

La Blockchain : de la Cryptomonnaie au Web 3

Najah NAFFAH

Quantum Blockchain Secure

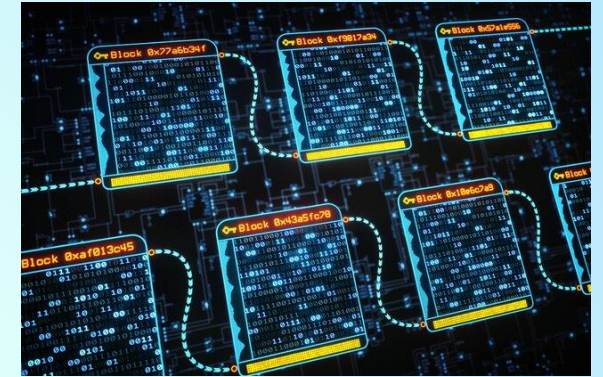
27 Mars, 2023

Rappel des Questions

- Blockchain
 1. Comment ça marche? (avec un glossaire, vu l'abondance des sigles)
 2. A quoi ça sert (hors cryptomonnaies)
- Cryptomonnaies
 1. Comment ça marche ?
 2. Avantages et inconvénients ?
 3. Perspectives ?
- Description de l'environnement permettant d'utiliser les cryptomonnaies
- Quels sont les déterminants économiques de leur valeur ?
- Quelle pourrait être l'influence la limitation du nombre de bitcoins sur l'évolution de sa valeur ?

Sommaire

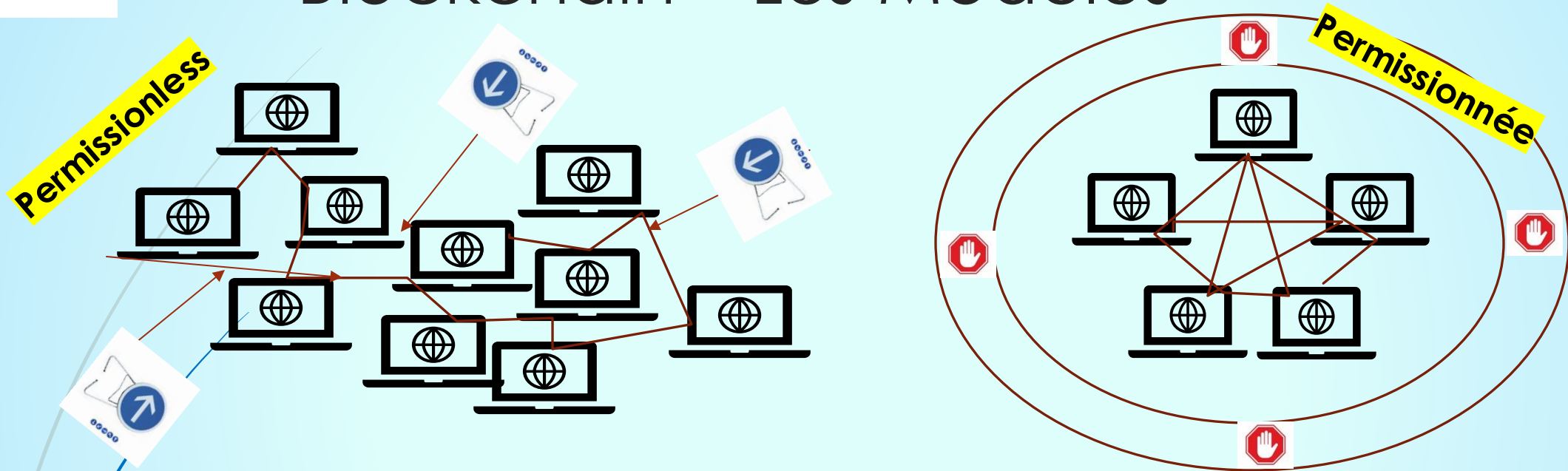
- Définitions – concepts clefs
- La Blockchain
- La Cryptomonnaie – Le Bitcoin
- Les Blockchains Programmables – un nouvel espace d'applications décentralisées
- Les Blockchains d'Entreprise
- Les Tendances les plus récentes
 - La DeFi
 - Les NFT
 - L'Identité
 - Le Web 3
- Perspectives -



Glossaire

- **Cryptomonnaie** – monnaie digitale minée par algorithme et acceptée par les citoyens et les commerçants, sans intermédiaire financier
- **La Blockchain** – base de données à copies multiples, résiliente, composée d'une chaîne de blocs (transactions groupées) liés cryptographiquement – **permissionless & permissionnée**
- **Le Consensus** – se mettre d'accord sur l'état de la base de données de la Blockchain entre valideurs qui ne se connaissent pas (trustless)
- **Minage** – générer de la monnaie suite à un acte réussi de validation
- **Décentralisation** – système non hiérarchisé, sans autorité centrale, administré par consensus entre les participants
- **dApps- Applications décentralisées** - nouvelle gamme d'applications où l'utilisateur est au centre: échange de valeur, notariation, ancrage, preuve, lutte contre le Fake,...(DeFi, et autres)
- **Smart Contracts** - programmes déterministes déployés sur la Blockchain pour exécuter des fonctions sous certaines conditions
- **Wallet/portefeuille numérique** – permet l'accès à la Blockchain, soumettre des transactions, gère les clefs de l'utilisateur
- **Les Tokens/jetons – (FT, NFT)** représentation digitale d'un actif et manipulés par des Smart Contracts – Fongibles FT et non Fongibles NFT
- **Le Web 3** – Stack technologique regroupant des outils et des applications décentralisées (reprise de contrôle par l'utilisateur)

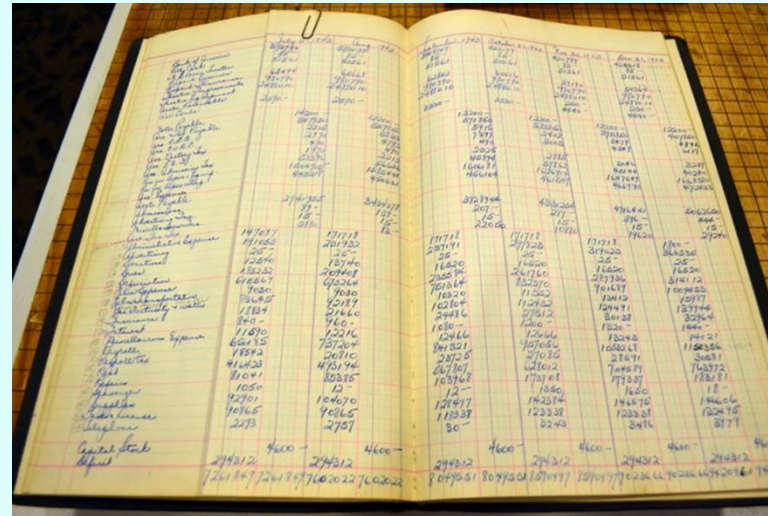
Blockchain – Les Modèles



- **Blockchain Permissionless** – liberté de rejoindre le réseau en téléchargeant le logiciel de nœud sans autorisation mais en suivant les règles prédéfinies dans le logiciel
- **Blockchain Permissionnée** – passer par un processus d'onboarding (avec autorisation/qualification) afin de faire partie du réseau de nœuds

Une Blockchain – Raison d'être ?

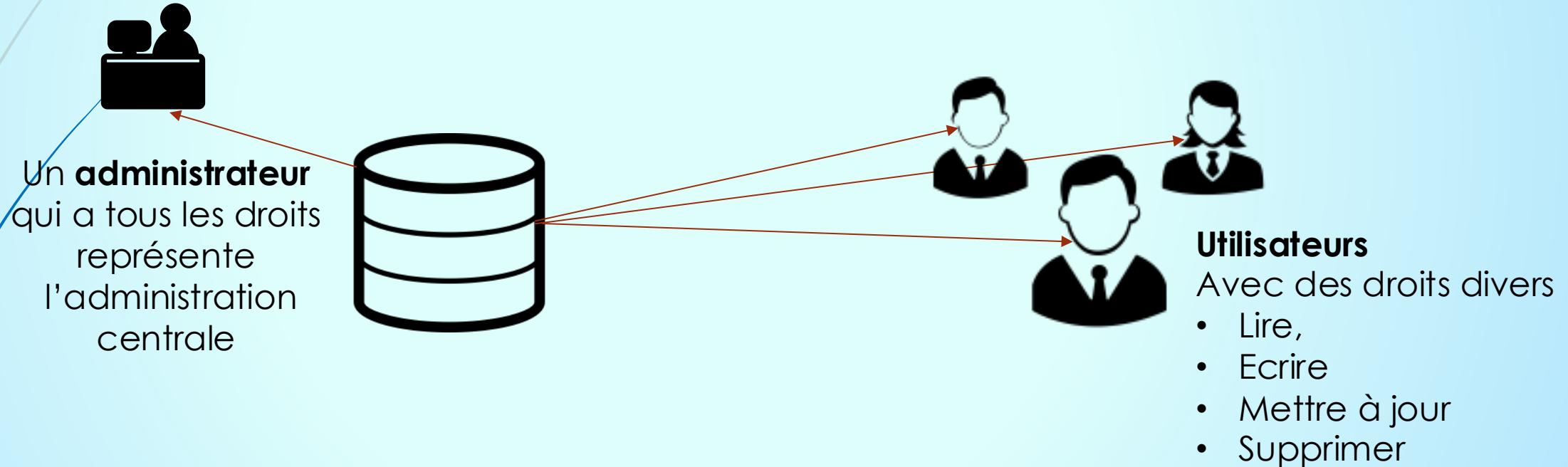
**Un Livre
Comptable**



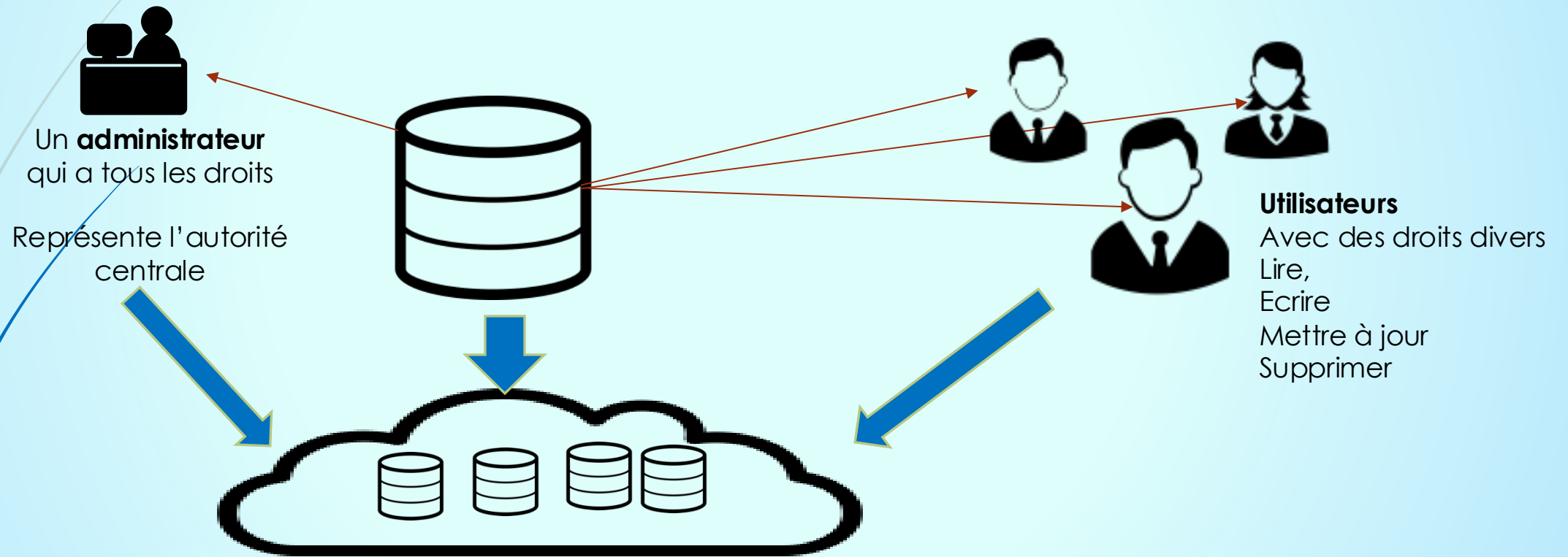
Ledger

**une Base de Données
Développée sur une technologie qualifiée de
- DLT (Distributed Ledger Technology)
- ou Blockchain**

Rappel – Qu'est ce qu'une Base de Données dans l'informatique Classique



Rappel – Une BD Classique et sa version distribuée



Peut exister sous forme distribuée dans un cloud mais avec la même Logique Opérationnelle – Administrateur unique dépendant d'une autorité centrale Et des utilisateurs qui ont des droits et obligations

Qu'est ce qu'une Blockchain ?

