# Exploiting Blockchain Technology to Design an Attribute based Access Control System


**Paolo Mori**
Istituto di Informatica e Telematica
Consiglio Nazionale delle Ricerche

**Damiano Di Francesco Maesa**
Department of Computer Science and Technology
University of Cambridge, UK

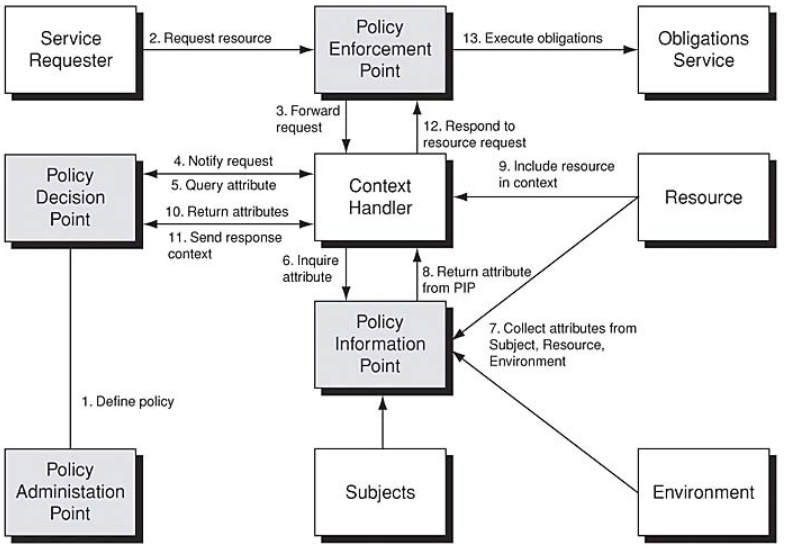
**Laura Ricci**
Dipartimento di Informatica
Università di Pisa

# Agenda

- Background
  - Attribute Based Access Control
  - XACML
- Our Proposal
  - Implementation of the XACML based Access Control Service exploiting the Blockchain tecnology
  - Examples of Application Scenarios
  - Experimental Results

# Background:

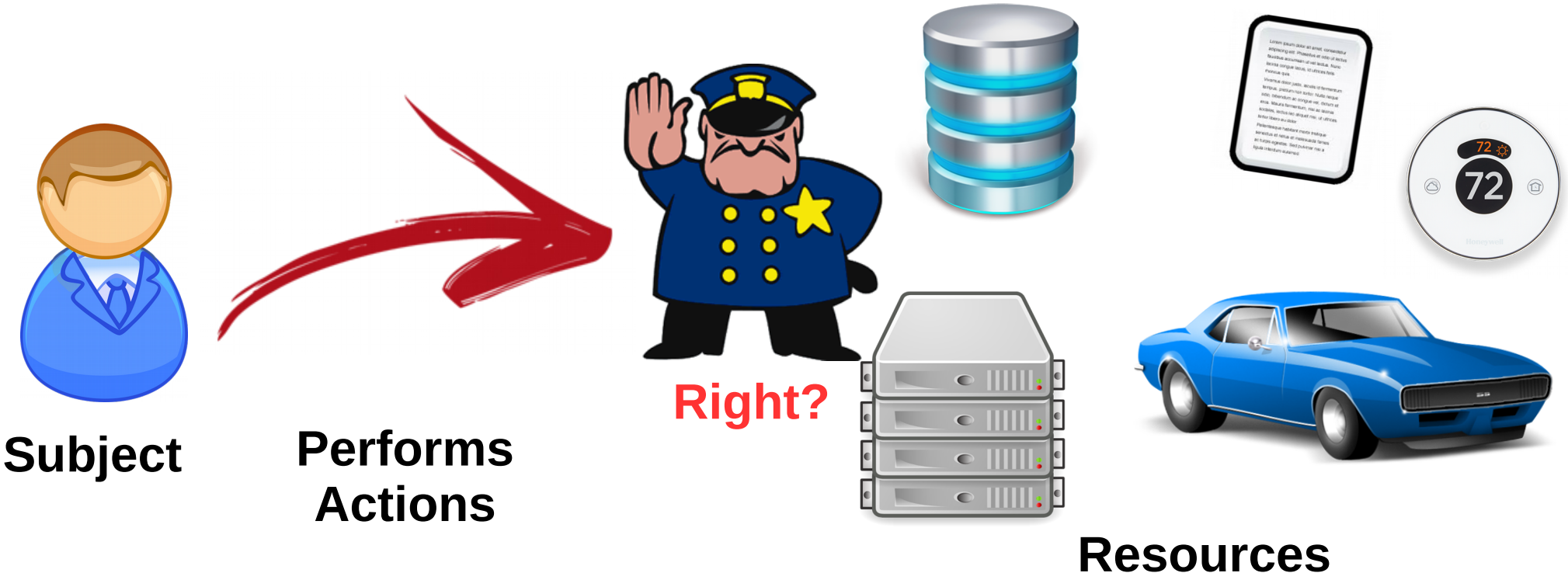
# Access Control and XACML




OASIS

# 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



# **Attribute Based** Access Control (ABAC)

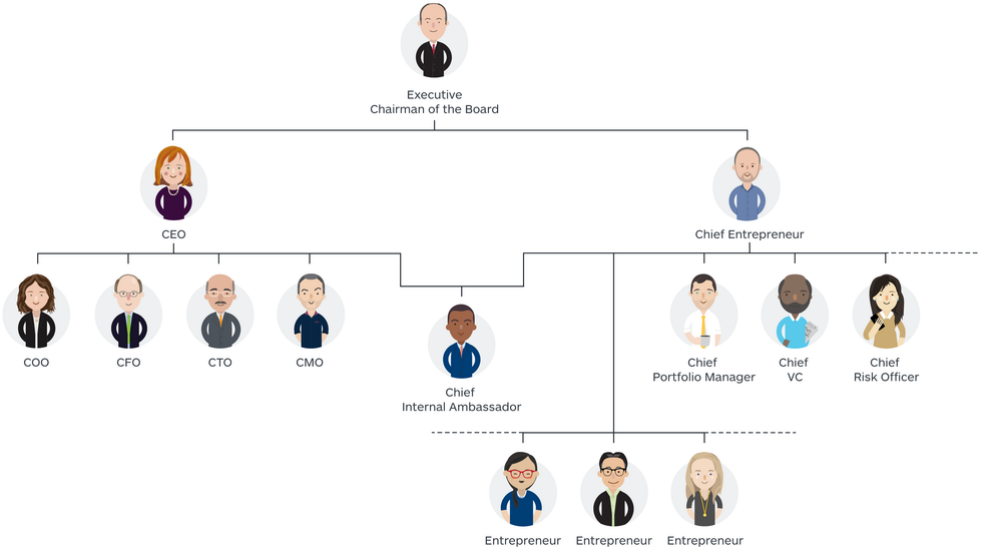
An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publication 800-162

# Attributes

- Attributes represent characteristics of the
  - Subjects
  - Resources
  - Actions
  - Environment
- Examples:
  - Subject




