Access Control on Smart Contract

Paolo Mori, Andrea De Salve
Consiglio Nazionale delle Ricerche

Laura Ricci, Damiano Di Francesco Maesa, Andrea Lisi
Dipartimento di Informatica, Università di Pisa

Access Control

Technique to decide whether a Subject requesting to perform an Action on a Resource in a given Context holds the right the perform it

Access Control

Technique to decide whether a Subject requesting to perform an Action on a Resource in a given Context holds the right the perform it

Subject

Resources

Access Control

Technique to decide whether a Subject requesting to perform an Action on a Resource in a given Context holds the right the perform it

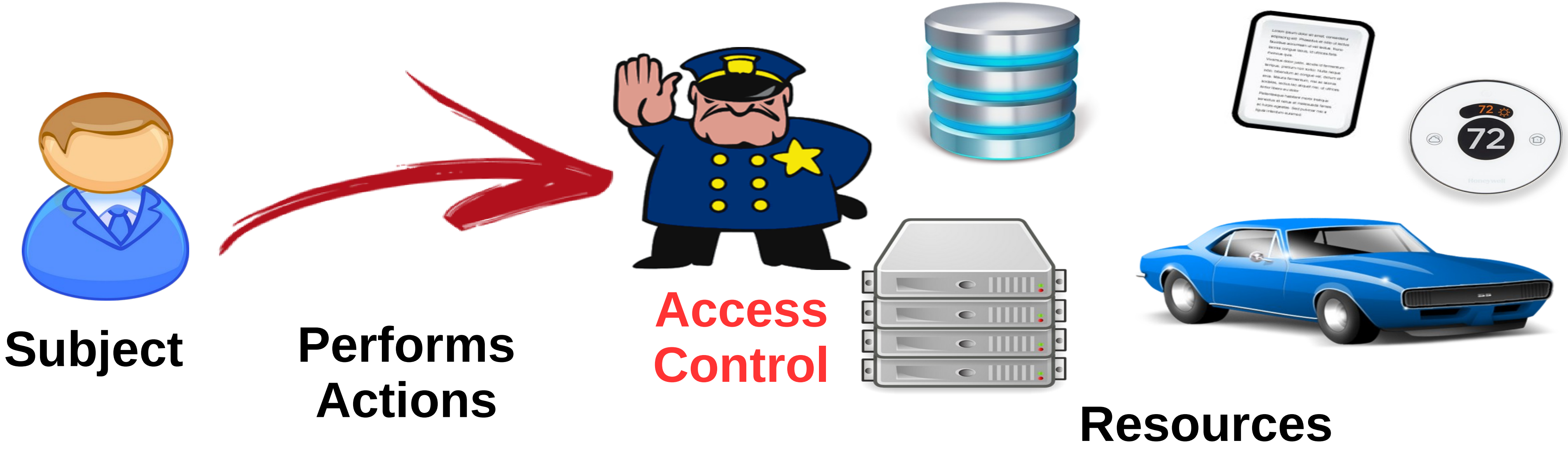
Subject

Performs Actions

Resources

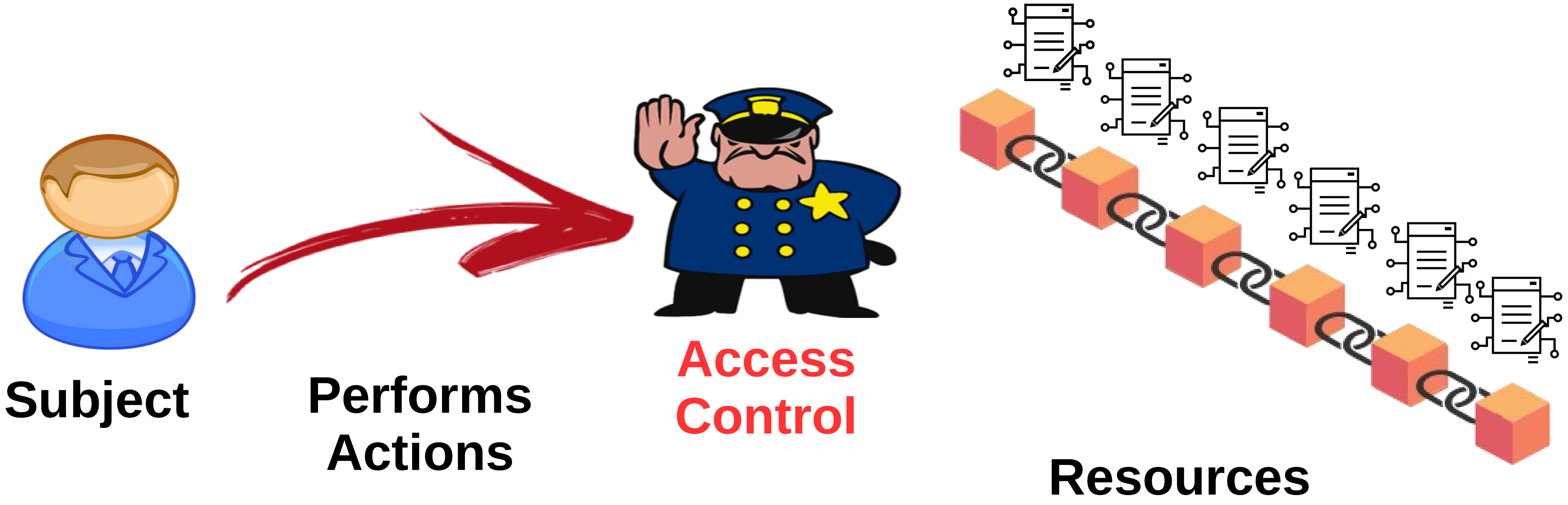
Access Control

