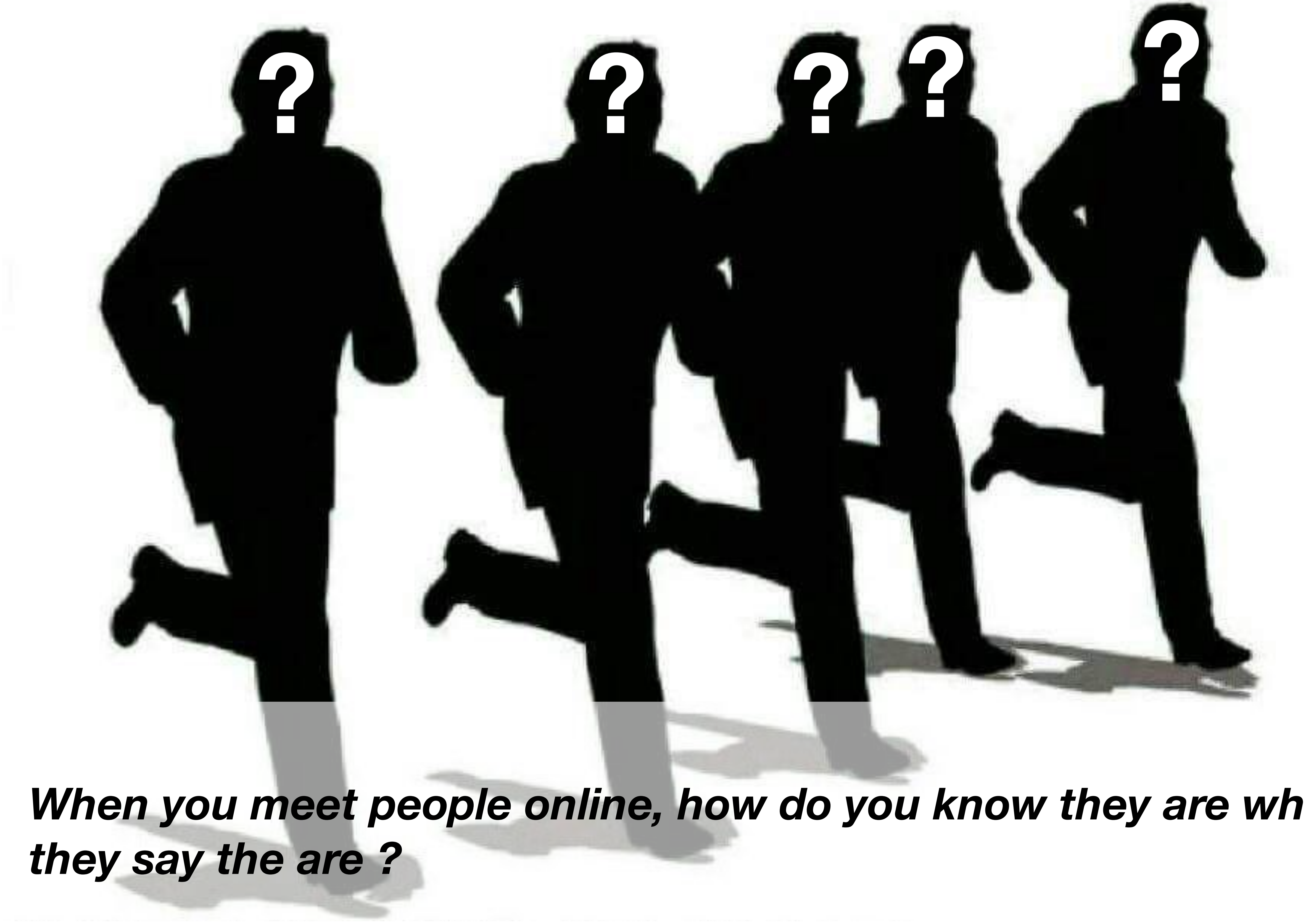
What are the characteristics of blockchains and challenges to stay compliant with legal regulations?

Author
Alberto Sonnino

University College London

March 2018

How do you know that your vote has actually been counted?



When you meet people online, how do you know they are who they say the are ?

Content

1. What are blockchain technologies?

2. What do they provide?

3. What are the main legal challenges?

What are blockchain technologies?

- What are blockchains?

Systems to store records that can be verified by anyone, that no-one can modify, and without a central authority

What are blockchain technologies?

- What are blockchains?

Systems to store records that can be verified by anyone, that no-one can modify, and without a central authority

Publicly verifiable

What are blockchain technologies?

- What are blockchains?

Systems to store records that can be verified by anyone, that no-one can modify, and without a central authority

Publicly verifiable

Immutable

What are blockchain technologies?

- What are blockchains?

Systems to store records that can be verified by anyone, that no-one can modify, and without a central authority

Publicly verifiable

Immutable

Decentralised

What are blockchain technologies?

- What are smart contracts?

What are blockchain technologies?

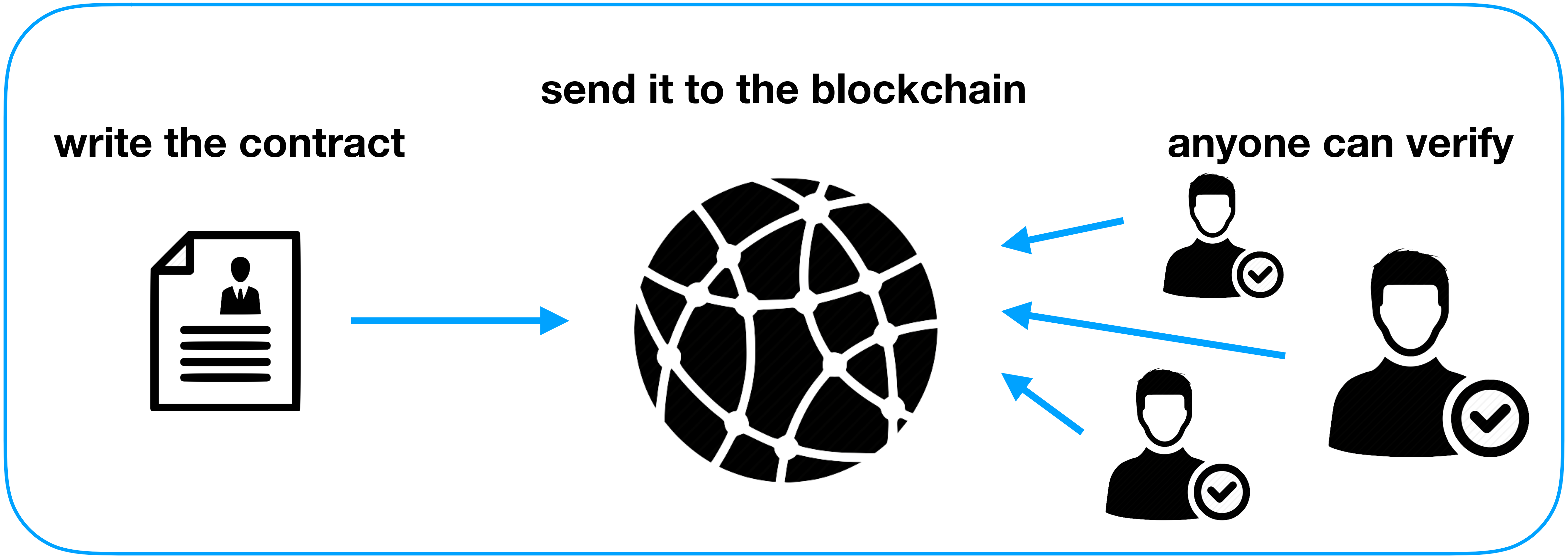
- What are smart contracts?

Smart contracts are computer programs that are ‘executed’ on the blockchain

What are blockchain technologies?

