An Outside Perspective On Cyber Crime And Data Security

Dipl. Math. X. Bogomolec
Algorithms | IT-Security
Vienna, June 2018

About Me

Education

Mathematics

Work Fields

Algorithms | IT-Security

Latest Projects

http://ceunix.eu/ | https://tiiqu.com | SOC Helaba

... and building foundations for X4pi

My Summit Mission

Revealing you recently perceived potentials

contact: indigomind@protonmail.ch
website: http://coder.tjingwan.com

My Perspective

From Europe (Regulations, Regulations, and Regulations)

GDPR, PSD2,
Instant Payments, ..

Science:
Quantum Technologies, AI, ...

Information Security

What is it and what do we want to be secure?

CIA, the heart of information security

- Confidentiality
- Integrity
- Accessibilty

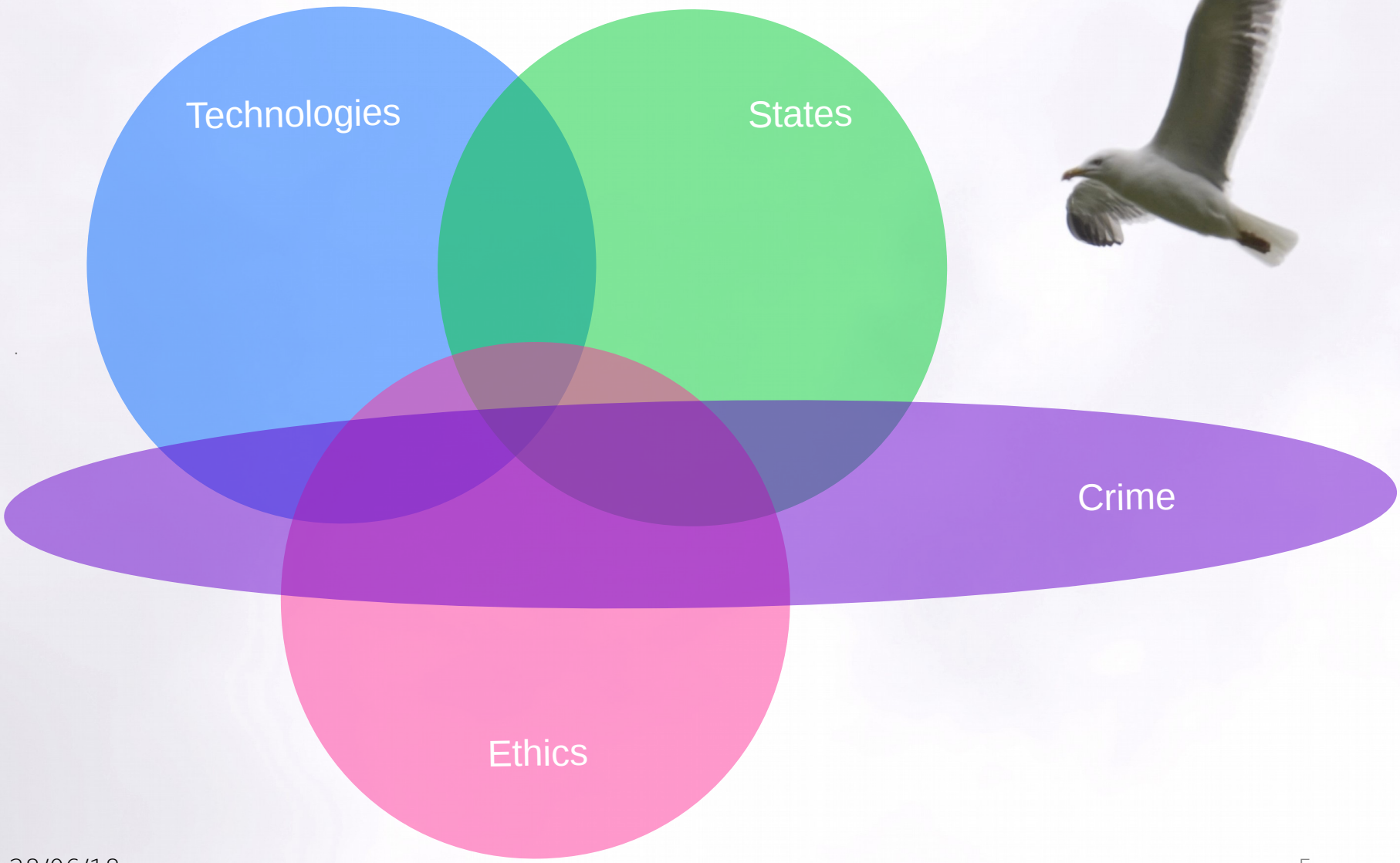
+ Controlled Deletability ←→ GDPR

Data representing

- Financial assets
- Knowledge
- Privacy
- Health
- Safety

Information Security

Influences and Challenges



Information Security

Influences and Challenges

Technologies

- Old
- Innovative

States

- Laws
- Surveillance
- Politics

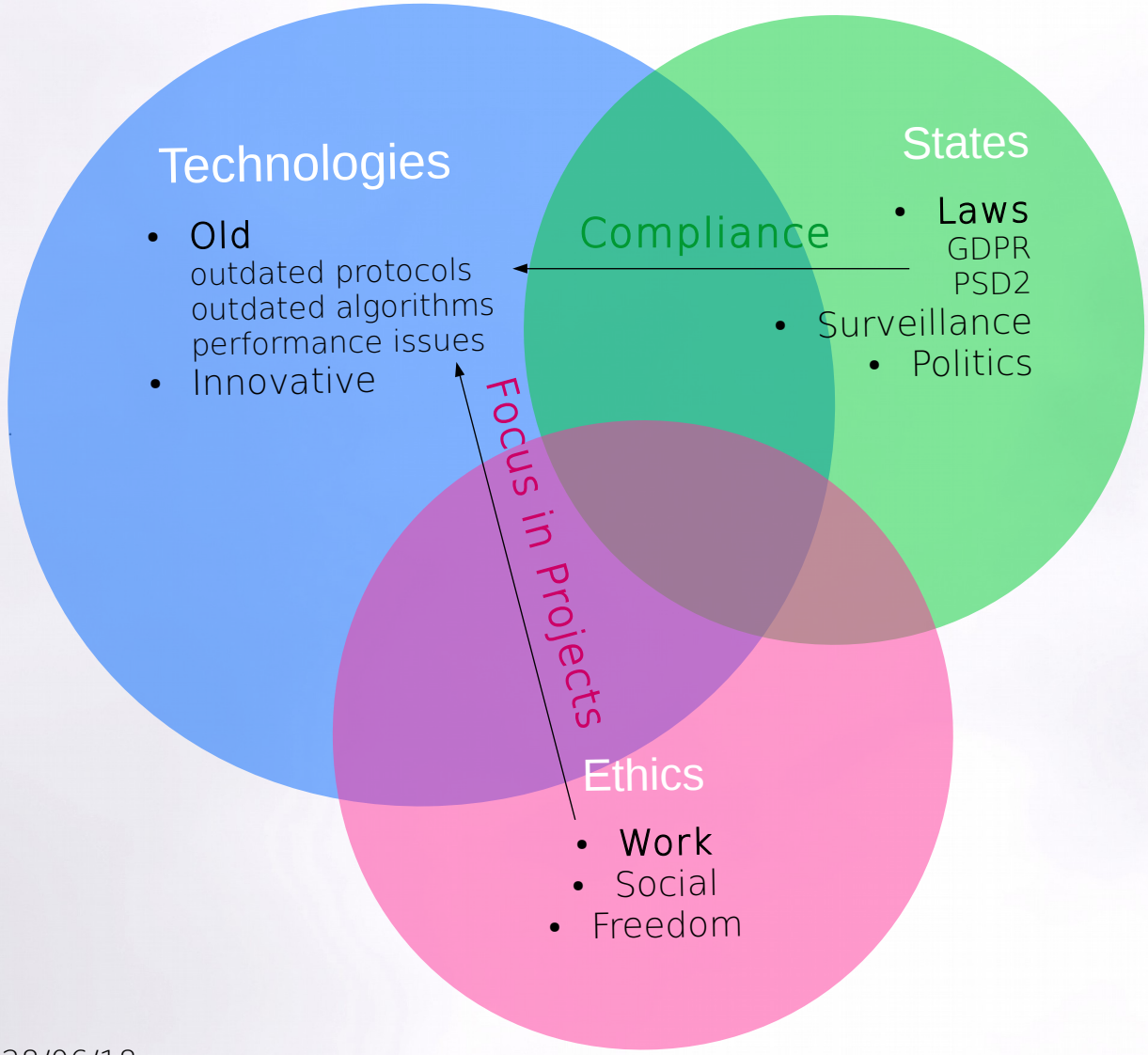
Crime

Ethics

- Work
- Social
