Law, Science and Technology
MSCA ITN EJD n. 814177

RISE
Rights of Internet of Everything

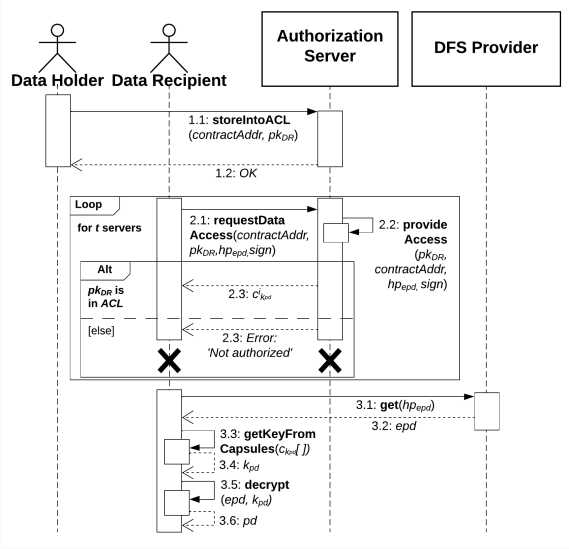
Mirko Zichichi

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

Universidad Politécnica de Madrid
University of Bologna
University of Turin

Decentralized Systems for the Protection and Portability of Personal Data

UML Diagram


Data Holder
Data Recipient
Authorization Server
DFS Provider
1.1: storeIntoACL (contractAddr, pkDR)
1.2: OK
Loop
for t servers
2.1: requestData Access(contractAddr, pkDR,hpepd,sign)
2.2: provide Access (pkDR, contractAddr, hpepd, sign)
Alt
pkDR is in ACL
2.3: c'kpd
[else]
2.3: Error: 'Not authorized'
3.1: get(hpepd)
3.2: epd
3.3: getKeyFrom Capsules(ckpd[ ])
3.4: kpd
3.5: decrypt (epd, kpd)
3.6: pd

