Blockchains & Accessibilité

Voyage au pays merveilleux des rêves cryptographiques

I. La blockchain

Quel est la première blockchain de l'histoire ?

Un peu d'histoire

MOTHERBOARD
TECH BY VICE

The New York Times

The World's Oldest Blockchain Has Been Hiding in the New York Times Since 1995

This really gives a new meaning to the "paper of record."

By Daniel Oberhaus


The New York Times.

TITANIC SINKS FOUR HOURS AFTER HITTING ICEBERG; 866 RESCUED BY CARPATHIA, PROBABLY 1250 PERISH; ISMAY SAFE, MRS. ASTOR MAYBE, NOTED NAMES MISSING

The Lost Titanic Sailing Toward Out of Belfast Harbor.

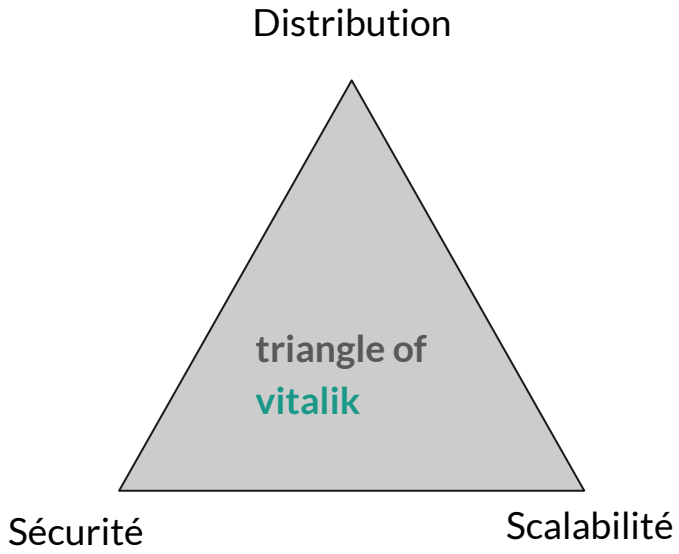
- 1982 - David Chaum, **premier protocol** de type blockchain : "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups."
- 1991 - **Arbres de Merkle** par Stuart Haber et W. Scott Stornetta
- 1995 - **Surety**, AbsoluteProof, **seau cryptographique** pour documents, intégré dans une blockchain et publiée dans les pages du **New York Times** en guise de preuves distribuées.

Le Bitcoin

- white paper published on **31 October 2008**.
- Satoshi Nakamoto
- Monnaie officielle du **Salvador** depuis 2021
- Accepté par l'**Ukraine** pour les donations
- **200 million** de tonnes de CO2 (University of Cambridge, Oct 2022)
- ATH: $66,974.77

Qu’est-ce qu’une blockchain

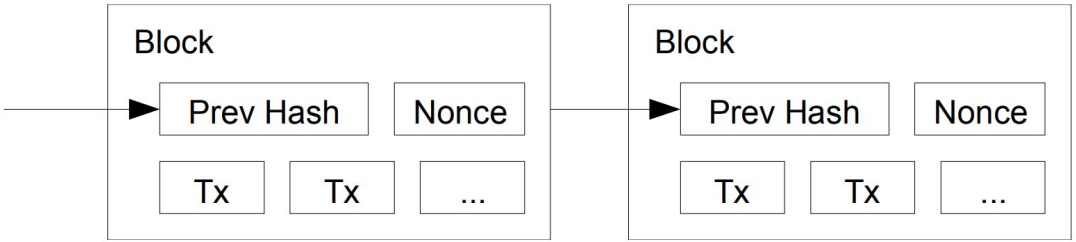
- **base de données** partagée -> les participants au réseau ont leur propre copie de la base
- Algo de **Consensus** -> accord commun
- **Distribution** -> infalsifiabilité et protection contre les pannes

