UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

A Decentralized Biometric Authentication Protocol based on Blockchain

Nibras Abo-Alzahab, Giulia Rafaiani, Massimo Battaglioni, Franco Chiaraluce, Marco Baldi

Dipartimento di Ingegneria dell'Informazione

Università Politecnica delle Marche

5th Distributed Ledger Technology Workshop (DLT 2023) Friday 26th May 2023

Introduction

- Biometrics is used for state-of-the-art authentication

Introduction

- Biometrics is used for state-of-the-art authentication
- Requirements include *template protection* and *authentication portability*

Introduction

- Biometrics is used for state-of-the-art authentication
- Requirements include *template protection* and *authentication portability*
- Single sign-on system allows to transfer authentication across various services, but relies on a *single device* -> security and scalability issues

Aim

- Our aim is to propose a solution to implement a **decentralized biometric authentication system**

Aim

- Our aim is to propose a solution to implement a **decentralized biometric authentication system**

- The proposal leverages the *blockchain technology*

- To provide privacy and security guarantees we use *fuzzy commitment scheme*

Initial setup phase

- A governmental body initiates the system by deploying a smart contract onto a blockchain and by adding one or more initial enrollment centers (ECs) to the smart contract list

Initial setup phase

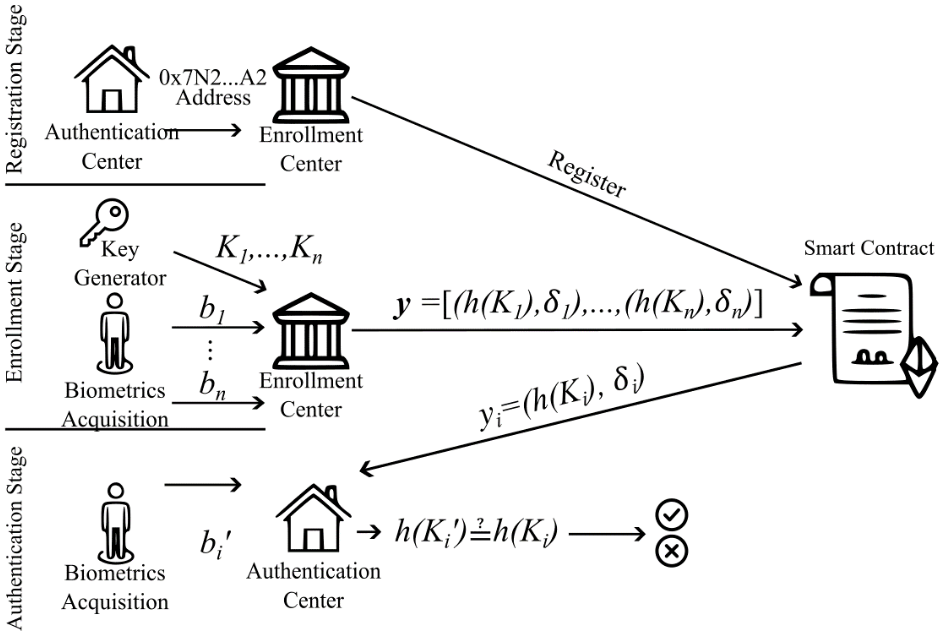
- A governmental body initiates the system by deploying a smart contract onto a blockchain and by adding one or more initial enrollment centers (ECs) to the smart contract list
- ECs can enroll end users and authentication centers (ACs)

Initial setup phase

- A governmental body initiates the system by deploying a smart contract onto a blockchain and by adding one or more initial enrollment centers (ECs) to the smart contract list
- ECs can enroll end users and authentication centers (ACs)
- The *smart contract* collects and maintains the data of users
- *ECs* can write and retrieve data
- *ACs* can only retrieve data, i.e., perform user authentication