    - Role (e.g., in a company: Worker, Employee, Executive, CEO...)
    - Projects assigned to the subject
    - Physical location
  - Resources
    - Owner/producer
    - Number of copies of a document
    - Project of a document
    - Security classification

# Extensible Access Control Markup Language 3.0 (XACML)

**XACML** defines:

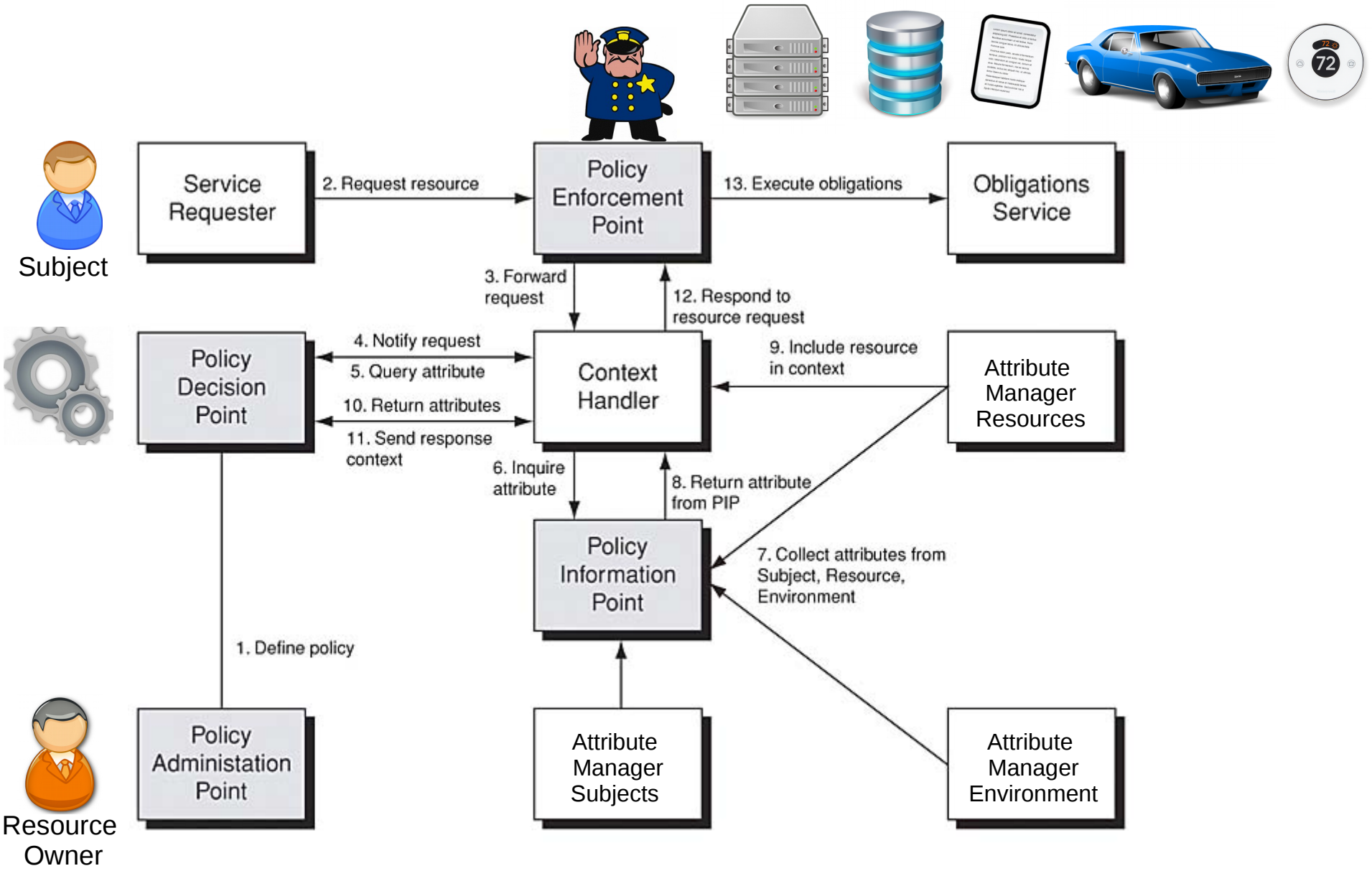
- A XML-based Language to express Attribute based Access Control Policies
- A reference architecture for the Access Control Framework

