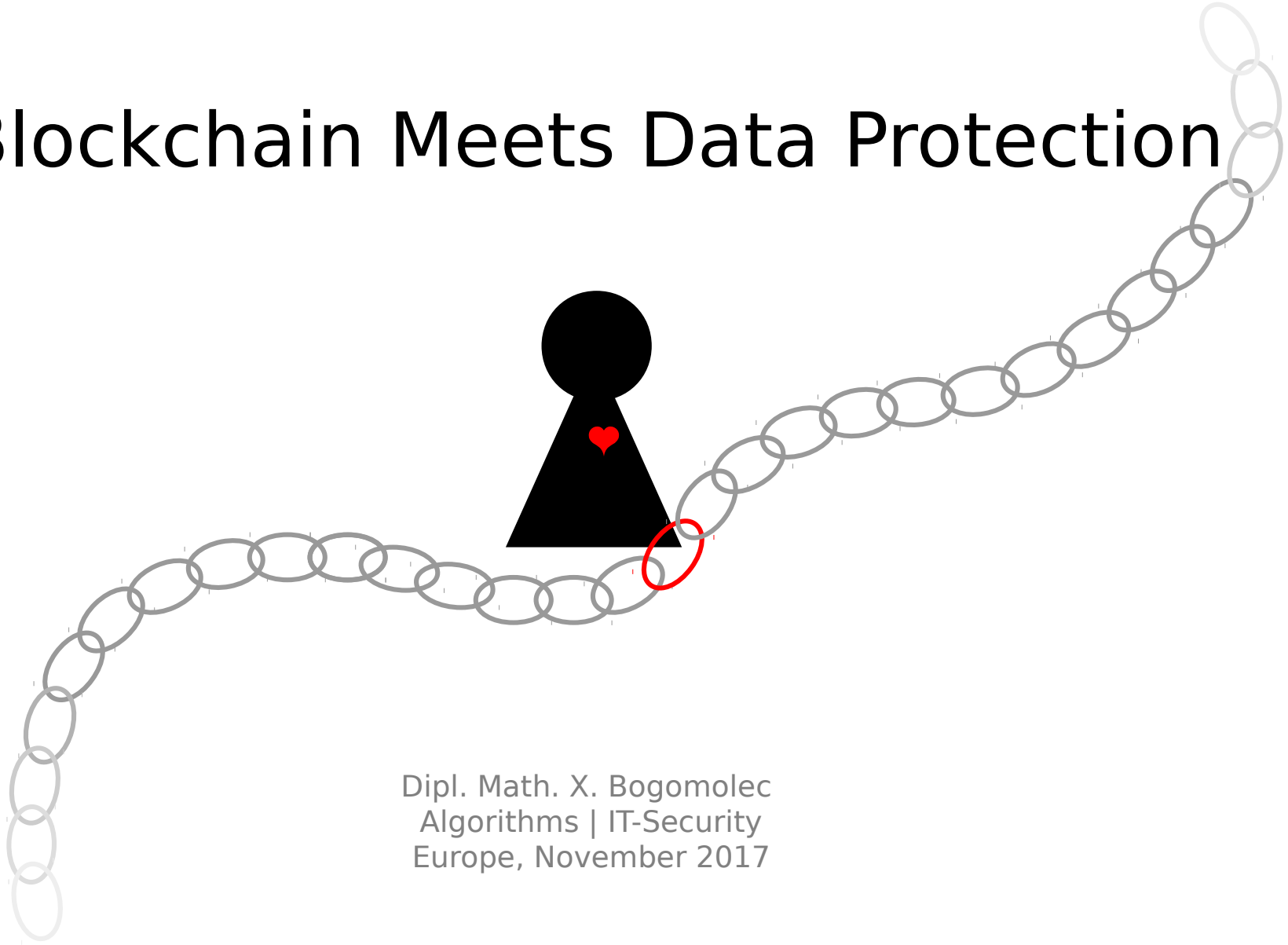
Blockchain Meets Data Protection



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

About Me

Education

Mathematics

Work Fields

from Computer Algebra to IT-Security

Projects

TiiQu (Ethereum) | CeuniX (http://ceunix.eu/)

Motivation

Love for Symbolic Languages | Sharing Knowledge | Protection of People's Personal Freedom

For a good introduction into the blockchain topic check out Silvan Jongerius's slides!

contact: indigomind@protonmail.ch

Data Protection in Europe

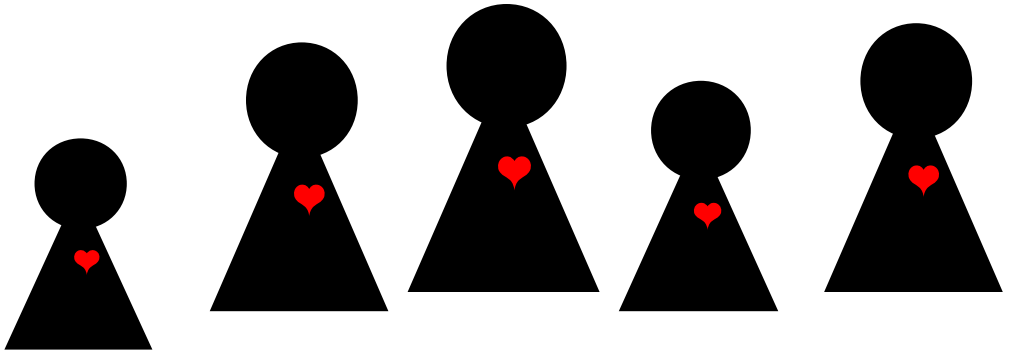
GDPR (General **D**ata **P**rotection **R**egulation)

- minimum requirement for data protection laws of EU-countries
- strengthen and unify data protection for all individuals living in the EU

Worldwide Uniqueness

While we can complain about weaknesses, loopholes or bad implementations of data protection, we have to appreciate the effort of the EU to protect its citizens.

As far as I know there is nothing similar being issued in the rest of the world. I would love to be corrected though!



Data Protection in Europe

Some Tech Requirements for Compliance

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

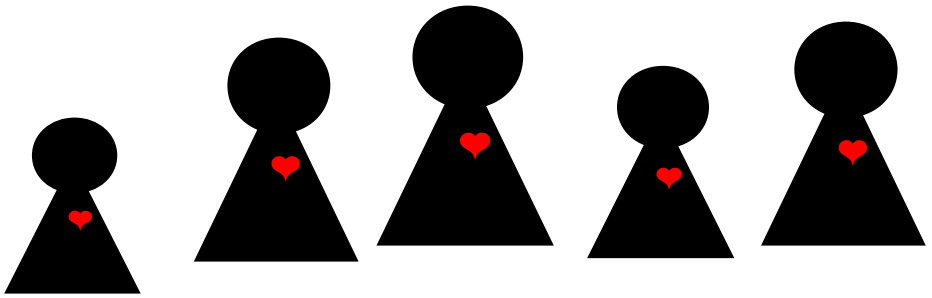
Right of Access means that a user is allowed to have insight into the data relating to him/her.

