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





Policy

Enforcement

Point

Policy

Point

3. Forward

request

4. Notify request

13. Execute obligations

9. Include resource

7. Collect attributes from

Subject, Resource, Environment

in context

12. Respond to

resource request

8. Return attribute

from PIP

Obligations

Service

Resource

Environment

Background:

Access Control and XACM Service 2. Request resource Requester



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

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...)

TOP SECRET

- Projects assigned to the subject
- Physical location
- Resources
 - Owner/producer
 - Number of copies of a document
 - Project of a document
 - Security classification

DLT 2019, Pisa, February 12, 2019



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

OASIS 3

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"> </Apply 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



DLT 2019, Pisa, February 12, 2019



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



nak



DLT 2019, Pisa, February 12, 2019

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

B NE	NS 🛅 Più	visitati •	G Google	a Tradu	uttore G	Google	e Maps 🛛 G	Gmail -	Google 🛲	SAN C	IMIGNANO	D - Ric	. 🍝 http:	//mail.	student.u	. 🕄 G	oogle Scho	lar G	Google Slide
OU	KMi n1																		
•	815063		815062)•	815061		815060		815059		815058		815057		815056		815055		815054
8	OU KMi n1	mined 4	3 🗛	OUK	KMi n2 mir	ned 53	A	Austin	n1 mined 0		A Pis	a n1 mi	ned 248						
Pendi	ng Transaction	ns:																	
Hash	From				To Value			Gas			Gas	Price							
ου	KMi n2																		
•	815063		815062		815061		815060		815059		815058		815057		815056		815055		815054
8	OU KMi n1 mined 43 A OU KMi n2 mined						3 Austin n1 mined 0				A Pisa n1 mined 248								(j)
Pendi	ng Transaction	ns:																	
Hash	Hash			From			To Value		e	Gas				Gas Price					
Aus	tin n1																		
Pendi	ng Transaction	ns:																	
Hash			From				То	Valu	e		Ga	s		Gas	Price				
Pisa	i n1																		
•	815063	•	815062		815061		815060	•	815059		815058		815057		815056		815055		815054
8	OU KMi n1	mined 4	اع A	OUK	KMi n2 mir	ned 53	8	Austin	n1 mined 0		A Pis	a n1 mi	ned 248						
Pendi	ng Transaction	ns:																	
Hash			From				То	Valu	e		Ga	s		Gas	Price				

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

Experimental Results: Gas Cost

Deployment and Evaluation Experimental Gas cost



Number of policy rules

Experimental Results: Policy Deployment Time on Academic Testnet



Experimental Results: Policy Deployment Time on Ropsten



Experimental Results: Policy Evaluation Time on Ropsten

Execution Time



Paolo Mori

Ongoing and Future Work

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





paolo.mori@iit.cnr.it