Technique to decide whether a Subject requesting to perform an Action on a Resource in a given Context holds the right the perform it



Access Control

Technique to decide whether a Subject requesting to perform an Action on a Resource in a given Context holds the right the perform it



Blockchain-based Access Control Systems

- The access control system logic is a smart contract on the blockchain
- The access control policies are on the blockchain
- The decision factors are on the blockchain
- The access decision process is executed on the blockchain

Blockchain-based Access Control Systems

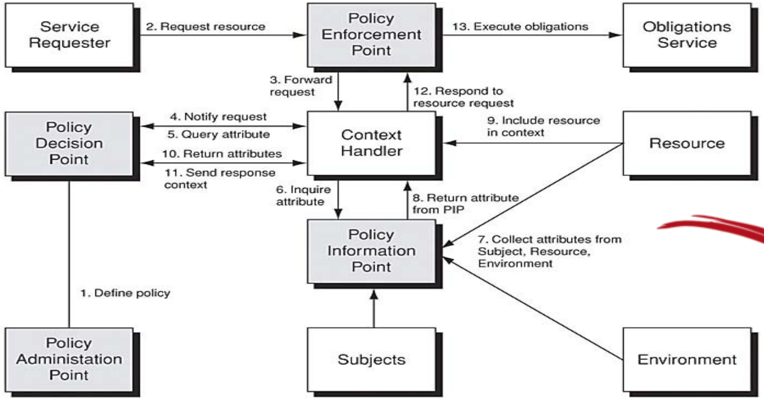
- The access control system logic is a smart contract on the blockchain
- The access control policies are on the blockchain
- The decision factors are on the blockchain
- The access decision process is executed on the blockchain

