GDPR and Blockchain Based Applications

Data Protection and Data Retention

Blockchain based applications are the **perfect tools for data retention**. **Data protection for individuals living in the European Union** will be regulated by the European General Data Protection Regulation from May 25th 2018.

In this presentation I will outline basic ideas on how to meet the challenges of the **GDPR**, under the assumption that person related data is uploaded to the ledger of a blockchain based application.

Dipl. Math. X. Bogomolec
Algorithms | IT-Security
Europe, October 2017

GDPR and Blockchain Based Applications

Data Protection and Data Retention

Blockchain based applications are the perfect tools for data retention. Physical deletion of data from the chain is not possible without destroying the integrity of blockchain itself.

On the other side, the GDPR will require the possibility of deletion and blocking of personal data amongst other features in any application addressing users living in the EU from May 25th 2018.

The only way to meet those requirements in blockchain based applications, is to only upload anonymous data to the blockchain, which can be mapped to natural persons by linking the data to the accounts.
Like this, logical deletion, which is accepted by the GDPR can be be enabled within the application.

If an application will not be able to meet such a request, the owning firm will have to pay a penalty of up to 4% of its yearly income.

GDPR and Blockchain Based Applications

Legal and Technical Denotations

The **GDPR** (General Data Protection Regulation) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union.

A **Natural Person** is a person that is an individual human being. (In legal meaning. i.e., one who has its own legal personality)

Person Related Data are informations which relate to an identified or identifiable natural person.

Blocking of Data is a designation of it, such that further processing or usage will be restricted.

Logical Deletion means to make data collections anonymous.

In the following slides, more detailed technical explanations will follow →

GDPR and Blockchain Based Applications

Blocks of Data in Blockchain

A blockchain literally is a chain of blocks of data with ordered entries. The entries are called transactions. They actually were transactions of cryptocurrency in the beginning, but in blockchain based applications they can be any kind of event.

Block 0	**Block 1**	**Block 2**
Transaction 0n_0 ⋮	Transaction 1n_1	Transaction 2n_2
Transaction 00	Transaction 10	Transaction 20

⟶ ⟶ ⟶

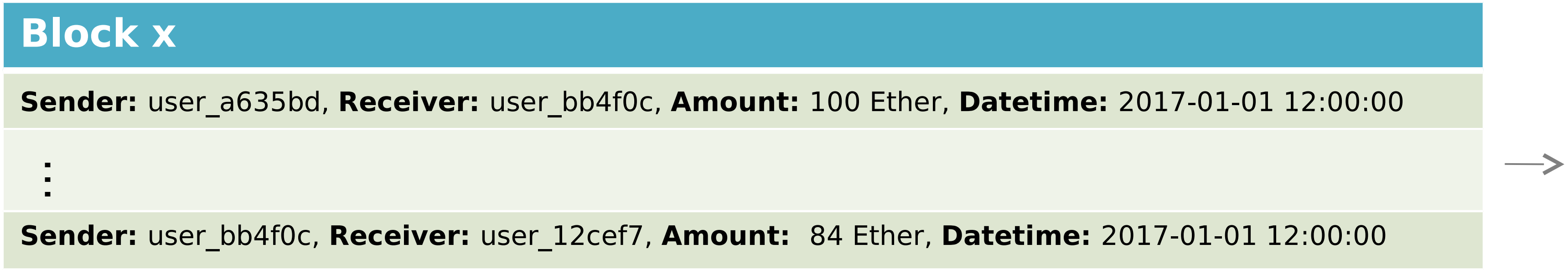
The denotations n_0, n_1, n_2, … show that the number of transactions in a block can vary.

A closer look at a transaction →

GDPR and Blockchain Based Applications

Blocks of Data | Deletion by User

A transaction is a collection of informations. For example it can be:



Block x

Sender: user_a635bd, **Receiver:** user_bb4f0c, **Amount:** 100 Ether, **Datetime:** 2017-01-01 12:00:00

⋮

Sender: user_bb4f0c, **Receiver:** user_12cef7, **Amount:** 84 Ether, **Datetime:** 2017-01-01 12:00:00

In this example, the transactions can only be related to the natural persons, if the user IDs (e.g. user_a635bd) can be linked to their accounts.
As soon as an account is deleted, the data in the blockchain can be considered anonymous.

If someone kept track of a user’s ID and his identity, a linking to the person will still be possible. But if that happened out of the scope of the application, it will also be out of control of the GDPR.