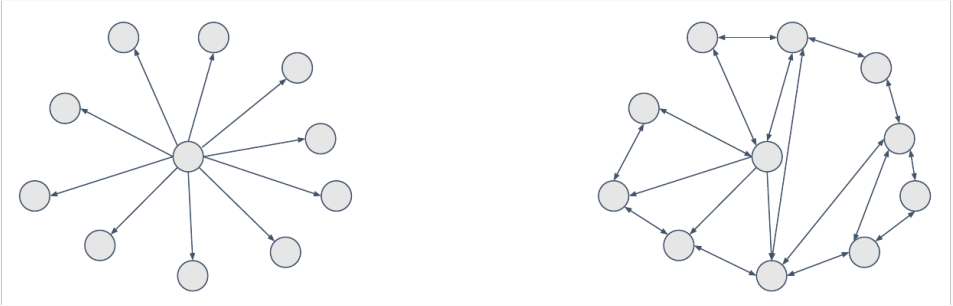
Single point of failure

Single point of failure

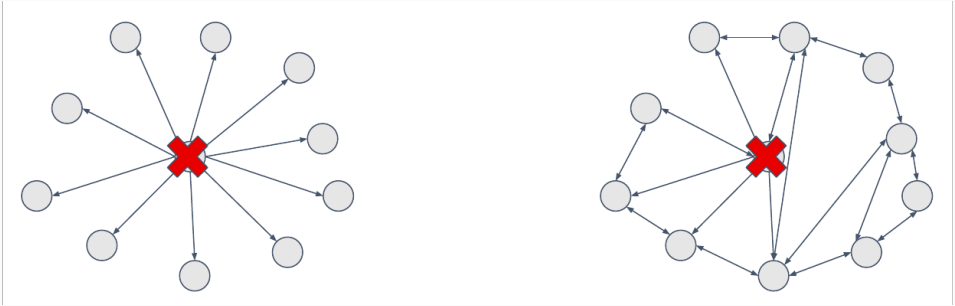
Single point of failure

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

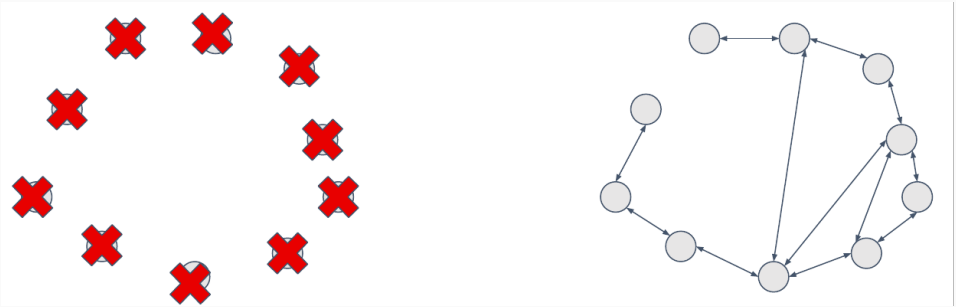
Single point of failure



Single point of failure



Single point of failure



But what can its opposite, de-centralization, do?

- Systems theory: a system is decentralized when lower-level components operate on **local** information to achieve **global** goals.

But what can its opposite, de-centralization, do?

- Systems theory: a system is decentralized when lower-level components operate on **local** information to achieve **global** goals.
- Such a system operates through the **emergent** behavior of its component parts rather than as a result of the *influence of a centralized part.*

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*.

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*.
- Nakamoto has made possible the **coordinated operation** of nodes in a network without needing to control their access to the system itself, i.e., a *permissionless transactional decentralized system*.

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*.
- Nakamoto has made possible the **coordinated operation** of nodes in a network without needing to control their access to the system itself, i.e., a *permissionless transactional decentralized system*.
  - Transactions of information are placed in a block

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*.
- Nakamoto has made possible the **coordinated operation** of nodes in a network without needing to control their access to the system itself, i.e., a *permissionless transactional decentralized system*.
  - Transactions of information are placed in a block
  - Other network nodes accept only if it “solves a puzzle”

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*.
- Nakamoto has made possible the **coordinated operation** of nodes in a network without needing to control their access to the system itself, i.e., a *permissionless transactional decentralized system*.
  - Transactions of information are placed in a block
  - Other network nodes accept only if it "solves a puzzle"
  - Solving this "crypto-puzzle" requires intensive computation work that consumes time.

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*.
- Nakamoto has made possible the **coordinated operation** of nodes in a network without needing to control their access to the system itself, i.e., a *permissionless transactional decentralized system*.
  - Transactions of information are placed in a block
  - Other network nodes accept only if it "solves a puzzle"
  - Solving this "crypto-puzzle" requires intensive computation work that consumes time.
- This creates a **consensus**, an *order within decentralization*, i.e., a *chain* of blocks.

Bitcoin

- Transactions of information are placed in a block

Bitcoin

- Transactions of information are placed in a block
- Other network nodes accept only if it “solves a puzzle”

Bitcoin

- Transactions of information are placed in a block
- Other network nodes accept only if it “solves a puzzle”
- Solving this “crypto-puzzle” requires intensive computation work that consumes time.

Bitcoin

- Transactions of information are placed in a block
- Other network nodes accept only if it “solves a puzzle”
- Solving this “crypto-puzzle” requires intensive computation work that consumes time.
- This creates a **consensus**, an *order within decentralization*, i.e., a *chain* of blocks.

Is it any good?

- Criticisms: issue of trust.

Is it any good?

- Criticisms: issue of trust.
- Blockchain attempts to replace trust with code, i.e., consensus algorithm

Is it any good?

- 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"*):

Is it any good?

- 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.

Is it any good?

- 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

Is it any good?

- 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.

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.

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:

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

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).

