Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

”Decentralized Systems for the Protection and Portability of Personal Data”

Mirko Zichichi

Supervisors:
dr. Víctor Rodríguez-Doncel, dr. Stefano Ferretti
Mentor: dr. Massimo Durante

Ontology Engineering Group, **Universidad Politécnica de Madrid**
CIRSFID & DISI, **University of Bologna**
Department of Law, **University of Turin**

Overview i

1. Introduction
   - Onlife
   - Methodology
   - De-centralization
   - Thesis Structure

Overview ii

2 PDS

- Personal Data Storage
- Architecture
- Implementation and Evaluation

3 DIX

- Decentralized Indexing
- Architecture
- Hypercube DHT

Overview iii

4. DAUTH
   - Distributed Authorization
   - Architecture
   - GDPR
   - Evaluation
5. PPAC
   - Privacy-policy-based Access Control
   - Architecture
   - Example

Overview iv

6 SSI

- Self Sovereign Identity
- Architecture
- Implementation

7 Conclusions

- Bibliography

Introduction

Information Communication Technologies (ICTs)

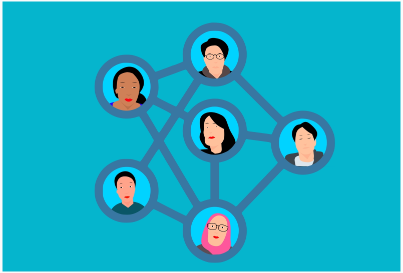
ICTs of early 2000s broke the boundaries between Internet **consumption** and **participation**:

the users of the Web produce the data that other users consume.

Content consists often in **personal data** that involves users or their family, friends, ...

Onlife

- **Onlife** represents the human experience in a society
  - where ”it no longer distinguishes between online or offline”
  - where ”it is **no** longer **reasonable** to ask whether one is **online or offline**” [Floridi, 2014]



- ICTs innovations: *information scarcity* → *information abundance*
- *Benefits* vs. ***privacy*** of the users who inhabit the onlife world.

Informational Privacy and Inference

Informational privacy → an individual's freedom from informational interference achieved by a restriction on facts about him or her that are unknown or unknowable.

- **"anonymous" data** and **little background knowledge (OSNs)** can lead to **identify** individuals and discover their **private attributes** [Qian et al., 2016].
- **social structures** allow to infer: (i) **friendships** links and (ii) fine-grained **users' data** even when they **keep their data private** but their friends do not [Sadilek et al., 2012, Jurgens, 2013].
- obtain "**co-location**" information from a privacy sensitive user' friends [Olteanu et al., 2014], e.g. pictures and **messages** [Ajao et al., 2015] or metadata such as **spatiotemporal correlations** [Yamaguchi et al., 2014].
- Location data allows to **infer individuals activities** (health information, social status, political and religious associations) that individuals **never intended or agreed to share** [Keßler and McKenzie, 2018].

Economics of Personal Information

- A user's "**digital twin**" can be depicted using information collected by digital ITCs from him or his friend, and sold in the **adtech industry** [Zuboff, 2019].
- ↑ understanding **activity** and **lifestyle** patterns ⇒ ↑ intrusive **recommendations**.

Consumers Privacy Paradox [Norberg et al., 2007]

attitude: profess their need for privacy (general)

behavior: remain user of the tech that track and share their data (contextual)

- "**Privacy Calculus**" [Laufer and Wolfe, 1977]:

$$\text{utility of the perceived value of disclosure} = \frac{\mathtt{privacy\ risk}}{\mathtt{benefits}}$$

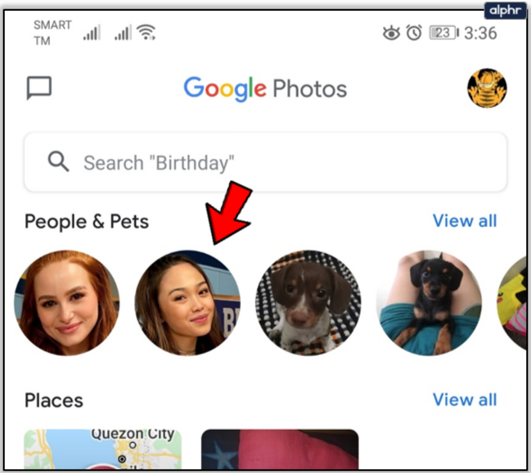
- Correct estimation undermined by **asymmetric information** or **unawareness of possible alternative solutions** [Acquisti et al., 2016].

*Honest**

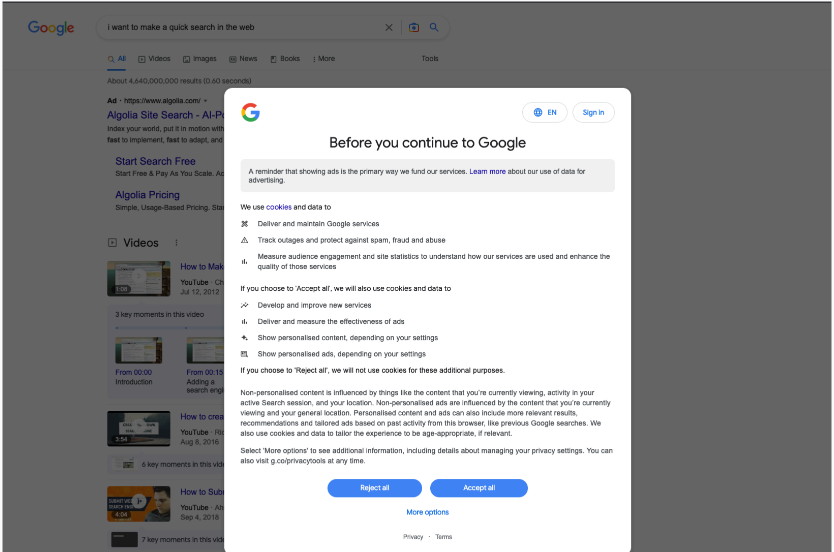
- *but curious
-

I'm feeling curious

Photo storage



Privacy Terms - difficulties in cognitively processing such information


Google
i want to make a quick search in the web
All
Videos
Images
News
Books
More
Tools
About 4,640,000,000 results (0.60 seconds)
Ad · https://www.algolia.com/
Algolia Site Search - AI-P
Index your world, put it in motion with
fast to implement, fast to adapt, and
Start Search Free
Start Free & Pay As You Scale. Ac
Algolia Pricing
Simple, Usage-Based Pricing. Sta
Videos
How to Mak
YouTube · Ch
Jul 12, 2012
1:08
3 key moments in this video
From 00:00
Introduction
From 00:15
Adding a
search engi
How to crea
YouTube · Ri
Aug 8, 2016
3:54
6 key moments in this vid
How to Sub
YouTube · Ah
Sep 4, 2018
4:04
7 key moments in this vid
EN
Sign in

Before you continue to Google

A reminder that showing ads is the primary way we fund our services. Learn more about our use of data for advertising.

We use cookies and data to

- Deliver and maintain Google services
- Track outages and protect against spam, fraud and abuse
- Measure audience engagement and site statistics to understand how our services are used and enhance the quality of those services

If you choose to 'Accept all', we will also use cookies and data to

- Develop and improve new services
- Deliver and measure the effectiveness of ads
- Show personalised content, depending on your settings
- Show personalised ads, depending on your settings

If you choose to 'Reject all', we will not use cookies for these additional purposes.

Non-personalised content is influenced by things like the content that you're currently viewing, activity in your active Search session, and your location. Non-personalised ads are influenced by the content that you're currently viewing and your general location. Personalised content and ads can also include more relevant results, recommendations and tailored ads based on past activity from this browser, like previous Google searches. We also use cookies and data to tailor the experience to be age-appropriate, if relevant.

Select 'More options' to see additional information, including details about managing your privacy settings. You can also visit g.co/privacytools at any time.

General Objective of this work

To investigate methodologies and to design systems that direct the **personal data control** flow towards **individuals** in the *European Union regulatory framework*.

General Objective of this work

To investigate methodologies and to design systems that direct the **personal data control** flow towards **individuals** in the *European Union regulatory framework*.

Data protection is thus conveyed assuming that:
"privacy is not the opposite of sharing– rather, it is control over sharing"
[Acquisti et al., 2016]
following these authors' definition of informational privacy: [Westin, 1967, Floridi, 2014, International Association of Privacy Professionals, 2011].

General Data Protection Regulation (GDPR)

- Personal data **processing** must be lawful, fair, and transparent to the **Data Subject**.
- **Data Processor** must process data for the legitimate purposes specified explicitly to the Data Subject.
- The **Data Controller** is responsible for being able to demonstrate GDPR compliance.
- Integrity and confidentiality, data minimization, accuracy, storage limitation, etc.

”A European strategy for data” - COM(2020) 66 final

- *“[Citizens] can be empowered to be in control of their data through tools and means to decide at a granular level about what is done with their data (‘**personal data spaces**’). This could be supported by enhancing the portability right for individuals under Article 20 of the GDPR, **giving them more control over who can access and use machine-generated data**”*

Sub-Objectives of this work

O1. To identify the systems that can be used to **de-centralize the exploitation of personal information** and their *legal compliance* with the EU regulation.

O2. To design and implement systems that **store and/or trace personal data**, and that provide access to them only through **policies** set by data subjects or based on GDPR legal bases.

