

Blockchains et NFTs

Comment partager sa richesse



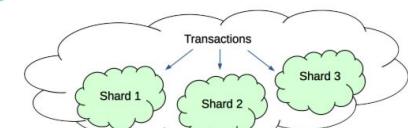


Linus Gasser



DEDIS

Decentralized Distributed Systems Laboratory





Notre journée NFT

- Pratique + 4 x Théorie / pratique
- But final: chaque groupe a son NFT
- Sujets:
 - Pourquoi les Blockchains?
 - Utilisation des Blockchains
 - Faire de l'art avec des NFTs
 - Comment utiliser des NFTs



Deux règles

Ne faites pas l'andouille

- Pas de connections sur les autres comptes
- Respectez les espaces électroniques mises à disposition: Discord et Spreadsheet
- Ne pas savoir n'est pas grave, il y a des étudiants qui sont là pour vous aider!

Faites-vous remarquer par votre gentillesse

- Aidez les autres s'ils n'arrivent pas
- Expliquez, ne faites pas à leur place (pas touche à la souris ou au clavier)
- Changez qui utilise le clavier

Pourquoi les Blockchains?



Blockchain

Crypto Billionaires: 11 Ir Crazy Rich with Crypto



Ruholamin Haqshenas

Cryptocurrency Journalist

Last updated: 30 August, 2023

99'376.57 USD

+91,355.59 (1,138.96%)↑ past 5 years

6 Jan, 08:29 UTC · Disclaimer

1D | 5D | 1M | 6M | YTD | 1Y | **5Y** | Max

100'000

80'000

60'000

40'000

20'000

0

2022

2024

KEY TAKEAWAYS

The rise of cryptocurrencies has undeniably created some of the world's most wealthy individuals. These individuals have earned their fortunes in different ways, from early investors to founders of major companies. They have all been willing to take risks and embrace the future of digital currency.

Heroes to zeroes in 12 months: How the two biggest crypto billionaire CEOs proved the critics right

PUBLISHED SAT, DEC 30 2023-11:36 AM EST | UPDATED SAT, DEC 30 2023-11:55 AM EST



SHARE in

KEY POINTS

- After a brutal 18 months of bankruptcies, company failures and criminal trials, the crypto market is starting to claw back some of its former standing.
- But even as prices swell, the sector's reputation has struggled to regain ground after names virtually synonymous with bitcoin have both been found guilty of crimes directly related to their multibillion-dollar crypto empires.
- FTX's Sam Bankman-Fried and Binance's Changpeng Zhao went from industry titans to convicted frauds in the span of 12 months.

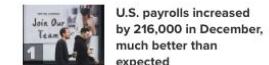


Combination showing Former FTX CEO, Sam Bankman-Fried (L) and Zhao Changpeng (R), founder and chief executive officer of Binance.

Getty Images / Reuters

Squawk on the Street UP NEXT | Money Movers 11:00 am ET Listen

TRENDING NOW



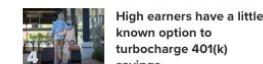
U.S. payrolls increased by 216,000 in December, much better than expected



S&P 500 opens flat, heads for first losing week in 10 following hot jobs report



4 in-demand side hustles for 2024—one pays as much as \$150 per hour



High earners have a little-known option to turbocharge 401(k) savings



Blank Street Coffee bets on subscription program to win over daily coffee drinkers



Bitcoin: vision de Satoshi Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System

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

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Une version de la monnaie électronique sans serveur central permettrait de faire des paiements en ligne et de les envoyer directement d'une partie à une autre sans passer par une institution financière.



Une version simplifiée d'une banque

Jean donne 0.5 bitcoin à Stéphanie
Claude donne 1.3 bitcoin à Marie
Marie donne 0.5 bitcoin à Anne
Chloé donne 0.2 bitcoin à Claude
...



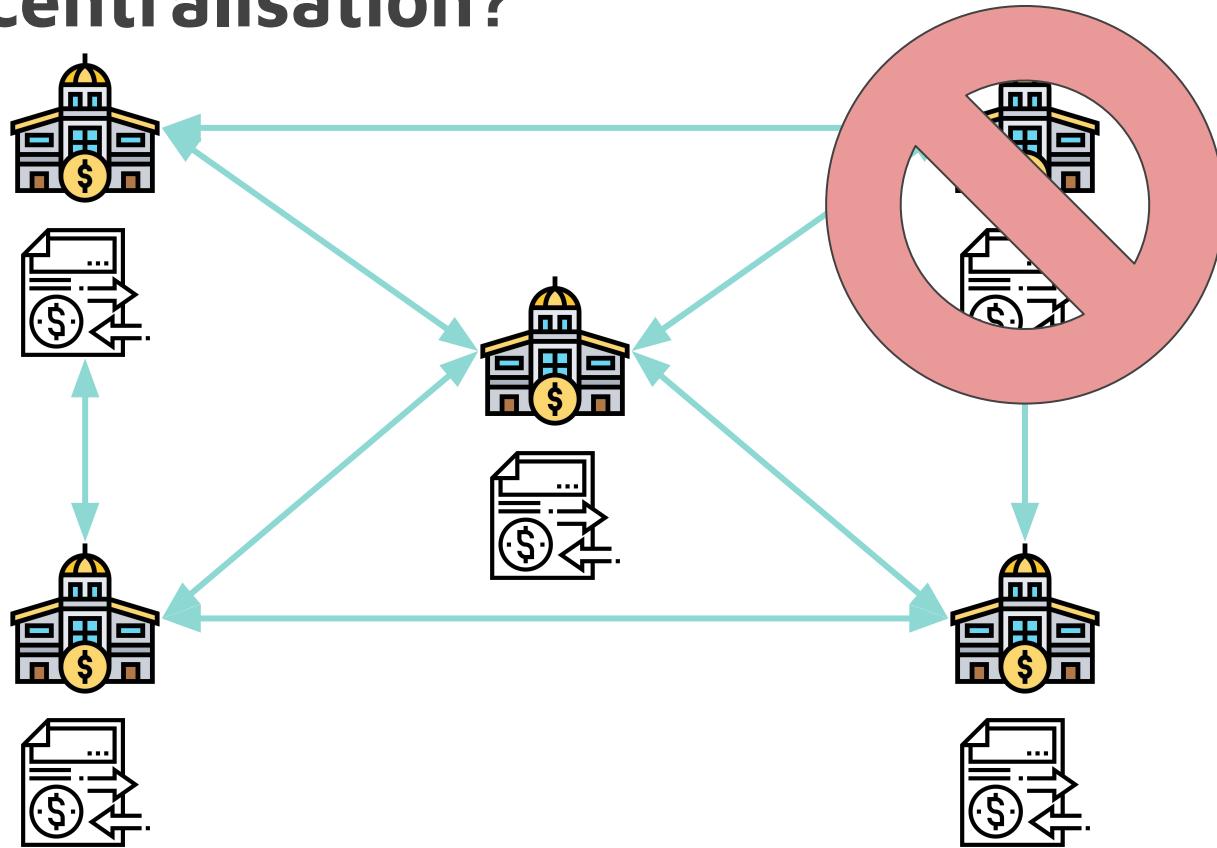
Registre
(Ledger)



Problème de la centralisation



Decentralisation?