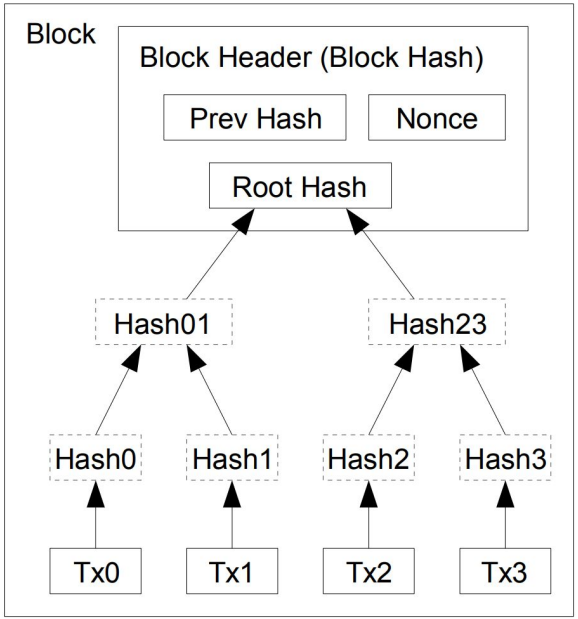


La chaîne de blocs

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org





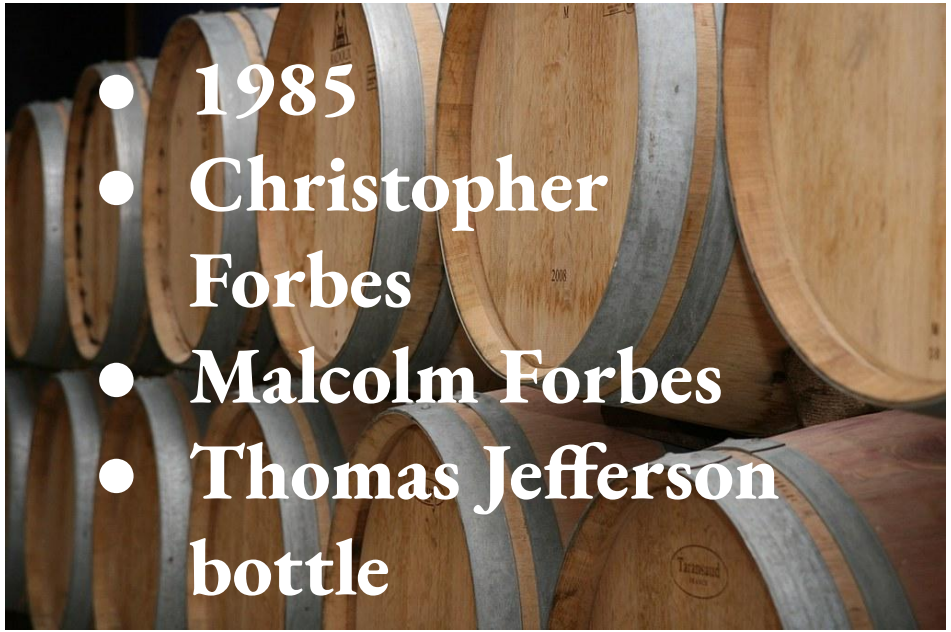
Transactions Hashed in a Merkle Tree

Idées reçues

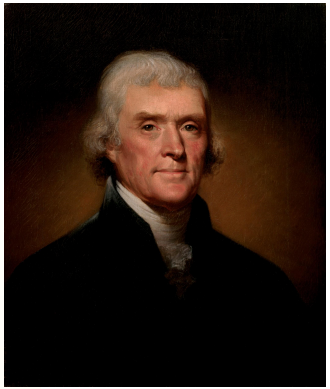
- Anonymité
- Publique
- Sécurisé

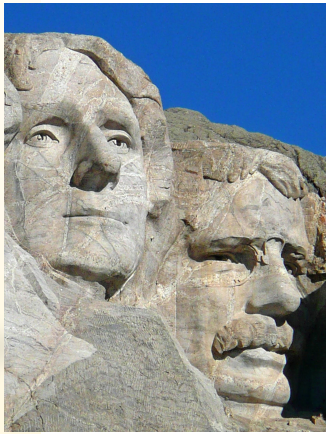
“Ni l'anonymat, ni le chiffrage des données mises sur un fichier blockchain, ni la présence d’un jeton comme celui du Bitcoin ne sont des caractéristiques fondamentales obligatoires d’une blockchain”. P27-28 *Au delà du Bitcoin*, Jean-Paul Delahaye

