Introduction aux Blockchains : fonctionnement et usages

Alexis Direr

3 juin 2023

Plan de la leçon

Qu'est-ce qu'une blockchain ?

Une technologie de stockage et de transmission d'informations sécurisée et sans autorité centrale (Wikipedia).

Une base de données distribuée enregistrant l'ensemble des transferts de propriété et opérations liées à un (ou plusieurs) *crypto-actif(s)*.

Qu'est-ce qu'un crypto-actif ?

Une représentation digitale d'une valeur ou d'un droit inscrit sur une blockchain et transférable de compte à compte.

▷ des unités associées à des comptes sur un registre en ligne

▷ protégées par des techniques cryptographiques de la contrefaçon, du vol, la duplication, la suppression

→ différent des objets digitaux stockés sur un ordinateur ou en ligne comme un article, des fichiers musicaux, vidéos, ... : modifiables, altérables, duplicables, ...

Une base de donnée particulière

Accès à la base :

▷ en lecture : libre. Chacun a accès sans permission à l'ensemble de la base et son historique complet.

▷ en écriture : strictement encadré par des règles de consensus, payant pour les utilisateurs

▷ en modification/effacement : impossible. Une fois qu'une transaction est validée par le réseau, elle ne peut plus être modifiée ou effacée.

Un système décentralisée

Système dans lequel un comportement complexe émerge grâce aux interactions de composants de niveau inférieur opérant sur des informations locales, et non sur les instructions d'un contrôleur central.

Blockchains : pas d'autorité centrale contrôlant le système. Les décisions sont issues d'un consensus entre les noeuds informatiques d'un réseau.

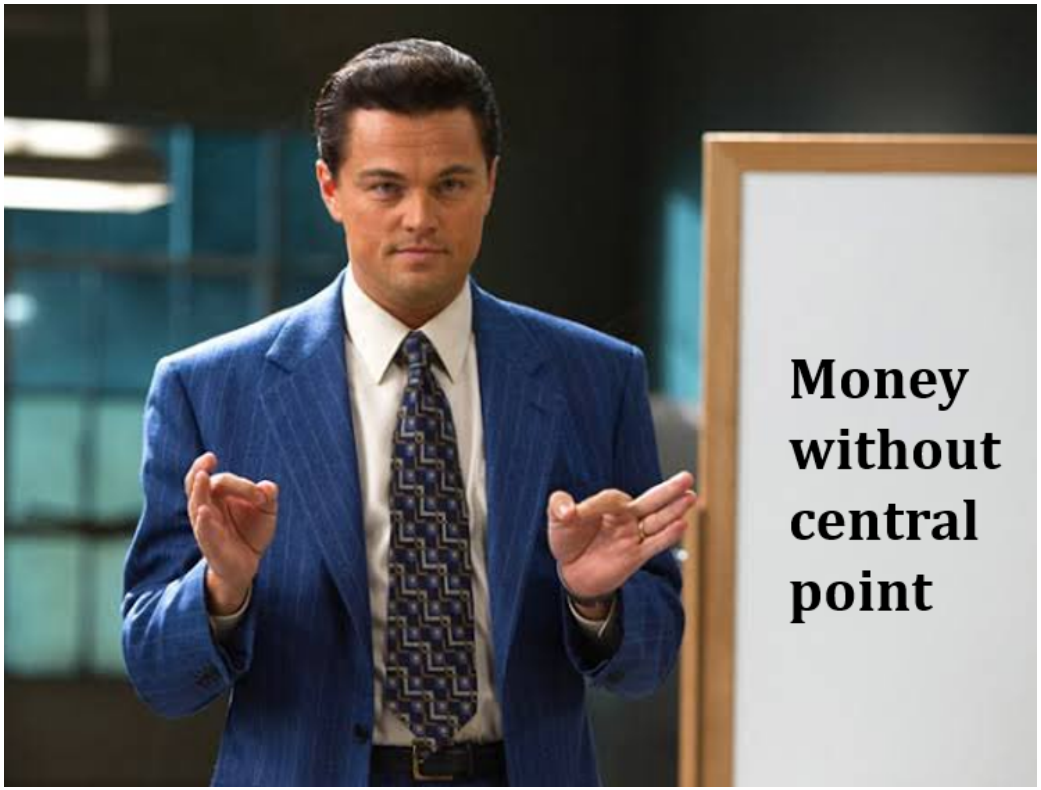
Internet : une structure composée de millions d'appareils reliés entre eux dans un réseau ouvert empêche qu'un acteur se l'approprie, la contrôle, en limite l'accès ou la débranche.

Autres exemples :

- le langage, les normes sociales (consensus)
- les vols d'étourneaux suivent un algorithme local :
  - se déplace vers ses semblables
  - en évitant éviter de s'écraser sur d'autres oiseaux
  - se déplace dans la même direction que les autres oiseaux
- un réseau de noeuds bitcoin suit aussi un algorithme local :
  - valident les transactions reçues
  - transmettent les transactions valides aux autres noeuds
  - valident les blocs reçus, ...

Intérêts de la décentralisation

Des actifs sans intermédiaires pour les créer, sécuriser, et déplacer.



Intérêts des blockchains décentralisées :

→ Pas de dépendance vis à vis de tiers (banque, fonds d'investissement, ...)

→ résistance à la collusion entre les noeuds

→ résistance aux attaques et à la censure

De plus, chaque noeud conserve une copie de la blockchain

→ tolérance aux pannes et la suppression d'une partie du réseau (V. Buterin)

La blockchain : un système à l'échelle mondiale, ouvert et sans permission

→ La responsabilisation (*empowerment*) des usagers

Internet : appropriation du savoir :

- médical
- juridique
- financier, ...

Blockchains : appropriation de la valeur (souveraineté monétaire)

⟶ propriété digitale sans intermédiaires et tiers de confiance

Une infrastructure publique

Réseau Internet : protocole informatique décentralisé permettant de transférer des paquets de données d'un serveur à des clients distants.

$\longrightarrow$ chacun peut accéder à Internet, lire son contenu, créer un site, interagir avec une application, ...

Blockchain : protocole informatique décentralisé permettant de transférer de la valeur sans tiers de confiance (Balaji)

$\longrightarrow$ chacun peut accéder à une blockchain, lire son contenu, créer un compte ou déployer une application, transmettre des unités d'un compte à un autre, interagir avec une application, ...

Autres infrastructure publique : routes, ponts, ports, réseaux ferroviaires, réseaux de fibre optique, ...

Trois propriétés des infrastructures publiques

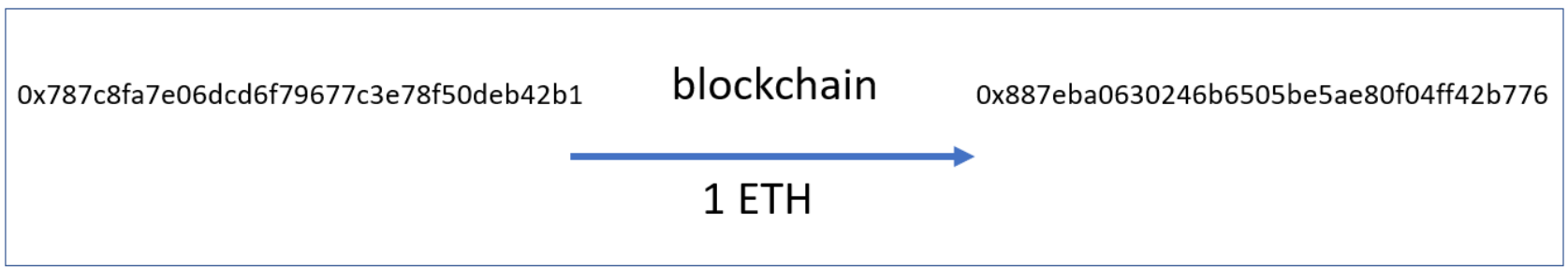
▷ coûteux à construire, mais une fois construite, le coût d'usage est très bas.

▷ ... mais peut augmenter rapidement en cas de congestion (problèmes de scalabilité)

▷ Effets de réseau : l'utilité d'une technique ou d'un produit s'accroît avec le nombre de ses utilisateurs.

Un registre transparent et pseudonymisé

Banques vs blockchain :



Une transaction sur Ethereum :

From:	0x4EB558e421Efa555Ca9D16eDC51f90FcE477bDcE
To:	0xE2F7fe0a7DF14b51D0FE2f7e8AC970a1D03DC3e4
Value:	0.7877033174757864 37 ETH ($1,476.57)
Transaction Fee:	0.000453243007644 ETH ($0.85)
Gas Price:	21.583000364 Gwei (0.000000021583000364 ETH)

source

Quelques explorateurs de blockchains :

- Bitcoin : Blockstream.info
- Ethereum : Etherscan
- Polygon : Polygonscan
- Tron : Tronscan
- Ripple : Xrpscan

Un pseudonymat revendiqué

Le mouvement cypherpunks préconise l'utilisation généralisée de la cryptographie comme moyen de protection de la vie privée.

Manifeste des cypherpunks (9 March 1993) :

> *Le respect de la vie privée est nécessaire pour une société ouverte à l'ère électronique. La vie privée n'est pas le secret (...) [Elle] est le pouvoir de se révéler au monde de manière sélective. (...)*
> *Lorsque mon identité est révélée par le mécanisme sous-jacent de la transaction, (...) je ne peux pas me révéler de manière sélective ; je dois toujours me révéler.*

Réf : Liste de diffusion, post

Extrait du white paper de Satoshi Nakamoto :

> *La nécessité de publier toutes les transactions interdit [la confidentialité des transaction], mais celle-ci peut encore être maintenue (...) en gardant les clés publiques anonymes. Le public peut voir que quelqu'un envoie un montant à quelqu'un d'autre, mais sans information permettant de relier la transaction à qui que ce soit.*

Les six propriétés de la blockchain

1) Transmission pair à pair, absence d'intermédiaires (décentralisation)

2) Transparence du code et des transactions (traçabilité, provenance)

3) Libre accès et utilisation (marché mondial par défaut)

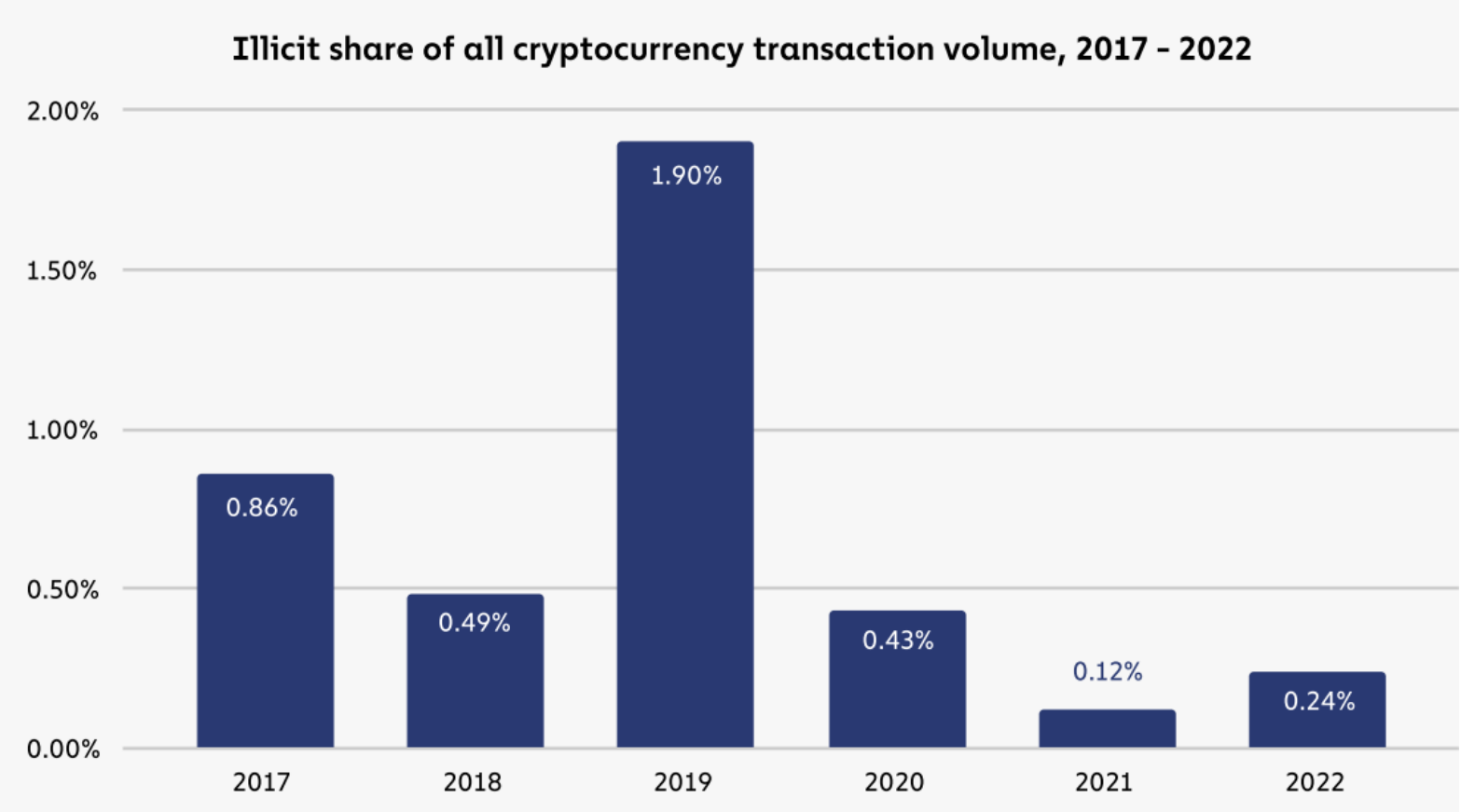
4) Immuabilité des transactions (sécurité des échanges)