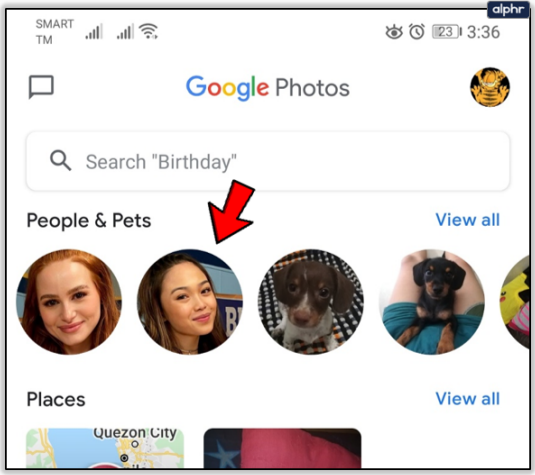
*Honest**

- *but curious

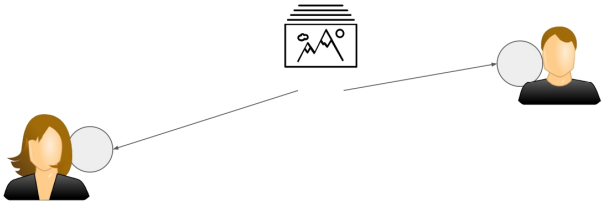
*Honest**

- *but curious
-

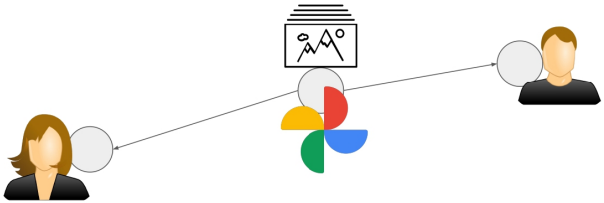
Photo storage



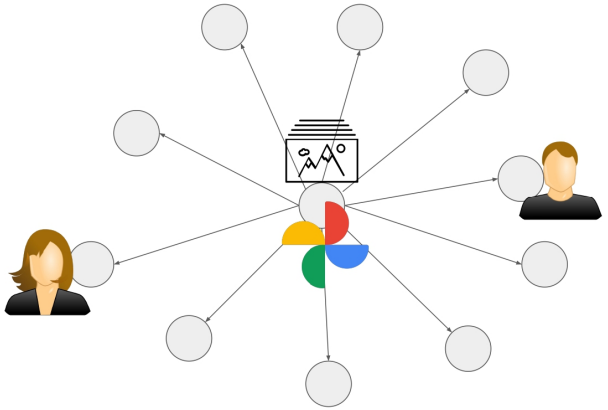
Centralized



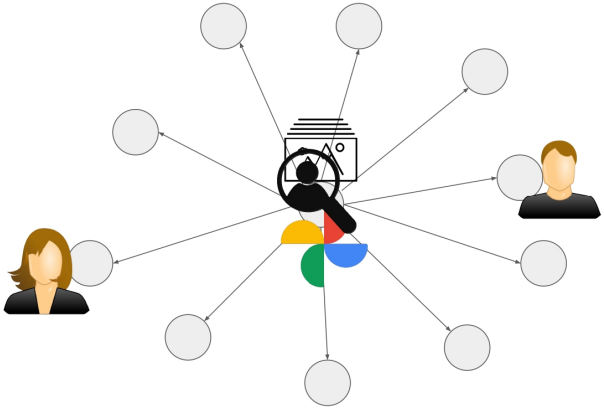
Centralized



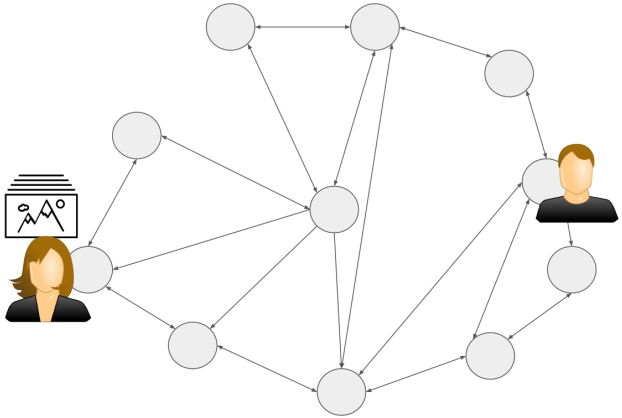
Centralized



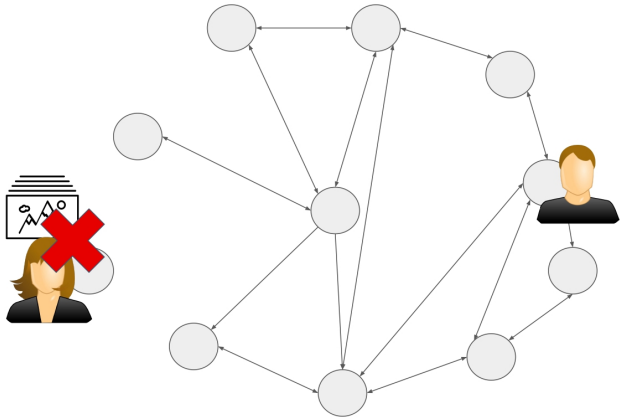
Centralized



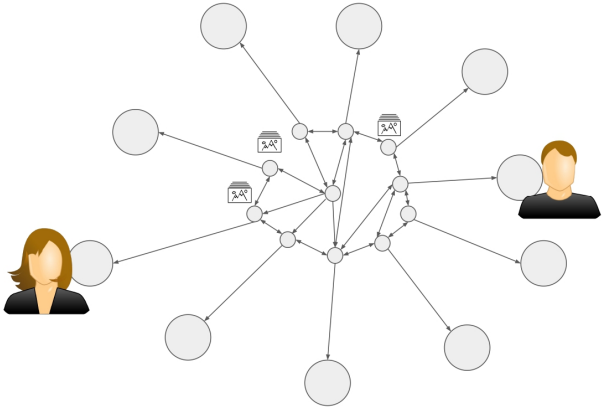
De-entralized



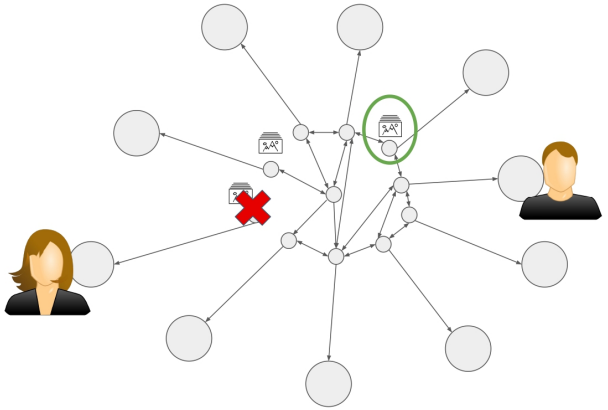
De-entralized



Permissioned



Permissioned



Permissioned blockchains to the rescue

- In permissioned decentralized systems, the nodes executing the consensus mechanism are identified and access to the P2P network is restricted.

Permissioned blockchains to the rescue

- In permissioned decentralized systems, the nodes executing the consensus mechanism are identified and access to the P2P network is restricted.
- Different actors with different interests (possibly clashing between themselves) constantly monitor their “adversary-peers”

Permissioned blockchains to the rescue

- In permissioned decentralized systems, the nodes executing the consensus mechanism are identified and access to the P2P network is restricted.
- 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.

Permissioned blockchains (are not used for the average crypto meme)

- **single source of verifiable truth** among de-centralized organizations.