Bitcoin: vision de Satoshi Nakamoto



Argent

- Il suffit de stocker les transactions
- L'argent doit être libre
- Le gouvernement est inutile



Réseau sans ordinateur central

Tout est décentralisé

Personne ne peut

- l'arrêter
- le censurer



Banque centrale

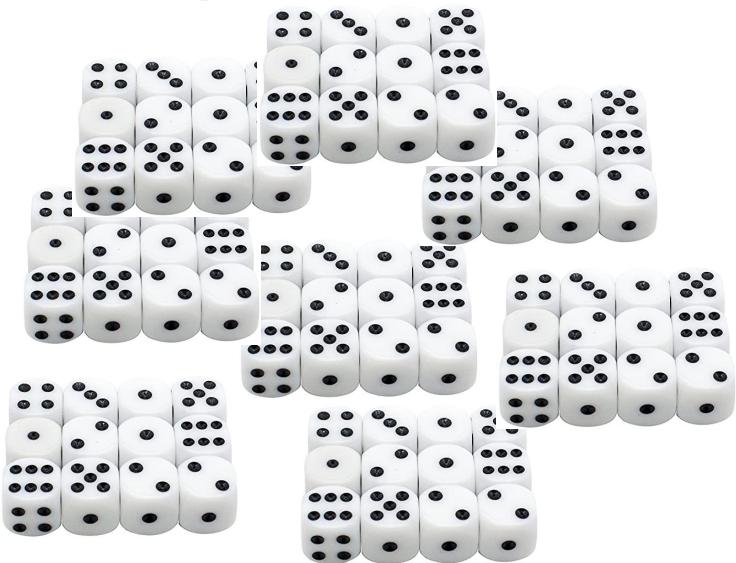
- Empêche l'utilisation libre de l'argent
- Doit disparaître

Sécuriser l'envoie des bitcoins

Création d'un
système de paiement
décentralisé



Sécuriser l'envoie des bitcoins



Création d'un secret
aléatoire
(clé privée)

Cryptographie
asymétrique

mr9i7SQcTLEJ8FtW5zr
ivGxeAoFPnXMHzw



Calcul de l'adresse
publique

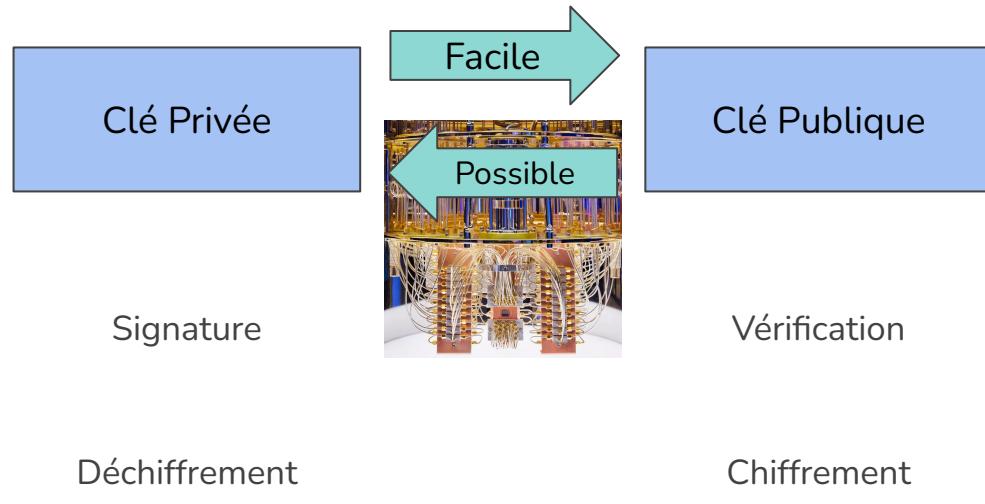


Cryptographie Asymétrique

Functions à chemin unique:

Signature électronique
blockchains, mises à jours, httpS

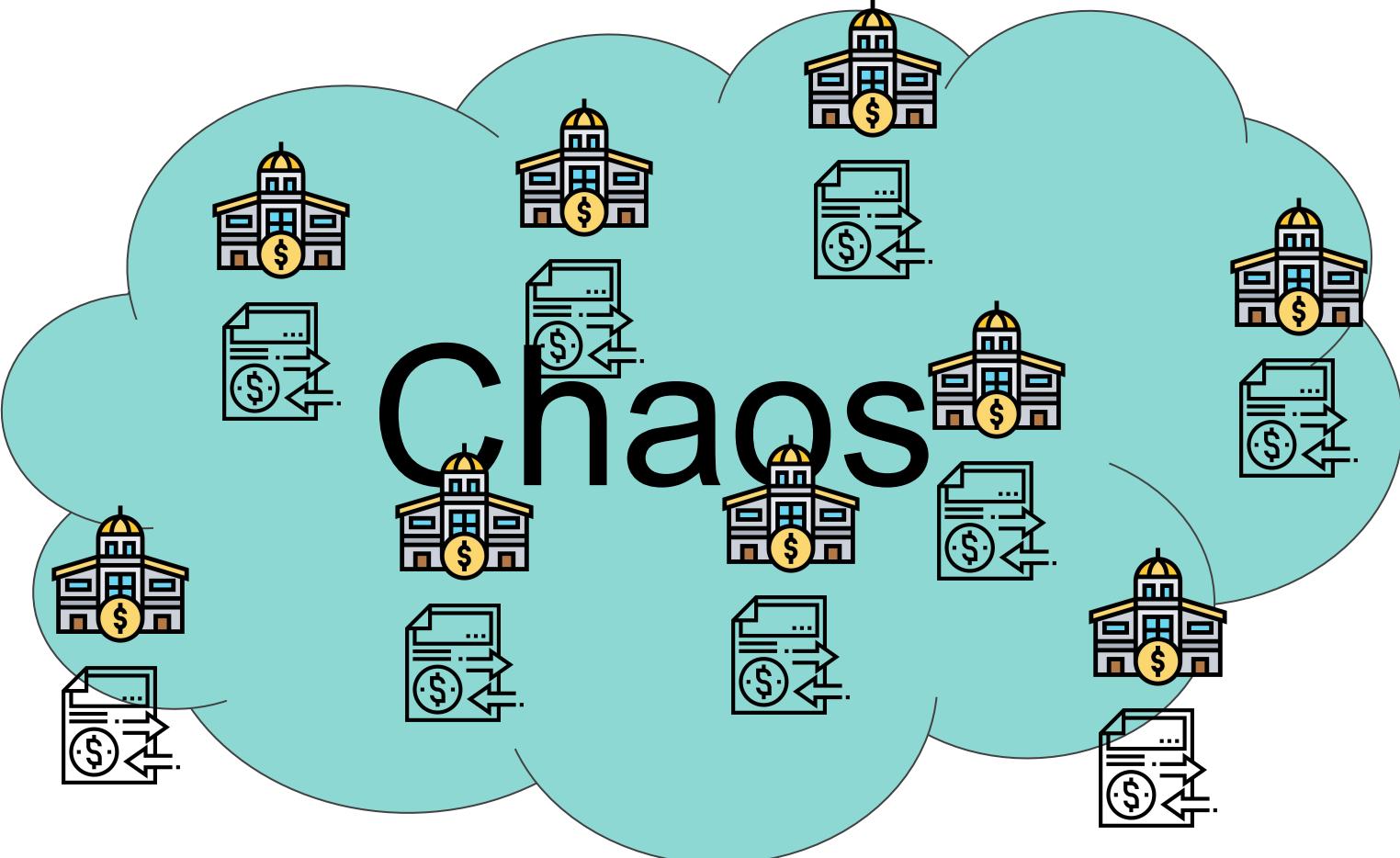
Chiffrement électronique
httpS, chat





mr9i7SQcTLEJ8FtW5zrivGxe
AoFPnXMHzw

Création d'un système de paiement décentralisé





mr9i7SQcTLEJ8FtW5zrivGxe
AoFPnXMHzw

Création d'un système de paiement décentralisé

Aussi lentement
que nécessaire...



Aussi lentement que nécessaire, aussi vite que possible



Une nouvelle
liste chaque 10'



Tirage au sort

SUDOKU									ANSWER:								
2	9					6			2	1	9	5	4	3	6	7	8
4		8	7				1	2	5	4	3	8	7	6	9	1	2
8			1	9	4				8	7	6	2	1	9	3	4	5
3		7			8	1			4	3	2	7	6	5	8	9	1
6	5			8	3				7	6	5	1	9	8	2	3	4
1			3				7	9	1	9	8	4	3	2	5	6	7
		6	5	7	9				3	2	1	6	5	4	7	8	9
6	4				2				6	5	4	9	8	7	1	2	3
8	3	1	4	5					9	8	7	3	2	1	4	5	6

Sudoku géant



mr9i7SQcTLEJ8FtW5zrivGxe
AoFPnXMHzw

Création d'un système de paiement décentralisé

SUDOKU								
2	9			6				
	4		8	7			1	2
8				1	9	4		
	3	7			8	1		
	6	5				3		
1				3			7	
			6	5	7	9		
6	4					2		
	8	3		1	4	5		

ANSWER:								
2	1	9	5	4	3	6	7	8
5	4	3	8	7	6	9	1	2
8	7	6	2	1	9	3	4	5
4	3	2	7	6	5	8	9	1
7	6	5	1	9	8	2	3	4
1	9	8	4	3	2	5	6	7
3	2	1	6	5	4	7	8	9
6	5	4	9	8	7	1	2	3
9	8	7	3	2	1	4	5	6

