

La confidentialité numérique et les blockchains

Linus Gasser - C4DT / EPFL



<https://go.epfl.ch/ssie-2022>



Outline

- Confidentialité numérique
 - Pourquoi c'est important?
 - Abus de vos données personnelles
- Blockchains
 - Qu'est-ce que c'est?
 - Quels types de blockchain existent?
- Des blockchains confidentielles
 - Zero Knowledge Proofs
- Conclusion



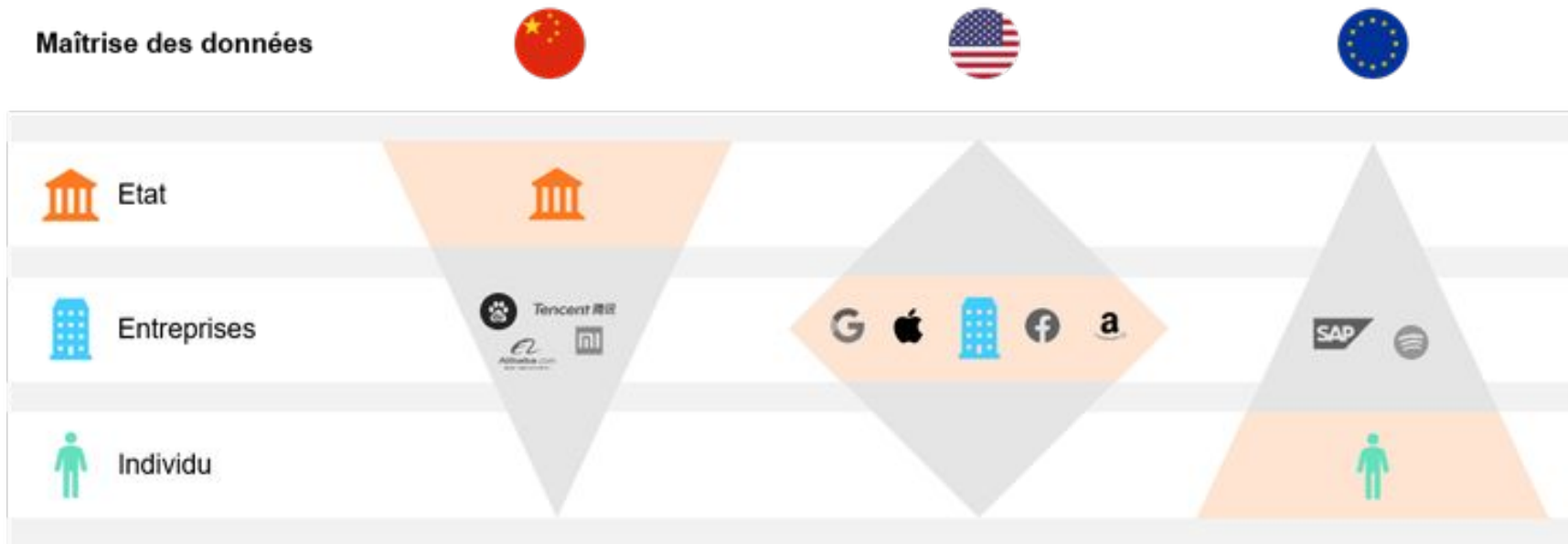
<https://go.epfl.ch/ssie-2022>



Confidentialité numérique

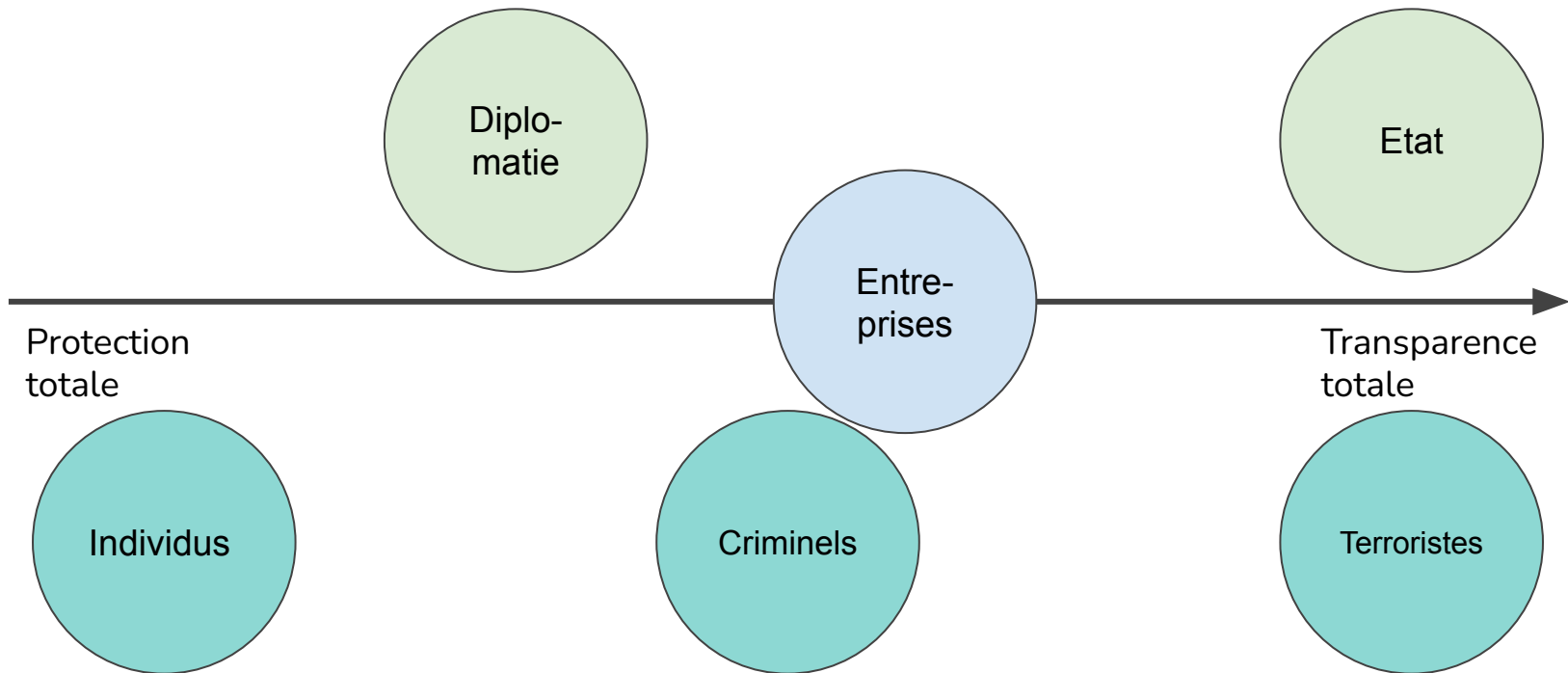
Propriété des données dans le monde

Maîtrise des données





Confidentialité de données



Abus de vos données personnelles

Quelles attaques et abus de la confidentialité?

Individus



Vol de données
Exploitation
Chantage

L'état

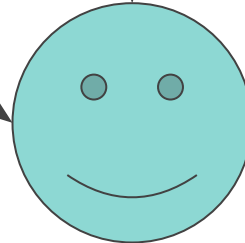


Surveillance abusif
Restrictions des
libertés

Entreprises
Groupements



Profilage
Vente produit
Influence politique



Attaques par des individus

U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

see Note: The Breach Notification Portal will be offline for maintenance from Sat Apr 24 10:00 PM EDT to Sat Apr 24 11:00 PM EDT. Any information being entered when the Portal is taken off-line will be lost.

Under Investigation Archive Help for Consumers

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.
[Show Advanced Options](#)

Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
⊕	Optum360, LLC	MN	Business Associate	11500000	07/01/2019	Hacking/IT Incident	Network Server
⊕	Florida Healthy Kids Corporation	FL	Health Plan	3500000	01/29/2021	Hacking/IT Incident	Network Server
⊕	Dominion Dental Services, Inc., Dominion National Insurance Company, and Dominion Dental Services USA, Inc.	VA	Health Plan	2964778	06/21/2019	Hacking/IT Incident	Network Server
⊕	Immediata Health Group, Corp.		Healthcare Clearing	1565338	05/07/2019	Unauthorized Access/Disclosure	Network Server

SRF News Sport Meteo Kultur DOK

News > Schweiz >

Datenleck bei Impfplattform?