Blockchain Brings to Access Control Systems

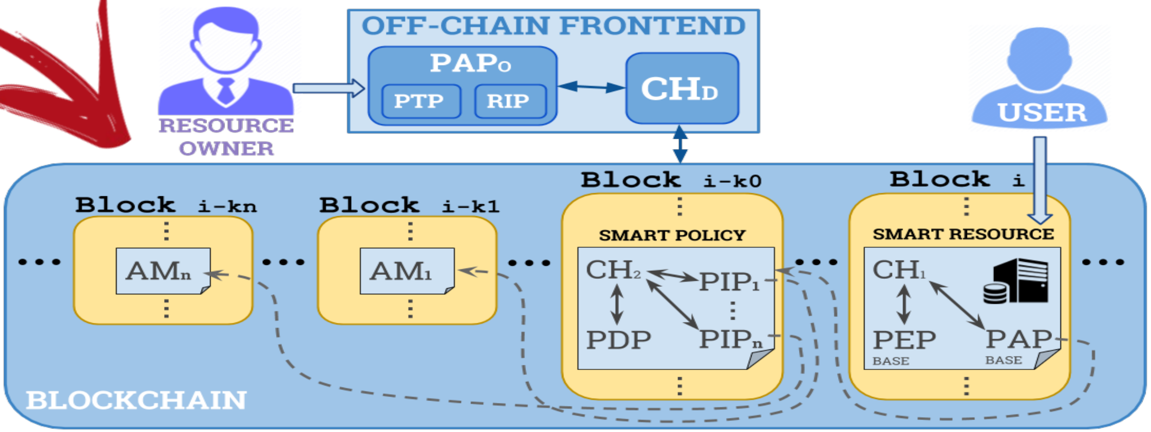
- Trusted execution environment
- Transparency
- Auditability

Attribute Based Access Control on Blockchain

- Decision factors are attributes paired to subjects and objects
- OASIS XACML is a well known standard for ABAC



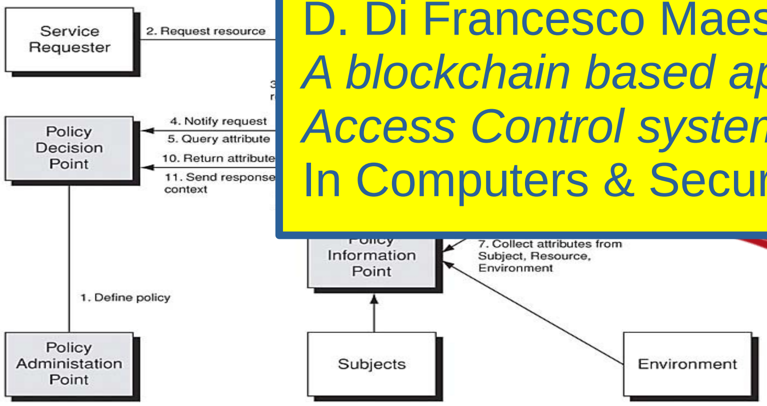
OASIS XACML
reference architecture



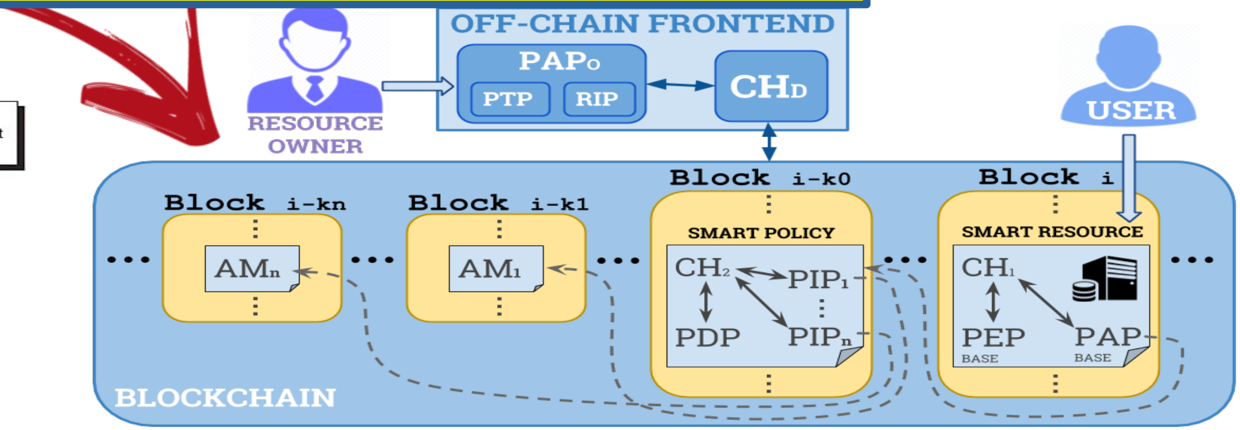
Attribute Based Access Control on Blockchain