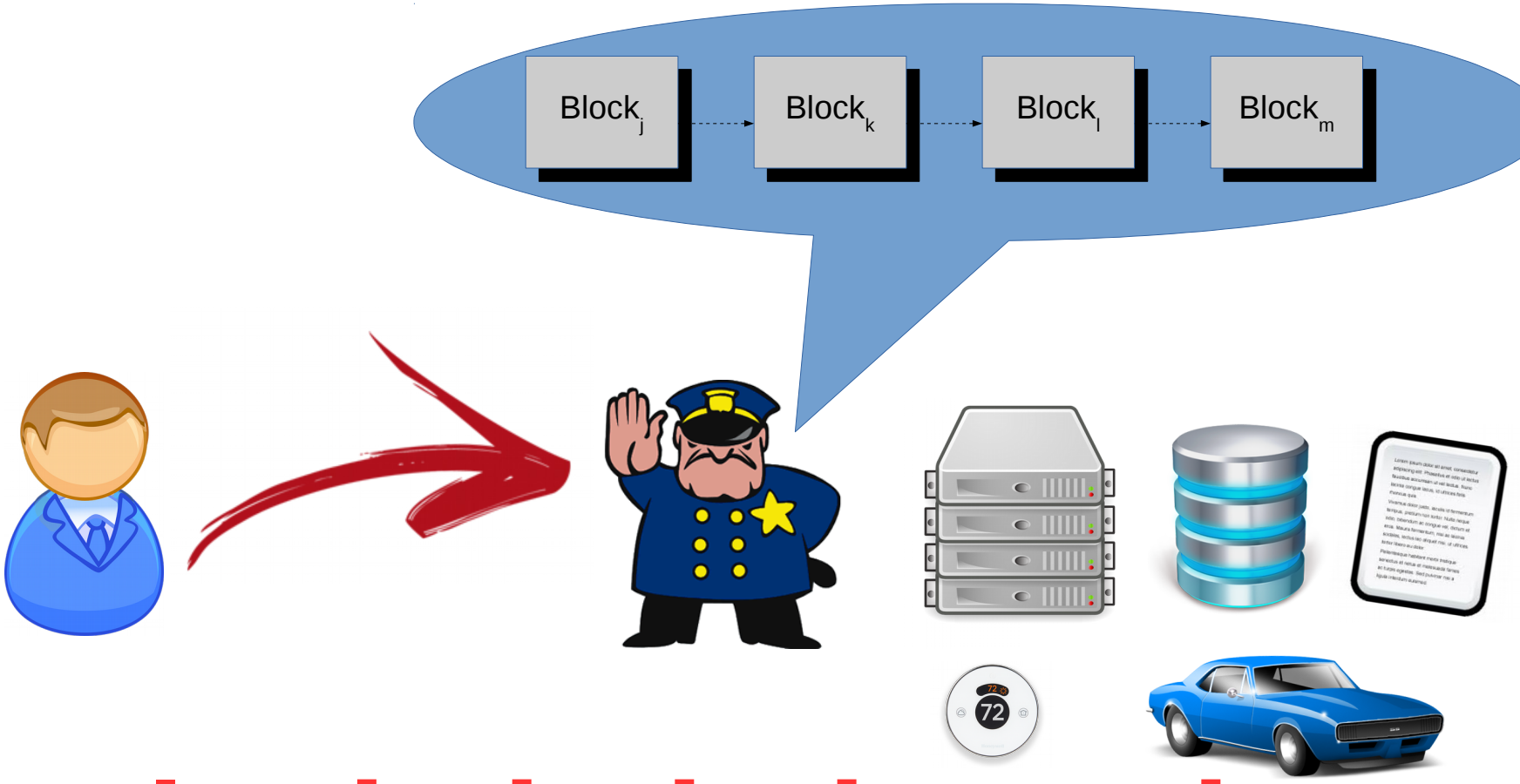

eXtensible Access Control Markup Language (XACML) Version 3.0 Plus Errata 01. OASIS Standard incorporating Approved Errata. 12 July 2017

# XACML: Policy Example

**<Condition>**
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and"> <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal"> <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only"> <AttributeDesignator
AttributeId="**urn:oasis:names:tc:xacml:1.0:subject:subject-location**"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/> </Apply>
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">**EUROPA**</AttributeValue> </Apply>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal"> <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only"> <AttributeDesignator
AttributeId="**urn:oasis:names:tc:xacml:1.0:subject:subject-role**"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/> </Apply>
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">**Executive**</AttributeValue>
</Apply></Apply>
</Condition>
</Rule>

# XACML: Reference Architecture






# Blockchain based Access Control

# Main Idea

Implement a XACML based Access Control Framework exploiting the Blockchain technology

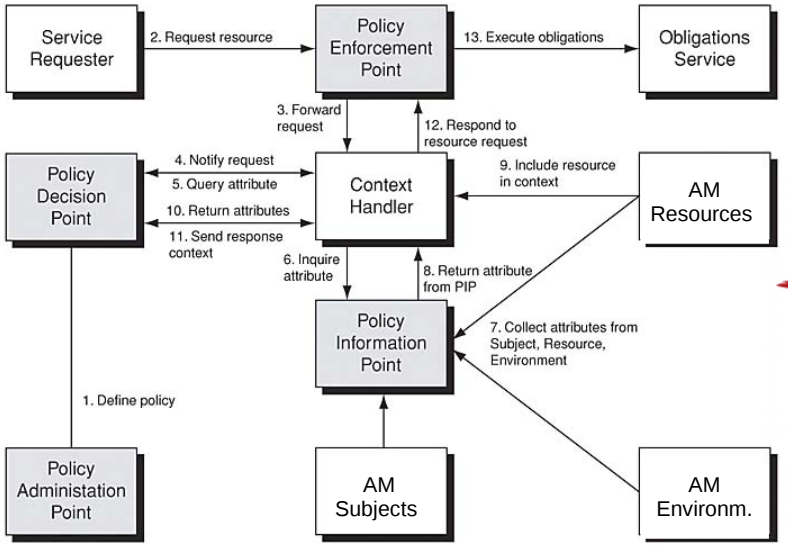
# Advantages

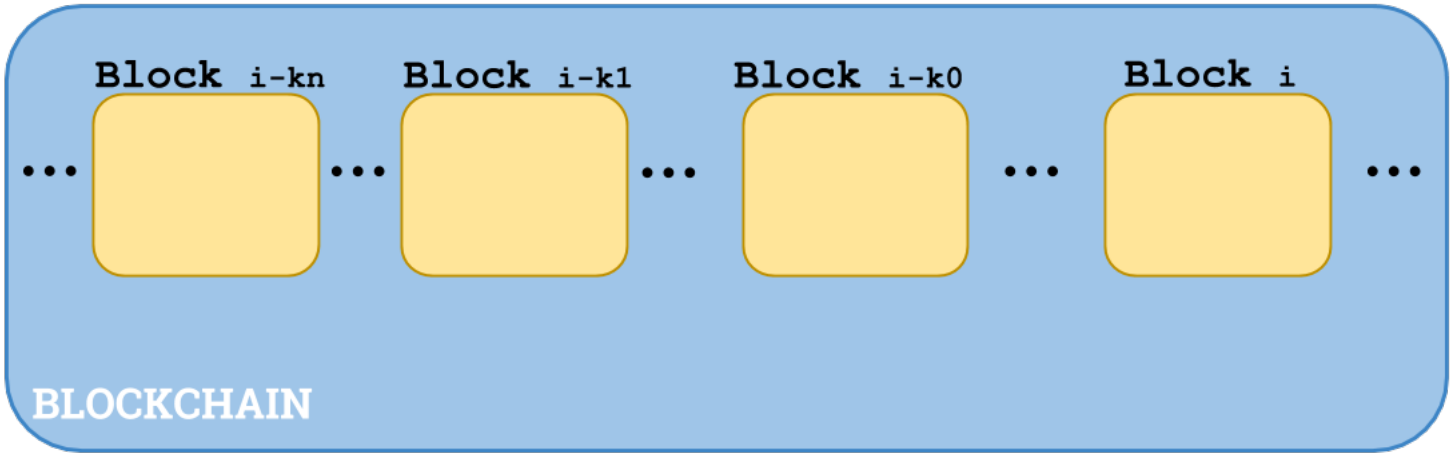
- Outsource the access control decision process
- No need of a Trusted third party to perform the access control decision process
- Auditability