Datenschutzler eröffnet Verfahren gegen meineimpfungen.ch

Dienstag, 23.03.2021, 11:13 Uhr
Aktualisiert um 12:15 Uhr

[f](#) [t](#) [w](#) [m](#)

Dieser Artikel wurde 19-mal geteilt.

- Der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat ein formelles Verfahren gegen die Betreiberin der Plattform www.meineimpfungen.ch eröffnet.

Abus par l'état

← Thread

 **Carmela Troncoso** @carmelatroncoso · 20. Apr. ...

More on Digital Green Certificates claiming that they are "secure & private by design" As I dive into at length in the thread below, this claim is not well supported by documentation. I find so worrisome that the term privacy-by-design is used in a frivolous manner by regulators

Transparency and data protection

- Privacy- and security-by-design
- All software developed in Open Source and made publicly available to the community for scrutiny
- The EU Gateway stores only Public Keys – no personal data
- Verifier app does not store personal data
- Both paper and digital versions



 **Carmela Troncoso** @carmelatroncoso · 9. Apr.

We hear that the Digital Green Certificate (DGC) is good news as it will enable "safe free movement". Safe free movement is great news, the technical proposal not so much

A long thread coming 🗨️ [twitter.com/EU_Commission/...](https://twitter.com/EU_Commission/)
[Diesen Thread anzeigen](#)

2 17 33

the **guardian**

NSA FILES: *DECODED*

What the revelations mean for you.





Abus par les entreprises et les organisations

All the Ways Facebook Tracks You—and How to Limit It

If you have a Facebook account—and even if you don’t—the company is going to collect data about you. But you can at least control how it gets used.



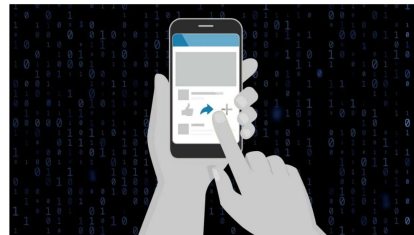
ILLUSTRATION: ELENA LACEY; BETTY IMAGES

How Facebook Tracks You, Even When You're Not on Facebook

Facebook and others use the data to target consumers. Here's what you need to know—and what you can do about it.

By Allen St. John

April 11, 2018



istock 648828446 and istock-856692422

**Trusted Advice
Delivered Straight
To Your Inbox**

Get insights and tips from our
experts on everyday decisions.

Email

[Privacy Policy](#)

Sign Up

Attaques sur vos opinions

The New York Times

SUBSCRIBE FOR

Cambridge Analytica and Facebook: The Scandal and the Fallout So Far

Revelations that digital consultants to the Trump campaign misused the data of millions of Facebook users set off a furor on both sides of the Atlantic. This is how The Times covered it.

Give this article

Support the Guardian

Available for everyone, funded by readers

Contribute →

Subscribe →

News Opinion Sport Culture Lifestyle More

World Europe US Americas Asia Australia Middle East Africa Inequality Global development

Jair Bolsonaro

This article is more than 1 year old

WhatsApp fake news during Brazil election 'favoured Bolsonaro'

Analysis suggests vast majority of viral messages with false information were rightwing

Daniel Avelar

Wed 30 Oct 2019 16:00 GMT

3,307



The Takeaway

Stories Episodes Special Projects Contact Us Team

LISTEN FOR FREE

SUPPORT US

How Fake News in India is Causing Real Violence

LISTEN Download Embed

July 30, 2018

Share

DW Made for minds.