O3. To design and implement interoperable mechanisms that enable the **universal identification of personal data, policies and credentials**, in such a way that the data subjects can be sovereign to decide how to store and share their data.

Hypotheses of this work

H1.1. **Decentralized systems based on Distributed Ledger Technologies** can support the replacement of current ICTs-platform-centered personal data management in terms of *feasibility, efficiency, and legal compliance*.

H1.2. The distributed execution of **smart contracts** and dedicated cryptographic schemes can be efficiently employed to provide *personal data access control* without relying on a trusted third party.

H1.3. A decentralized personal information management system can effectively be integrated with, and **Semantic Web technologies** and standards to (i) enforce data subjects's and/or GDPR-based data access policies, (ii) provide an interoperable way to move personal data and trace related processes, and (iii) identify information related to a data subject's online identity universally.

decentralized Personal Information Management System

- A dPIMS can provide individuals with tools for **managing the collected data and access control** to other parties wishing to use such data
  - It acts as a strong **facilitator for the consent** of individuals (and not only)
  - **Decentralized architectures** fits perfectly with data sovereignty
  - Studies that identify roles and adherence of DLTs to GDPR:
    EU blockchain forum, **CNIL** in France, **AEDP** in Spain, Finck and Pallas, etc...
- Data interoperability and collaboration between services can be strongly backed up by the use of standards and related technologies (Semantic Web)
  - **Common API** for requests to Data Controller
  - Machine readable access control policies (**MPEG-21, W3C Open Digital Rights Language**)

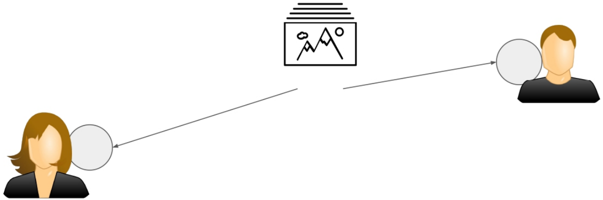
Main Research Question:

Are **decentralized technologies** and **semantic web standards** able to support individuals' *personal data protection and portability* ***optimally***?

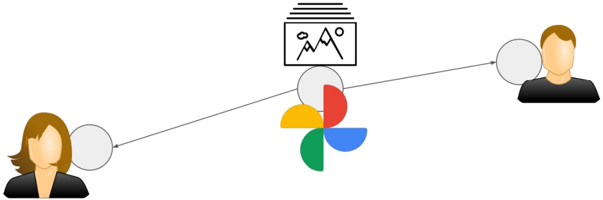
Research Questions:

- **RQ1.1** - Are **decentralized technologies** able to support the *replacement* of current **platform-centered data protection management**?
- **RQ1.2** - How can **semantic web vocabularies and disintermediation** foster a convergence between the protection of individuals' data and the development of *data sharing solutions*?
- **RQ1.3** - To what extent can **decentralized systems and EU regulations** such as the GDPR coexist in order to effectively shift the de facto *control of personal data sharing* to data subjects?

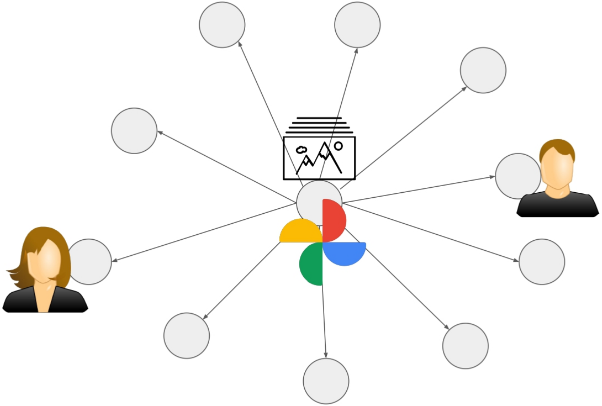
Centralized - Honest (but curious)



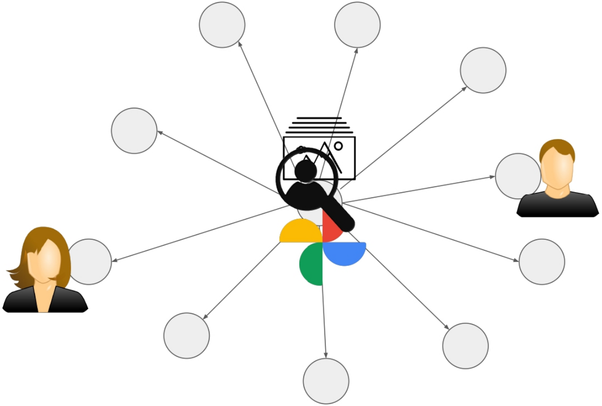
Centralized - Honest (but curious)



Centralized - Honest (but curious)



Centralized - Honest (but curious)

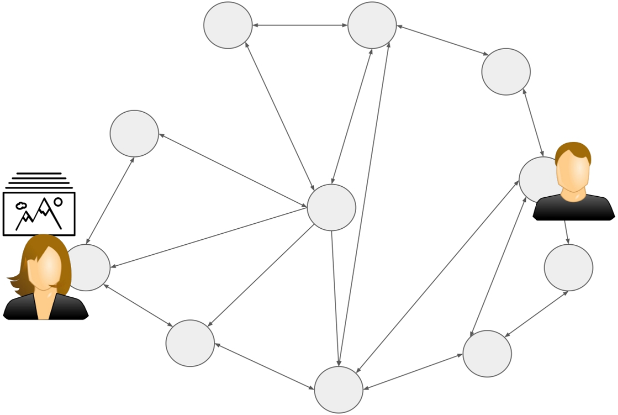


Single point of failure

Single point of failure

Part of a system that, if it *fails*, will **stop** the entire system from **working**.

De-centralized Permissionless



Bitcoin

- The first **Peer-to-Peer (P2P)** cryptocurrency that brought a new wave of development of decentralized systems to *combat the single point of failure issue*.
- Such a system operates through the **emergent** behavior of its component parts rather than as a result of the *influence of a centralized part*.
- Nakamoto has made possible the **coordinated operation** of nodes in a network without needing to control their access to the system itself
- a *permissionless transactional decentralized system*.

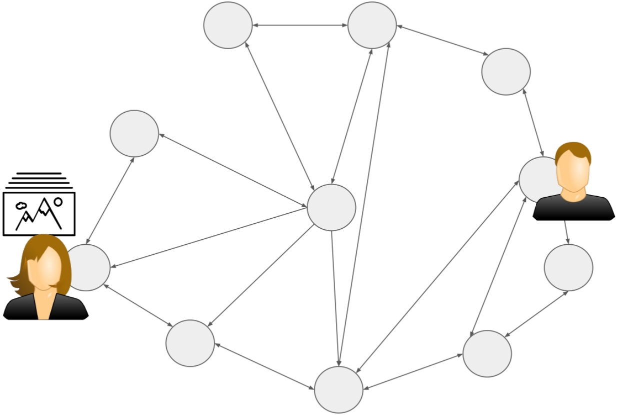
Does it solve the single point of failure issue?

- Criticisms: issue of trust.
- Blockchain attempts to replace trust with code, i.e., consensus algorithm
- Bruce Scheiner (*“On the Dangers of Cryptocurrencies and the Uselessness of Blockchain”*):
  - This makes these technologies less trustworthy than non-blockchain systems.
  - Non-blockchain systems are based on other general mechanisms humans use to incentivize **trustworthy behavior** that make consensus mechanisms unnecessary
  - *morals, reputation, institutions, and security mechanisms.*

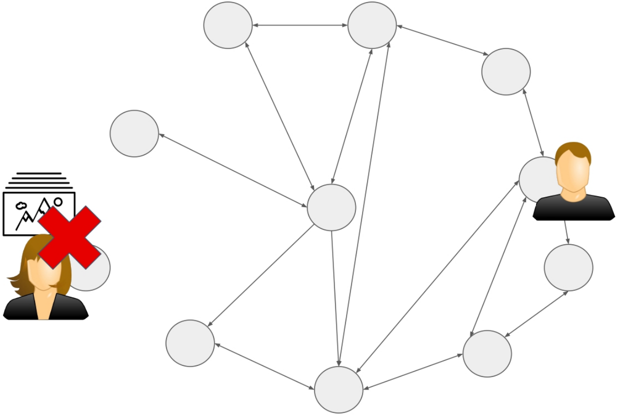
Reasons

- Consensus mechanisms shift the *trust in people and institutions* to *trust in the technology*. When that trust turns out to be misplaced, there is no recourse.
- In such a permissionless environment it may be infeasible to incentivize participants to adequately provide functions like quality control or coordination of system development and evolution.
- Centralization emerges de facto:
  - hierarchy of the small number of developers controlling the blockchain software
  - the few numbers of centralized networks that control the consensus mechanism execution (mining pools).

