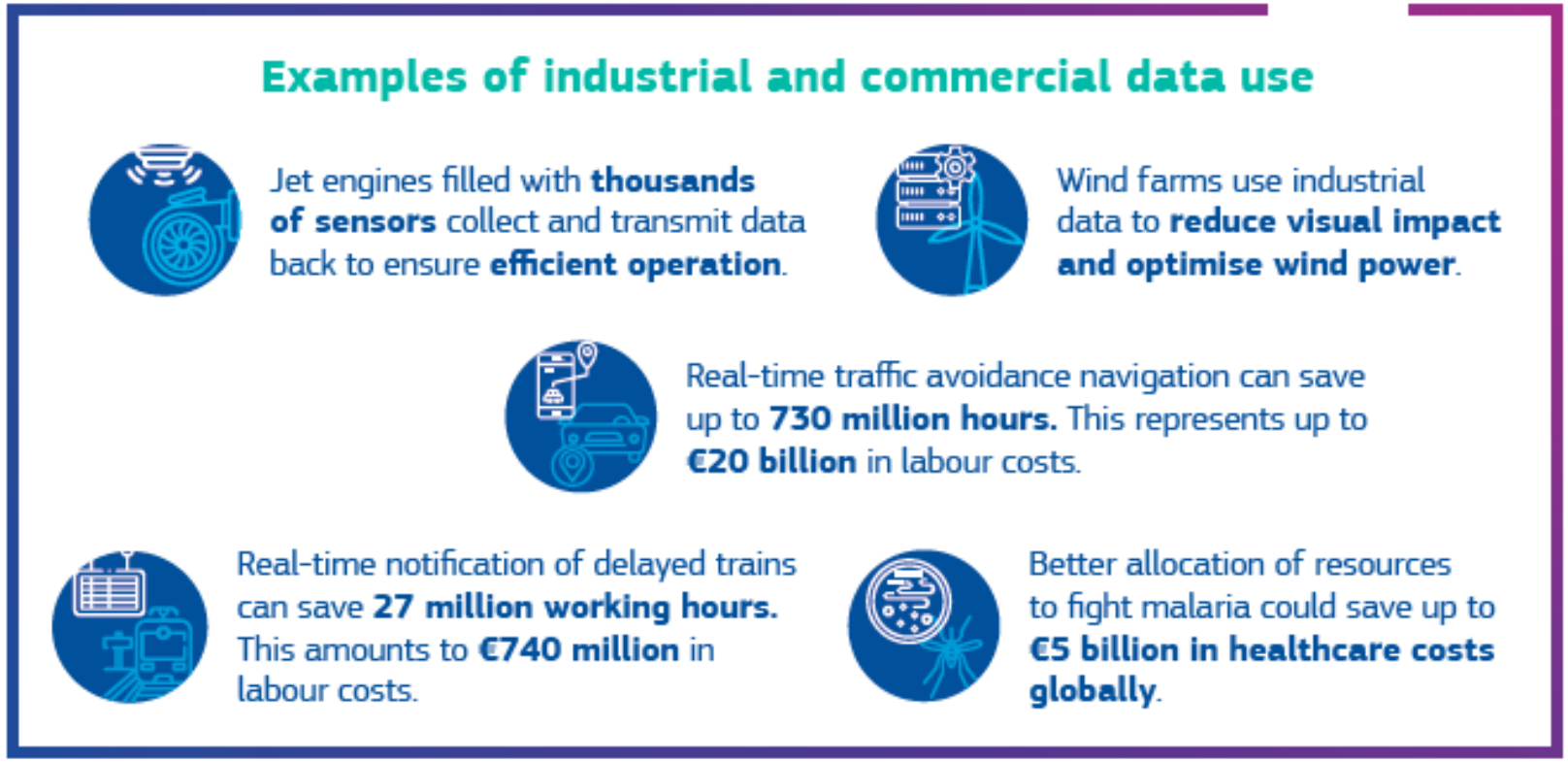
Data markets

Data markets: introduction

- Data markets: multi-party platforms
- Main actors: data creators/providers and purchasers
  - Connected via intermediaries
  - Examples of intermediaries: Microsoft Azure Marketplace, Amazon Data Marketplace
- The European data economy at a glance
  - Overall value of the EU data economy in 2019: 325 billion Euros
    - 2.6% of the European GDP
  - Overall value of the EU data economy by 2025: 550+ billion Euros
    - 4% of the European GDP

