Supporting Privacy with Zero Knowledge in SSI and Blockchain based Access Control

2nd Edition TUM Blockchain Salon

Munich, 16 May 2024

Laura Ricci

laura.ricci@unipi.it

Dipartimento di Informatica

Università degli Studi di Pisa

THE PISA DISTRIBUTED LEDGER LAB

- Permanent/semi-permanent position
  - *Laura Ricci* full professor
  - *Fabrizio Baiardi*, full professor
  - *Barbara Guidi*, Tenure Track
  - *Damiano Di Francesco Maesa*, Junior Researcher
  - *Andrea Michienzi,* Junior Researcher
- PhDs
  - *Domenico Tortola*
  - *Ricardo Lopez Almeida*
  - *Andrea Pelosi*
  - *Francesco Donini*
  - *Giuseppe Galano*
  - *Yitbarek Yimame*
- Post Docs
  - *Matteo Loporchio*
- Collaborations
  - *Paolo Mori, IIT CNR, Pisa*
  - *Anna Bernasconi,* University of Pisa
  - *Andrea De Salve, ISASI, CNR, Lecce*
  - *Roberto Di Pietro*, Hamad Bin Kalifa University, Quatar
  - *Nishanth Sastry*, University of Surrey

https://sites.google.com/unipi.it/pisadltlaboratory

e-mail: laura.ricci@unipi.it

ACCESS CONTROL

set of techniques to decide whether a `Subject` requesting to perform an `Action` on a `Resource` in a given `Context` holds the right the perform it

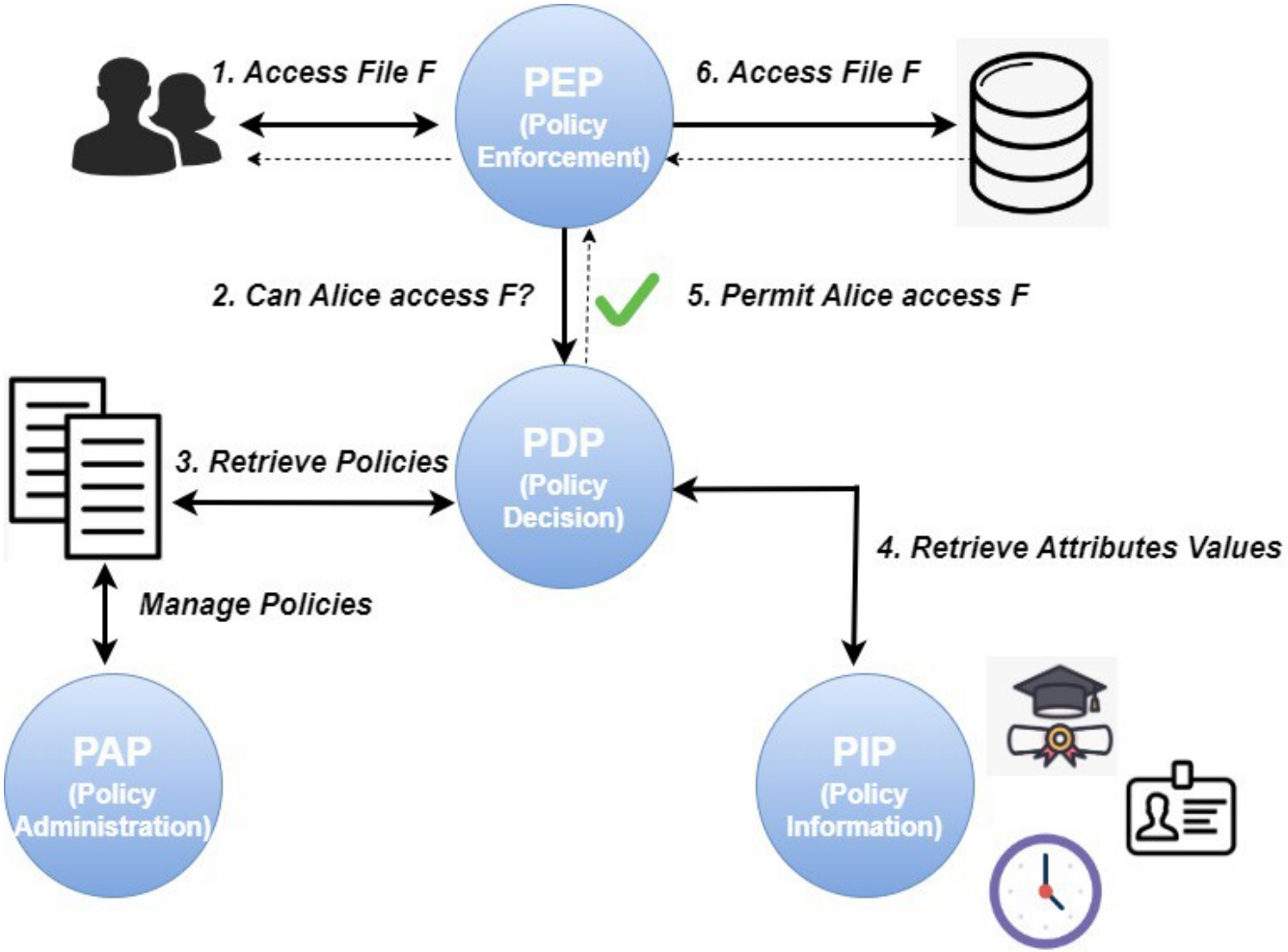
ATTRIBUTE BASED ACCESS CONTROL (ABAC)

