La confidentialité numérique et les blockchains

Linus Gasser - C4DT / EPFL

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

Outline

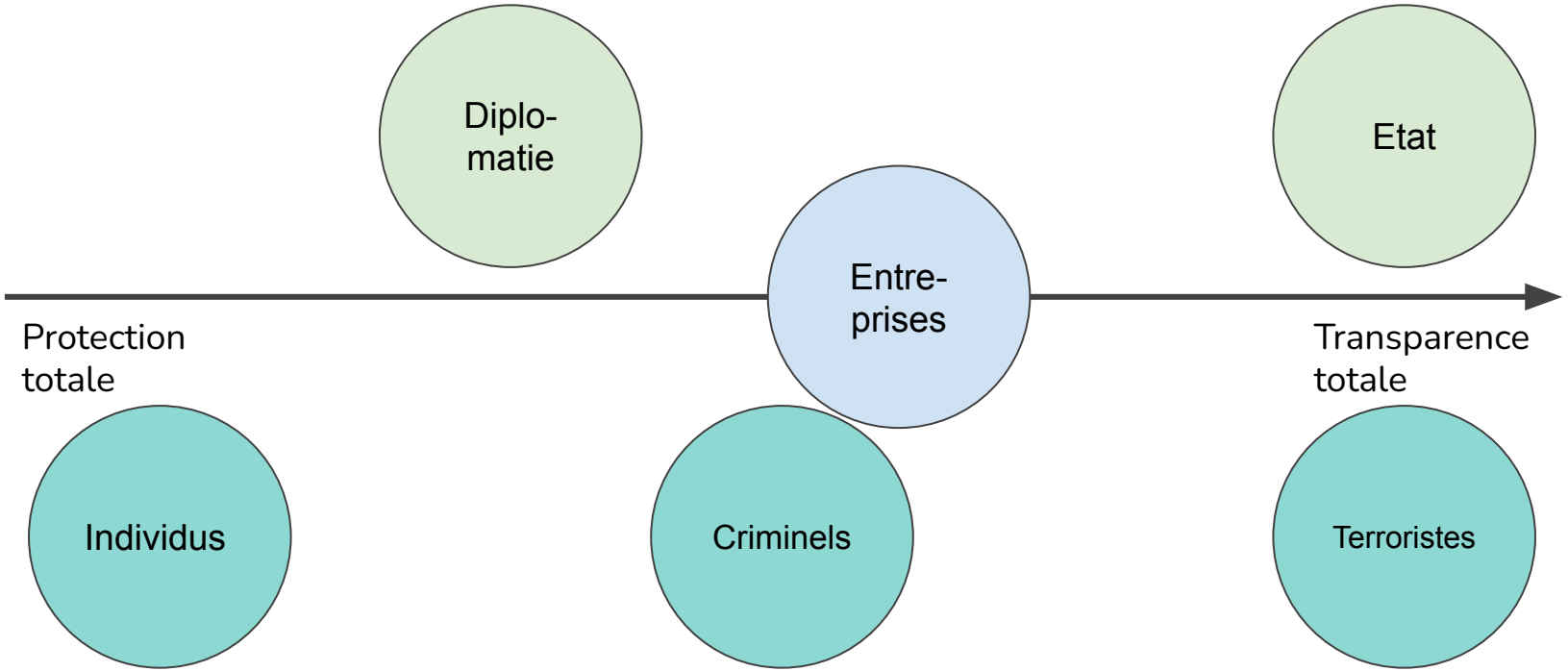
- Confidentialité numérique
  - Pourquoi c'est important?
  - Abus de vos données personnelles
- Blockchains
  - Qu'est-ce que c'est?
  - Quels types de blockchain existent?
- Des blockchains confidentielles
  - Zero Knowledge Proofs
- Conclusion