# Drawbacks

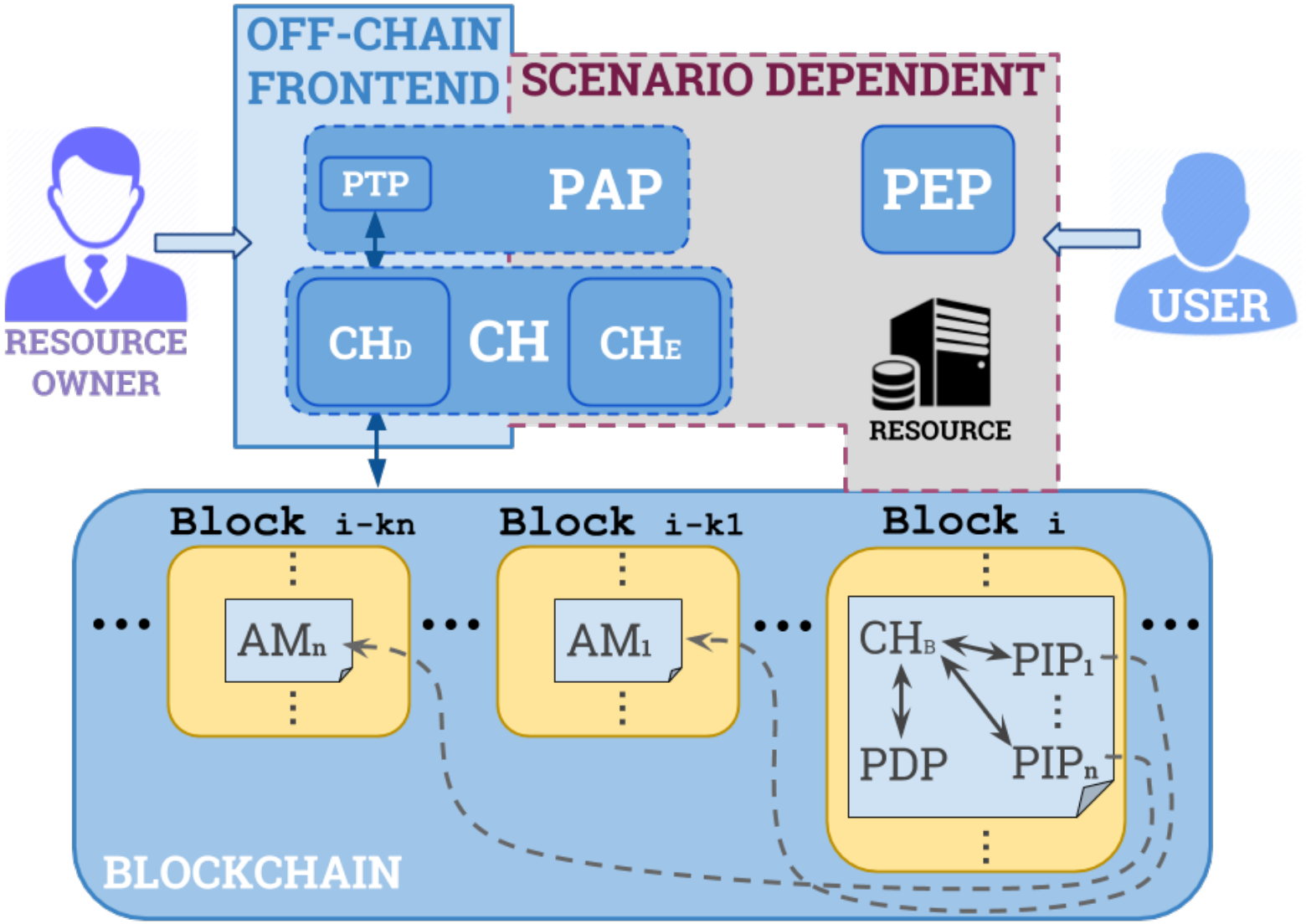
- Cost
- Performance
- Privacy

# Framework Design



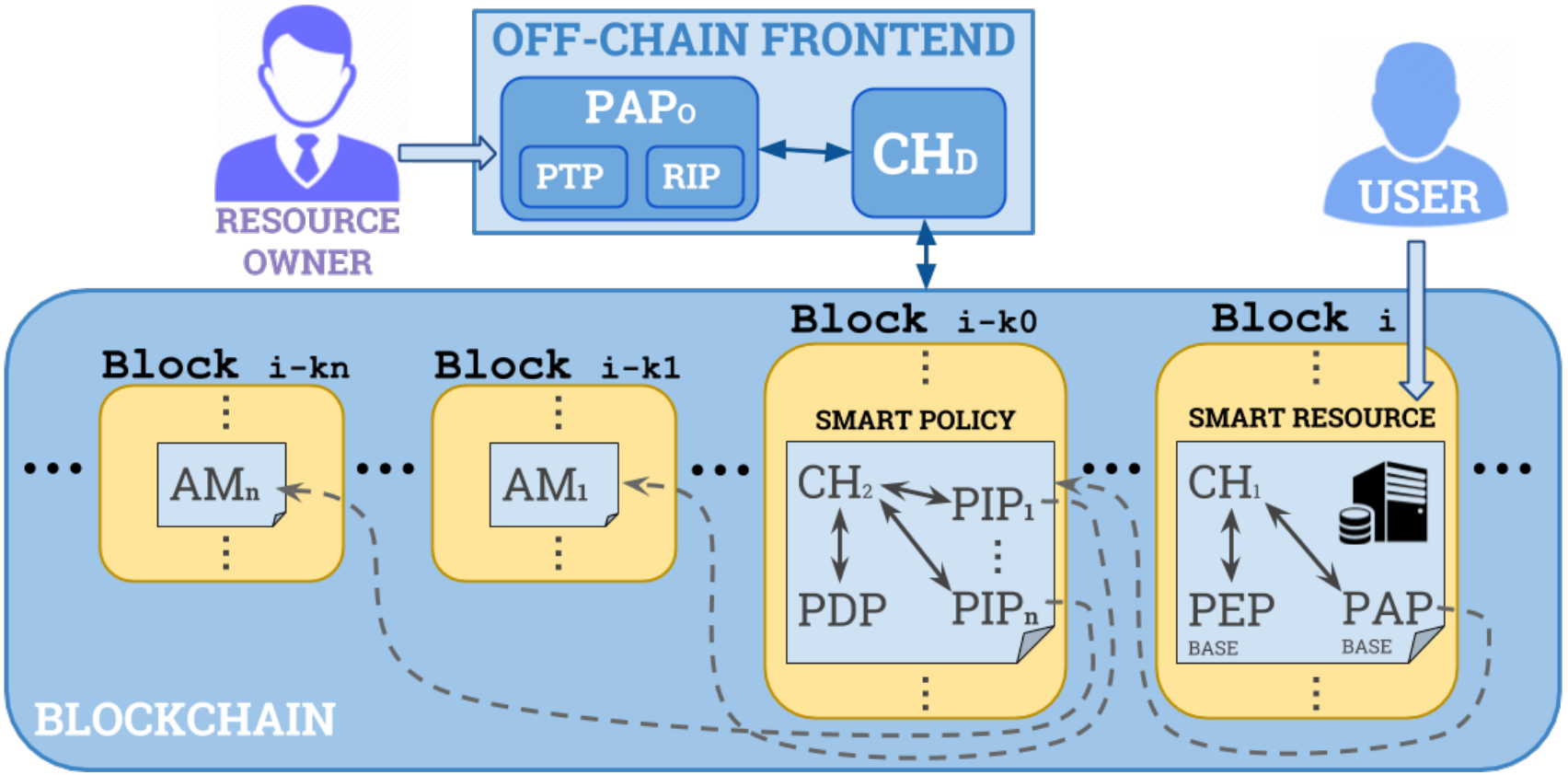



# Blockchain based Access Control System