- Freedom

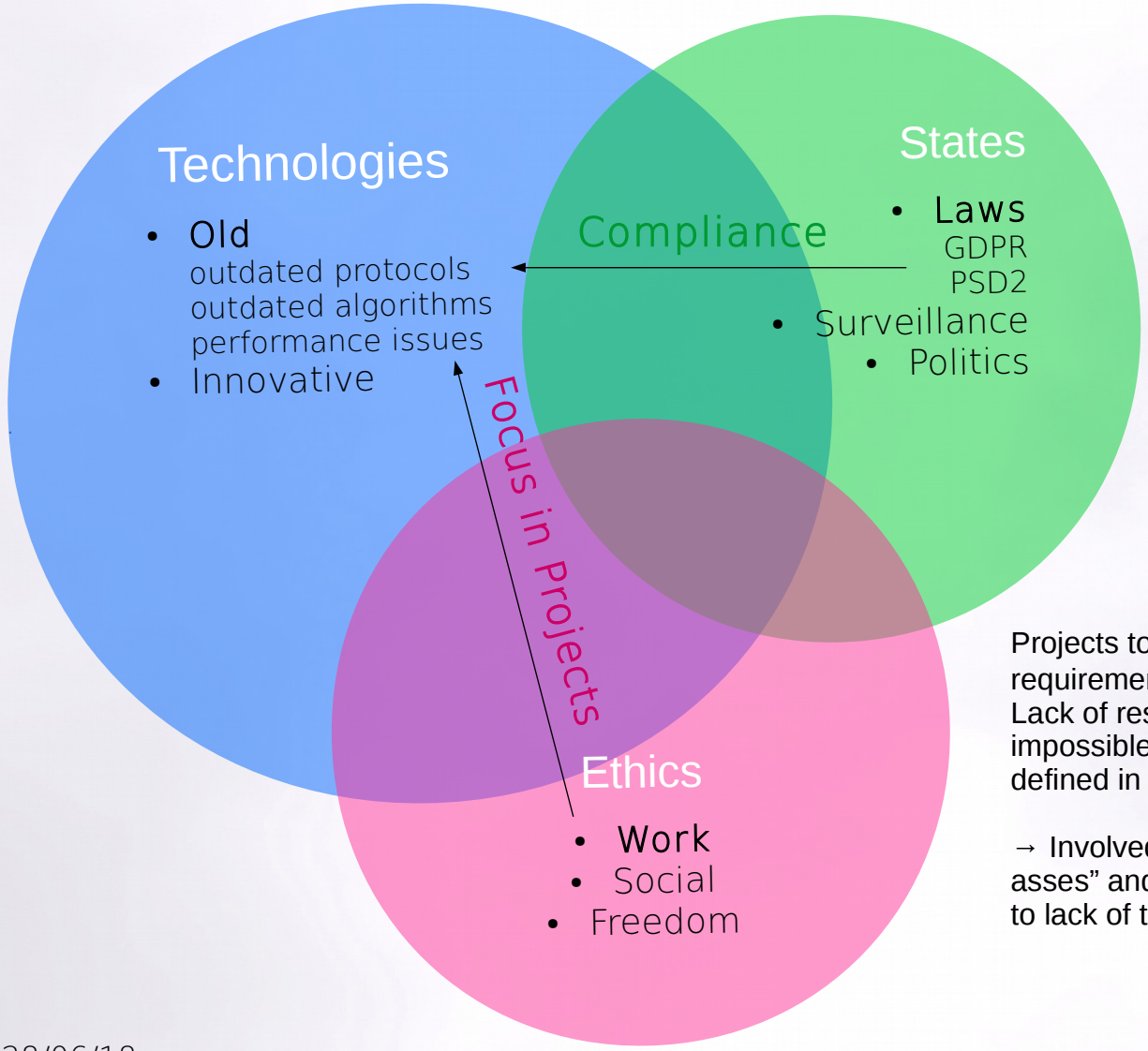
Information Security

Challenges for Old Technologies



Information Security

Challenges for Old Technologies

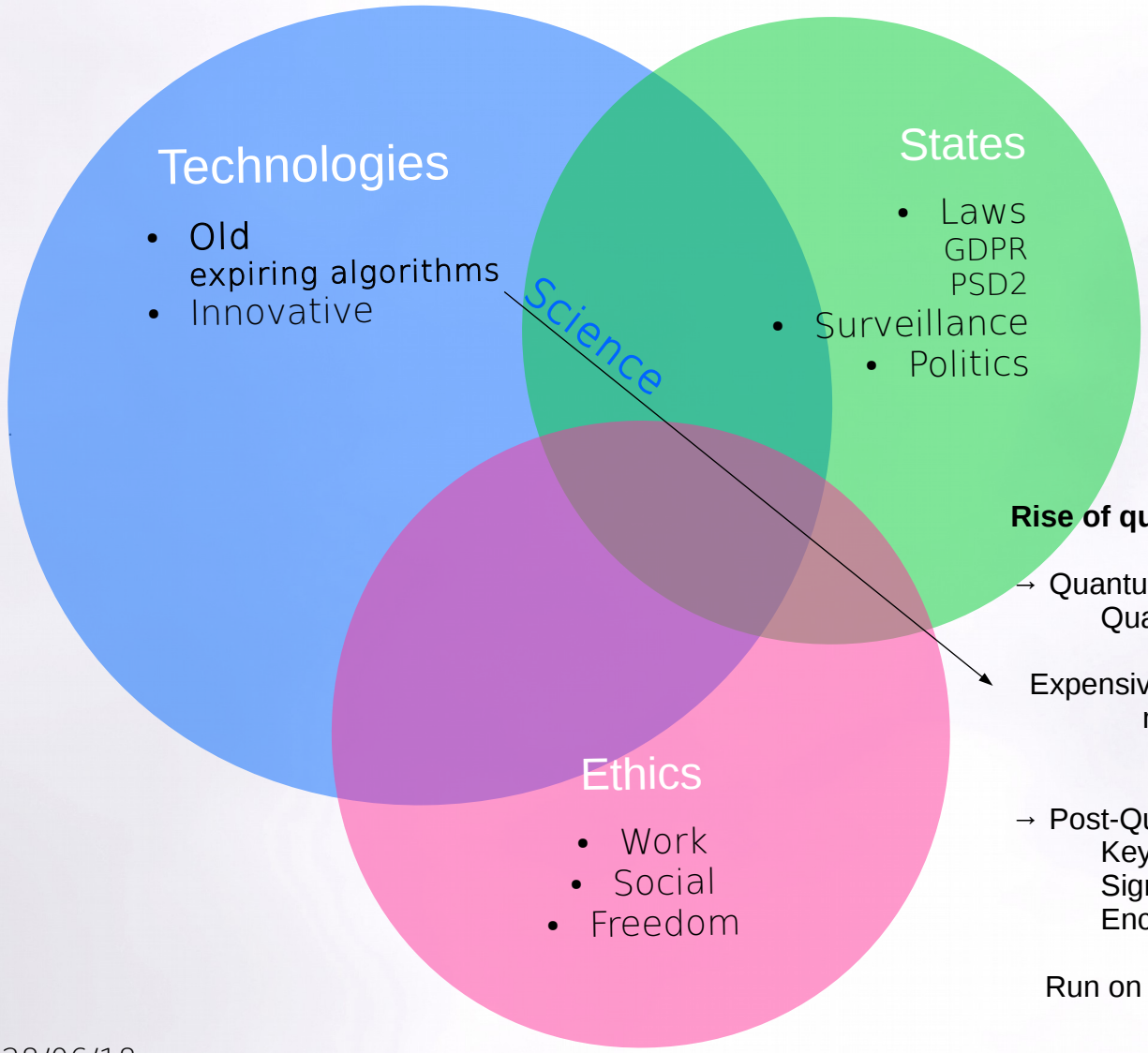


Projects to fulfill regulatory or legal requirements are often highly demanding. Lack of resources and time make it impossible to reach company standards defined in less demanding times.

→ Involved parties want to “save their own asses” and realization efficiency suffers due to lack of team focus.

Information Security

Challenges for Expiring Algorithms



Rise of quantum technology threats

→ Quantum Cryptology
Quantum Key Distribution

Expensive new hardware and no genuine message authentication!

→ Post-Quantum Cryptology
Key Exchange
Signature
Encryption

Run on classical devices and resist QC attacks!

Quantum Computers and Crypto

An upcoming Bliss with side Effects

Rise of Quantum Computers Technology offers

- More computation power
- Possibility to build complex materials
- Different kind of algorithms to solve certain problems (integer factorization, needle in haystack, etc.)