- requests to perform operations on objects are granted or denied based on
  - assigned attributes of the SUBJECT
  - assigned attributes of the RESOURCE
  - environment conditions
  - and a set of policies that are specified in terms of those attributes and conditions
- XACML: a standard for ABAC which defines
  - a XML-based language to express Attribute based Access Control Policies
  - a reference architecture

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

OASIS

XACML: THE REFERENCE ARCHITECTURE

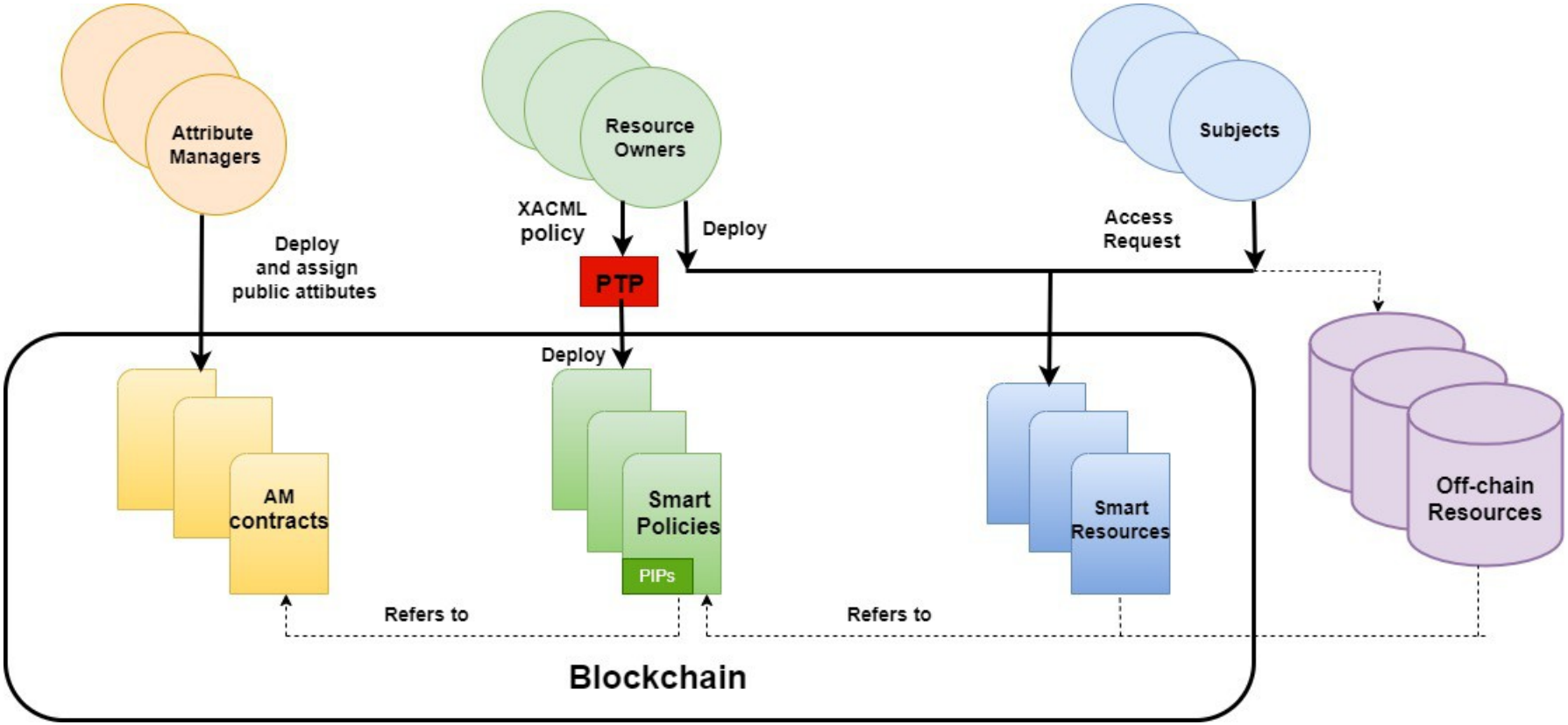


THE XACML FRAMEWORK ON ETHEREUM

- the key idea [1]:
  - implement an ABAC system on top of a blockchain
  - execute on-chain the logic of XACML policies through SmartPolicies implemented by smart contracts
- advantages
  - outsource the access control decision process
  - no need of a trusted third party to perform the access control decision process
  - auditability, decentralization
- potential drawbacks
  - cost
  - performance
  - privacy

[1] D. Di Francesco Maesa,P. Mori,L. Ricci "A blockchain based approach for the definition of auditable access control systems"
Computer and Security 84, 93-119, 2019