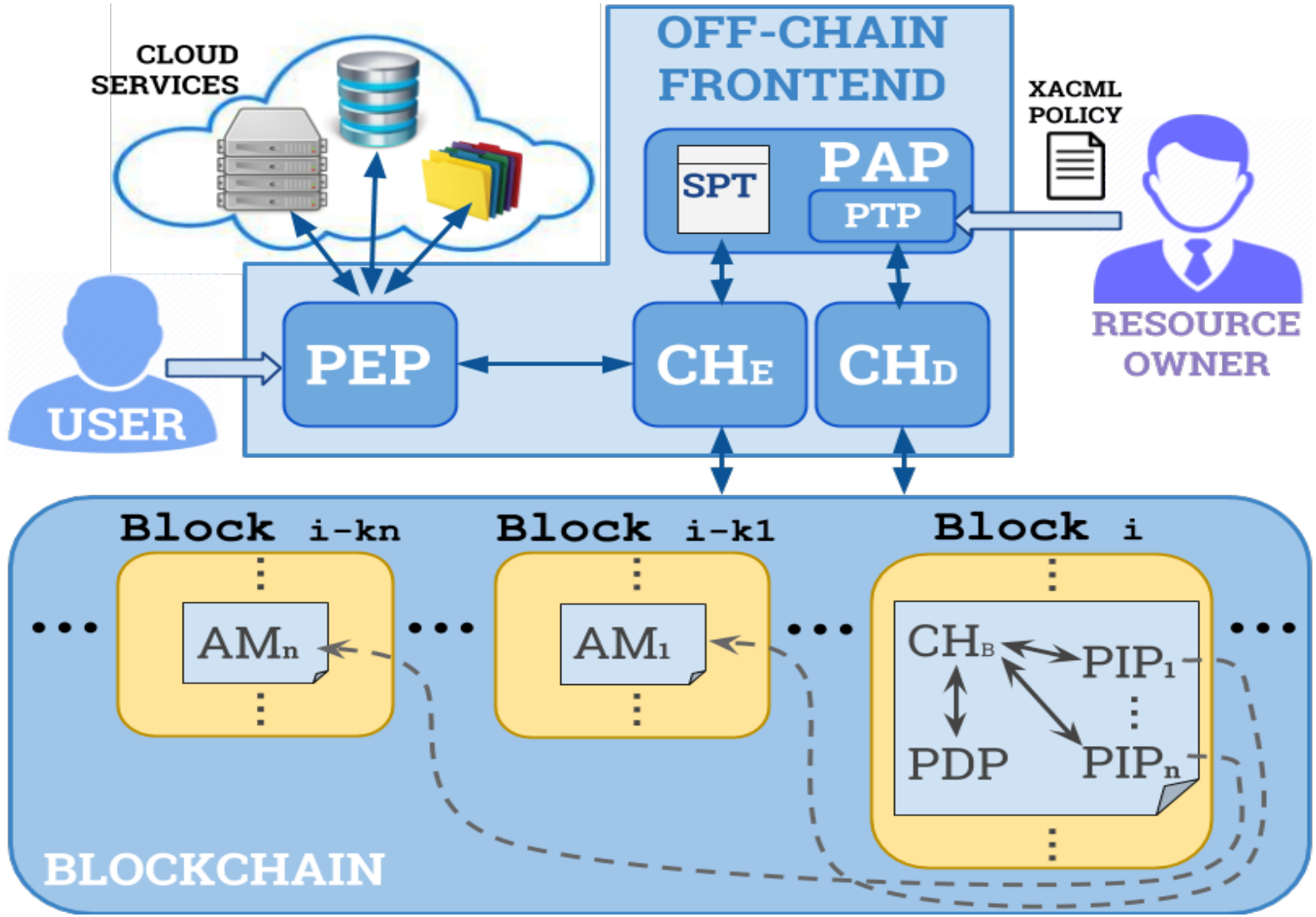


# Examples of Application Scenarios

# Application Scenario 1: **Smart Contracts**



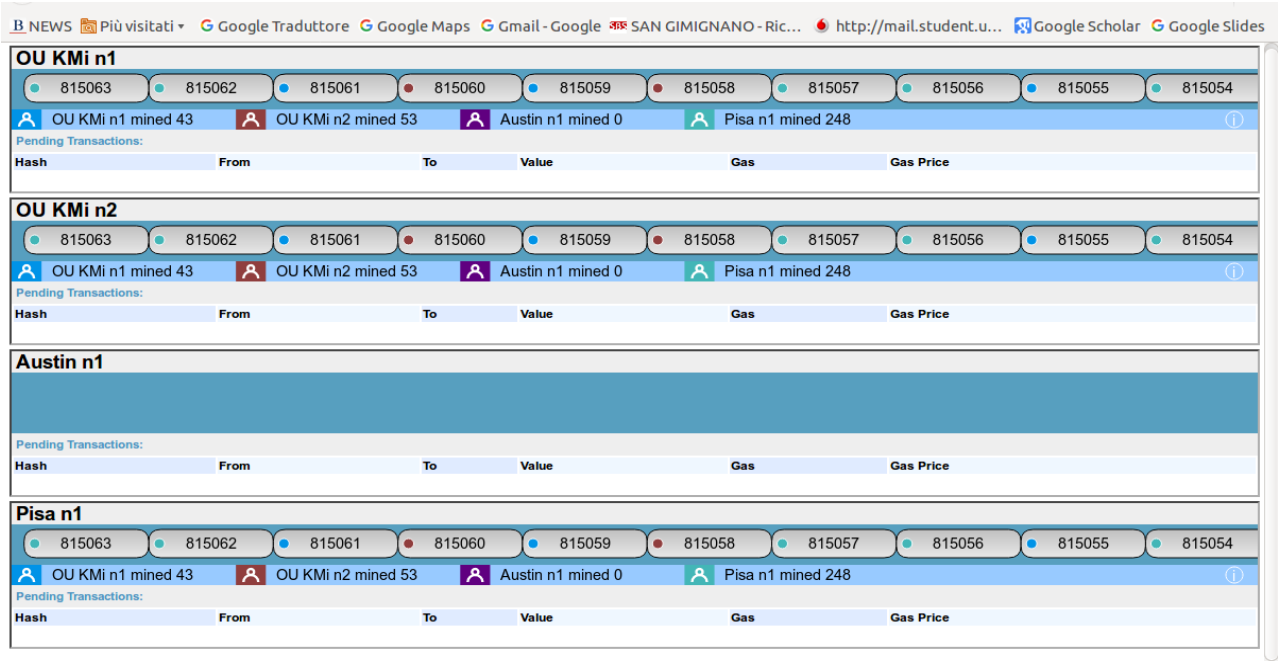
# Application Scenario 2: **Cloud Services**