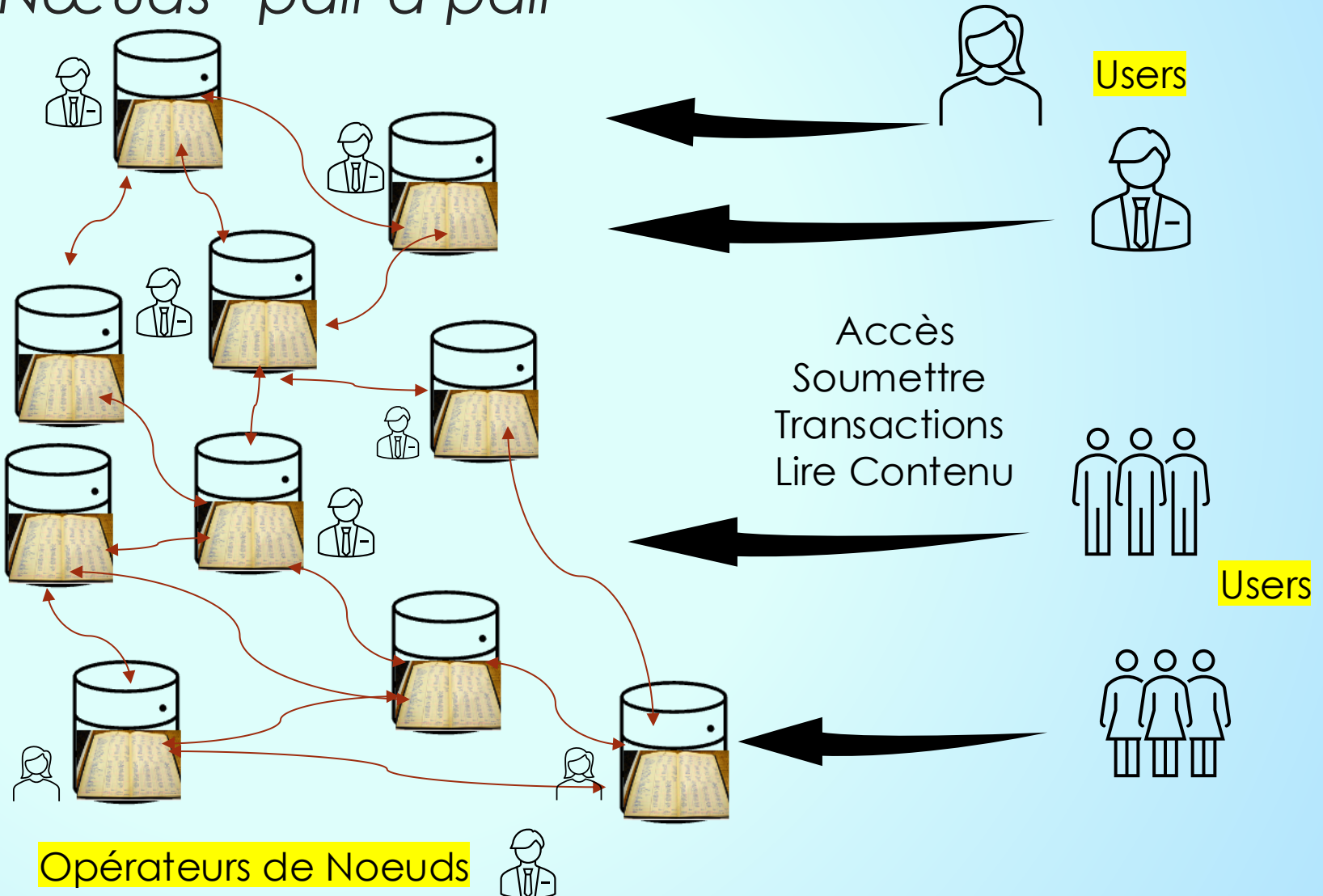
Réseaux de Nœuds "pair à pair"

Même Copie
(tous les Nœuds)

Blocs chaînés
(append-only)

Immuable,
Transactions publiées
(non modifiables)

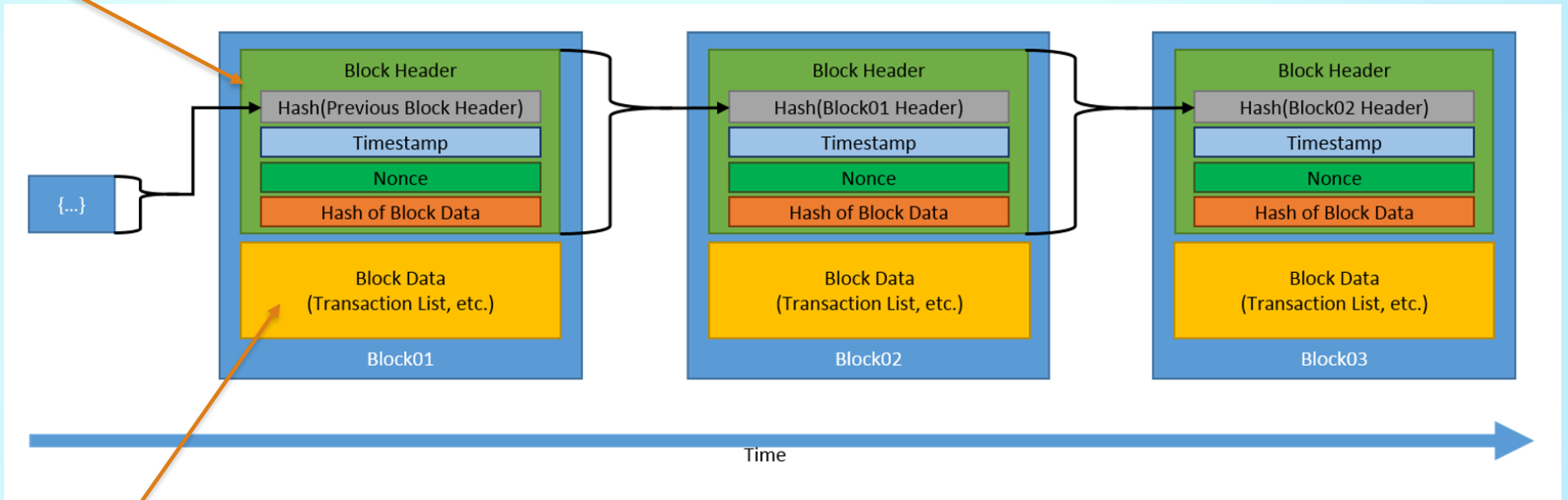
Tous les Blocs et les Tx et
le chaînage sont
Sécurisés par
Cryptographie



Chaînage des Blocs



Entête de Bloc
Informations
Chaînage



Transactions soumises
Validées

Alice commande un café à Bob à Auteuil « Bob's Café »

Bob affiche le prix en
€ ou en Satoshis ,
(1,5 € ou 5000 satoshis)
Alice choisit de payer en
Bitcoin



Un QR code « demande de
paiement » généré par l'appareil
du vendeur, et scanné par Alice
avant d'appuyer sur Envoi

Facilité d'usage

Alice commande un café à Bob à Auteuil – *Diffusion dans le réseau*

Bob affiche le prix en €
ou en Satoshis ,
(1,5 € ou 5000 satoshis)
Alice choisit de payer en
Bitcoin



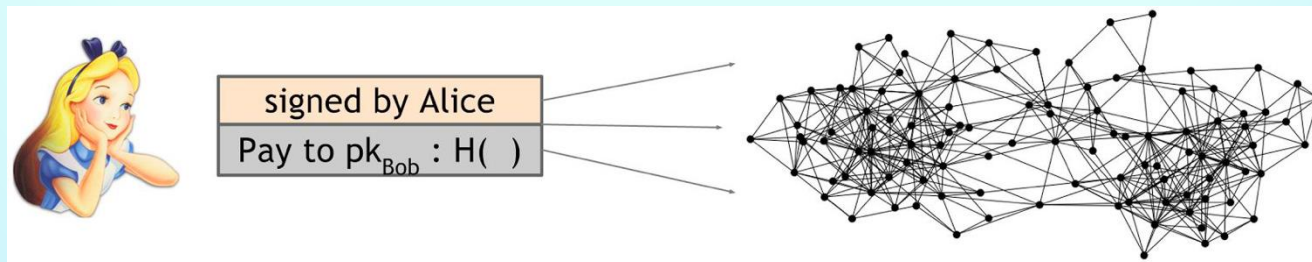
Un QR code « demande de
paiement » généré par l'appareil
du vendeur, et scanné par Alice
avant d'appuyer sur Envoi
(Alice avait au préalable reçu 0,1
Bitcoin reçu de Joe)

A Bitcoin address: "1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA »

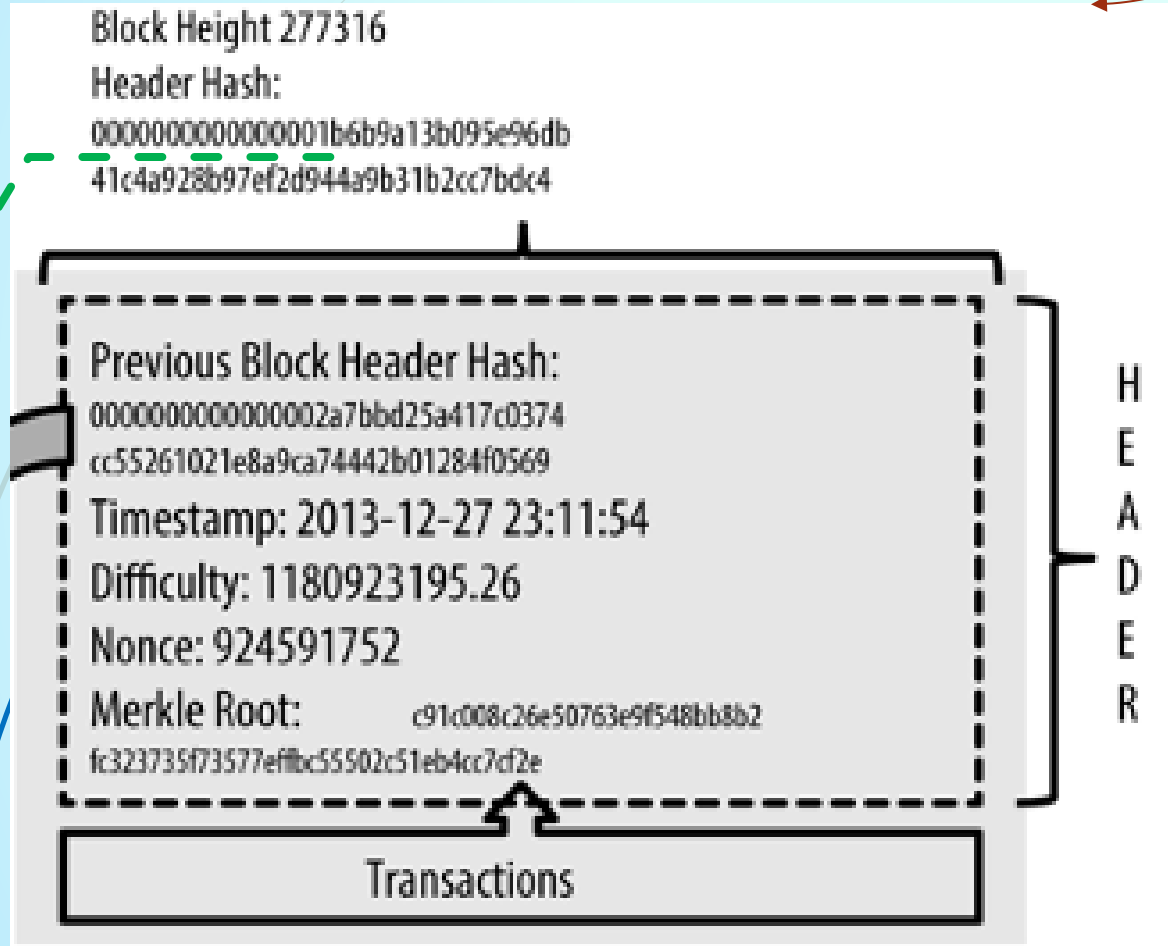
The payment amount: "5000 S"

A label for the recipient address: "Bob's Cafe"

A description for the payment: "Purchase at Bob's Cafe"



Un Zoom sur la Chaîne de Blocs



Plus il y a des zéros, plus c'est difficile à trouver

Block Height 277316
Header Hash:
0000000000000001b6b9a13b095e96db
41c4a928b97ef2d944a9b31b2cc7bdc4

Previous Block Header Hash:
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569

Timestamp: 2013-12-27 23:11:54
Difficulty: 1180923195.26
Nonce: 924591752

Merkle Root: c91c008c26e50763e9f548bb8b2
fc323735f73577effbc55502c51eb4cc7d2e

H
E
A
D
E
R

Transactions

Block Height 277315
Header Hash:
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569

Previous Block Header Hash:
00000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249

Timestamp: 2013-12-27 22:57:18
Difficulty: 1180923195.26
Nonce: 4215469401

Merkle Root: 5e049f4030e0ab2debb92378f5
3c0a6e09548aea083f3ab25e1d94ea1155e29d

Transactions

Block Height 277314
Header Hash:
00000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249

Previous Block Header Hash:
00000000000000038388d97cc6f2c1d
fe116c5e879330232f3bff1c645920bdf

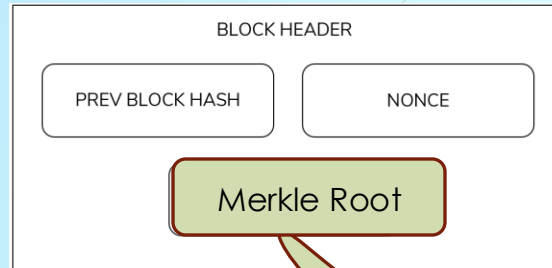
Timestamp: 2013-12-27 22:55:40
Difficulty: 1180923195.26
Nonce: 3797028665