- What are smart contracts?

Smart contracts are computer programs that are 'executed' on the blockchain



What do they provide?

- Key blockchains features

Decentralisation

e.g.
- Payement system without trusting a central bank

High Integrity

e.g.
- No-one can tamper with bank records
- No-one can suppress someone else's bank account

High Availability

e.g.
- No blackouts or equipment failure can prevent users from using their bank account

Transparency

e.g.
- Anyone can verify that a given deposit has been paid

Authenticity

e.g.
- Coin transfers come from the rightful owner

Non-Repudiation

e.g.
- Users cannot deny having received or sent coins

What are the main legal challenges?

Disclaimer: I am not a lawyer

What are the main legal challenges?

Disclaimer: I am not a lawyer

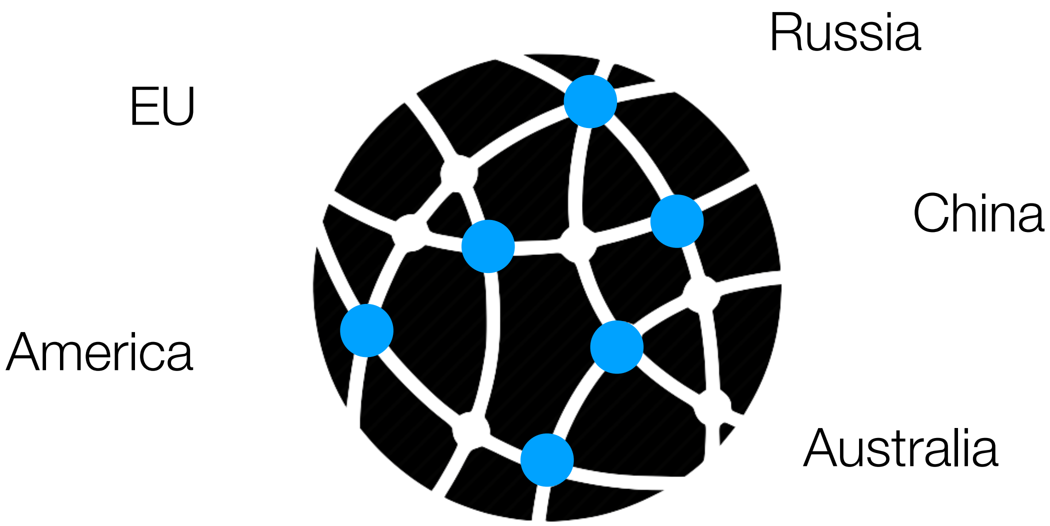
- When blockchains meet the GDPR…

What if these records are personal data?

Who is data processor?
Who is data controller?

Cannot delete or modify data
Cannot 'stop' a smart contract

Where are these data stored?



Hard to control geo locations

What are the main legal challenges?

- Problems come from the foundation of blockchains

What are the main legal challenges?

- Problems come from the foundation of blockchains

Systems to store records…

Publicly verifiable

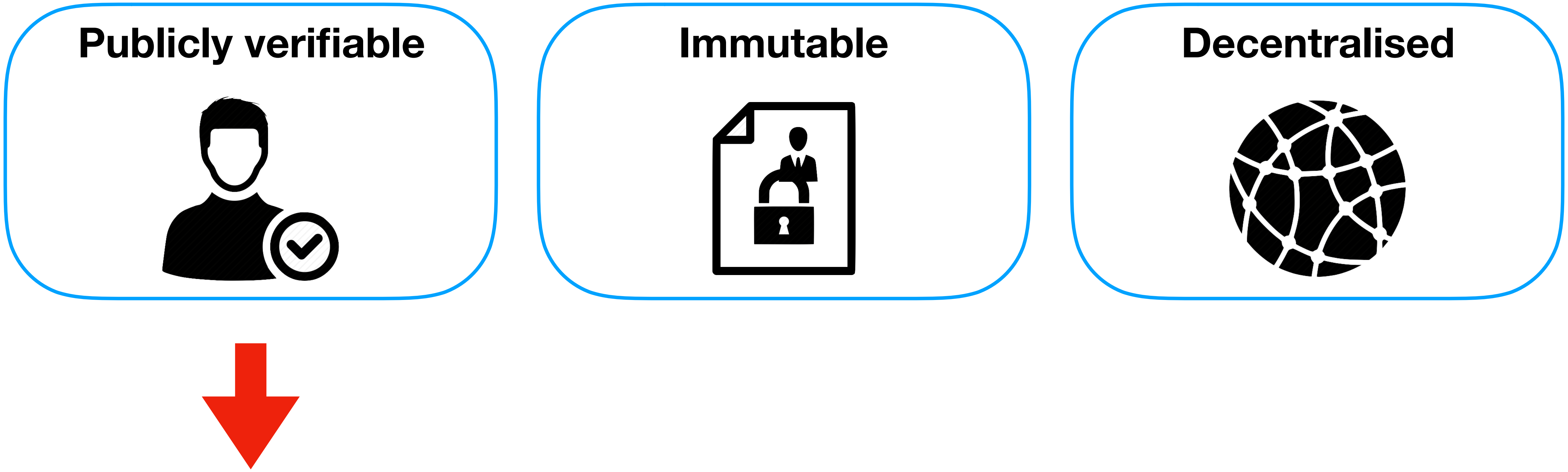
Immutable

Decentralised

What are the main legal challenges?

- Problems come from the foundation of blockchains

Systems to store records…



Publicly verifiable

Immutable

Decentralised

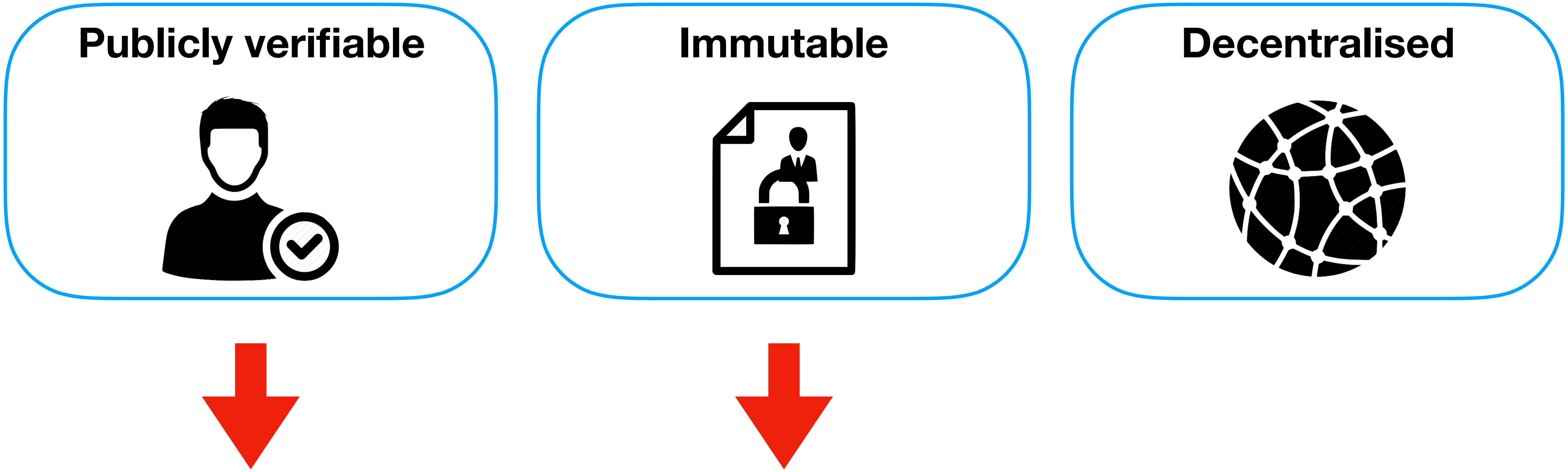
What if these records are personal / sensitive?