# Experimental Results

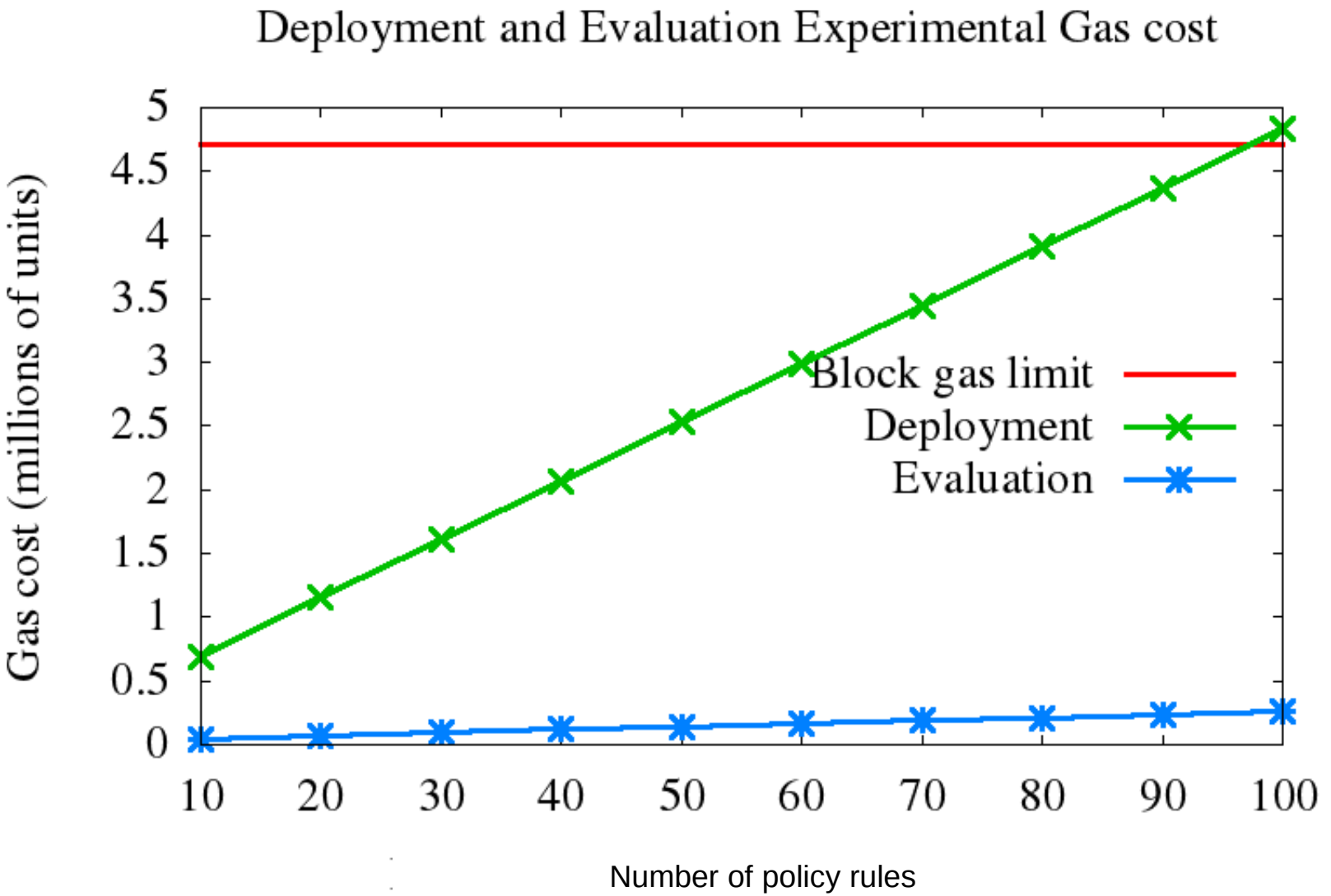
# Testbeds

- International Educational Blockchain Academic Testnet (http://blockchain.open.ac.uk/)
  - Ethereum based