Parlons de choses sérieuses



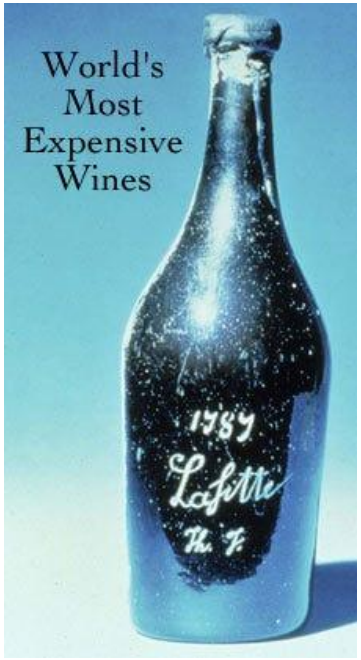
- 1985
- Christopher Forbes
- Malcolm Forbes
- Thomas Jefferson bottle



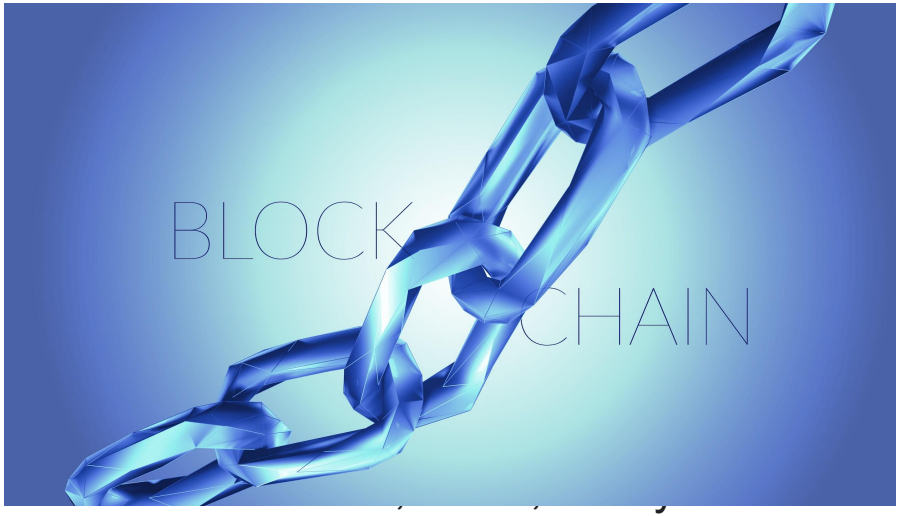


$157,000

($400000 aujourd’hui)



Usages possibles



- *Blockchain de cryptomonnaie*
  - **Bitcoin, Ethereum…**
- *Blockchain de diplôme*
  - **BCdiploma :** used by TOEIC,
- *Blockchain logistique ou de traçage*
  - **Tracr**, for diamond supply chain, by Diamond Trading Company
  - **ISTMOS**, par Origintrail and TagItSmart : *La chine vend 30000 bouteilles de vin de contrefaçon par heure, dangereux pour la santé*
  - **MADRE**, Banque de France, *délivre des identifiant SEPA*

II. Accessibilité ?

Accessibilité

L’accessibilité - monde du **handicap**, des **enfants** ou des **personnes** âgées, étendu à l'**ensemble des citoyens** et utilisé pour désigner **l'accès** aux domaines suivants :

- Physique, déplacement
- Éducatif
- Civique, droit de vote ;
- Culturel, numérique,
- Travail
- Santé

