Law, Science and Technology
MSCA ITN EJD n. 814177


Mirko Zichichi[1,2], Stefano Ferretti[3],
Gabriele D'Angelo[2], Víctor Rodríguez-Doncel[1]

[1]Universidad Politécnica de Madrid
[2]University of Bologna
[3]University of Urbino "Carlo Bo"

# Personal Data Access Control Through Distributed Authorization

# Overview

1. Introduction
2. Architecture Design
3. Experimental Evaluation
4. Conclusion

# Introduction

# Personal Data Sovereignty

**Data-driven technologies** are having a significant impact on the economy and society and individuals are the main sources of such data:

- EU's **GDPR**
- **absence** of technical tools and standards
- make it easy to exercise **one's rights**

Our aim
$\rightarrow$**sovereignty over their data**
$\rightarrow$data **confidentiality**.

**Personal Information Management System (PIMS)**
based on a distributed software architecture

# Distributed Ledger Technologies and Smart Contracts

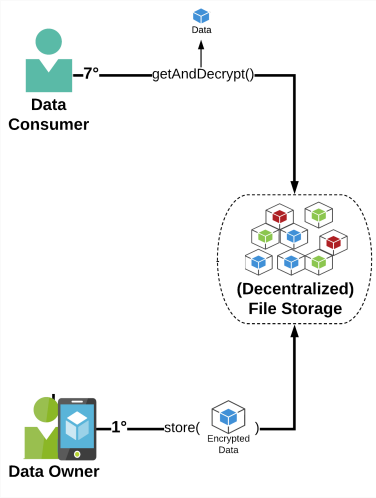
- **Distributed Ledger Technologies (DLTs)**:
  immutable data ledger + untampered data availability
- **DLTs** shift trust from a human intermediary to a protocol
- **Smart contracts**:
  immutable set of **instructions executed deterministically by several participants** in a network

# Access Control Mechanisms

- **Secret Sharing (SS)**:
  - $(t, n)$-threshold scheme
  - secret reconstructed using any subset of $t$ (with $t \leq n$) shares, but no subset $< t$
  - mostly honest nodes $\rightarrow$ privacy
- **Proxy Re-Encryption (PRE)**:
  - a proxy transforms a ciphertext $c$, encrypted with a public key $pk_1$, into a ciphertext decryptable with a private key $sk_2$, without learning anything about the plaintext
  - re-encryption key $rk_{1-2}$, generated by the data owner

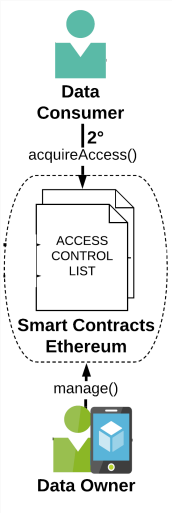
# Architecture Design

# Data Storage System




- Personal data → *encrypted* + off-chain
- In a (possibly decentralized) **File Storage (FS)** and then referenced in a DLT
- **Digest** → verification of **integrity** + **pepper and salt**
- **GDPR** → requires the modification or deletion of data under certain circumstances

# Smart Contract Access Control List

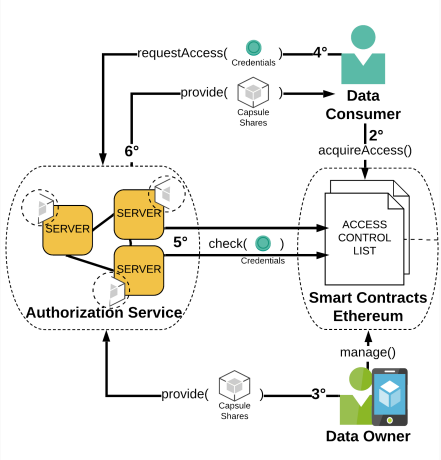



- **Ethereum smart contracts** → access to the data enabled by the owner or purchased
- The smart contract maintains an **Access Control List (ACL)** that represents the rights to access a bundle of data.
- Once a **consumer is listed in the ACL**, he can access data through an access key, which is provided by the authorization service.

# Cryptosystem

- **Hybrid encryption scheme** ← symmetric enc. efficiency + asymmetric enc. benefits
- **Key Encapsulation Mechanism (KEM)** →
  asymmetric public key part to encrypt a key
- **Data Encapsulation Mechanism (DEM)** →
  symmetric secret key part to encrypt actual data

# Authorization Service Network



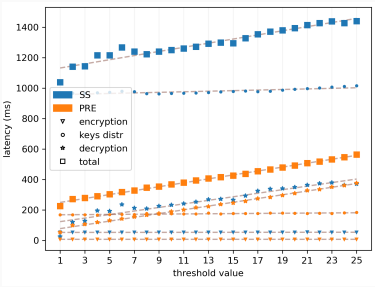

- Enforces the **access rights** specified in the ACLs
- A valid data consumer request enact the release of the "**capsule**" that holds the $k_{DEM}$ secret key, needed to decrypt the desired data
  - **SS** - splits capsule in $n$ shares, but only $t$ shares ($t < n$) are needed to "open" it
  - **Threshold PRE** - splits capsule in in $n$ shares and uses a $(t, n)$-threshold scheme with $t$ "re-encryption shares" to re-encrypt it for consumer

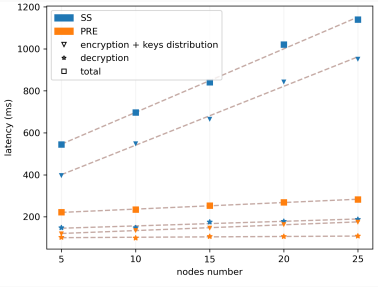
# Experimental Evaluation

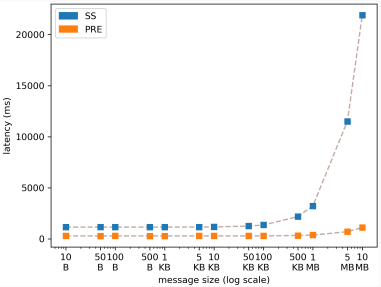
# Access Control Network Performances

- We measured the amount of time required to perform access control operations
- We resort to:
  - **SS** $\rightarrow$ OpenEthereum (Parity) client Secret Store
  - **Threshold PRE** $\rightarrow$ NuCypher
- network of 25 interconnected nodes
- emulated from 10 to 100 data consumers asking for access to some data

# Threshold, number of nodes, message size variations



# Conclusion

# Conclusion

- Architectural solution for a PIMS based on a **decentralized approach for managing access to data**
- We have focused on **data protection through encryption**, using two different schemes: SS and PRE
- In respect to SS, **PRE is**:
  - more efficient when increasing the threshold value
  - more scalable
  - faster when increasing the size of the messages
- In future work we will pursue a more complex policy expression framework (instead of ACL)