5) Pseudonymat (*privacy*)

6) Certification (propriété, transactions, identités)

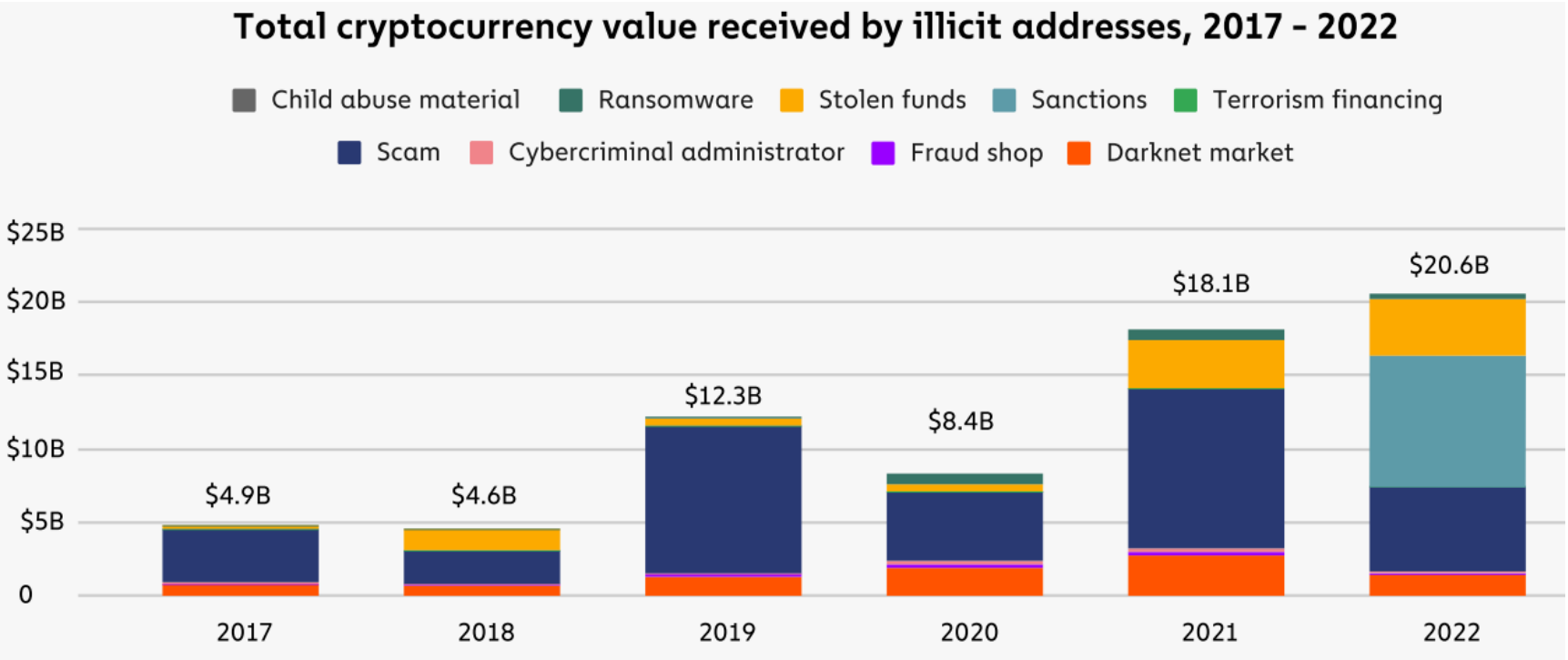
Critiques adressées aux blockchains

- Argent des criminels (pseudonymat et décentralisation)
- Dépenses d'énergie (preuve de travail)


Illicit share of all cryptocurrency transaction volume, 2017 - 2022
2.00%
1.50%
1.00%
0.50%
0.00%
0.86%
0.49%
1.90%
0.43%
0.12%
0.24%
2017
2018
2019
2020
2021
2022

source

Décomposition des échanges illicites



source

Les mesures contre le blanchiment et FT sur les blockchains

Le Groupe d'action financière (GAFI, *FATF*) : organisation intergouvernementale qui élabore et promeut des politiques pour lutter contre le blanchiment d'argent et le financement du terrorisme

Le GAFI a émis des recommandations vis à vis des prestataires de services liés aux actifs virtuels (VASP).

VASP : entreprises ou entités qui offrent des services liés à l'achat, la vente, le transfert, l'échange, la gestion ou la garde de cryptoactifs.

Recommandations du GAFI vis à vis des VASP :

- Identification et vérification des clients (KYC)
- Surveillance et déclaration des transactions suspectes
- Conservation des registres de toutes les transactions effectuées sur leur plateforme, pendant une période minimale

Règle du voyage : (*travel rule*) : si Pierre envoie des cryptoactifs de son wallet sur le compte Coinbase de Jacques, Coinbase doit vérifier l'identité de Jack mais aussi de Pierre.

Transactions concernées :

plateforme centralisée $\leftrightarrow$ plateforme centralisée

plateforme centralisée $\leftrightarrow$ wallet

Quels flux estimés de l'argent du crime au niveau mondial ?

▷ Entre 800 et 2 000 milliards de dollars / an, soit environ 2 à 5 % du PIB mondial (Office des Nations Unies contre la drogue et le crime)

▷ 3 % du PIB mondial (1 200 $ b) selon le Groupe d'action financière (GAFI), une organisation intergouvernementale chargée de lutter contre le blanchiment d'argent et le financement du terrorisme

$\longrightarrow$ flux crypto $\approx$ 1,5 % des flux totaux

source : 1, 2, 3, 4

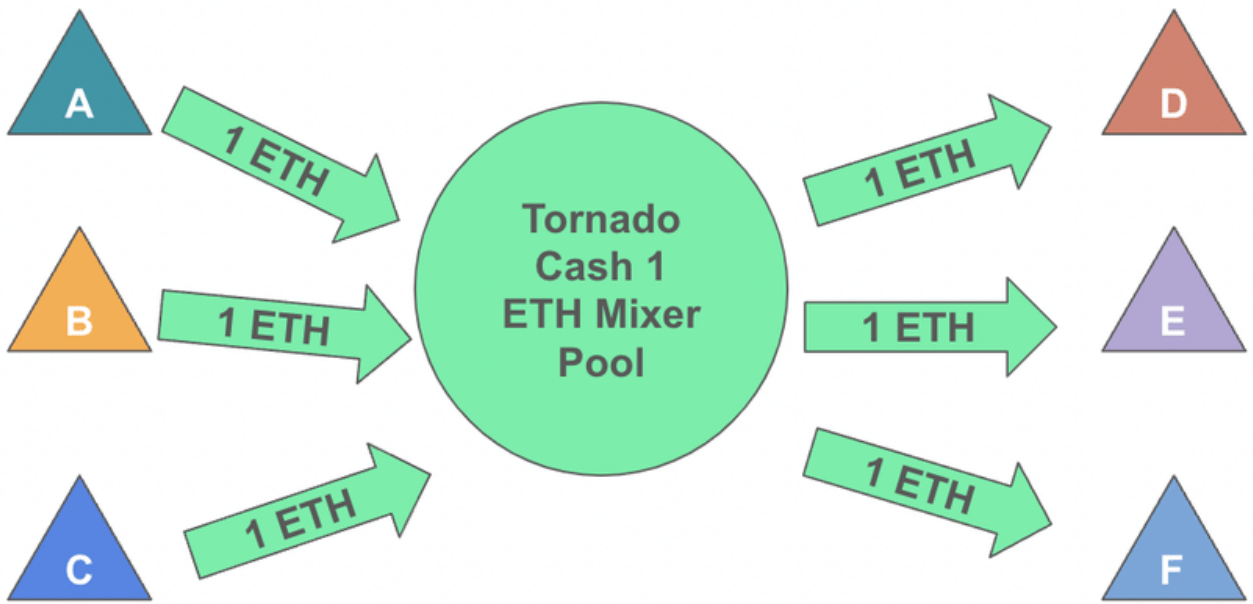
Principaux acteurs et adresses blockchains sanctionnés par l'OFAC (*Office of Foreign Assets Control*), l'agence du département du Trésor, en 2022 :

- Garantex, une plateforme d'échange russe
- Hydra, Place de marché sur le draknet (fermée en 2023)
- Blender.io et Tornado Cash, deux mixeurs de cryptoactifs
- Groupe Lazarus, un groupe de cyberhackers financés par la Corée du Nord

▷ *considérés comme des menaces pour la sécurité nationale et la politique étrangère des États-Unis*

source : 1

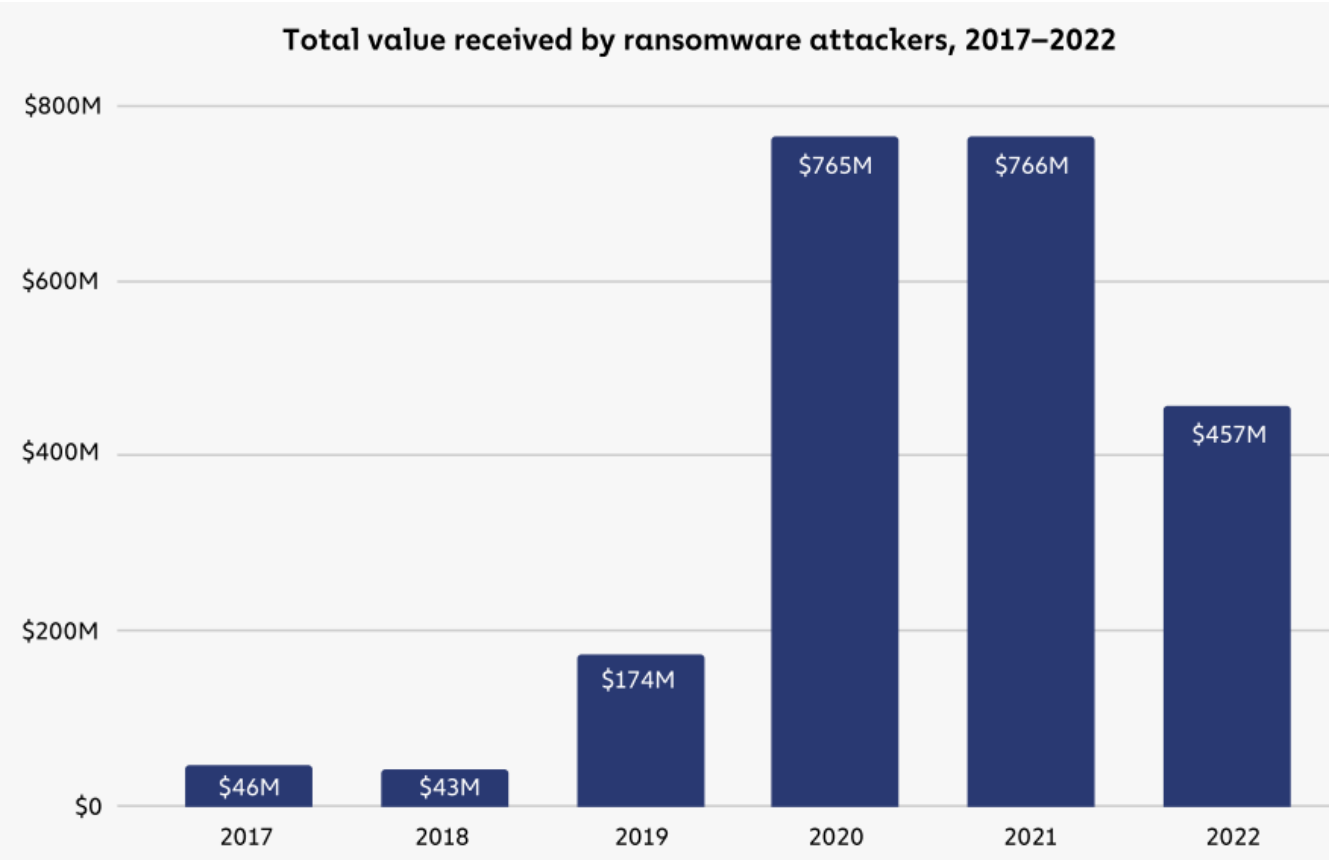
Mixeur : service dissimuler la provenance des fonds des utilisateurs en rompant le lien entre l'expéditeur et le destinataire des transactions.