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

Confidentialité numérique

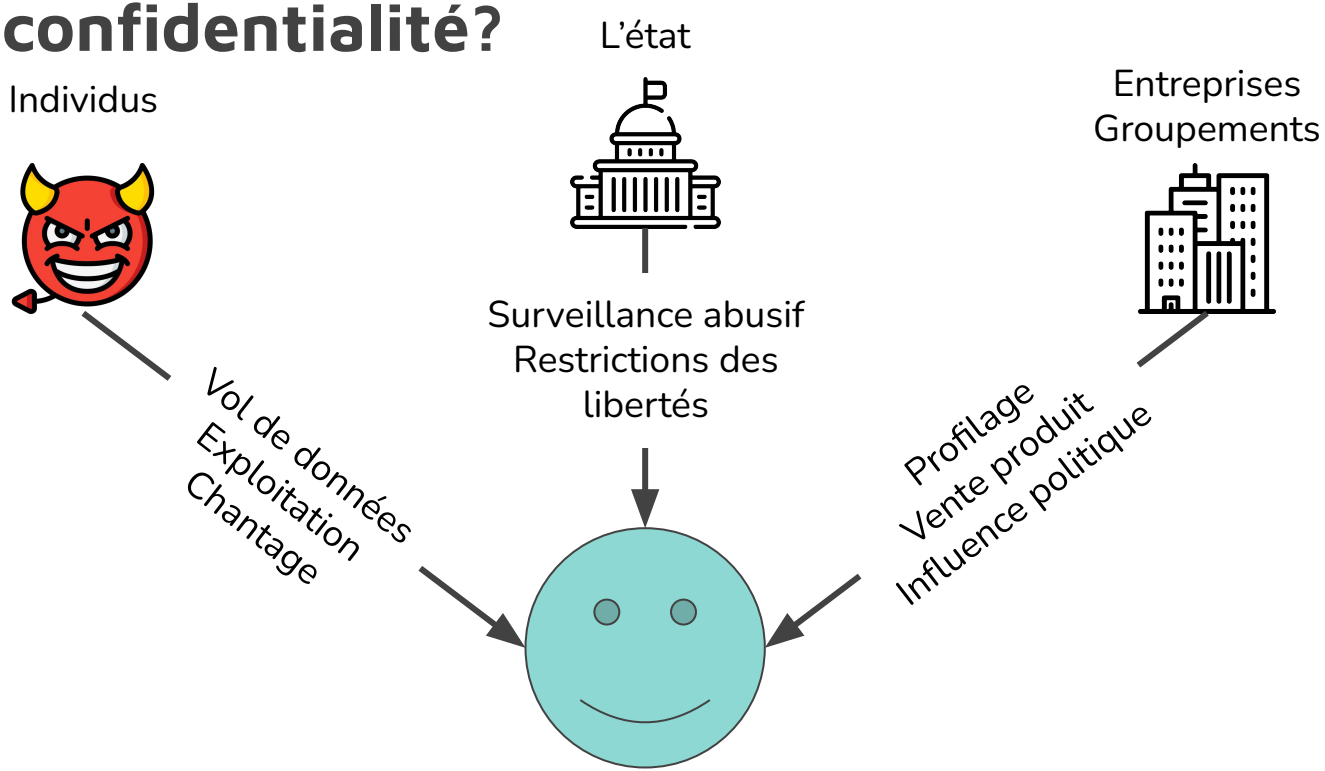
Propriété des données dans le monde

Confidentialité de données

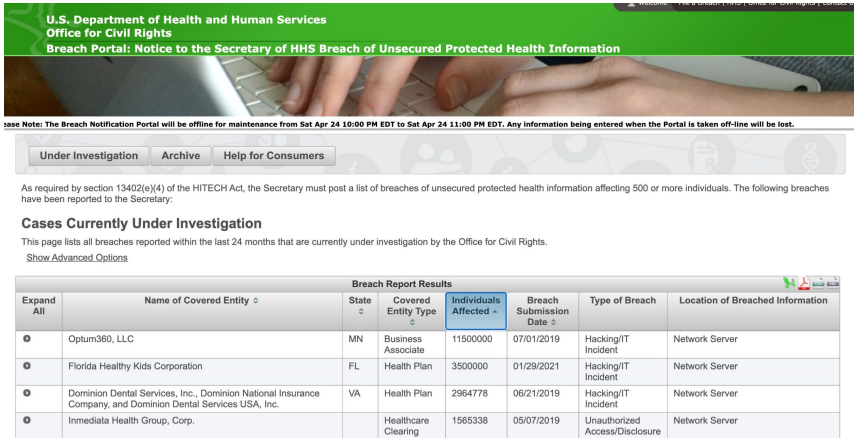


Abus de vos données personnelles

Quelles attaques et abus de la confidentialité?



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

ease 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:

