Data Protection in the Scope of Distributed Ledger Technologies

Dipl. Math. X. Bogomolec
Algorithms | IT-Security
Berlin, May 2018

About Me

Education

Mathematics

Work Fields

Algorithms | IT-Security

Projects

TiiQu (https://tiiqu.com) | CeuniX (http://ceunix.eu/) | Banks (confidential:)

My Re:Publica Mission

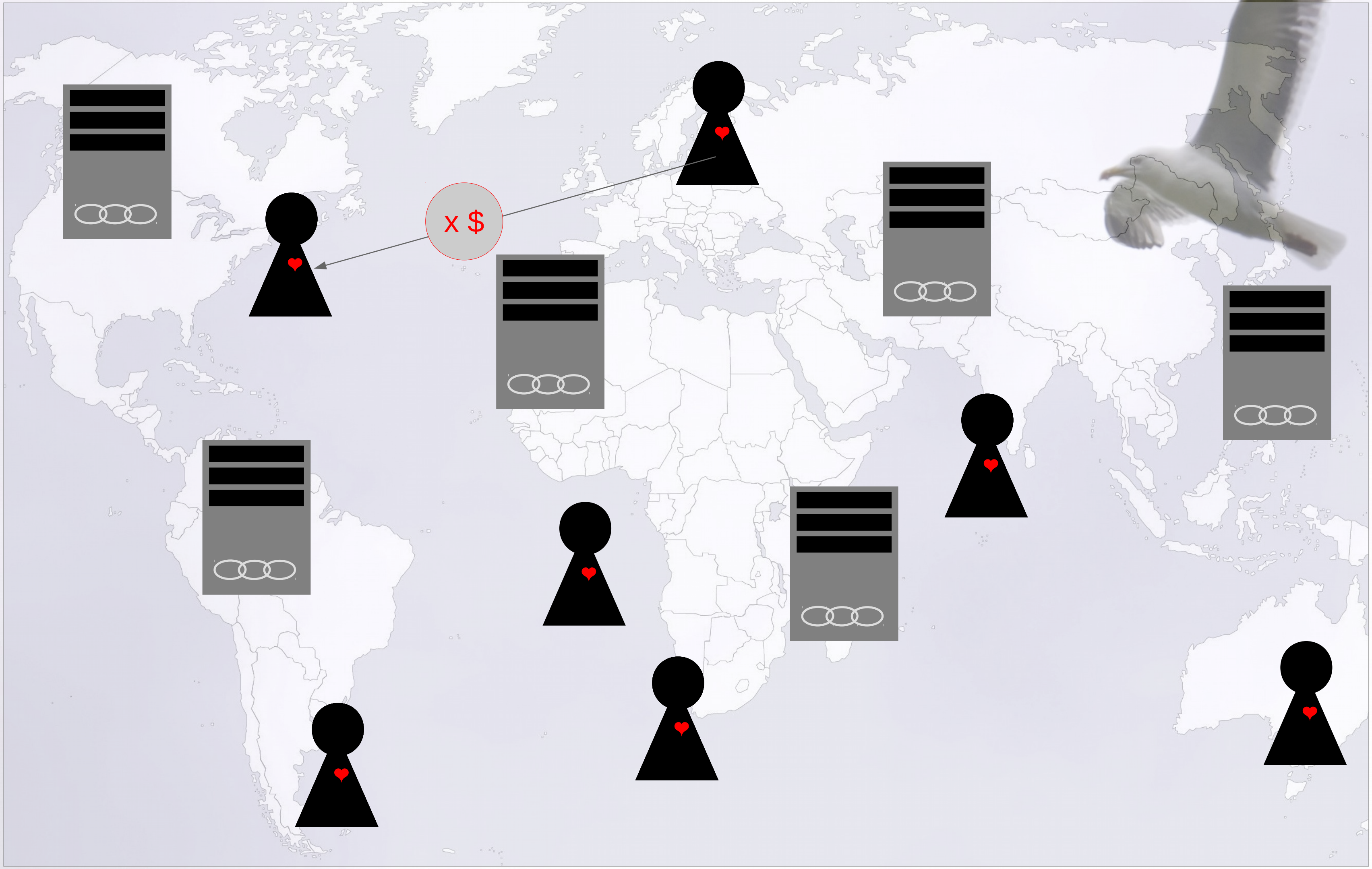
Guiding you through darkness to the light