De-centralized Permissionless



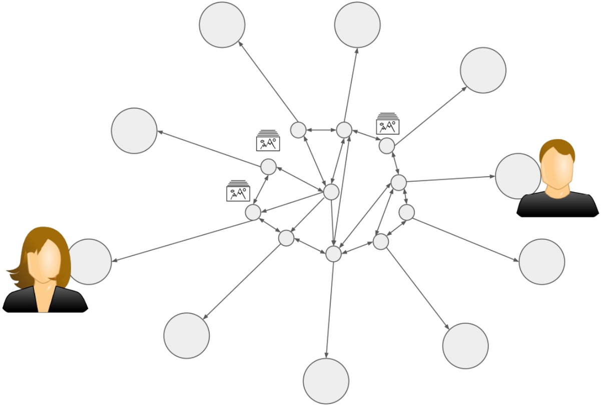
De-centralized Permissionless



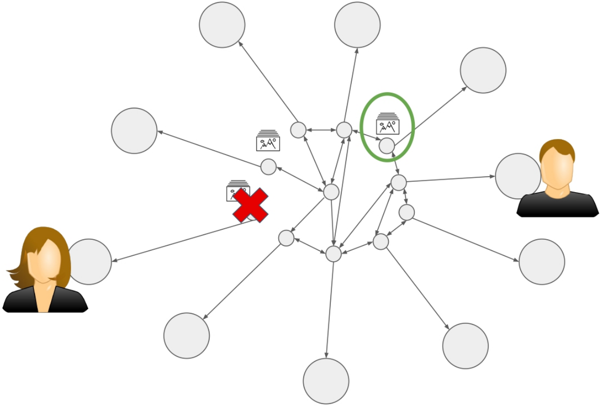
Permissioned DLTs

- Different actors with different interests (possibly clashing between themselves) constantly monitor their “adversary-peers”
- control if one of them attempts to alter or inadvertently change previously agreed-upon information.
- **single source of verifiable truth** among de-centralized organizations.

De-centralized Permissioned



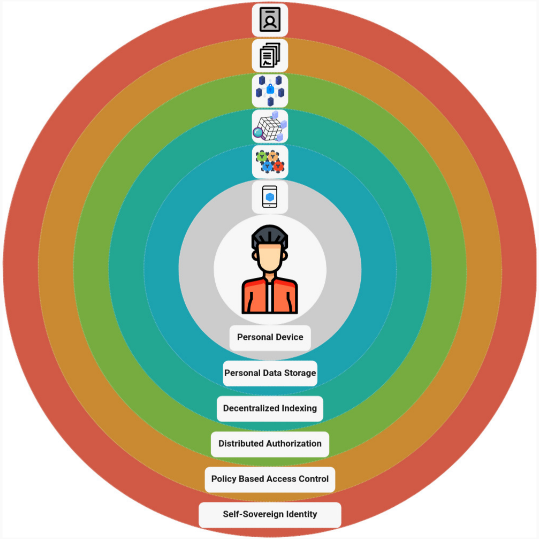
De-centralized Permissioned



Permissioned DLTs + Law

- **Absolutist Law perspective**
  Creating laws without looking for ways to approach technology → does not preserve the survival of new technologies
- **Absolutist Technology perspective**
  Designing technology without relying on laws → creates ”temporarily autonomous zones” to which is difficult to enter into/exit from.
- **Law + technology**
  complement each other while trying to preserve their sphere of influence → maintaining the distinctive features of DLTs while being allowed to enforce the law.

Individuals at the center of a Privacy-by-Design System



PDS

Chapter 4 - Personal Data Storage (PDS)

Personal data are kept in a Personal Data Storage (**PDS**) -> set of encrypted data referring to the subject that is stored in a **Decentralized file storage (DFS)**.

Contributions:

1. First, we provide an **interdisciplinary analysis of technical and non-technical drivers for the design of a PDS**. In particular, in the background, related work, and architecture description, *we refer to the GDPR* and work/analyses related to this.
2. Second, we describe the decentralized PDS system based on the use of **DFS for the off-chain storage** of personal data and a **DLT for data integrity and traceability**.
3. Third, we provide a prototype implementation of the described system, and we evaluate its performance using an experimental evaluation (IPFS/SIA & IOTA).

Personal Data Storage (PDS) Architecture

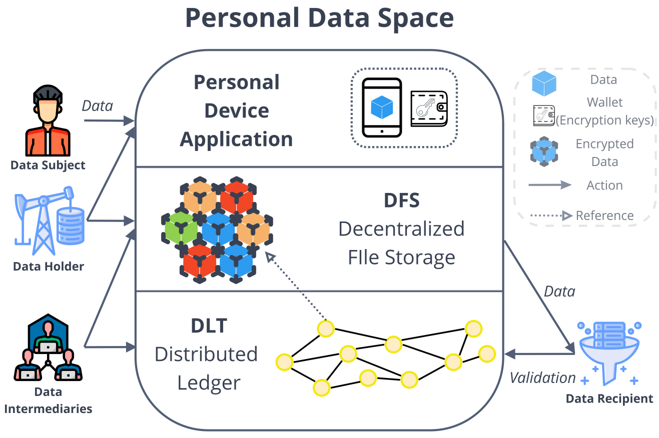


Figure 1: Diagram showing a layered vision of the whole PDS architecture.

Data classification and use in the architecture

Data	Type	Source	Storage Location
Personal Data	*Personal*	Subject Personal Device or Data Holder Device	Private: • Subject Personal Device • Data Holder Private Storage
Encrypted Data	*Pseudonymous**	Encrypting personal data	Private/Public: • Decentralized File Storage • Data Holder Private Storage
On-chain Hash Ptr	*Pseudonymous**	Hashing Encrypted Data using Single-Use Salt	Private/Public: • DLT
Address	*Pseudonymous*	Created from the Subject Personal Device Wallet	Private/Public: • DLT

Cryptosystem

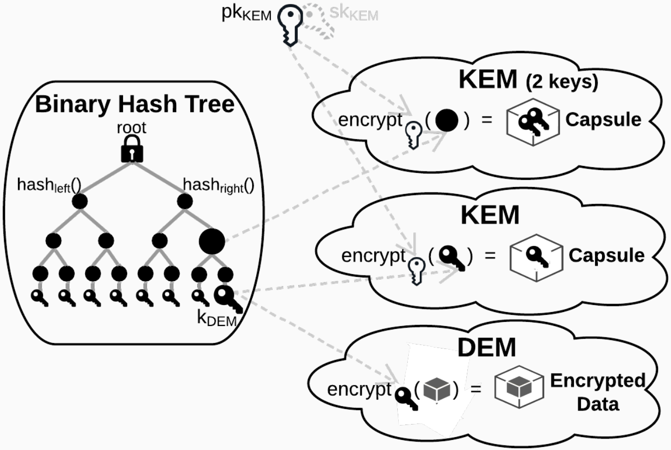


Figure 2: Data and key encapsulation mechanisms.

Decentralized Urban Crowdsourcing Simulation

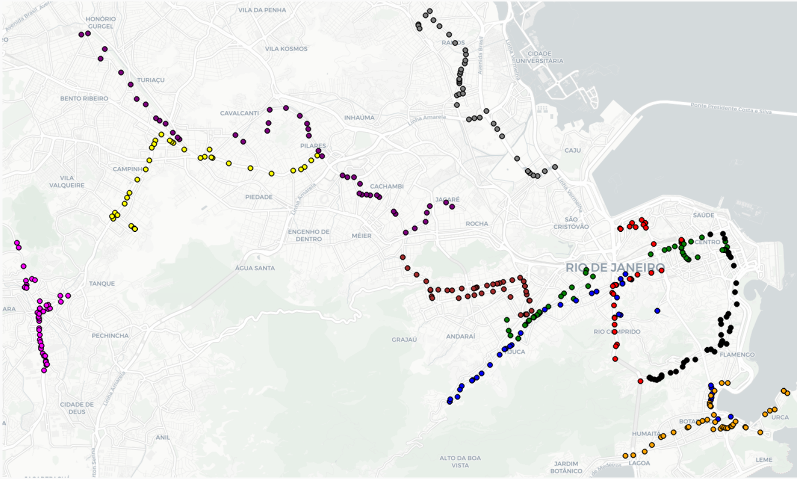
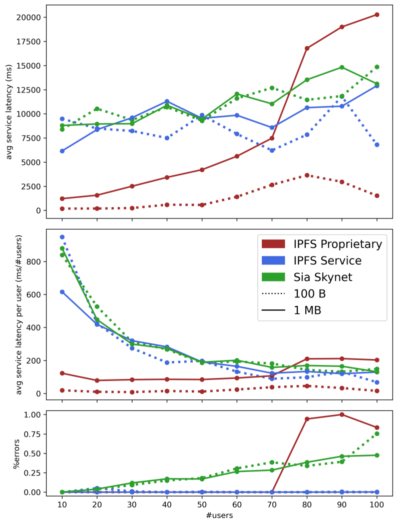
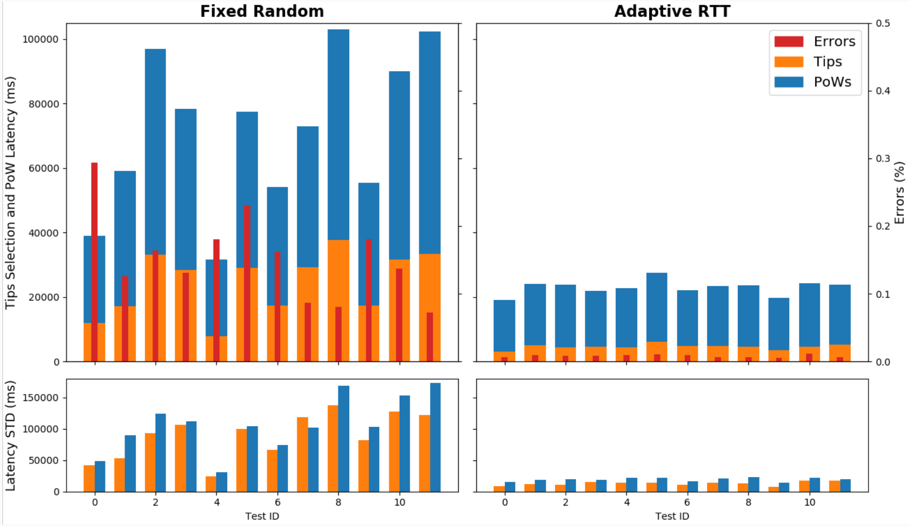


Figure 3: Users in buses in Rio de Janeiro simulation.