- Decision factors are attributes paired to subjects and objects
- OASIS XACML is a well known standard for ABAC

D. Di Francesco Maesa, P. Mori, L. Ricci:
A blockchain based approach for the definition of auditable Access Control systems.
In Computers & Security, Elsevier Science, vol. 84, 2019

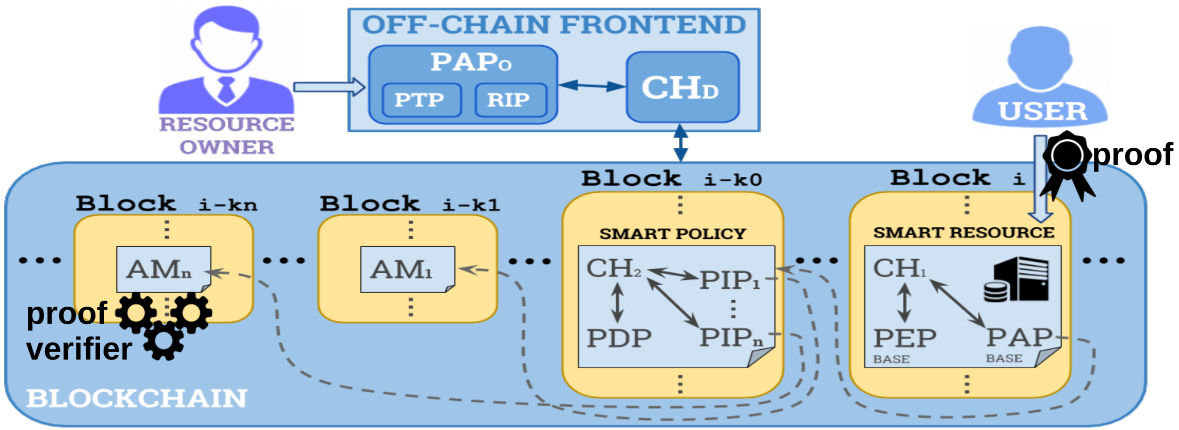


XACML reference architecture



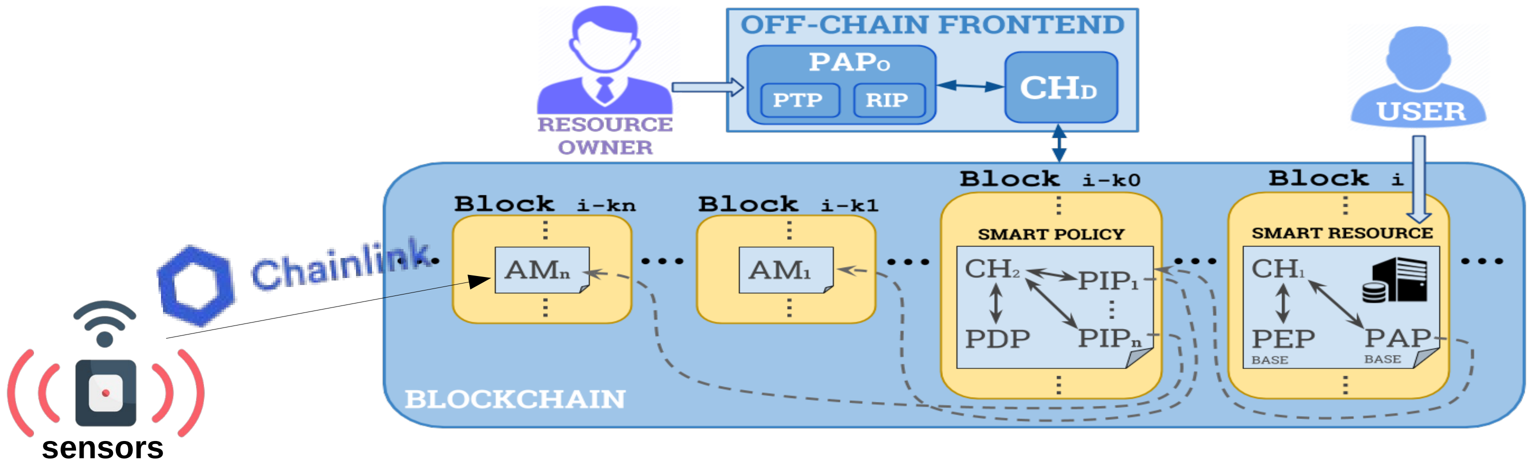
Attribute Based Access Control on Blockchain with **Privacy** Preserving Attribute Management