Search TOP STORIES

TOP STORIES MEDIA CENTER TV RADIO LEARN GERMAN

GERMANY CORONAVIRUS WORLD BUSINESS SCIENCE ENVIRONMENT CULTURE SPORTS

TOP STORIES / WORLD / ASIA

ASIA

Bangladesh: Fake news on Facebook fuels communal violence

Fake news spread via Facebook has triggered several communal clashes resulting in deaths in Bangladesh. Bangladesh's post and telecommunication minister told DW Facebook failed to create measures to identify hate speech.

f t y e +

Date 01.11.2019

Author Rahat Raza

Related Subjects Facebook, Asia, Fake news

Keywords Asia, Bangladesh, Facebook, fake news, violence

Send us your feedback

Print Print this page

Permalink https://p.dw.com/p/3SL3E3





**THE TECHNOLOGY THAT CONNECTS
US
ALSO DIVIDES US**



The Social Dilemma

- Fait par Netflix - qui profite aussi de nous...
- Regardez:
 - Mouvement IRL -> virtuel
 - Personnages “cyber” représentent des algorithmes d’intelligence artificielle
- Jaron Lanier
 - De quelle manipulation parle-t-il?
 - Est-ce que vous êtes soumis·e·s à la même manipulation?



Pourquoi je dois me protéger?

- Votre opinion vaut de l'argent
 - Pour des achats compulsifs
 - Changer l'opinion politique
- Changement individuels
 - Discussions entre amis
 - Recherche approfondie sur sujet
- Manipulations en masse
 - Visualisation et partage de fake news
 - Influence d'opinion abusif par des pubs



Comment changer cela?

1/2

- Cadre légal
 - RGPD en Europe depuis 2018
 - nLPD en Suisse pour Septembre 2023
- Logiciels
 - AdBlocker / Pi-Hole
 - Sauvegardes (contre les cryptages)
 - Authentification avec un deuxième facteur



Comment changer cela?

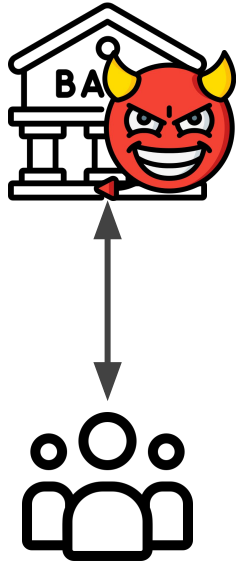
2/2

- Vous-mêmes
 - N'utilisez les réseaux sociaux aussi peu que possible
 - Eteignez les notifications
 - Créez des zones et plages horaires sans écran
 - Désinstallez des applications
- Vos élèves
 - Aidez-les à comprendre l'enjeu
 - Faites des défis
 - 2 heures / jours sans téléphone
 - proposer d'autres activités