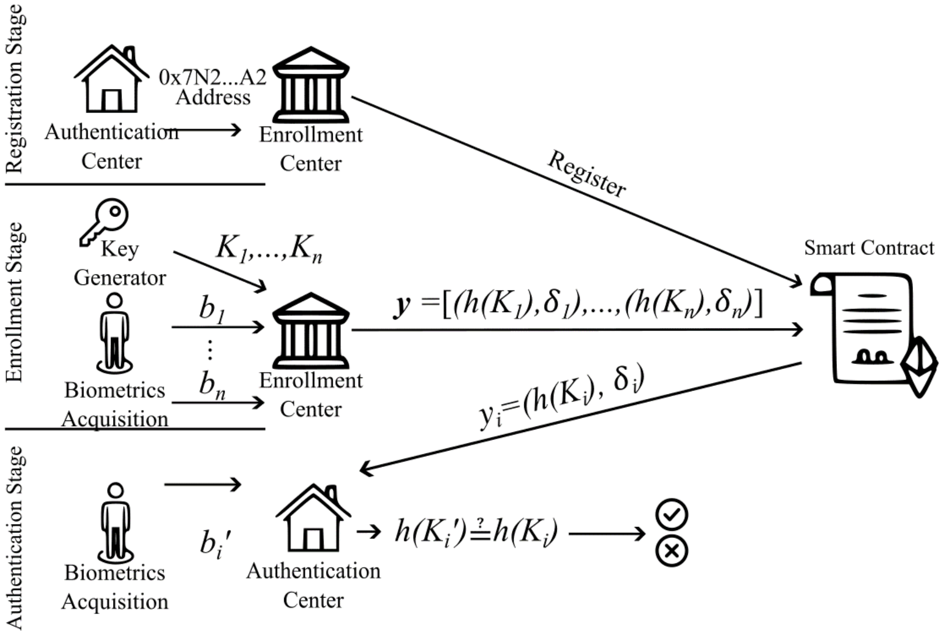
Protocol stages

- Registration stage
- Enrollment stage
- Authentication stage

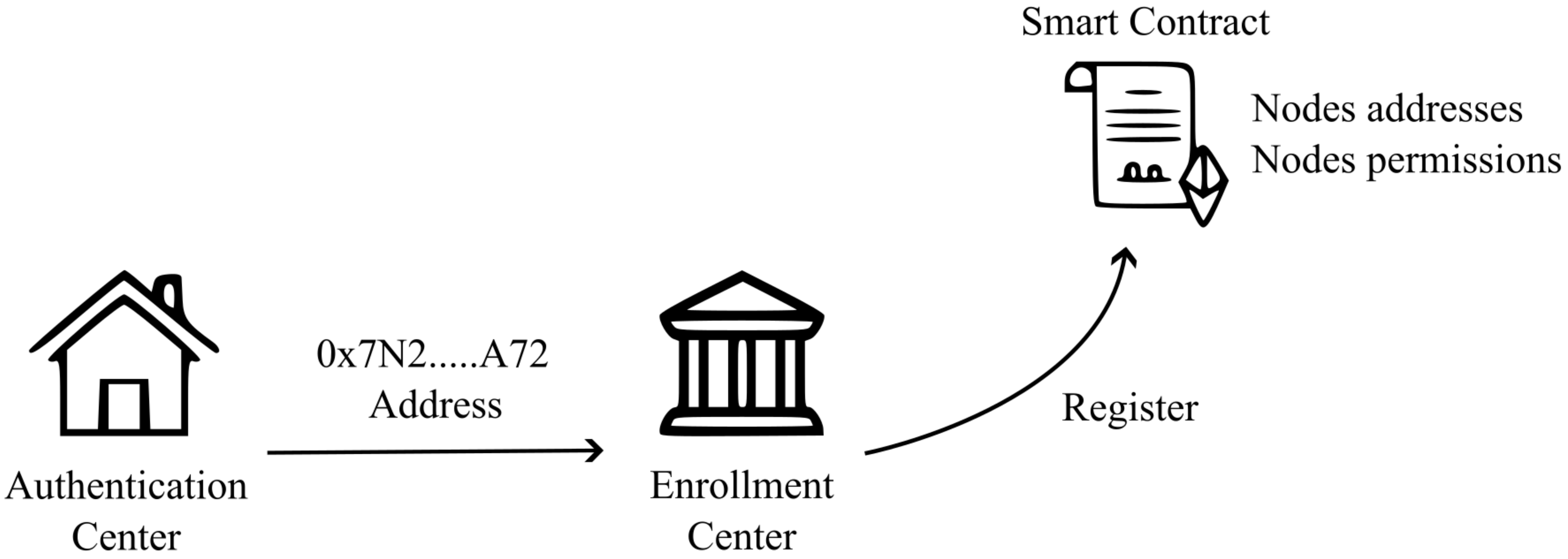


Protocol stages

- **Registration stage**
- Enrollment stage
- Authentication stage



Registration stage



Smart Contract

Nodes addresses
Nodes permissions

0x7N2.....A72
Address

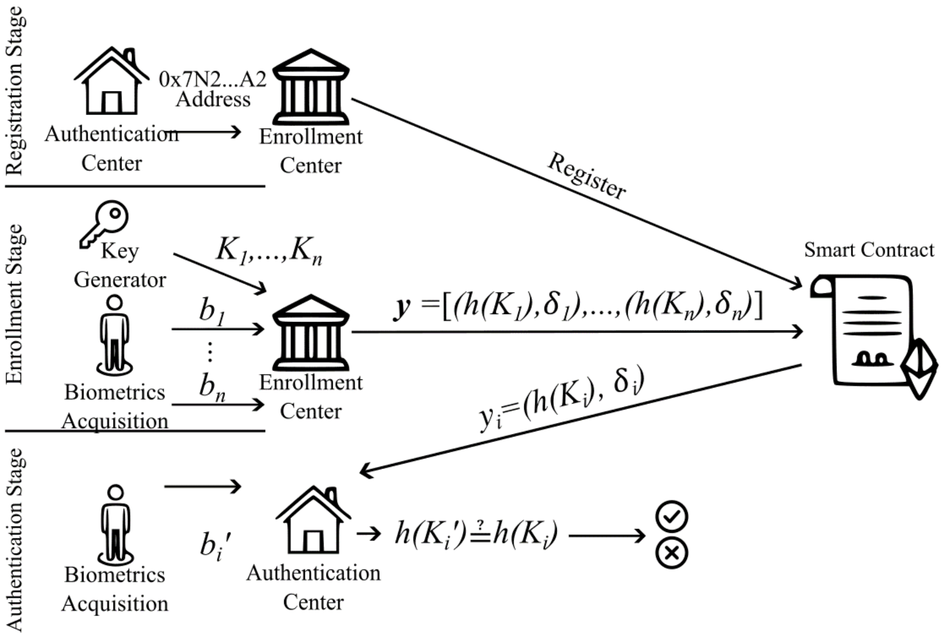
Register

Authentication Center

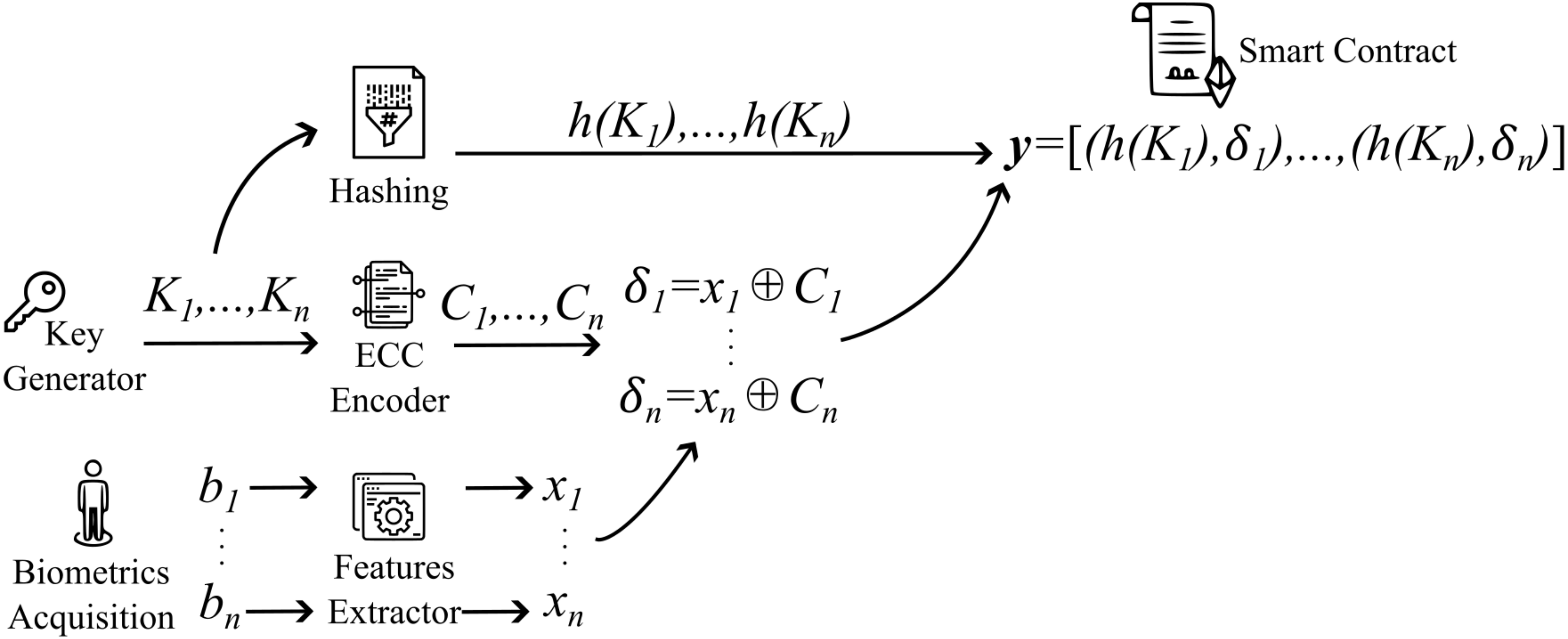
Enrollment Center

Protocol stages

- Registration stage
- **Enrollment stage**
- Authentication stage

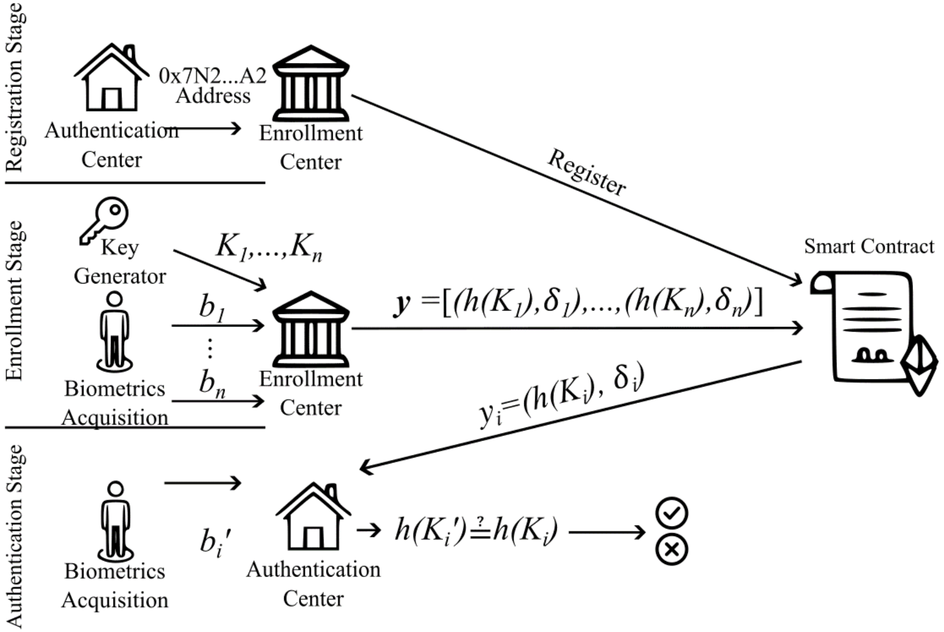


Enrollment stage

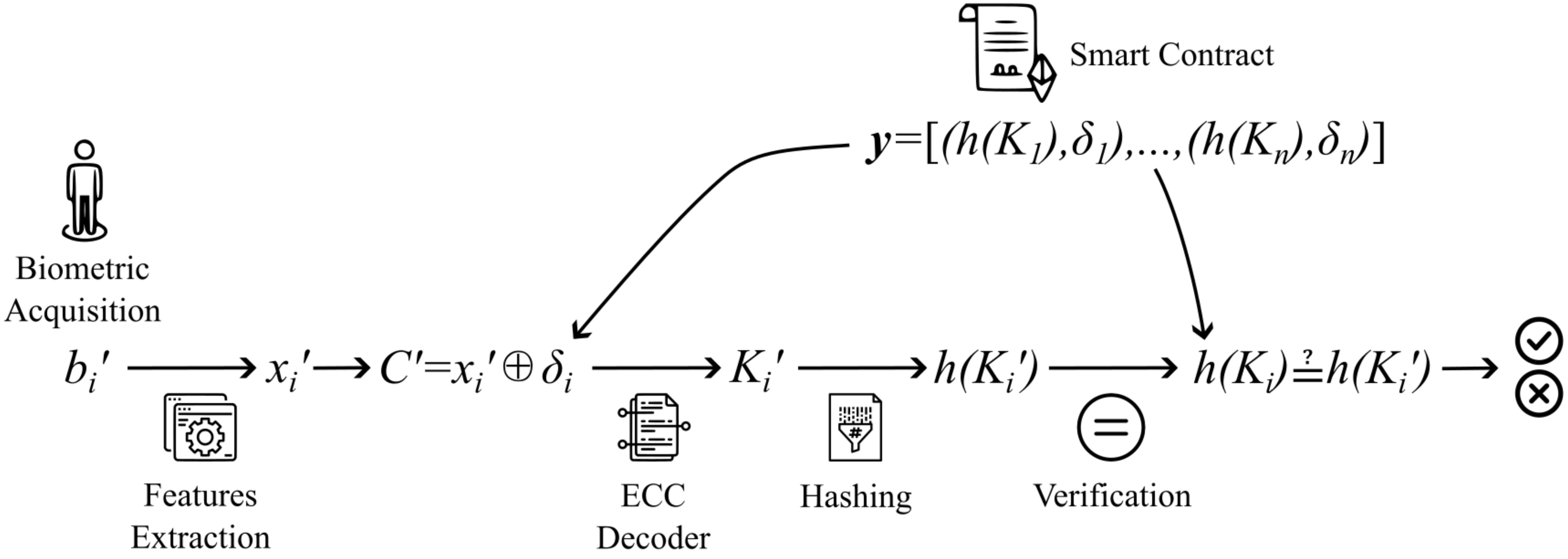


Protocol stages