Source: "Building a data economy" European Commission

Data markets: introduction



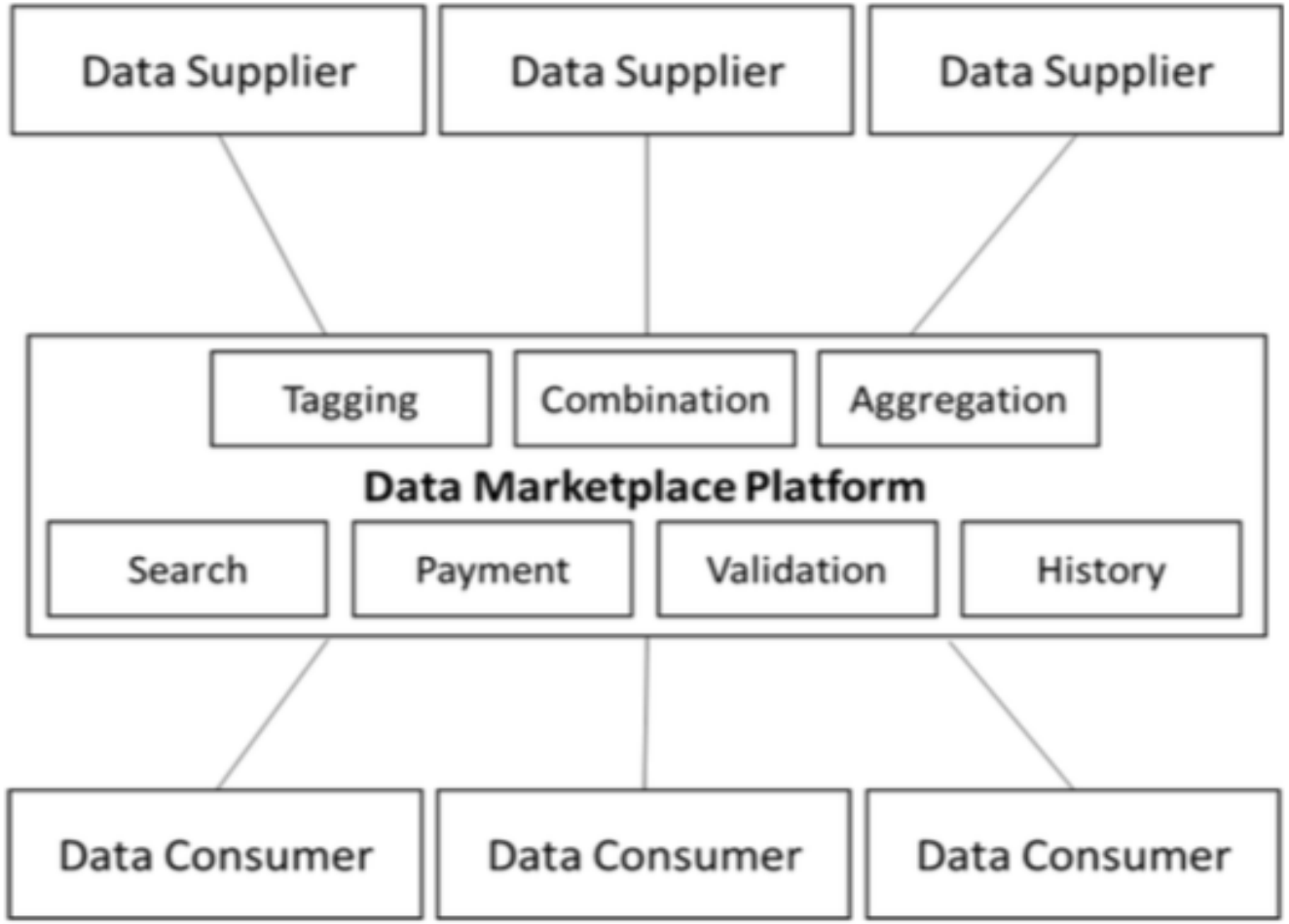
Source: "Building a data economy" European Commission