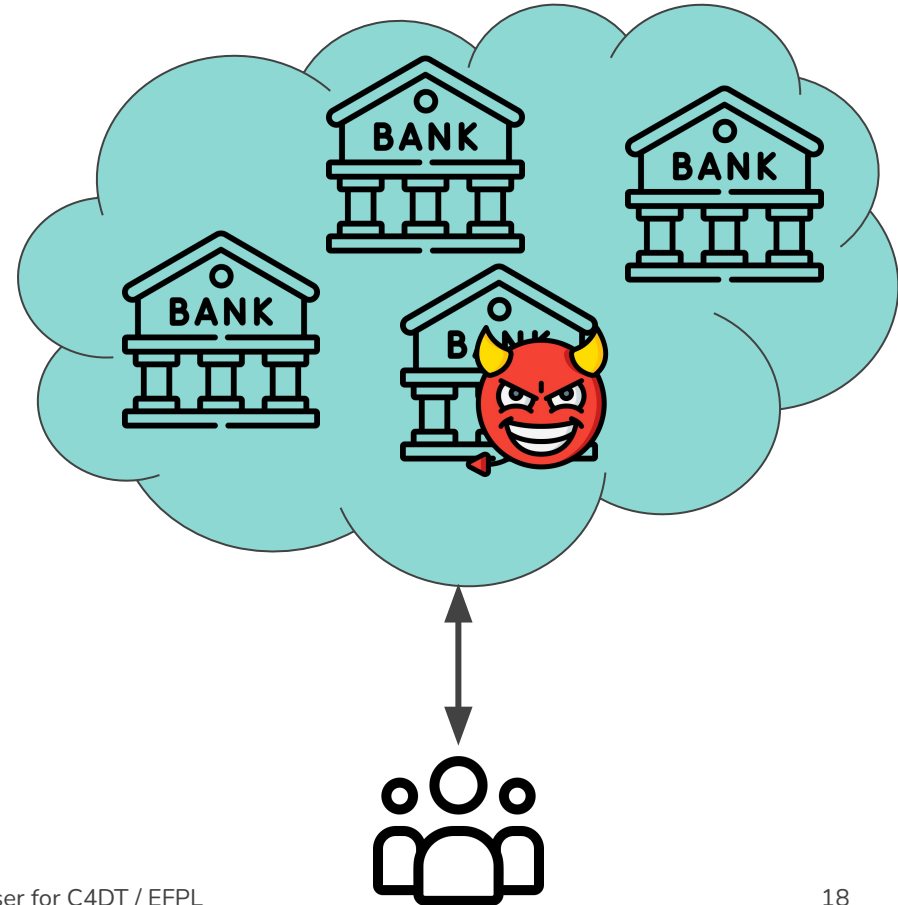


Blockchains - confiance et confidentialité

Qu'est-ce que c'est qu'une blockchain?



Satoshi 2008



Miami jury rules in favor of Craig Wright, who invented Bitcoin



MacKenzie Sigalos
@KENZIESIGALOS

SHARE [f](#) [t](#) [in](#) [✉](#)

KEY POINTS

- Australian computer scientist Craig Wright prevailed in a Miami civil case that pitted him against the family of his late business partner and computer forensics expert, David Kleiman.
- At stake was half of both the 1.1 million bitcoin mined and held by Satoshi, a cache currently worth around \$54 billion.



Mystery in Big Sky Country

WATCH LIVE

UP NEXT | **Dateline** 03:00 am ET

[Listen](#)

TRENDING NOW



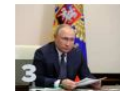
1

2-year Treasury yield tops 10-year rate, a 'yield curve' inversion that could signal a recession



2

Americans are 'wasting too much money on housing,' says economist —here are 4 ways to get 'house rich'



3

Russian troops leave Chernobyl; UK spy chief says Putin 'massively misjudged' war



Problèmes résolus par Satoshi en 2008

- Qui fait parti des banques?
 - Bitcoin: une loterie statistique qui choisit une nouvelle banque toutes les 10 minutes
 - Proof-of-work
 - Autres: chaque nouvelle banque doit faire un dépôt
 - Proof-of-stake
- Avantages
 - Ne pas dépendre d'une entité centrale
 - Environnement peu régulé
- Désavantages
 - Bitcoin: utilisation excessive d'énergie, lenteur d'une transaction
 - Cours très volatil

Quelques types de blockchains

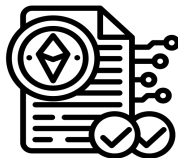
Confiance
distribuée

Confidentielles



Cryptomonnaies

 **bitcoin**

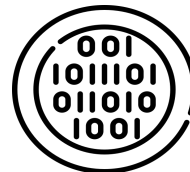


Smart Contracts



ethereum

AVALANCHE



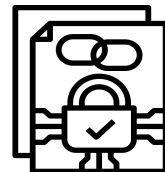
Cryptomonnaies
protégeant la
sphère privée



MONERO



Zcash



Zero-Knowledge-
Proof based
blockchains



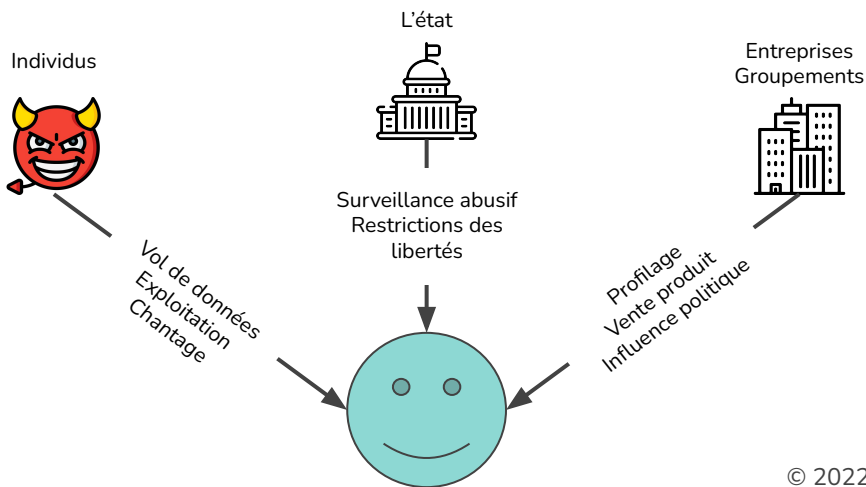
Mina
(MINA)