- Some user attributes could be **sensitive information**
- Zokrates is used to allow zero-knowledge evaluation of conditions on sensitive attributes



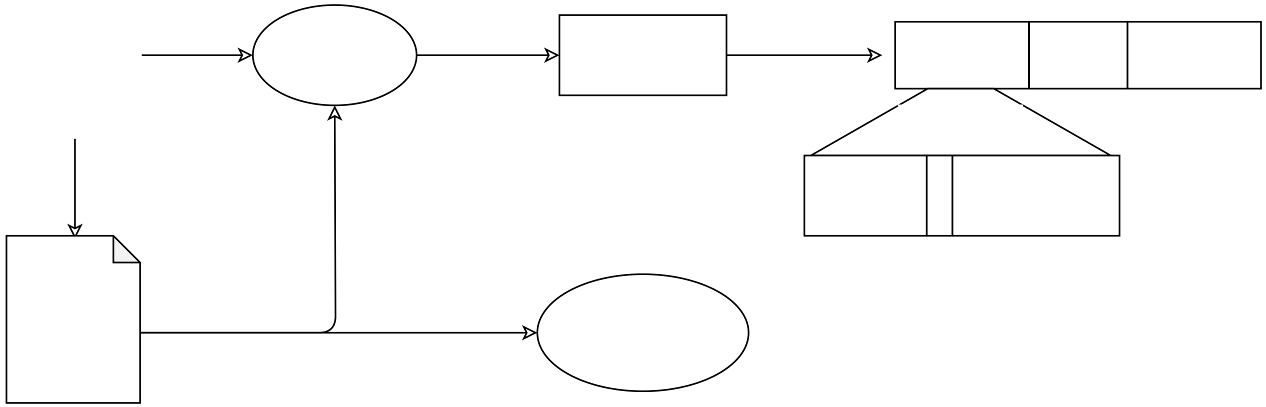
Attribute Based Access Control on Blockchain with **Externally Produced Attributes**

- Some attribute values are produced outside the blockchain (physical sensors)
- Chainlink is used to import externally produced values on the blockchain