Furthermore: European Strategy for data

Data markets: centralized vs. decentralized

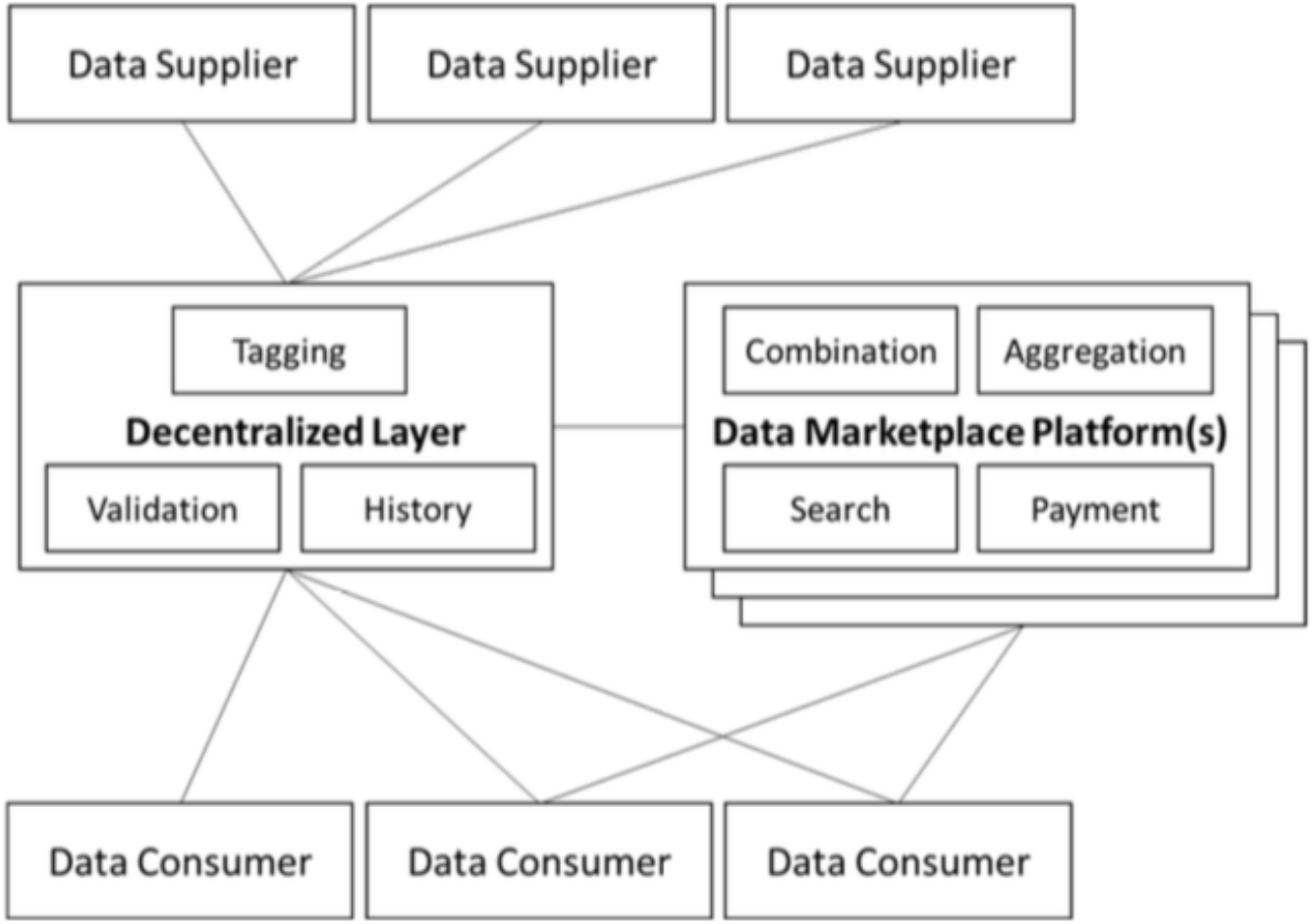
- Various participants
  - E.g., data creators, managers, analysts, service providers, aggregators
- Centralized
  - Services: search, retrieval, transaction validation and history, payments
  - Clear benefits for big suppliers of data compared to smaller suppliers
  - Cost of maintenance
- Decentralized
  - Commonalities with centralized data markets
  - Direct trades
  - Some operations are conducted in decentralized mode
    - Tagging
    - Validation
    - History