Sudoku géant



mr9i7SQcTLEJ8FtW5zrivGxe
AoFPnXMHzw

Garantir une
historique unique

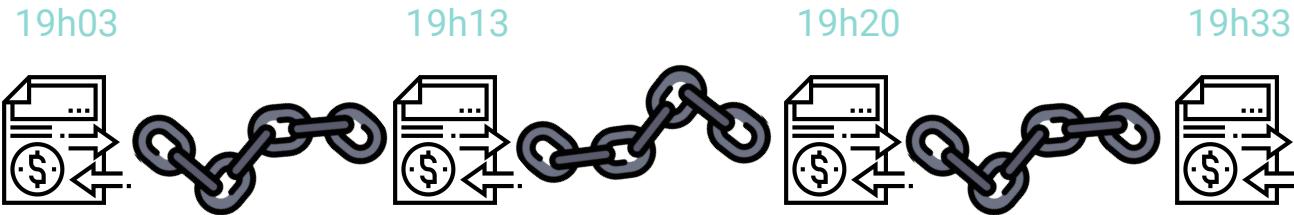
Création d'un système de paiement décentralisé

SUDOKU									ANSWER:								
2	9				6				2	1	9	5	4	3	6	7	8
	4		8	7				1	2	5	4	3	8	7	6	9	1
8				1	9					8	7	6	2	1	9	3	4
	3	7			8			1		4	3	2	7	6	5	8	9
	6	5			8					7	6	5	1	9	8	2	3
1			3					7		1	9	8	4	3	2	5	6
			6	5		7		9		3	2	1	6	5	4	7	8
6	4					2				6	5	4	9	8	7	1	2
	8		3		1	4	5			9	8	7	3	2	1	4	5

Sudoku géant



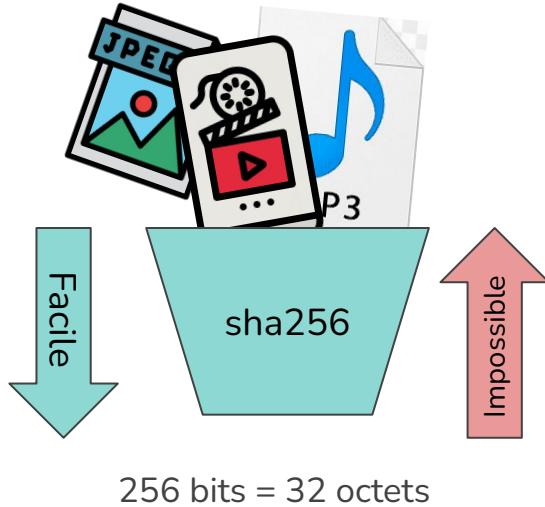
Garantir une historique unique



1 nouvelle liste
au registre
chaque 10'

Enchaîner les
listes

Fonction de hachage



fa05721d43e6a1c22ce08c8336d1553d
30eebf15998b2bbc2a9c9deb1dca50ec

- Créer une empreinte unique
 - 2^{256} possibles valeurs
- Peut être utilisé comme fonction à chemin unique
 - Protégé contre ordinateurs quantiques
- Exemples d'utilisation:
 - Signatures
 - Vérification de documents
 - Chaînage de blocs
 - Proof-of-work



mr9i7SQcTLEJ8FtW5zrivGxe
AoFPnXMHzw



Listes enchaînées

Création d'un système de paiement décentralisé

SUDOKU									ANSWER:								
2	9				6				2	1	9	5	4	3	6	7	8
4		8	7			1	2		5	4	3	8	7	6	9	1	2
8			1	9	4				8	7	6	2	1	9	3	4	5
3	7			8	1				4	3	2	7	6	5	8	9	1
6	5			8	3				7	6	5	1	9	8	2	3	4
1		3			7				1	9	8	4	3	2	5	6	7
		6	5	7	9				3	2	1	6	5	4	7	8	9
6	4				2				6	5	4	9	8	7	1	2	3
8	3		1	4	5				9	8	7	3	2	1	4	5	6

Sudoku géant



mr9i7SQcTLEJ8FtW5zrivGxe
AoFPnXMHzw



Listes enchaînées

Création d'un système de paiement décentralisé

SUDOKU									ANSWER:								
2	9				6				2	1	9	5	4	3	6	7	8
4		8	7			1	2		5	4	3	8	7	6	9	1	2
8			1	9	4				8	7	6	2	1	9	3	4	5
3	7			8	1				4	3	2	7	6	5	8	9	1
6	5			8	3				7	6	5	1	9	8	2	3	4
1		3			7				1	9	8	4	3	2	5	6	7
		6	5	7	9				3	2	1	6	5	4	7	8	9
6	4				2				6	5	4	9	8	7	1	2	3
8	3	1	4	5					9	8	7	3	2	1	4	5	6

Sudoku géant

Trouver des participants



Comment trouver des participants?



Récompense



mr9i7SQcTLEJ8FtW5zrivGxe
AoFPnXMHzw



Listes enchaînées

Création d'un système de paiement décentralisé

SUDOKU									ANSWER:								
2	9				6				2	1	9	5	4	3	6	7	8
4		8	7			1	2		5	4	3	8	7	6	9	1	2
8			1	9	4				8	7	6	2	1	9	3	4	5
3		7		8	1				4	3	2	7	6	5	8	9	1
6	5			8	3				7	6	5	1	9	8	2	3	4
1			3			7	7		1	9	8	4	3	2	5	6	7
		6	5		7	9			3	2	1	6	5	4	7	8	9
6	4				2				6	5	4	9	8	7	1	2	3
8		3		1	4	5			9	8	7	3	2	1	4	5	6

Sudoku géant



Récompense



Cryptographie Asymétrique



Blockchain

Création d'un système de paiement décentralisé

SUDOKU									ANSWER:								
2	9				6				2	1	9	5	4	3	6	7	8
	4		8	7				1	2	5	4	3	8	7	6	9	1
8				1	9	4				8	7	6	2	1	9	3	4
	3	7			8	1				4	3	2	7	6	5	8	9
	6	5			8	3				7	6	5	1	9	8	2	3
1			3			7				1	9	8	4	3	2	5	6
										3	2	1	6	5	4	7	8
			6	5		7	9			6	5	4	9	8	7	1	2
6	4									9	8	7	3	2	1	4	5
	8	3		1	4	5											

Proof-of-work



Mining Reward



Transaction sur Bitcoin

Positif:

- Ouverture du “compte” très simple
- Durée de transaction 10’ à 1h

Attention

- Perte d’argent si: erreur dans l’adresse, perte de la clé privée
- Une identité pseudonyme (pas anonyme) - l’adresse est visible!
- Pour convertir en Euros -> bureau de change -> possibilité de désanonymisation



Blockchain - définition

Une blockchain permet de stocker de l'information de façon *publique* et *permanente*: tout le monde peut lire l'information, et personne ne peut l'enlever. Un ensemble d'ordinateurs appelés *nœuds* gèrent la blockchain. Ils créent un *consensus* sur toute nouvelle information à publier en appliquant des *règles précises*.



II.1 - Cartes de suivi

1. Vous mettez la carte "À l'écoute" sur vos écrans
2. Je vous montrer comment faire la procédure
3. Vous mettez la carte "Au travail" et exécutez le travail.
Si vous avez des questions, demandez aux assistants.
4. Une fois que vous avez terminé, mettez la carte "Terminé"
5. Assurez-vous que tout le monde dans le groupe ait bien compris
6. Si vous avez des questions, mettez la carte "J'ai une question"



II.2 - Firefox

- Commencez avec <https://qo.epfl.ch/sismondi25>
 - Vous y trouverez le lien vers "Discord"
 - Dans "Discord" vous trouverez les autres liens
- NOTES_NFTs doit être ouvert sur votre compte Sismondi!
 - Si votre compte se bloque, c'est votre sauvegarde!
 - Assurez-vous que les informations importantes y sont



II.3 - Fonctionnement Metamask

1. Création d'un numéro aléatoire pour la clé privée
2. Calcul de la clé publique correspondante
3. Protection de la clé privée avec un mot de passe
4. Interactions avec la blockchain
 - a. Demande du solde
 - b. Envoi de jetons
 - c. Vérification d'un NFT entré
 - d. Transfert de NFTs



II.5 - Recevoir des Jetons: Miner, robinets, acheter

Miner

- Récompense pour la participation au consensus
- Pour le proof-of-work et pour le proof-of-stake