As a consequence, classical asymmetric crypto is about to expire!

Official Quantum Tech Achievements

- IBM: 20 qubits QC commercially available in 2017
- IBM, Google: 50 qubits prototypes in 2017
- Google: 72 qubit prototype March 2018!
- D-Wave 2048 qubits for quantum annealing to solve optimization problems in 2016
- Topological quantum bits announced in 2017
  (If successful, error correction problem which slows down quantum computation development will be considerably mitigated.)

Expiring Crypto Algorithms

Explaining a simple Term in a complex Context

What does “expire” mean in this context?

As soon as potent enough quantum computers are available, it will be possible to compute RSA, ECC and Diffie-Hellmann private keys with the knowledge of the public keys.

When will they expire?

We don’t know that and estimations vary. But IBM believes that they will be broken within 5 years:

https://www.afterdawn.com/news/article.cfm/2018/05/22/ibm-all-current-encryption-methods-will-be-broken-instantly-in-5-years-time

What will remain safe?

AES-256 is expected to be quantum computer attack proof with a security level comparable to AES-128 against binary computer attacks. So all encryption of static data is safe.

New Crypto Solutions

Replacements for up to 40 Years old Algorithms

Quantum Key Distribution

Quantum key distribution, key exchange based on quantum mechanical effects

- Expensive new hardware (ID quantique)
- Only for short distances (300-1200km in 2017)
- No genuine message authentication included, man in the middle is possible if no extra message authentication is added

QUESS: 2000km quantum communication channel between Shanghai and Bejing

SwissQuantum

SECQC Austria

Tokyo QDK Network

DARPA USA

Post-Quantum Cryptography

Alternative algorithms for key exchange based on hardness of mathematical problems other than integer factorization

- Being standardized by the NIST (2017-20219
- Some of them were already used for years and haven't been broken
- Run effectively on classical devices
- Can be enabled by software updates

Isara USA

KPN in Netherlands

Infineon

Microsofts experimental VPNs with algorithms that haven't been exposed publicly

some examples of established solutions

Post-Quantum Crypto

When does it make sense to start with Implementations?