The information from this presentation can be used under the GNU GPLv3 License:
https://www.gnu.org/licenses/gpl-3.0.de.html

contact: indigomind@protonmail.ch

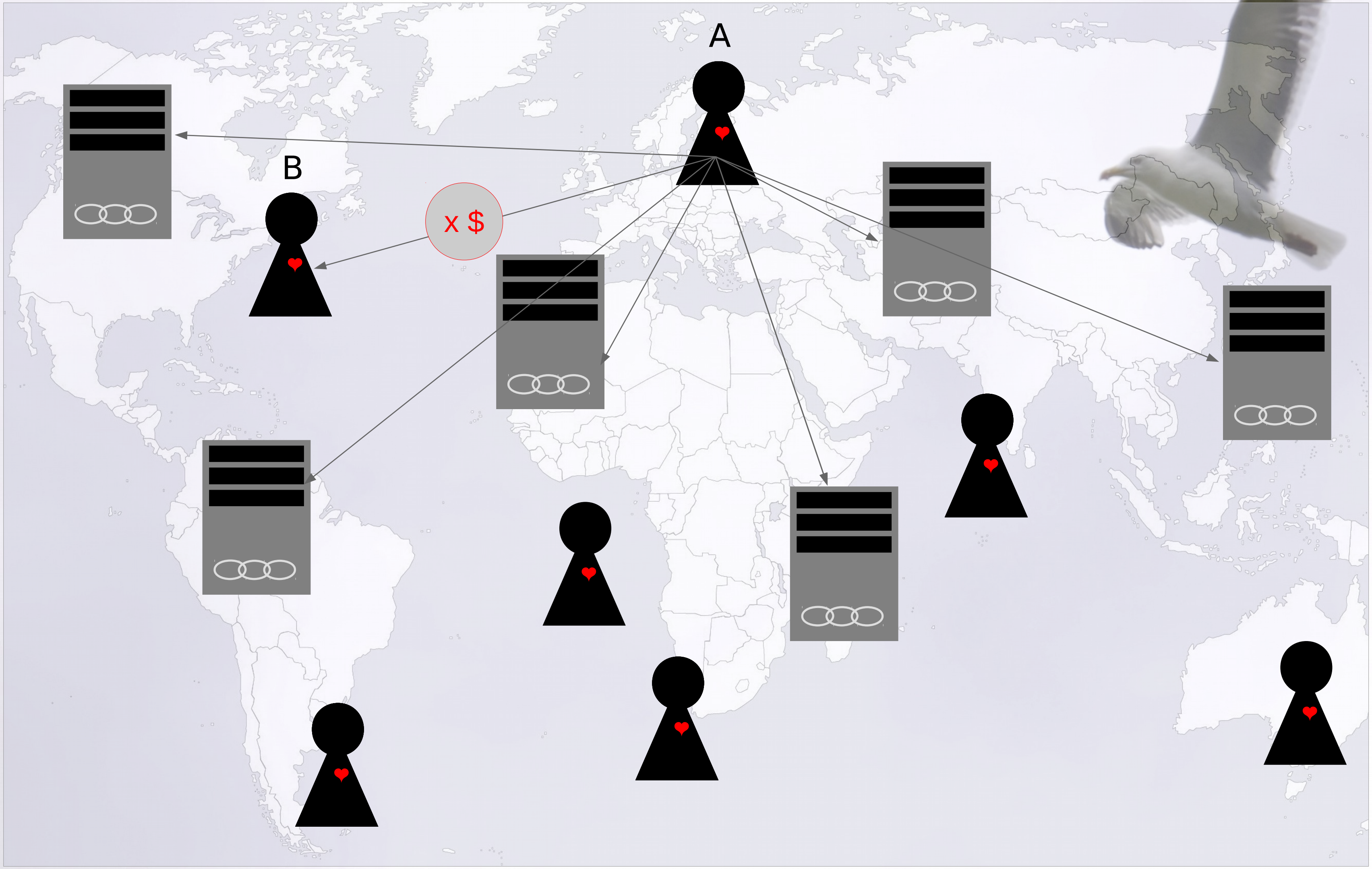
DLTs

Public Blockchain | Transaction



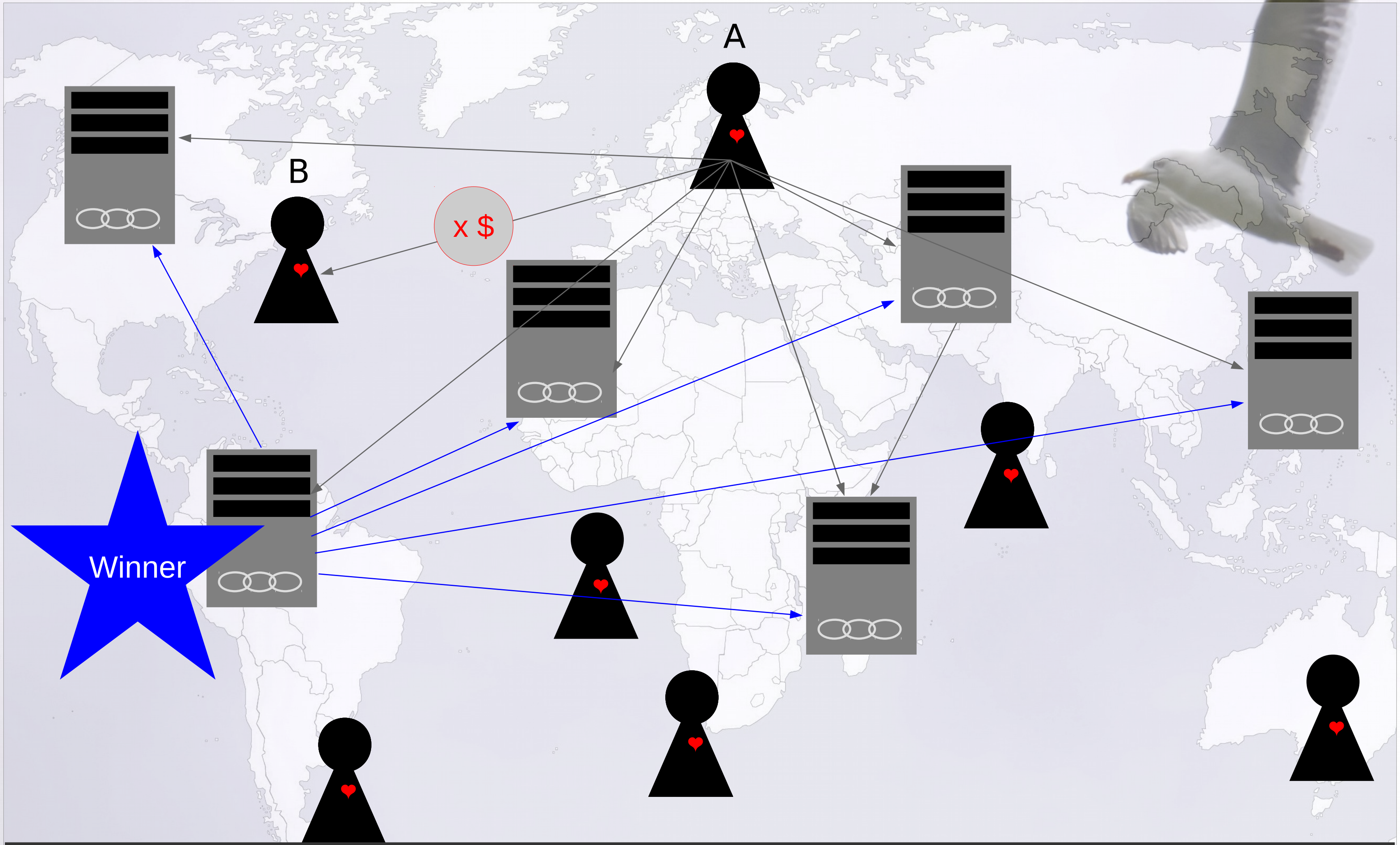
DLTs