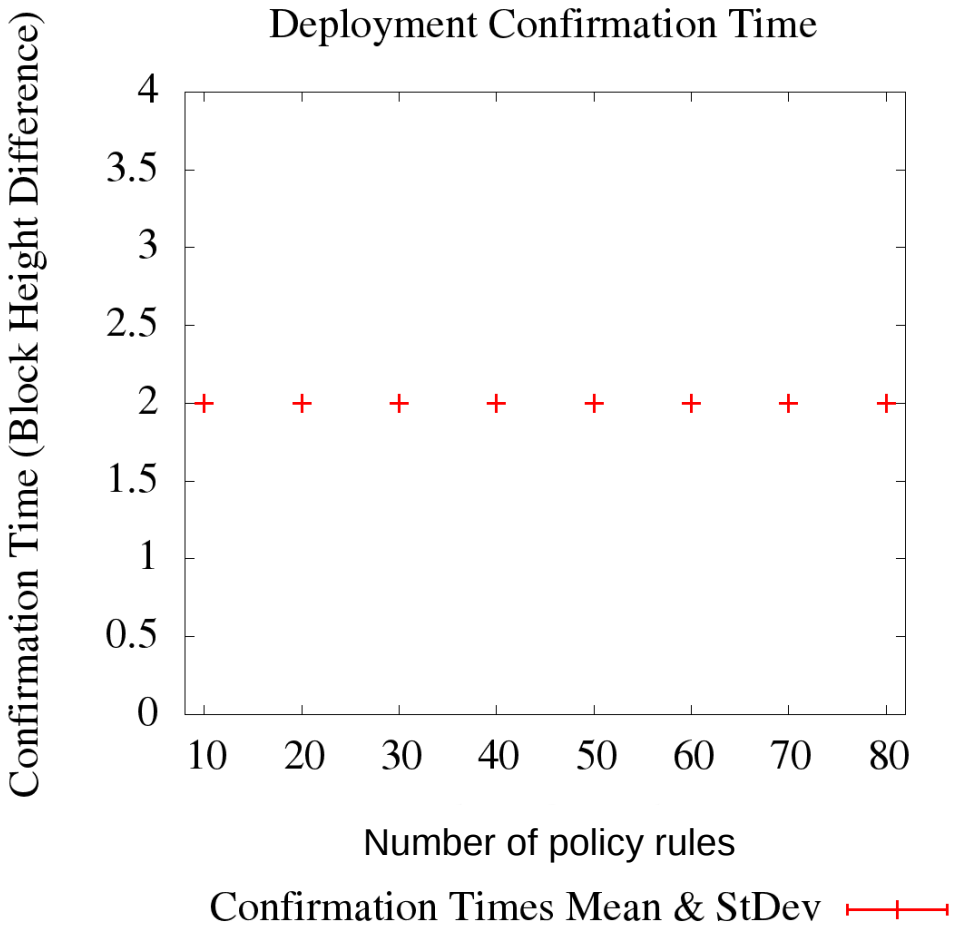


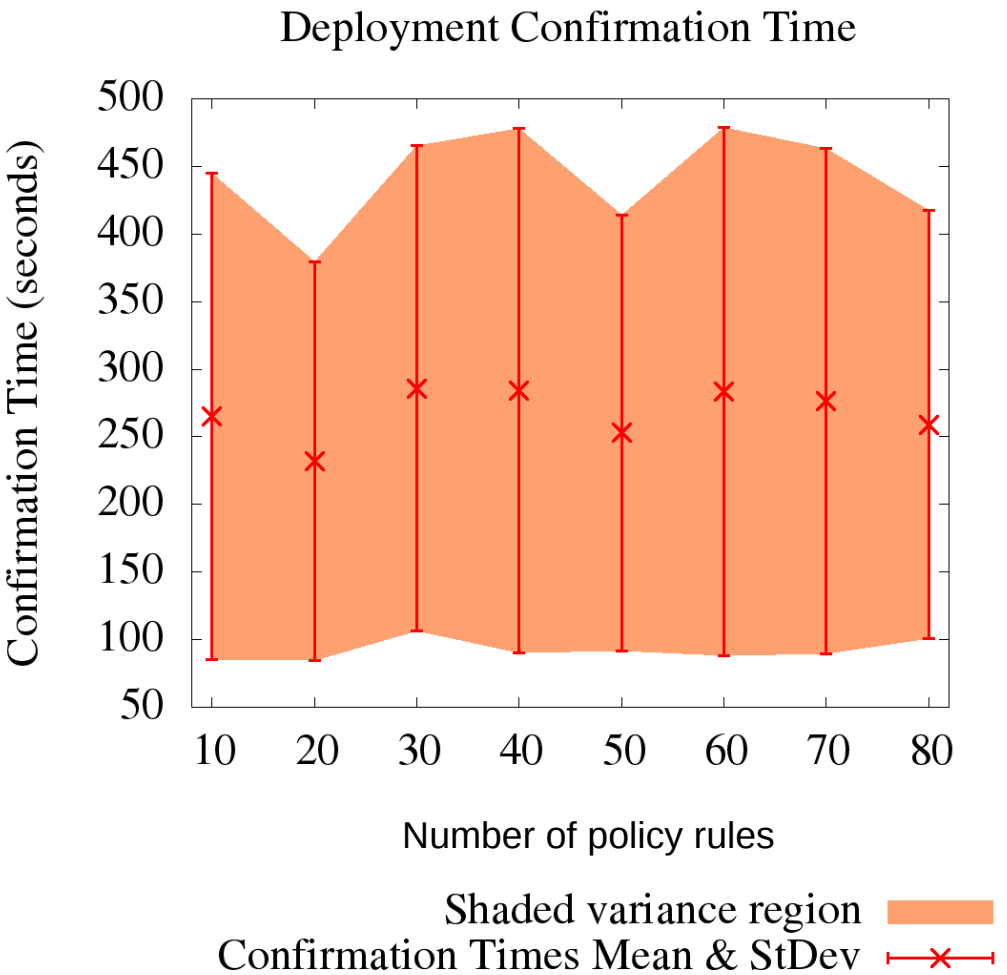

- Ropsten testnet
  - Good reproduction of the Ethereum main network for testing

# Experimental Results: Gas Cost

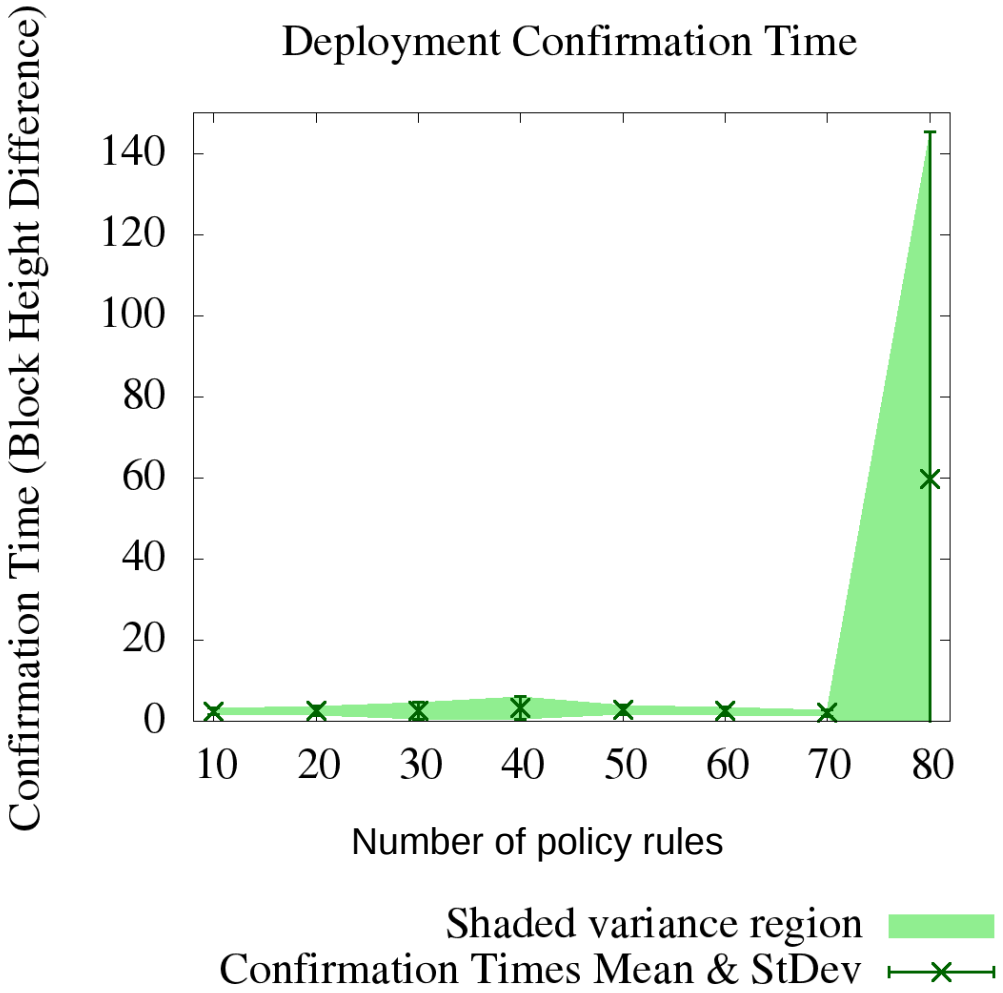


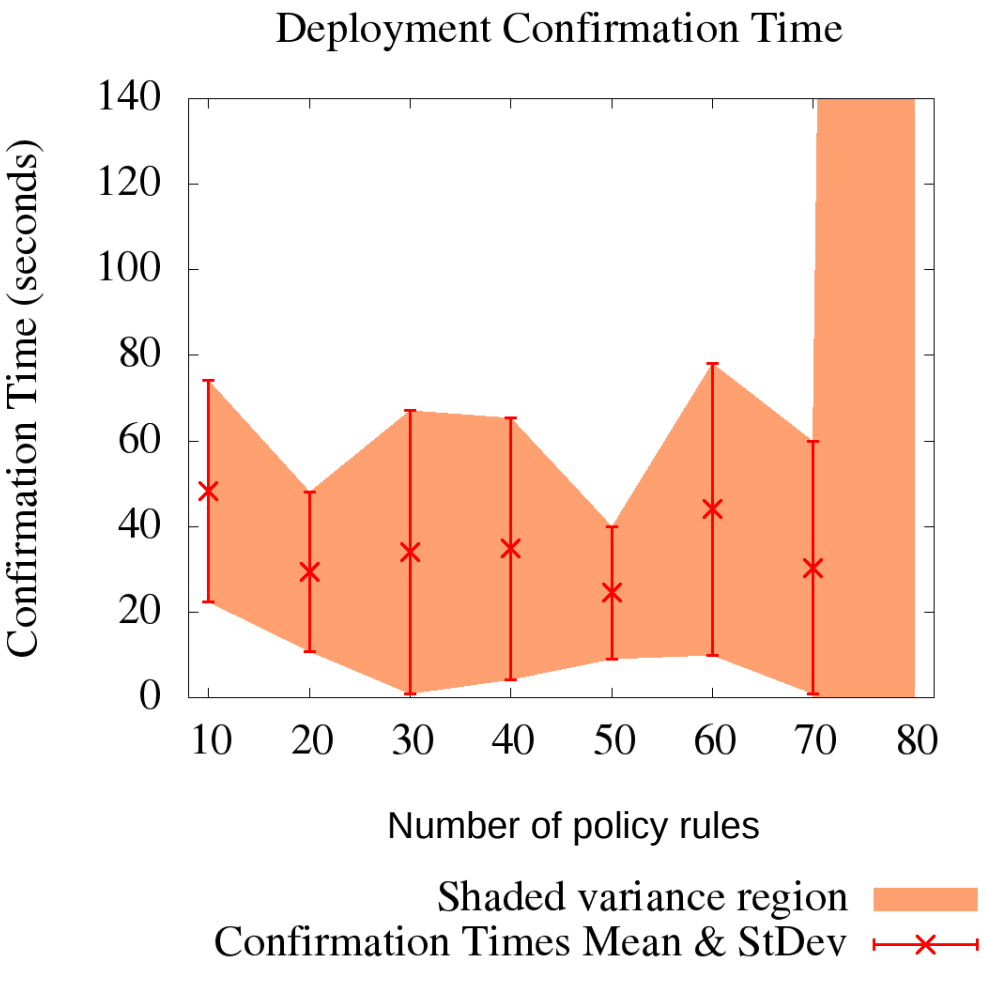
# Experimental Results: Policy Deployment Time on Academic Testnet