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

Right of Revocation means that users must be able to revoke their consent.

Blocking of Data is marking of data such that its processing can be restricted.

Right to Portability requires the possibility of data transfer to third parties.



Blockchain Technologies

Alternative Financial Market

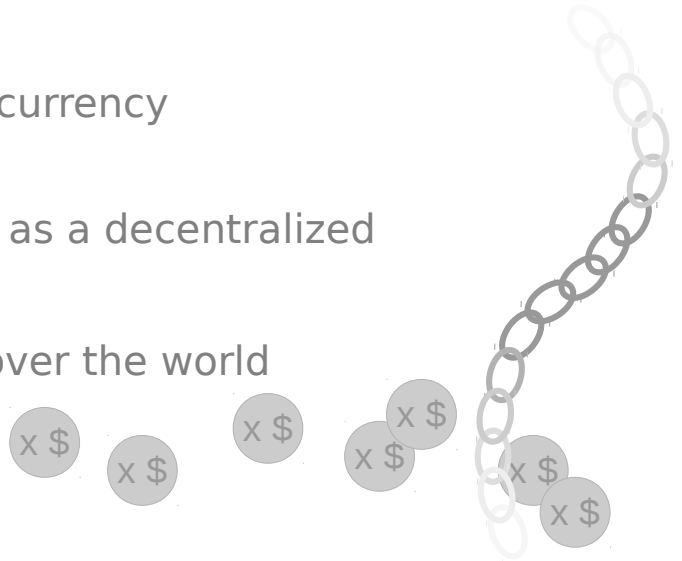
Built for Perfect Data Retention

Originally, the blockchain protocol was built for Bitcoin, in order to offer

1) an alternative financial market
2) a possibility to invest electrical energy into a digital currency

The “bank” for this monetary values should be realized as a decentralized database with

- Limitless copies of the transactions on machines all over the world
- Verifiable content from the first data entry



One single copy of the database is enough to prove what happened * from the beginning!

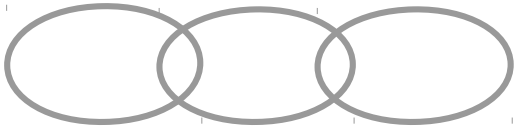
* “happened” in the sense of what was digitally agreed upon in the community

Blockchain Technologies

Architectural Components

Distributed Ledger

- actual chain of data blocks
- distributed all over the world in open networks

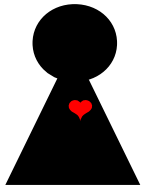


Nodes/Pools

- machines or collections of machines
- determine the order of the transactions within data blocks

Accounts

- represent members of the network
- can send or receive transactions
- located on devices such as PC’s or mobile phones

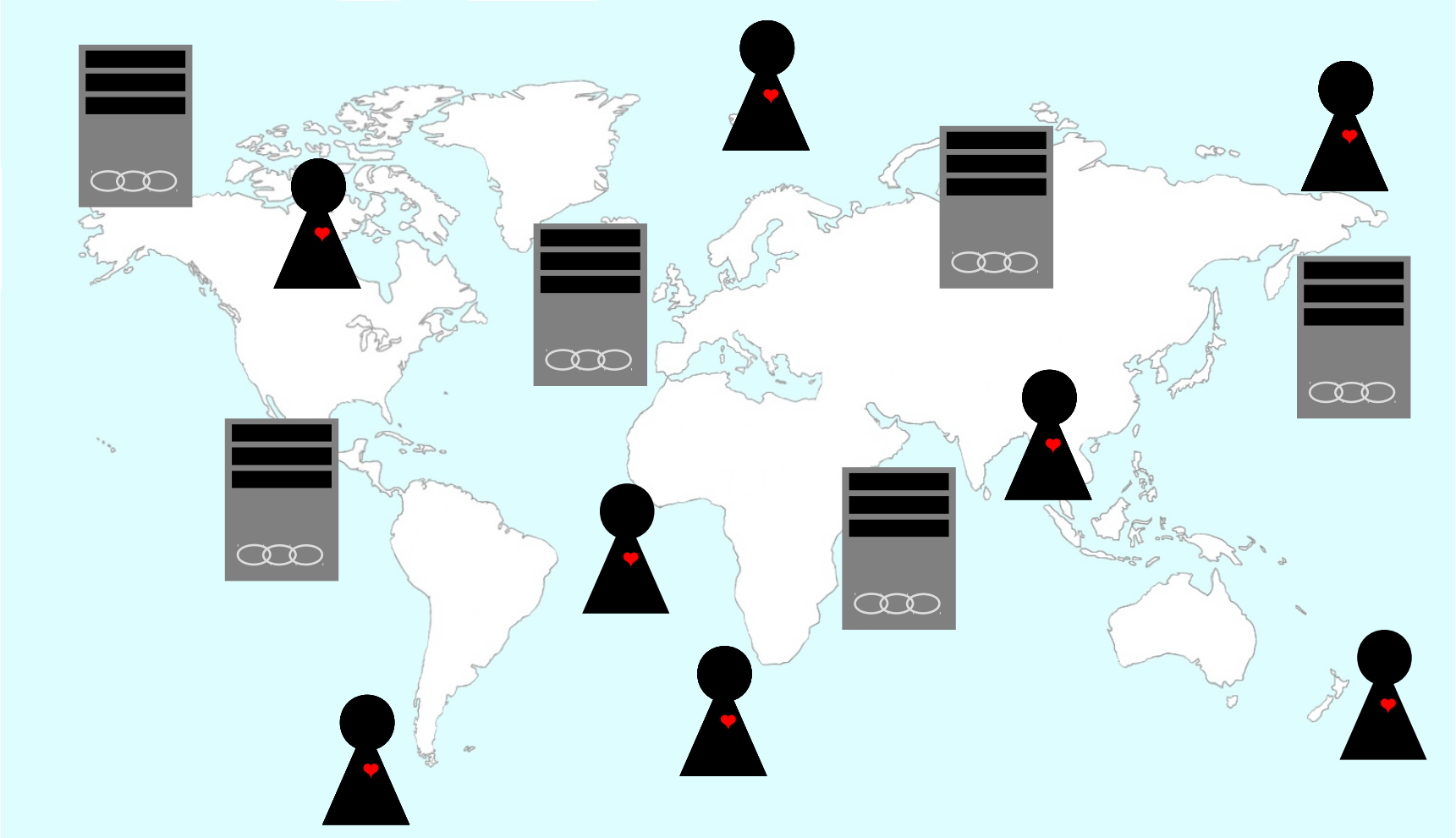


Other instances (e.g. webservers)

- serve information about the ledger to accounts
- act as controlling instances for network communication