Public Blockchain | Transaction Info Distribution



DLTs

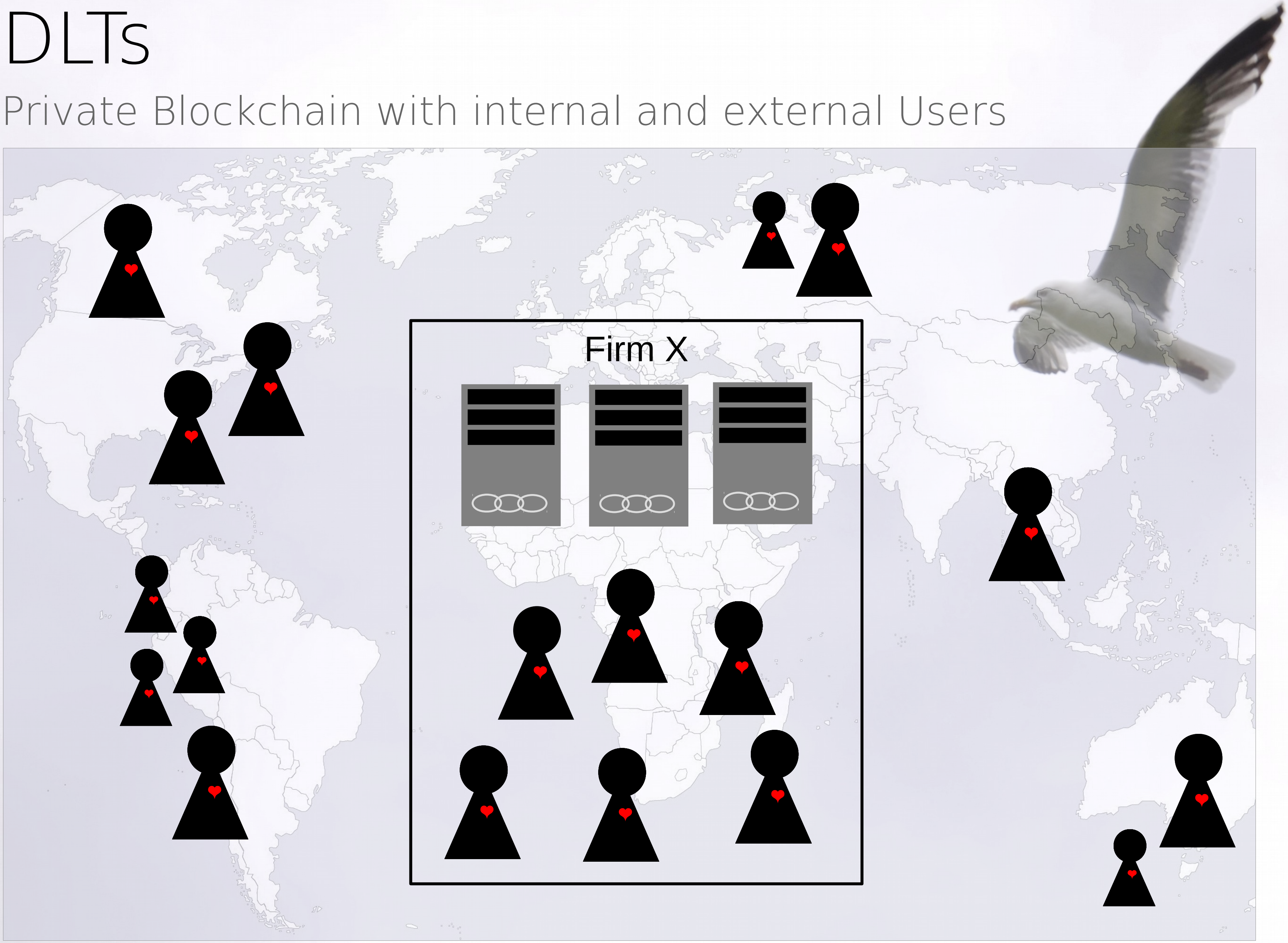
Public Blockchain | Proof of Work/Stake* Distribution



