Blockchange: Making Blockchain Conformant with parts of GDPR and Transparency Principle Compliance with BlockChain

Iraklis Paraskakis, Andreas Kotoulas, Bashir Sheban

SEERC

Recap and contextualise our presentatrion: Right to Privacy and Blockchain

- Distributive nature of Blockchain implies that each node Is a Data Controller/Processor effectively
- Right to be forgotten-a huge technical issue with wide implications
- Above issues seem intractable – so that some companies in EU have given up on use of blockchain in recording transactions
- **Current effort in research to overcome the problem and make Blockchain GDPR compliant without loosing the essence of immutability**
- **Could revolutionise application of GDPR and enforce rigorous application of GDPR provided certain notions of data ownership are altered.**

Two proof of concepts applications

- BlockChange – proof of concept addressing right to be forgotten

and

- Transparency Principle Compliance with BlockChain – allowing data to be accounted as and when is processed.

BlockChange: Aim of the project

Automated transactions demand transparency, traceability and immutability. These characteristics are fully provided by Blockchain technology and transactions under this technology are assured these attributes. However, GDPR gives the right to the European individuals to request the deletion of their personal data, thus data that was guaranteed not to be amendable now it is required to change. Therefore, the **aim** of this project is the following:

Investigate how the Blockchain technology can be altered to accommodate requirement as stipulated by the GDPR, that is, making the Blockchain GDPR compliant

Objectives of the project

- Understand in which cases GDPR is applicable regarding the right to be forgotten.
- Develop a proof of concept solution which implements an application with underlying Blockchain technology, where data can be deleted or modified.

Motivations

- Automation of transactions
- Transparency of transactions
- The right of privacy of natural person (right to be forgotten-implies full erasure of data right to rectification)

Therefore there is a need to balance the transparency of transactions with the right of privacy.

Blockchain main characteristics

Because transactions need to be performed in automated manner, data involved in such transactions should be transparent and immutable. Blockchain offers both of the characteristics.

- Immutability
- Timestamp
- Auditability

Possible Solutions

- Change Blockchain’s architecture, so data stored on the Blockchain can be deleted or edited (editable Blockchain)
- Use state of art cryptographic techniques to conceal the content that is written on the Blockchain or prevent the identification of users (soft erasure)
- Storing personal data in an external database and erase them when requested (hard erasure)

BlockChange choice: Off-chain storage

For BlockChange the approach of hard erasure (off-chain storage) is selected.

The reasons are the following:

- It can be used for all the types of Blockchain (permissioned and permissionless).
- It can be implemented in combination with the currently available Blockchain networks, such as Bitcoin, Ethereum or Hyperledger, without any changes in the source code of these networks.

On the contrary changing the architecture of the blockchain requires the currently available networks to change their source code in order to integrate the changes, and then to be able to delete or modify data.

The soft erasure is not actually delete or modify data that is stored on the Blockchain. It is only conceal the content and the identification of the individual in order making GDPR not relevant.

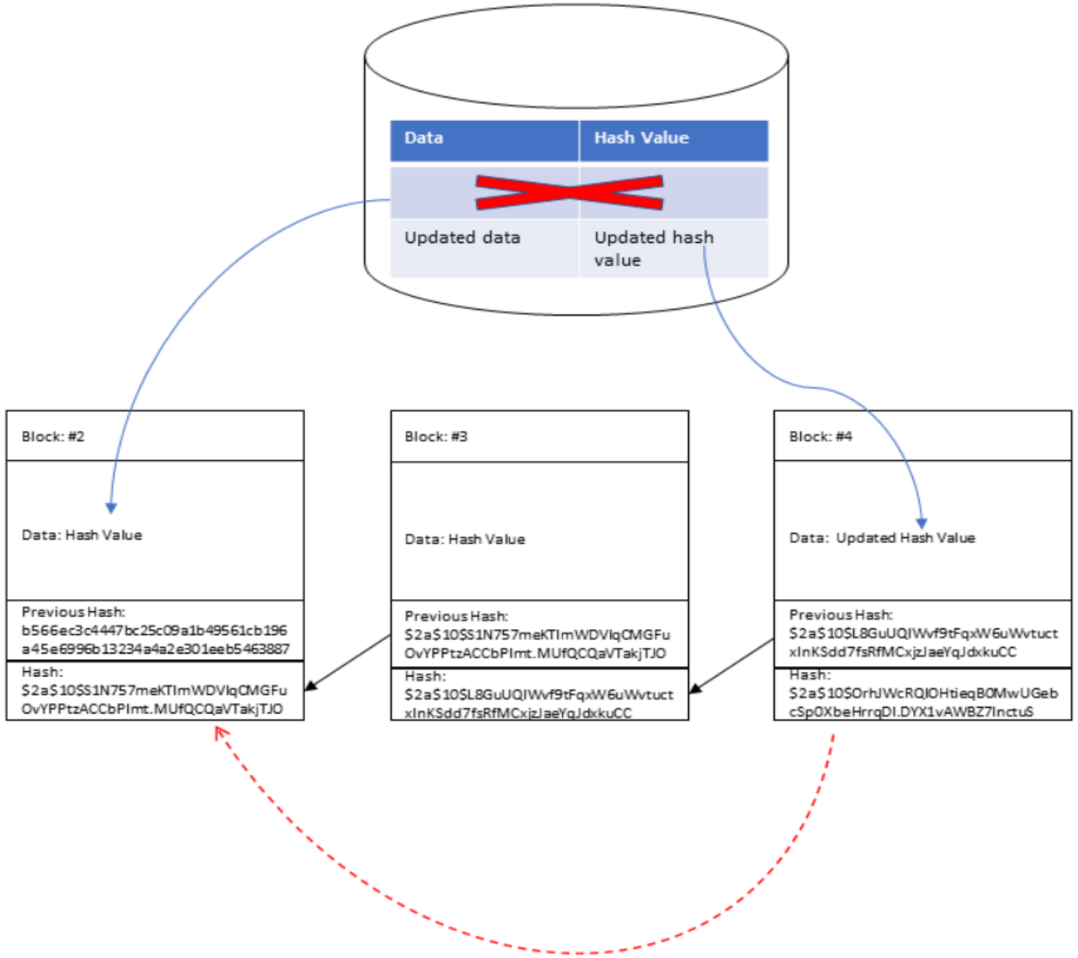
Hard erasure (off-chain storage) - Addressing right to erasure