Permissioned blockchains (are not used for the average crypto meme)

- **single source of verifiable truth** among de-centralized organizations.
- the system **authority can be distributed** among many trusted actors so that the compromise of one or even a few authorities does not destroy the consensus.

Permissioned blockchains (are not used for the average crypto meme)

- **single source of verifiable truth** among de-centralized organizations.
- the system **authority can be distributed** among many trusted actors so that the compromise of one or even a few authorities does not destroy the consensus.
- **intrinsic cryptographical properties** of blockchains can enable distributed safe computation and data minimization.

Permissioned blockchains (are not used for the average crypto meme)

- **single source of verifiable truth** among de-centralized organizations.
- the system **authority can be distributed** among many trusted actors so that the compromise of one or even a few authorities does not destroy the consensus.
- **intrinsic cryptographical properties** of blockchains can enable distributed safe computation and data minimization.
- the networked collaboration environment can be easily exploited for the **audit and accountability** of operations.

Permissioned blockchains (are not used for the average crypto meme)

- **single source of verifiable truth** among de-centralized organizations.
- the system **authority can be distributed** among many trusted actors so that the compromise of one or even a few authorities does not destroy the consensus.
- **intrinsic cryptographical properties** of blockchains can enable distributed safe computation and data minimization.
- the networked collaboration environment can be easily exploited for the **audit and accountability** of operations.
- P2P networks offer an essential solution for **data resiliency**.

De-centralize

Solving one threat at a time: de-centralize personal data management

- Blockchains can provide functionalities that are impossible in traditional cloud services.

Solving one threat at a time: de-centralize personal data management

- Blockchains can provide functionalities that are impossible in traditional cloud services.
- Favor the creation of **decentralized Personal Information Management Systems (PIMS)**, guaranteeing, by design, data sovereignty and enabling users to control what personal data they want to share.

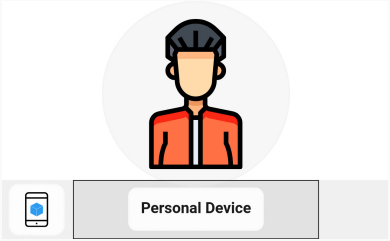
Solving one threat at a time: de-centralize personal data management

- Blockchains can provide functionalities that are impossible in traditional cloud services.
- Favor the creation of **decentralized Personal Information Management Systems (PIMS)**, guaranteeing, by design, data sovereignty and enabling users to control what personal data they want to share.
- Allow data collectors to prove their compliance with regulations.

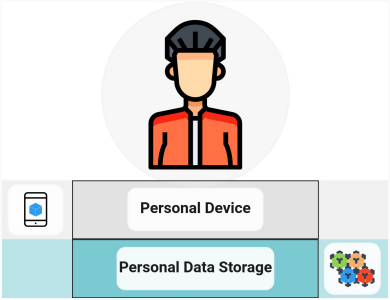
Solving one threat at a time: de-centralize personal data management

- Blockchains can provide functionalities that are impossible in traditional cloud services.
- Favor the creation of **decentralized Personal Information Management Systems (PIMS)**, guaranteeing, by design, data sovereignty and enabling users to control what personal data they want to share.
- Allow data collectors to prove their compliance with regulations.
- Benefit the creation of a single data market that capitalizes on **data interoperability between data spaces** for the *social and economic good*.