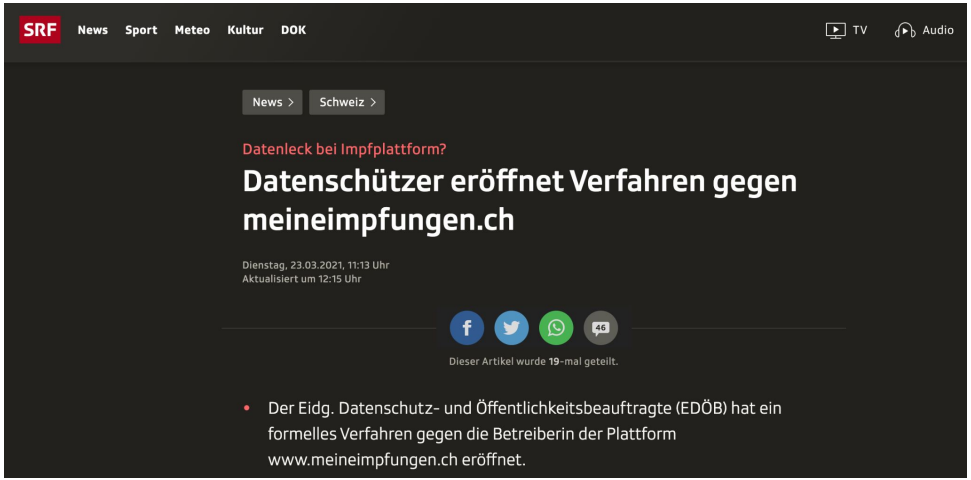
Cases Currently Under Investigation

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
	Inmediata Health Group, Corp.		Healthcare Clearing	1565338	05/07/2019	Unauthorized Access/Disclosure	Network Server



SRF News Sport Meteo Kultur DOK TV Audio

News > Schweiz >

Datenleck bei Impfplattform?

Datenschützer eröffnet Verfahren gegen meineimpfungen.ch

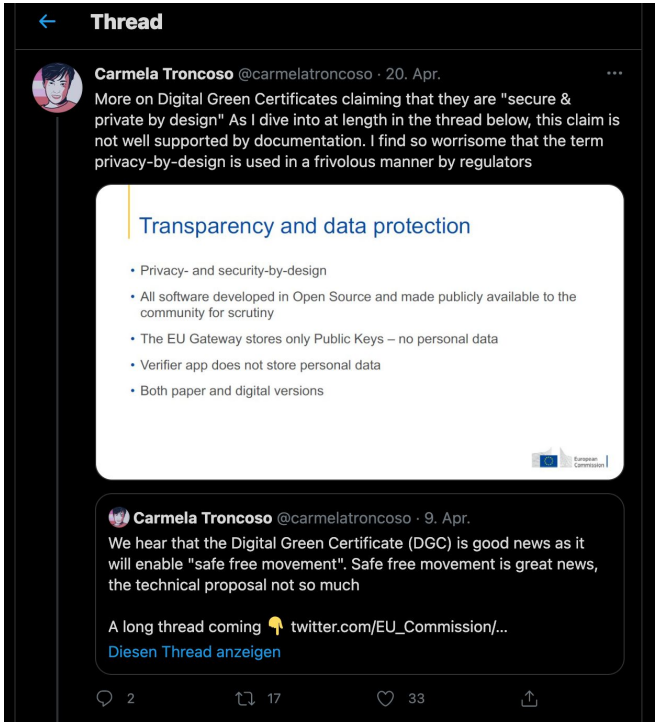
Dienstag, 23.03.2021, 11:13 Uhr
Aktualisiert um 12:15 Uhr

46

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



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; GETTY IMAGES

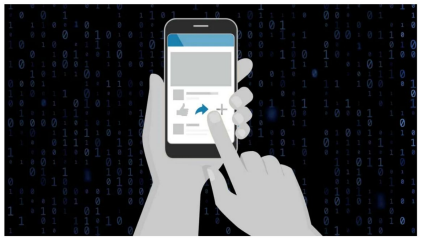
How Facebook Tracks You, Even When You're Not on Facebook

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

43



iStock 648828446 and iStock-856692422

Trusted Advice Delivered Straight To Your Inbox

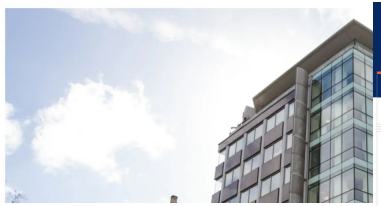
Get insights and tips from our experts on everyday decisions.