DFS: IPFS vs. SIA



DLT: IOTA Tangle (2020) - 60 bus tests



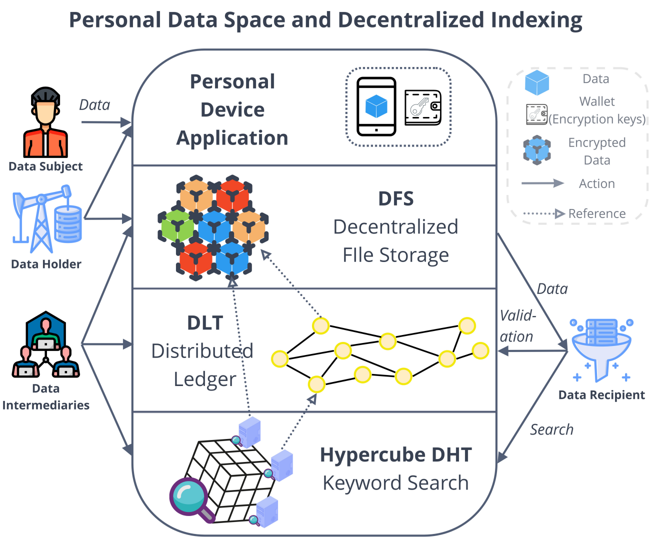
DIX

Chapter 5 - Decentralized Indexing

Contributions:

- *Integrity, verifiability, linkability and indexing* of the encrypted PDS personal data -> *reference data and their content* (**hash pointer**) on a DLT, on-chain.
- we provide a decentralized system for **key-value metadata-based lookup** (**Hypercube DHT**), which allows retrieving contents stored in DLTs and/or DFS.
- Third, we provide a prototype implementation of the described system, and we evaluate its performance by employing an experimental evaluation.

Decentralized Indexing Architecture



Keywords Sets

- O $\leftarrow$ set of stream channel announcement links in the IOTA DLT
- o $\in O$ is mapped to a **keyword set K$_o$** $\subseteq W$
- By using a **uniform hash function**
  $h : W \rightarrow \{0, 1, \ldots, r-1\}$
  K$_o$ can be represented by a string of bits **u** $\rightarrow$ 101001
- in **u the 1s are set in the positions** given by
  $one(u) = \{h(k) \mid k \in K\}$
- E.g.: $o = Stream\ link\ 6bb...00{:}219$, $K = \{temperature, celsius\}$
  $h(temperature) = 3, h(celsius) = 5$
  K is represented by $u = 000101 \Rightarrow$ **DHT stores (000101,*6bb...00:219*)**

Hypercube based DHT

- We use these r-bit strings to identify logical nodes in a r-dimensional **hypercube based DHT**
- network topology $\rightarrow H_r(V, E)$ **hypercube**
- **V** set of vertices that represent **logical nodes**
- **E** set of edges formed when two vertices differ of only one bit (they are also network **neighbors**), e.g. 1011 and 1010.
- **Pin Search** - $\{o \in O \mid K_o = K\}$
  e.g. *pinSearch({Wikipedia, Rome})* = (*000**101**,QmbW...MnR*), (*000**101**,QmbP...3Lx*), ...
- **Superset Search** - $\{o \in O \mid K_o \supseteq K\}$
  e.g. *superSetSearch({Wikipedia, Rome})* = (*000**101**,QmbW...MnR*), (*000**111**,QmbZ...aaD*), ...

Hypercube based DHT

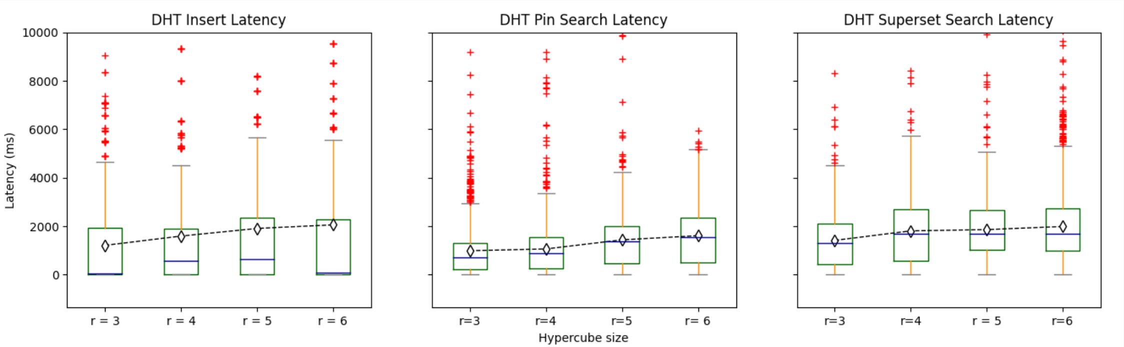


Figure 7: Hops in the order of **logarithm of the hypercube logical nodes number** $\rightarrow \frac{\log(n)}{2} = \frac{r}{2}$.

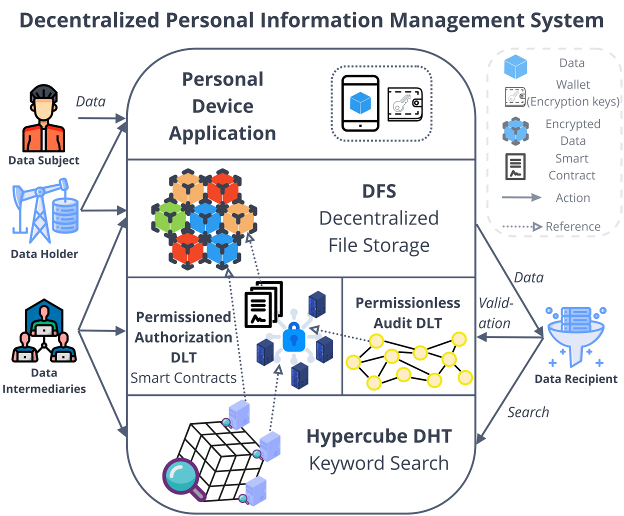
DAUTH

Chapter 6 - Distributed Authorization

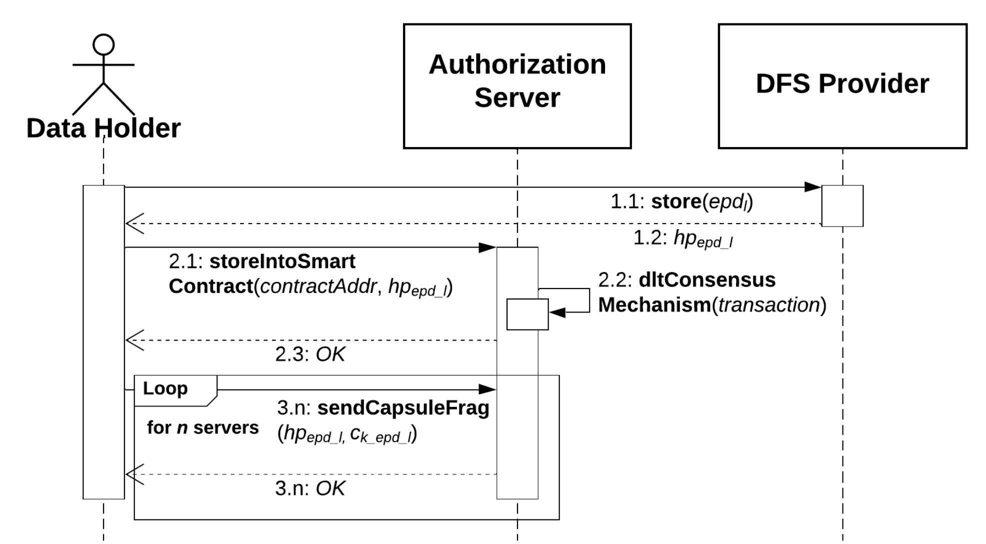
Access to the data stored on a PDS can be allowed by the data holder through **smart contracts**. It creates a **Personal Information Management System (PIMS)**.

1. First, we describe a novel PIMS based on a **multi-DLT GDPR-compliant design**. Extension of PDS and DIX system with a **secure control of access to personal data** component. Multi-DLT system where a *permissioned DLT provides the authorization mechanism*, and a *permissionless DLT provides security*.
2. Second, we provide an interdisciplinary analysis of technical and non-technical drivers for designing a GDPR-compliant decentralized PIMS that can be generalized to different systems handling personal data. Furthermore, we discuss our proposal's **security and privacy properties based on a privacy impact assessment**.
3. Third, we provide a prototype implementation of the described system, and we evaluate its performance by employing an experimental evaluation (Consensys Quorum).