Merkle Root: 02327049330a25d4d17e53e79f
478cb79c53a509679b1d8a1505c5697afb326

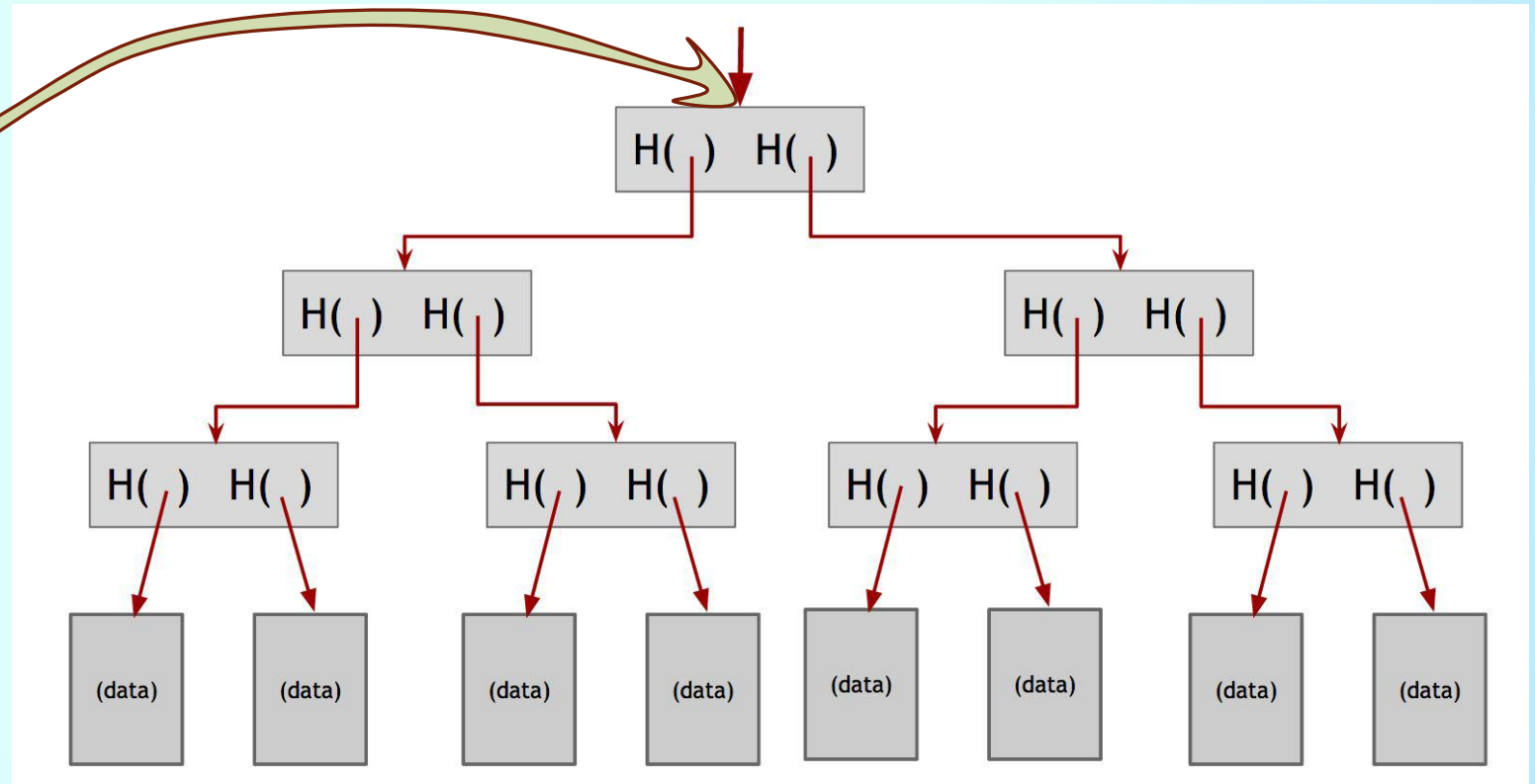
Transactions

Blockchain Data Structure

Backup



blockID refers to the hash of the concatenated components
 $\text{blockID} = H(\text{blockHeader}) = H(\text{prevBlockHash} \parallel \text{merkleRoot} \parallel \text{nonce})$



In a Merkle tree, data blocks are grouped in pairs and the hash of each of these blocks is stored in a parent node. The parent nodes are in turn grouped in pairs and their hashes stored one level up the tree. This continues all the way up the tree until we reach the root node.

Le Bitcoin

Le Début de la Cryptomonnaie Peer to Peer

L'Annonce de Satoshi ...

Il y a **14 ans et demi (Oct. 2008)**, Satoshi Nakamoto a annoncé publiquement dans un email la diffusion de l'article sur le cash électronique

➡ **“I’ve been working on a new electronic cash system that’s fully peer-to-peer, with no trusted third party.”**

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshi@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.

Le Bitcoin – Historique -1

- Le Bitcoin a été Inventé en 2008, avec la publication de l'article « **Bitcoin: A Peer-to-Peer Electronic Cash System** » sous le pseudo **Satoshi Nakamoto**
- Il s'est inspiré d'inventions antérieures **b-money** et **HashCash** pour concevoir une monnaie complètement décentralisée qui ne s'appuie sur aucune autorité centrale: **création, dépense, paiement, validation...**
- L'invention clef est dans le traitement informatique du consensus appelé « **Proof of Work** » ou *preuve de travail*, qui permet de:
 - Valider les transactions (pas de double dépense)
 - Se mettre d'accord sur l'état des transactions validées
 - Générer chaque 10 minutes (environ) des nouveaux bitcoins

Le Bitcoin – Historique -2

- Le réseau Bitcoin a été « **mis en production** » 2009, sur la base d'une implémentation de référence publiée par Nakamoto et révisée depuis par de nombreux autres programmeurs.
- La mise en œuvre de l'algorithme de "**Proof of Work**" ou preuve de travail (minage) qui assure la sécurité et la résilience du bitcoin a augmenté de **façon exponentielle** et dépasse désormais la puissance de traitement combinée des meilleurs HPC (ordinateurs haute performance) du monde.
- La valeur totale du marché du bitcoin a parfois dépassé **1000* milliards** de dollars américains.
- La plus grosse transaction traitée à ce jour s'élève à **1,1 milliard de dollars** américains, transmise instantanément et traitée pour un coût de **0,68 dollar**

* 24 Mars 18:40 – Mcap 535.407.543,351 \$

Le Bitcoin – Historique - 3



- Satoshi Nakamoto s'est **retiré du public** en avril 2011, laissant la responsabilité du développement du code et du réseau à un groupe de **volontaires** (bénévoles).
- **L'identité** de la ou des personnes à l'origine de Bitcoin est toujours **inconnue**.
- Cependant, ni Satoshi Nakamoto ni personne d'autre **n'exerce de contrôle individuel sur le système Bitcoin**, qui fonctionne sur la base de principes mathématiques totalement transparents, d'un **code open source** et d'un **consensus résilient** entre les participants.
- L'invention elle-même est **disruptive** et a déjà donné naissance à de nouveaux domaines dans *l'informatique distribuée (Web3)*, *l'économie (Cryptocurrencies)* et la *gouvernance des organisations (DAO)*

Depuis le 26 avril 2011....10:29

Backup

- Après l'envoi du mail ci-dessous, Satoshi Nakamoto entre dans un Silence total !
 - ***I've moved on to other things. It's in good hands with Gavin and everyone***
- Qui est Gavin ?
- Gavin Andresen was the lead developer for a part of the bitcoin digital currency project, working to create a secure, stable "cash for the Internet."

Subject: alert key

Satoshi Nakamoto satoshin@gmx.com

26 Apr. 2011, 10:29

I've moved on to other things and will probably be unavailable. Here's the CAlert key and broadcast code in case you need it. You should probably give it to at least one or two other people. There are a few long-time users who are always around all the time.

Une Comparaison avec le \$ ou l'€

FIAT DOLLARS

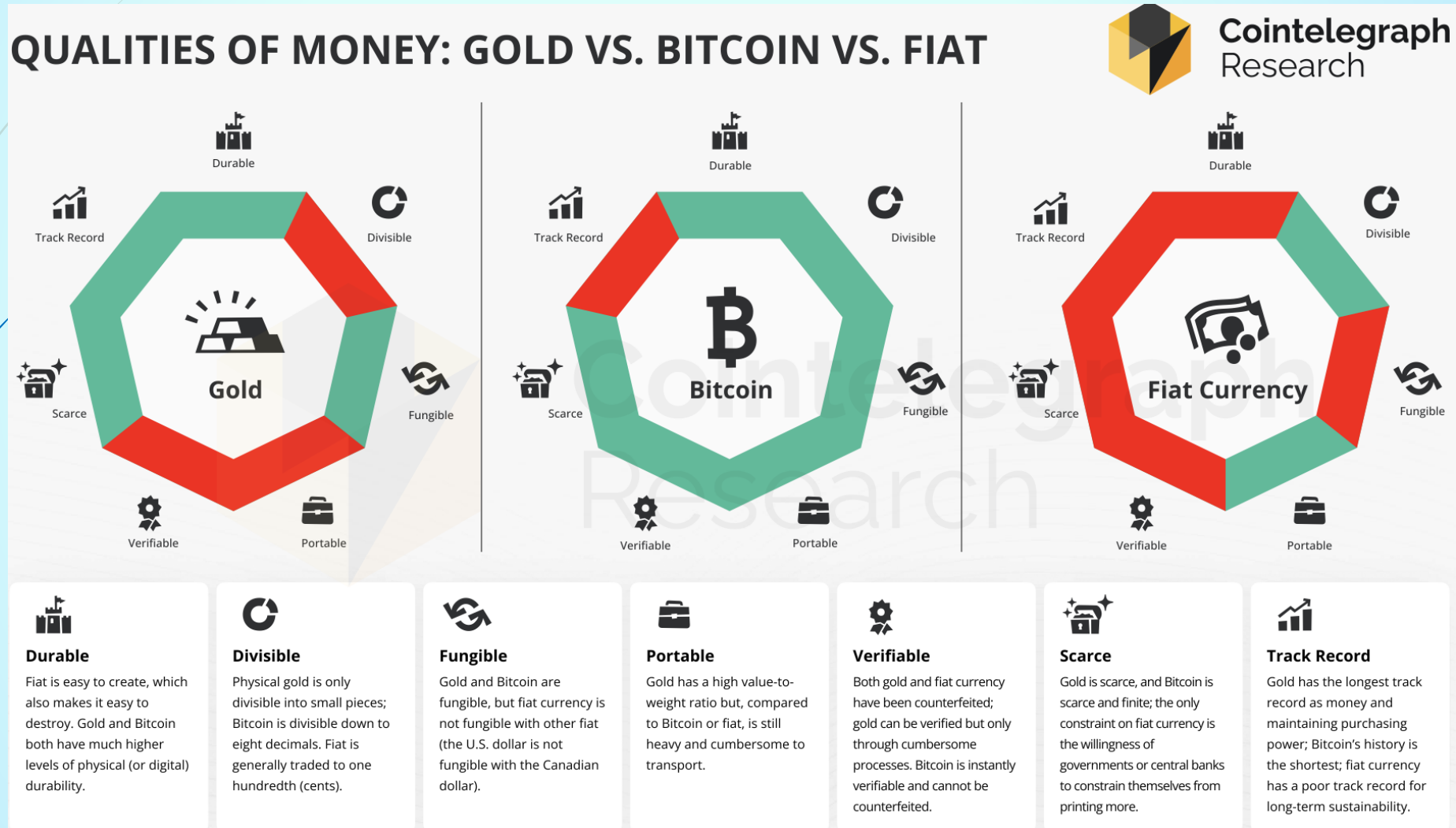
- \$ Issued and distributed by the government
- \$ Commonly counterfeited
- \$ Unlimited supply
- \$ Susceptible to fraud
- \$ High global transfer fees, slow transfer times
- \$ Banks operate weekdays 9-5, closed on weekends and holidays

BITCOIN

- ฿ Secured by cryptography and energy
- ฿ Impossible to counterfeit
- ฿ Fixed supply at 21 million
- ฿ Private and secure
- ฿ Low universal fees, fast transaction times
- ฿ Open and accessible 24/7



Comparison Or, Fiat(\$/€), Bitcoin



La Courbe de Minage Génération des Bitcoins

Tous les 4 Ans:

210.000 Blocks, validés et chaînés
Rémunération/bitcoins minés diminue de 50%

50 - 25 - 12,5 - **6,25** - 3,125....

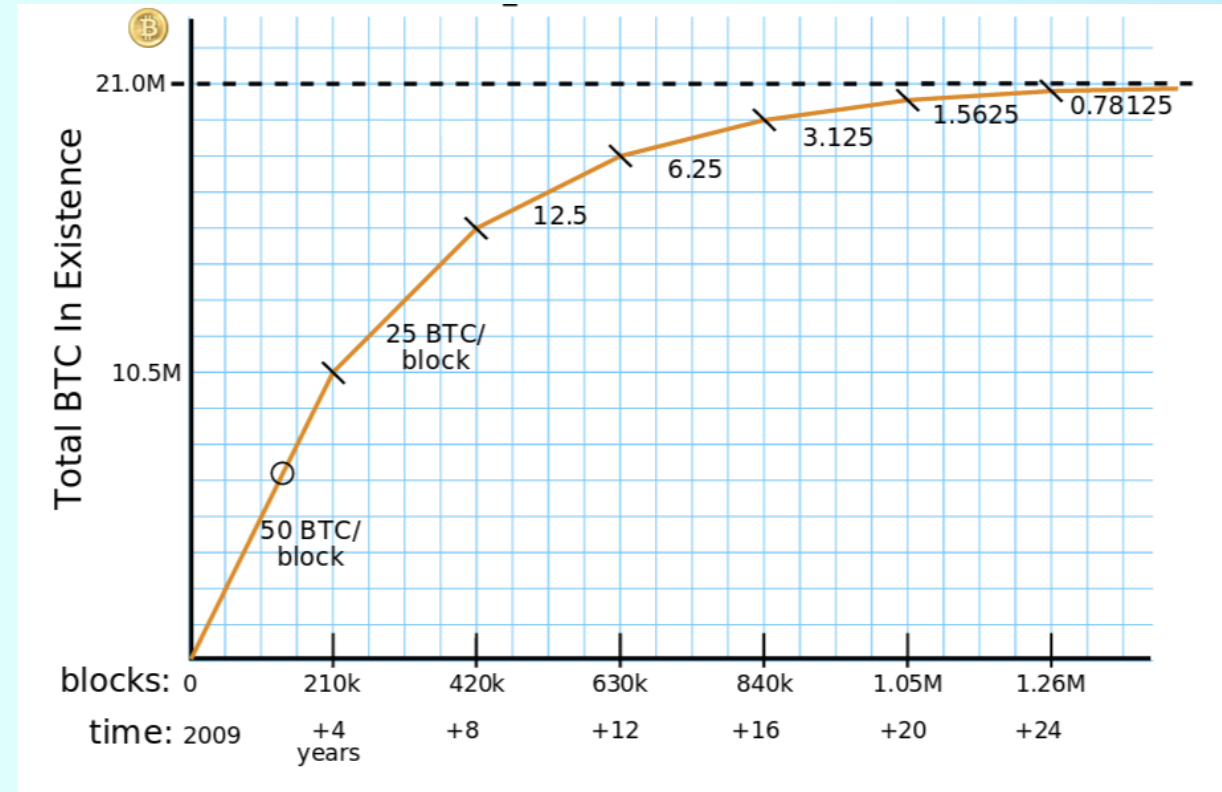
1/1/2009 - 50

11/2012 - 25

.....