Capitalisme

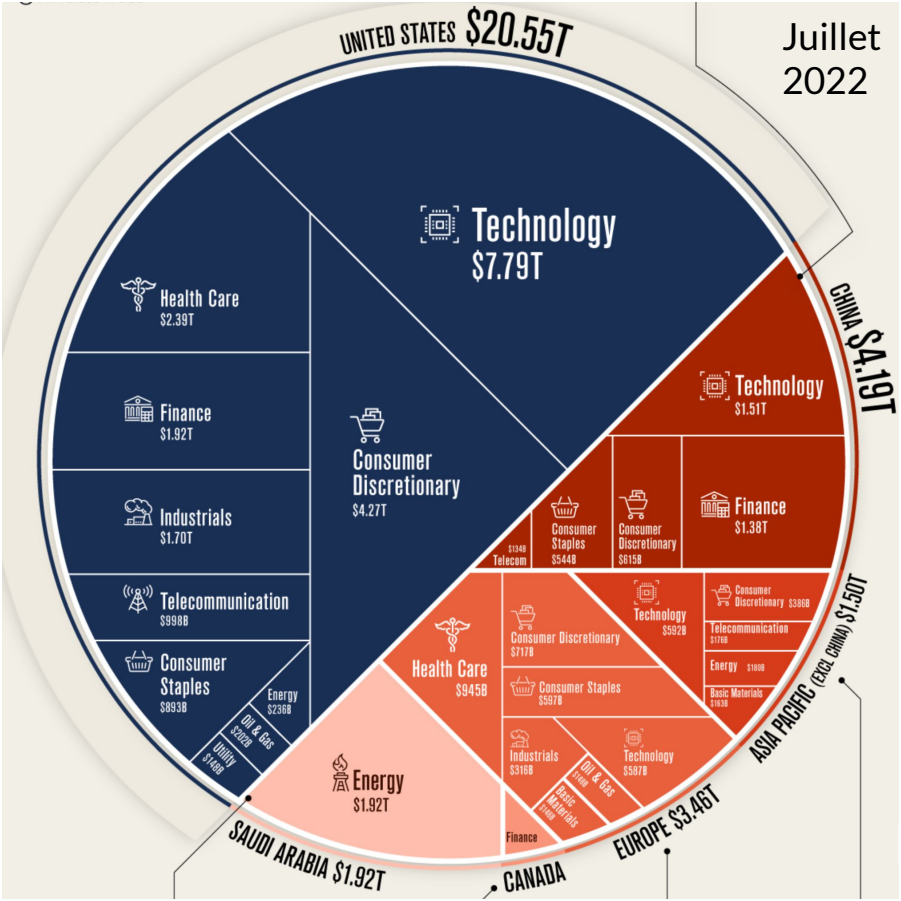
Le **capitalisme** est un système économique caractérisé par la propriété privée des moyens de production et la liberté de concurrence.

Ce qui compte → La possession du **capital**

Quelles sont les entreprises les plus valorisées au monde ?

1. Apple
2. Aramco
3. Microsoft
4. Alphabet (Google)
5. Amazon
6. Tesla
7. Berkshire Hathaway

Nov 2022



La Data, le nouvel or noir

> *"Information is the **oil** of the 21st century, and **analytics is the combustion engine.**" — Peter Sondergaard, 2011*

- 2,5 quintillion bytes of data every day (2018)
- 285 Milliards d'€ en 2015, en Europe 2% PIB

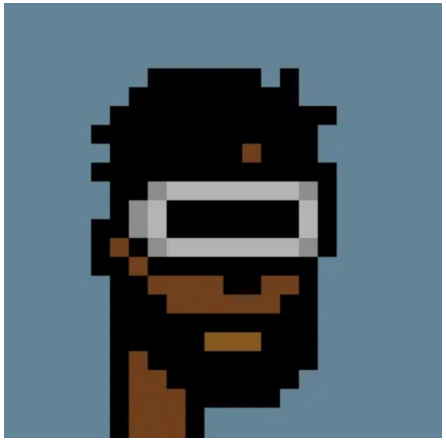
L'année 2015 [modifier | modifier le code]

- En juillet 2015, l'implication de Cambridge Analytica dans les primaires présidentielles du Parti républicain américain de 2016 est dévoilée[6].

« Sans Cambridge Analytica, il n'y aurait pas eu de Brexit[14]. »

Selon Wylie, Cambridge Analytica, dans le cadre du Brexit n'a pas agi seule : « sans AggregateIQ, le camp du 'Leave' n'aurait pas pu gagner le référendum, qui s'est joué à moins de 2 % des votes »[14, 17].

Cypherpunk



A **cypherpunk** is any individual advocating:

- cryptography
- privacy-enhancing technologies
- social and political change.

Originally communicating through the Cypherpunks electronic mailing list, informal groups aimed to achieve privacy and security through proactive use of cryptography. Since late 1980s.

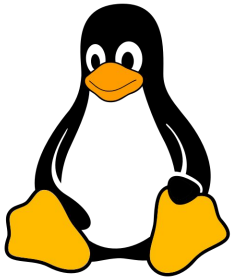
David Chaum

"Security without Identification: Transaction Systems to Make Big Brother Obsolete" (1985).