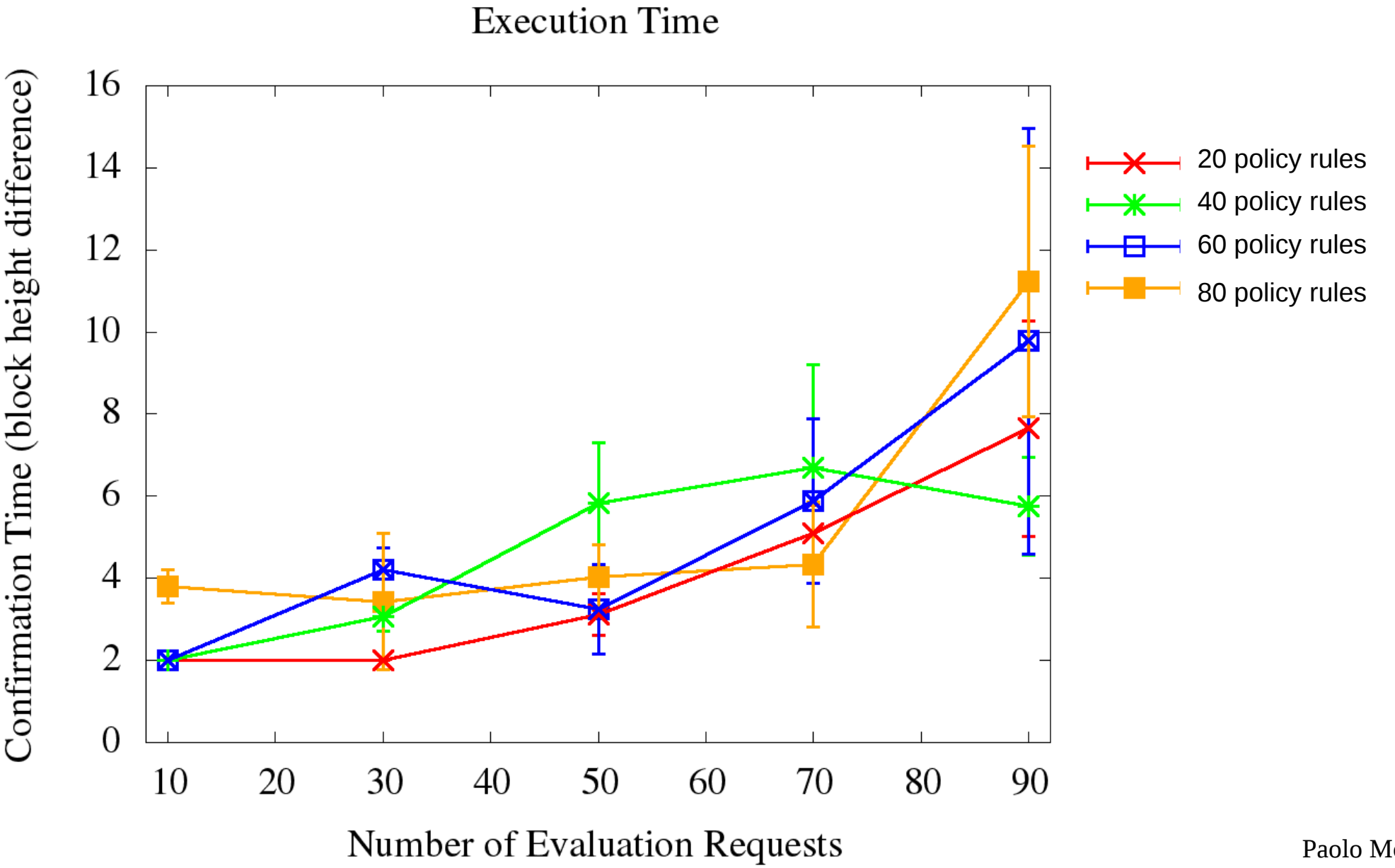



# Experimental Results: Policy Deployment Time on Ropsten



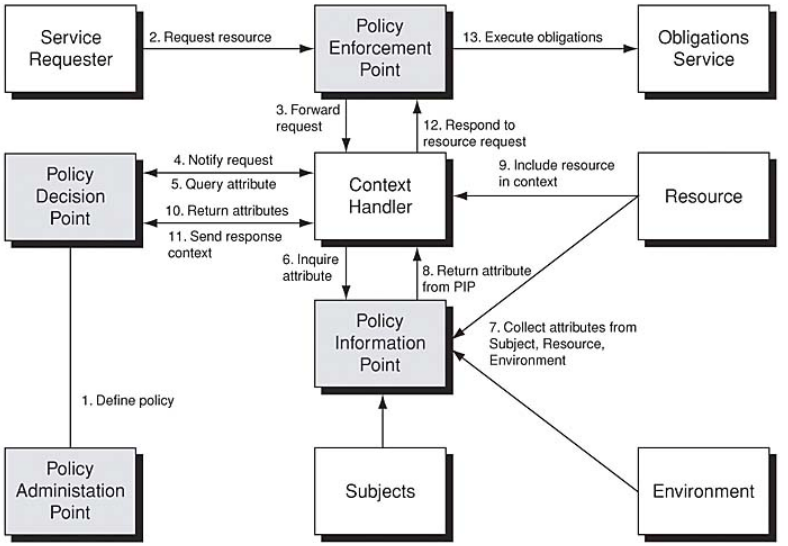



# Experimental Results: Policy Evaluation Time on Ropsten



# Ongoing and Future Work

- Performance evaluation on other testbeds
  - Optimization
- Other access control models




paolo.mori@iit.cnr.it