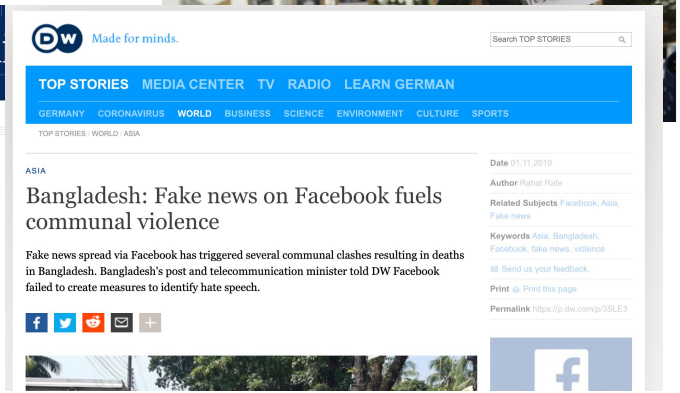
Email

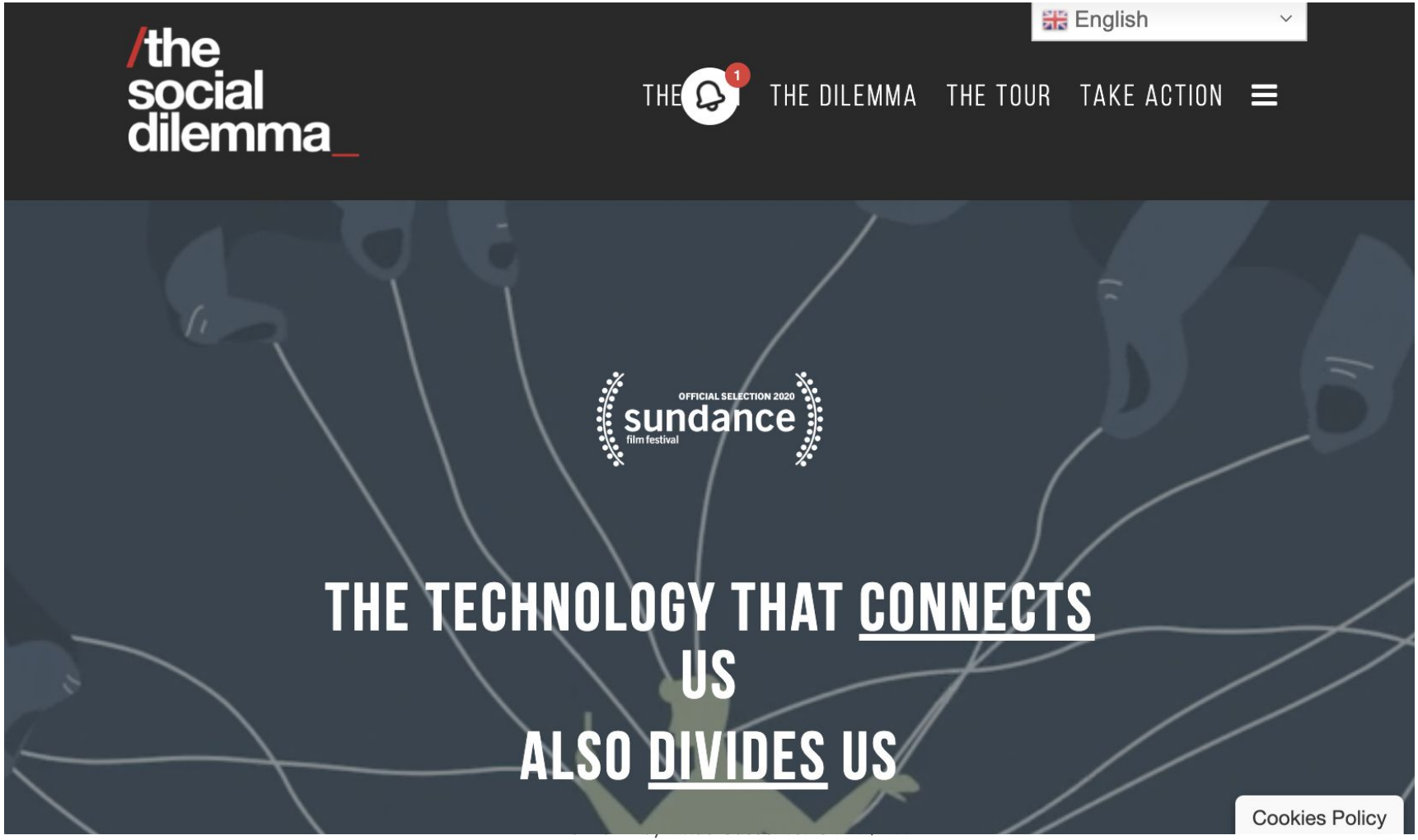
Privacy Policy

Sign Up

Attaques sur vos opinions






English
/the social dilemma_
THE
1
THE DILEMMA
THE TOUR
TAKE ACTION
OFFICIAL SELECTION 2020
sundance
film festival
THE TECHNOLOGY THAT CONNECTS
US
ALSO DIVIDES US
Cookies Policy

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

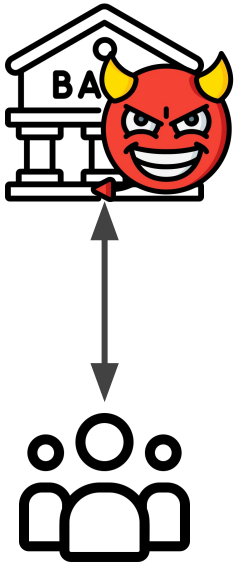
- Cadre légal
  - RGPD en Europe depuis 2018
  - nLPD en Suisse pour Septembre 2023
- Logiciels
  - AdBlocker / Pi-Hole
  - Sauvegardes (contre les cryptages)
  - Authentification avec un deuxième facteur