THE XACML FRAMEWORK ON ETHEREUM

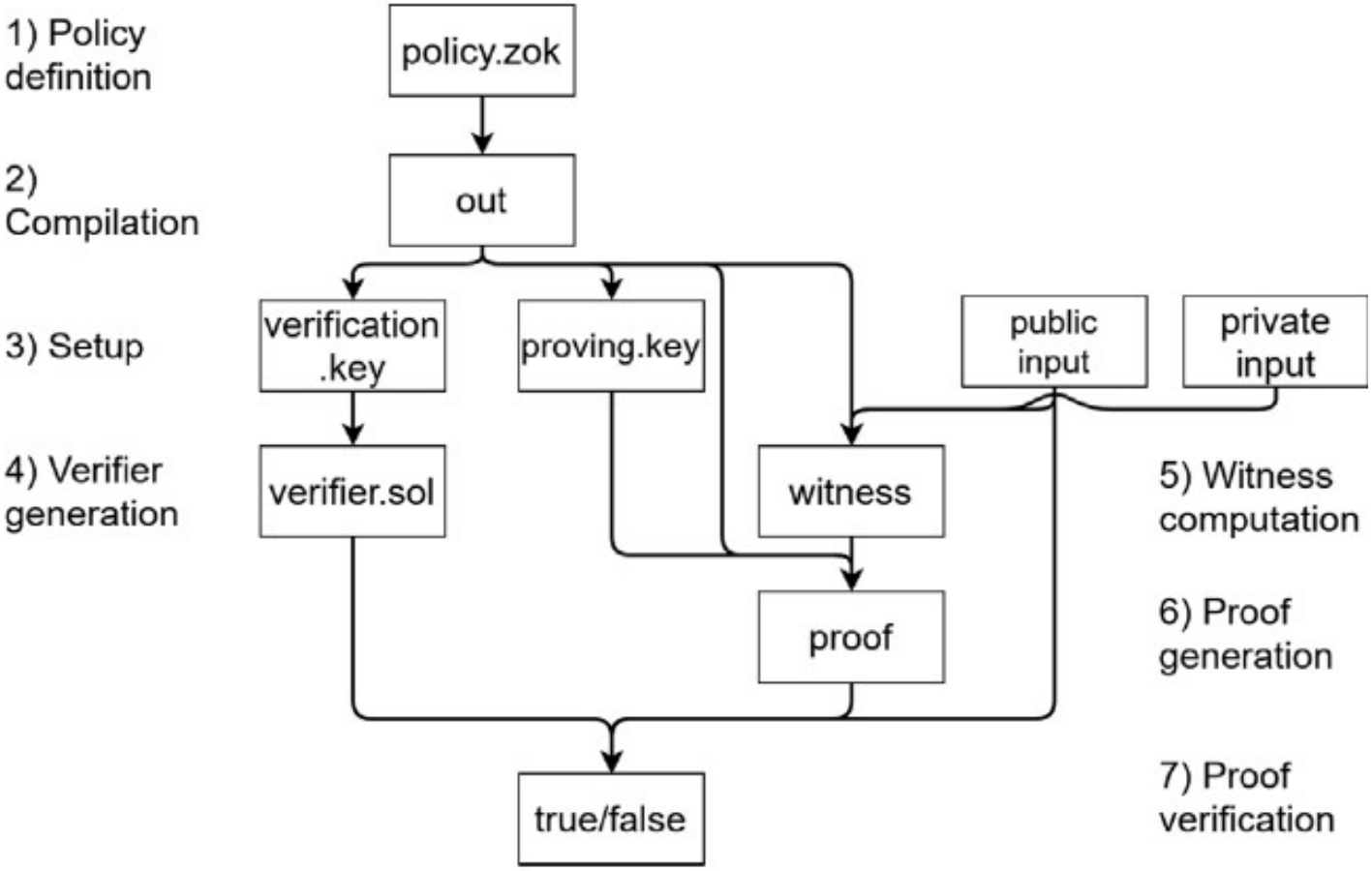


INTRODUCING PRIVACY

- in our first proposal
  - values are provided in clear on-chain from Attribute Managers to Smart Policies
  - guarantees the decision auditability
  - but comes at cost of privacy
- in [2] we improved the original proposal to support private attributes
  - they still contribute to the policy evaluation, but are not disclosed on-chain
  - a solution based on
    - Self Sovereign Identity
    - Zero Knowledge

[2]Damiano Di Francesco Maesa,Andrea Lisi, Paolo Mori, Laura Ricci, Gianluca Boschi
Self sovereign and blockchain based access control: Supporting attributes privacy with zero knowledge
Journal of Network and Computer Applications, Volume 212, 2023