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

DLTs

Private Blockchain with internal and external Users



DLT Facts

Explaining Myths

Is Blockchain the new Internet?

Blockchain mostly runs on the old internet!

Do Blockchain users have complete control over their data?

Data which is once uploaded can neither be deleted nor changed
Sensitive data can neither be deleted nor changed
Wrong data can neither be deleted nor changed

Do you believe you have control over your data if it is accessible by everyone?

What about encrypted data on the Blockchain?

Crypto Facts

Status Quo

- GDPR accepts anonymous data on ledgers only
- Encrypted personal data is still considered personal and not anonymous
- For encrypted data on ledgers keys have to be shared with authorized participants

- Classical asymmetric Crypto is about to expire
- NIST has begun a standardization process of new crypto algorithms in 2017
- ITU discusses if public keys have to be considered personal data

GDPR Proof Solutions

Status Quo

Use Blockchain for completely anonymous data

Anonymized big data sets accessible for everyone to use for predictive analysis or simple knowledge transfers.

Use Blockchain for verifications of offchain data

With one way linking mechanisms (E.g. Zero Knowledge Proofs) data integrity can be verified by participants who have copies of the data.

(Hashing is not accepted as anonymization by the Working Party:-( )

Financial DLT Hacks

History of Examples

DAO Hack

https://wired.de/collection/business/wie-aus-dem-hack-des-blockchain-fonds-dao-ein-wirtschaftskrimi-wurde/

12 Bitcoin Hacks

https://arstechnica.com/tech-policy/2017/12/a-brief-history-of-bitcoin-hacks-and-frauds/

Financial DLT Hacks

Possible Examples

Your mobile wallet

- Has not enough storage space for the blockchain
- Connects to a central server storing a blockchain
- Gets your individual information from this server

If the server is hacked, he might send you manipulated information

Financial DLT Hacks

Possible Examples

Your mobile or desktop wallet

If your device is hacked, and the attacker gets access to your private key, he can authorize transactions in your name.

How likely is it that this is going to happen?

- Remember ransomware hacks 2017!
- How interesting get personal devices for hackers if the percentage of total financial assets on them grows?
- Banks are requested to implement 24/7 monitoring of their IT-infrastructures.
- How will we monitor our own devices?
- Who will give warranty for transactions which are authorized from our devices with our signatures?

Another Consideration

Byzantine Fault Tolerance

BFT means

… there is a moment in time, when all involved parties know with 100% security that a transaction actually happened.

The Blockchain protocol offers no BFT.