- Financial data
- Company assets
- Identity data

What are the main legal challenges?

- Problems come from the foundation of blockchains

Systems to store records…



Publicly verifiable

Immutable

Decentralised

What if these records are personal / sensitive?

- Financial data
- Company assets
- Identity data

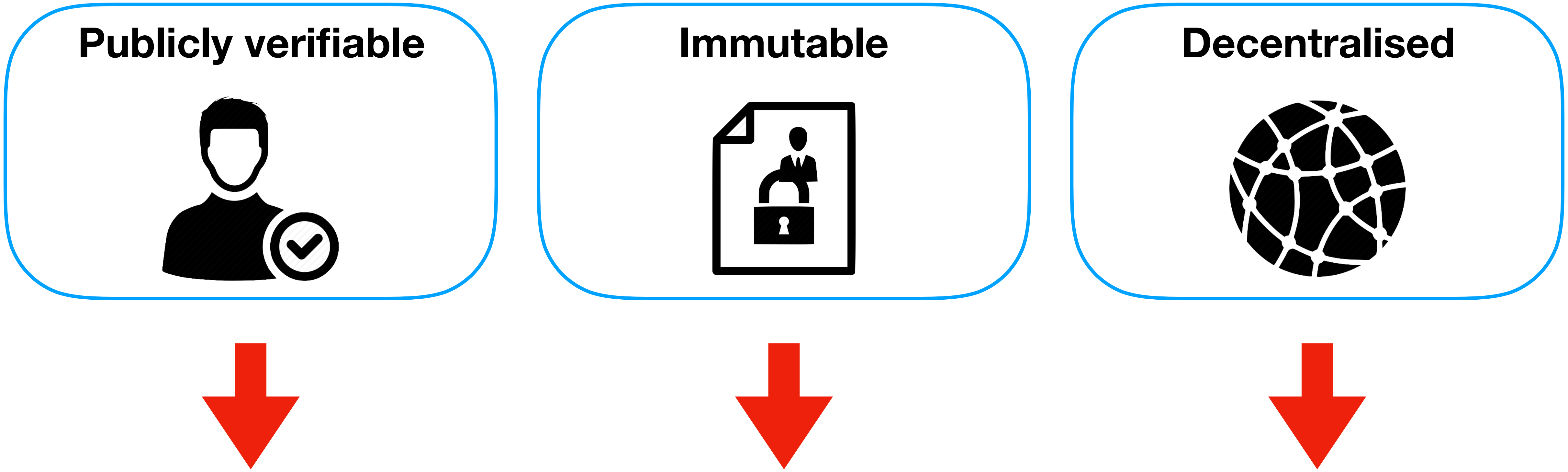
And the right to be forgotten?

- Copyright pictures
- Defamatory statements
- Leaked data

What are the main legal challenges?

- Problems come from the foundation of blockchains

Systems to store records…



Publicly verifiable

Immutable

Decentralised

What if these records are personal / sensitive?

- Financial data
- Company assets
- Identity data

And the right to be forgotten?

- Copyright pictures
- Defamatory statements
- Leaked data

Who do we blame?
How do we shut it down?

- International legislations
- Huge massive of users

What are the main legal challenges?

- Possible mitigations

What are the main legal challenges?

- Possible mitigations

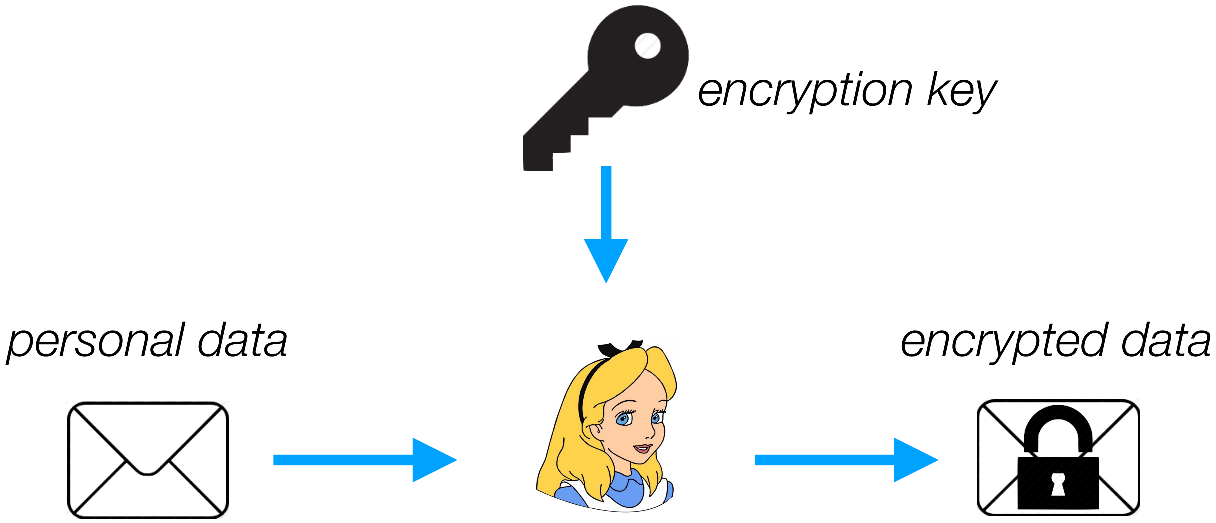
Idea I. Use encryptions

What are the main legal challenges?

- Possible mitigations

Idea I. Use encryptions

A user, *Alice*, wants to encrypt her personal data

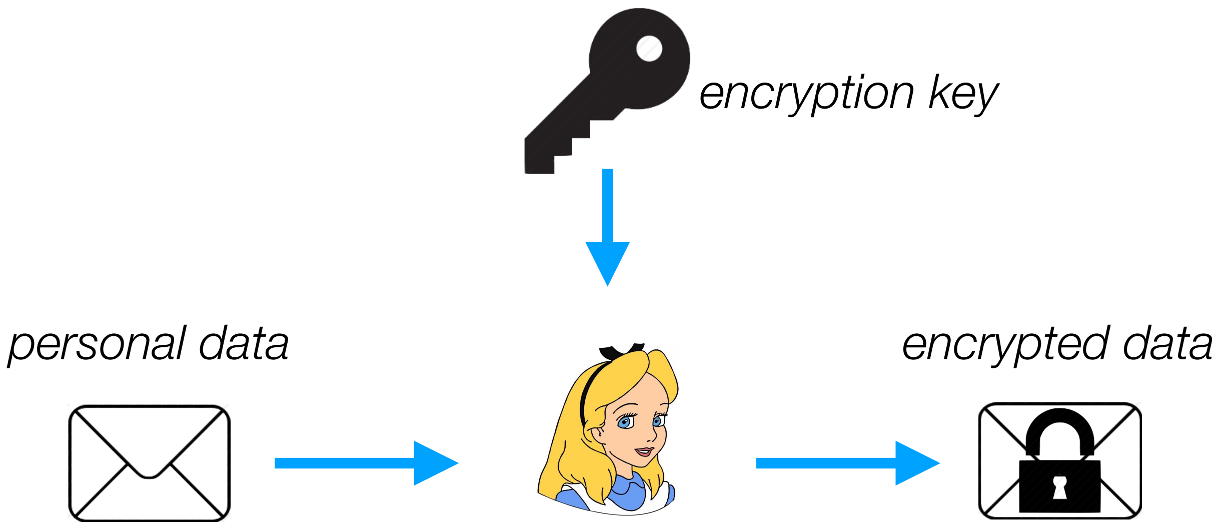


What are the main legal challenges?