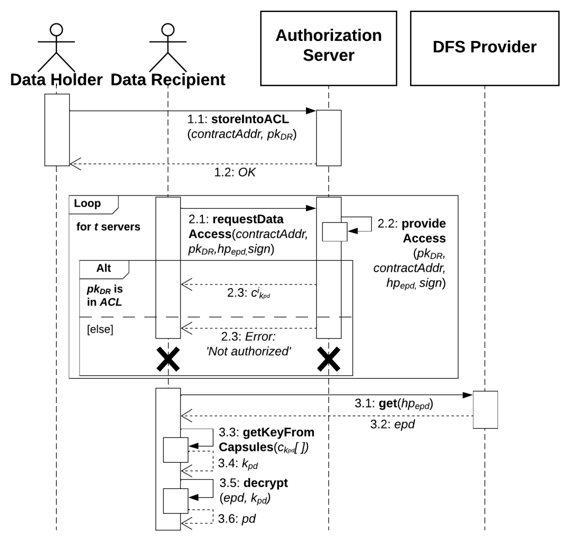
Decentralized Personal Information Management System (PIMS) Architecture



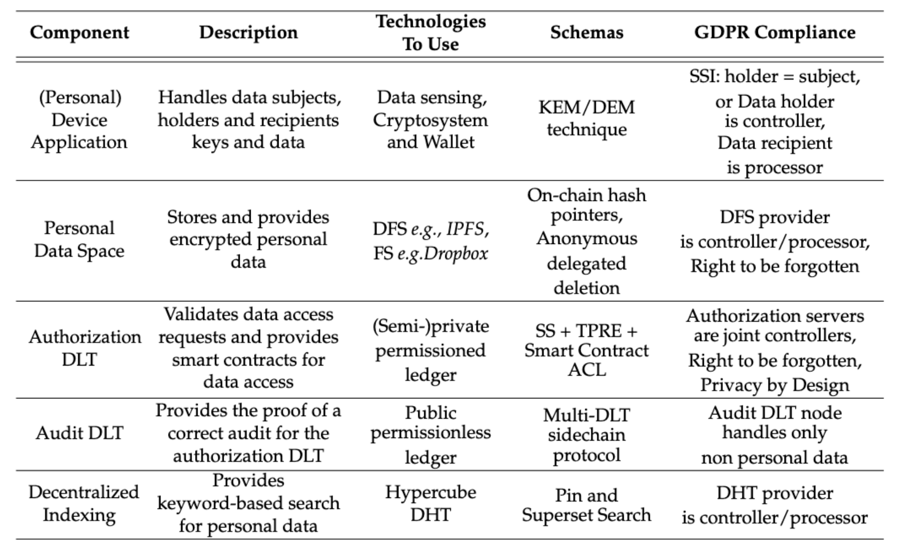
(Semi-)Private Authorization DLT [1/2]


Data Holder
Authorization Server
DFS Provider
1.1: **store**(*epd*$_l$)
1.2: *hp*$_{epd\_l}$
2.1: **storeIntoSmart Contract**(*contractAddr*, *hp*$_{epd\_l}$)
2.2: **dltConsensus Mechanism**(*transaction*)
2.3: *OK*
Loop
for *n* servers
3.n: **sendCapsuleFrag** (*hp*$_{epd\_l}$, *c*$_{k\_epd\_l}$)
3.n: *OK*

(Semi-)Private Authorization DLT [2/2]


Data Holder
Data Recipient
Authorization Server
DFS Provider
1.1: **storeIntoACL** (*contractAddr*, pk_{DR})
1.2: *OK*
Loop
for *t* servers
2.1: **requestData Access**(*contractAddr*, pk_{DR},hp_{epd},*sign*)
2.2: **provide Access** (pk_{DR}, *contractAddr*, hp_{epd}, *sign*)
Alt
pk_{DR} is in *ACL*
2.3: $c^{i}_{k_{pd}}$
[else]
2.3: *Error: 'Not authorized'*
3.1: **get**(hp_{epd})
3.2: *epd*
3.3: **getKeyFrom Capsules**($c_{k_{pd}}$[ ])
3.4: k_{pd}
3.5: **decrypt** (*epd*, k_{pd})
3.6: *pd*

GDPR Compliance [1/2]



Component	Description	Technologies To Use	Schemas	GDPR Compliance
(Personal) Device Application	Handles data subjects, holders and recipients keys and data	Data sensing, Cryptosystem and Wallet	KEM/DEM technique	SSI: holder = subject, or Data holder is controller, Data recipient is processor
Personal Data Space	Stores and provides encrypted personal data	DFS *e.g., IPFS*, FS *e.g.Dropbox*	On-chain hash pointers, Anonymous delegated deletion	DFS provider is controller/processor, Right to be forgotten
Authorization DLT	Validates data access requests and provides smart contracts for data access	(Semi-)private permissioned ledger	SS + TPRE + Smart Contract ACL	Authorization servers are joint controllers, Right to be forgotten, Privacy by Design
Audit DLT	Provides the proof of a correct audit for the authorization DLT	Public permissionless ledger	Multi-DLT sidechain protocol	Audit DLT node handles only non personal data
Decentralized Indexing	Provides keyword-based search for personal data	Hypercube DHT	Pin and Superset Search	DHT provider is controller/processor

GDPR Compliance [2/2]

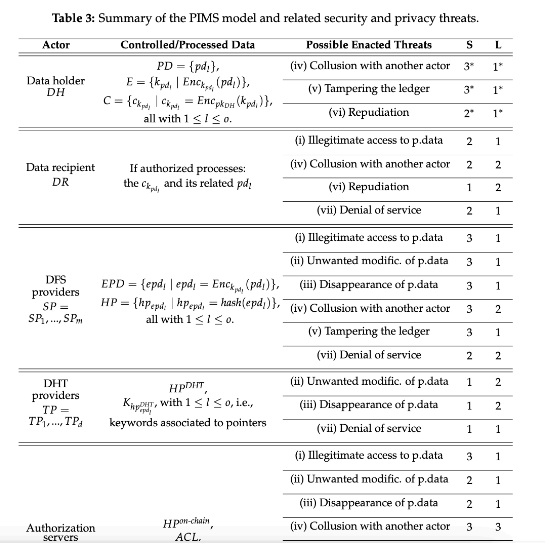
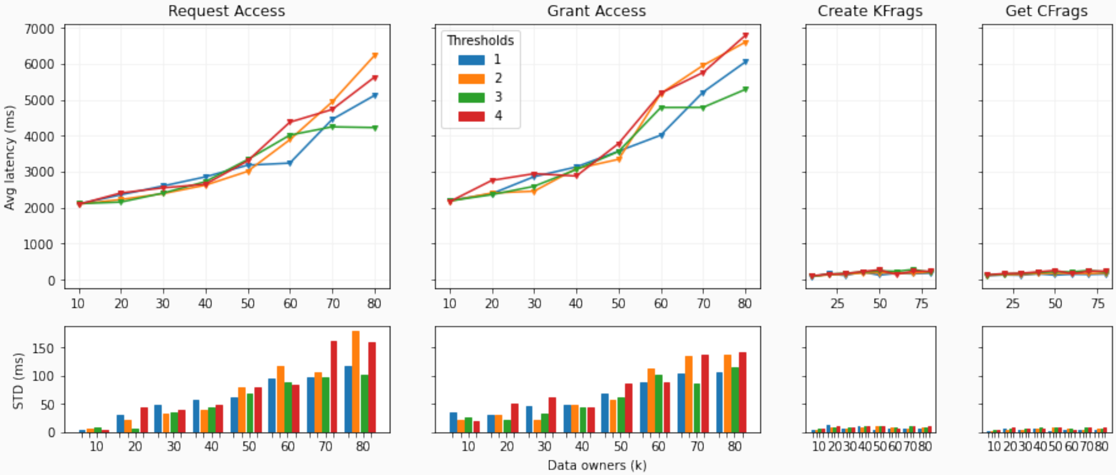


Table 3: Summary of the PIMS model and related security and privacy threats.