THE ZOKRATES FRAMEWORK



- our solution exploits the `ZoKrates toolbox` implementation of `zkSNARK`

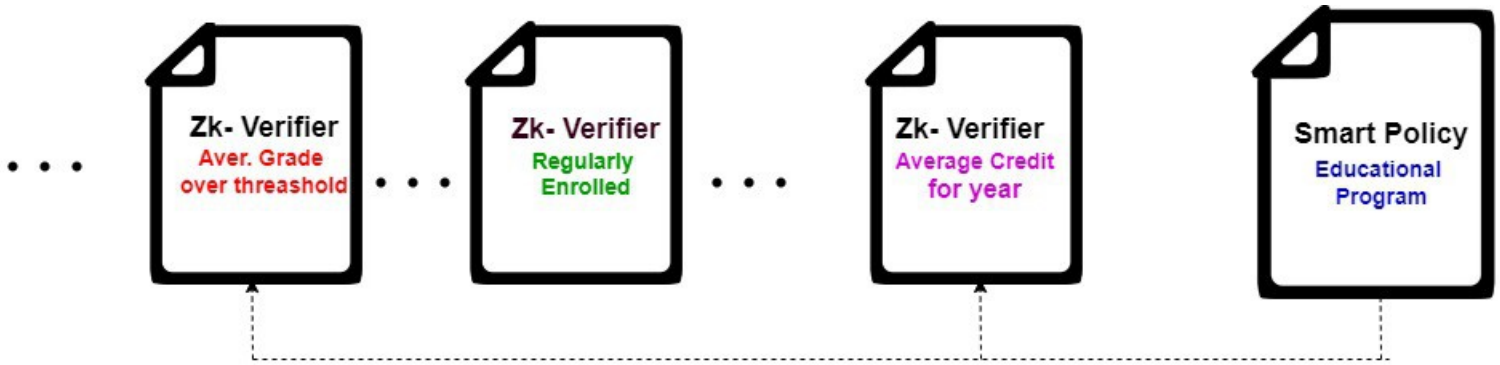
THE ROLE OF ENTITIES

- ATTRIBUTE MANAGERS (AM) are trusted entities providing attributes (as in the previous proposal), but now they
  - manage SUBJECTS's private attributes without disclosing them on-chain
  - define a set of predefined conditions on the private attributes they manage
  - generate a set of zero-knowledge circuits (zkVerifiers) to verify such conditions without disclosing the value of the private attributes
    - zkVerifiers are generated by exploiting the Zokrates toolbox
- RESOURCE OWNERS (RO)
  - deploy smart contracts implementing the policies
  - may check pre-defined conditions defined by ATTRIBUTE MANAGERS (AM) on private attributes by referring the corresponding zkVerifier

AM AND RO IN A REAL SCENARIO

- ATTRIBUTE MANAGER: the University administration
  - deploy on chain a set of ZK-verifiers
  - each verifier implements predicates on the attributes they manage
- RESOURCE OWNER: an educational program assigning prizes to students, under certain conditions
  - deploy a policy on chain, defining the conditions:

    assign prizes to students who have an average grade above a given threshold and are being enrolled by no more that 3 years
  - refer the ZK-verifiers to check the conditions



THE ROLE OF SUBJECTS

- SUBJECTS
  - receive from the ATTRIBUTE MANAGER a PROVING KEY for each condition involving their private attribute
  - do not submit their private attributes on-chain
  - instead produce a ZK proofs, on their premise, exploiting the proving keys
- but...what if a malicious SUBJECT use in their proofs fake values instead of the value received by the ATTRIBUTE MANAGER?
- we need
  - a way to link the private attributes used to generate the ZK-proofs to the values of the attributes received from the ATTRIBUTE MANAGER