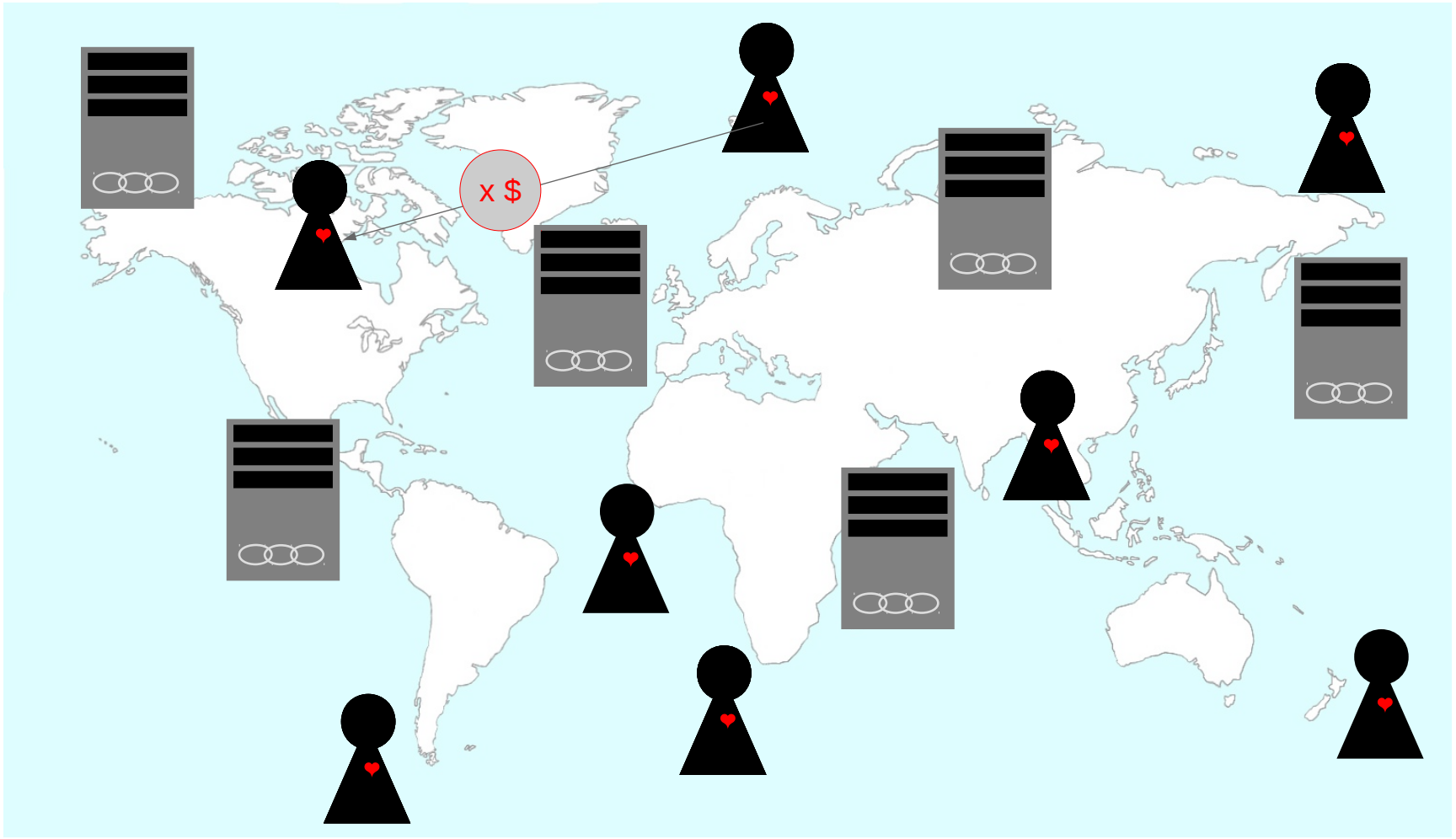
Blockchain Technologies

Schematic View of Architecture with Regard to Network



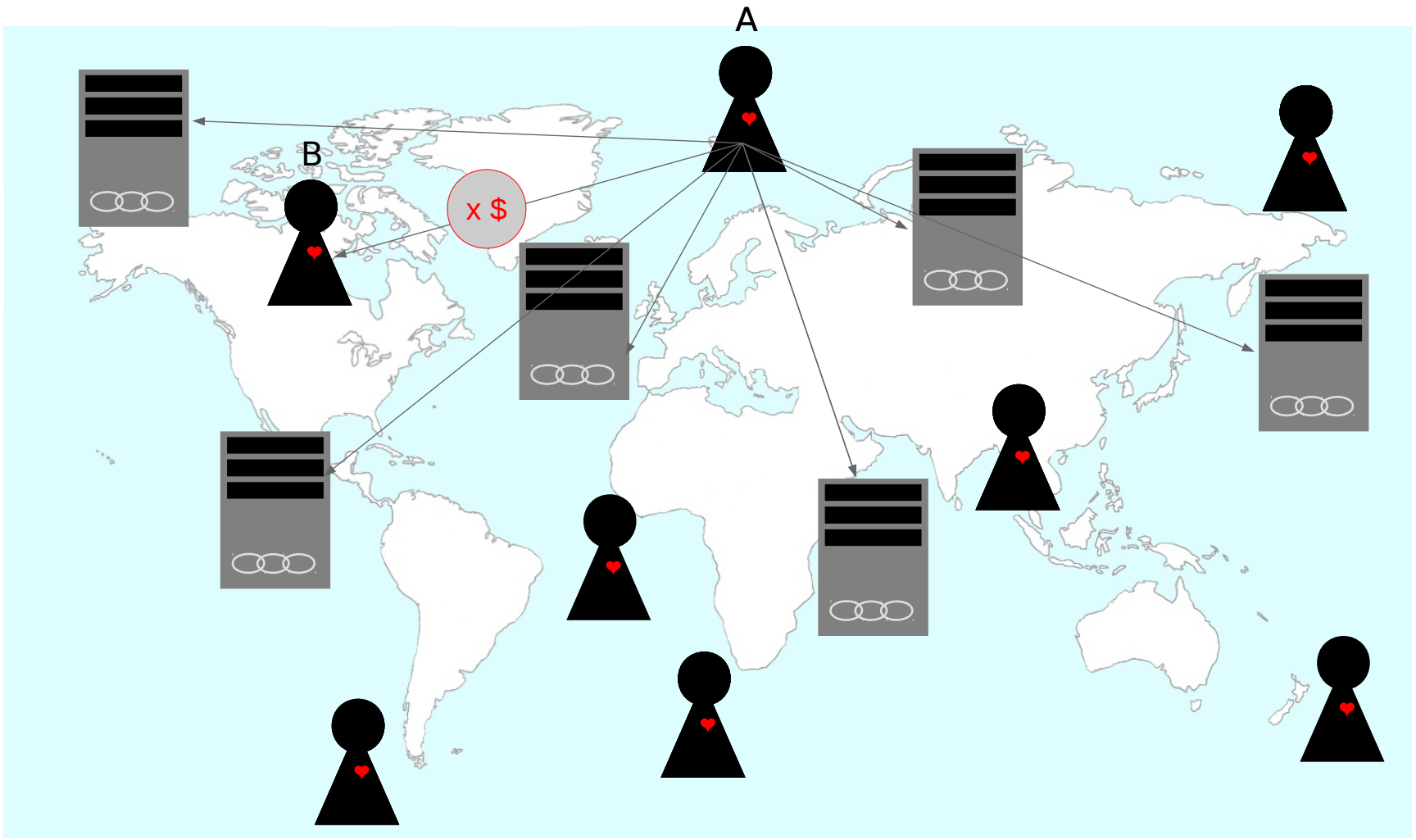
Blockchain Technologies

Information Flow | Transaction



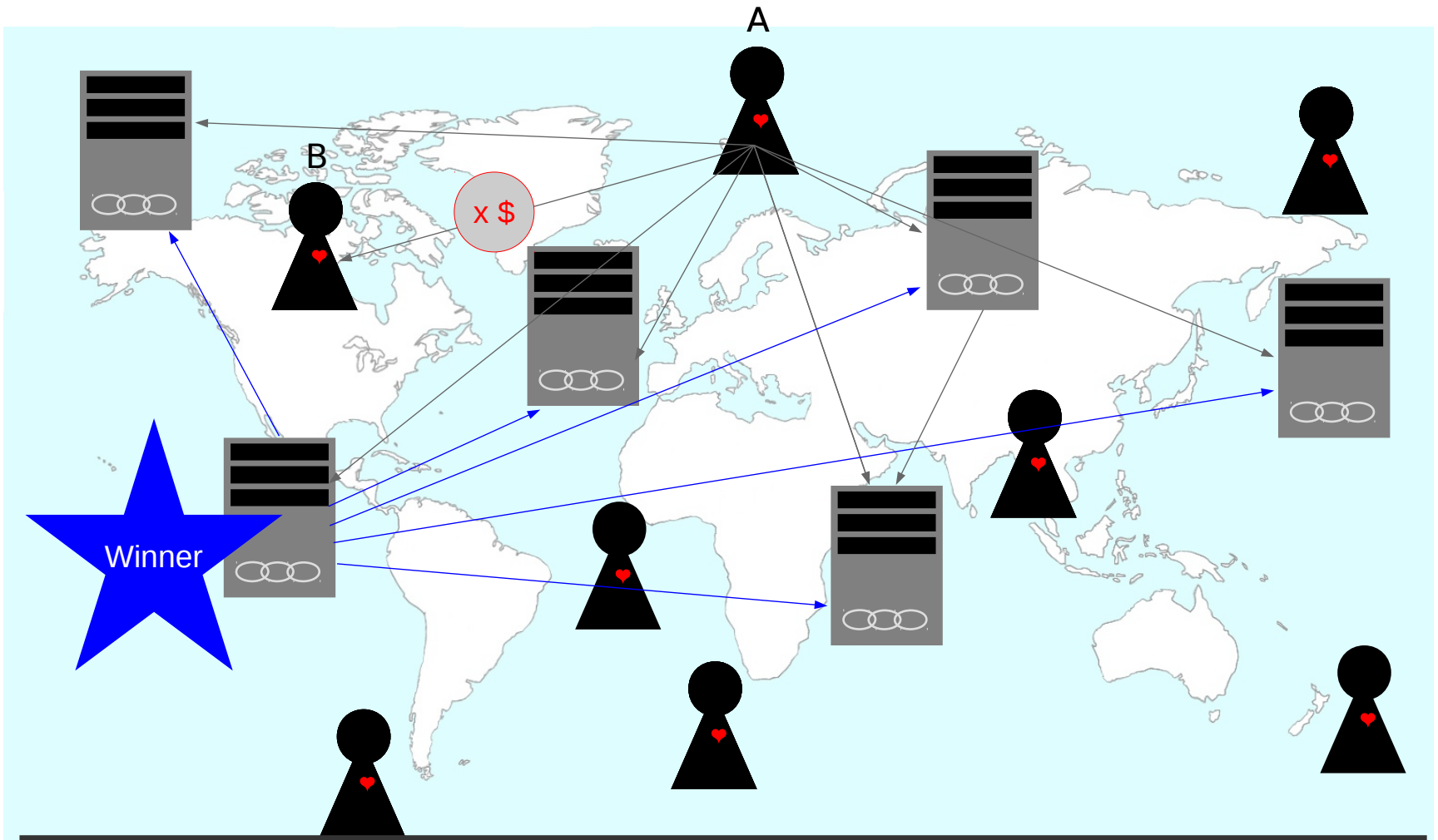
Blockchain Technologies

Information Flow | Transaction Info Distribution



Blockchain Technologies

Information Flow | Proof of Work/Stake* Distribution



* Contest for which node is allowed to determine the order of the transactions in a block.