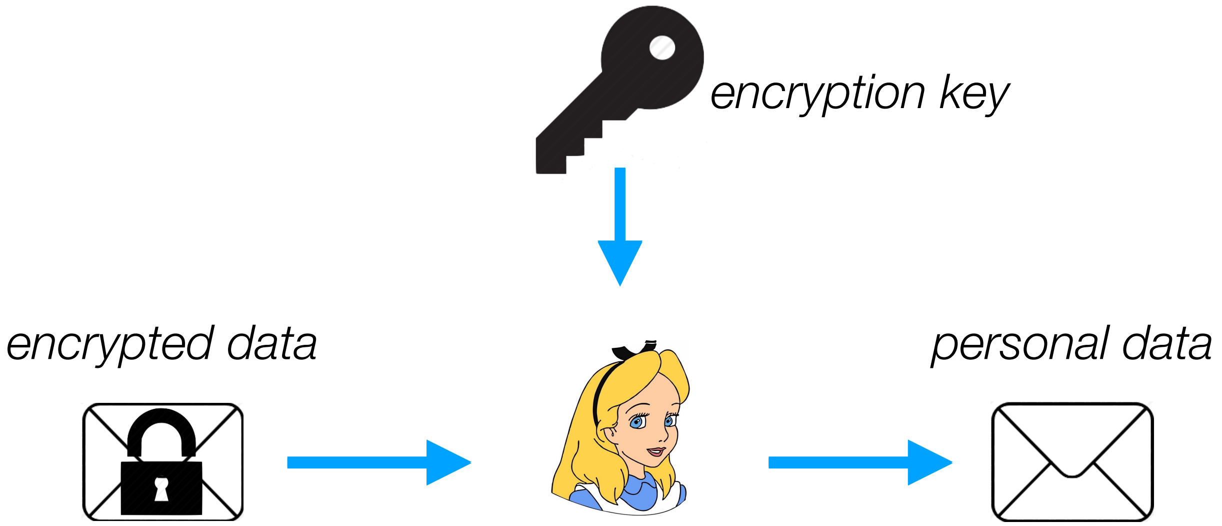
- Possible mitigations

Idea I. Use encryptions

A user, *Alice*, wants to encrypt her personal data



Only who has the encryption key can recover the data

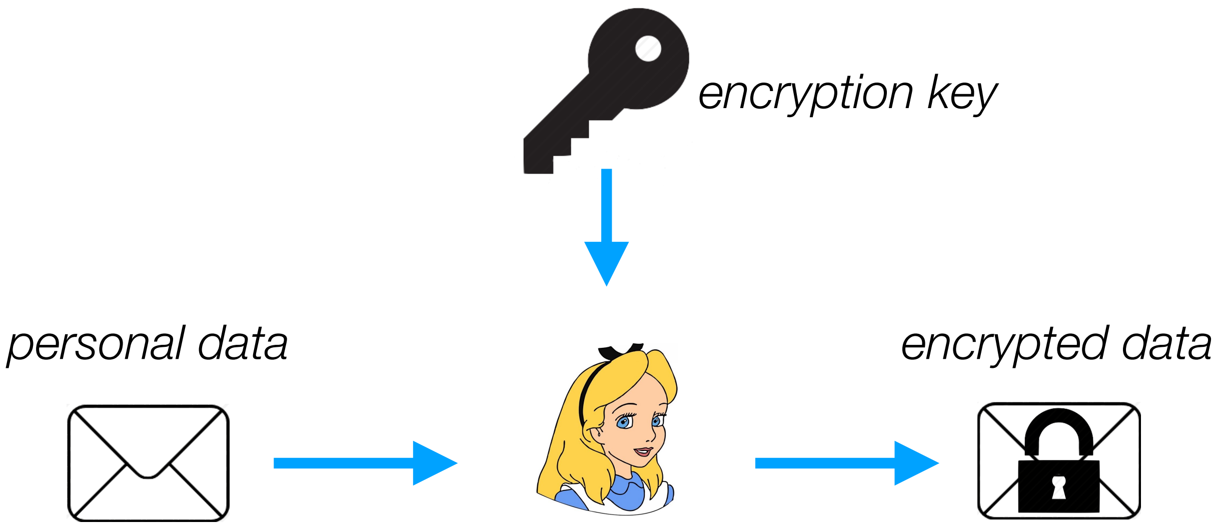


What are the main legal challenges?

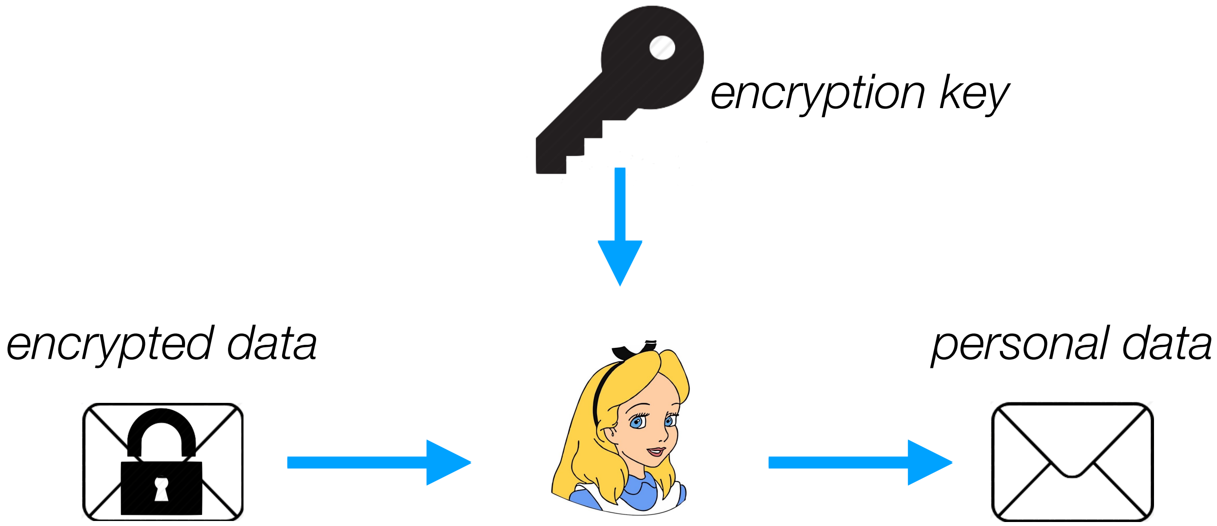
- Possible mitigations

Idea I. Use encryptions

A user, *Alice*, wants to encrypt her personal data



Only who has the encryption key can recover the data



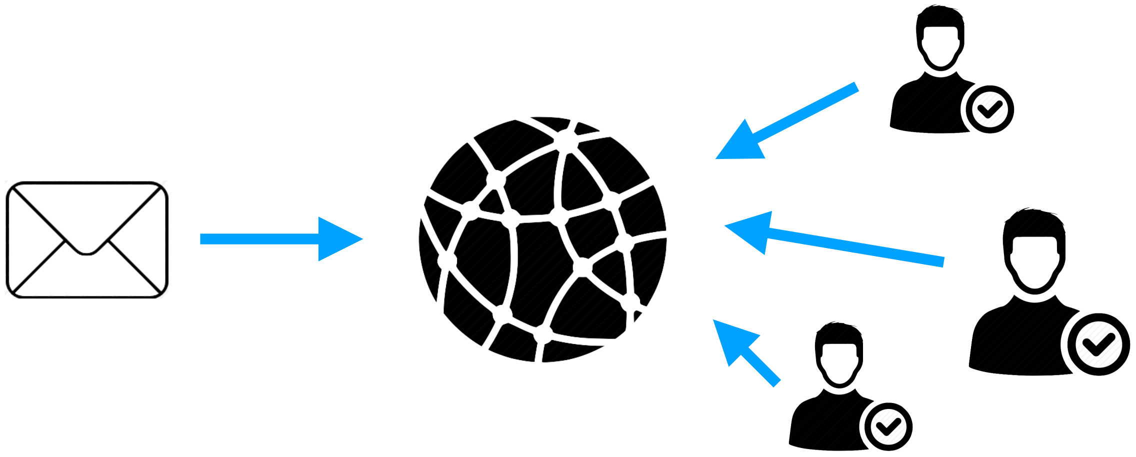
Encrypted data (🔒) look like random numbers (01010 -0—1 11000)

What are the main legal challenges?