05/2020 - 6.25

.....

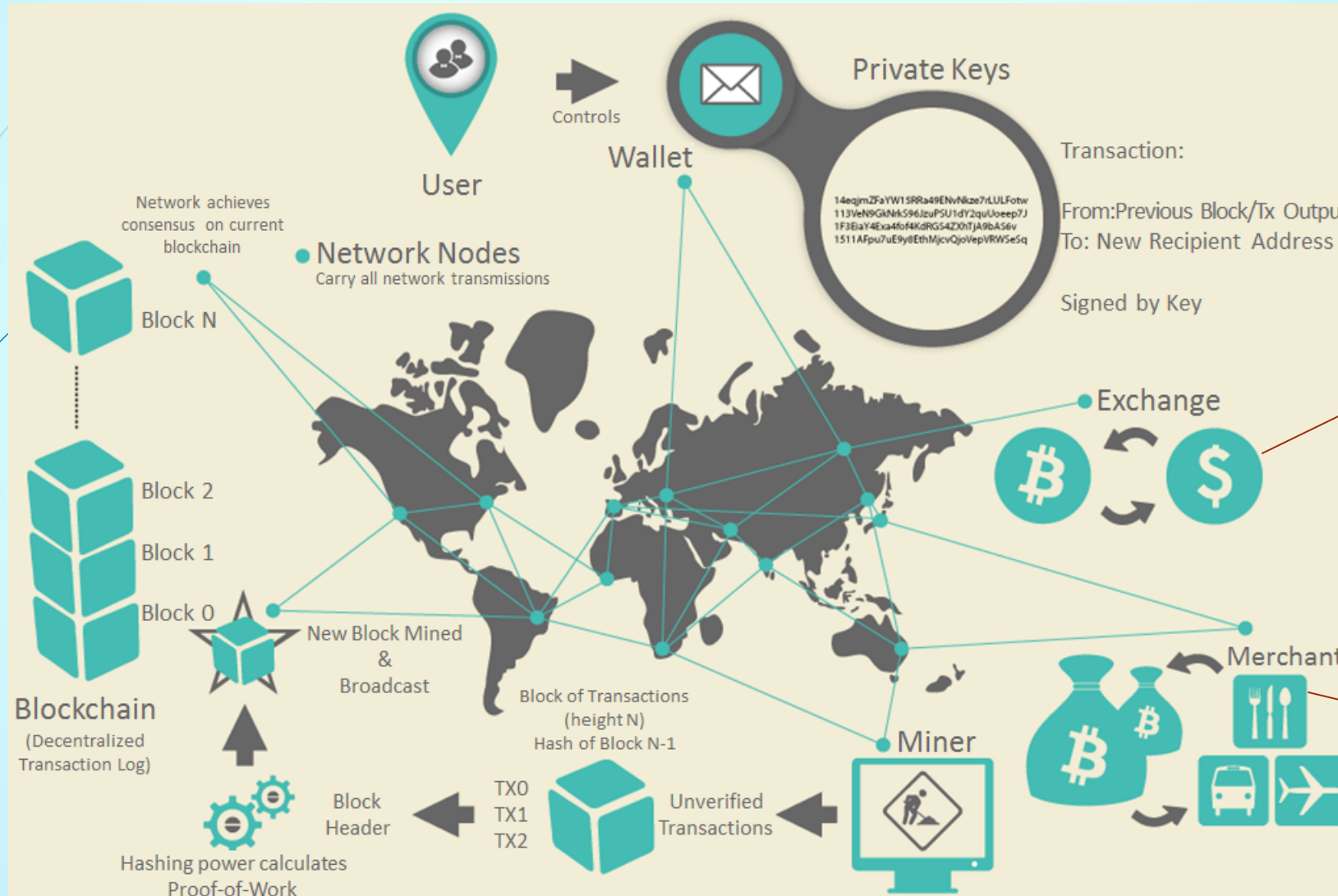


In 2140, 21 million bitcoins, auront été minés

Le minage se fait par une transaction spéciale écrite par le valideur;

Coinbase transaction: **Pay Jing's address 25.09094928 bitcoin**

L'écosystème du Bitcoin



Nombreux
273

Très peu
Nombreux

08:40

en.m.wikipedia.org

Jan 2009 – Mar 2010	basically nothing	No exchanges or market, users were mainly cryptography fans who were sending bitcoins for hobby purposes representing low or no value. In March 2010, user "SmokeTooMuch" auctioned 10,000 BTC for \$50 (cumulatively), but no buyer was found. ^[151]
May 2010	less than \$0.01	On 22 May 2010, ^[152] Laszlo Hanyecz made the first real-world transaction by buying two pizzas in Jacksonville, Florida , for 10,000 BTC, an amount that would surpass \$600 million if held in April 2021. ^[153]
Feb 2011 – April 2011	\$1.00▲	Bitcoin takes parity with US dollar. ^[154]
Nov 2013	\$350–\$1,242▲	Price rose from \$150 in October to \$200 in November, reaching \$1,242 on 29 November 2013. ^[155]

Some History

On s'amuse

- May 22, 2010, **Laszlo Hanyecz** purchased \$25 worth of pizza for 10,000 BTC
- Fun fact: 10,000 BTC is now equivalent to ~\$81,000,000
- **World's first ever Bitcoin transaction for a tangible asset**
- Bitcoin went from worthless internet money to something with real value

669 M\$
Oct. 2021



Parité \$

Ça bouge... 1242\$

16 February 2021	\$50,000 ▲	Bitcoin price reached new all-time high of \$50,000. ^[176]
10 April 2021	\$60,000 ▲	Bitcoin back above \$60,000 as Coinbase gets ready to go public on the stock market. ^[177]
14 April 2021	\$64,800 ▲	The all-time high price of \$64,800 was reached on April 14, 2021. ^[178]
19 May 2021	\$30,000 ▼	Bitcoin price drops to \$30,000 at one point following suggestions that Tesla has sold or will sell its Bitcoin holdings ^[179] and a new set of regulations from the Chinese government to support their cryptocurrency crackdown. ^[180]
2 September 2021	\$50,128 ▲	Bitcoin price recovered to \$50,000 ^[181]
17 October 2021	\$62,600 ▲	Bitcoin price returned near to ATH ^[182]
20 October 2021	\$66,974.77 ▲	Bitcoin price hits all-time high above \$66,000 ^[183]

50 k\$

66 k\$

Si Vous voulez Explorer le Bitcoin et d'autres coins...

Visiter les explorers (<https://bitinfocharts.com>) –
exemple BTC Nov 14, 2022

Nouveaux Bitcoins

19.206.626*
(vs 21 M)

Volatile
Fut 1 T

La Cadence

Bitcoin (Explorer, top100)	
Total	19,206,626 BTC
Price	1 BTC = 16,723.26 USD coinbasepro: 16,701.7 USD p2pb2b: 16,738.29 USD bitstamp: 16,708 USD bitfinex: 16,713 USD kraken: 16,695.6 USD 1 USD = 0.00006 BTC
Market Capitalization	\$321,197,372,960
Transactions last 24h	241,094
Transactions avg. per hour	10,046
Sent last 24h	467,498 BTC (\$7,818,085,492) 2.43% market cap
Sent avg. per hour	19,479 BTC (\$325,753,562)
Avg. Transaction Value	1.94 BTC (\$32,428)
Median Transaction Value	0.025 BTC (\$412.88)
Block Time	10m 17s
Blocks Count	763,130
Blocks last 24h	139
Blocks avg. per hour	6

Reward Per Block	6.25+0.1264 BTC (\$106,634.75)
Reward last 24h	868.75+17.57 BTC (\$14,822,230.13)
Difficulty	36.762 T
Hashrate	251.507 Ehash/s -15.76% in 24 hours
Mining Profitability	0.0589 USD/Day for 1 THash/s
Top 100 Richest	2,898,784 BTC (\$48,477,113,897) 15.09% Total
Wealth Distribution Top 10/100/1,000/10,000 addresses	5.95% / 15.09% / 33.77% / 57.12% Total
Addresses richer than 1/100/1,000/10,000 USD	34,555,307 / 13,228,504 / 5,038,641 / 1,309,307
Active Addresses last 24h	821,982
100 Largest Transactions	last 24h: 1,972,981 BTC (\$32,994,665,604) 422.03% Total
First Block	2009-01-09
Blockchain Size	491.50 GB
Reddit subscribers	4,698,827
Tweets per day	106,990
Github release	v23.0 (2022-04-25)
Github stars	66886
Github last commit	2022-11-10

Energie

La Genèse

Poids Social
(Elon)

*24 Mars 2023, 18:50, 19.326.643 BTC en circulation.

Bitcoin Rich List Oct 20, 2022

Backup

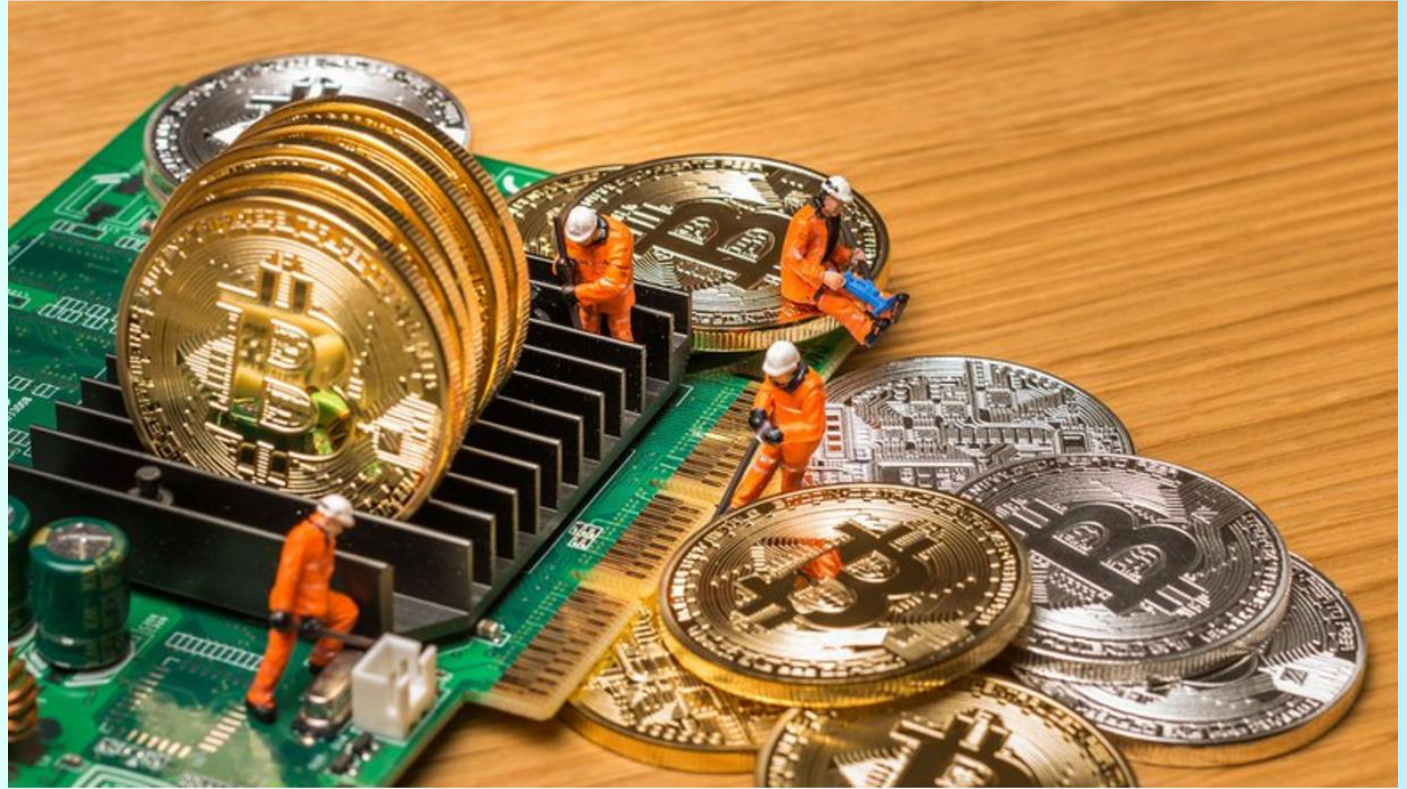
Bitcoin distribution					
Balance, BTC	Addresses	% Addresses (Total)	Coins	USD	% Coins (Total)
(0 - 0.00001)	3180318	7.29% (100%)	15.18 BTC	\$254,044	0% (100%)
[0.00001 - 0.0001)	8169115	18.73% (92.71%)	352.59 BTC	\$5,900,359	0% (100%)
[0.0001 - 0.001)	10461381	23.98% (73.98%)	4,028 BTC	\$67,409,829	0.02% (100%)
[0.001 - 0.01)	10732170	24.6% (50%)	40,695 BTC	\$681,001,670	0.21% (99.98%)
[0.01 - 0.1)	7097613	16.27% (25.39%)	234,475 BTC	\$3,923,782,856	1.22% (99.77%)
[0.1 - 1)	3044852	6.98% (9.12%)	945,637 BTC	\$15,824,629,662	4.92% (98.54%)
[1 - 10)	783075	1.8% (2.14%)	1,963,828 BTC	\$32,863,405,880	10.23% (93.62%)
[10 - 100)	135757	0.31% (0.35%)	4,353,745 BTC	\$72,857,157,922	22.67% (83.39%)
[100 - 1,000)	13786	0.03% (0.04%)	3,875,883 BTC	\$64,860,435,808	20.18% (60.72%)
[1,000 - 10,000)	1987	0% (0%)	4,696,870 BTC	\$78,599,125,112	24.46% (40.54%)
[10,000 - 100,000)	115	0% (0%)	2,399,361 BTC	\$40,151,776,068	12.49% (16.08%)
[100,000 - 1,000,000)	4	0% (0%)	689,423 BTC	\$11,537,059,731	3.59% (3.59%)