Actor	Controlled/Processed Data	Possible Enacted Threats	S	L
Data holder DH	$PD = \{pd_l\}$, $E = \{k_{pd_l} \mid Enc_{k_{pd_l}}(pd_l)\}$, $C = \{c_{k_{pd_l}} \mid c_{k_{pd_l}} = Enc_{pk_{DH}}(k_{pd_l})\}$, all with $1 \leq l \leq o$.	(iv) Collusion with another actor	3*	1*
		(v) Tampering the ledger	3*	1*
		(vi) Repudiation	2*	1*
Data recipient DR	If authorized processes: the $c_{k_{pd_l}}$ and its related pd_l	(i) Illegitimate access to p.data	2	1
		(iv) Collusion with another actor	2	2
		(vi) Repudiation	1	2
		(vii) Denial of service	2	1
DFS providers $SP =$ $SP_1, ..., SP_m$	$EPD = \{epd_l \mid epd_l = Enc_{k_{pd_l}}(pd_l)\}$, $HP = \{hp_{epd_l} \mid hp_{epd_l} = hash(epd_l)\}$, all with $1 \leq l \leq o$.	(i) Illegitimate access to p.data	3	1
		(ii) Unwanted modific. of p.data	3	1
		(iii) Disappearance of p.data	3	1
		(iv) Collusion with another actor	3	2
		(v) Tampering the ledger	3	1
		(vii) Denial of service	2	2
DHT providers $TP =$ $TP_1, ..., TP_d$	HP^{DHT}, $K_{hp^{DHT}_{epd_l}}$, with $1 \leq l \leq o$, i.e., keywords associated to pointers	(ii) Unwanted modific. of p.data	1	2
		(iii) Disappearance of p.data	1	2
		(vii) Denial of service	1	1
Authorization servers	$HP^{on\text{-}chain}$, ACL.	(i) Illegitimate access to p.data	3	1
		(ii) Unwanted modific. of p.data	2	1
		(iii) Disappearance of p.data	2	1
		(iv) Collusion with another actor	3	3

Operating with the authorization DLT (Consensys Quorum)



PPAC

Chapter 7 - Privacy-policy-based Access Control

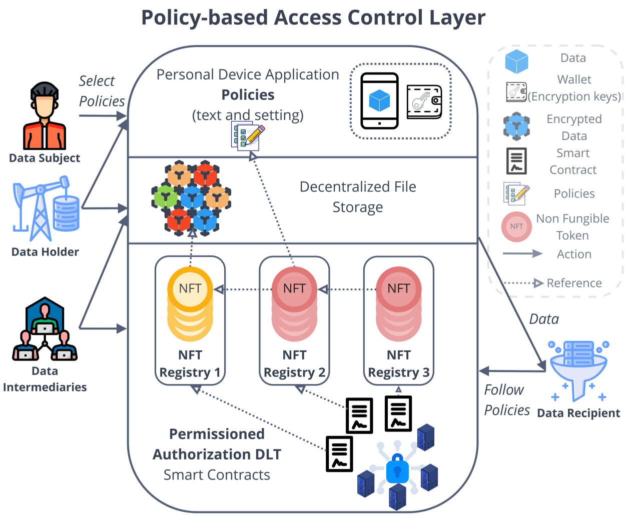
Policies can be used to enrich the expressiveness of the access control mechanism and to let the data holder express privacy policies to be enacted through the smart contracts.

- We provide a specification of **Privacy Policy Objects** created through a set of Semantic Web technologies and standards: *ISO/IEC 21000 MPEG-21 framework, Media Contract Ontology (MCO), Smart Contract for Media, W3C Data Privacy Vocabulary (DPV).*
- We provide some use cases to enforce legitimate data access rights that may take precedence over those of users, e.g. the GDPR's vital interest legal base for data processing.
- The link between the operational side of the smart contracts and the narrative clauses of a policy are completely mapped thanks to the use of the above mentioned standards.

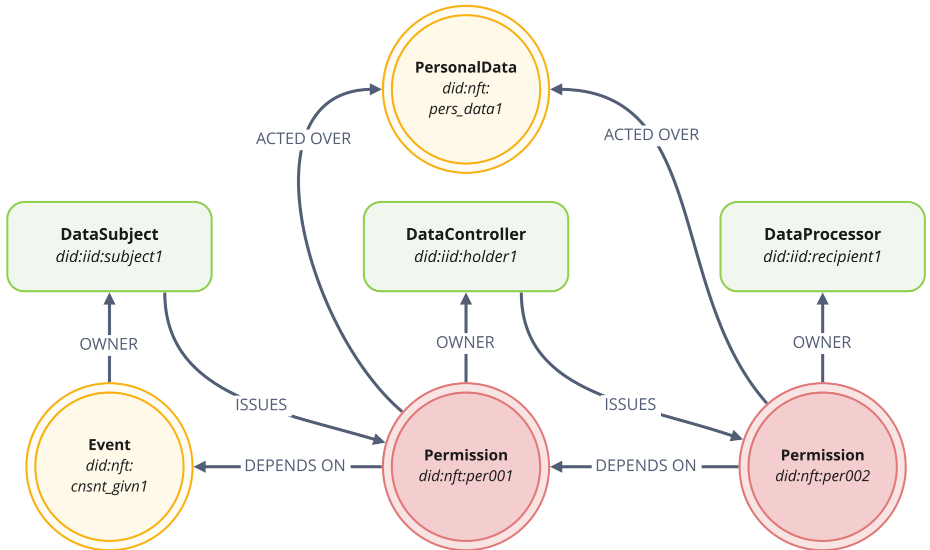
Encoding clauses as assets through NFTs

- What is generally non-trivial is the use of NFTs to encode information related to the ownership of certain rights, such as **permissions, obligations, and prohibitions**.
- Thanks to the ISO/IEC 21000 Smart Contract for Media Deontic Expression object representation, **we can create referable rights and duties** -> clauses.
- It is possible to save the association between this reference and the relevant party directly in the ledger in an immutable way through **NFTs**.

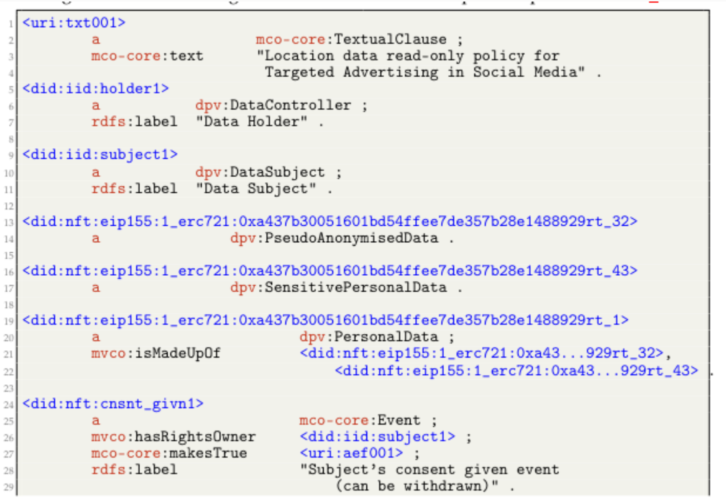
Privacy-policy-based Access Control layer



Privacy-policy-based Access Control - Example

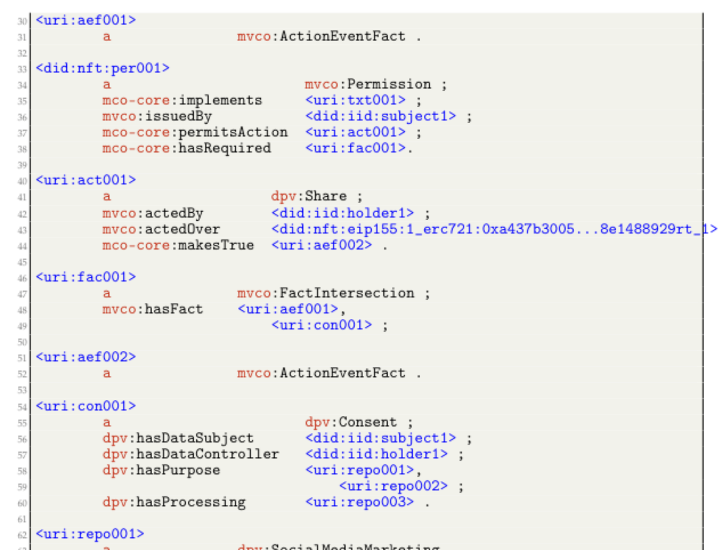


Privacy-policy-based Access Control - Example



```
<uri:txt001>
        a                  mco-core:TextualClause ;
        mco-core:text      "Location data read-only policy for
                            Targeted Advertising in Social Media" .
<did:iid:holder1>
        a            dpv:DataController ;
        rdfs:label   "Data Holder" .

<did:iid:subject1>
        a            dpv:DataSubject ;
        rdfs:label   "Data Subject" .

<did:nft:eip155:1_erc721:0xa437b30051601bd54ffee7de357b28e1488929rt_32>
        a                  dpv:PseudoAnonymisedData .

<did:nft:eip155:1_erc721:0xa437b30051601bd54ffee7de357b28e1488929rt_43>
        a                  dpv:SensitivePersonalData .

<did:nft:eip155:1_erc721:0xa437b30051601bd54ffee7de357b28e1488929rt_1>
        a                        dpv:PersonalData ;
        mvco:isMadeUpOf          <did:nft:eip155:1_erc721:0xa43...929rt_32>,
                                     <did:nft:eip155:1_erc721:0xa43...929rt_43> .

<did:nft:cnsnt_givn1>
        a                        mco-core:Event ;
        mvco:hasRightsOwner      <did:iid:subject1> ;
        mco-core:makesTrue       <uri:aef001> ;
        rdfs:label               "Subject’s consent given event
                                     (can be withdrawn)" .
```

Privacy-policy-based Access Control - Example



```
<uri:aef001>
        a                       mvco:ActionEventFact .

<did:nft:per001>
        a                               mvco:Permission ;
        mco-core:implements             <uri:txt001> ;
        mvco:issuedBy                   <did:iid:subject1> ;
        mco-core:permitsAction          <uri:act001> ;
        mco-core:hasRequired            <uri:fac001>.

<uri:act001>
        a                           dpv:Share ;
        mvco:actedBy                <did:iid:holder1> ;
        mvco:actedOver              <did:nft:eip155:1_erc721:0xa437b3005...8e1488929rt_1>
        mco-core:makesTrue          <uri:aef002> .

<uri:fac001>
        a                       mvco:FactIntersection ;
        mvco:hasFact            <uri:aef001>,
                                    <uri:con001> ;

<uri:aef002>
        a                       mvco:ActionEventFact .

<uri:con001>
        a                               dpv:Consent ;
        dpv:hasDataSubject              <did:iid:subject1> ;
        dpv:hasDataController           <did:iid:holder1> ;
        dpv:hasPurpose                  <uri:repo001>,
                                            <uri:repo002> ;
        dpv:hasProcessing               <uri:repo003> .

<uri:repo001>
        a                       dpv:SocialMediaMarketing
```