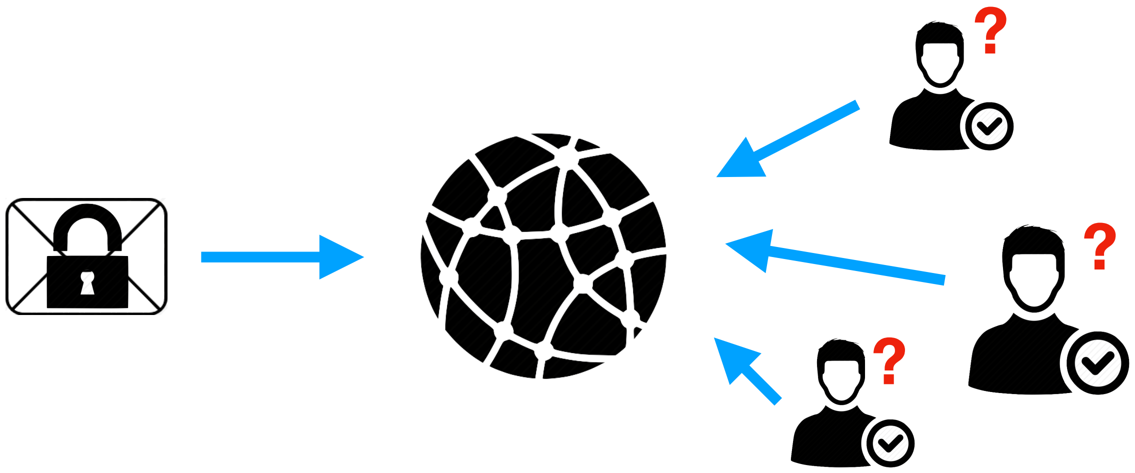
- Possible mitigations

Idea I. Use encryptions

Instead of sending data directly to the blockchain…



Send only the encryptions (i.e., the encrypted data)



What are the main legal challenges?

- Possible mitigations

How can we be sure that users encrypted the correct data?

(i.e., if data are encrypted, what about public verifiability?)

What are the main legal challenges?

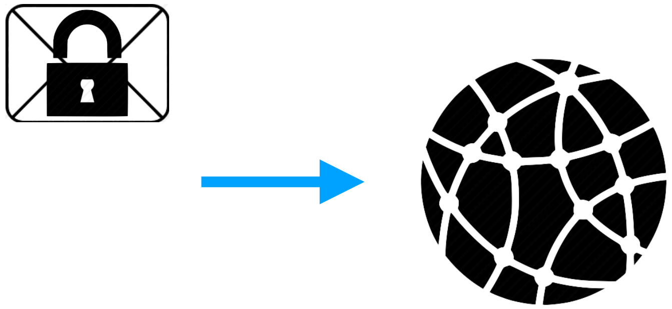
- Possible mitigations

Idea II. Verify encryptions with zero-knowledge proofs

What are the main legal challenges?

- Possible mitigations

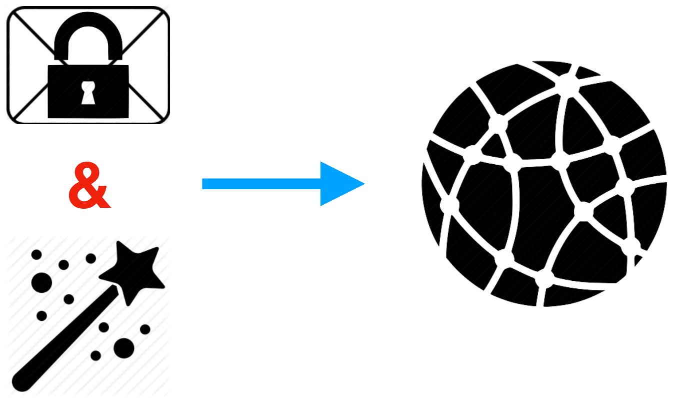
Idea II. Verify encryptions with zero-knowledge proofs



What are the main legal challenges?

- Possible mitigations

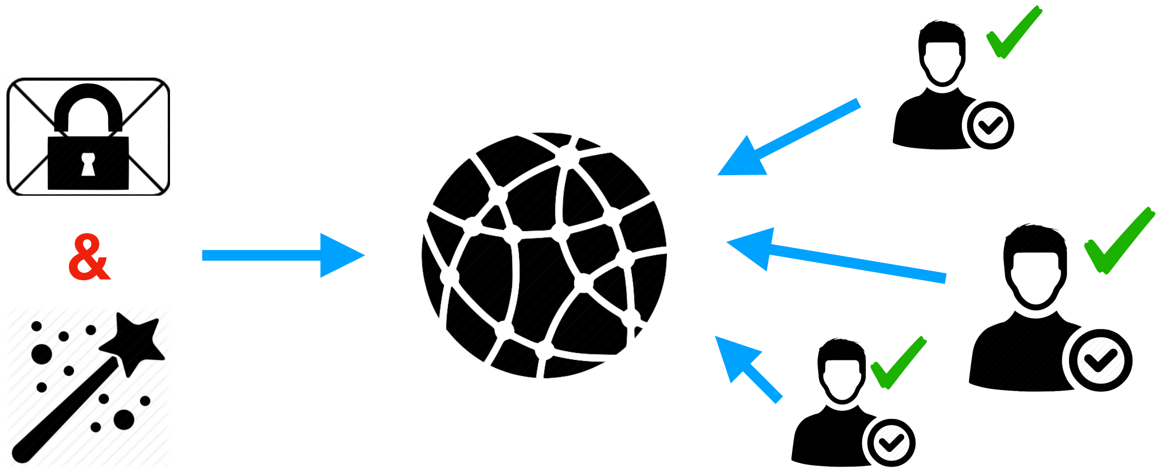
Idea II. Verify encryptions with zero-knowledge proofs



What are the main legal challenges?

- Possible mitigations

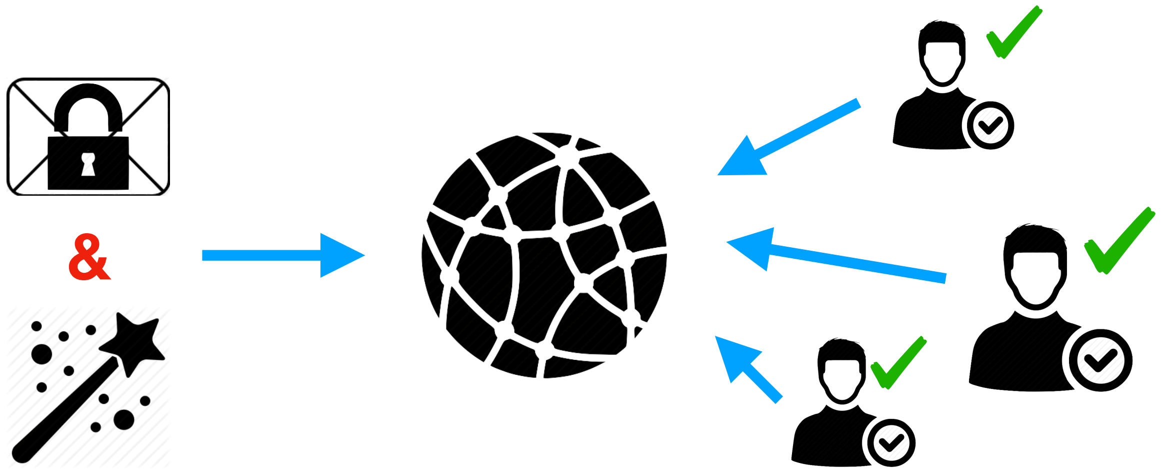
Idea II. Verify encryptions with zero-knowledge proofs



What are the main legal challenges?