Blockchain Technologies

From Coin Transfer to Smart Contracts

Meaning of Transactions

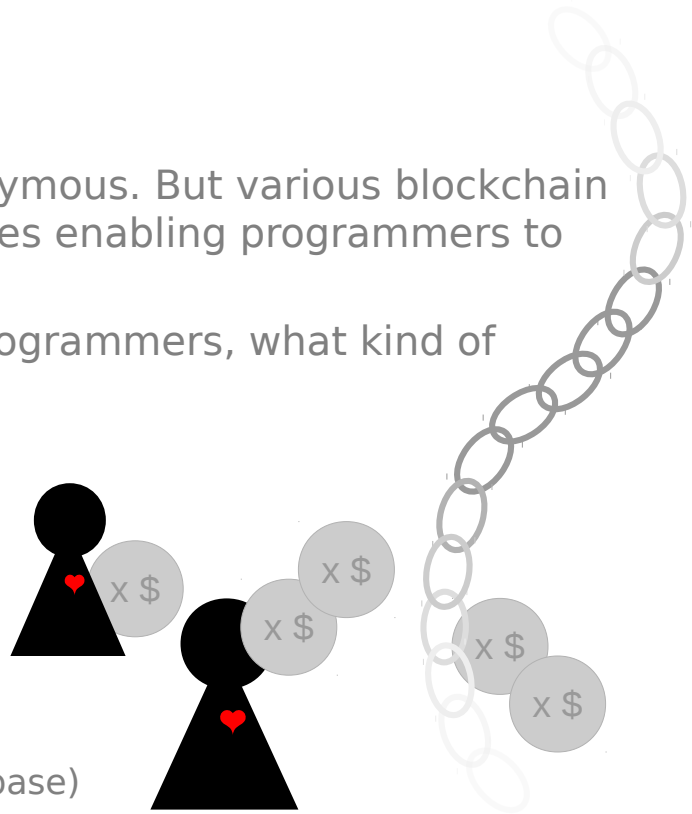
Bitcoin or other crypto currencies: Transfer of monetary values

Smart contracts: Any kind of event

Data in the Great Wide Open

Traditional blockchain: uploaded data usually is anonymous. But various blockchain based applications, e.g. Ethereum are virtual machines enabling programmers to run their own code on top of the given functions.