Robinet

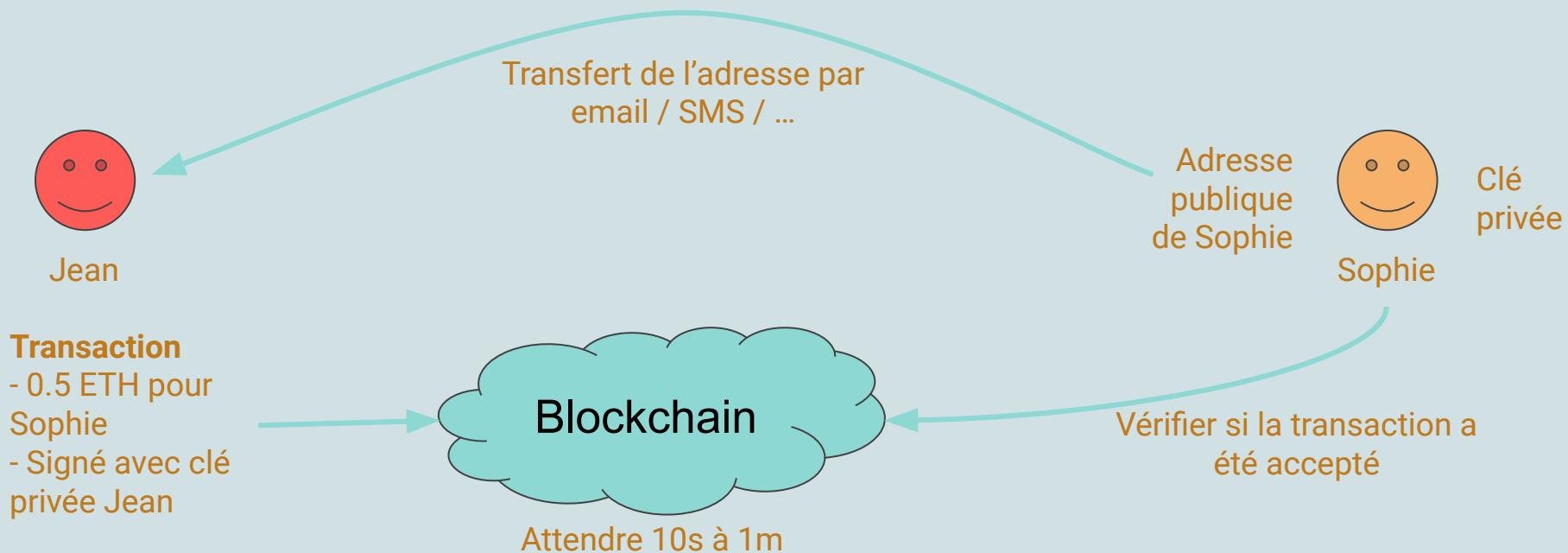
- Partage de jetons sur les chaînes de test
- Souvent protégé, pour éviter les abus

Acheter

- Utiliser une plateforme d'échange cryptos
- Pour les chaînes de tests: sites spécialisés



Exemple d'une transaction sur Bitcoin



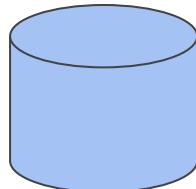
Utilisation des Blockchains



Éléments d'une blockchain

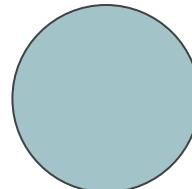
État

Le graal sacré de la blockchain. Immutable (ne change jamais), au moins celui du passé. Les nœuds peuvent décider de mettre à jour l'état si les utilisateurs le demandent.



Nœuds

Les travailleurs de la blockchains. Les utilisateurs interagissent avec les nœuds. Ensemble, les nœuds définissent l'état global de la blockchains.
Normalement un nœud tourne sur un serveur.



Utilisateurs

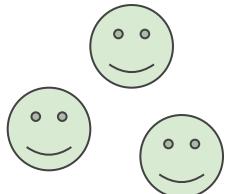
Payent pour la blockchain. Ils interagissent avec les nœuds en envoyant des transactions signées vers un ou plusieurs nœuds.