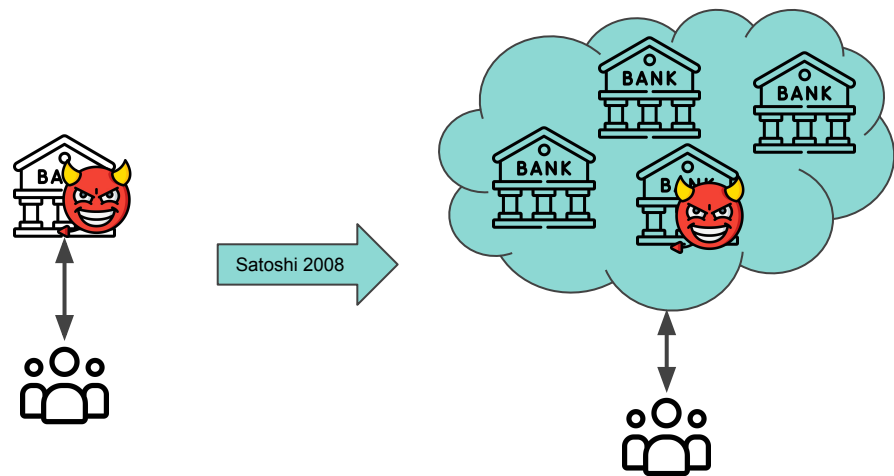
Des blockchains confidentielles

Confidentialité et blockchains

Besoin de confidentialité



Aucune autorité centrale





Zero-Knowledge Proofs

Preuves à divulgation nulle de connaissance

Un algorithme avec



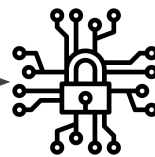
Trusted Entity
Tiers de confiance

Émet un
certificat de
l'adresse



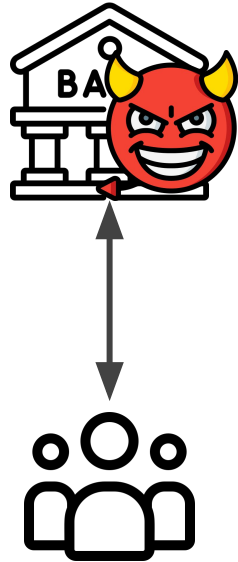
Prover
Émission de preuve

J'habite en
Suisse

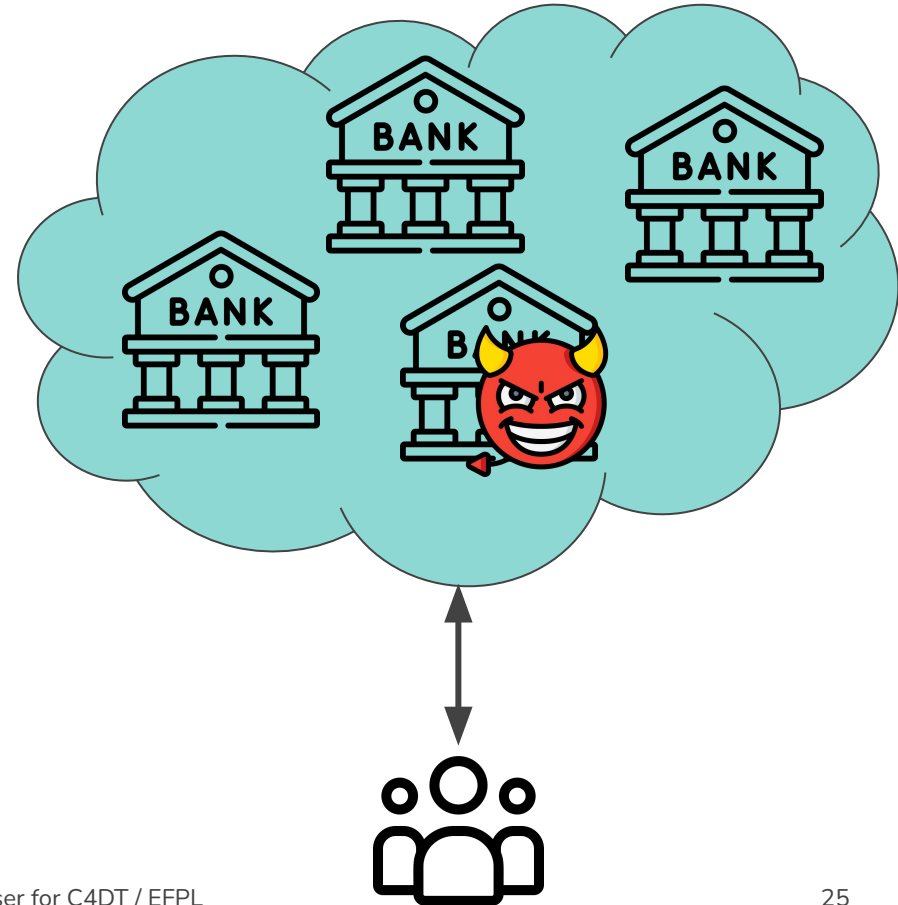


Verifier
Vérification de la preuve

Qu'est-ce que c'est qu'une blockchain?