$\longrightarrow$ préserve la confidentialité et l'anonymat des utilisateurs.

sources : 1, 2

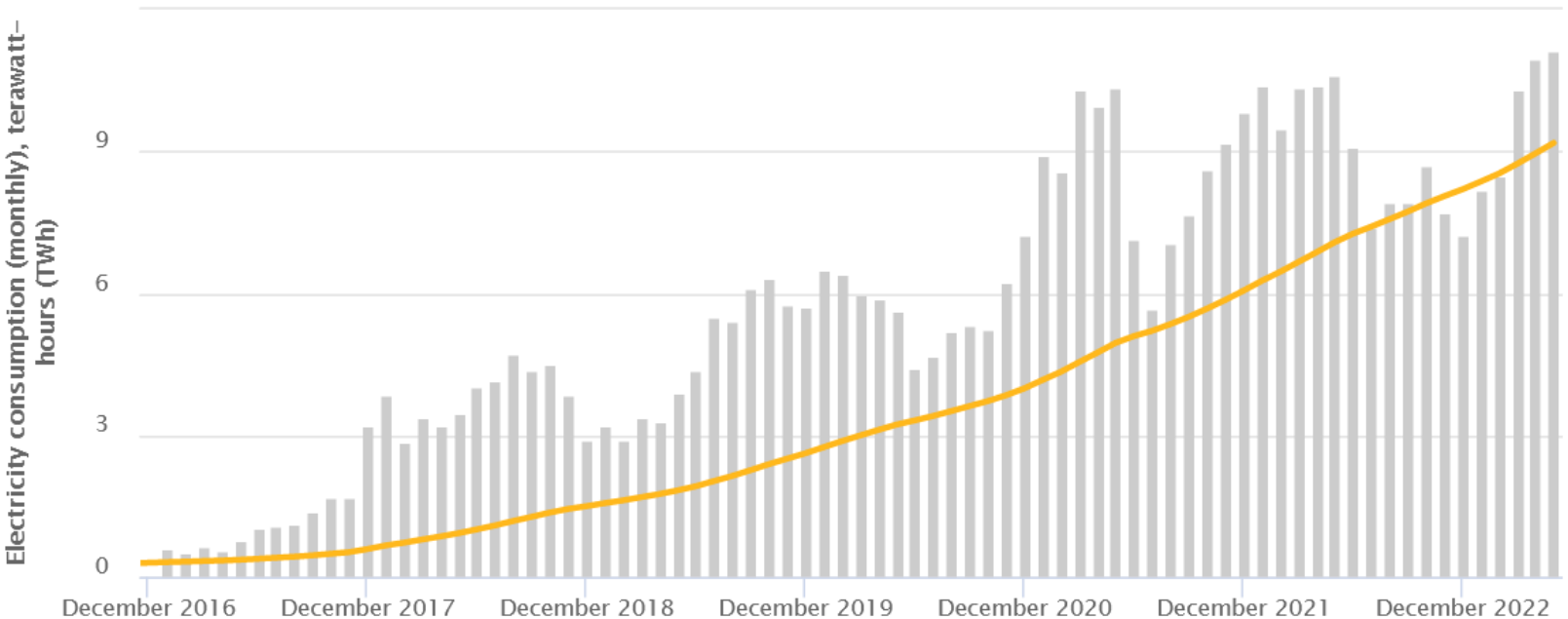
Valeur reçues par les attaquants par ransomware



sources : 1, 2

Dépenses d'énergie

Consommation d'électricité de Bitcoin



source

Comparaisons

Electricity

Production

26 730 TWh

Consumption

22 315 TWh

Bitcoin share

0.64%

Energy

Production

167 716 TWh

Bitcoin share*

0.22%

Gold mining

131

TWh per year

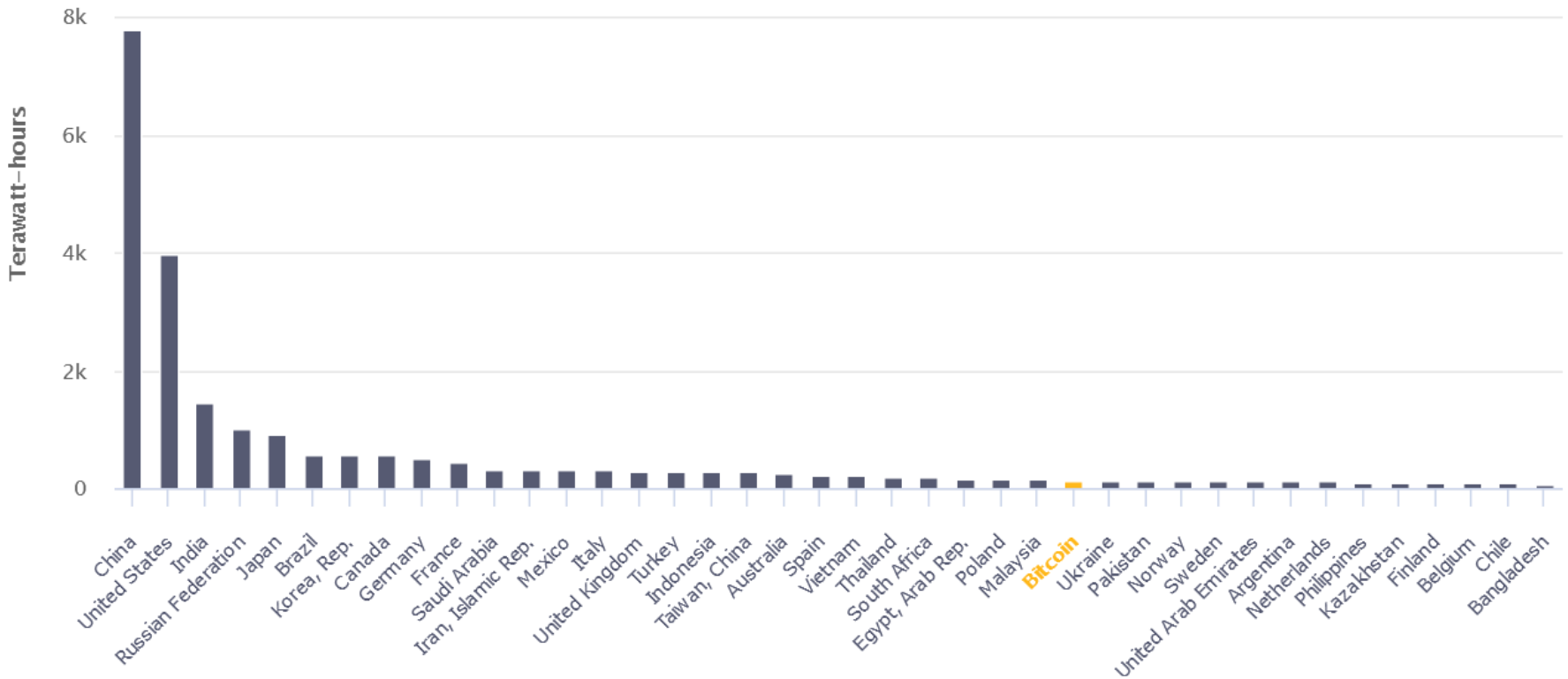
Bitcoin

141.89

TWh per year

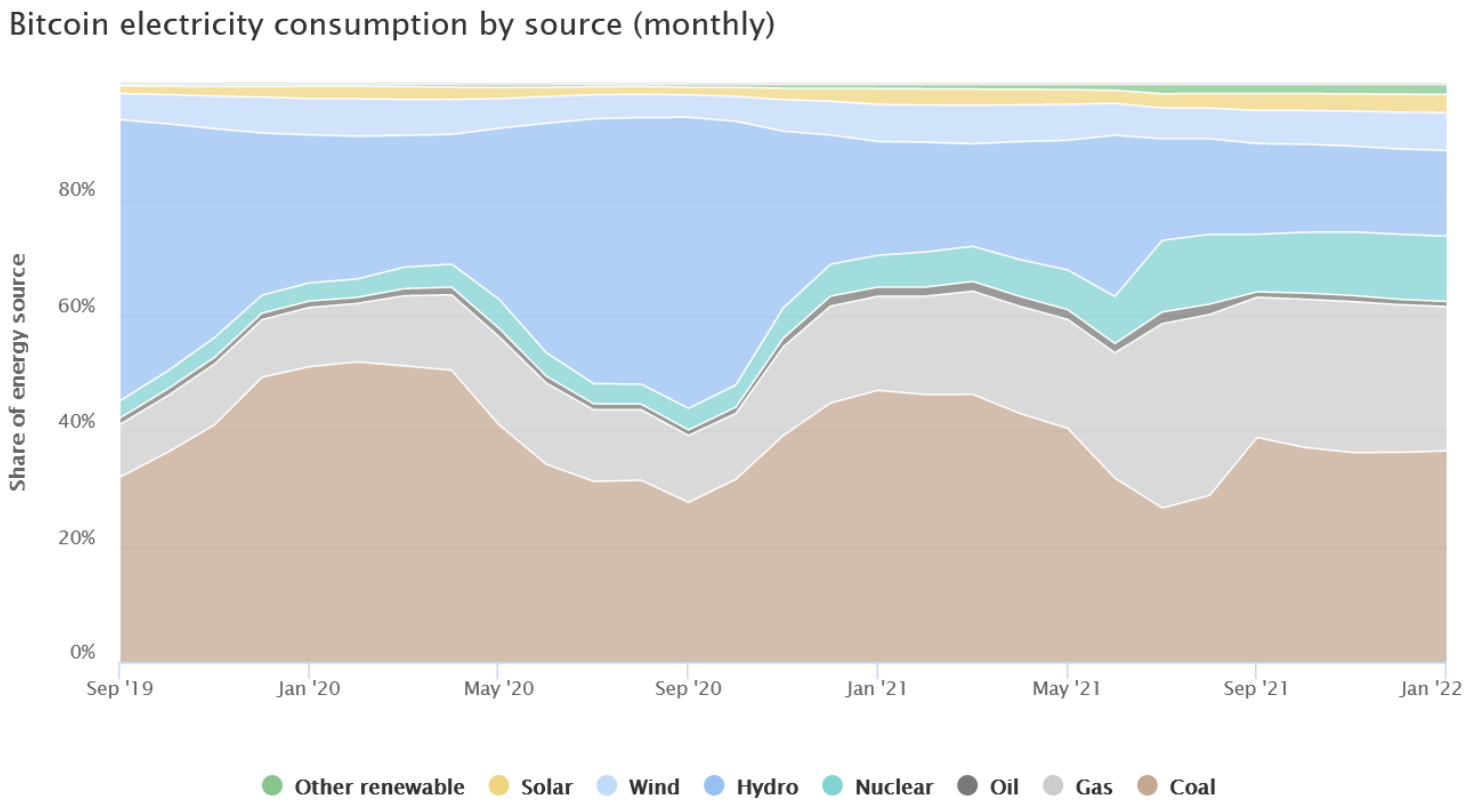
source

Comparaisons internationales



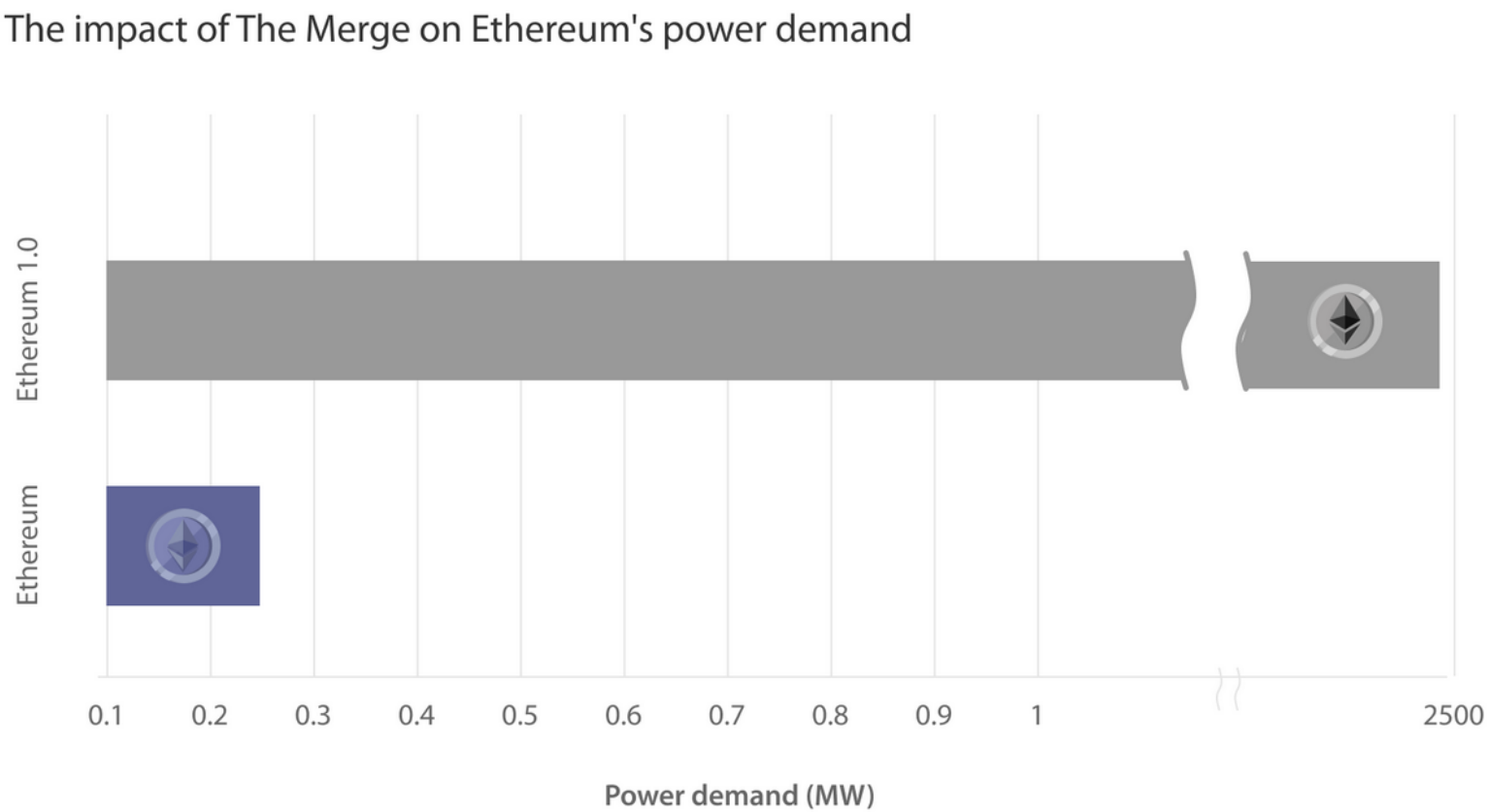
source

Mixte énergétique : 25 % d'énergies renouvelables



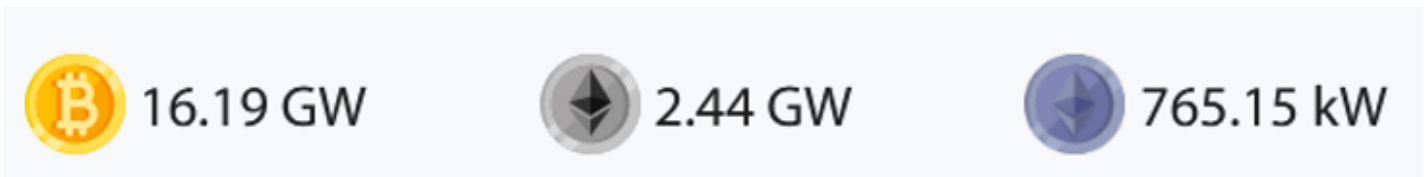
sources : 1, 2, 3

Ethereum : dépenses d'énergie avant et après le passage en preuves d'enjeu (*the merge*)