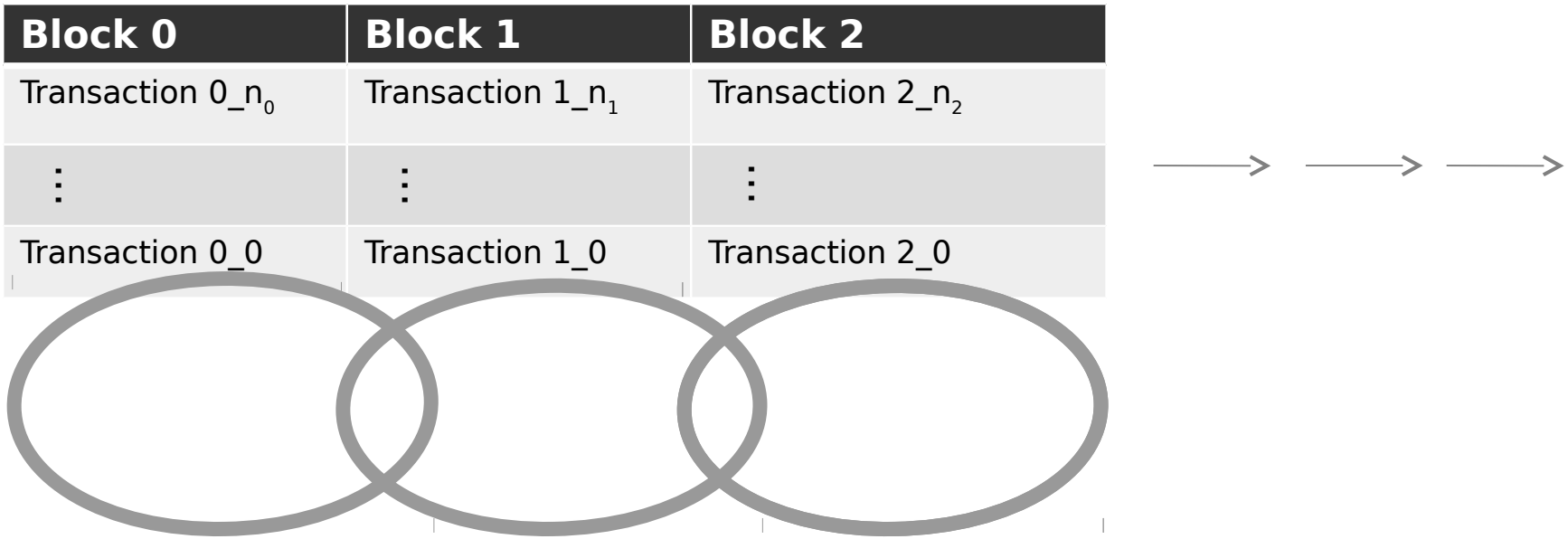
For **smart contracts** it is under the control of the programmers, what kind of data is uploaded to the so called **ledger** *.



* The actual chain of blocks of transactions (distributed database)

Blockchain Technologies

Blocks of data with ordered Transactions



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

Blockchain Technologies

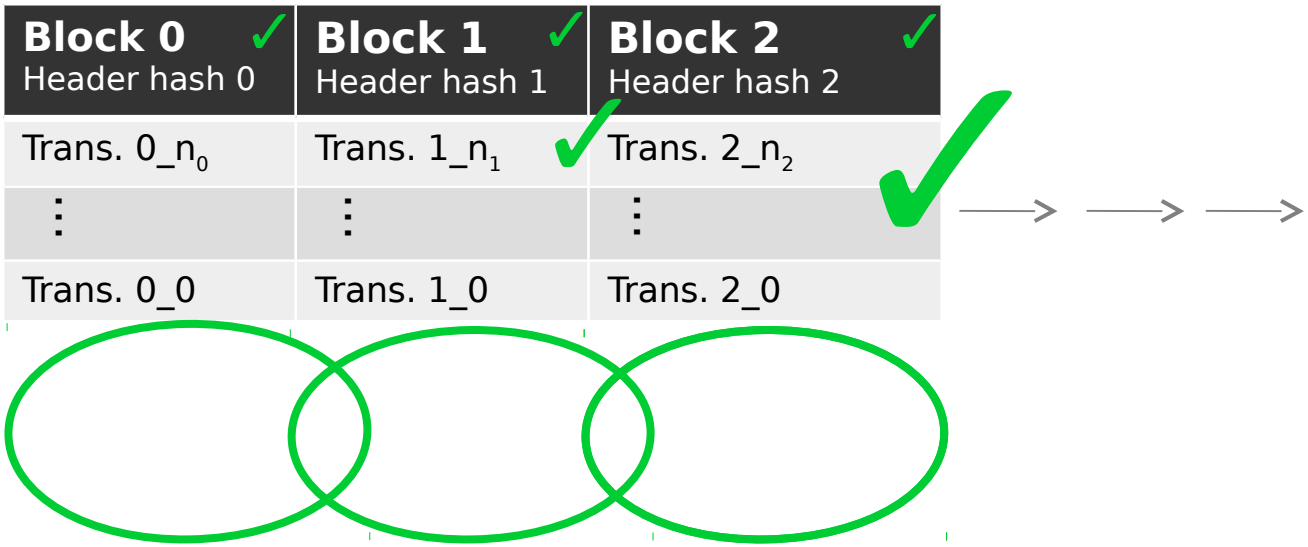
Fixing Order and Content of Transactions

First block:
hash of its own content

All following blocks:

hash of their own content + the header hash of the previous block

With one header hash, all previous blocks can be verified!



Blockchain Technologies

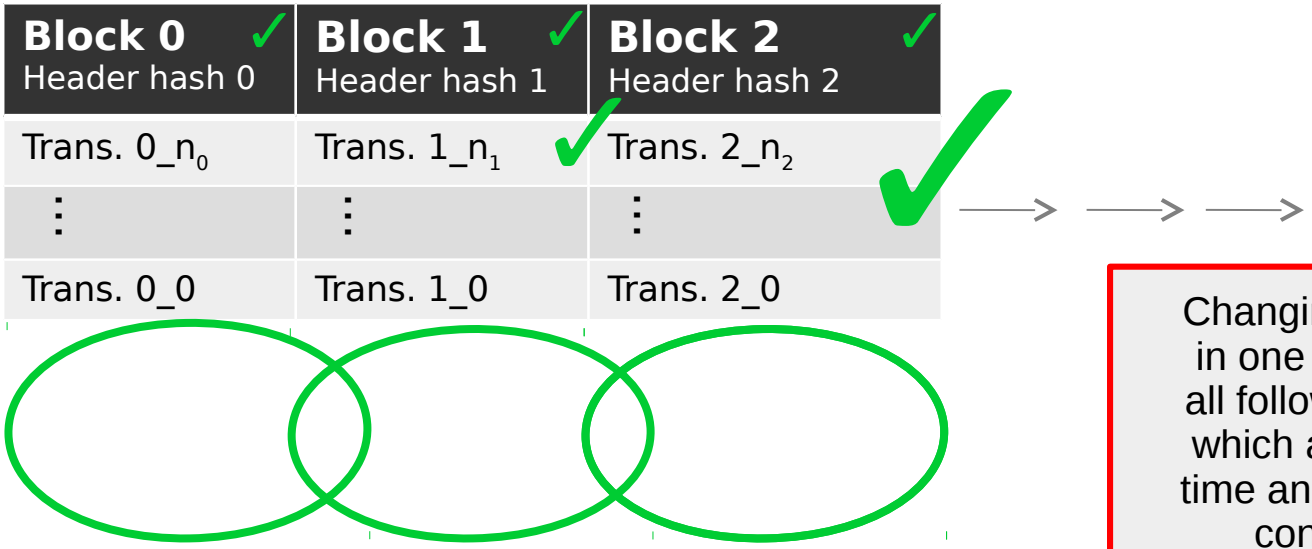
Fixing Order and Content of Transactions

First block:
hash of its own content

All following blocks:

hash of their own content + the header hash of the previous block

With one header hash, all previous blocks can be verified!