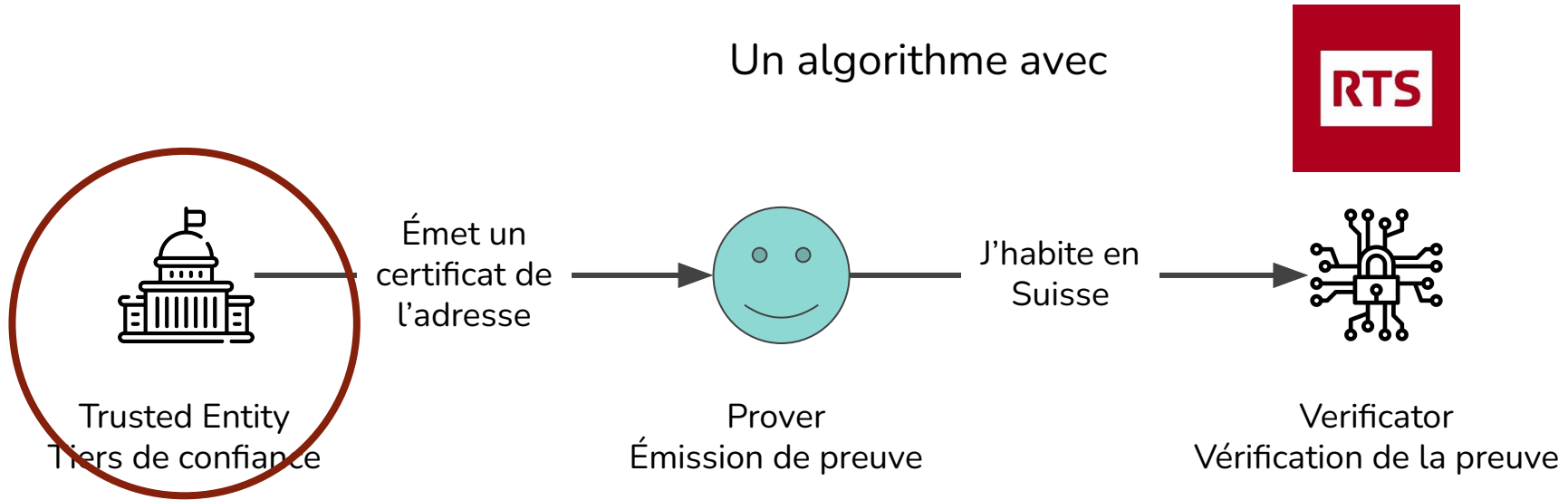


Satoshi 2008



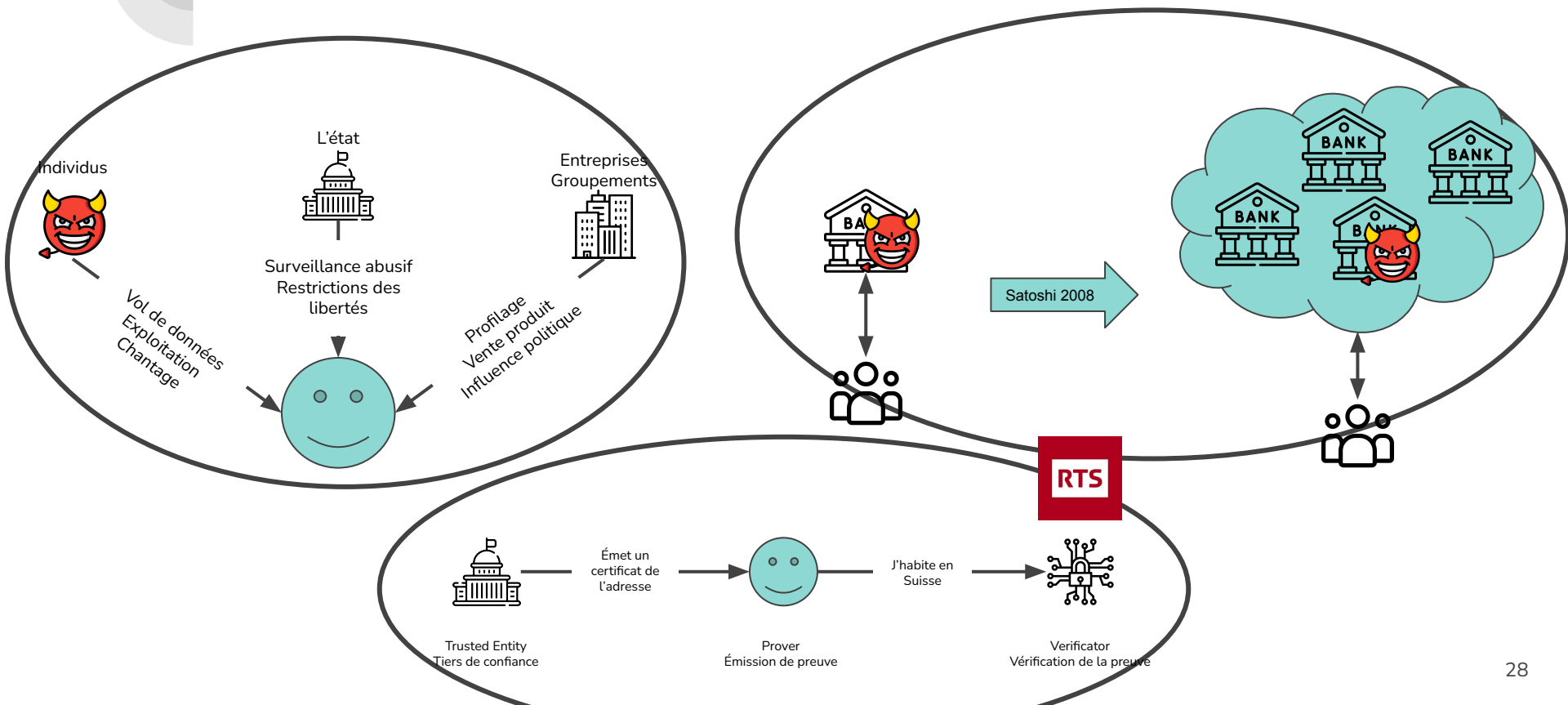
Zero-Knowledge Proofs

Preuves à divulgation nulle de connaissance



Conclusion

Résumé





Conclusion

- Prenez soin de vos données
 - Minimisez le nombre d'applications et comptes sur internet
 - Soyez prudent quand et où vous partagez des informations personnelles
- Ne soyez pas des mauvaises influenceu·ses·res
 - Réfléchissez deux fois avant de visualiser et de partager une vidéo
 - Ne répondez pas à toutes les provocations
- Des outils techniques pour protéger votre confidentialité
 - Le **cadre légal** doit être mis en place
 - Une **blockchain** peut décentraliser la confiance
 - Les preuves à divulgation nulle de connaissances (**ZKP**) sont un outil intéressant