Data markets: centralized design



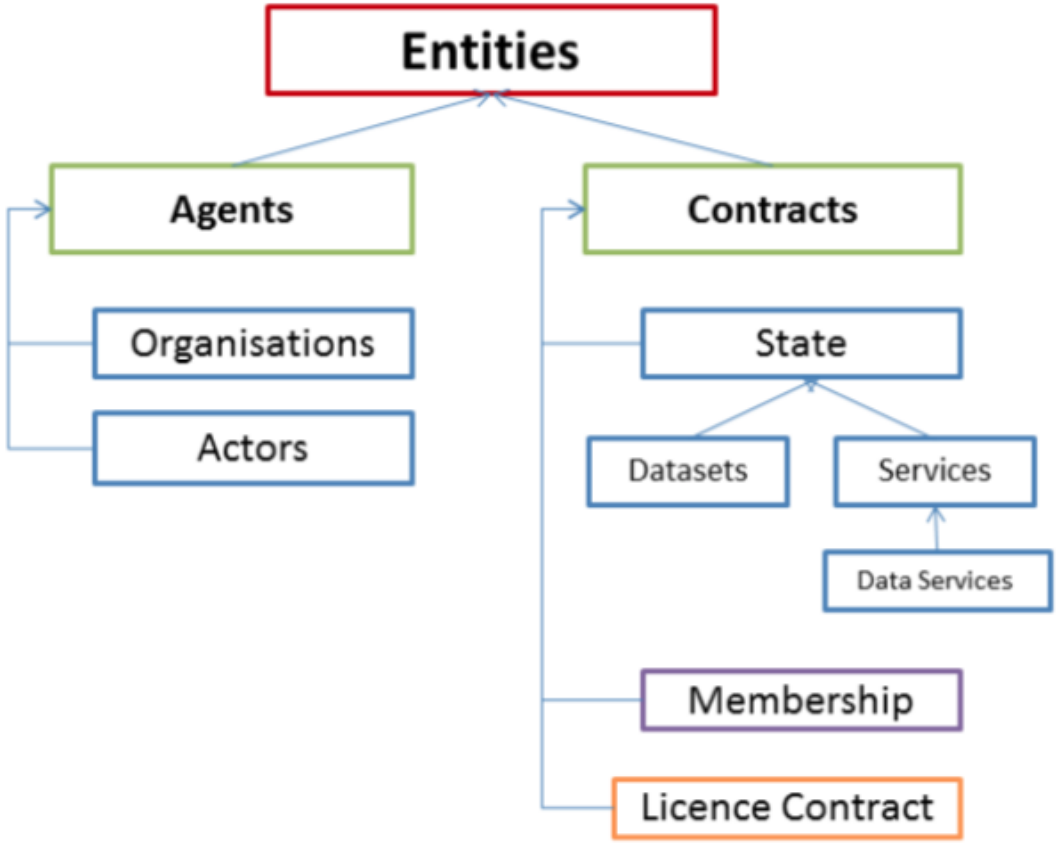
Source: Koutroumpis et al. (2017), "The (Unfulfilled) Potential of Data Marketplaces"