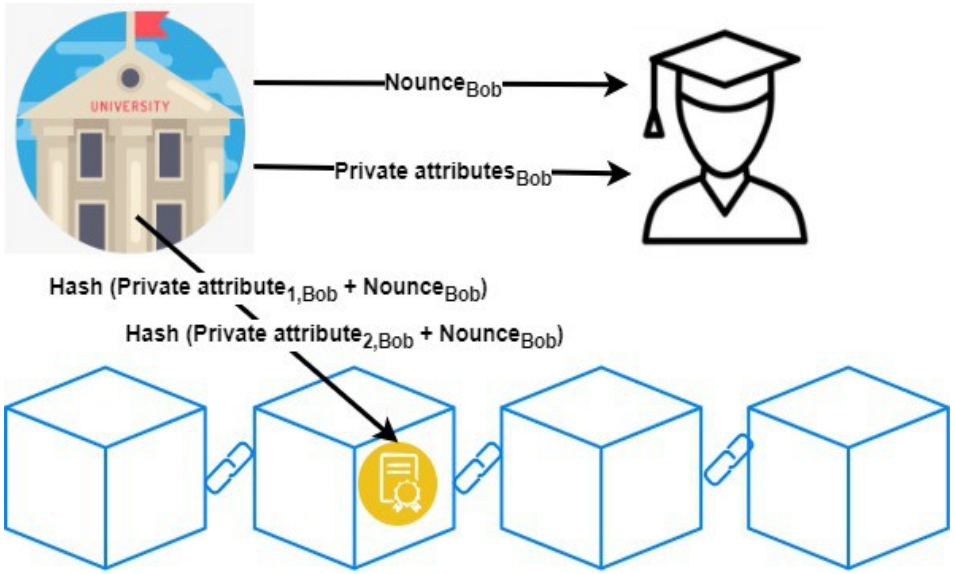
A SAFE SOLUTION

- Bob requires their private attribute to the `University`

  `AverageGrade = 28`

  `EnrollmentYear = 2`

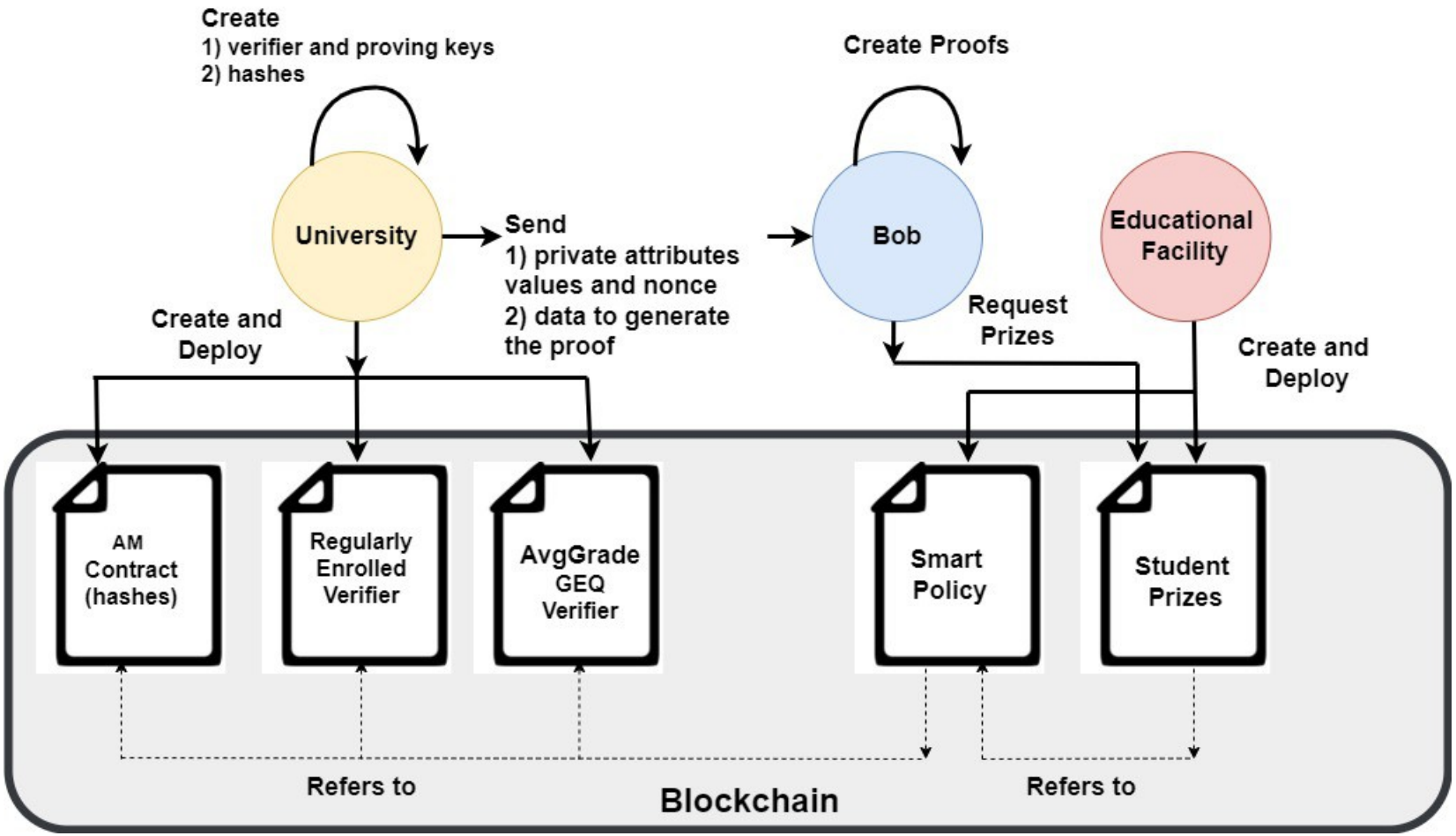
- the `ATTRIBUTE MANAGER`
  - computes the hash of the values + a unique nounce
  - register the hash on the blockchain
  - sends the nounce and the value of the attributes to `Bob`