- Possible mitigations

Idea II. Verify encryptions with zero-knowledge proofs

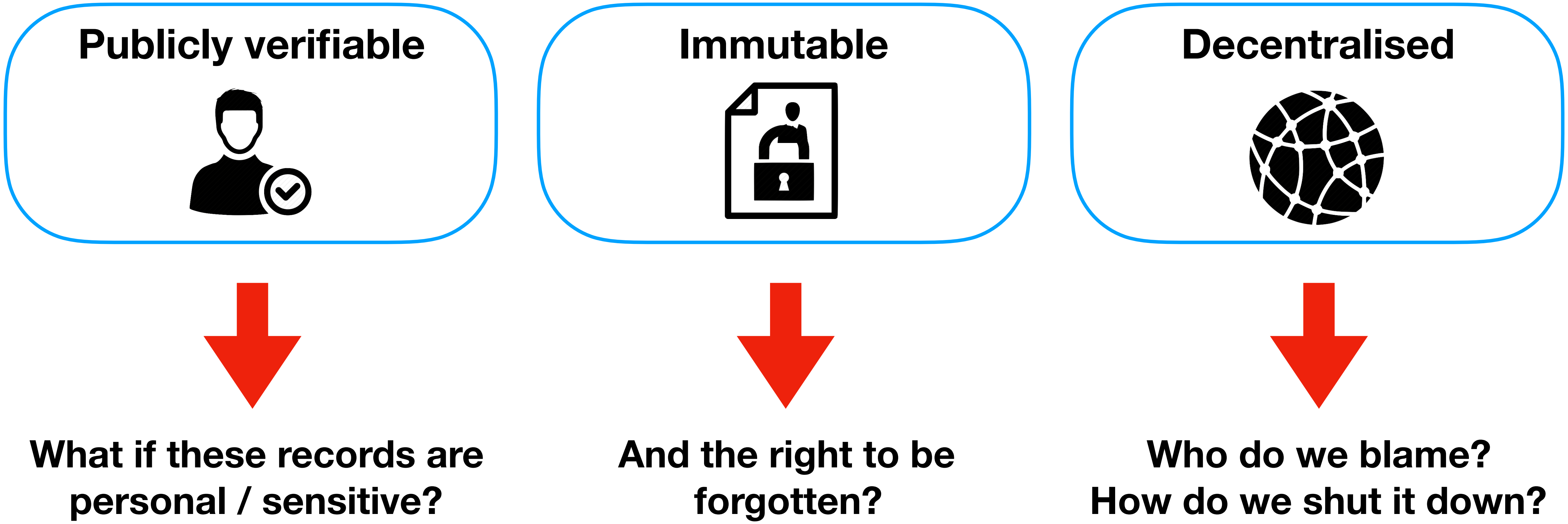


In a few words:

- 🪄 prove that 🔒 is correct
- 🪄 don’t leak info about ✉
- 🪄 can only be generated by who knows ✉

What are the main legal challenges?

- How does it mitigate the problems?



Publicly verifiable

What if these records are personal / sensitive?

Immutable

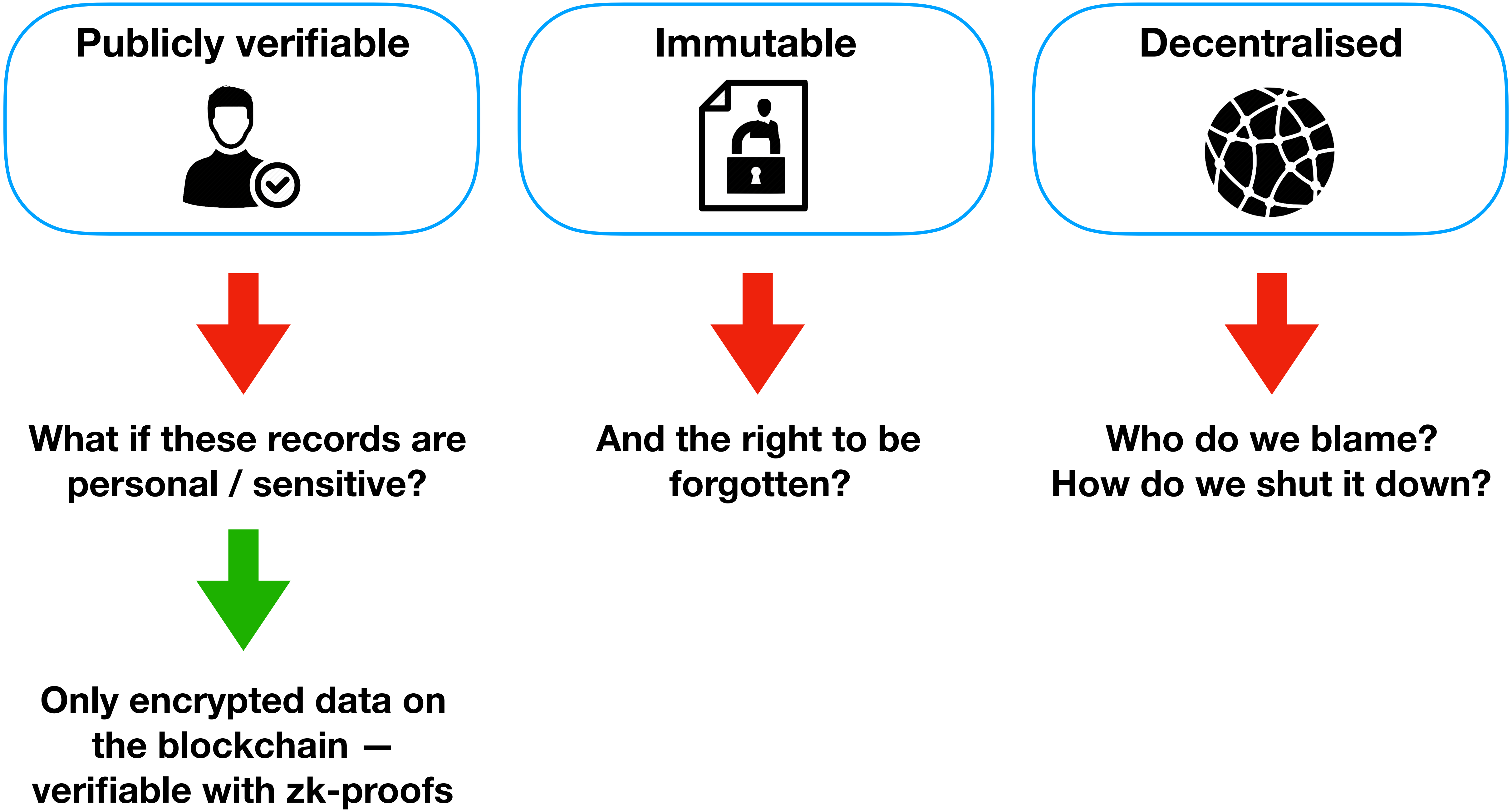
And the right to be forgotten?

Decentralised

Who do we blame?
How do we shut it down?

What are the main legal challenges?

- How does it mitigate the problems?



Publicly verifiable

What if these records are personal / sensitive?