Le Crypto-Dream

A Cypherpunk's Manifesto

by Eric Hughes 1993



Nous ne pouvons pas nous attendre à ce que les gouvernements, les entreprises ou d'autres grandes organisations sans visage nous accordent la confidentialité par simple bienfaisance. C'est à leur avantage de parler à notre place, et nous devons nous attendre à ce qu'ils le fassent.

Nous, les Cypherpunks, sommes dédiés à la construction de systèmes anonymes. Nous **défendons notre vie privée** avec la cryptographie, avec des systèmes de transfert de courrier anonymes, avec des signatures numériques et avec de la monnaie électronique.

Les Cypherpunks **écrivent du code**. Nous savons que quelqu'un doit écrire un logiciel pour défendre la vie privée, et puisque nous ne pouvons pas obtenir la vie privée à moins que nous ne le fassions tous, nous allons l'écrire. Nous publions notre code afin que nos collègues Cypherpunks puissent s'entraîner et jouer avec. Notre **code est gratuit pour tous**, dans le monde entier.

cannot here selectively reveal myself; I must *always* reveal myself.

Therefore, privacy in an open society requires anonymous transaction systems. Until nc
system. An anonymous system empowers individuals to reveal their identity when desi

III. Houston, on a un problème

En quelle année à eu lieu le premier hack ?

Piratage du télégraphe Chappe

- Entre 1834 et 1836
- Louis et François Blanc

Lorsque la rente à 3 %, variation significative, colis codé à la station télégraphique de Tours : des chaussettes en cas de baisse et des gants en cas de hausse

1. Le directeur du télégraphe et son assistant répercutent l'information dans les dépêches corrigées.
2. Le message final est déchiffré par Pierre Renaud, qui loue une chambre avec une vue sur la Tour Chappe de Bordeaux6.

Le détournement a fonctionné parfaitement pendant deux ans, malgré des suspicions croissantes sur les succès boursiers des frères Blanc.