When does it make sense to start with implementations?

If you are sending data out of your own network of which you think it might interesting enough for someone to collect now and decrypt it as soon as quantum computers are potent enough.

Signatures on documents which have to be valid longer than you believe it takes before the Quantum Computer threat becomes real and which cannot be easily updated. For example signatures on electronic passports.

Data on public blockchains which will have to remain private for longer than you believe it takes before the Quantum Computer threat becomes real. Think about the fact that copies of those chains are intended to exist forever.

Information Security

Challenges

Technologies

- Old
  expiring algorithms
- Innovative

States

- Laws
  GDPR
  PSD2
- Surveillance
- Politics

Crime

Undetected information leakage
Data manipulations
Uncovered secrets in collected data

Ethics

- Work
- Social
- Freedom

Rise of quantum technologies

→ Quantum Cryptology
Quantum Key Distribution

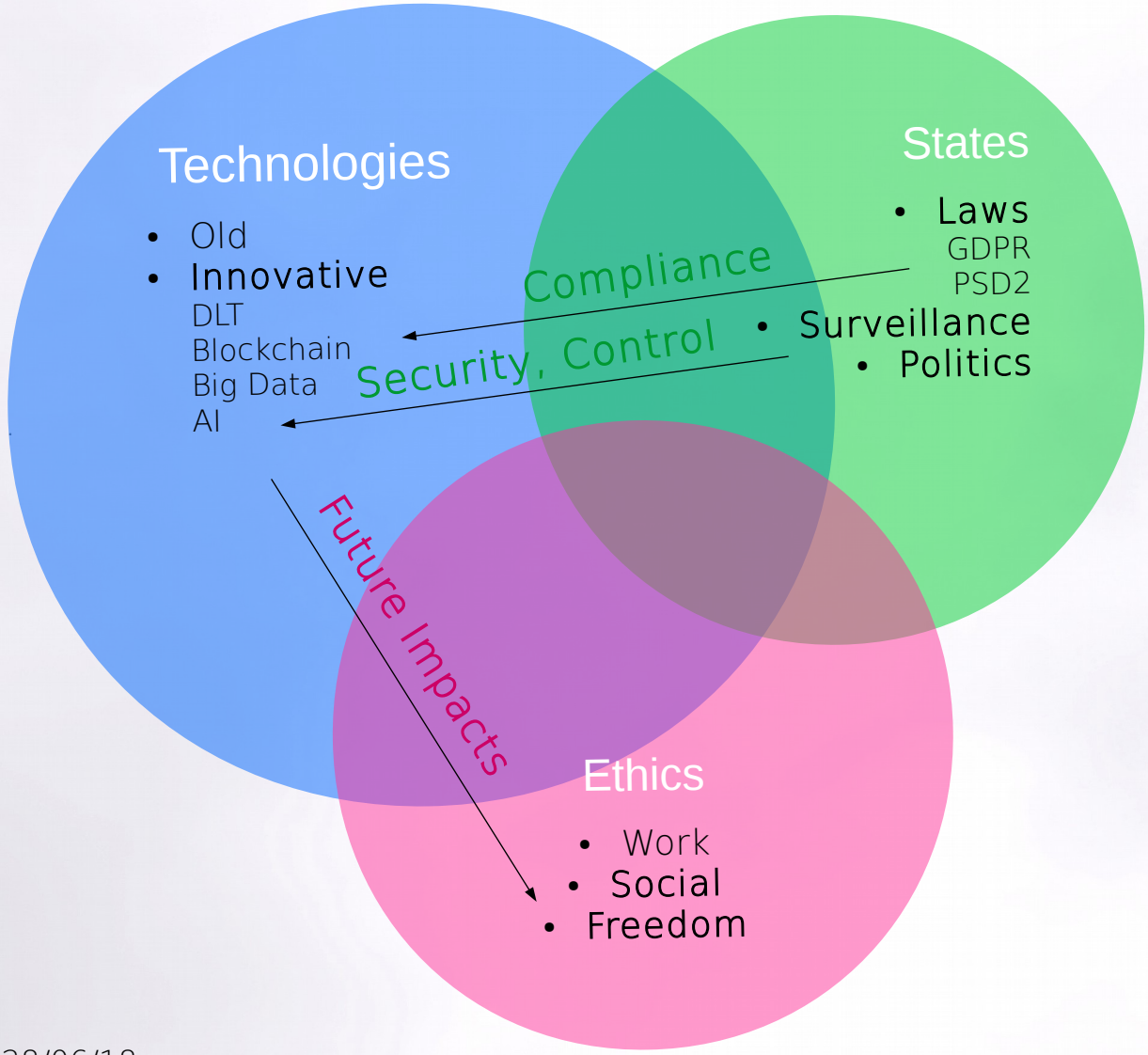
Expensive new hardware and no genuine message authentication!