Only encrypted data on the blockchain — verifiable with zk-proofs

Immutable

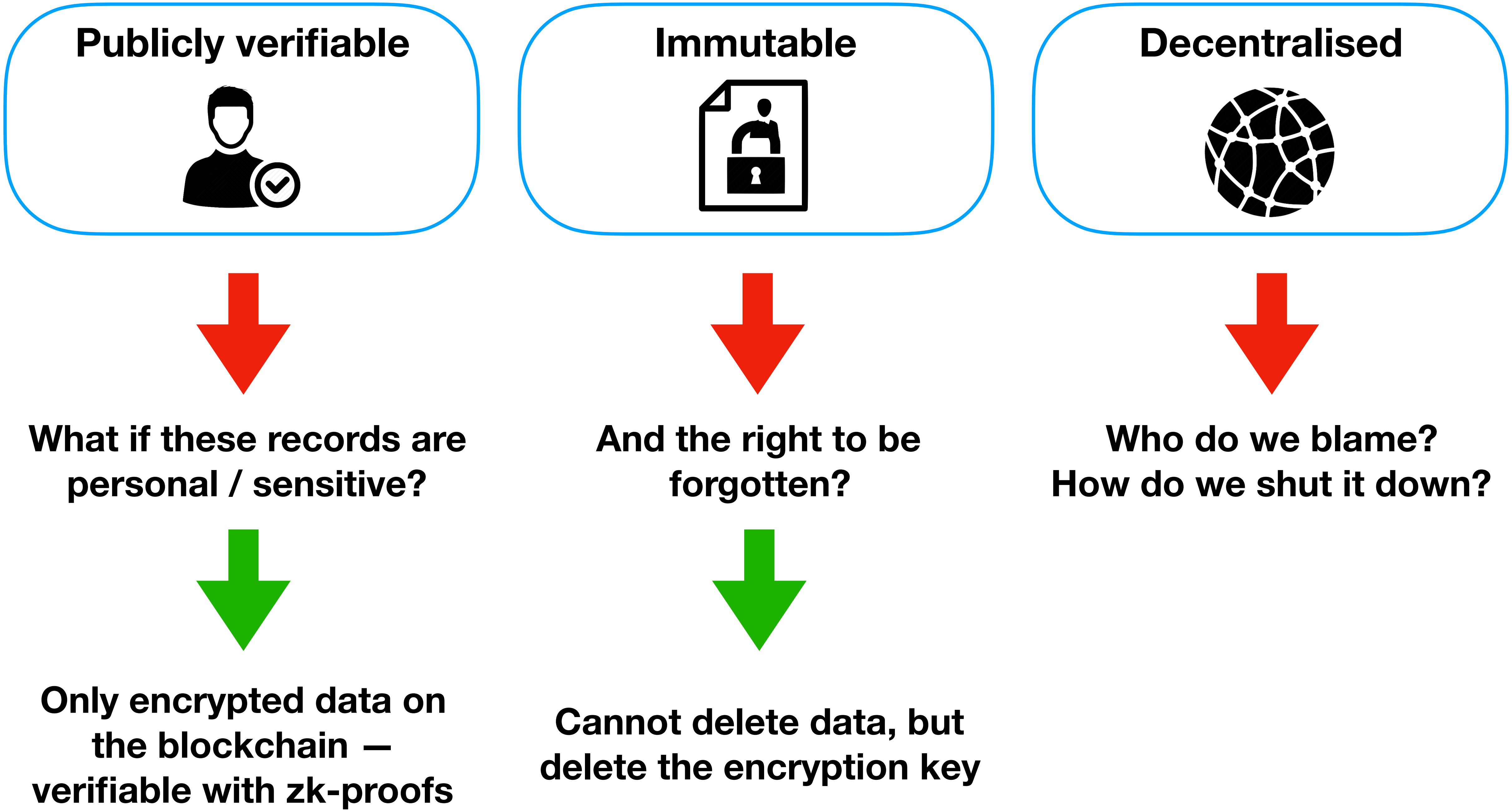
And the right to be forgotten?

Decentralised

Who do we blame?
How do we shut it down?

What are the main legal challenges?

- How does it mitigate the problems?



Publicly verifiable

What if these records are personal / sensitive?

Only encrypted data on the blockchain — verifiable with zk-proofs

Immutable

And the right to be forgotten?

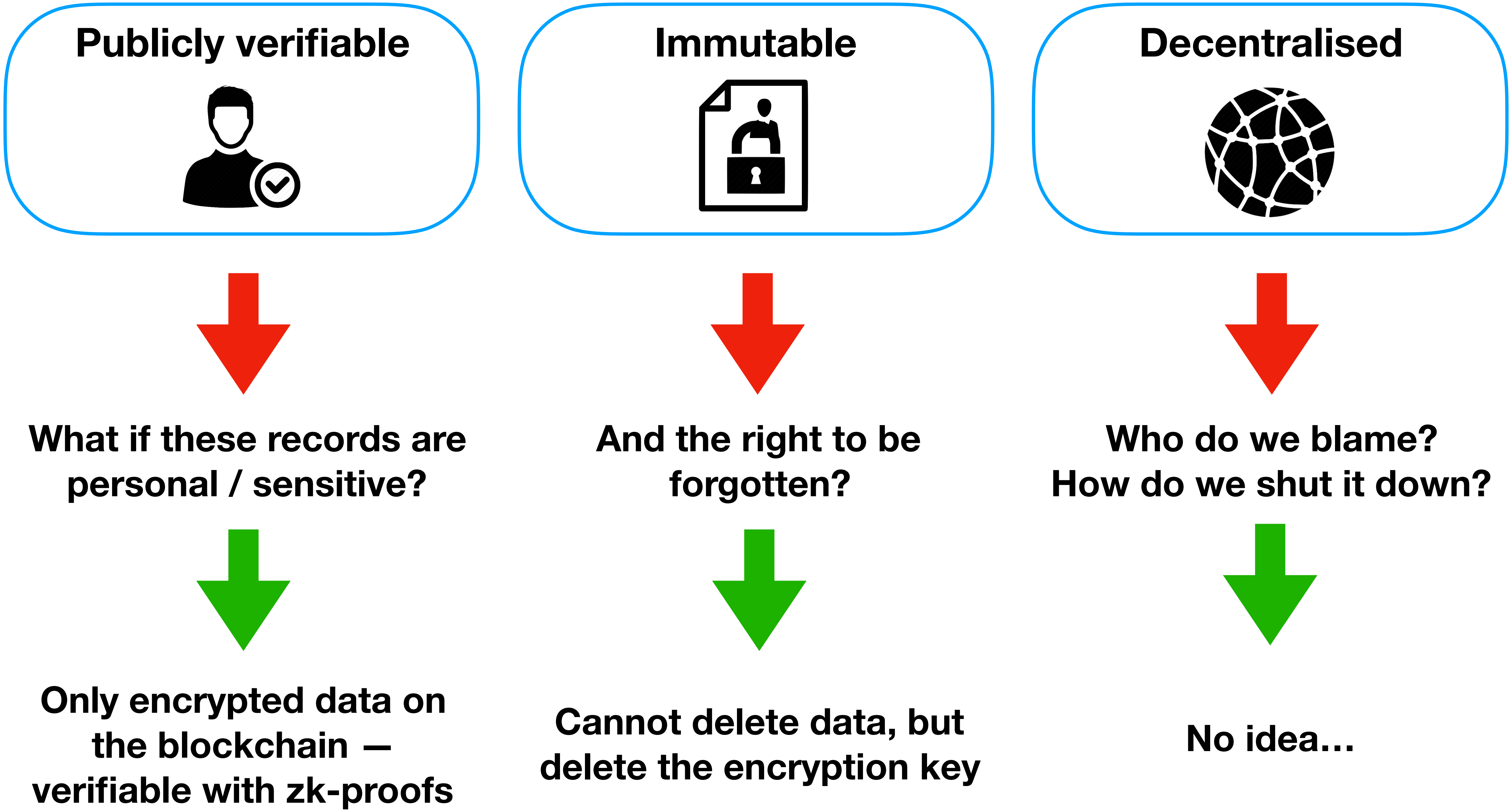
Cannot delete data, but delete the encryption key

Decentralised

Who do we blame?
How do we shut it down?