History

Addresses richer than						
\$1	\$100	\$1,000	\$10,000	\$100,000	\$1,000,000	\$10,000,000
34,555,307	13,228,504	5,038,641	1,309,307	210,656	23,691	3,860

1 bitcoin = 100 millions satoshis

Mining



Une nouvelle approche pour
créer une Monnaie

Répartition des centres de Minage

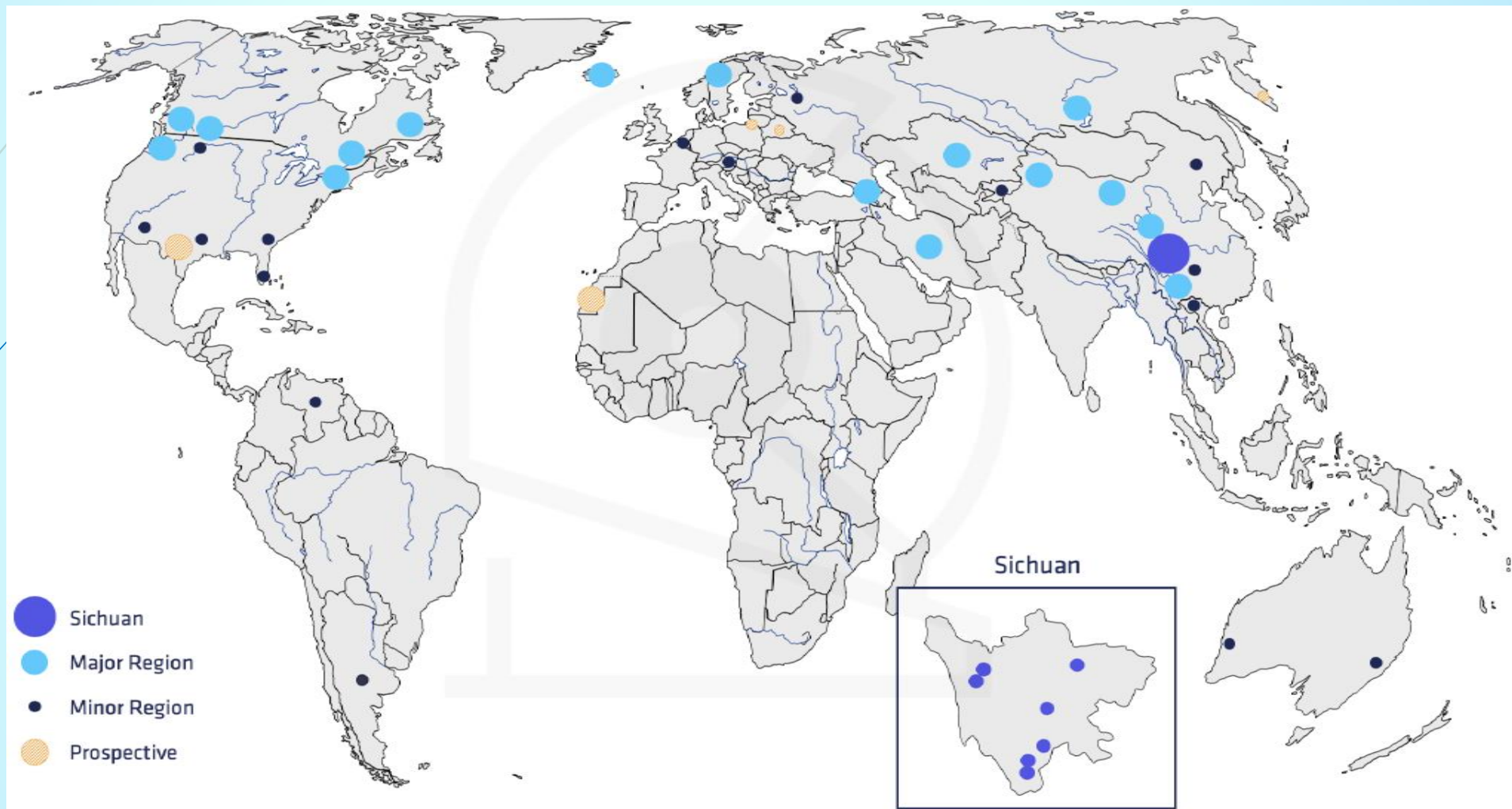


TABLE 1: TOTAL KNOWN POWER DRAW OF GLOBAL MINING COUNTRIES (DEC 2021)

Country	Total Known Power Draw (MW)
Azerbaijan	36
Canada	529
China	1
Georgia	38
Iceland	153
Kazakhstan	787
Norway	66
Russia	268
Sweden	80
United States	1,380
Sum	3,338

TABLE 2: TOTAL CARBON INTENSITY OF ALL GLOBAL MINING COUNTRIES (DEC 2021)

Region	Carbon Intensity (g/kWh)
Azerbaijan	638
Canada	234
China	318
Georgia	95
Global	492
Iceland	0
Iran	507
Kazakhstan	787
Malaysia	589
Norway	7
Russia	477
Sweden	19
United States	447
Weighted Average	466

Table 2 details the individual and weighted average carbon intensity scores of each individual mining country. All numbers reflect estimates as of December 2021.

Backup

Electricity



Production
26 730 TWh

Consumption
22 315 TWh
Bitcoin share
0.43%

Energy



Production
167 716 TWh

Bitcoin share*
0.15%

2nd Generation Blockchains –

Programmable Smart Contract Platforms , Market Cap

March 22, 2023 \$ 346 B

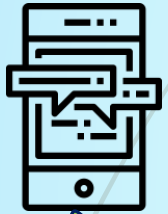
- ➔ **Ethereum (62,91 %)**
- ➔ BNB
- ➔ Cardano
- ➔ **Solana**
- ➔ **Polkadot**
- ➔ TRON
- ➔ **Avalanche**
- ➔ Cosmos
- ➔ Ethereum Classic
- ➔ **Aptos**
- ➔ (11)... Hedera, Near, VeChain, Algorand, Stacks
- ➔ **Tezos** (20) Market Cap 1,08 B\$ (XTZ = 1,16\$)

Screeners				
Smart Contract Platfo...		24H		
Mcap: \$346B		ROI: -0.69%		ETH dominance: 62,91%
#	Asset	Price	24H	Mcap
1	 Ethereum	\$1,805.42	-0.59%	\$218B
2	 BNB	\$327.76	-3.09%	\$51.78B
3	 Cardano	\$0.375	+6.17%	\$13.05B
4	 Solana	\$22.65	-1.54%	\$8.70B
5	 Polkadot	\$6.27	-0.57%	\$7.62B
6	 TRON	\$0.0672	+0.71%	\$6.13B
7	 Avalanche	\$17.63	+1.58%	\$5.76B
8	 Cosmos	\$11.77	-2.43%	\$3.38B
9	 Ethereum ...	\$20.55	-1.04%	\$2.88B
10	 Aptos	\$12.18	-1.36%	\$2.17B
11	 Hedera Ha...	\$0.0633	+0.71%	\$1.91B
12	 NEAR Prot...	\$2.03	-1.54%	\$1.76B
13	 VeChain	\$0.0231	-3.27%	\$1.68B
14	 Algorand	\$0.224	+3.23%	\$1.60B
15	 Stacks	\$1.14	-3.43%	\$1.57B

Ethereum Champion

Vitalik Buterin

Blockchain (SC)
(Smartphone)



Bitcoin
(calculatrice)



Dernière présentation publique
<https://youtu.be/UcM5lwJsbAc>

- Né le **31 Janvier 1994**, Kolomna, Moscow Oblast, Russie. (29 a)
- Russe/Canadien
- Programmeur qui a écrit l'article (white paper) en 2013 sur Ethereum
- L'équipe de développement (co-fondateurs) :
 - Anthony Di Loria,
 - Charles Hoskinson, (**Cardano**)
 - Miha Alisie,
 - Amir Chetrit,
 - Joseph Lubin (**ConsenSys**)
 - Gavin Wood. (**Polkadot**)
- ICO en 2014 : 31000 BTC
- Fondation open-source (Suisse)
- 1er Bloc - 30 Juillet 2015

Ethereum (The Leader) and its Ecosystem

350,000+

Developers
globally

**World's largest blockchain
technology developer
community**

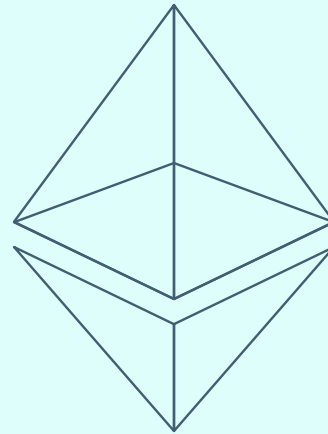
- 10x larger than second
largest blockchain community

**Public/private network
interoperability**

- for long term reliability and global
interoperability of trading venues

30,000+

New developers each month
(and growing)



**No long-term dependence on
any technology provider**

95%+

New token launches

**Adopted by the world's largest
enterprises**

for live production projects

J.P.Morgan

covantis

LiquidShore



Santander

komgo

LVMH

**Advanced and globally adopted
standards**



ERC
Standards

Scaling Ethereum

Layer 2:

Plus rapide
Nombre réduit de Nœuds
Utilise L1 pour la notarisation
et l'interopération

Layer 2
Execution

Layer 2
Execution

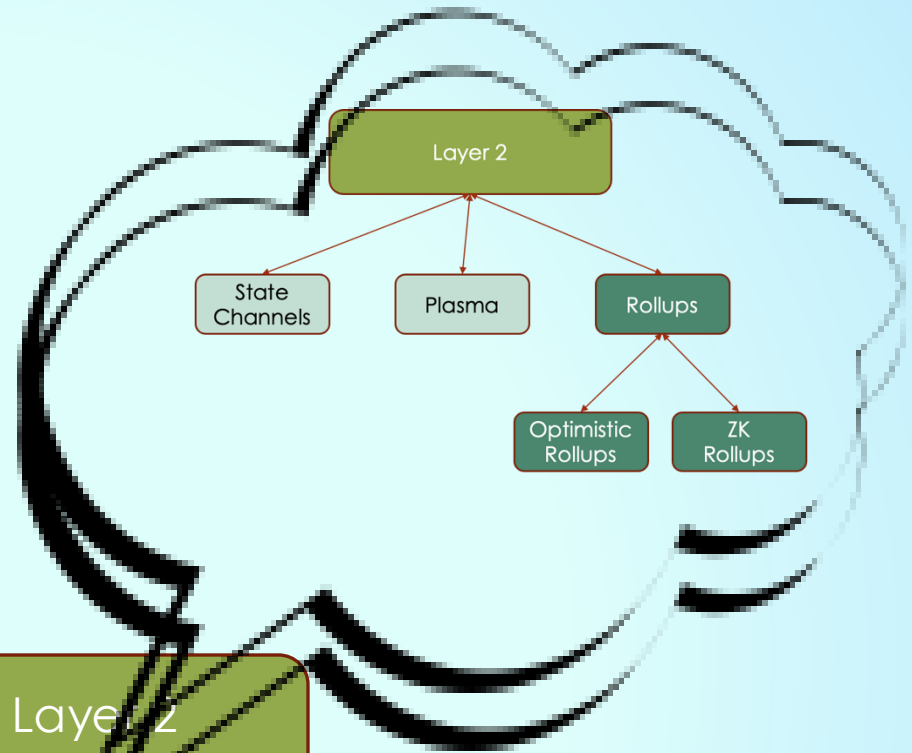
Layer 2
Execution

Layer 1
Verification

POS

Layer 1:

Base de settlement,
Décentralisation massive
Résilience



Sharding

I fully expect ZK-SNARKs to be **as important as blockchains** in the next 10 years.

idem pour d'autres Blockchains : Tezos

Blockchain Core Components

- Blockchain technology can be simplified by examining **core components** individually.
 - **Cryptographic hash functions,**
 - **Transactions,**
 - **Asymmetric-key cryptography,**
 - **Addresses,**
 - **Blocks**
 - **The Ledger**
- **More components** are needed to operationalize Blockchain-based Solutions....

Hash Functions Properties

- ▶ They are **preimage resistant** : they are one-way
 - ▶ it is **computationally infeasible** to compute the correct input value given some output value
- ▶ They are **collision resistant** : one cannot find two inputs that hash to the same output
- ▶ **Secure Hash Algorithm (SHA)** with an output size of 256 bits (SHA-256) is used in many Blockchains.
- ▶ Many computers support this algorithm in hardware, making it fast to compute.