Changing a single character in one block would change all following header hashes which are determined by a time and energy consuming consensus protocol!

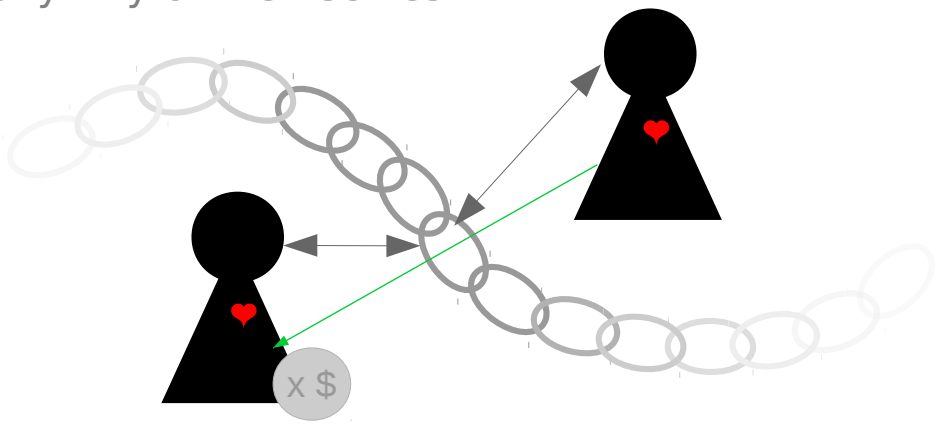
Blockchain and Data Protection

Transactions in Blocks are Data Collections

Block 0 Header Hash 0
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

These transactions can only be related to the sender and receiver, if the user's IDs (e.g. user_a635bd) can be linked to the users as natural persons.

If this information is stored in their own accounts only, the users have complete control over the anonymity of themselves.



Blockchain and Data Protection

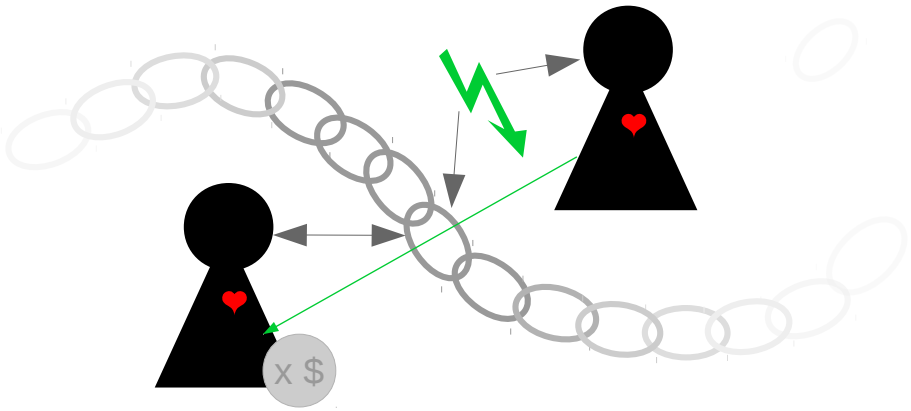
Location of Person Related Data | Possibilities

If each participant's personal data is stored in his own account only:

Only the user can see that the transaction belongs to himself. For everybody else, the data in the blockchain is anonymous *✓

If each participant's personal data is stored in both user's accounts but nowhere else:

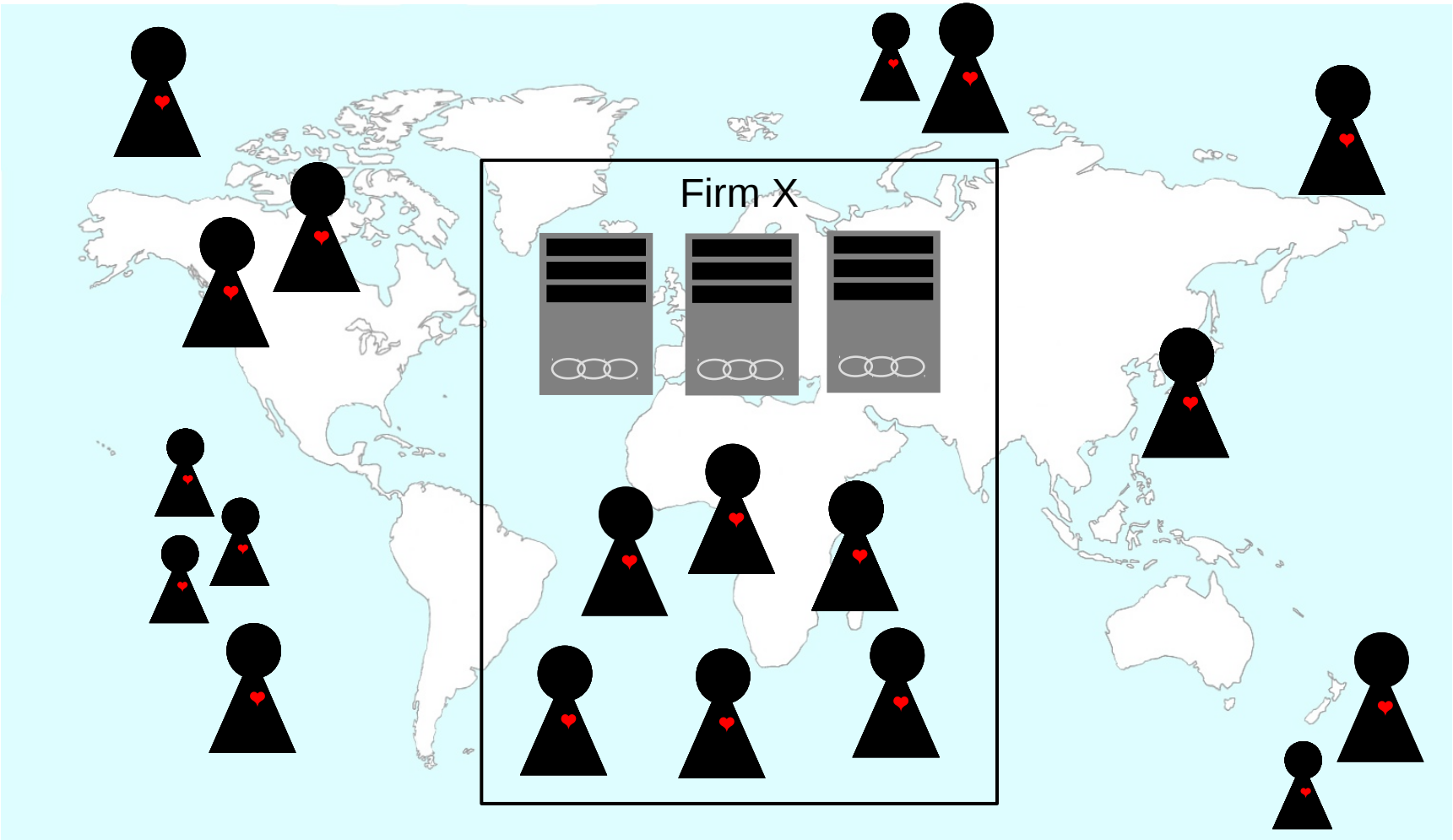
Both users can see that the transaction belongs to themselves and the other user. If one of the users wants to make the transaction anonymous, a function to delete the personal information in the other account has to be available. ✓



