Blockchain-based Registries of User Choices and Their Challenges

Albenzio Cirillo, Diego Pennino, Maurizio Pizzonia, Andrea Vitaletti, Marco Zecchini

Introduction

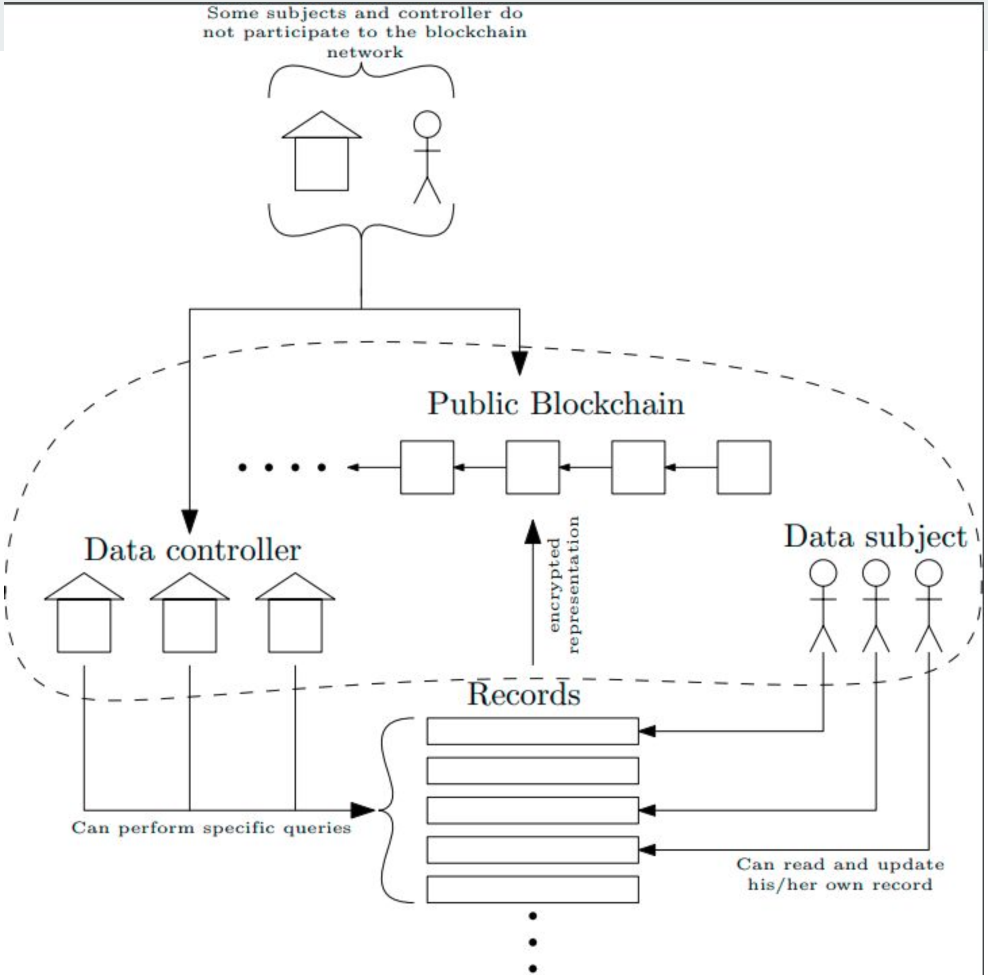
- European General Data Protection Rules (*GDPR*) states that where processing is based on the *data subject*'s consent, the *data controller* should be able to demonstrate that the *data subject has given consent* to the processing operation
- At any time, the *data subject* should be able to object to processing of personal data concerning him/her.

There is no single platform that allows to check all opt-in consents given by a specific *data subject*.