Data markets: decentralized design



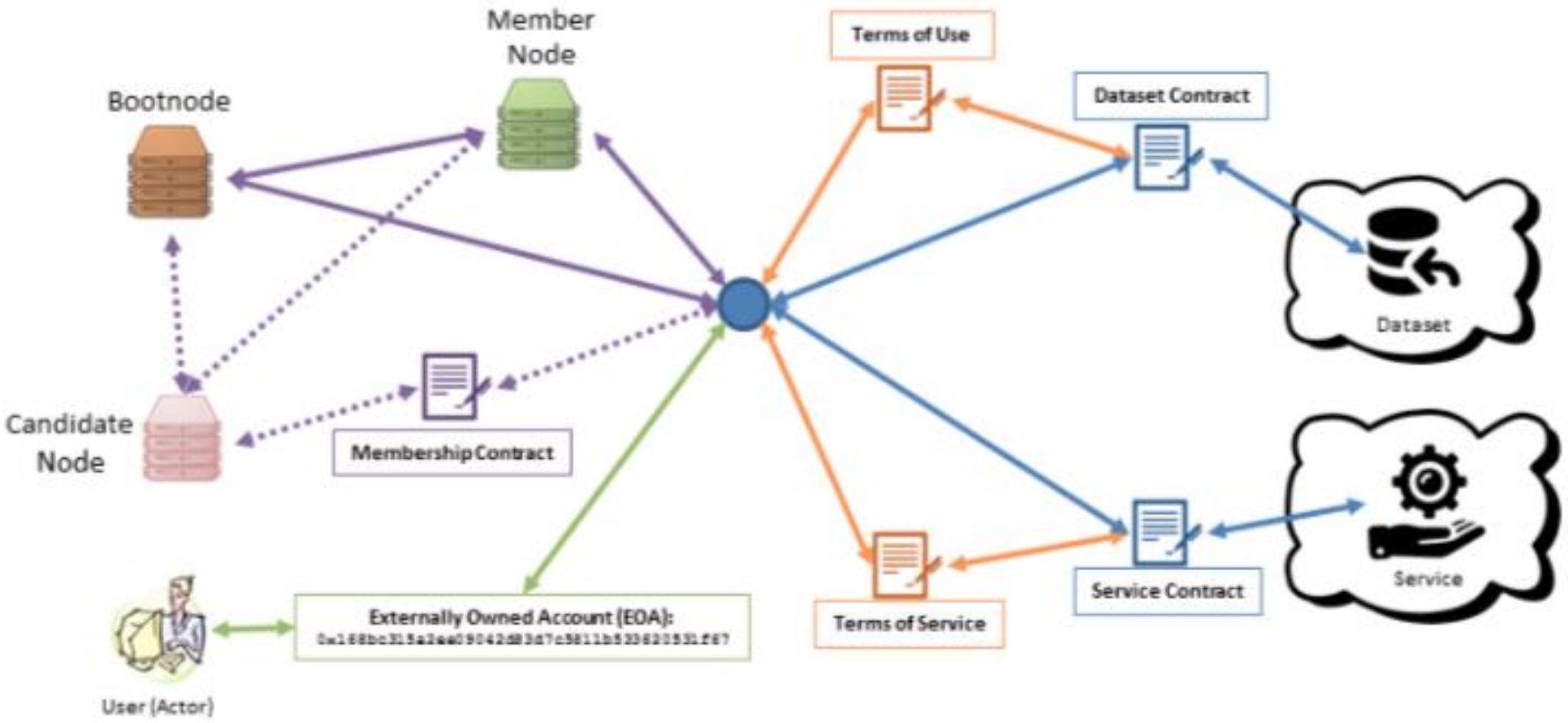
Source: Koutroumpis et al. "The (Unfulfilled) Potential of Data Marketplaces"