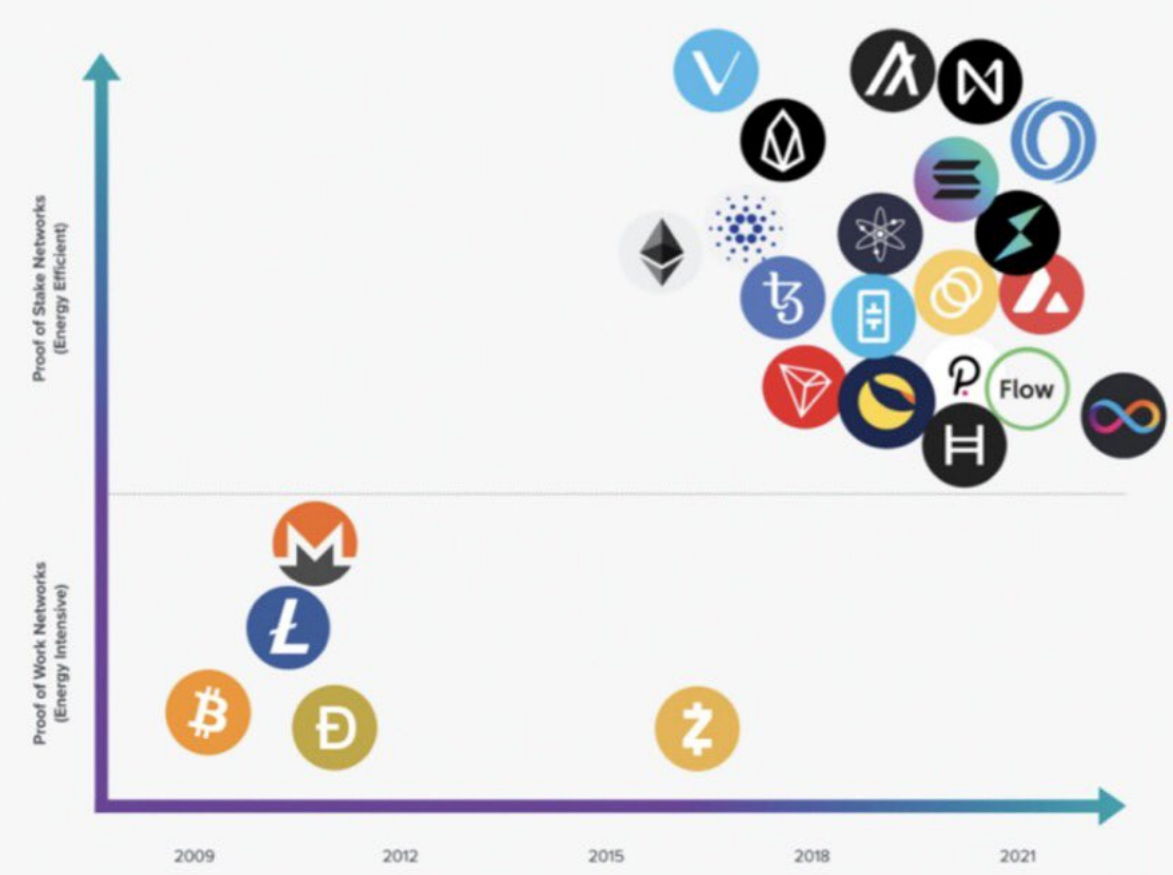
source

Comparaison Bitcoin vs. Ethereum avant et après la transition vers la preuve d'enjeux



source

Prédominance des blockchains à preuve d'enjeu

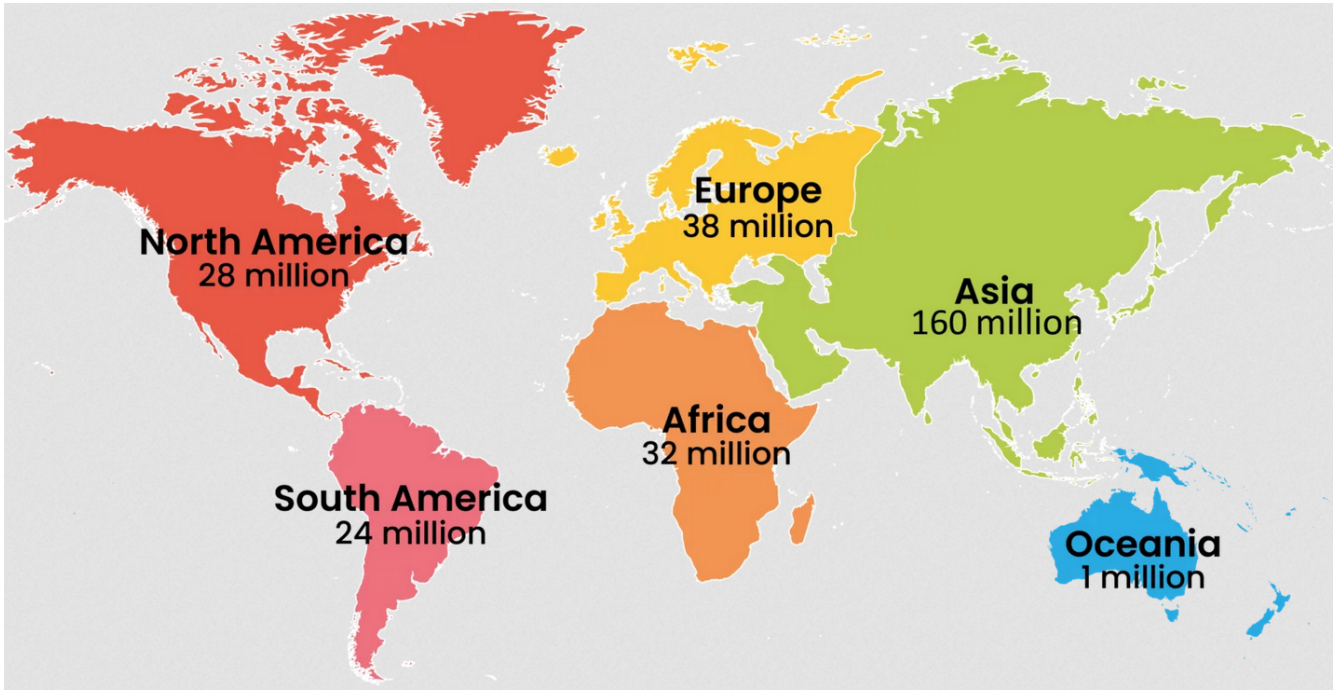


source

Statistiques d'adoption

- ▷ Quelle part de la population mondiale détient des cryptoactifs ?
- ▷ Comparaison avec Internet
- ▷ Comparaison pays à revenus élevés vs. moyens et bas
- ▷ Exemple de l'Argentine, les E-U et la France

320 millions d'utilisateurs dans le monde (entre 4 et 8 % de la population mondiale)



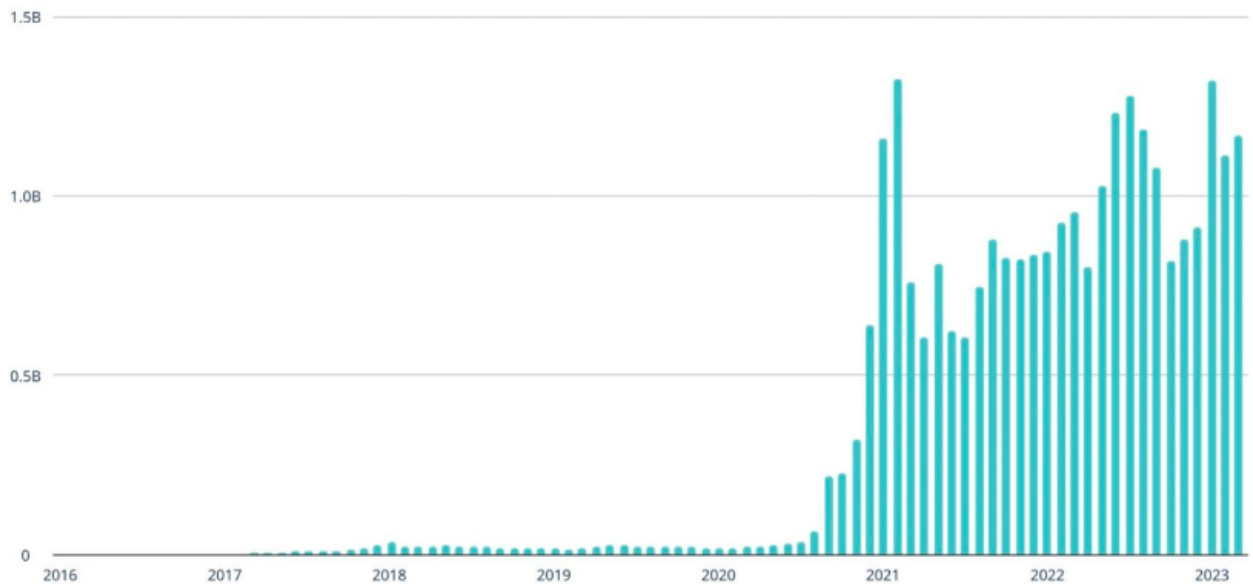
Inde (100 million), EU (27 million), Nigeria (13 million), Vietnam (6 million), GB (3.3 million)

Source : 1, 2

1 milliards de transactions chaque mois

Transactions

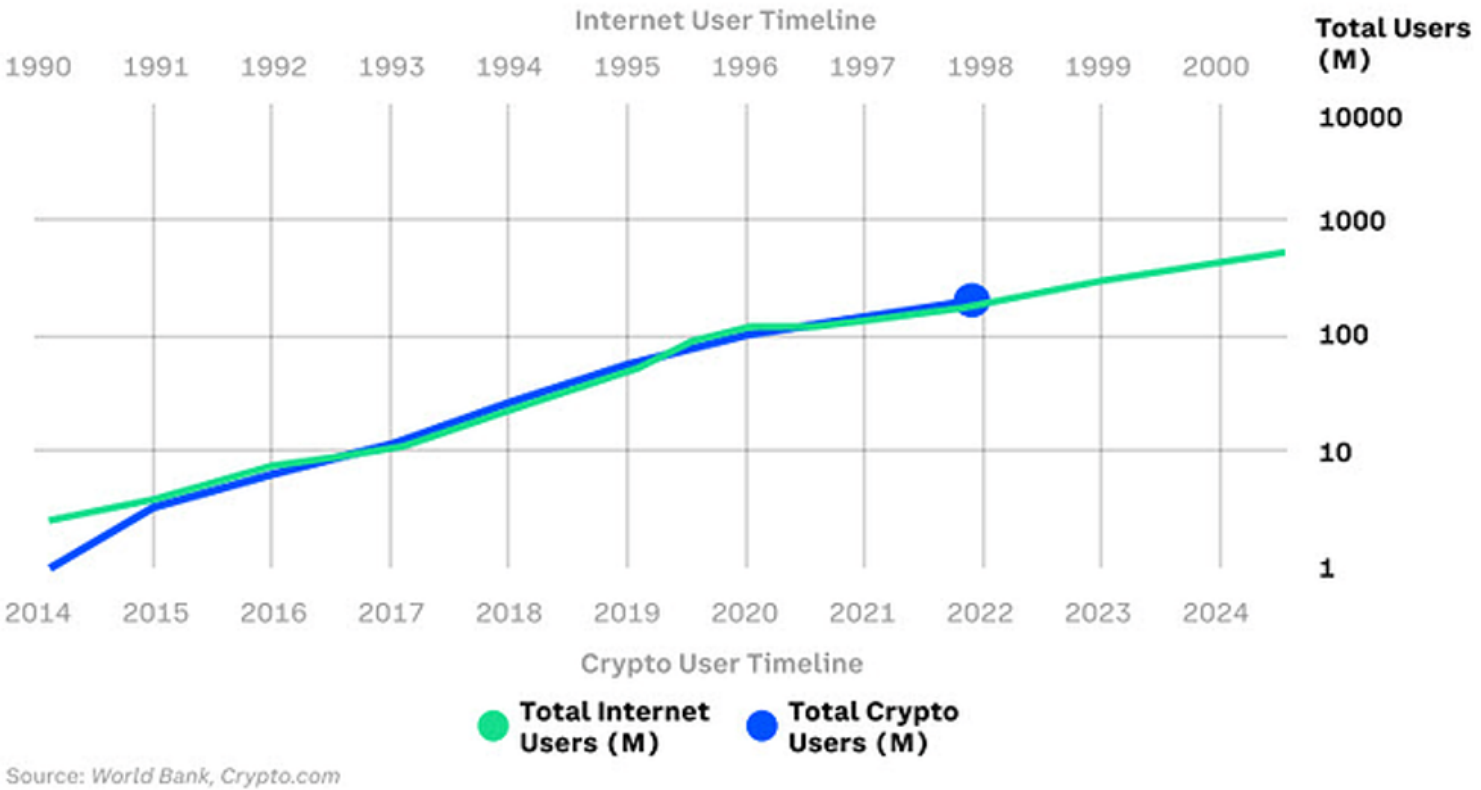
Number of successful transactions across all tracked blockchains during the month.