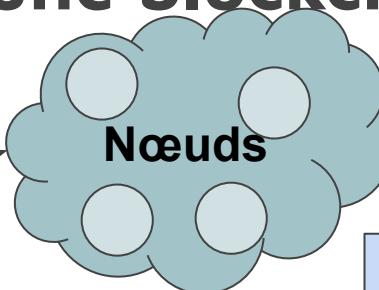


Éléments d'une blockchain

Utilisateurs

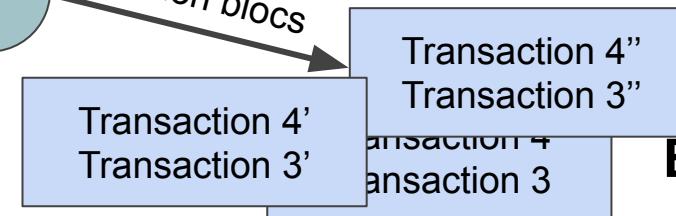


Envoi de transactions



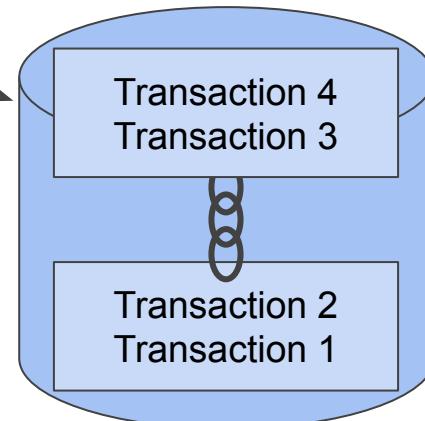
Nœuds

Création blocs



Blocs

Vérification des transactions et de l'état



Appliquer consensus

**Ledger /
Blockchain**

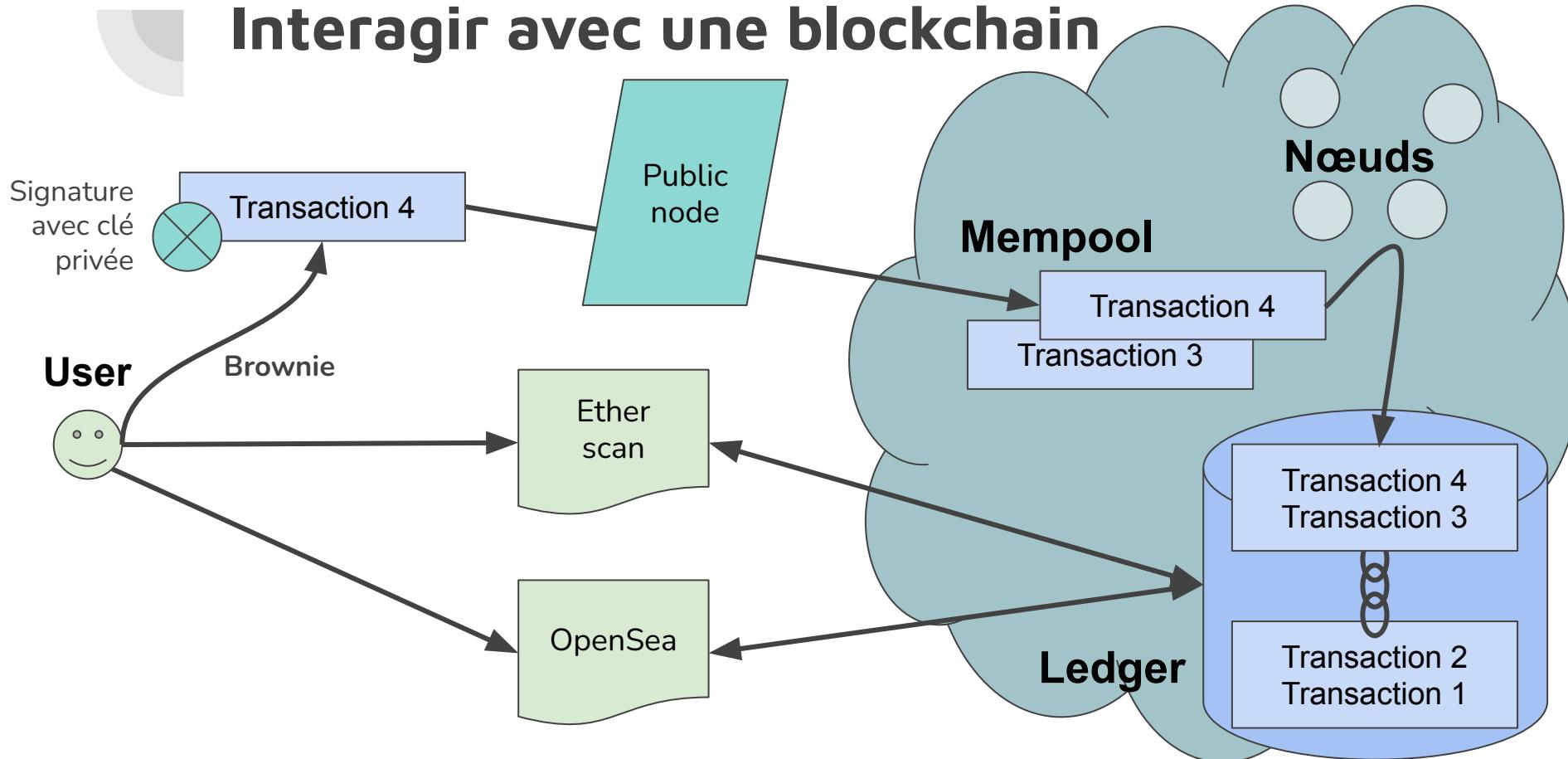


Contenu d'une transaction

Une transaction est une commande qui peut utiliser des

- *Assets*
 - La devise de la chaîne: Bitcoin, Ether, ...
 - La blockchain va s'assurer que la somme totale de la devise reste constante
 - Sauf pour le minage (création d'un nouveau bloc) qui va ajouter de la devise
- *Tokens*
 - Représentation digitale d'un objet (du monde réel)
 - Des *smart contracts* peuvent définir comment les *tokens* sont échangés
- *Smart contracts*
 - Sont des petits logiciels qui s'appliquent aux données de la blockchain
 - Permettent d'étendre la fonctionnalité de la blockchain
 - Sont vérifiés par le consensus des nœuds

Interagir avec une blockchain





Mempool et "Gas Price"

- Le "Mempool" contient les transactions POTENTIELLES
- Chaque transaction contient une "récompense"
- Seulement un nombre limité de transactions peuvent être ajouté à un bloc
- Les nœuds choisissent les transactions avec la plus grande récompense
- Plus il y a de transactions, plus la récompense doit être élevée

Pour Sepolia, le prix < 100 est bon marché -> votre contrat coûtera < 0.3 SepoliaETH

Un prix entre 100 et 200 est élevé -> votre contrat coûtera jusqu'à 0.6 SepoliaETH

Le prix peut monter jusqu'à 2000! -> votre contrat coûtera alors 6 SepoliaETH!

Pour voir le prix actuel: <https://owloracle.info/sepolia>



Le 7 janvier 2025





Ethereum, Sepolia, Development

	Ethereum mainnet	Sepolia testnet	Development
Géré par	Des "miners" professionnels	Des développeurs Ethereum	Votre ordinateur
Recevoir des jetons	Miner avec un nœud Acheter sur un échange	Acheter avec des ETHs	Démarrer le réseau: --network development
Coûts pour un SismondiNFT	~300US\$	~0.1US\$	Gratuit



III.1 - Etherscan

- Montre les transactions de la blockchain
- Indique les soldes des comptes
- Reconnaît certains smart contracts et peut interpréter les données
- Existe pour la chaîne principale et les chaînes de test

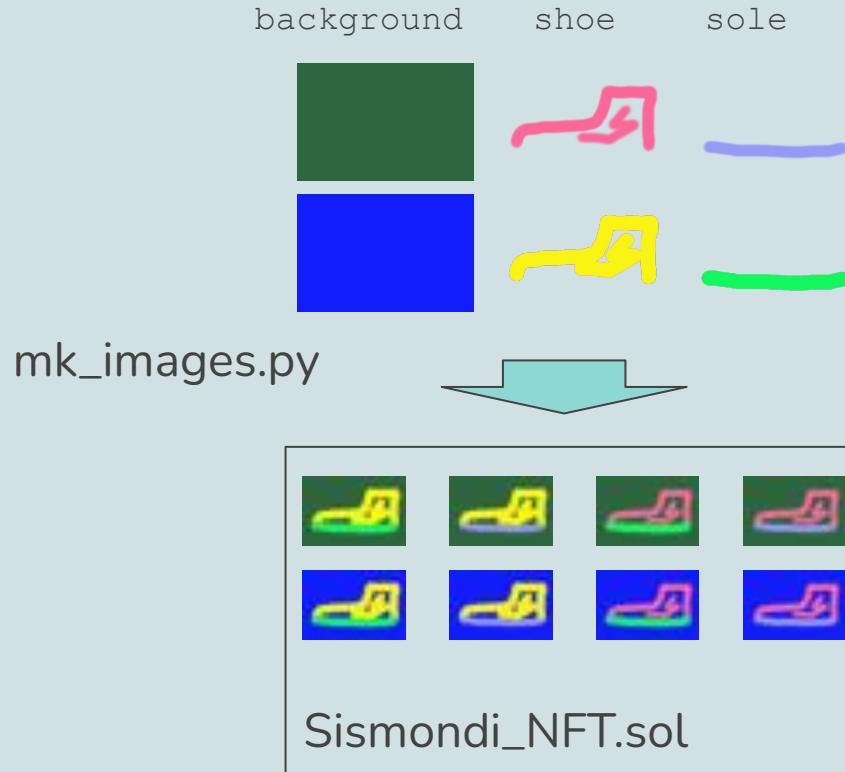


III.2 - Organisation du répertoire

- contracts/ - contient le *smart contract* pour le NFT
- images/ - pour les images qui doivent figurer dans le NFT
- scripts/ - logiciels pour convertir les images et utiliser le *smart contract*
- README.md - avec des instructions pas-à-pas
- NOTES.md - mettez-y vos adresses et clés
- env.example - exemple pour le fichier .env
- brownie.sh - lance les commandes qui ont besoin d'accéder la blockchain
- operations.log - va être créé par *brownie.sh* et contient le journal des opérations



III.3 - Installation Images





III.3 - Le script *images.py*

- Source des images dans les variables *backgrounds*, *shoes*, *soles*
 - Deux images par type de source
 - Répertoire relatif au script *images.py*
- Exécuter le script pour
 - Créer les 8 combinaisons d'images: b1s1o1, b1s1o2, b1s2o1, ..., b2s2o2
 - Afficher les deux blocs pour remplacer
 - Le préfix, qui est le même pour toutes les images
 - Les 8 images
 - Les données sont affichées en Base64, pour interprétation directe

Faire de l'art avec les NFTs



Ethereum: vision de Vitalik Buterin

A Next-Generation Smart Contract and Decentralized Application Platform

Satoshi Nakamoto's development of Bitcoin in 2009 has often been hailed as a radical development in money and currency, being the first example of a digital asset which simultaneously has no backing or [intrinsic value ↗](#) and no centralized issuer or controller. However, another - arguably more important - part of the Bitcoin experiment is the underlying blockchain technology as a tool of distributed consensus, and attention is rapidly starting to shift to this other aspect of Bitcoin. Commonly cited alternative applications of blockchain technology include using on-blockchain digital assets to represent custom currencies and financial instruments ([colored coins ↗](#)), the ownership of an underlying physical device ([smart property ↗](#)), non-fungible assets such as domain names ([Namecoin ↗](#)), as well as more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules ([smart contracts ↗](#)) or even blockchain-based [decentralized autonomous organizations ↗](#) (DAOs). What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.

[...] des applications plus complexes impliquant que les actifs numériques soient directement contrôlés par un morceau de code mettant en œuvre des règles arbitraires (**smart contract**) ou même des organisations autonomes décentralisées (**DAO**) basées sur la blockchain.



Exemples de *Smart Contracts*

La blockchain va parvenir à un consensus sur l'application du contrat. Par exemple:

- *Tokens* qui représentent
 - Une devise virtuelle: [Ethereum ERC20 tokens](#)
 - Un service qui doit être payé: [filecoin](#), [nym](#)
 - Un lien vers un objet et certaines droits: [NFT](#)
- Chaîne logistique - création, transport, transformation d'éléments
- Gestion de l'identité - avec un [contrôle d'accès](#) et une gestion du consentement
- Jeux - comme [Crypto Kitties](#) qui enregistrent des chatons virtuels sur Ethereum



Smart Contract <-> Contrat légal

	Smart Contract	Contrat légal
Définit par	du code informatique	du langage courant
Protégé par	les nœuds de la blockchain	le système légal du pays
Champ d'application	les jetons de la blockchain	tout objet au sens légal
Erreurs possibles	dans la programmation	texte contraire à la loi
Conséquences	exécution des erreurs	jugement par un tribunal



NFT - définition

Un *Non Fungible Token* (NFT), parfois appelé *jeton numérique*, est défini par un *smart contract* sur une blockchain. Les NFTs permettent de transférer des *droits d'utilisation* entre des comptes. Certains NFTs offrent aussi une approche *ludique* pour créer des nouvelles œuvres d'art.