Preimage resistance:

Given $H(x)$, it is computationally difficult to determine x



Fingerprint analogy:

Whose fingerprint is this?

SHA 256 Properties

- SHA-256 has an output of **32 bytes** (1 byte = 8 bits, 32 bytes = 256 bits), generally displayed as a **64-character hexadecimal string**
- There are $2^{256} \approx 10^{77}$, or 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936 possible digest values.
- The algorithm for **SHA-256**, is specified in Federal Information Processing Standard **(FIPS) 180-4**

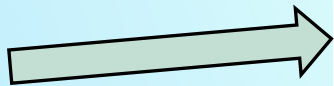
Input Text	SHA-256 Digest Value
1	0x6b86b273ff34fcea19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Hello, World!	0xdf6d6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

La menace Quantique – Algorithme de Shor

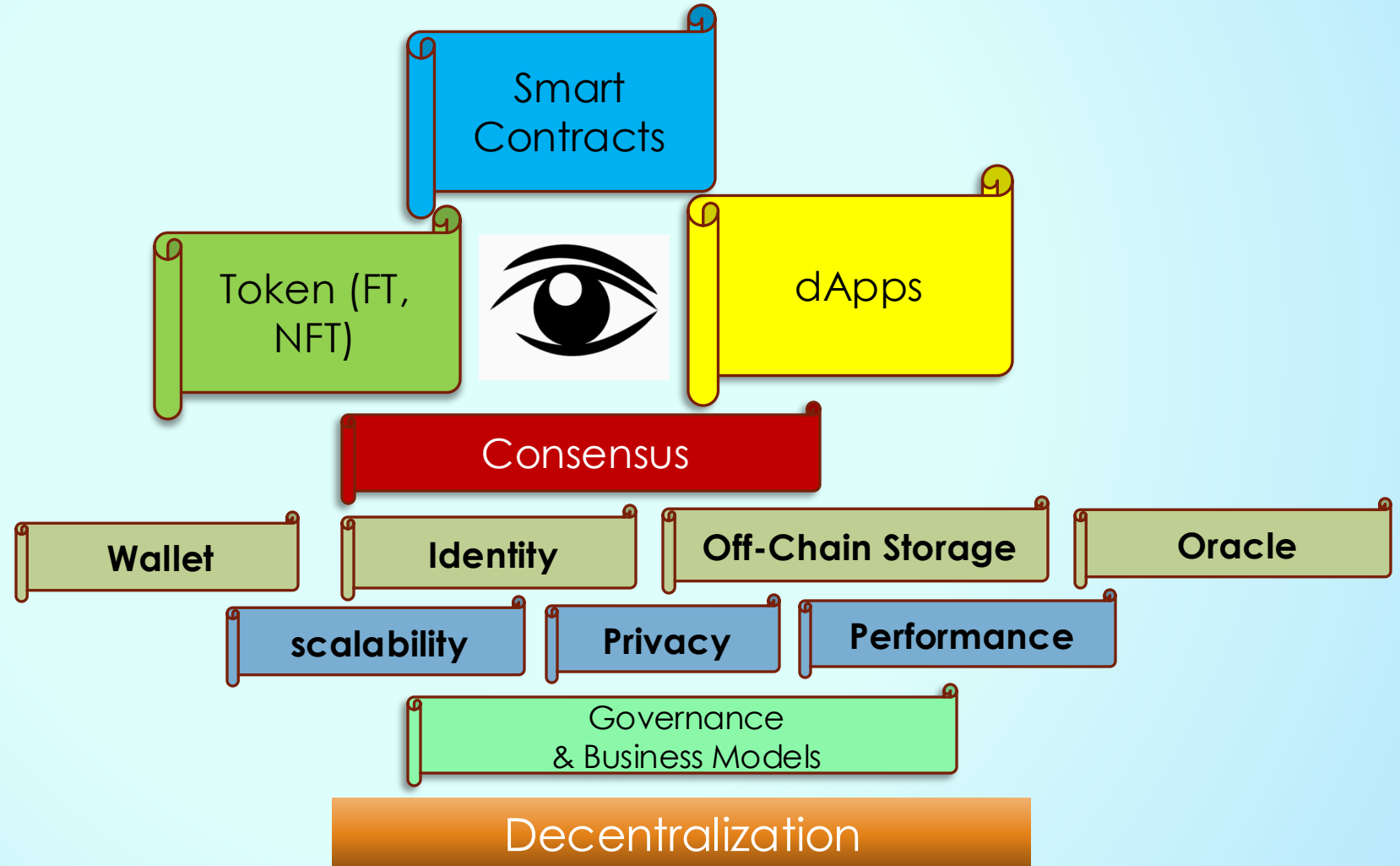
Combien de Qubits ? Et dans combien de temps ?

TABLE 4.1 Literature-Reported Estimates of Quantum Resilience for Current Cryptosystems, under Various Assumptions of Error Rates and Error-Correcting Codes

Cryptosystem	Category	Key Size	Security Parameter	Quantum Algorithm Expected to Defeat Cryptosystem	# Logical Qubits Required	# Physical Qubits Required ^a	Time Required to Break System ^b	Quantum-Resilient Replacement Strategies
AES-GCM ^c	Symmetric encryption	128 192 256	128 192 256	Grover's algorithm	2,953 4,449 6,681	4.61×10^6 1.68×10^7 3.36×10^7	2.61×10^{12} years 1.97×10^{22} years 2.29×10^{32} years	
RSA ^d	Asymmetric encryption	1024 2048 4096	80 112 128	Shor's algorithm	2,050 4,098 8,194	8.05×10^6 8.56×10^6 1.12×10^7	3.58 hours 28.63 hours 229 hours	Move to NIST-selected PQC algorithm when available
ECC Discrete-log problem ^{e,g}	Asymmetric encryption	256 384 521	128 192 256	Shor's algorithm	2,330 3,484 4,719	8.56×10^6 9.05×10^6 1.13×10^6	10.5 hours 37.67 hours 55 hours	Move to NIST-selected PQC algorithm when available
SHA256 ^h	Bitcoin mining	N/A	72	Grover's Algorithm	2,403	2.23×10^6	1.8×10^4 years	
PBKDF2 with 10,000 iterations ⁱ	Password hashing	N/A	66	Grover's algorithm	2,403	2.23×10^6	2.3×10^7 years	Move away from password-based authentication

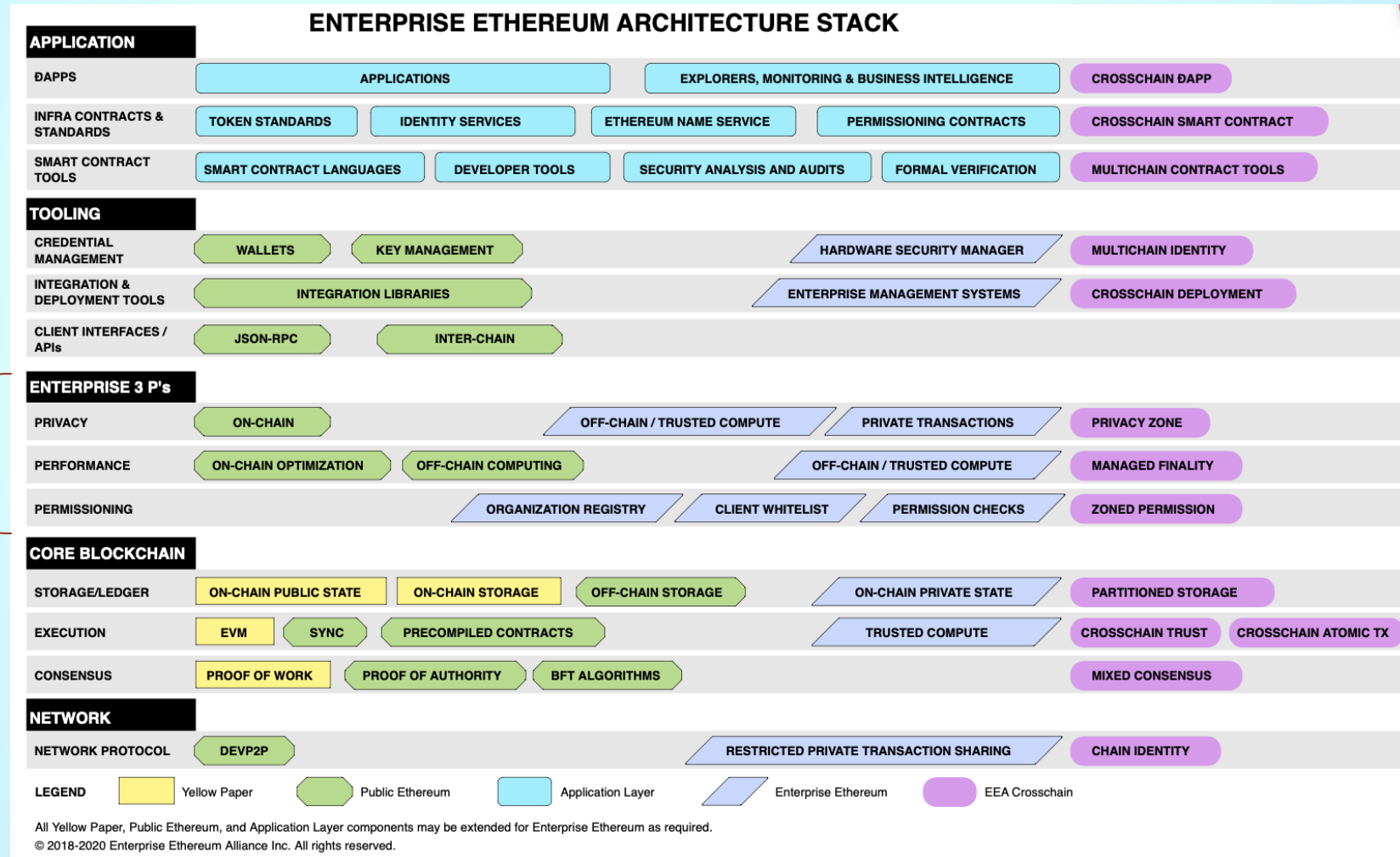


Rendre Opérationnelle une Blockchain...



Déployer un Stack Technologique

Conforme à l'architecture de "l'Alliance Ethereum Enterprise EEA"



Consensus Protocols

BFT Byzantine Fault Tolerance

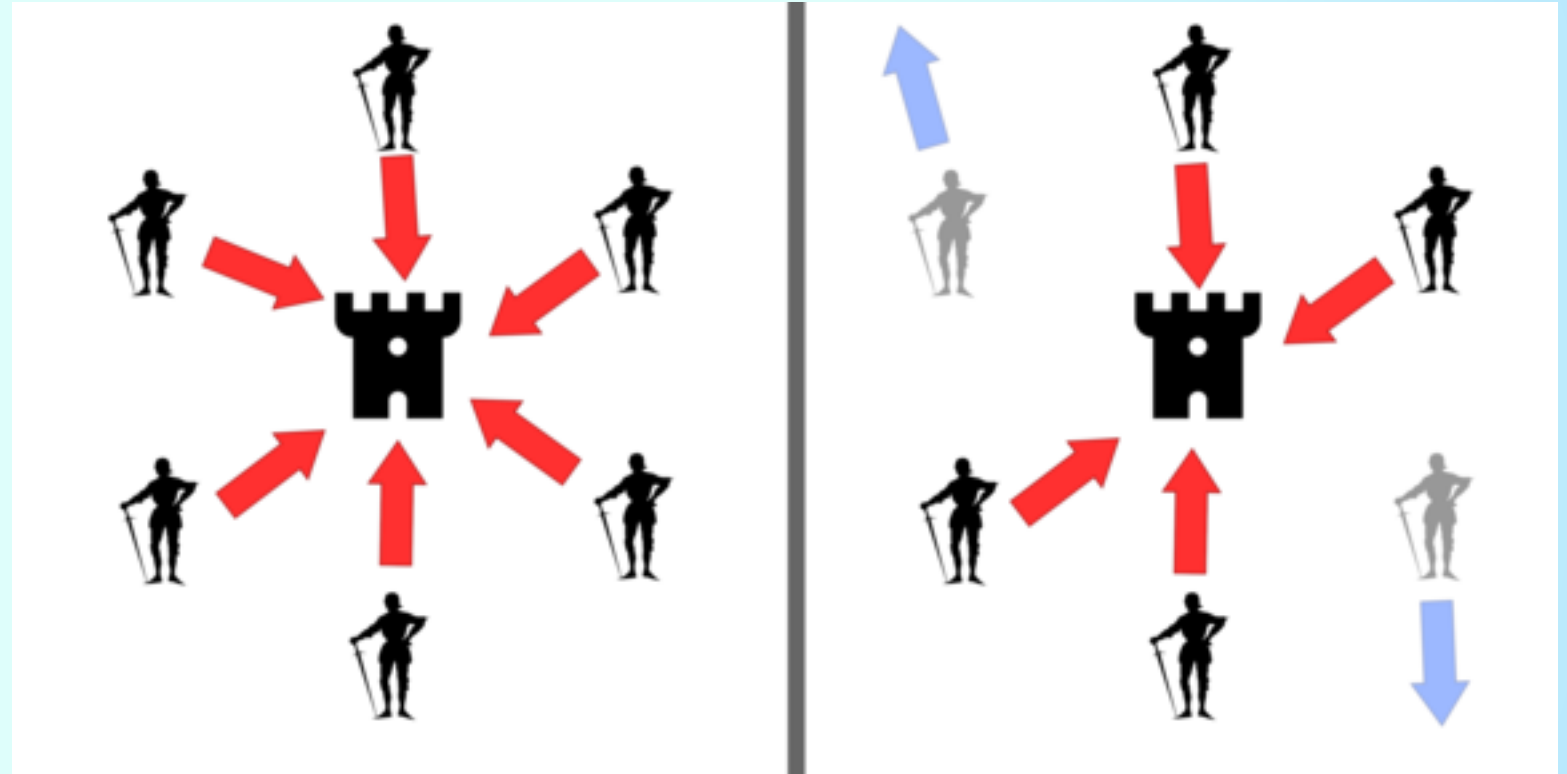


- Les généraux doivent seulement décider s'ils attaquent ou se retirent.
- Certains généraux préfèrent attaquer, d'autres se retirer et d'autres « suspects »
- Comment s'accorder sur une décision commune ?
- Le problème est compliqué par la présence de généraux traîtres qui peuvent émettre des votes contradictoires de façon sélective.
- Si neuf généraux votent, dont quatre sont pour l'attaque et quatre autres pour la retraite, le neuvième général peut envoyer un vote de retraite aux généraux en faveur de la retraite, et un vote d'attaque aux autres.
- Le problème est encore compliqué par le fait que les généraux doivent envoyer leurs votes par l'intermédiaire de messagers qui ne livrent pas les votes ou les falsifient.