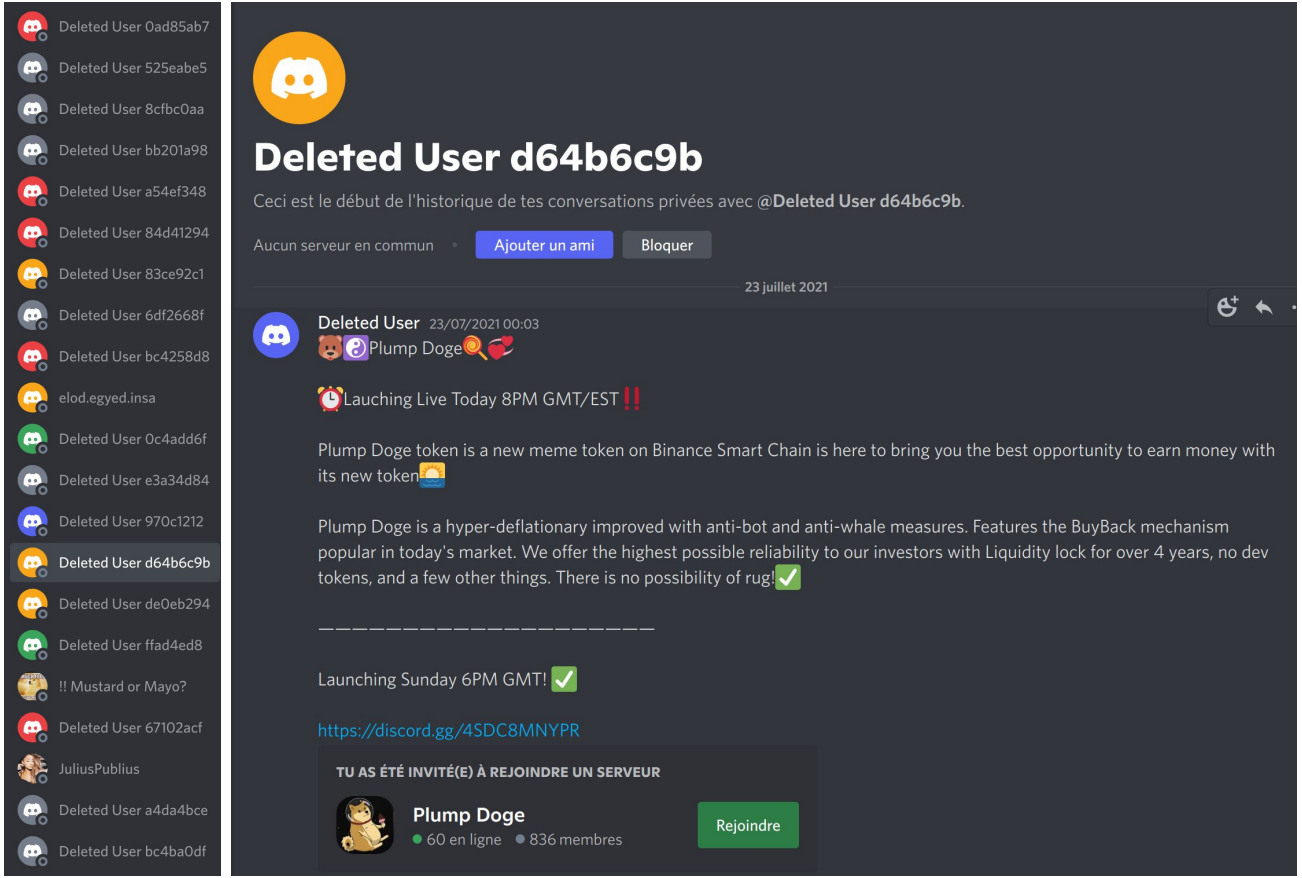
Du rêve au cauchemar

- Arnaques (ICO, Pump & dump)
- Spéculation
- Problèmes de sécurités
- Hacks
- Blanchiment d’argent

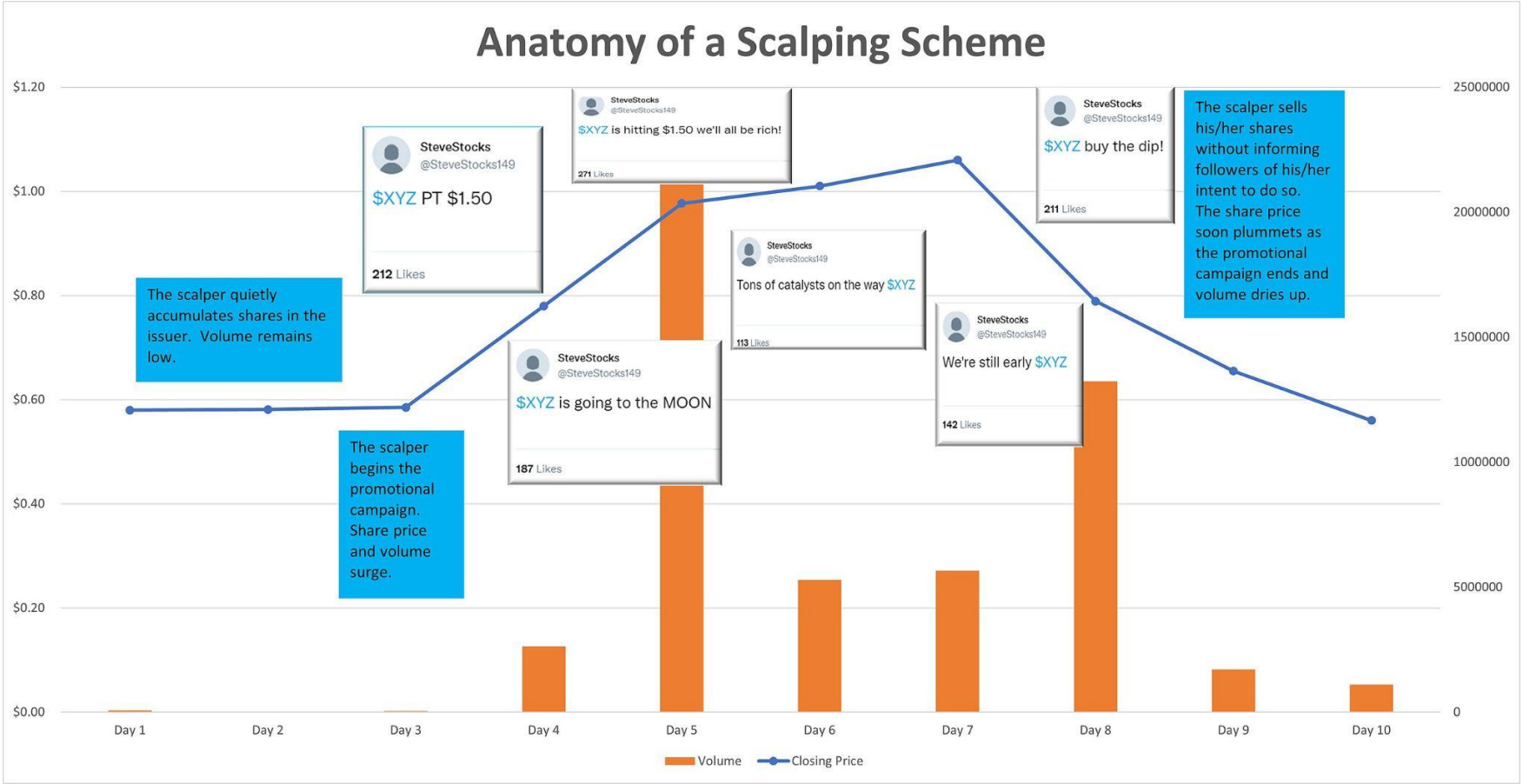
- Volatilité et non-régulation
- Évasion fiscale
- Pays sous embargo
- Cybercrime
- Pollution