Comment changer cela? 2/2

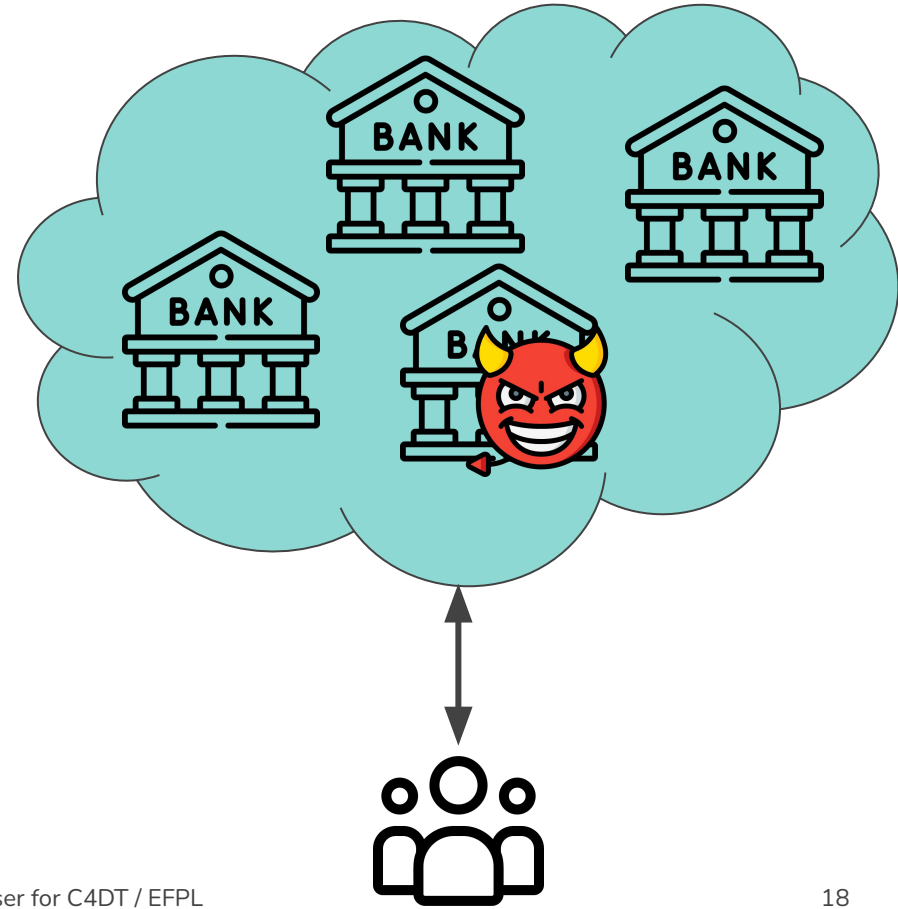
- Vous-mêmes
  - N’utilisez les réseaux sociaux aussi peu que possible
  - Eteignez les notifications
  - Créez des zones et plages horaires sans écran
  - Désinstallez des applications
- Vos élèves
  - Aidez-les à comprendre l’enjeu
  - Faites des défis
    - 2 heures / jours sans téléphone
    - proposer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

Blockchains – confiance et confidentialité

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



Satoshi 2008



TECH

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

MacKenzie Sigalos
@KENZIESIGALOS

SHARE

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.

TRENDING NOW

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

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

Russian troops leave Chornobyl; 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

Smart Contracts

Cryptomonnaies protégeant la sphère privée

Zero-Knowledge-Proof based blockchains

bitcoin

ethereum

AVALANCHE

MONERO

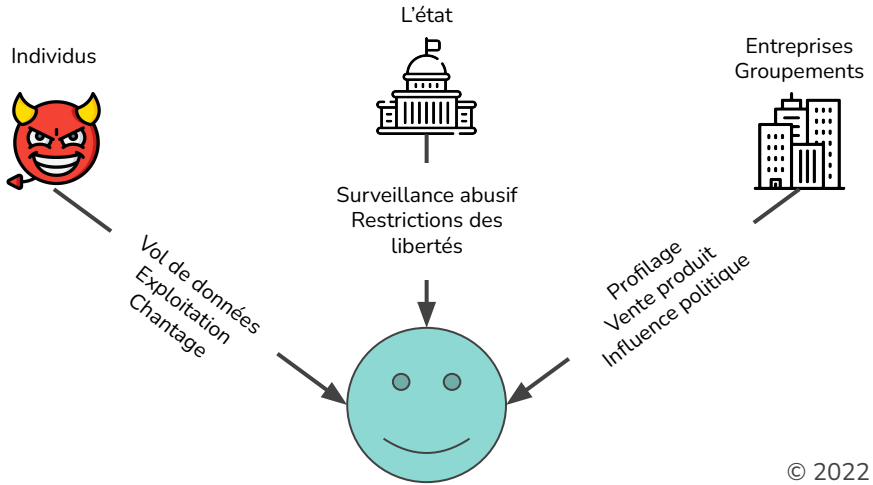
Zcash

Mina (MINA)