* If the network activities are not being monitored and related to a person by other criteria like IP addresses etc.

Blockchain Technologies

Private Blockchain | Firm X with internal and external Users



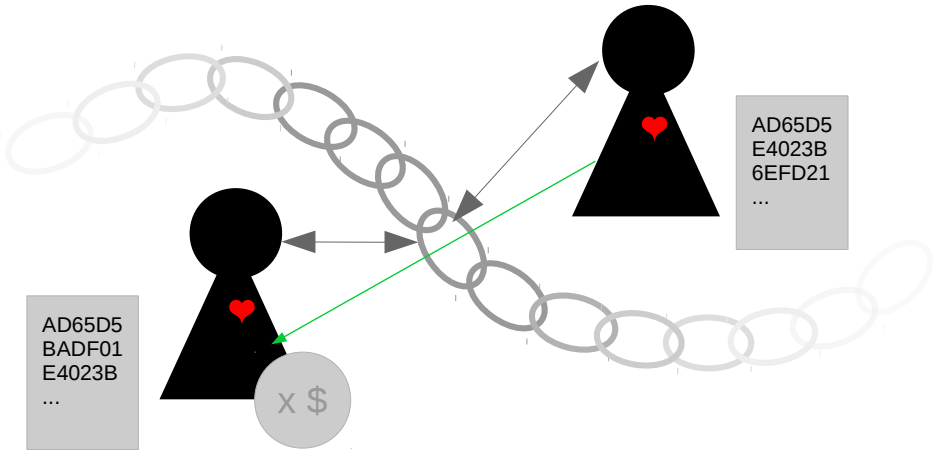
Blockchain and Data Protection

Accounting Use Case in private Blockchain | Nested Identifiers

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

Given the example of a company having its own blockchain and the accounts of participants on the company's computers. Then they cannot delete an account of a participant to unlink the proof of a business transaction, as long as the participant still uses the application.

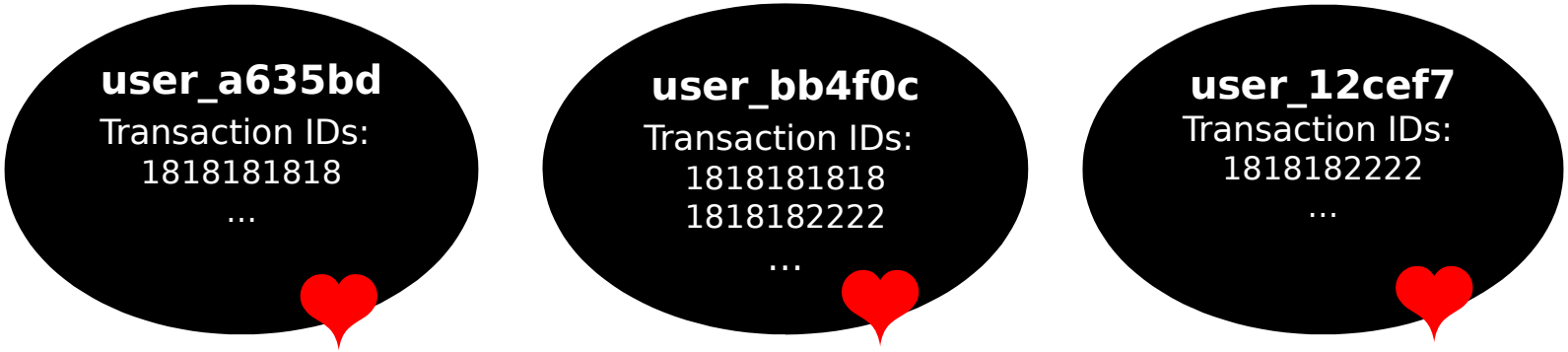
In this case, the business transaction should get an ID itself, which is stored in the user's account and can be deleted after the legally defined retention time.



Blockchain and Data Protection

Accounting Use Case | Nested Identifiers

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



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.

Blockchain and Data Protection

TiiQu Platform

TiiQu is a blockchain based platform for companies and independent experts.

TiiQu profiles are

- digital professional “passports”
- can be relied on as proof of an individual's trustworthiness, identity, qualifications, certifications, memberships, previous work experience, performance metrics and education.

TiiQu is in development and starting its first run with test users and institutions soon.

More Infos:
http://tiiqu.com/

White Paper:
https://github.com/TiiQu-Network/TiiQu-Network/wiki/White-Paper

Blockchain and Data Protection

TiiQu Platform | Use Case Member Certificate

Block x
University ID; Certificate Hash; Signature; University's Public Key;
⋮
Alumnus ID; Certificate Hash; Signature; Alumnus' Public Key;

If both university and alumnus have uploaded the hash of the certificate and verified the other ones upload and signature, the alumnus' certificate is confirmed.