Source: Nansen Query. Tracked blockchains include Ethereum, Polygon, Solana, Avalanche, Fantom, Celo, Optimism, and Arbitrum.

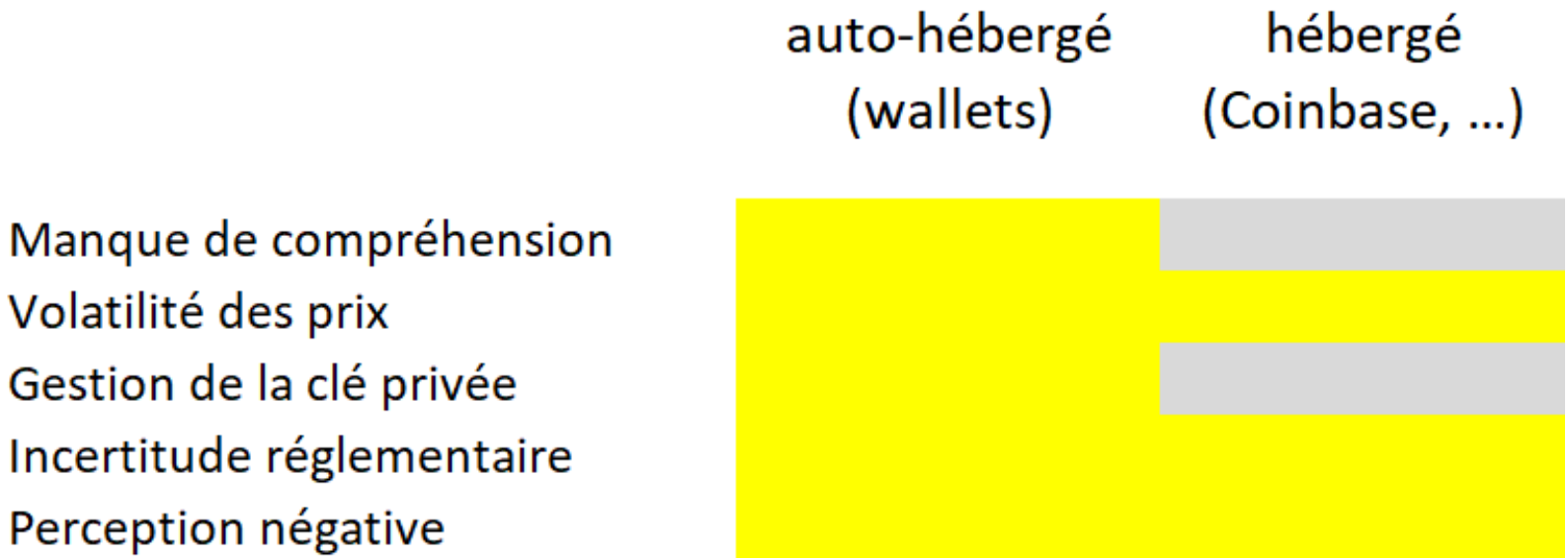
Source : A16z

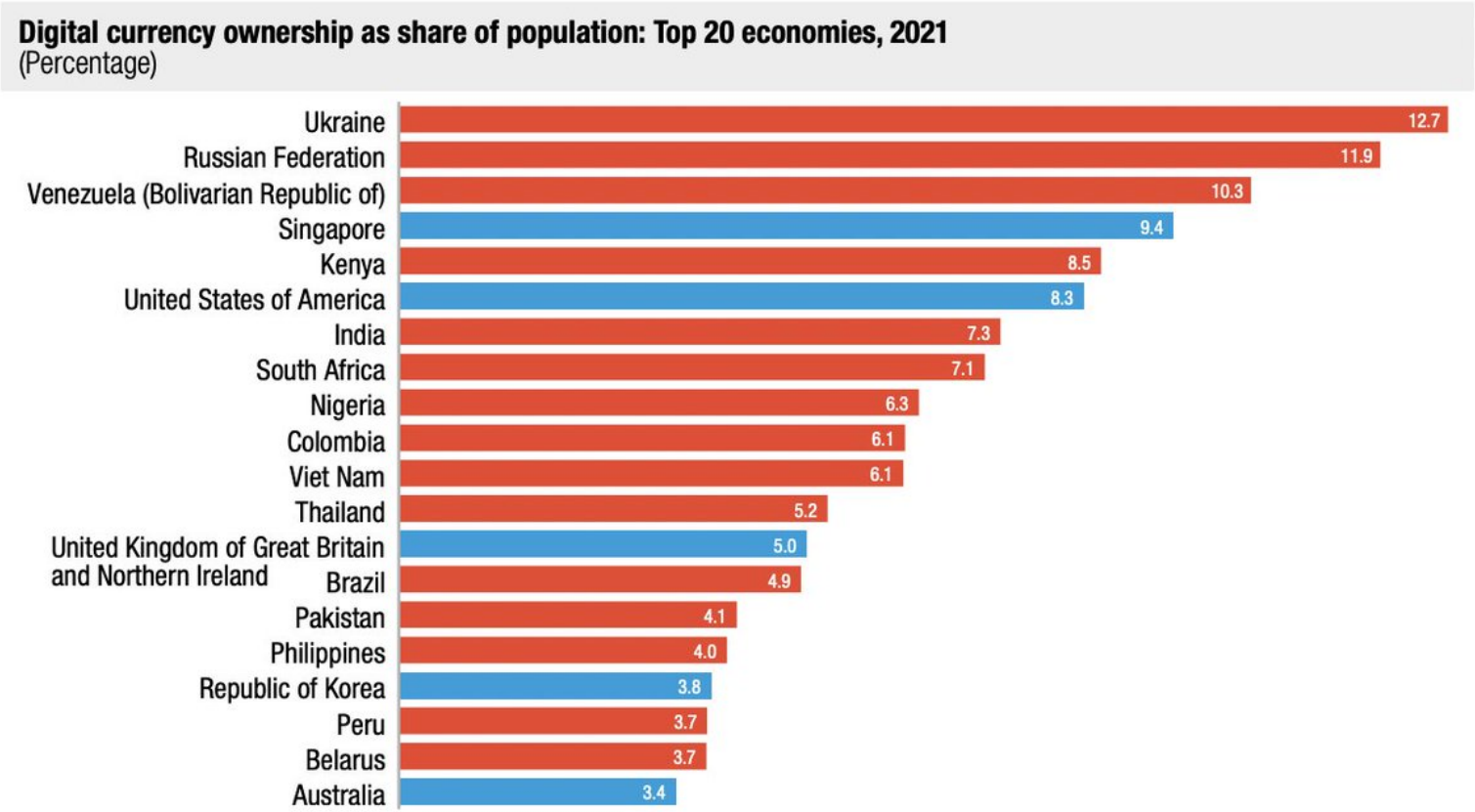
Adoption d'Internet vs. des cryptoactifs



Source

Facteurs de freins en matière d'adoption, selon que le compte est :




Digital currency ownership as share of population: Top 20 economies, 2021
(Percentage)
Ukraine 12.7
Russian Federation 11.9
Venezuela (Bolivarian Republic of) 10.3
Singapore 9.4
Kenya 8.5
United States of America 8.3
India 7.3
South Africa 7.1
Nigeria 6.3
Colombia 6.1
Viet Nam 6.1
Thailand 5.2
United Kingdom of Great Britain and Northern Ireland 5.0
Brazil 4.9
Pakistan 4.1
Philippines 4.0
Republic of Korea 3.8
Peru 3.7
Belarus 3.7
Australia 3.4
Source: UNCTAD, based on data from https://triple-a.io/crypto-ownership/.
Note: The classification of economies (blue, advanced economies; red, emerging and market economies) is based on that in International Monteray Fund, 2020, World Economic Outlook: A Long and Difficult Ascent (Washington, D.C.).

Source

Country (currency)	% Likely to purchase cryptocurrency within next year (base: non-owners)	% devaluation against USD 2011-2021
Norway (NOK)	3%	46.43%
Denmark (DKK)	4%	16.67%
Hong Kong (HKD)	5%	0.00%
Australia (AUD)	6%	-25.00%
Singapore (SGD)	7%	8.33%
France (EUR)	8%	-14.29%
UK (GBP)	8%	0.00%
Ireland (EUR)	9%	-14.29%
Germany (EUR)	11%	-14.29%
South Africa (ZAR)	32%	102.74%
Mexico (MXN)	32%	63.71%
India (INR)	40%	58.58%
Brazil (BRL)	45%	217.65%

Source : Gemini

L'exemple de l'Argentine

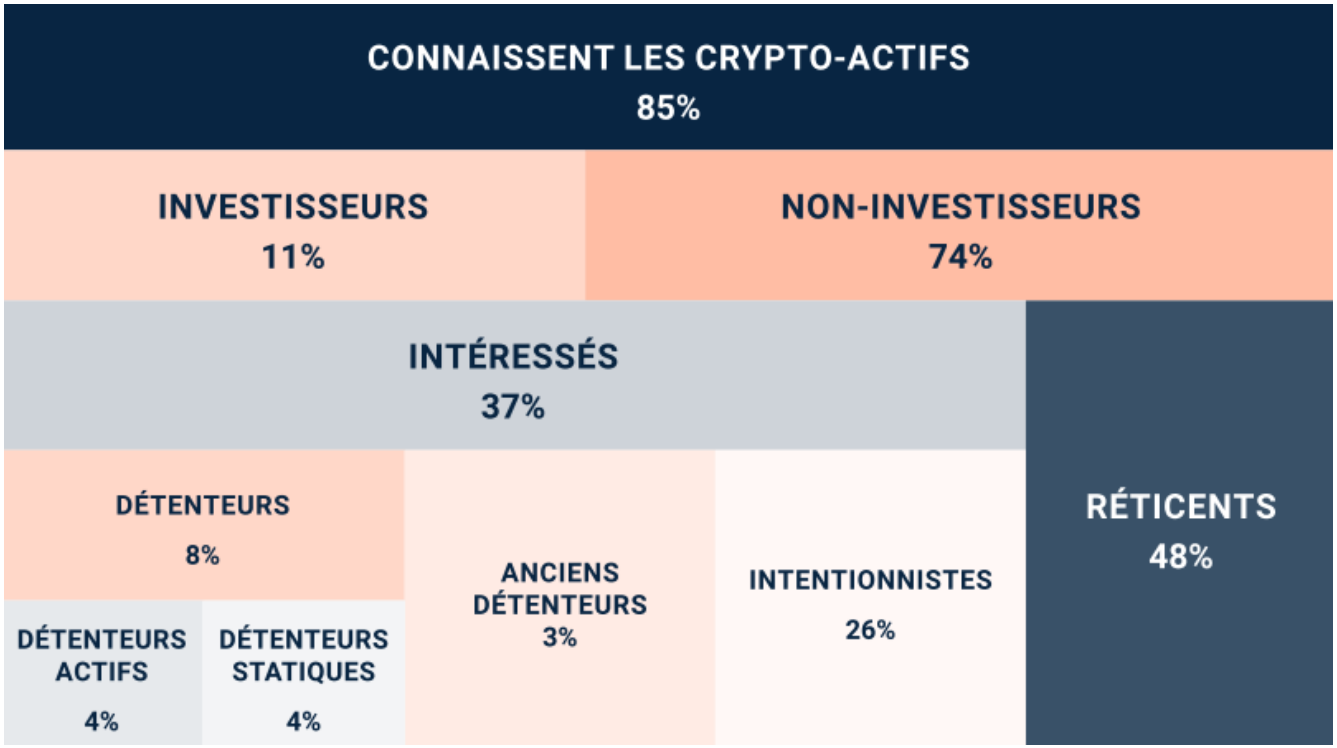
▷ 100 % d'inflation en 2022, forte défiance vis à vis de la monnaie nationale et du système bancaire (gel des avoirs en 2001 (*corralito*)), dollarisation rampante de l'économie.

source


Level of Cryptocurrency Adoption in Argentina
1 in 4
respondents buy cryptocurrencies
frequently
25-39
44% of crypto buyers in Argentina included in this survey are in this age range
Crypto buyers Argentina*
66% are men, the highest percentage in Latin America
34% of crypto buyers are women
Gender gap:
AMI estimates show the number of women saying they "don't know much" is 4 times higher than the men saying the same.