Arnaques (ICO, Pump & dump)

Pump and dump (P&D) is a form of securities fraud that involves artificially inflating the price of an owned stock through false and misleading positive statements, in order to sell the cheaply purchased stock at a higher price. Once the operators of the scheme "dump" (sell) their overvalued shares, the price falls and investors lose their money.



Anatomy of a Scalping Scheme



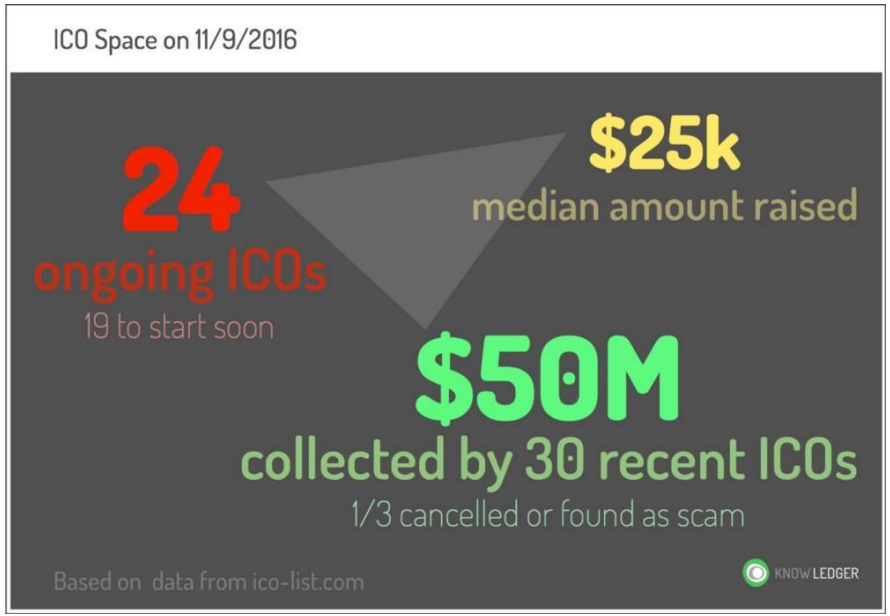
Effondrement

Chute de FTX 1Nov au 13Nov

Bloomberg à 16 milliards de dollars

1 semaine: 0

Samuel Bankman-Fried,
fondateur et PDG de FTX



La plate-forme, qui emploie 300 salariés, était considérée comme l'une des plus sûres du monde. Elle laisse sur le carreau quelque 100 000 clients ayant déposé leurs jetons électroniques et capitaux chez elle. Selon la presse américaine, Sam Bankman-Fried a tout simplement utilisé plus de la moitié des 16 milliards de dollars de capitaux déposés par ses clients pour financer sa propre société cryptofinancière Alameda, basée aux Bahamas. Selon le *Wall Street Journal*, Alameda, qui prenait des paris financiers extrêmement risqués, doit 10 milliards de dollars à FTX. Et au moins 1 milliard de dollars puisé dans les dépôts des clients a disparu, selon Reuters.