What are the main legal challenges?

- How does it mitigate the problems?



Publicly verifiable

What if these records are personal / sensitive?

Only encrypted data on the blockchain — verifiable with zk-proofs

Immutable

And the right to be forgotten?

Cannot delete data, but delete the encryption key

Decentralised

Who do we blame?
How do we shut it down?

No idea…

What are the main legal challenges?

- Is it satisfying enough?

What are the main legal challenges?

- Is it satisfying enough?

Since encrypted data are indistinguishable from random, are they still considered ‘personal data’?

What are the main legal challenges?

- Is it satisfying enough?

Since encrypted data are indistinguishable from random, are they still considered ‘personal data’?

Let’s ask Alice: “*Are* 🔒 *real data or random numbers?*”

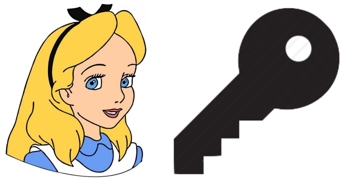
What are the main legal challenges?

- Is it satisfying enough?

Since encrypted data are indistinguishable from random, are they still considered ‘personal data’?

Let’s ask Alice: “*Are* 🔒 *real data or random numbers?*”

If Alice knows the encryption key, she can tell apart encrypted data from random



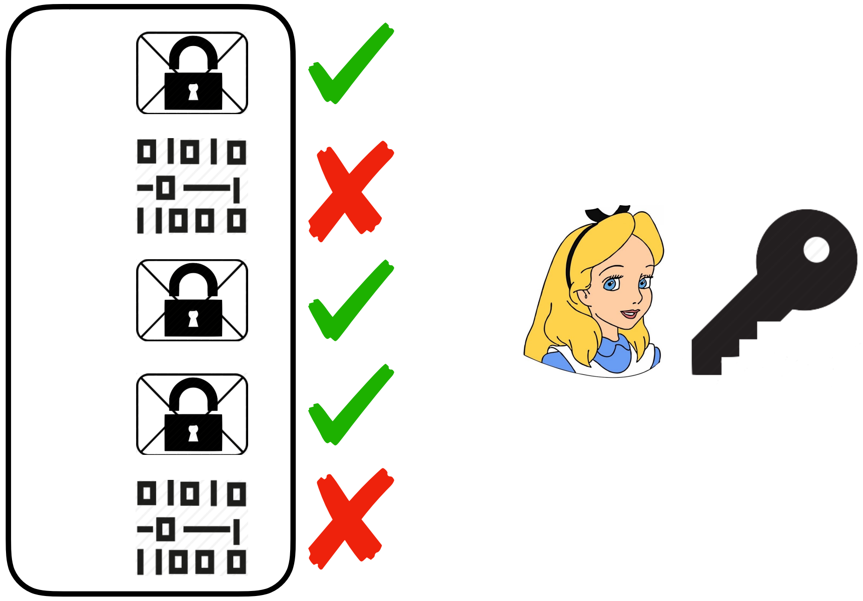
What are the main legal challenges?

- Is it satisfying enough?

Since encrypted data are indistinguishable from random, are they still considered ‘personal data’?

Let’s ask Alice: “*Are* 🔒 *real data or random numbers?*”

If Alice knows the encryption key, she can tell apart encrypted data from random



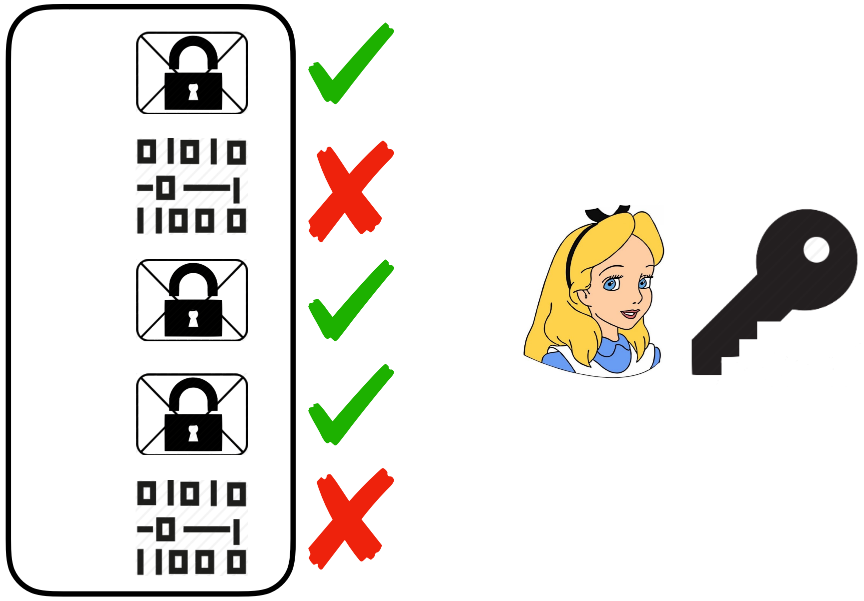
What are the main legal challenges?

- Is it satisfying enough?

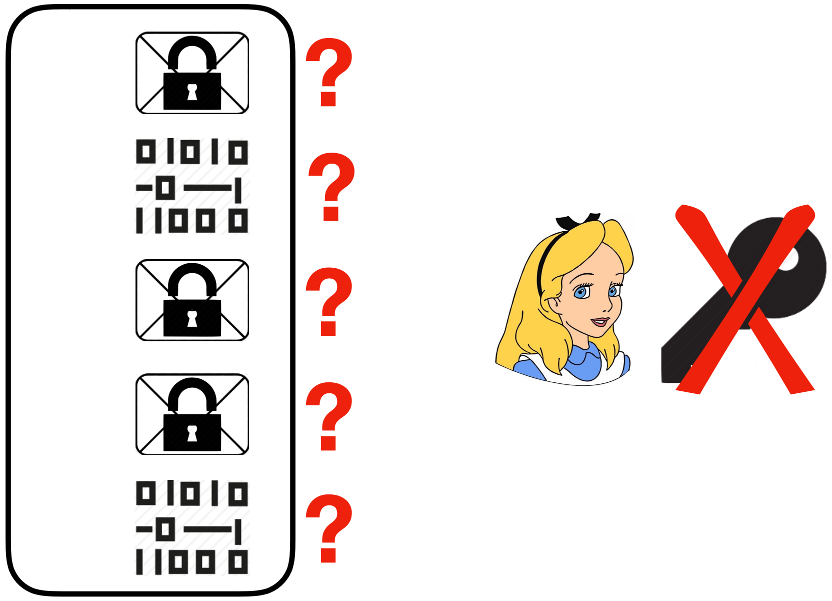
Since encrypted data are indistinguishable from random, are they still considered ‘personal data’?

Let’s ask Alice: “*Are* 🔒 *real data or random numbers?*”

If Alice knows the encryption key, she can tell apart encrypted data from random



If Alice does not know the encryption key (i.e, the key has been deleted), she cannot



Conclusion

- What did we talked about?

Blockchains are cool for engineers

provide unique properties
enable many useful applications

Conclusion

- What did we talked about?

Blockchains are cool for engineers

provide unique properties
enable many useful applications

But give headache to lawyers

nothing can be erased or modified
no-one to blame, international, …

Good Luck

Thank you for you attention
Questions?

Alberto Sonnino
alberto.sonnino@ucl.ac.uk