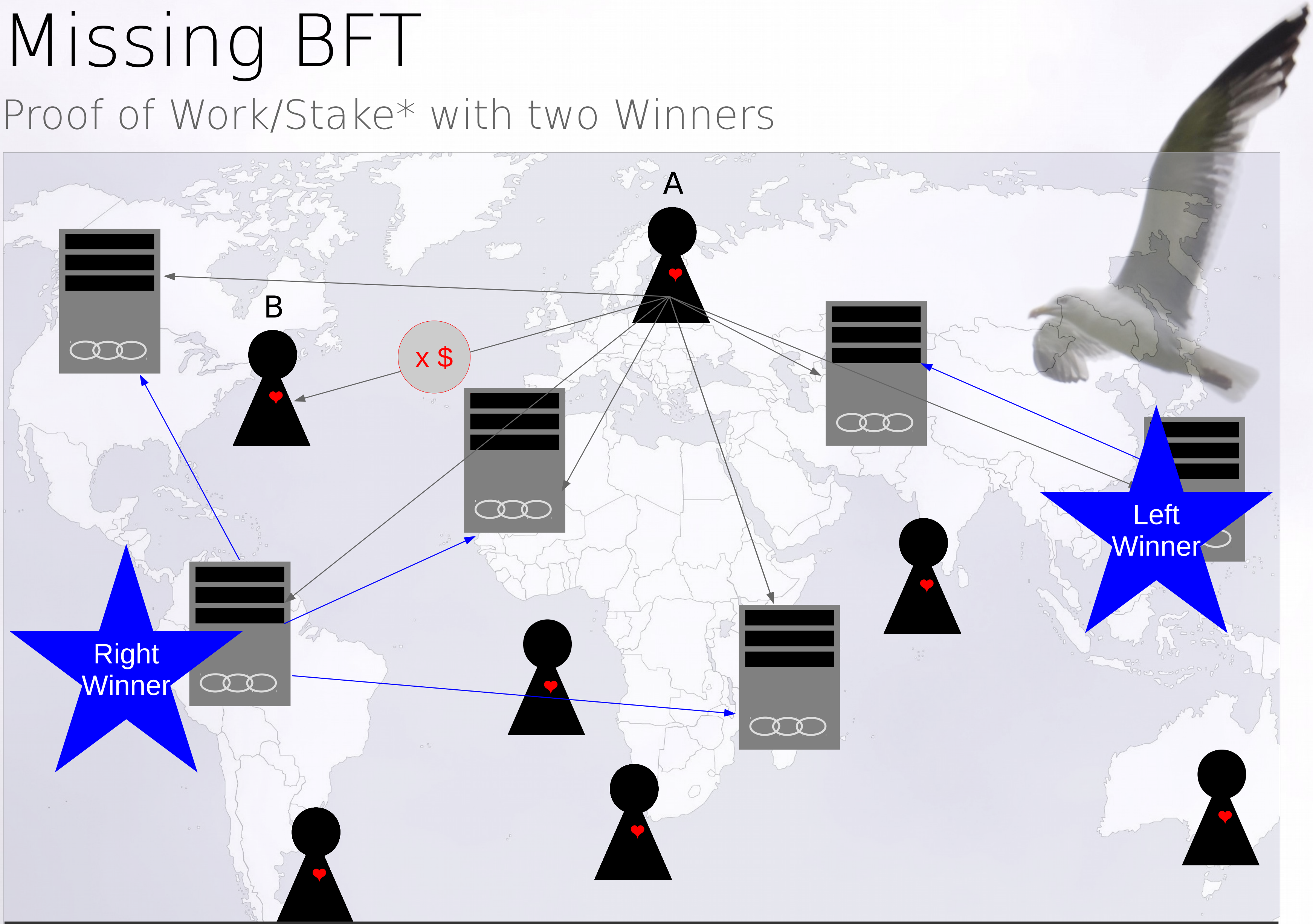
A completely open network will create various branches which will correct themselves after some time, so the Blockchain community agreed to accept 6 confirmations as 100% security that the transaction really happened

… but it is actually not 100%!

With a malicious firewall between nodes and accounts, various branches can exist for much longer than 6 confirmations.

Missing BFT

Proof of Work/Stake* with two Winners



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

My Message

Security

… is hardly ever absolute.

Blockchain

… is great for specific applications but not the solution for all our security problems.

Appendix

Technical GDPR Requirements

Decision 05/2014 (Working Party 216)

Hashing = pseudonymisation technique
Logical deletion requires anonymisation technique

Mathematical perspective

Sensible hashing only allows linking from source data to the hash value, but not the other way around.

EC 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/

Appendix

Data Collections | Machine Learning | AI

What kind of data can be possibly related to a person in the future?

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	