NFT - exemple



69 M US-\$
chez "Christies"

L'acheteur de EVERYDAYS: THE FIRST 5000 DAYS détient:

- Une entrée dans Ethereum avec un lien vers sa clé publique
- Cette entrée pointe vers ce fichier: [metadata file](#)

Ce fichier est stocké sur IPFS, un système de fichiers distribué. Il contient de l'information sur l'artiste et des liens sur l'image.

Au niveau légal, un NFT peut (ou pas) donner des droits d'utilisation de l'œuvre d'art en question.

Au niveau technique, un NFT vous donne la capacité de le passer à quelqu'un d'autre: [technical details](#)



IV.2 - La blockchain locale de développement

- Elle tourne seulement sur l'ordinateur de développement
- Elle est réinitialisée après chaque commande
- Permet une vérification rapide du contrat
- Nécessite un traitement spécial pour lancer plusieurs transactions

Pour l'utiliser, lancez la commande

```
./brownie.sh sismondi.py deploy_mint --network development
```

IV.2 - Utilisation SismondiNFT

User 1



mk_images.py



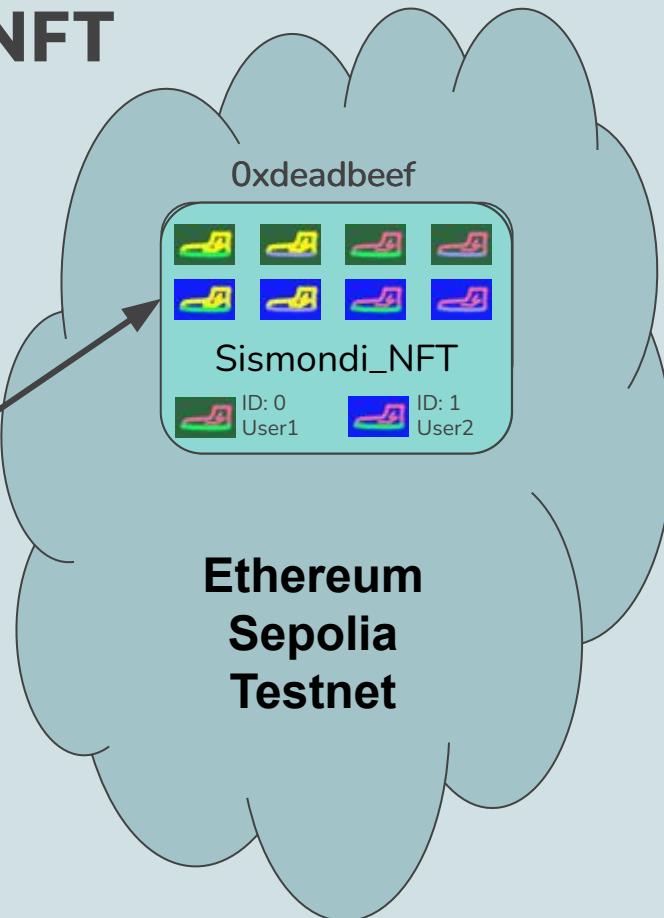
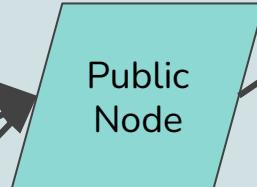
deploy

\$ mint 0xdeadbeef
00

User 2



\$ mint 0xdeadbeef
01





IV.4 - Le contrat SismondiNFT

- Utilise un contrat existant pour la base
- Permet
 - l'installation du contrat sur une blockchain
 - la création de jusqu'à 10 nouveau NFTs par n'importe qui
 - la lecture d'un NFT et du nombre total de NFTs créés
- Chaque NFT contient aléatoirement
 - une des 8 images (la combinaison de $2 * 2 * 2$ images)
 - un des 8 mots dans la *wordList*
- Peut être configuré avec
 - un préfix et 8 images personnalisée, en copiant depuis la sortie de *images.py*
 - une liste de 8 mots qui sont ajoutés aléatoirement

Recherche sur les blockchains



Cryptographie
Asymétrique

SUDOKU									ANSWER:								
2	9				6				2	1	9	5	4	3	6	7	8
4		8	7			1	2		5	4	3	8	7	6	9	1	2
8			1	9		4			8	7	6	2	1	9	3	4	5
3		7			8		1		4	3	2	7	6	5	8	9	1
6	5				8		3		7	6	5	1	9	8	2	3	4
1			3			7			1	9	8	4	3	2	5	6	7
		6	5		7		9		3	2	1	6	5	4	7	8	9
6	4					2			6	5	4	9	8	7	1	2	3
8		3		1	4	5			9	8	7	3	2	1	4	5	6

Proof-of-work



Blockchain

Création d'un
système de paiement
décentralisé



Mining Reward



Gestion des clés



Lenteur du système

Limitations des choix de Satoshi

SUDOKU								
2	9		6					
4		8	7		1	2		
8			1	9	4			
3		7		8	1			
6	5			8	3			
1			3		7			
		6	5	7	9			
6	4				2			
8		3	1	4	5			

ANSWER:								
2	1	9	5	4	3	6	7	8
5	4	3	8	7	6	9	1	2
8	7	6	2	1	9	3	4	5
4	3	2	7	6	5	8	9	1
7	6	5	1	9	8	2	3	4
1	9	8	4	3	2	5	6	7
3	2	1	6	5	4	7	8	9
6	5	4	9	8	7	1	2	3
9	8	7	3	2	1	4	5	6

Consommation
d'énergie



Trop de
mineurs



Gestion des clés

Perte de la clé privée

- Plus de transactions
- Pas de banque centrale pour refaire le NIP / la clé privée

Envoyer vers la mauvaise adresse (clé publique)

- Immuabilité de la transaction -> on ne peut pas la changer!
- Les jetons sont perdus
- Pas de banque centrale pour rediriger les fonds



Lenteur du système

19h03



1 nouveau bloc
tout les 10'

3600
transactions
dans un bloc

6 transactions
par seconde au
niveau mondial



Trop de mineurs

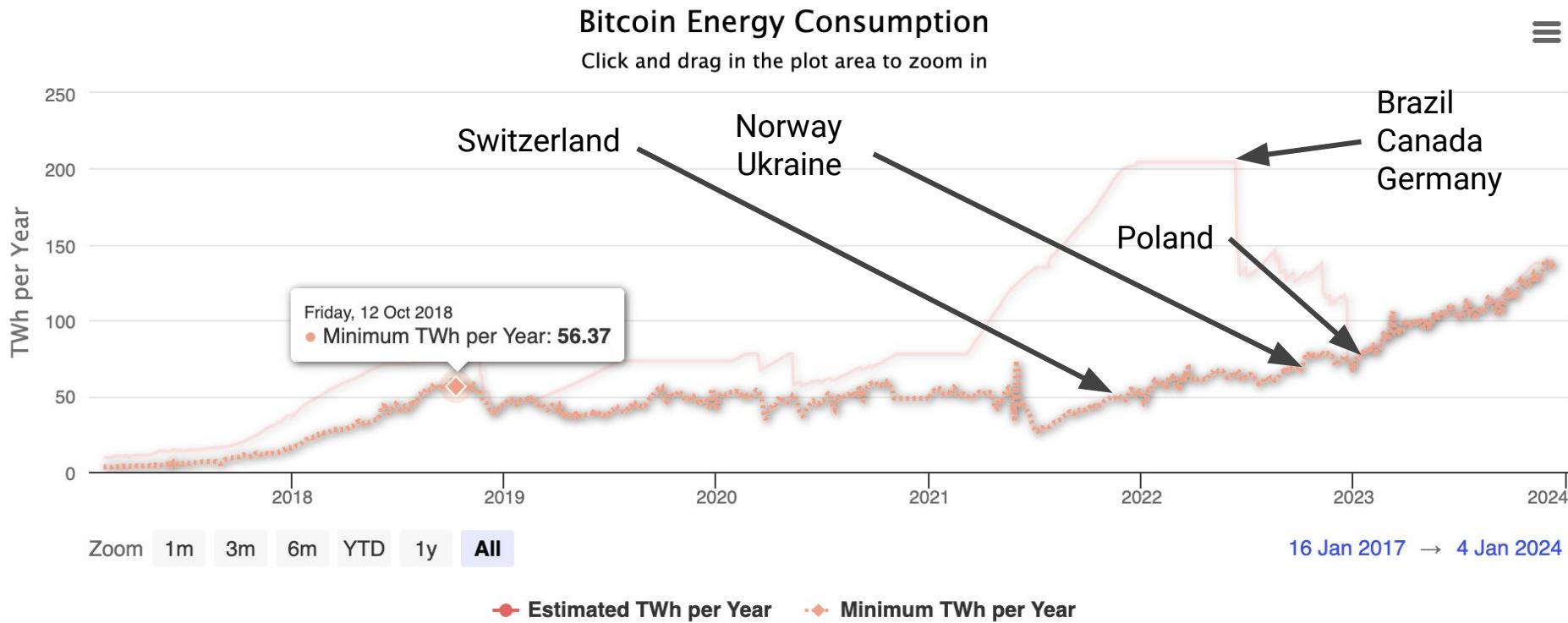
Impossible de miner ses propres bitcoins maintenant:

- Il faut les acheter
- C'est devenu un jeton spéculative





Consommation d'énergie excessive





Gestion des clés



Vitesse:
Nouveaux protocols

Etat des blockchains 2024

SUDOKU									ANSWER:								
2	9				6				2	1	9	5	4	3	6	7	8
4		8	7			1	2		5	4	3	8	7	6	9	1	2
8			1	9		4			8	7	6	2	1	9	3	4	5
3		7			8		1		4	3	2	7	6	5	8	9	1
6	5				8		3		7	6	5	1	9	8	2	3	4
1			3			7			1	9	8	4	3	2	5	6	7
		6	5		7		9		3	2	1	6	5	4	7	8	9
6	4					2			6	5	4	9	8	7	1	2	3
8		3		1	4	5			9	8	7	3	2	1	4	5	6

Energie:
Proof of Stake



Trop de
mineurs



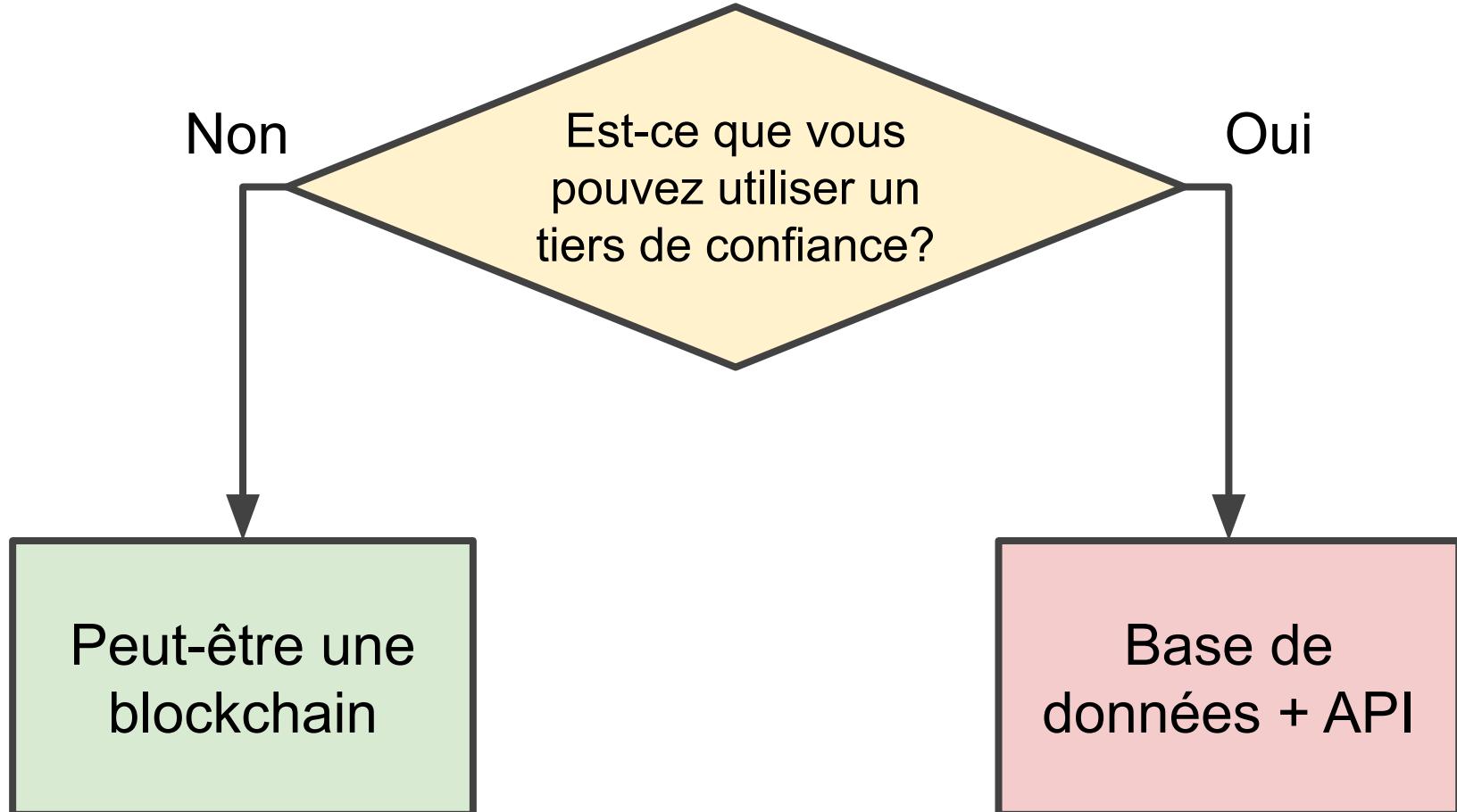
Utilisation des blockchains

Economique

- Spéculation, surtout Bitcoin
- DeFi - Decentralized Finance
 - Place de jeu pour nouveaux algorithmes
 - Echange entre banques
- Payment pour tout le monde
 - Pas assez rapide
 - Trop compliqué (clés privées)
 - Pas assez d'avantages

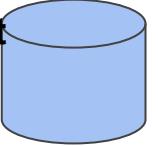
Décentralization

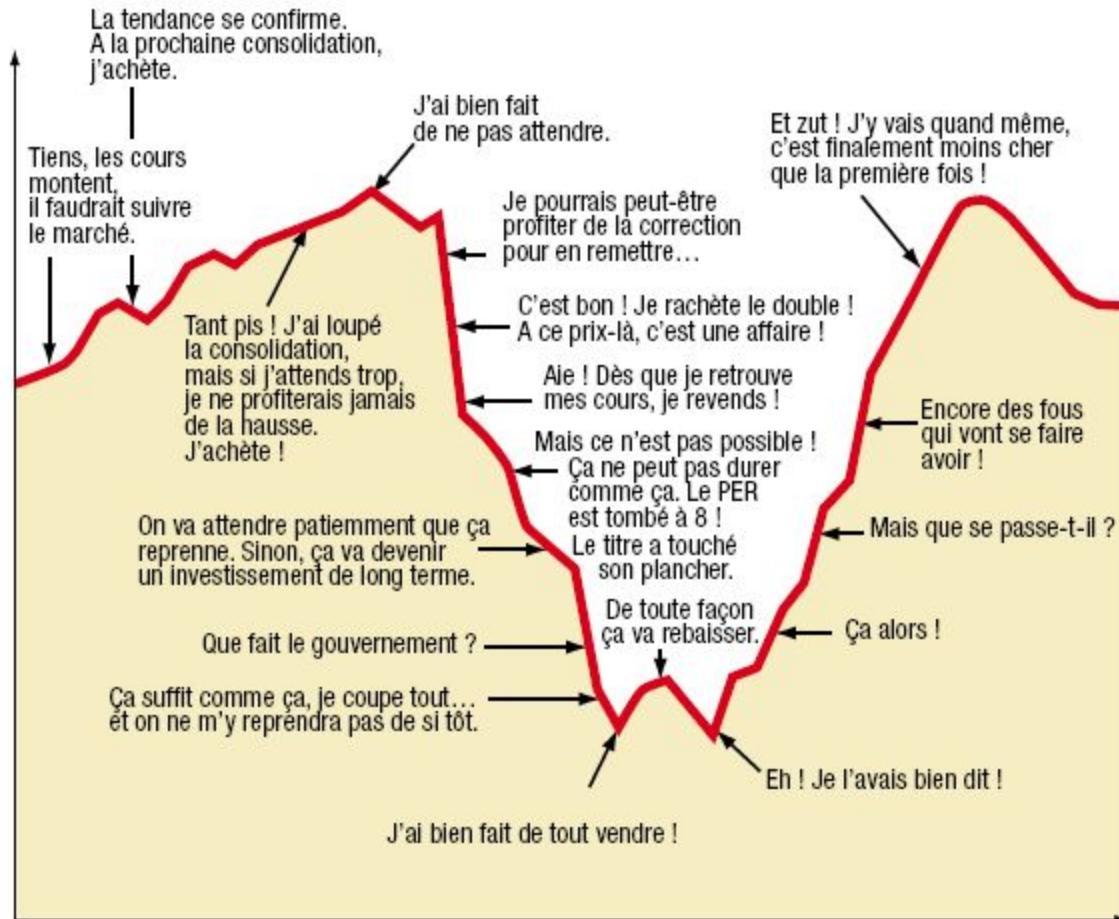
- Déléguer la confiance à plusieurs
- Nouvelles façon de sécuriser
- Rarement besoin d'une blockchain
 - Email
 - HTTPS
 - DNS
- Un contre-exemple
 - Fledger - vaporware et idées du présentateur