→ Post-Quantum Cryptology
Key Exchange
Signature
Encryption

Run on classical devices and resist QC attacks!

Information Security

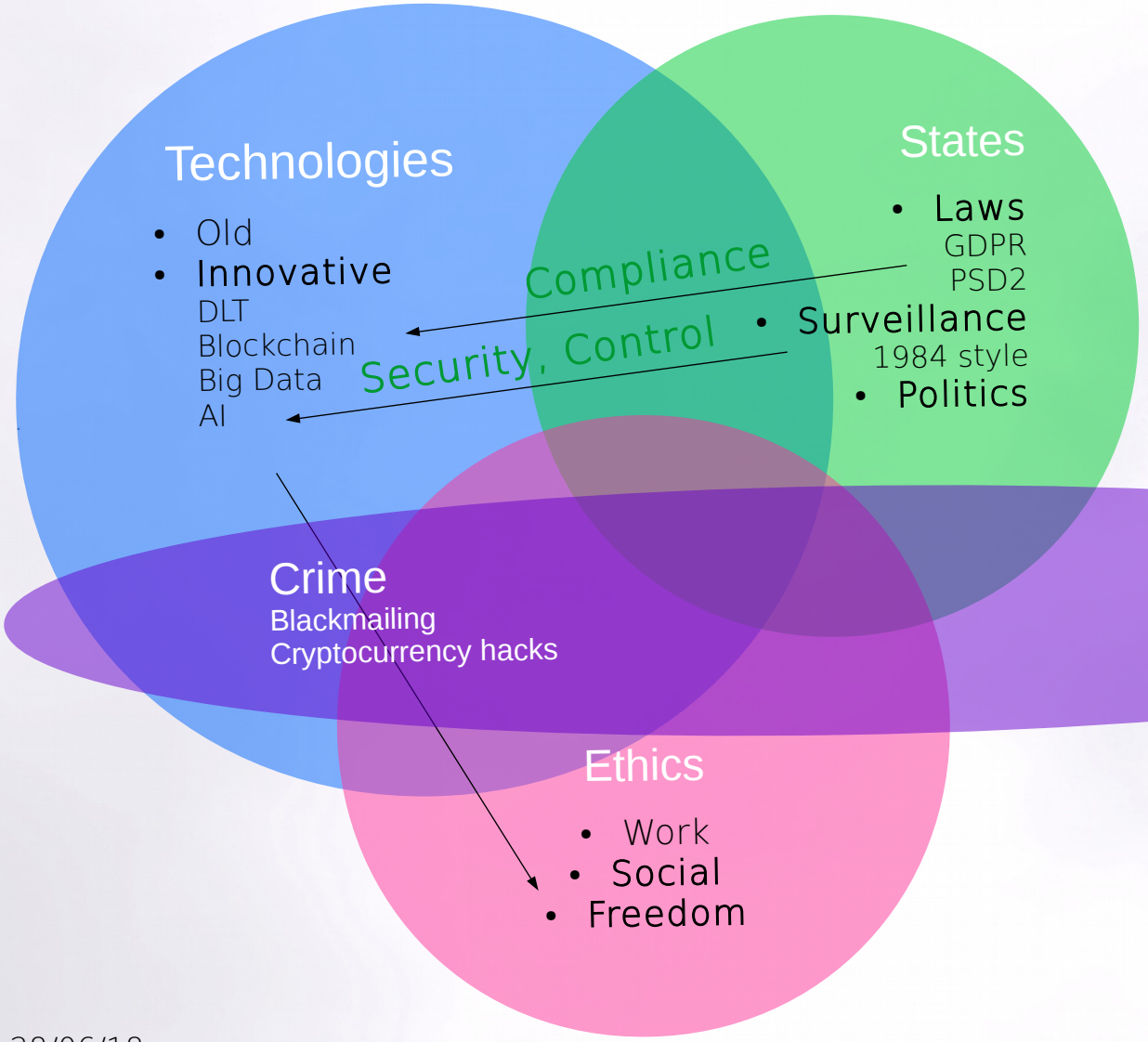
Challenges



- How to monitor decentralized mechanisms?
- Hardly any control mechanisms on data uploads in DLT apps
- Personal data on blockchains
- Undeletable data on public blockchains
- Blockchain branching not taken into account
- Online investigations allow states to easily monitor private activities
- Information availability with personalized algorithms
- Pricing based on personalized web requests
- ...