Our Contribution

- A novel approach based on the blockchain for managing *data consents*. *Data subjects* express their consent in the form of a suitable transaction on the blockchain
    - *Integrity* is guaranteed (i.e. nobody can modify a stored content)
    - Issues on *identity*, *privacy*
- Give research direction for these issues

Model for DLT-based Registries of User Choices



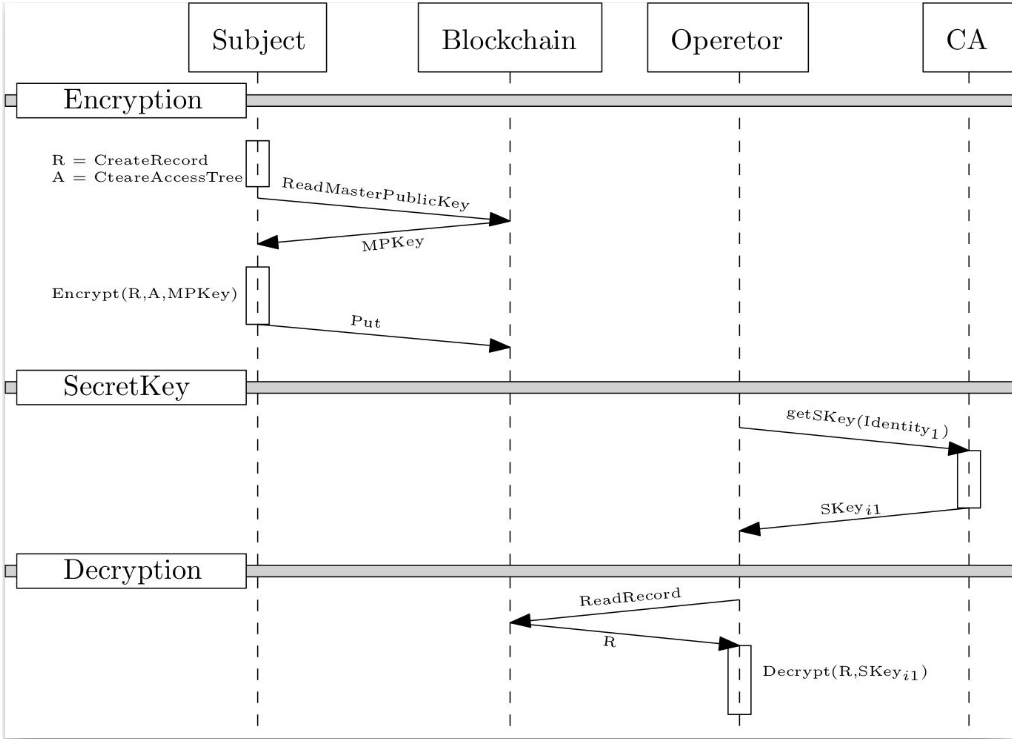
Some subjects and controller do not participate to the blockchain network
Public Blockchain
. . . .
encrypted representation
Data controller
Data subject
Records
Can perform specific queries
Can read and update his/her own record

Research Challenges

1. Confidentiality
2. Secure Access Without Direct Blockchain Involvement
3. Data Subject Identities in the Blockchain
4. Scalability