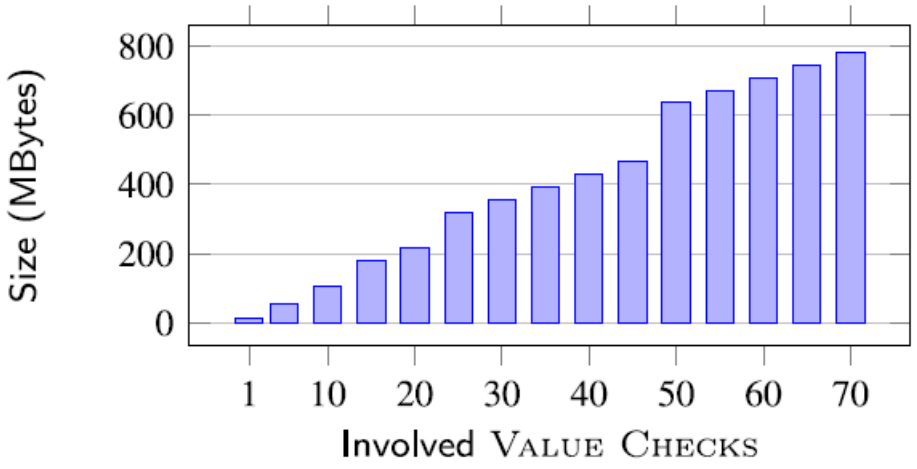
A REAL SCENARIO

- when Bob request his prize
  - generates a proof that takes as input private parameters
    - the private attributes
    - the nonce
- the verifier
  - verifies that hashing the nonce with the private attributes is equal to the value published on-chain by the ATTRIBUTE MANAGER
  - that the conditions on the private attributes are fullfilled