Privacy-policy-based vs. ACL-based Access Control

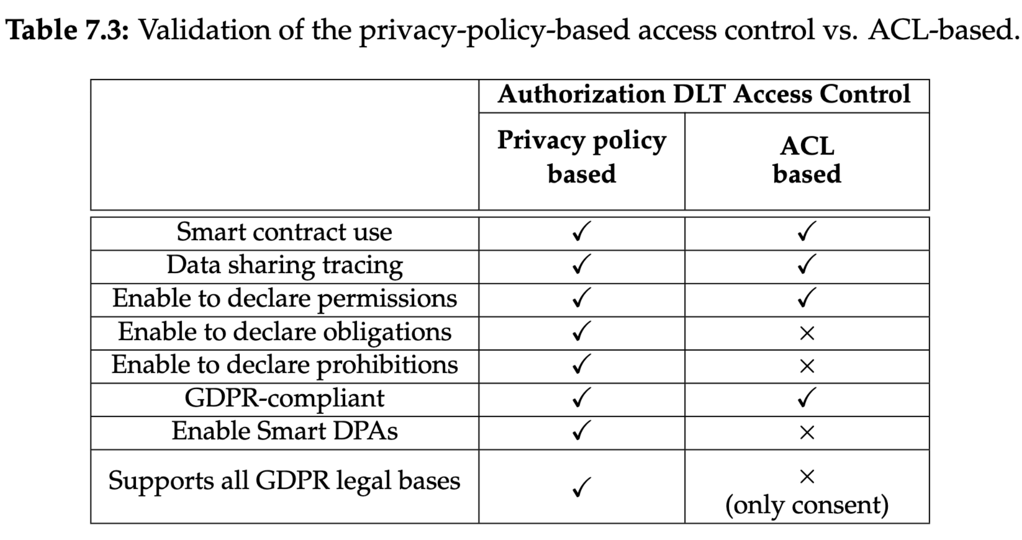


Table 7.3: Validation of the privacy-policy-based access control vs. ACL-based.

	Authorization DLT Access Control	
	Privacy policy based	**ACL based**
Smart contract use	✓	✓
Data sharing tracing	✓	✓
Enable to declare permissions	✓	✓
Enable to declare obligations	✓	×
Enable to declare prohibitions	✓	×
GDPR-compliant	✓	✓
Enable Smart DPAs	✓	×
Supports all GDPR legal bases	✓	× (only consent)

SSI

Chapter 8 - Self Sovereign Identity

SSI and it creates a **port** to let any ICTs service interact with the onlife identity of an individual.

- We provide the *Intelligible Decentralized Identity and Verifiable Certificate* -> set of technological components that are deployed in decentralized environments for the purpose of providing, requesting and obtaining qualified data in order to negotiate and/or execute electronic transactions.
- Specialization of a W3C Decentralized Identifier (DID) and Verifiable Credentials (VCs).
- Intelligibility is conveyed by linking (i) resources that make up the document or define their legal contexts; (ii) the agents that involved; (iii) the digital resources that describe how to perform operations with the identities.

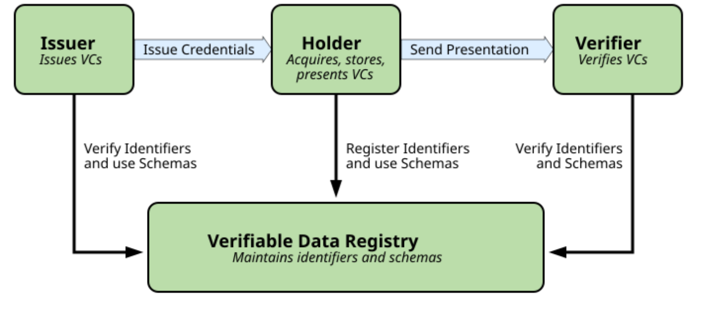
Self-Sovereignty for Social Good

Self-Sovereign Identity
users at the center of the identity process + the ability to be **rulers of their own identity** (The Path to Self-Sovereign Identity, [Christopher Allen, 2016])

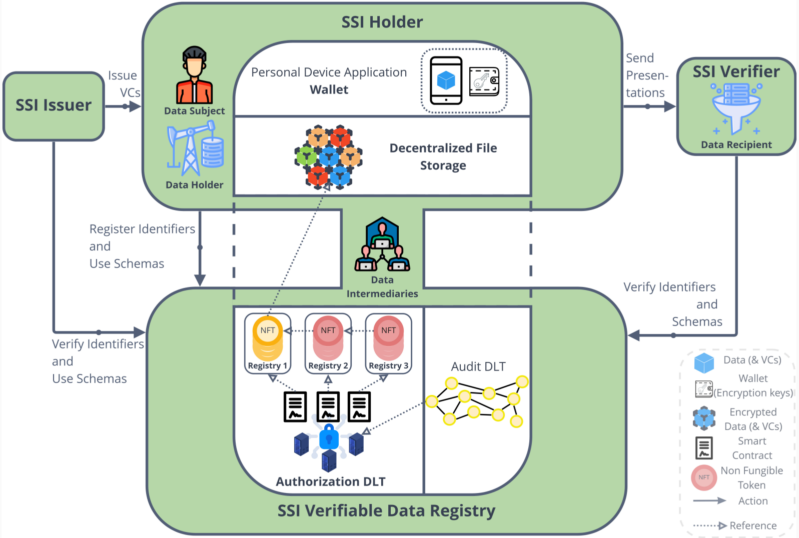
for

Social Good?
facilitate individuals to allow the **use of data they generate for the public good**, if they wish to do so, in compliance with GDPR → *"Data Altruism"*

W3C Decentralized Identifier (DID) and Verifiable Credentials (VCs) Model


Issuer
Issues VCs
Issue Credentials
Holder
Acquires, stores, presents VCs
Send Presentation
Verifier
Verifies VCs
Verify Identifiers and use Schemas
Register Identifiers and use Schemas
Verify Identifiers and Schemas
Verifiable Data Registry
Maintains identifiers and schemas

W3C Decentralized Identifier (DID) and Verifiable Credentials (VCs) Model



SSI Issuer

Issue VCs

SSI Holder

Data Subject

Data Holder

Personal Device Application
Wallet

Decentralized File Storage

Send Presentations

SSI Verifier

Data Recipient

Register Identifiers and Use Schemas

Data Intermediaries

Verify Identifiers and Schemas

Verify Identifiers and Use Schemas

NFT

Registry 1

NFT

Registry 2

NFT

Registry 3

Audit DLT

Authorization DLT

SSI Verifiable Data Registry

Data (& VCs)

Wallet (Encryption keys)

Encrypted Data (& VCs)