Project: Data Market Austria - https://datamarket.at



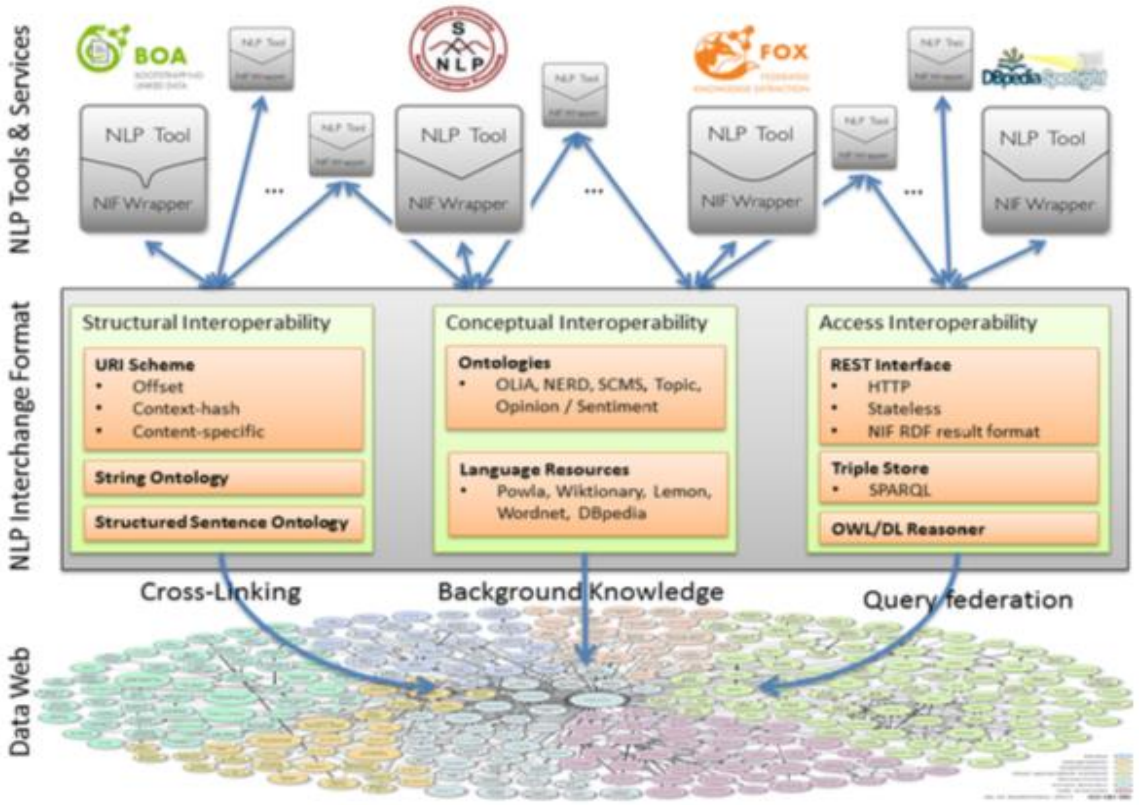
Project: Data Market Austria - https://datamarket.at

- Blockchain at the center of the architecture Also, replicated on nodes



Decentralized, interlinked and interoperable web data

- WWW: largest source of data
- Various technologies
  - Interoperability types
    - Structural
    - Conceptual
    - Access
  - Techs for data analytics
    - Info. retrieval
    - Info. extraction
    - Natural Lang. Proc.
    - …
    - Sentiment analysis



Source: http://www.lrec-conf.org/proceedings/lrec2012/keynotes/LREC 2012.Keynote Speech 1.Soeren Auer.pdf

Conclusions

Conclusions

- The Internet was designed without an identity layer
- Currently, the identity-related issues are addressed at an ad-hoc basis (mainly) utilizing <username, password> credentials
- The evolution of identity models consists of four phases: centralized, federated, user-centric, and self-sovereign
- No examples of truly self-sovereign models
- Data markets: extend the concept of identity models covering various data types created by users
- Data markets: currently, no examples of fully decentralized architectures

References

- Christopher Allen "**The Path to Self-Sovereign Identity**"
- Koutroumpis, Pantelis, Aija Leiponen, and Llewellyn DW Thomas. "**The (Unfulfilled) Potential of Data Marketplaces**". No. 53. The Research Institute of the Finnish Economy.
    - Pages 24 - 32

Webography

- Phil Windley "An Internet for Identity"
  - http://www.windley.com/archives/2016/08/an_internet_for_identity.shtml
- Sovrin
  - https://sovrin.org

  "The Inevitable Rise of Self-Sovereign Identity", A white paper from the Sovrin Foundation
- IBM Blockchain Blog
  - Self-sovereign identity

Additional Bibliography (optional)

- Dirk van Bokkem et al. "Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology"
- Zachary Diebold."Self-Sovereign Identity using Smart Contracts on the Ethereum Blockchain", MSc Dissertation, University of Dublin, Trinity College
- Djuri Baars. "Towards Self-Sovereign Identity using Blockchain Technology", Rabobank and University of Twente
- Data Market Austria Project. "DMA Blockchain Design", D5.2 public deliverable

UNIVERSITY *of* NICOSIA

Instructor’s Email:
iosif.e@unic.ac.cy