- The idea is that the personal data is stored on an external database while the hash value of that data is stored on the Blockchain.
- The database also store the reference to this data on the Blockchain.
- In order to verify that the data that is stored on the external database, has not been modified, the hash value of the data can be recalculated and compared it with the hash that is written on the Blockchain. Since Blockchain is immutable, if the hashed match each other the data has not been modified.
- If an individual request his data to be forgotten, one only need to erase the personal data that is stored on the database.
- This approach it can be implemented on both permissioned and permissionless networks.

Blockchange operation

- *Blockchange* is a Blockchain solution which now is GDPR compliant.
- Regarding the right to be forgotten, if the individual requested his data to be deleted the personal data is being deleted from the external database. The “salt” is deleted as well. Thus a brute force attack , in order to extract the initial value, on the hash value stored on the Blockchain is almost impossible.
- Regarding the right to rectification, if the individual requested his data to be modified the following steps are trigged.
    - The updated data is inserted as a new data and a new block is created in the Blockchain.
    - In order to keep track of the modification steps the database links the new block with the old block through its hashes.
    - The old data is deleted from the database
- The implementation of the *Blockchange* utilises the Blockchain as a tool to enhance compliance with the law. One aspect of accountability’s principle is for the controller to keep internal record of the data processing. *Blockchange* satisfies this by storing all the deletions or modifications as transactions on the Blockchain.

Data rectification



Data	Hash Value
Updated data	Updated hash value

Block: #2

Data: Hash Value

Previous Hash:
b566ec3c4447bc25c09a1b49561cb196
a45e6996b13234a4a2e301eeb5463887

Hash:
$2a$10$S1N757meKTImWDVIqCMGFu
OvYPPtzACCbPImt.MUfQCQaVTakjTJO

Block: #3

Data: Hash Value

Previous Hash:
$2a$10$S1N757meKTImWDVIqCMGFu
OvYPPtzACCbPImt.MUfQCQaVTakjTJO

Hash:
$2a$10$L8GuUQIWvf9tFqxW6uWvtuct
xInKSdd7fsRfMCxjzJaeYqJdxkuCC

Block: #4

Data: Updated Hash Value

Previous Hash:
$2a$10$L8GuUQIWvf9tFqxW6uWvtuct
xInKSdd7fsRfMCxjzJaeYqJdxkuCC

Hash:
$2a$10$OrhJWcRQIOHtieqB0MwUGeb
cSp0XbeHrrqDI.DYX1vAWBZ7InctuS

Testing and Evaluation

In order to test the application, automated and manual testing were conducted. The intention of the testing were to evaluate whether the project meets its initial requirements.

The automated tests, which were conducted on the smart contract are the following:

- The first test validates whether the smart contract is successfully deployed on the network.
- The second test validate whether the smart contract can store values on the blockchain.
- The third test validates whether the value that is stored on the Blockchain is the expected value.

The manual tests were performed with intention to validate that the application satisfies the functional requirements. The manual tests which were conducted are the following:

- Data controller can insert data subject’s personal data
- Data controller can delete data subject’s personal data
- Data controller can modify or update data subject’s personal data
- Track changes

The testing have passed and together with the in depth literature review and the research prototype the aim and objectives of the project have been achieved.

Thank you!

Ευχαριστώ

Merci!

Grazie!

¡Gracias!