En informatique distribuée , ce problème est général et implique des ordinateurs, des routeurs, des liaisons télécom, et des opérateurs divers

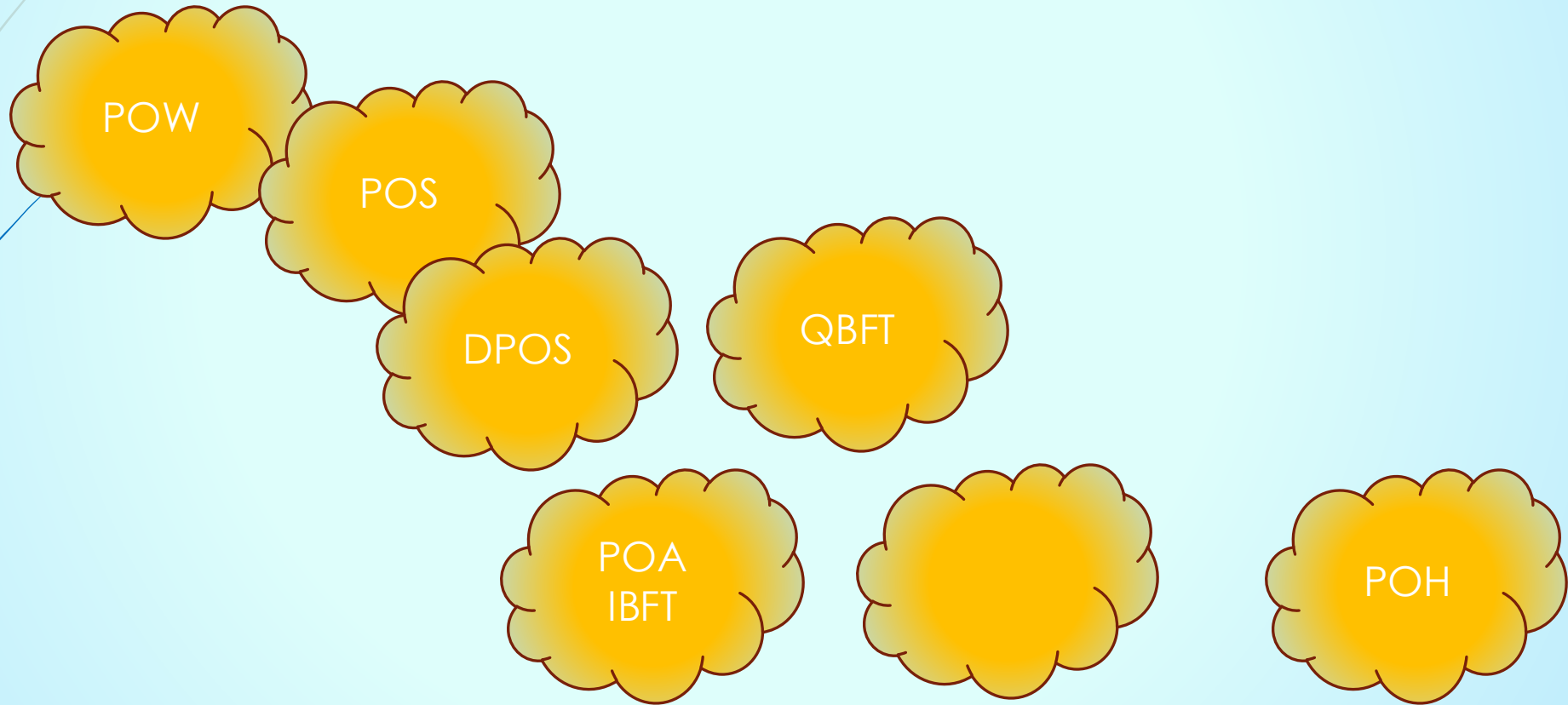
BFT Pratique

- Si n est le nombre de généraux au total,
- t est le nombre de traîtres dans ce n ,
- alors il n'y a de solutions que lorsque
 - $n > 3t$
 - et que la communication est synchrone (délai borné)



pBFT - practical Byzantine Fault Tolerance model relies on certain assumptions. The most prominent refers to the fact that the number of malicious nodes in the network could not be equal to or more than one-third of the total nodes in the system

Variantes du BFT



Wallets et Tokens

Le Wallet- Sécurisation des Clés Privées

- Dans une blockchain publique, les utilisateurs doivent gérer et stocker en toute sécurité leurs propres clés privées.
- Ils utilisent souvent un **logiciel, appelé Wallet**
- Le wallet peut stocker les clés privées, les clés publiques et les adresses associées.
- Le wallet peut également offrir d'autres fonctions, comme le calcul du nombre total d'actifs numériques qu'un utilisateur peut posséder.
- Si un utilisateur **perd une clé privée**, tout bien numérique associé à cette clé est perdu.
- Si une clé privée est volée, l'attaquant aura un **accès complet à tous les actifs numériques** contrôlés par cette clé privée.

Tokens & Fungibility

- Les jetons sont fongibles (FT) lorsqu'on peut substituer n'importe quelle unité à une autre sans aucune différence dans sa valeur ou sa fonction.
- Les jetons non fongibles (NFT) sont des jetons qui représentent chacun un élément physique ou virtuel unique et ne sont pas interchangeables.
- Un jeton qui représente la propriété d'un tableau de Van Gogh spécifique n'est pas équivalent à un autre jeton qui représente un Picasso.
- Chaque jeton non fongible (NFT) est associé à un identifiant unique, tel qu'un numéro de série.



Que peut on représenter par un Jeton /Token ?

- **Une Monnaie** Un jeton peut représenter une monnaie, avec une valeur déterminée par des échanges privés.
- **Une Ressource** Un jeton peut représenter une ressource gagnée ou produite dans une économie de partage (jeton de stockage ou de CPU)
- **Un Actif** Un jeton peut représenter la propriété d'un actif, tangible : l'or, un bien immobilier, une voiture, du pétrole, de l'énergie,
- **Un Accès** Un jeton peut représenter des droits d'accès à un bien numérique ou physique, par exemple un site Web exclusif, une chambre d'hôtel ou une voiture de location.
- **Un Capital (Equity)** Un jeton peut représenter des capitaux propres dans une organisation numérique (par exemple, une DAO) ou une entité juridique (par exemple, une société).
- **Un Vote** Un jeton peut représenter des droits de vote dans un système numérique ou juridique.
- **Pièce de collection/œuvre d'art** Un jeton peut représenter une pièce de collection numérique (par exemple, CryptoPunks) ou physique (par exemple, un tableau). – la vague **NFT** !
- **Une Utilité (droit d'usage)** Un jeton peut être utilisé pour accéder ou payer un service.

Smart Contract

Smart Contracts (SC) dans Ethereum

- Les Smart Contracts sont des programmes informatiques ayant les caractéristiques suivantes:
 - **Immuable** Une fois déployé, le code d'un SC ne peut pas être modifié...
 - **Déterministe** Le résultat de l'exécution d'un SC est le même pour tous ceux qui l'exécutent
 - **Contexte d'exécution** Les SC fonctionnent dans un contexte d'exécution restreint. Ils peuvent accéder leur propre état, le contexte de la transaction qui les a appelés, et certaines informations sur les blocs les plus récents.
 - **EVM** Ils s'exécutent dans une machine virtuelle (Ethereum VM) dans chaque nœud. Fonctionnement qualifié de « *Single World Computer* »

Les principaux Langages des Smart Contracts sur Ethereum

- **LLL** A functional (declarative) programming language, with Lisp-like syntax. It was the first high-level language for Ethereum smart contracts but is rarely used today.
- **Serpent** A procedural (imperative) programming language with a syntax similar to Python. Can also be used to write functional (declarative) code, though it is not entirely free of side effects.
- **Solidity** A procedural (imperative) programming language with a syntax similar to JavaScript, C++, or Java. The most popular and frequently used language for Ethereum smart contracts.
- **Vyper** A more recently developed language, similar to Serpent and again with Python-like syntax. Intended to get closer to a pure-functional Python-like language than Serpent, but not to replace Serpent.
- **Bamboo** A newly developed language, influenced by Erlang, with explicit state transitions and without iterative flows (loops). Intended to reduce side effects and increase auditability. Very new and yet to be widely adopted.

Tokens Smart Contracts Standards

- ERC20 : la norme de jeton la plus répandue pour les actifs fongibles,
- ERC721 : la solution de facto pour les jetons non fongibles, .
- ERC777 : une norme plus riche pour les jetons fongibles, permettant de nouveaux cas d'utilisation
- ERC1155 : une nouvelle norme pour les jetons multiples, permettant à un seul contrat de représenter plusieurs jetons fongibles et non fongibles, ainsi que des opérations groupées optimise la consommation du gaz. (27538 SC sur le Net au 14 nov.)

ERC20 required functions and events

- **totalSupply** Returns the total units of this token that currently exist. ERC20 tokens can have a fixed or a variable supply.
- **balanceOf** Given an address, returns the token balance of that address.
- **Transfer** Given an address and amount, transfers that amount of tokens to that address, from the balance of the address that executed the transfer.
- **transferFrom** Given a sender, recipient, and amount, transfers tokens from one account to another. Used in combination with approve.
- **approve** Given a recipient address and amount, authorizes that address to execute several transfers up to that amount, from the account that issued the approval.
- **allowance** Given an owner address and a spender address, returns the remaining amount that the spender is approved to withdraw from the owner.
- **Transfer** *Event* triggered upon a successful transfer (call to transfer or transferFrom) (even for zero-value transfers).
- **Approval** *Event* logged upon a successful call to approve.

Qu'est ce qu'une DAO ?

Decentralized Autonomous Organization

A DAO is commonly defined by these five characteristics:

- **Flat organisation** — A DAO, in principle, has no hierarchy, and decisions are made by its stakeholders or members instead of leaders or managers; although usually, in practice, certain spheres of decision-making may be delegated to a core or selected team.
- **Transparency** — A DAO must be **open-source**. Anyone can inspect the code on the smart contract or view the DAO's transaction history on the blockchain.
- **Open access** — Anyone can, in theory, be a member of the DAO, as long as they fulfil the predetermined requirements, such as **holding its governance token**.
- **Democracy** — Depending on the voting mechanism, it may be the case that **no single party can veto a request** once it passes the voting process.
- **Minimal human resources** — DAOs operate mostly algorithmically, **governed by code**. Occasionally, members of the DAO may hire a person to fix issues on the smart contract, such as bugs or updates.

Decentralized Autonomous Organization – Comment mettre en place une DAO ?

How to Form a DAO

- Unlike traditional organisations, decentralised autonomous organisations (DAOs) are transparent, flat, and open.
- Here are the four phases of launching one.
 - **1st phase.** Create the smart contract, which dictates rules and purpose of the DAO.
 - **2nd phase.** Deploy the smart contract on a testnet, checking for weaknesses and errors.
 - **3rd phase.** Work on funding and governance structure. Typically, tokens that give voting rights are distributed to participants.
 - **4th phase.** Launch the DAO on the blockchain. The original creators will usually hand over control to the stakeholders.

Top Blockchain DAO Tokens by Market Capitalization

Top Blockchain DAO Tokens by Market Capitalization⁷⁴

	Uniswap (UNI) \$4.98 billion	A decentralized marketplace that manages liquidity pools of different tokens, which also allows users to safely trade those tokens peer-to-peer.
	Lido DAO (LDO) \$2.54 billion	Lido allows participants to stake Ether and receive yield in return.
	ApeCoin (APE) \$1.87 billion	A governance token that is used to grant permission for the Ape Foundation to carry out proposals agreed upon by the community.
	Internet Computer (ICP) \$1.77 billion	A full end-to-end decentralized "world computer" that does not need traditional IT services.
	BitDAO (BIT) \$1.19 billion	A DeFi protocol that supports other DAOs, NFTs and GameFi with research and development and funding.
	Aave (AAVE) \$1.14 billion	One of the most established DeFi protocols that enables borrowing and lending to earn yield on cryptocurrency assets.
	Dash (DASH) \$792.6 million	An inexpensive and fast global payments network, which is the longest running DAO to date.
	CurveDAO (CRV) \$725.2 million	By managing liquidity through an automated market maker, Curve is a decentralized exchange for stablecoins, with participants using the token CRV for governance.
	Maker (MKR) \$711.7 million	MakerDAO issues the Dai stablecoin, which is pegged to the U.S. dollar, and utilizes its token, <u>MKR</u> , for proposals and governance voting.
	Synthetix (SNX) \$632.5 million	Through pooled collateral systems, Synthetix issues the SNX token, which can be used to create synthetic assets. Synthetix is a decentralized exchange, and SNX can be used by participants to earn yield by staking SNX.