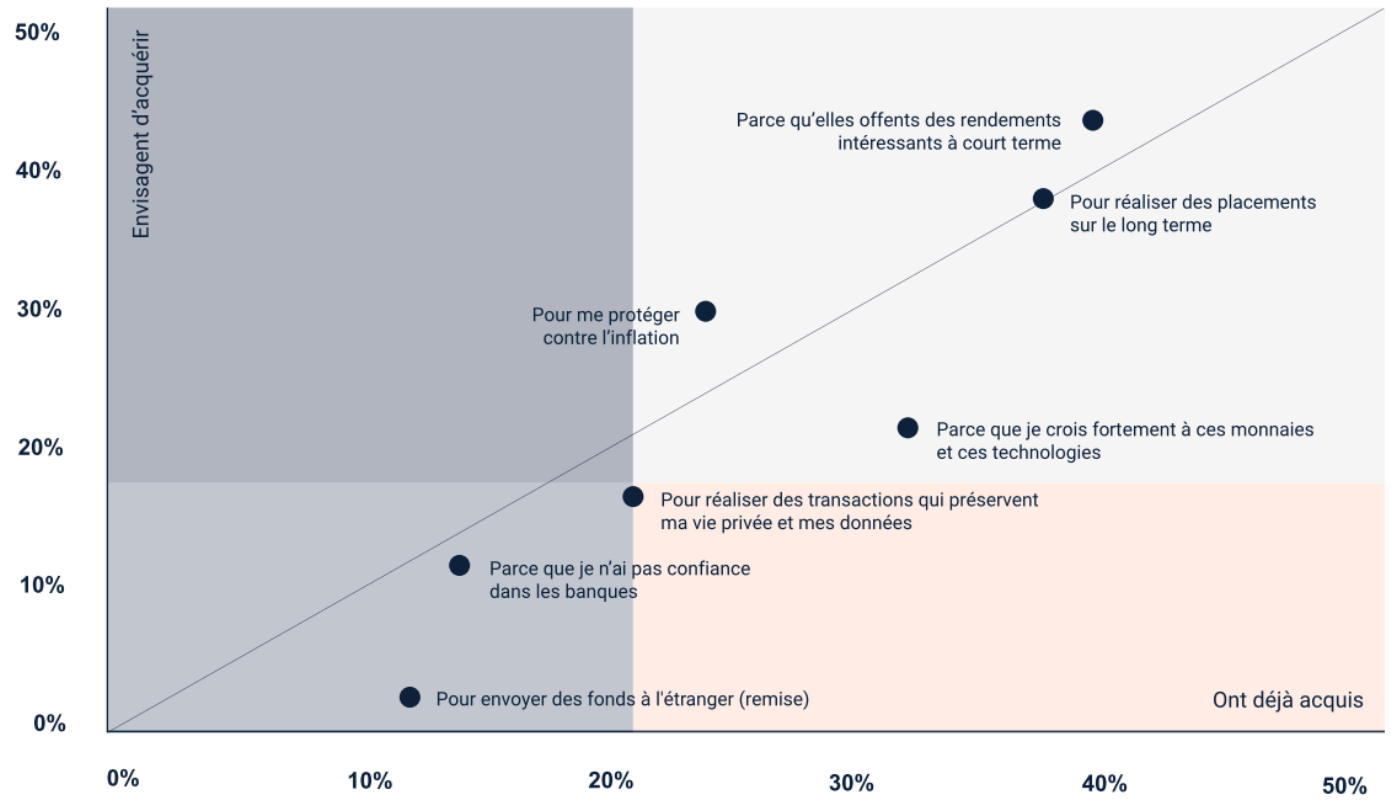
sources : 1, 2

Adoption en France



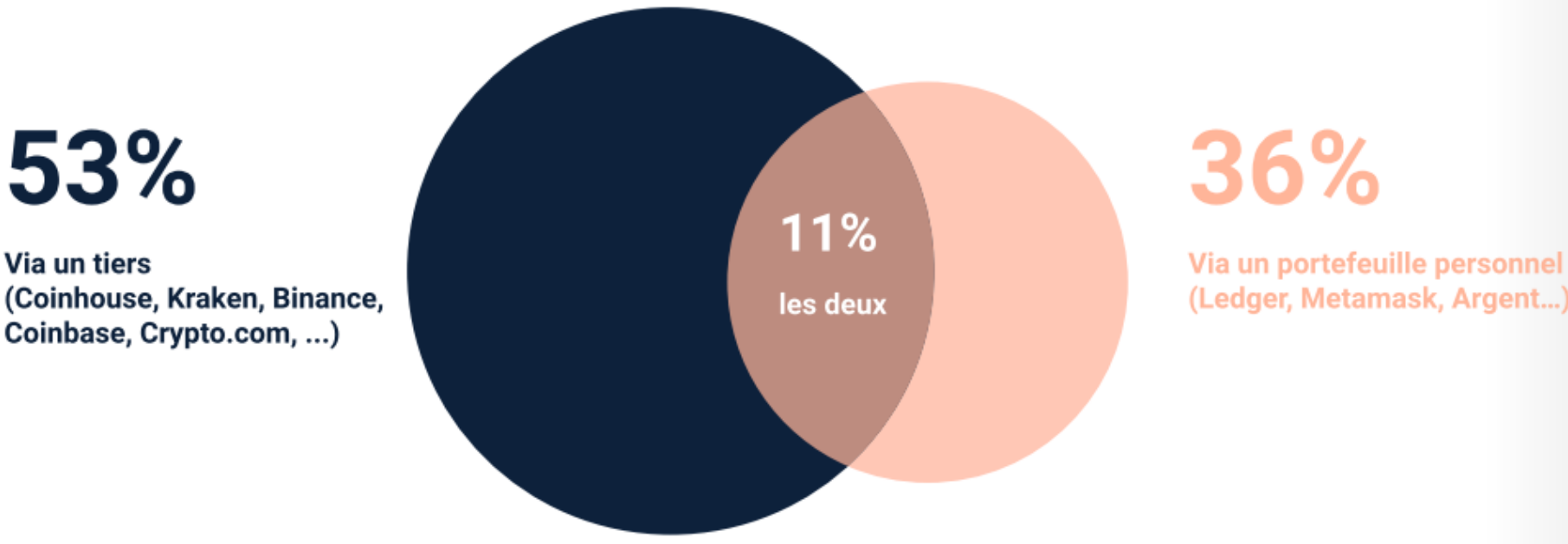
Source

Raisons d'acquérir des cryptoactifs



Source

Mode de conservation



Source

Adoption aux E-U

Characteristic	Invest-ment only	Transac-tions	Any
Family income			
Less than $25,000	5	4	9
$25,000–$49,999	5	2	7
$50,000–$99,999	8	2	10
$100,000 or more	10	2	12
Age			
18–29	10	4	14
30–44	11	4	15
45–59	7	2	10
60+	2	1	3

source

Motivations

Table 20. Main reason people used cryptocurrency for financial transactions

Reason	Percent
Person or business recieving the money preferred cryptocurrency	21
To send the money faster	21
Privacy	20
Cheaper	13
Safer	9
Don't trust banks	5
Other	10

Note: Among adults who used cryptocurrency for financial transactions.

source

Utilités des blockchains

Réserve de valeur et paiement : conserver et transférer la propriété digitale de manière sécurisée

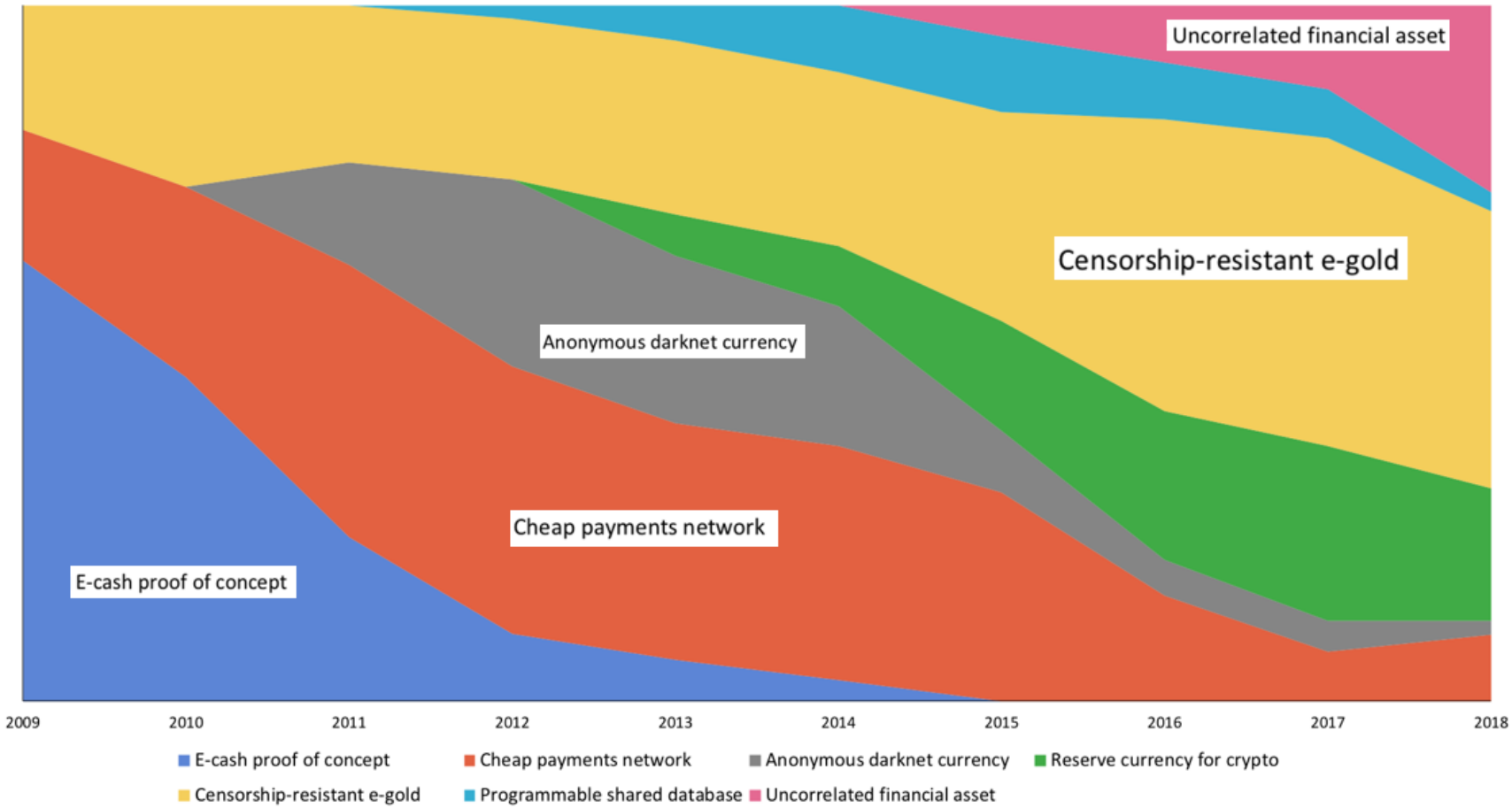
1200 milliards de dollars de valeurs sont sécurisés par des blockchains

Principaux cryptoactifs () :