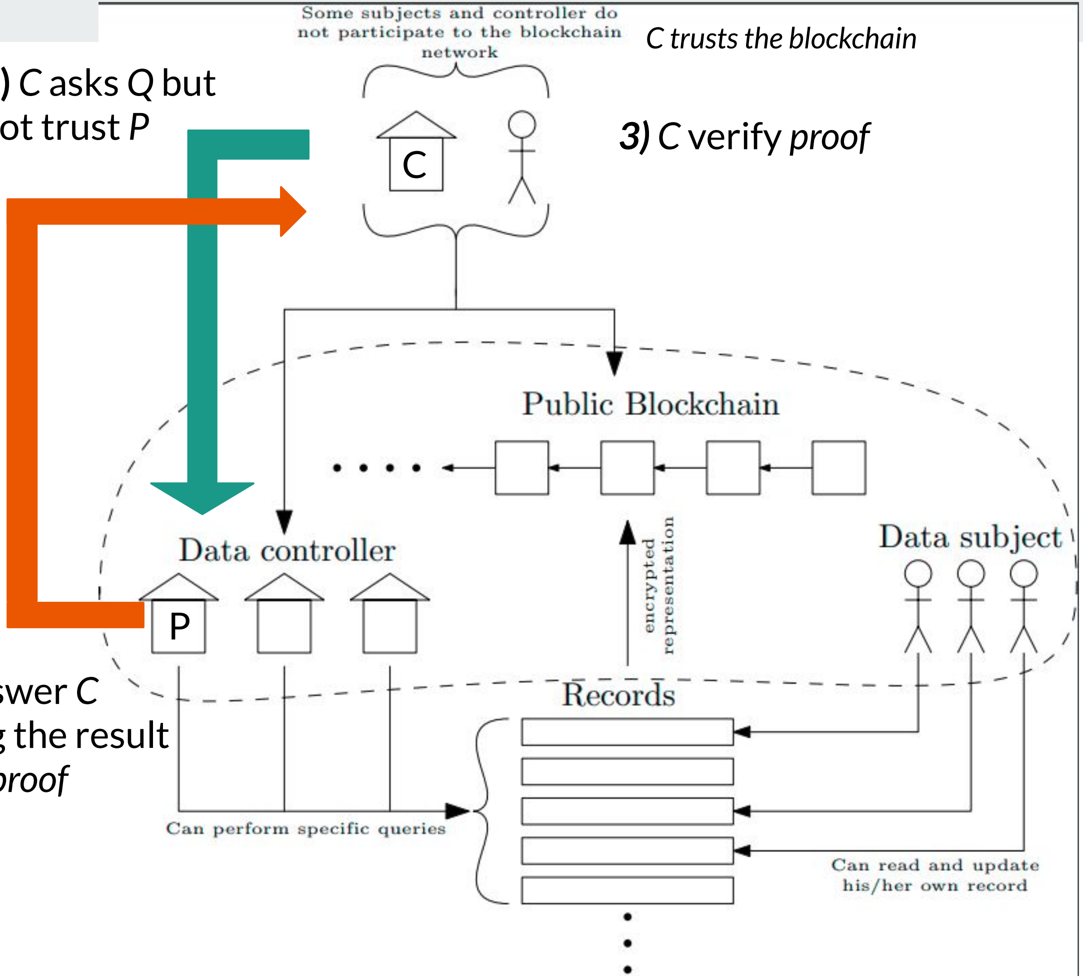
1) Confidentiality

- Policy of our model contrasts with the fact that we assume the blockchain to be public
- Considering *Cipher-policy Attribute-based encryption, CP-ABE,* where the capability to decrypt depends on a policy expressed by a logic formula on the value of certain *attributes.*



2) Secure Access without direct blockchain involvement

Use of *Authenticated data structure*


Some subjects and controller do not participate to the blockchain network
C
P
Public Blockchain
Data controller
encrypted representation
Data subject
Records
Can perform specific queries
Can read and update his/her own record

1) *C* asks *Q* but not trust *P*

2) P answer *C* proving the result with a *proof*

3) C verify *proof*

C trusts the blockchain

3) Data Subject Identities in the blockchain

- Each record is associated with its data owner and data controllers need to know this association.
- Common technique relies on the adoption of a *central authority (CA).*
    - Association in form of *certificates*
- *CA* requires that all participants trust it. Interesting research direction is to study solution in which also *CA* is decentralized.

4) Scalability

- Blockchain-based registries may be subject to a high rate of updates, since the number of users may be in order of millions
- Subject do not change their mind very often.

Scalability issues are pertinent to the blockchain infrastructure.

Conclusions

- Idea of decentralized register based on a public blockchain to store *data subject* choices that *data controller* can use
- Listed some challenges highlighting some research directions.

Thank you for the attention