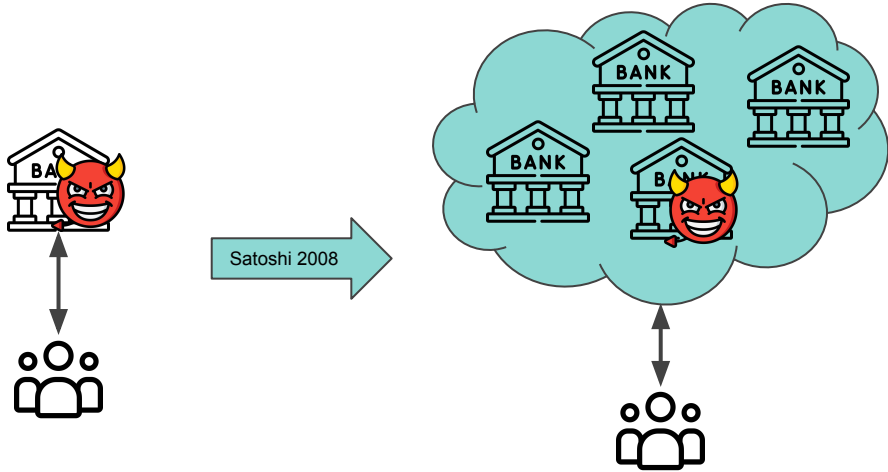
Des blockchains confidentielles

Confidentialité et blockchains

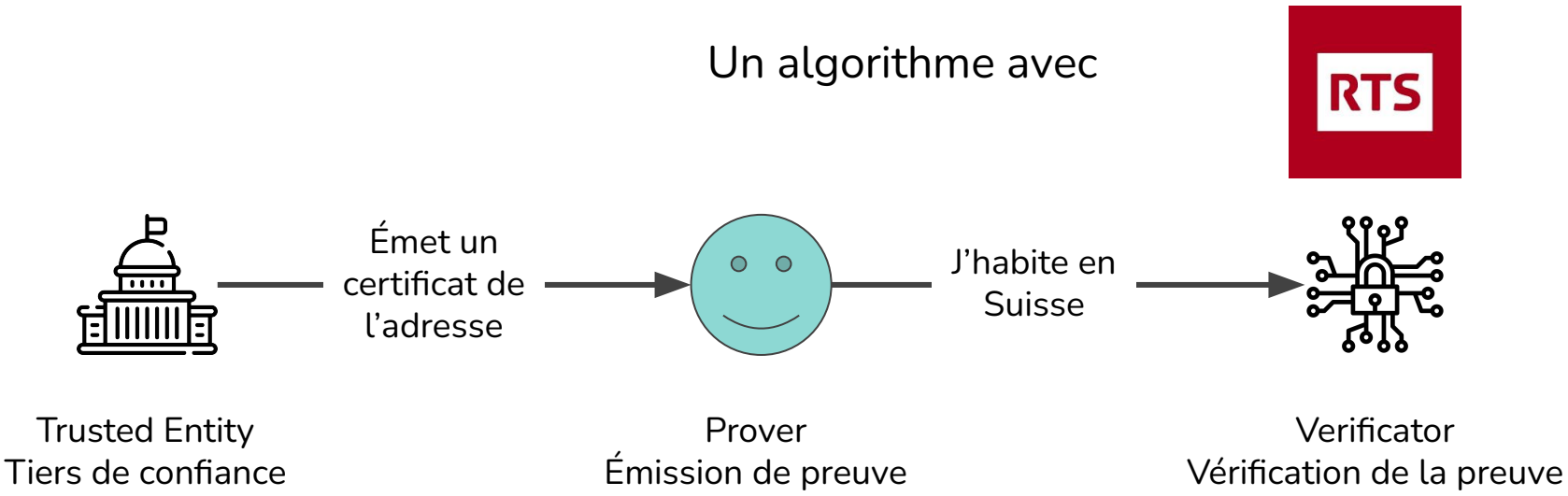
Besoin de confidentialité



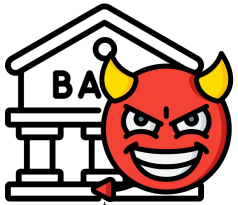