- Bitcoin (40 %, 550 b$)
- Ethereum (20 %, 225 b$)
- BNB (3 %, 50 b$)
- Ripple (1,5 %, 26 b$)

source : 1, 2

Bitcoin : narratifs

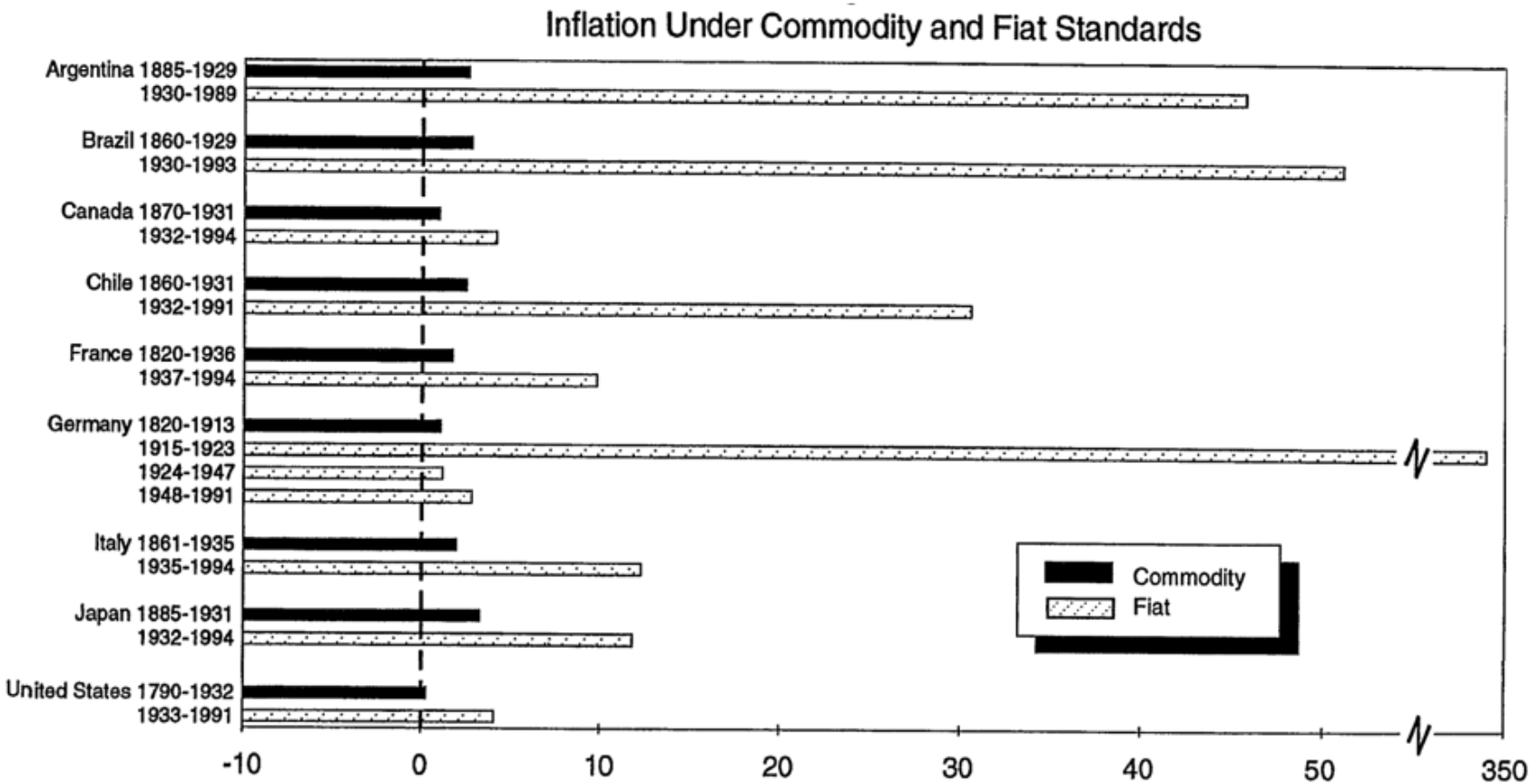


source

Bitcoin, l'or digital

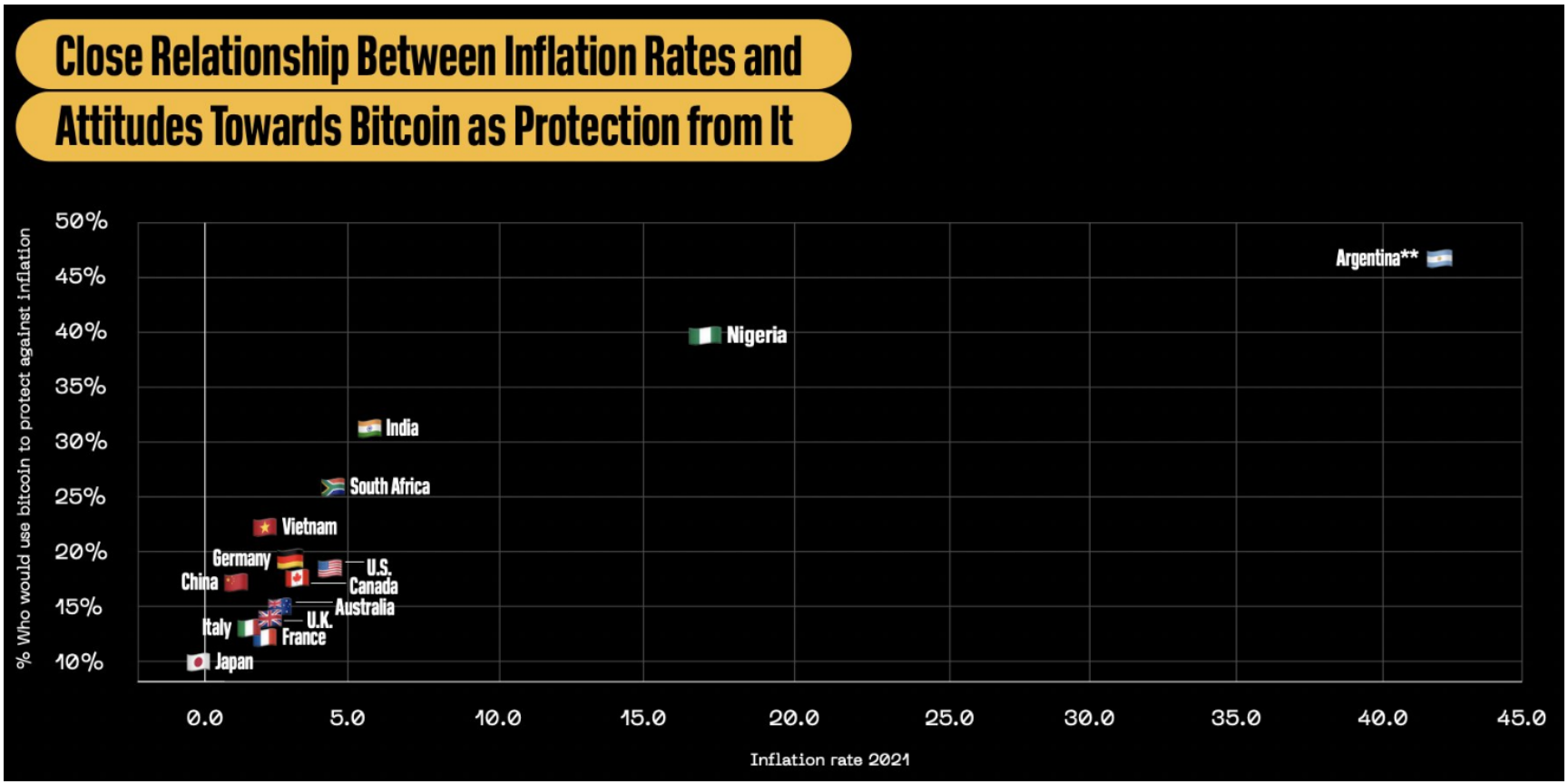
	Bitcoin	Or	Monnaie
Ancienneté	13 ans	5000 ans	2500 ans
Offre totale	fixe	fixe	illimitée
Nouvelles émissions	limitées	limitées	importante
volatilité du prix	élevé	faible	nulle
Potabilité	élevée	faible	élevée
Divisibilité	élevée	faible	élevée
Moyen de paiement	peu adéquat	peu adéquat	adéquat

Une défiance vis à vis du système monétaire fondé sur la monnaie fiduciaire



sources : 1, 2

Bitcoin et inflation : "Utiliseriez-vous Bitcoin comme protection contre l'inflation ?"



Réserve de valeurs et transferts de fonds

Dans les pays en développement, plus de la moitié des adultes ne disposent pas d'un compte bancaire (69% au Vietnam).

Les envois de fonds des travailleurs émigrés vers les pays à bas et moyen revenu ont représenté près de 600 milliards de dollars en 2021.

sources : 1, 2, 3, 4

Les stablecoin (1 jeton = 1 $)

- protection contre la volatilité des prix
- conversion stablecoin $\leftrightarrow$ crypto sans déclenchement fiscal et contrôle AML
- moyen de paiement rapide, transparent, sans frontière et à faible coût
- échanges entre devises
- transferts quasi-instantané (transferts bancaires entre 1 et 5 jours ouvrables)

$\triangleright$ 130 b$ de stablecoins (environ 10 % de la valeur totale des cryptoactifs)

$\triangleright$ 30 b$ de volumes échangées journaliers

source : 1, 2

La propriété digitale non fongible

Les NFT (*non fungible tokens*) sont des actifs non divisibles aux caractéristiques uniques.

Dans le monde physique, une peinture de Léonard Di Vinci ou une toccata de Jean-Sébastien Bach est une oeuvre unique.

Dans l'univers digital :

– avatars (*page's profile picture, pfp*) : Bored Ape Yacht Club, Cryptopunks, ...

– oeuvres digitales
  - fixes (Fragments of an infinite fields, ...)
  - animées (Assemblage, Geometry Runners, ...)
  - auto-générées (Autoglyphs, Chromie Squiggle, ...)

– œuvres musicales (Eulerbeats,...)

– caractères et items de jeu sur blockchain (Axie Infinity,...)

– parts de mondes virtuels (Decentraland, Cryptovoxels, ...)

Intérêt des blockchains pour la propriété digitale non fongible

1) Transmission pair à pair, absence d'intermédiaires (décentralisation)

2) Transparence du code et des transactions (traçabilité, certification de la provenance)

3) Libre accès et utilisation (marché mondial par défaut)

4) Immuabilité des transactions (sécurité des échanges)

5) Gestion des droits d'auteur et distribution du contenu

La finance décentralisée

▷ Ensemble des primitives financières (échanger, prêter, emprunter, levier, options, ...) codées sur les blockchains de smart contract

⟶ Infrastructure financière qui élimine le besoin de tout intermédiaire financier (banque, courtier, chambre de compensation, back office, ...)

→ *50 milliards de dollars de valeurs déposées dans des protocoles de finance décentralisée* (Defillama)

Exemples : Uniswap, une plateforme d'échange de cryptomonnaie décentralisée, Aave une plateforme de prêts.

Les noms de domaine

Un nom de domaine est un identifiant textuel de domaine internet. Le but de celui-ci est de communiquer facilement l'adresse d'un ensemble de serveurs informatiques. Ils sont plus digestes que les adresses IP, et plus facile à retenir.

Un nom de domaine permet donc d'avoir un identifiant qui peut être ensuite traduit en une adresse IP unique compréhensible par un ordinateur.

Par exemple, le nom de domaine amiens.fr revoie à l'adresse IP 185.86.48.21 : il s'agit de l'adresse IP du serveur qui héberge le site de la municipalité d'Amiens.

Des autorités centrales vont maintenir les bases de données nécessaires, contenant tous les noms de domaines et leur adresses IP associées. L'ICANN a pour mission d'allouer l'espace de ces adresses de protocoles Internet et de les attribuer.

Intérêts des noms de domaine décentralisés

- Une autorité centrale peut censurer des sites sous la pression des entreprises et des gouvernements.
- Acheter un site Internet nécessite de dévoiler ses informations personnelles

3Ea2Jz1VwtbCfMjG7AHqJA6Ti2cbGX4Tyk (bitcoin)
0xd8dA6BF26964aF9D7eEd9e03E53415D37aA96045 (ethereum)

s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jjppqkvwwqtyd.onion/

(Tor)

sont des noms de domaine décentralisés, mais non compréhensibles par des humains.

Histoire des nom de domaine (ou DNS) décentralisés

Première proposition sur BitcoinTalk en Novembre 2010 (bitDNS) : algorithme de preuve de travail est utilisé afin de stocker les noms de domaines de manière distribuée, sans autorité centrale.

Satoshi Nakamoto propose d'avoir deux chaînes et réseaux différents mais de laisser la possibilité à un mineur de soumettre une solution pour les deux services en parallèle (*merged mining*).

Ce projet s'est concrétisé sous la forme de Namecoin, qui fonctionne depuis Avril 2011.

sources : 1, 2, 3

Les noms de domaine sur Ethereum

Ethereum Name Service (ENS) lancé en mai 2017

0xd8dA6BF26964aF9D7eEd9e03E53415D37aA96045 $\longrightarrow$ pierre.eth

2,2 millions de noms de domaines créés

sources : 1, 2

Cas d'usage émergents

- ▷ Web3 et réseaux sociaux décentralisés (web3)
- ▷ Preuve d'humanité/unicité
- ▷ Tokénisation des actifs financiers (cf. leçon sur les stablecoins)

Web 3.0

Web 1.0 : les utilisateurs accèdent à du contenu en ligne (html, css)