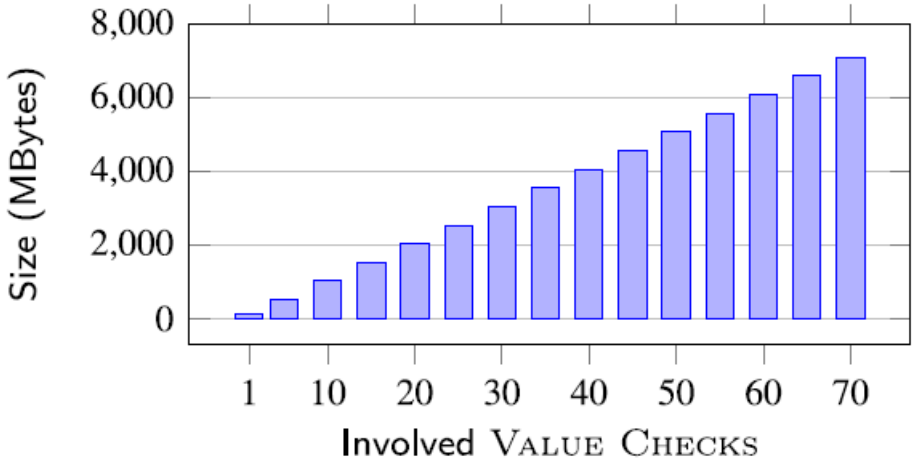
THE OVERALL ARCHITECTURE



EXPERIMENTAL RESULTS

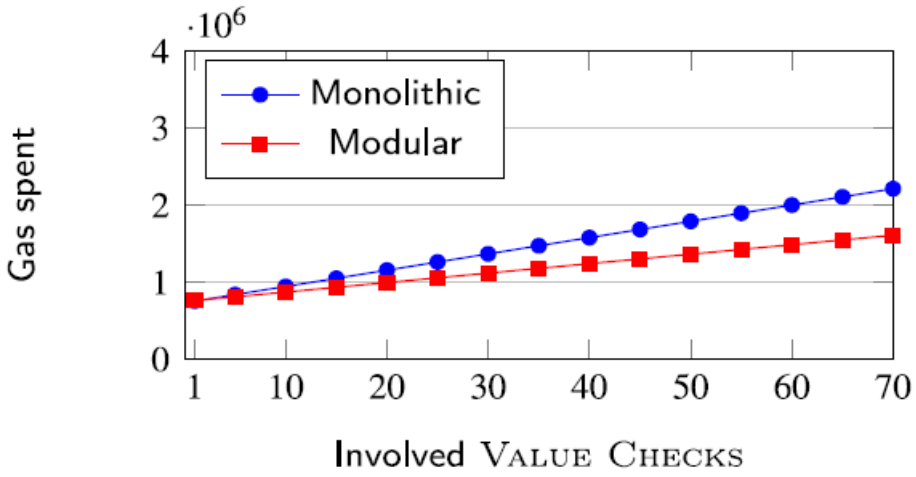


(a) Proving key size in MB.

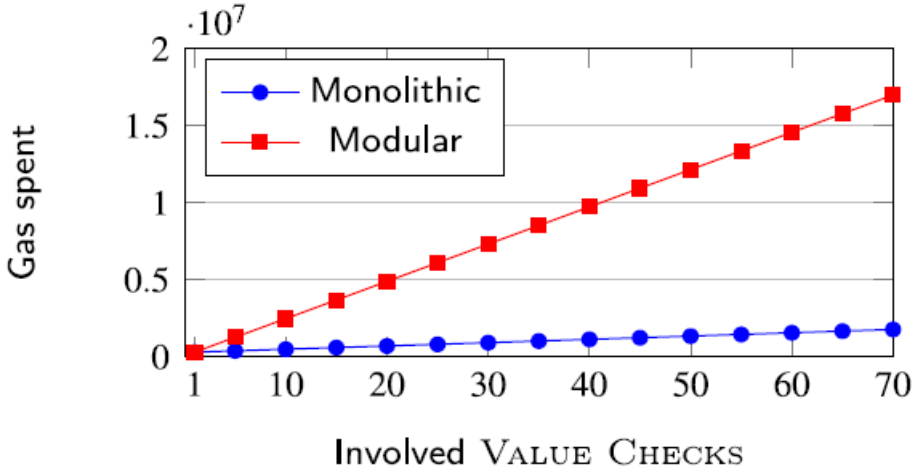


(b) Circuit size in MB.

EXPERIMENTAL RESULTS



(a) SMARTPOLICY deployment cost.



(b) SMARTPOLICY evaluation cost.

RESEARCH TOPICS OF THE PISA LAB

- works related to blockchain-based access control
  - a multi-layer framework to evaluate trust of ATTRIBUTE MANAGERS
  - a full integration of SSI in the XACML standards
- other themes
  - application of cryptographic techniques to blockchain
    - authenticated data structure
    - Zero Knowledge (ZK)
      - evaluate different ZKSnarks libraries, Circom and alternative approaches not requiring trusted setups
  - cross-chain technologies
  - distributed oracles
  - transaction analysis
    - Bitcoin, Ethereum

CURRENT PROJECTS OF THE PISA LAB

- [2023-2025]

  "Awesome AWESOME: Analysis framework for WEb3 SOcial Media", PRIN, Italian National Project

- [2023-2025]

  "DLT-FRUIT: A user centered framework for facilitating DLTs FRUITion", PRIN, Italian national project

- [2022]

  "Cross chain authenticated queries", Ethereum Foundation Grant

- [2024]

  "Authenticated and Efficient Inter Block Event Queries on Ethereum", Ethereum Foundation Grant

- [2024-2025]

  "Advanced and Quantum-safe Solutions for Digital Identity and digital Tracing" (AquSDIT), PNNR Project

Any Questions?