Aucune autorité centrale

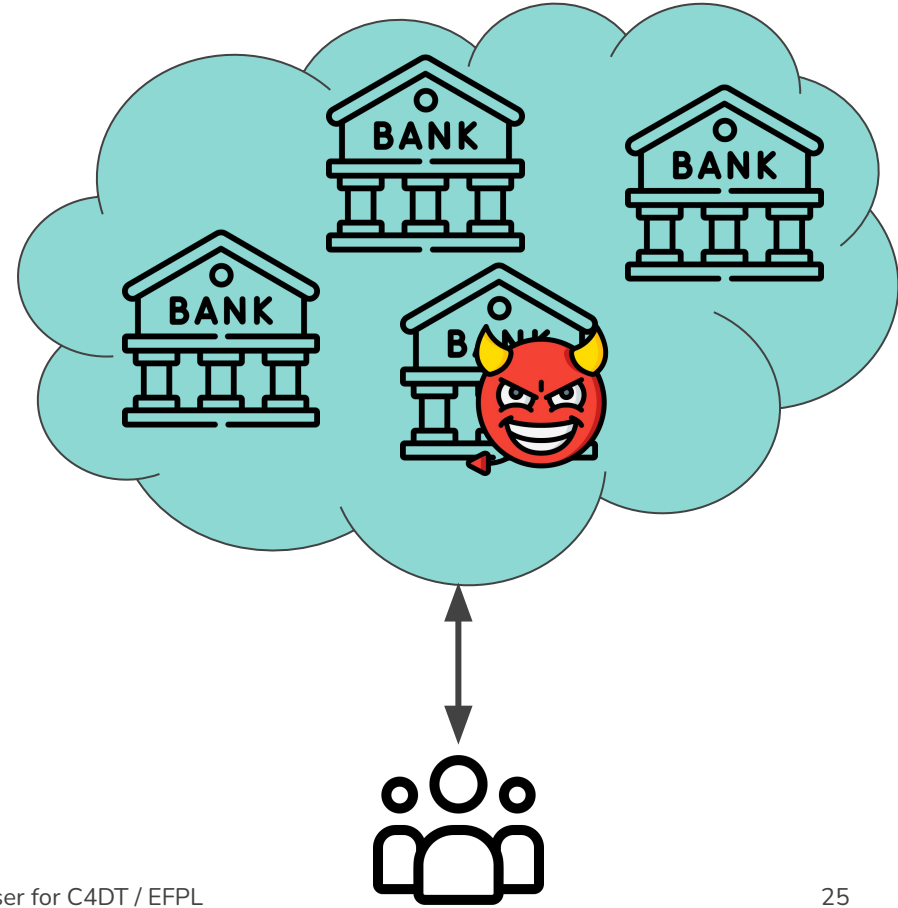


Zero-Knowledge Proofs
Preuves à divulgation nulle de connaissance

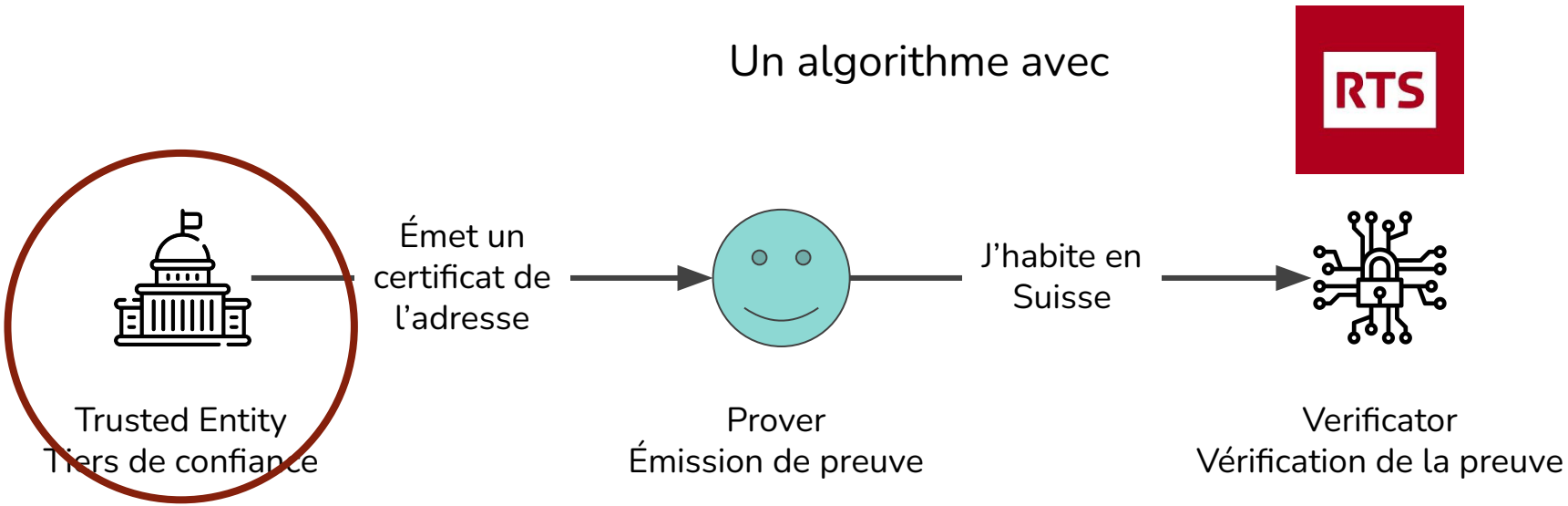


Qu’est-ce que c’est qu’une blockchain?