Other kinds of information collections →

GDPR and Blockchain Based Applications

Deletion after Rentention Expiration

When building a blockchain based application, one will have to be very careful about the data that is uploaded to the blockchain.

In accounting for example, not only person related data, but also contract related data has to be deleted after the legally defined retention time (e.g. 10 years).

But you cannot delete an account of a person to unlink the proof of a business transaction, as long as the person still uses the application.

In this case, the business transaction should get an ID itself, which is stored in the users account and can be deleted after the legally defined retention time.

Deletion by user owned transaction →

GDPR and Blockchain Based Applications

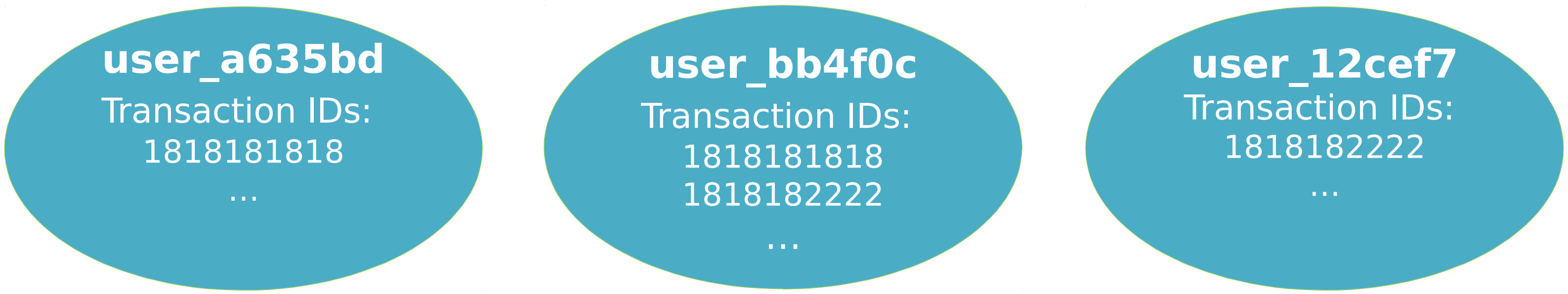
Blocks of Data | Deletion after Retention Expiration

Block x

Transaction ID: 1818181818, **Amount:** 100 Ether, **Datetime:** 2017-01-01 12:00:00

⋮

Transaction ID: 1818182222, **Amount:** 84 Ether, **Datetime:** 2017-01-01 12:00:00



user_a635bd
Transaction IDs:
1818181818
…

user_bb4f0c
Transaction IDs:
1818181818
1818182222
…

user_12cef7
Transaction IDs:
1818182222
…

The transactions can be related to the users by transaction IDs in the user’s account. As soon as the legal retention time is expired, the transaction IDs can be deleted in the users accounts and thus the proof of transaction is logically deleted.

Deletion by user owned transaction →

GDPR and Blockchain Based Applications

Considerations of information collections

If a collection of informations is considered person related or not has to be reviewed by **legal experts**.
For example the following collections of data would be considered as person related or not:

Data Collection	Person Related
John Smith	yes
iPhone 7	no
John Smith, iPhone 7	yes
Man, 43 years, iPhone 7	no
Man, 43 years, iPhone 7, MAC-address 23-DE-A4-00-1B-8F	yes
Man, 43 years, Contract Number 123456	yes

Cooperation of technical and legal experts →

GDPR and Blockchain Based Applications

Cooperation of technical and legal experts

How to enable logical deletion in the context of a blockchain based application has to be decided by **technical experts**.

For a sensible planning, **a team of legal and technical experts** has to work together and determine the handling of storage of data in the blockchain and the accounts of the users before the first actual block is uploaded!

Data Protection by Design and by Default can be applied by proceeding like this.

Because no block nor transaction can be deleted from a blockchain without destroying its integrity!

More hints in the context of blockchain based applications and the GDPR →

GDPR and Blockchain Based Applications

More to think about...

Consent requires a clear understandable form which has to be agreed upon before a user signs up to an application.

Right of Revocation means that users must have the possibility to revoke their consent.

Right to Erasure is handled by physical or logical deletion of data.

Blocking of data has to be considered in a similar way.

Right to portability might require tools to read from a blockchain such that personal informations can be sent to third parties.

There is a lot that has to be considered!
And note that blockchain isn’t the new internet, it runs on the old internet:-)