Information Security

Challenges



- How to monitor decentralized mechanisms?
- Hardly any control mechanisms on data uploads in DLT apps
- Personal data on blockchains
- Undeletable data on public blockchains
- Blockchain branching not taken into account
- Online investigations allow states to easily monitor private activities
- Information availability with personalized algorithms
- Pricing based on personalized web requests
- ...

Blockchain

Restrictions for Data to be uploaded

Bitcoin

Max transaction size is around 100 kB.
If the current blocksize < 27 kB for free, else 0.01 BTC per kB.

Ethereum

No direct limit, fast transactions are more expensive than slow ones. → Internet neutrality???

No content regulation, no content verification!

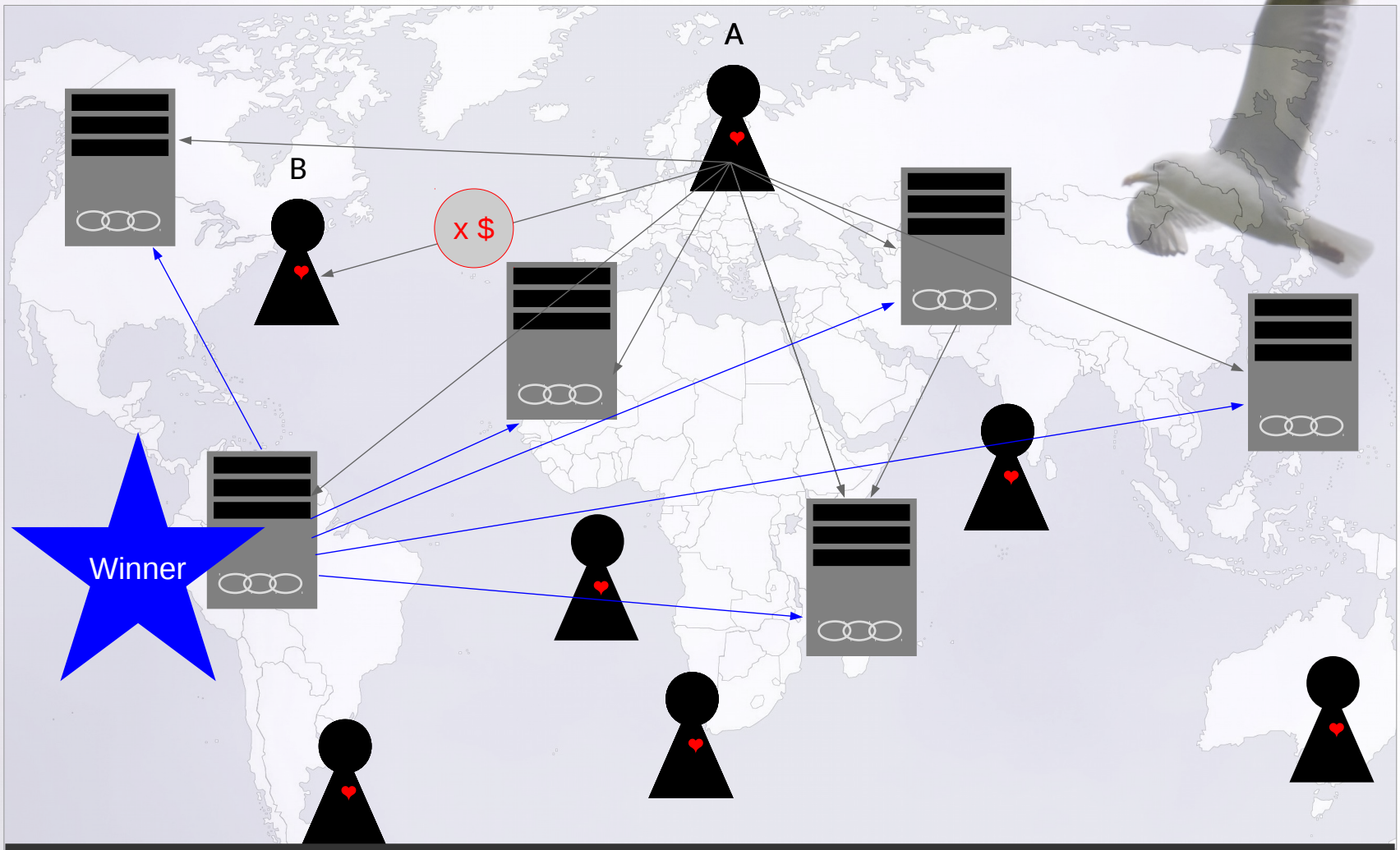
Links to videos with criminal content have been uploaded to the bitcoin blockchain.
Are users with offline wallets accountable for having them on their PCs?

Any information can be uploaded and never be deleted again!

In a private or consortium blockchain network it is possible to implement a layer for content check!