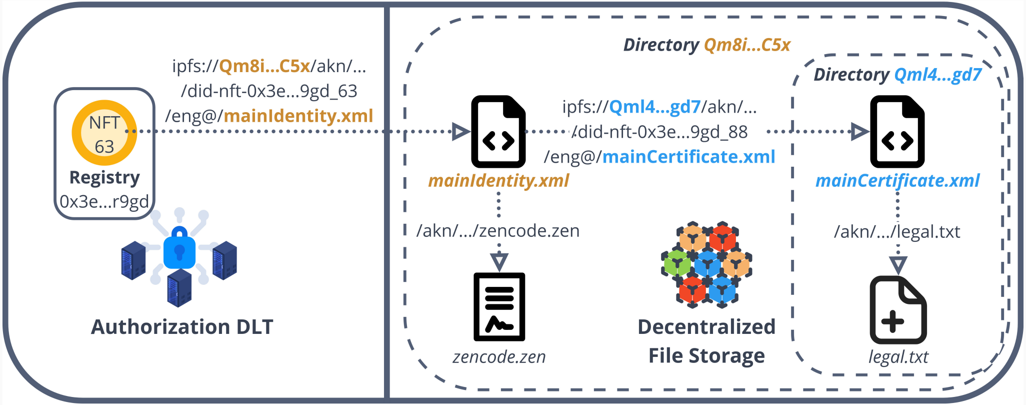
Smart Contract

Non Fungible Token

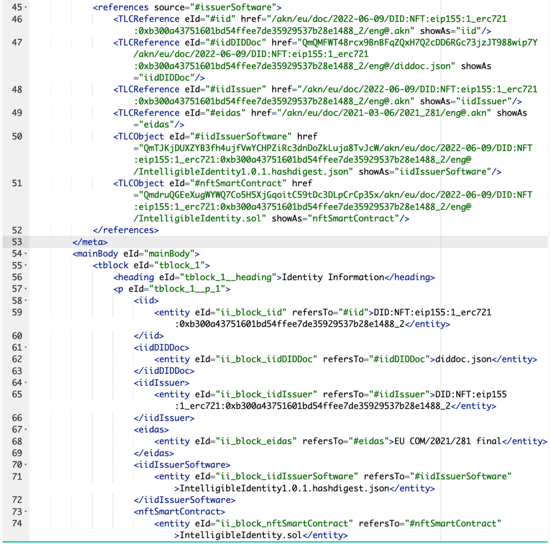
Action

Reference

Intelligible Decentralized Identity and Verifiable Certificate



Intelligible Decentralized Identity and Verifiable Certificate - Example



```
      <references source="#issuerSoftware">
        <TLCReference eId="#iid" href="/akn/eu/doc/2022-06-09/DID:NFT:eip155:1_erc721
            :0xb300a43751601bd54ffee7de35929537b28e1488_2/eng@.akn" showAs="iid"/>
        <TLCReference eId="#iidDIDDoc" href="QmQMFWT48rcx9BnBFqZQxH7Q2cDD6RGc73jzJT988wip7Y
            /akn/eu/doc/2022-06-09/DID:NFT:eip155:1_erc721
            :0xb300a43751601bd54ffee7de35929537b28e1488_2/eng@/diddoc.json" showAs
            ="iidDIDDoc"/>
        <TLCReference eId="#iidIssuer" href="/akn/eu/doc/2022-06-09/DID:NFT:eip155:1_erc721
            :0xb300a43751601bd54ffee7de35929537b28e1488_2/eng@.akn" showAs="iidIssuer"/>
        <TLCReference eId="#eidas" href="/akn/eu/doc/2021-03-06/2021_281/eng@.akn" showAs
            ="eidas"/>
        <TLCObject eId="#iidIssuerSoftware" href
            ="QmTJKjDUXZYB3fh4ujfVwYCHPZiRc3dnDoZkLuja8TvJcW/akn/eu/doc/2022-06-09/DID:NFT
            :eip155:1_erc721:0xb300a43751601bd54ffee7de35929537b28e1488_2/eng@
            /IntelligibleIdentity1.0.1.hashdigest.json" showAs="iidIssuerSoftware"/>
        <TLCObject eId="#nftSmartContract" href
            ="QmdruQGEeXugWYWQ7Co5H5XjGqoitC59tDc3DLpCrCp35x/akn/eu/doc/2022-06-09/DID:NFT
            :eip155:1_erc721:0xb300a43751601bd54ffee7de35929537b28e1488_2/eng@
            /IntelligibleIdentity.sol" showAs="nftSmartContract"/>
      </references>
    </meta>
    <mainBody eId="mainBody">
      <tblock eId="tblock_1">
        <heading eId="tblock_1__heading">Identity Information</heading>
        <p eId="tblock_1__p_1">
          <iid>
            <entity eId="ii_block_iid" refersTo="#iid">DID:NFT:eip155:1_erc721
                :0xb300a43751601bd54ffee7de35929537b28e1488_2</entity>
          </iid>
          <iidDIDDoc>
            <entity eId="ii_block_iidDIDDoc" refersTo="#iidDIDDoc">diddoc.json</entity>
          </iidDIDDoc>
          <iidIssuer>
            <entity eId="ii_block_iidIssuer" refersTo="#iidIssuer">DID:NFT:eip155
                :1_erc721:0xb300a43751601bd54ffee7de35929537b28e1488_2</entity>
          </iidIssuer>
          <eidas>
            <entity eId="ii_block_eidas" refersTo="#eidas">EU COM/2021/281 final</entity>
          </eidas>
          <iidIssuerSoftware>
            <entity eId="ii_block_iidIssuerSoftware" refersTo="#iidIssuerSoftware"
                >IntelligibleIdentity1.0.1.hashdigest.json</entity>
          </iidIssuerSoftware>
          <nftSmartContract>
            <entity eId="ii_block_nftSmartContract" refersTo="#nftSmartContract"
                >IntelligibleIdentity.sol</entity>
```

Conclusions

Conclusions

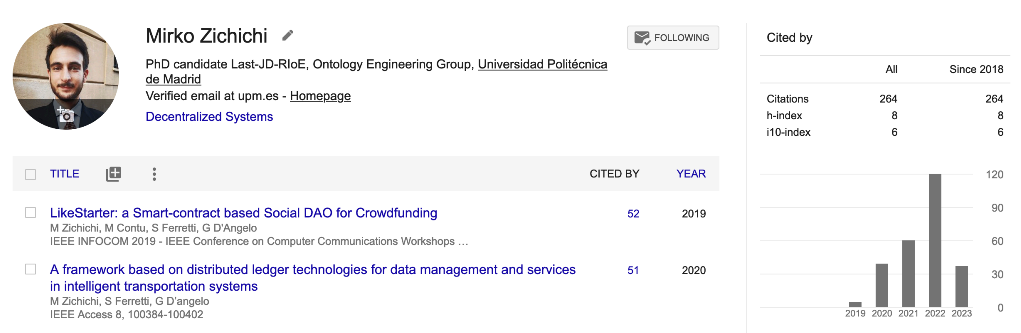
- The thesis presents a **user-centered decentralized personal information management system** that empowers data subjects and *complies with EU regulations*, such as GDPR and eIDAS.
- Decentralized systems such as *Distributed Ledger Technologies (DLTs) and Decentralized File Storage (DFS)* are used to guarantee **data sovereignty and control**.
- The design includes a **Personal Data Space (PDS)** based on encrypted personal data stored in a DFS and indexed using a **DLT-based decentralized indexing layer**.
- A network of **authorization servers and smart contracts** allows data subjects to define access to their data based on *access control lists, secret sharing, and threshold proxy re-encryption*.
- A **policy-based access control layer** based on the MPEG-21 framework and W3C Data Privacy Vocabulary (DPV) enables data subjects to express privacy policies

Future work

- Study and adapt EU legal framework for online user data protection compliance.
- Evaluate feasibility of a modularized system to comply with global data protection laws.
- Prototype a DLT-based system using latest advancements in technologies (e.g., IOTA 2.0).
- Use multi-party computation at data level instead of encryption keys.
- Design a technical assistant to provide information on personal data access and possible inferences.

Outreach

- **International Standard** - IS ISO/IEC 21000-23 Smart Contract for Media.
- **Refereed publications** -
  - 5 journal (+ 3 submitted) and 1 book chapter contributions
  - 22 conference and 5 workshop contributions



Mirko Zichichi

PhD candidate Last-JD-RIoE, Ontology Engineering Group, Universidad Politécnica de Madrid

Verified email at upm.es - Homepage

Decentralized Systems

Cited by

	All	Since 2018
Citations	264	264
h-index	8	8
i10-index	6	6

□ TITLE	CITED BY	YEAR
□ LikeStarter: a Smart-contract based Social DAO for Crowdfunding M Zichichi, M Contu, S Ferretti, G D'Angelo IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops …	52	2019
□ A framework based on distributed ledger technologies for data management and services in intelligent transportation systems M Zichichi, S Ferretti, G D'angelo IEEE Access 8, 100384-100402	51	2020

- Currently *Research Scientist* at **IOTA Foundation** developing the IOTA DLT.

Conclusion

Thank you.

Bibliography i

- Acquisti, A., Taylor, C., and Wagman, L. (2016).
  The economics of privacy.
  Journal of economic Literature, 54(2):442–92.

- Ajao, O., Hong, J., and Liu, W. (2015).
  A survey of location inference techniques on twitter.
  Journal of Information Science, 41(6):855–864.

- Christopher Allen (2016).
  The path to self-sovereign identity.

- Floridi, L. (2014).
  The fourth revolution: How the infosphere is reshaping human reality.
  OUP Oxford.

Bibliography ii

- International Association of Privacy Professionals (2011).
  Iapp information privacy certification: Glossary of common privacy terminology.
- Jurgens, D. (2013).
  That's what friends are for: Inferring location in online social media platforms based on social relationships.
  In *Seventh International AAAI Conference on Weblogs and Social Media*.
- Keßler, C. and McKenzie, G. (2018).
  A geoprivacy manifesto.
  Transactions in GIS, 22(1):3–19.

Bibliography iii

Laufer, R. S. and Wolfe, M. (1977).
Privacy as a concept and a social issue: A multidimensional developmental theory.
Journal of social Issues, 33(3):22–42.

Norberg, P. A., Horne, D. R., and Horne, D. A. (2007).
The privacy paradox: Personal information disclosure intentions versus behaviors.
Journal of consumer affairs, 41(1):100–126.

Olteanu, A.-M., Huguenin, K., Shokri, R., and Hubaux, J.-P. (2014).
Quantifying the effect of co-location information on location privacy.
In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 184–203. Springer.

Bibliography iv

Qian, J., Li, X.-Y., Zhang, C., and Chen, L. (2016).
De-anonymizing social networks and inferring private attributes using knowledge graphs.
In *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*, pages 1–9. IEEE.

Sadilek, A., Kautz, H., and Bigham, J. P. (2012).
Finding your friends and following them to where you are.
In *Proceedings of the fifth ACM international conference on Web search and data mining*, pages 723–732.

Bibliography v

Westin, A. F. (1967).
Privacy and freedom.
Atheneum.

Yamaguchi, Y., Amagasa, T., Kitagawa, H., and Ikawa, Y. (2014).
Online user location inference exploiting spatiotemporal correlations in social streams.
In *Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management*, pages 1139–1148.

Bibliography vi

Zuboff, S. (2019).
The age of surveillance capitalism: The fight for a human future at the new frontier of power.
Profile books.