- Registration stage
- Enrollment stage
- **Authentication stage**



Authentication stage



Revocation phase

- The system should guarantee the GDPR rights, such as the *right to be forgotten*

Revocation phase

- The system should guarantee the GDPR rights, such as the *right to be forgotten*
- Any EC can invoke a function of the smart contract that erases the user records from the list of enrolled users

Revocation phase

- The system should guarantee the GDPR rights, such as the *right to be forgotten*

- Any EC can invoke a function of the smart contract that erases the user records from the list of enrolled users

- The enrolling data are still stored in past transactions, but in an encrypted form, and no personal data of revoked users can be retrieved

Conclusions

- The proposed protocol incorporates blockchain technology into biometric systems, using Fuzzy Commitment Scheme

Conclusions

- The proposed protocol incorporates blockchain technology into biometric systems, using Fuzzy Commitment Scheme

- Using different blockchains, the protocol can be adapted to different scenarios, being both *efficient* and *cost-effective*

Conclusions

- The proposed protocol incorporates blockchain technology into biometric systems, using Fuzzy Commitment Scheme
- Using different blockchains, the protocol can be adapted to different scenarios, being both *efficient* and *cost-effective*
- A security analysis found the protocol to be *strong* and *secure*

Conclusions

- The proposed protocol incorporates blockchain technology into biometric systems, using Fuzzy Commitment Scheme
- Using different blockchains, the protocol can be adapted to different scenarios, being both *efficient* and *cost-effective*
- A security analysis found the protocol to be *strong* and *secure*
- Future work will address issues as scalability and interoperability, and will test the method in real-world scenarios

UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

Thanks for your kind attention!

g.rafaiani@univpm.it

5th Distributed Ledger Technology Workshop (DLT 2023) Friday 26th May 2023