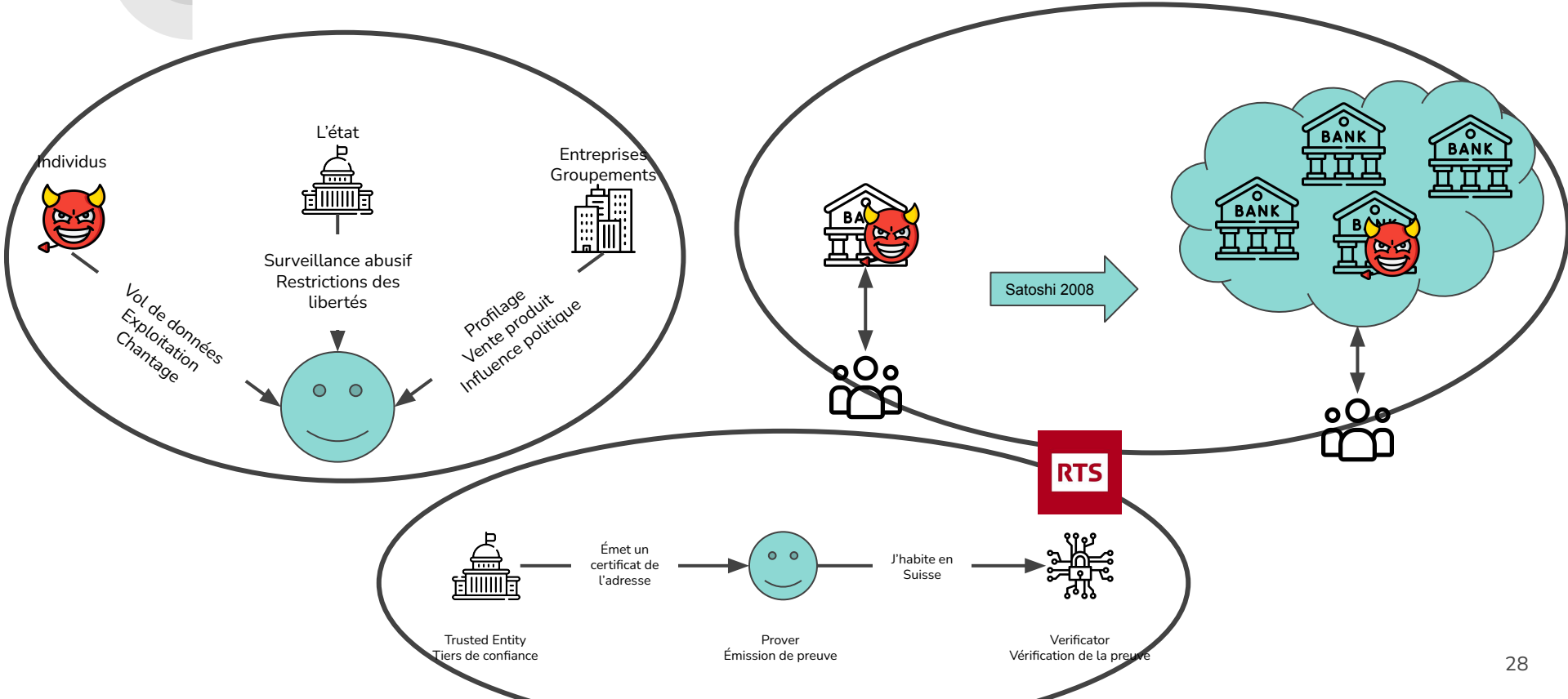


Zero-Knowledge Proofs
Preuves à divulgation nulle de connaissance



Conclusion

Résumé


Individus
L'état
Entreprises
Groupements
Surveillance abusif
Restrictions des libertés
Vol de données
Exploitation
Chantage
Profilage
Vente produit
Influence politique
Satoshi 2008
BANK
BANK
BANK
RTS
Émet un certificat de l'adresse
J'habite en Suisse
Trusted Entity
Tiers de confiance
Prover
Émission de preuve
Verificator
Vérification de la preuve

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