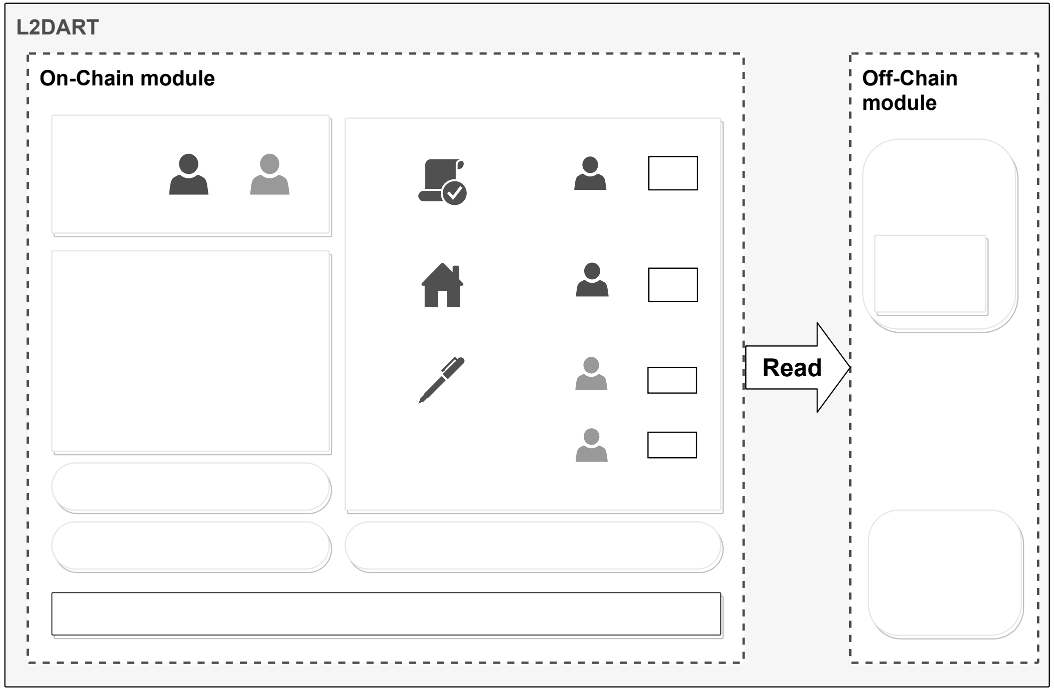
RTML-based Access Control on Blockchain

- Decision factors are roles paired to the subject
- Actors define Trust credentials
- Trust credentials allow to compute roles dinamically (RTML)



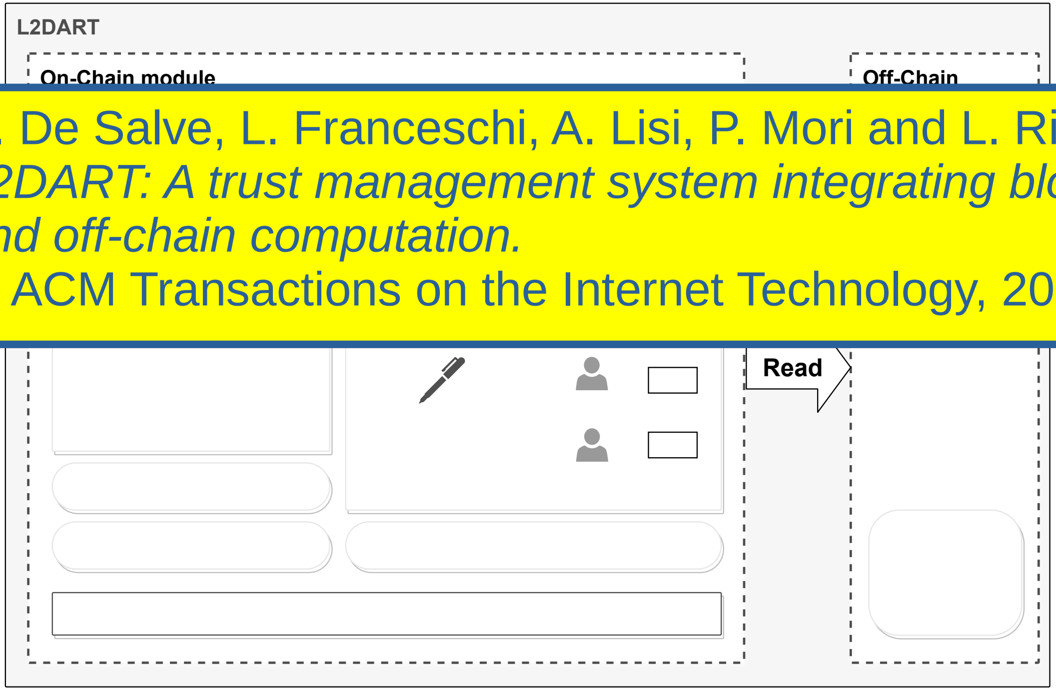
RTML-based Access Control on Blockchain with **Off-chain** Computation of Roles

- Roles computation is performed off-chain, along with the proof
- The proof is verified on-chain



RTML-based Access Control on Blockchain with **Off-chain** Computation of Roles

- Roles computation is performed off-chain, along with the proof
- The proof is verified on-chain



A. De Salve, L. Franceschi, A. Lisi, P. Mori and L. Ricci:
L2DART: A trust management system integrating blockchain and off-chain computation.
In ACM Transactions on the Internet Technology, 2022

Thank you!