Blockchain

Information Flow | Proof of Work/Stake* Distribution



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

Branching in Blockchain

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

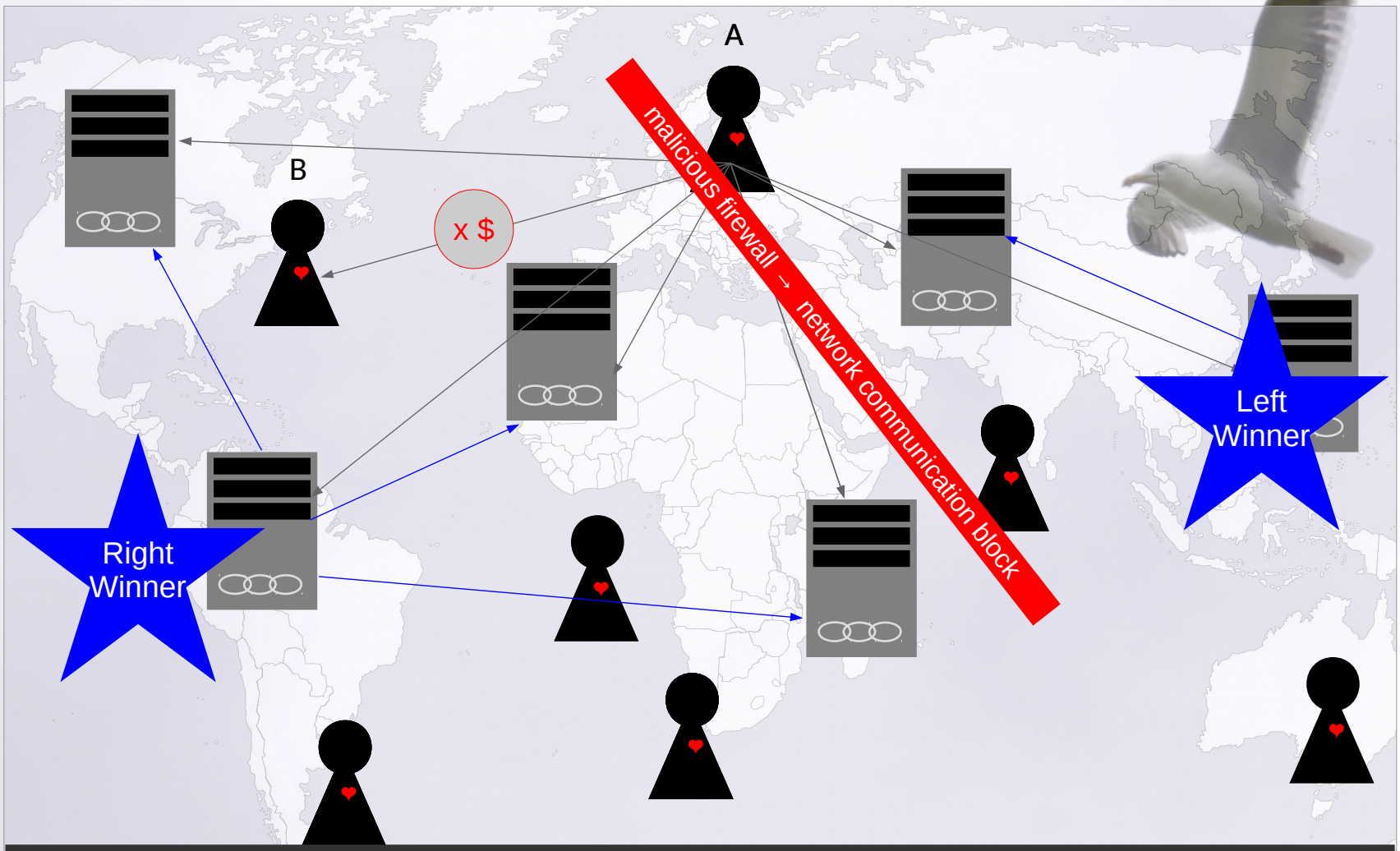
… but it is actually not 100%!

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

In a private or consortium network BFT for Blockchain is possible!

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

Right to Erasure in GDPR

… is a freedom tool which has no equivalent in the rest of the world

Post-Quantum Crypto

… don’t wait too long to integrate it for cases described in slide 13 and similar ones

contact: indigomind@protonmail.ch

Appendix

Cryptocurrency Hacks

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/

Appendix

Some Examples of GDPR Proof Blockchain Usage

Use Blockchain for 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:-((Opinion 216)) This opinion will be the base for considerations if legal cases go to court. Read my article on medium if you#re interested in the topic:

https://journal.tiiqu.com/open-questions-about-gdpr-compliance-in-the-context-of-blockchain-technologies-55f51860b048

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	✓
anonymous internet user, geolocation, date 1, time 1	???
anonymous internet user, geolocation, date 2, time 2	
anonymous internet user, geolocation, date 3, time 3	