Décentralisations dans les blockchains

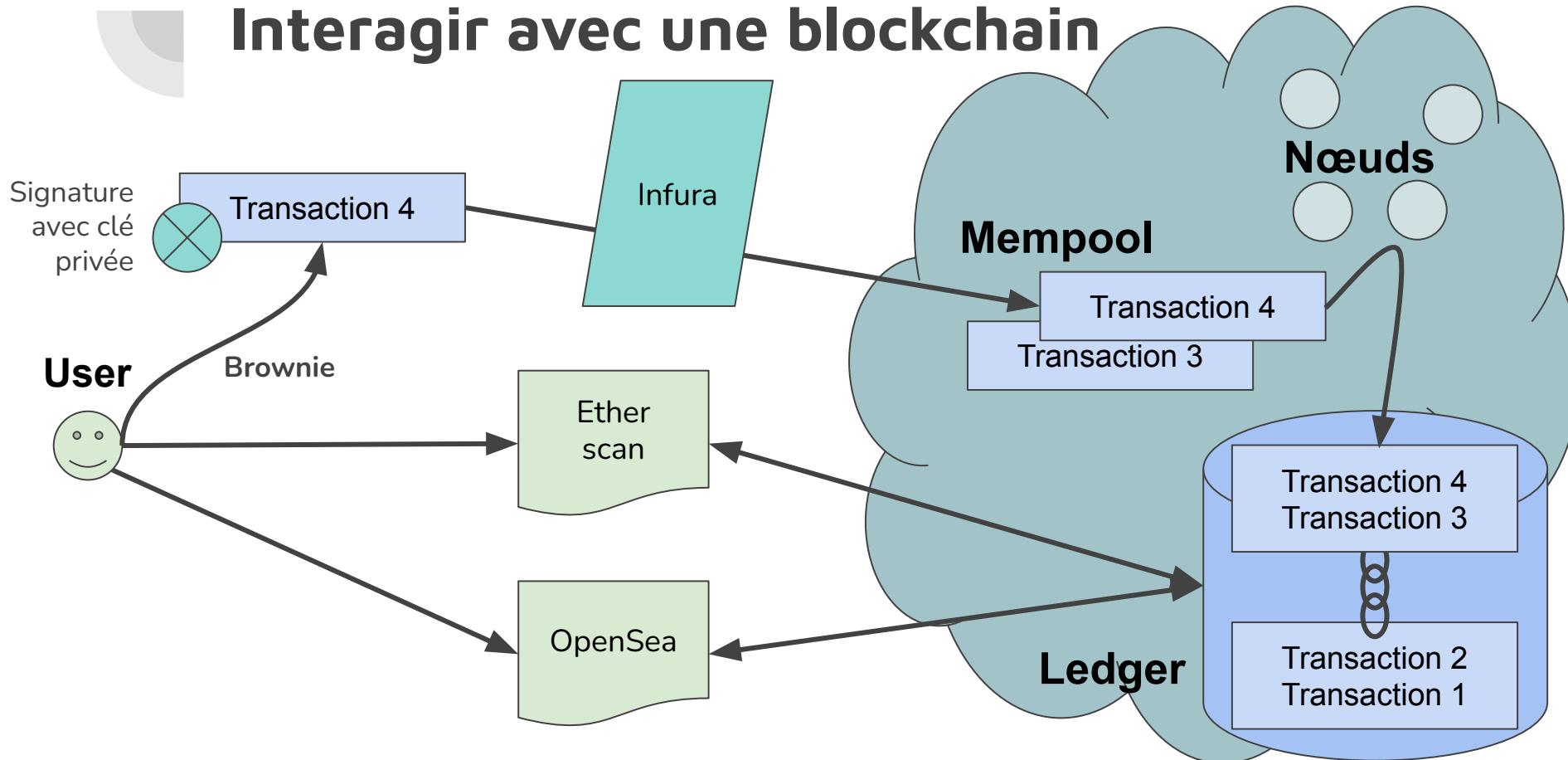
		Centralisé	Décentralisé
Gouvernance des nœuds 	Qui a le droit d'ajouter de nouveaux nœuds?	<i>Permissioned</i>	Google Cloud - une liste centrale <i>Unpermissioned</i> Bittorrent - tout le monde peut se joindre
Accès des utilisateurs 	Comment ajouter les nouveaux utilisateurs?	<i>Private</i>	EPFL email - il faut être embauché <i>Public</i> Gmail - tout le monde peut s'inscrire
État 	Qui peut changer les données?	<i>Central</i>	Windows Server - Accès administrateur <i>Shared</i> Google Cloud - vérification de l'accès



Source : Analyse technique. Théories et méthodes, Thierry Béchu, Eric Bertrand et Julien Nebenzahl

Comment utiliser les NFTs

Interagir avec une blockchain





V.2 - Utiliser SismondiNFT

Installer le contrat sur la blockchain de test Sepolia

- Noter l'adresse du contrat dans NOTES_NFTs

Minter un ou plusieurs NFTs

- Noter l'id - ça devrait commencer avec le 0

Regarder avec Etherscan

- Utilisez la chaîne Sepolia!
- Entrez l'adresse du contrat



V.2 - Visualiser un NFT sur OpenSea et le wallet

OpenSea

- Se connecter avec le wallet
- Entrer l'adresse publique de votre compte Metamask
- Visualiser les NFTs du contrat

Wallet

- On peut seulement ajouter des NFTs qui sont liés à l'adresse
- Vous pouvez les transférer à une autre adresse
- Malheureusement l'affichage ne marche pas



V.3 - Qui est le/la propriétaire d'un NFT?

Pour être propriétaire d'un NFT

- Il faut connaître l'adresse du contrat du NFT
- Il faut avoir l'id du NFT
- Le NFT doit être lié à votre clé publique

En tant que propriétaire, vous pouvez

- Transférer le NFT à un nouveau propriétaire

Résumé



Blockchain - définition

Une blockchain permet de stocker de l'information de façon *publique* et *permanente*: tout le monde peut lire l'information, et personne ne peut l'enlever. Un ensemble d'ordinateurs appelés *nœuds* gèrent la blockchain. Ils créent un *consensus* sur toute nouvelle information à publier en appliquant des *règles précises*.



NFT - définition

Un *Non Fungible Token* (NFT), parfois appelé *jeton numérique*, est défini par un *smart contract* sur une blockchain. Les NFTs permettent de transférer des *droits d'utilisation* entre des comptes. Certains NFTs offrent aussi une approche *ludique* pour créer des nouvelles œuvres d'art.



Liens

- Leçons sur les blockchains: [Introduction](#) - [Technique](#)
- [Article blockchains](#) du chambre vaudois de commerce et de l'industrie
- [Présentations blockchains](#) et utilité en Suisse (Anglais)
- [RTS découverte](#) sur les blockchains
- Une blockchain de recherche: [Fledger](#)
- Central Bank Digital Currency (CBDC) de [l'Union Européenne](#)
- La [régulation de la Finma](#) pour les blockchains
- Nouvelles des projets cassés: [Web 3 is going great](#)
 - 4 milliards US-\$ dans une année de pertes et fraudes pour
 - 10 milliards US-\$ d'investissements en "venture capital"
- Liste de la valuation des blockchains: [CoinMarketCap](#)