Hacks

Forb

CYBERSECURITY • EDITORS' PICK

North Korean Hackers Accused Of 'Biggest Cryptocurrency Theft Of 2020'—Their Heists Are Now Worth $1.75 Billion

rekt

1. **Ronin Network - REKT** *Unaudited*
   $624,000,000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
   $611,000,000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
   $586,000,000 | 10/06/2022
4. **SBF - MASK OFF** *N/A*
   $477,000,000 | 11/12/22
5. **Wormhole - REKT** *Neodyme*
   $326,000,000 | 02/02/2022
6. **BitMart - REKT** *N/A*
   $196,000,000 | 12/04/2021
7. **Nomad Bridge - REKT** *N/A*
   $190,000,000 | 08/01/2022
8. **Beanstalk - REKT** *Unaudited*
   $181,000,000 | 04/17/2022
9. **Wintermute - REKT 2** *N/A*
   $162,300,000 | 09/20/2022
10. **Compound - REKT** *Unaudited*
    $147,000,000 | 09/29/2021

Minage, pollution et contournements

FRANCE 24 LES OBSERVATEURS — La une | Emissions | Actualités | Contribuer

/ Moyen-Orient

ENQUÊTE

Enquête : en Iran, des pannes de courant monstres révèlent le business des fermes à bitcoins chinoises

Publié le : 01/02/2021 - 19:14

En haut, une ferme à bitcoins sur le sol iranien. En bas, une enquête par géolocalisation menée par la rédaction des Observateurs a révélé la présence de ces fermes en Iran. © Google Earth

PLANETE > ACTUALITÉS

Une transaction en bitcoin génère autant de déchets électroniques que la fabrication de deux iPhone

POLLUTION | CRYPTOMONNAIE | ENVIRONNEMENT — ACTUALITÉ · 2 MIN

GLOBAL CITIZEN — THÈMES | PASSEZ À L'ACTION | RÉCOMPENSES | PARTENAIRES | STORE | FRANÇ

ACTU — DÉFENDRE LA PLANÈTE

Bitcoin Is Massively Polluting the Earth — And We Should All Be Scared

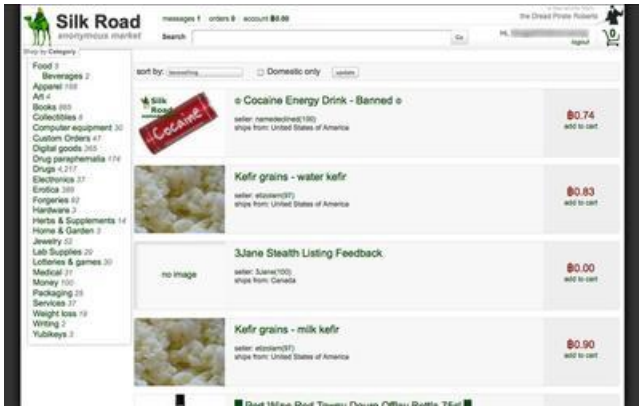
The digital currency uses as much energy as 28 million US household per year.

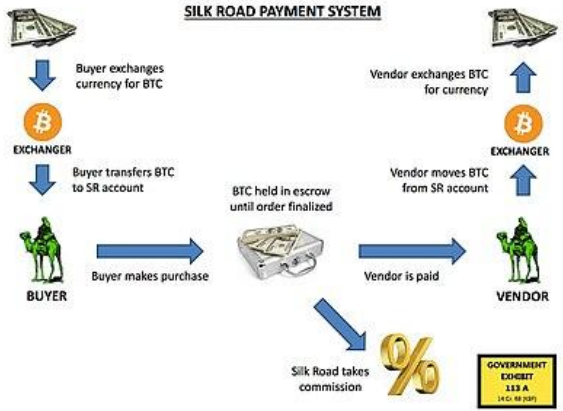
Terrorisme & trafiques

Financing terrorism through cryptocurrencies – a danger for Europe?

October 2018 · Journal of Money Laundering Control 21(2):00-00
DOI: 10.1108/JMLC-06-2017-0024

Fabian Maximilian Johannes Teichmann





Conclusion

- Le rêve d’un monde anonyme
- Echec de la sécurité
- Echec de l’Accessibilité
- Avenir incertain
- Est-ce encore souhaitable ?


merci de votre attention
> Questions ?