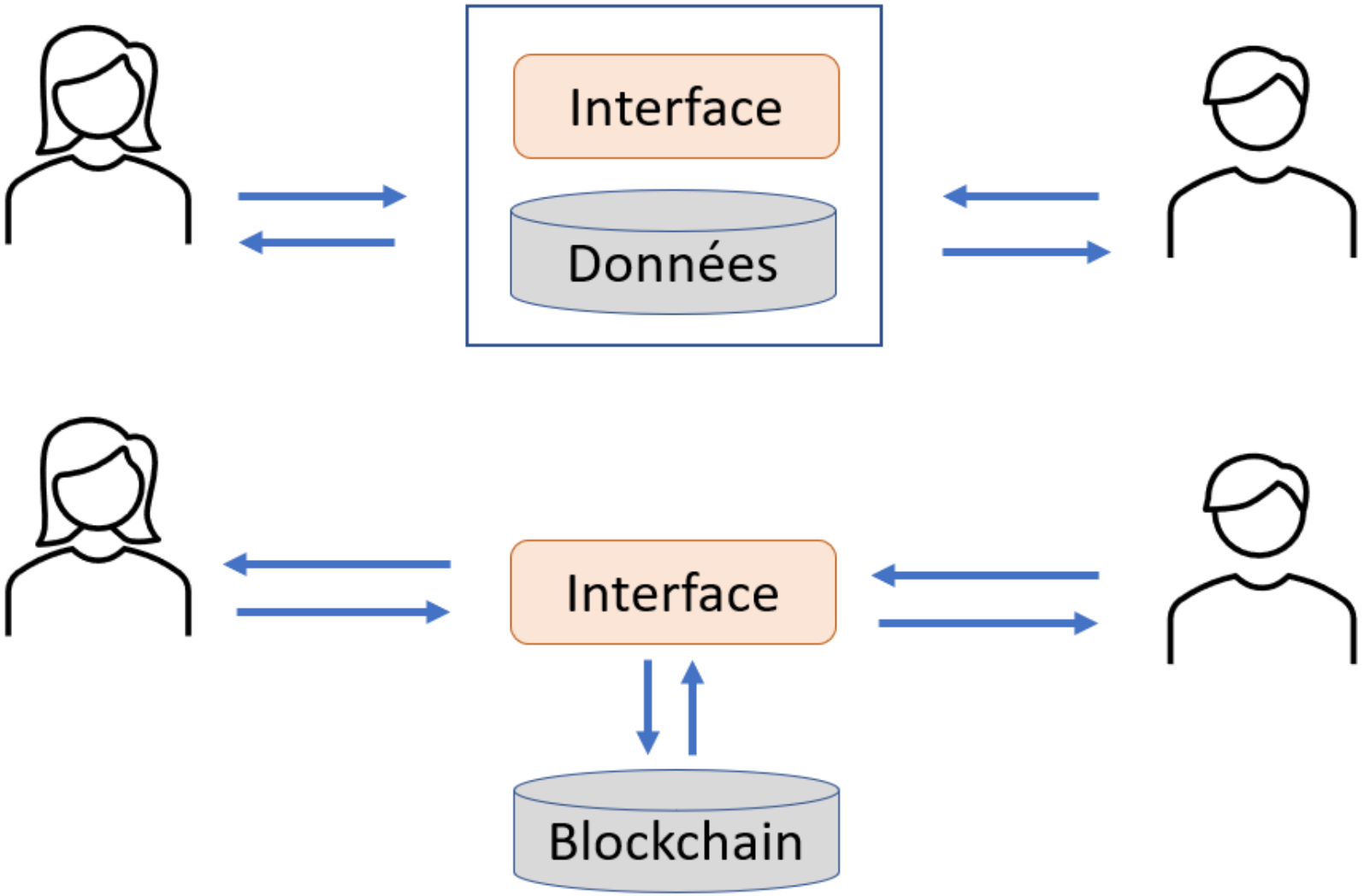
Web 2.0 : les utilisateurs créent le contenu, organisé et détenu par les GAFA, Leboncoin, Wikipedia, Tripadvisor, Twitter, ... (Php, Sql)

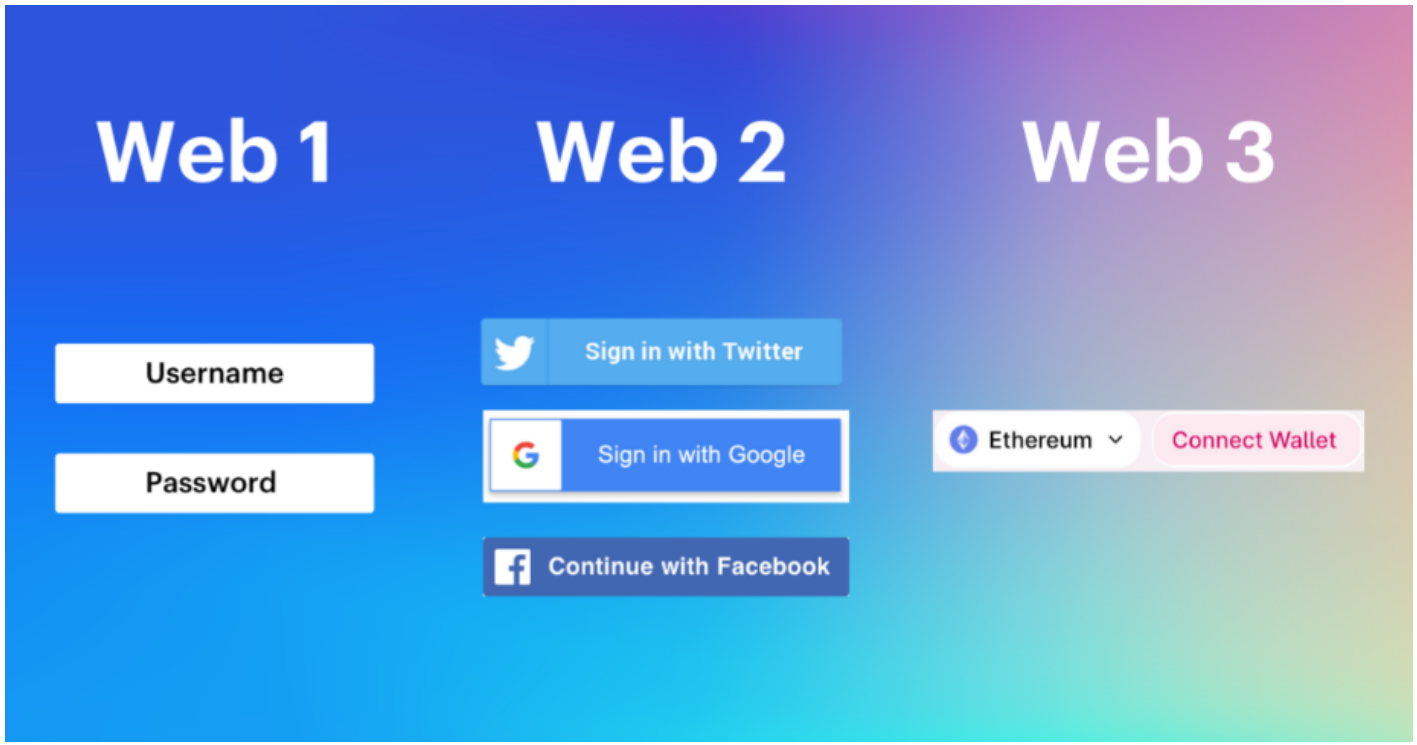
Web 3.0 : les utilisateurs possèdent les contenus qu'ils créent (propriété sécurisée par la blockchain).

Exemples :

- snax.eth sur Opensea, Zerion, et sur Rainbow.me

sources : 1

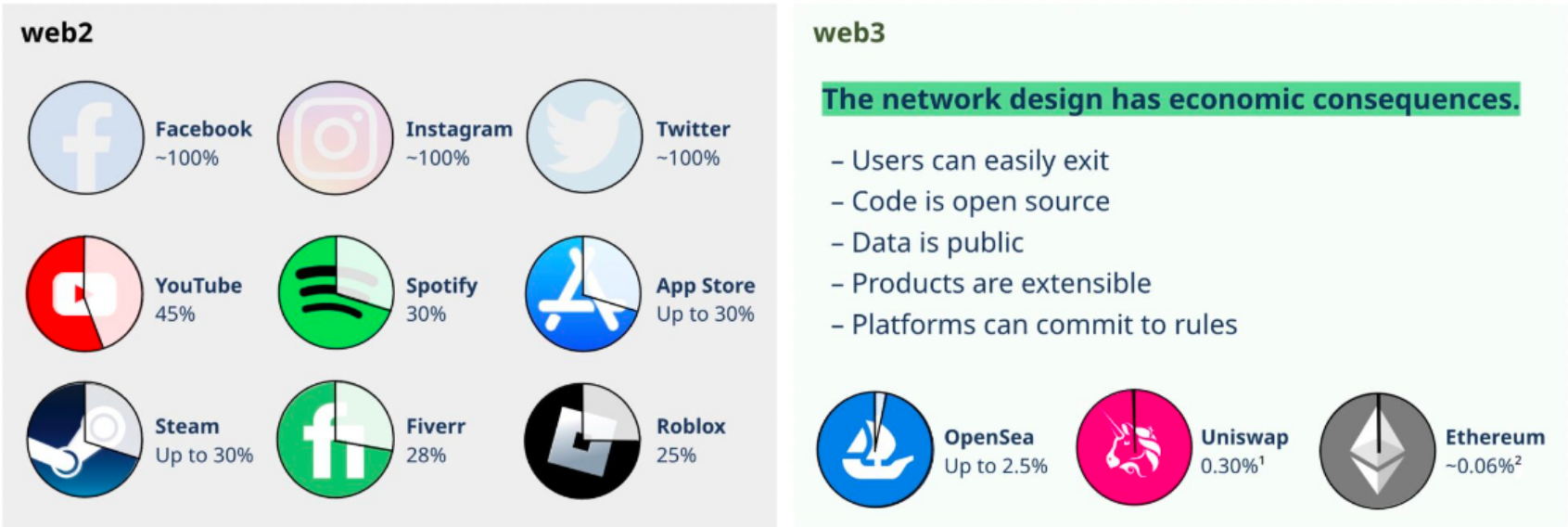

Interface
Données
Interface
Blockchain


Web 1
Web 2
Web 3
Username
Password
Sign in with Twitter
Sign in with Google
Continue with Facebook
Ethereum
Connect Wallet

sources : 1

Users have more power, and earn a greater share of revenue, on web3 versus web2 platforms

Comparison of take rates (% of revenue network owners take from users)



source

Réseaux sociaux décentralisés : Lens

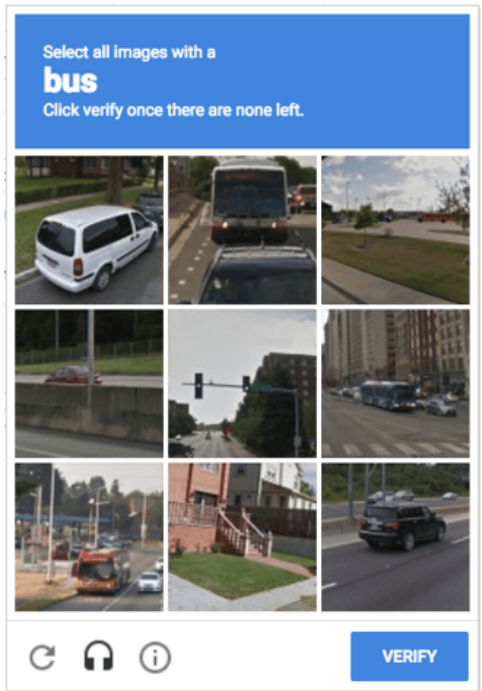
A PERMISSIONLESS, NON-CUSTODIAL SOCIAL MEDIA PROFILE

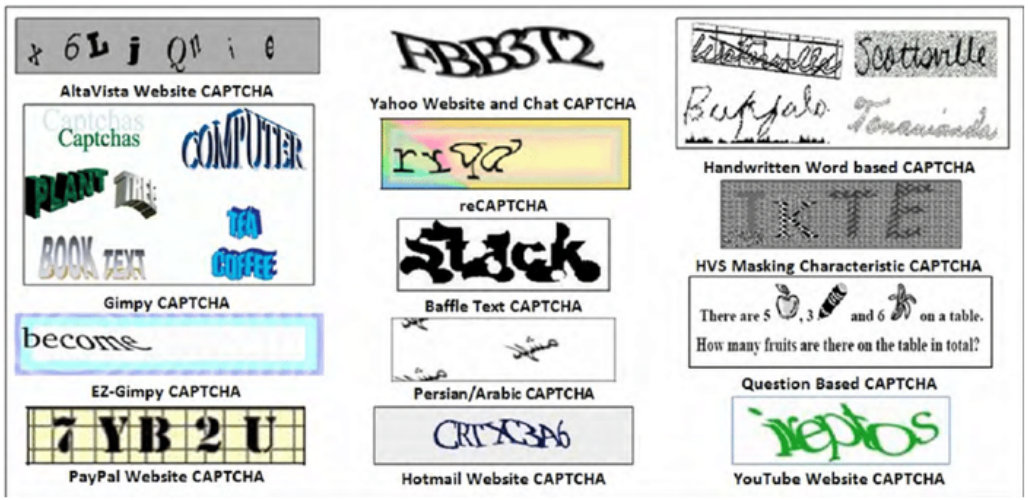
With Lens, you have complete ownership of your profile, connections, posts and data. Unlike traditional social media, you can easily switch to a new platform, taking your valuable content and followers with you.

Autre exemple : Farcaster (en phase beta)

Preuves d'humanité et unicité

Besoin de prouver son humanité dans les interactions en ligne





Comment prouver son unicité dans les interactions en ligne :

- systèmes de gouvernance 1 voix = 1 vote
- systèmes de réputation (likes, ...)
- forums de discussion (*upvotes* et *downvotes*)

$\longrightarrow$ prévention des attaques sybils ...

... non invasive pour la vie privée et maintenant les systèmes ouverts et décentralisés.

Dans la crypto, les preuves de travail et d'enjeu des blockchains sont des mesures anti-sybils

sources : 1

Worldcoin

▷ scanne l'iris de l'oeuil, en dérive un code unique (= identifiant) puis supprime la donnée biométrique

⟶ deux personnes ne peuvent avoir le même code

⟶ une personne ne peut avoir plusieurs codes différents

Aucunes données personnelles collectées

Fonctionne avec un wallet compatible avec Ethereum

sources : 1, 2, 3, 4

Autre application associée aux blockchains : revenu basique universel non gouvernemental (revenu distribué à tous sans condition)

- échelle mondiale
- faibles frais de transaction
- transparence des opérations
- préserve l'anonymat (Worldcoin)

Exemples d'initiative : UBI, GoodDollar

sources : 1