Data Protection and Blockchain

Requirements Check

Consent ✓ independent from ledger

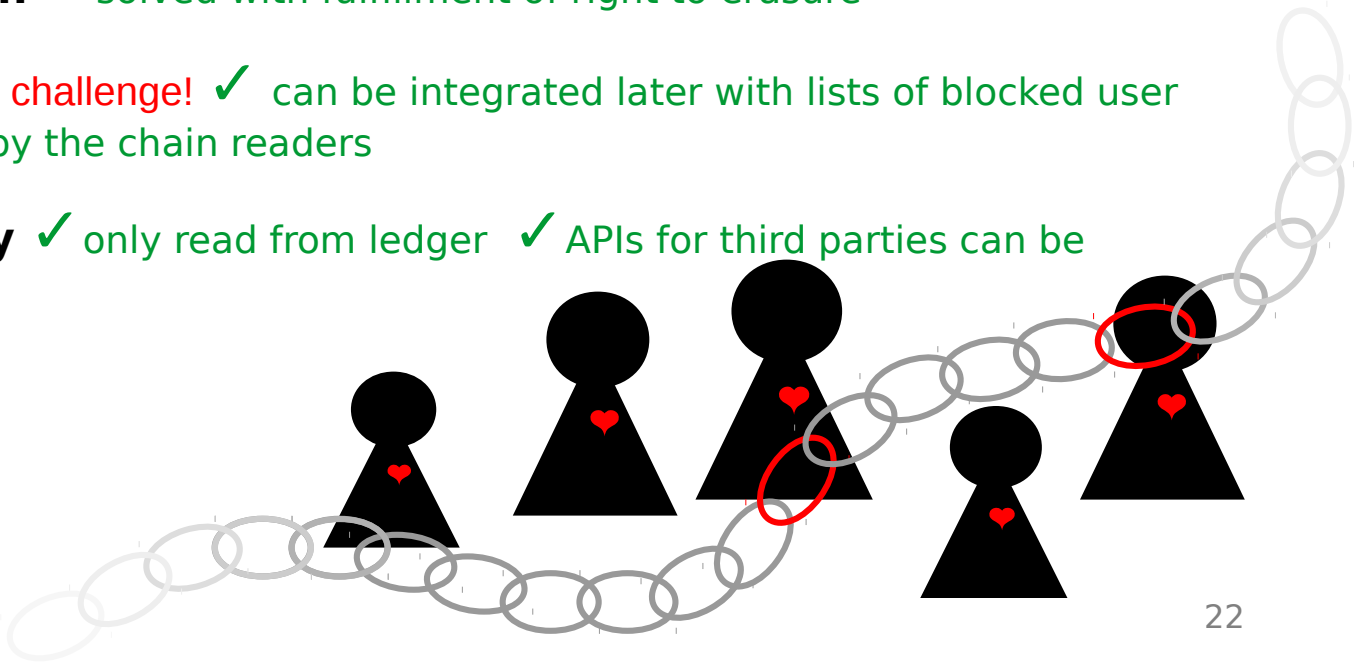
Right of Access ✓ only read from ledger ✓ usually already integrated (blockchain readers, e.g. Etherscan, mobile wallets, accounts)

Right to Erasure → challenge!!! Has to be planned before the first block!

Right of Revocation ✓ solved with fulfillment of right to erasure

Blocking of data → challenge! ✓ can be integrated later with lists of blocked user IDs taken into account by the chain readers

Right to portability ✓ only read from ledger ✓ APIs for third parties can be implemented any time



Data Protection and Blockchain

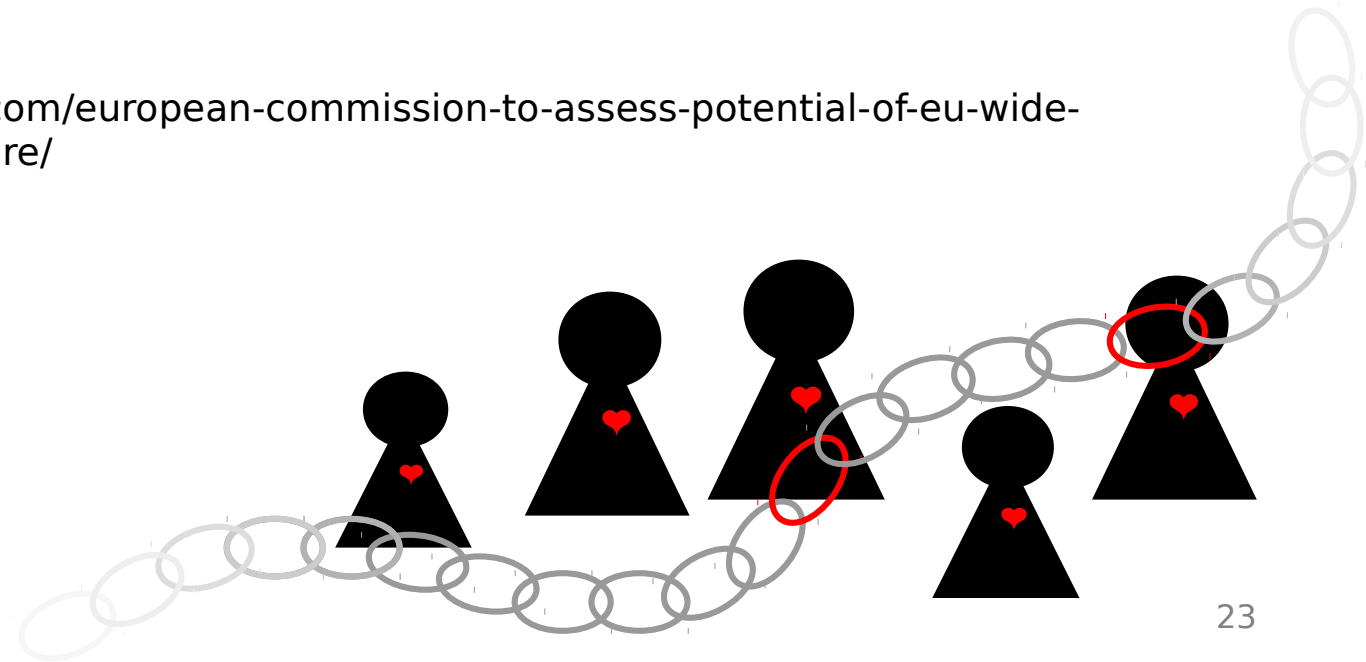
Unanswered Questions

The requirement to fulfill the Right to Erasure in the context of blockchain based applications is not yet finally officially clarified. It has been decided 05/2014 (WP 216) that hashing will generally be considered a pseudonymisation technique, not an anonymisation technique, because it allows linking of data.

From a mathematical perspective this is not correct, because hashing only allows linking from sourca data to the hash value, but not the other way around.

As the EU-comission also assesses the potential of an EU-wide blockchain infrastructure, guidelines for GDPR compliance in the context of blockchain technologies will have to be defined:

https://www.coindesk.com/european-commission-to-assess-potential-of-eu-wide-blockchain-infrastructure/



Data Protection

Data Collections

If a collection of informations is considered person related or not has to be reviewed by **legal experts**.

Data Collection	Person Related
John Smith	✓
iPhone 7	✘
John Smith, iPhone 7	✓
man, 43 years, iPhone 7	✘
man, 43 years, iPhone 7, MAC-address 23-DE-A4-00-1B-8	✓
man, 43 years, contract number 123456	✓
internet user, geolocation, date 1, time 1	???
internet user, geolocation, date 2, time 2	
internet user, geolocation, date 3, time 3	

Data Protection and Blockchain

Cooperation of Legal and Technical Experts

Legal experts
… have to decide which data collections might be considered person related.

Technical experts
… have to decide how to enable logical deletion in the context of a blockchain based application.

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

About Me

Education

Mathematics

Work Fields

from Computer Algebra to IT-Security

Projects

TiiQu (Ethereum) | CeuniX (http://ceunix.eu/)

Motivation

Love for Symbolic Languages | Sharing Knowledge | Protection of People's Personal Freedom

Thanks for the kind slide consultancy of Christoph Neumann!

contact: indigomind@protonmail.ch