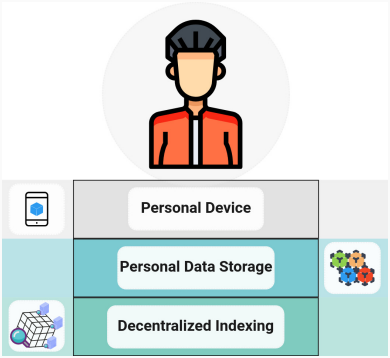
Internet of Persons - Person



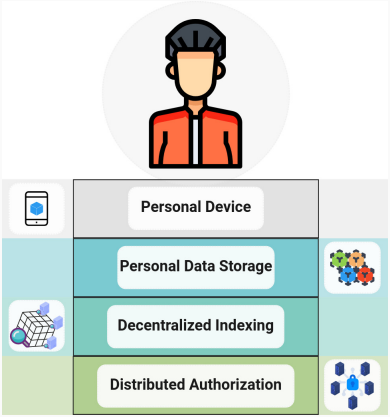
Internet of Persons - Person



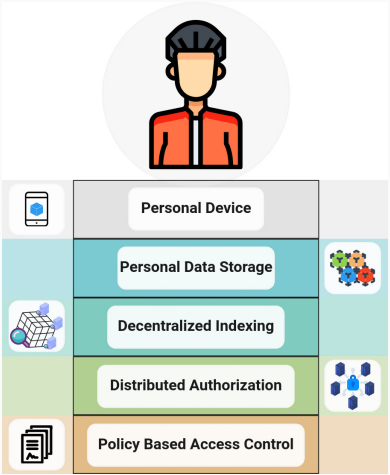
Internet of Persons - Person



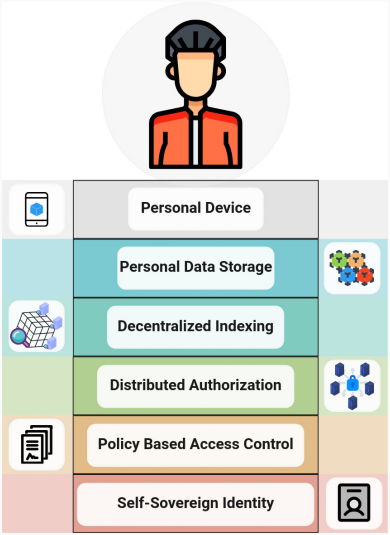
Internet of Persons - Person



Internet of Persons - Person

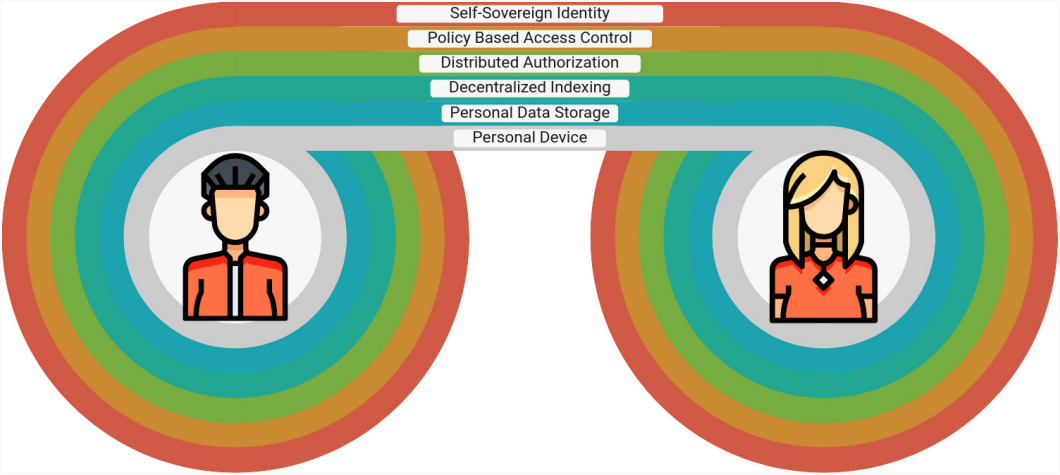


Internet of Persons - Person

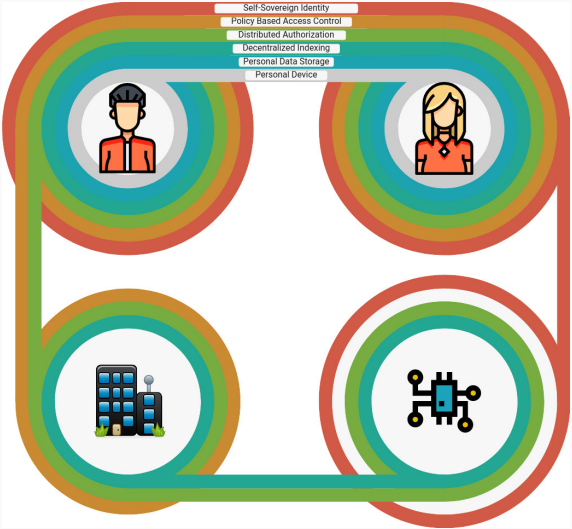


Internet of Persons - Person

Internet of Persons - Data Sharing



Internet of Persons - Data Sharing



Thesis

Thesis - Chapters 1,2,3

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.

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.

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).

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.

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, which allows retrieving contents stored in DLTs and/or DFS.

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, 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 (Hypercube DHT).

Chapter 6 - Distributed Authorization

Access to the data stored on a PDS can be allowed by the data holder through **smart contracts**. Contributions:

1. First, we describe a novel PIMS based on a multi-DLT GDPR-compliant design. We propose an extension of our PDS and decentralized indexing system with a component for the secure control of access to personal data. These components are aggregated through a novel multi-DLT system where a permissioned DLT provides the authorization mechanism, and a permissionless DLT provides security.

Chapter 6 - Distributed Authorization

Access to the data stored on a PDS can be allowed by the data holder through **smart contracts**. Contributions:

1. First, we describe a novel PIMS based on a multi-DLT GDPR-compliant design. We propose an extension of our PDS and decentralized indexing system with a component for the secure control of access to personal data. These components are aggregated through a novel 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.

Chapter 6 - Distributed Authorization

Access to the data stored on a PDS can be allowed by the data holder through **smart contracts**. Contributions:

1. First, we describe a novel PIMS based on a multi-DLT GDPR-compliant design. We propose an extension of our PDS and decentralized indexing system with a component for the secure control of access to personal data. These components are aggregated through a novel 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 (Ethereum).

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).*

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.

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.

Chapter 7 - 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 ;
```

Chapter 7 - 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>
```

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 decentralised environments for the purpose of providing, requesting and obtaining qualified data in order to negotiate and/or execute electronic transactions.

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 decentralised 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).

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 decentralised 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.

Conclusion

Outreach

- **International Standard** - IS ISO/IEC 21000-23 Smart Contract for Media.

Outreach

- **International Standard** - IS ISO/IEC 21000-23 Smart Contract for Media.
- **Refereed publications** -

Outreach

- **International Standard** - IS ISO/IEC 21000-23 Smart Contract for Media.
- **Refereed publications** -
  - 4 journal and 1 book chapter contributions

Outreach

- **International Standard** - IS ISO/IEC 21000-23 Smart Contract for Media.
- **Refereed publications** -
  - 4 journal and 1 book chapter contributions
  - 19 conference and 5 workshop contributions

Outreach

- **International Standard** - IS ISO/IEC 21000-23 Smart Contract for Media.
- **Refereed publications** -
  - 4 journal and 1 book chapter contributions
  - 19 conference and 5 workshop contributions

Mirko Zichichi

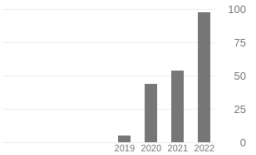
FOLLOWING

PhD candidate Last-JD-RIoE, Ontology Engineering Group, Universidad Politécnica de Madrid
Verified email at upm.es - Homepage
Decentralized Systems

TITLE	CITED BY	YEAR
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	43	2020
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 …	37	2019
A distributed ledger based infrastructure for smart transportation system and social good M Zichichi, S Ferretti, G D'Angelo 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC …	31	2020

Cited by

	All	Since 2017
Citations	201	201
h-index	8	8
i10-index	6	6



Public access VIEW ALL

Conclusion

Thank you.