Les Blockchains d'Entreprise

Pourquoi une Blockchain au Service des Entreprises



Collaborer en toute confiance avec ses partenaires

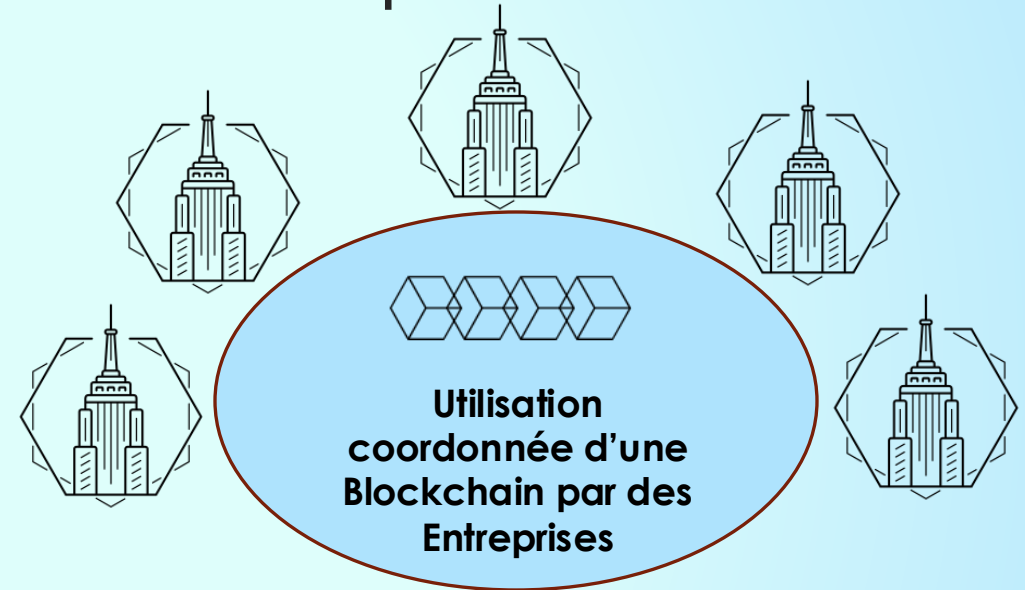
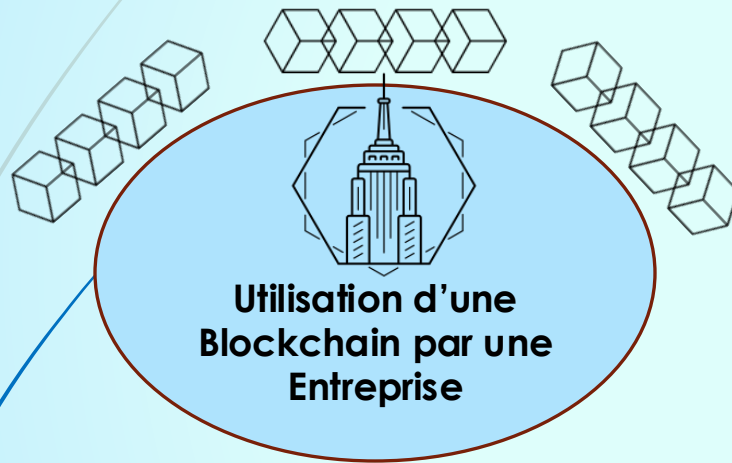
Compléter les solutions existantes par un nouveau **socle de confiance**



Fournir à ses clients ou administrés des services de confiance

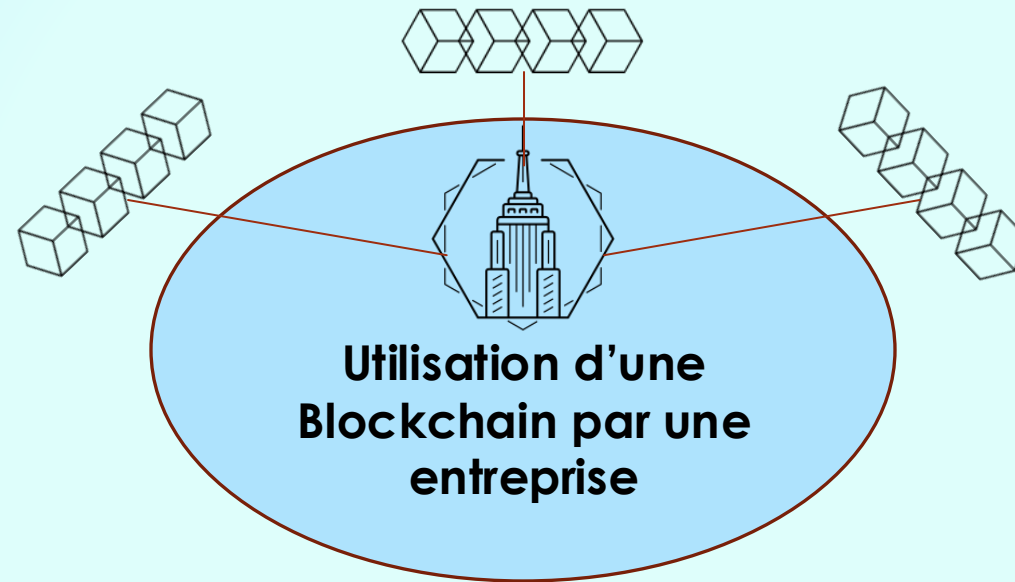
Contrôle et vérification de l'**authenticité des produits et services** (réciprocité)

Modèles de Déploiement des Blockchains dans les Entreprises



- Nouveaux types de collaboration entre les entreprises
- Fondés sur les principes de la décentralisation
- Réduire ou éliminer le besoin d'intermédiaires de « confiance »,
- Remplacer les structures centralisées par des structures décentralisées

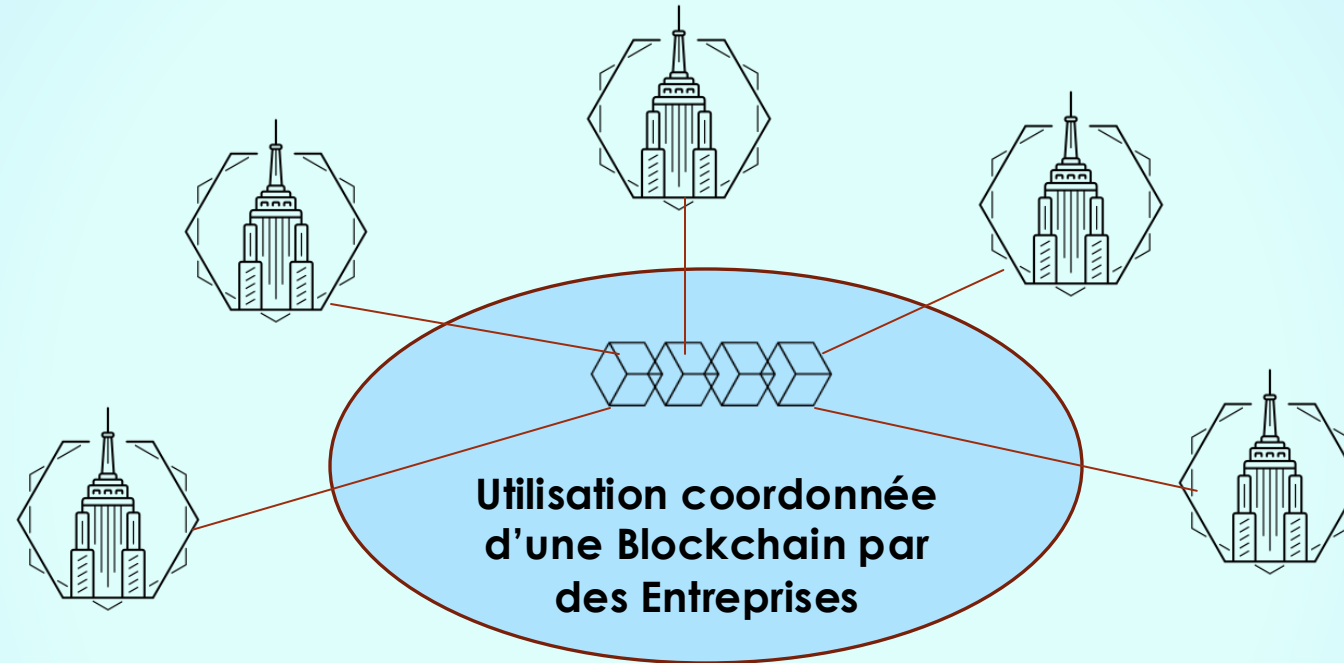
Blockchain d'Entreprise – Ciblage 1



Appel à des services externes

- Notarisation et vérification de titres de propriété (NFT-isation)
- Vérification de Pièces (Certificat, Diplôme, KYC, Recrutement)
- Finance Décentralisée...
- ...Autres

Blockchain d'Entreprise – Ciblage 2



Processus Métier Multi-acteurs

- Traçabilité (produits, décisions, actions,...)
- Chaînes Logistiques (Distribution, Alimentaire, Transport)
- Elaboration de contrats
- Gestion de Grands Projets

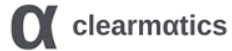
Bénéfices Attendus de la Blockchain pour les Entreprises

- **Efficacité** : remplacement des anciennes infrastructures et des pratiques traditionnelles
- **Automatisation et collaboration** : utilisation des Smart Contracts et dApps
- **Confiance et transparence** : renforcement de la confiance par une transparence « adaptée »
- **Nouveaux modèles commerciaux** : sur la base de la Tokenisation (FT et NFT)

Les 1^{ères} Tendances de la Blockchain d'Entreprises



Hyperledger – projet open-source sous l'égide de la Fondation Linux promu en grande partie par IBM



très médiatisés - domaines : financement du commerce, assurance, énergie, alimentation et produits de luxe.

Certains ont échoué
D'autres continuent...



Blockchains de Consortium

Pourquoi les Blockchains Publiques ont été au début écartées ?

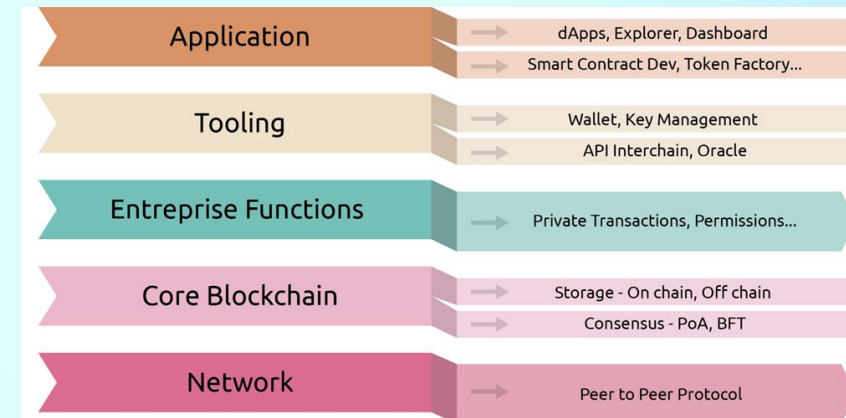
- Confidentialité des données:
 - Visibilité des données et des Smart Contracts ainsi que les traces des transactions (extrapolation par corrélations)
- Conformité
 - identification des utilisateurs, effacement, KYC impossible
- Scalabilité
 - TPS, congestion, sélectivité des Transactions, volatilité

Blockchains Privées – Les Freins



Le principal problème n'était pas d'ordre technologique, mais *organisationnel*.

- **Frein 1** : Beaucoup de consortia ont été lancés et *dominés par un seul acteur*.
- **Frein 2** : Adhésion des concurrents, et adoption de plans communs
- **Frein 3** : Scalabilité Technologique résolue, mais problème de "**scalabilité sociale** »
- **Frein 4** : Construction de Stack .



BLOCKDATA

BLOCKCHAIN CONSORTIUMS COMPARED (2021)



Finance

Trade Finance

Assurance

Supply Chain
Logistique

Transverse

Pharma

Luxe, S. Chain

Transfert paiement

Trade Finance

Automobile

PharmaLedger
Focus: HealthTech, Pharma

BLOCKCHAIN INFRASTRUCTURE

HYPERLEDGER
FABRIC

QUORUM

TECH PARTNERS

IBM

CONSENSYS

BotSoft

MEMBERS
(29 companies)

LifeSTech

gsk

Pfizer

abbvie

Boehringer Ingelheim

EF CCP

BAYER

INCM

PDM

NOVARTIS

Roche

AstraZeneca

janssen

CSL

Novartis

Novartis

AURA
Focus: Luxury Brands, Supply Chain

BLOCKCHAIN INFRASTRUCTURE

QUORUM

TECH PARTNERS

CONSENSYS

Microsoft

MEMBERS
(8 members)

LVMH

PRADA Group

OTB

HUBLOT

Cartier

BVLGARI

RICHEMONT

SPUNTA
ABI Lab DLT

Focus: Payments, Interbank Transfers

BLOCKCHAIN INFRASTRUCTURE

c.rda

sia CHAIN

TECH PARTNERS

sia

r3

NTT DATA

MEMBERS
(100+ members)

BANCA GENERALI

INTESA

SNBIOLO

BANCO BPM

BPER: cdp

MONTE DEI PASCHI DI SIENA

Allianz

Bank

Santander Consumer Bank

FINECO BANK

MEDIOBANCA

UniCredit

BNL

komgo

Focus: Trade Finance

BLOCKCHAIN INFRASTRUCTURE

QUORUM

TECH PARTNERS

CONSENSYS

MEMBERS
(20 shareholders, 180+ companies)

ABN-AMRO

BNP PARIBAS

SOCIETE GENERALE

ING

SGS

NATIXIS

SMBC

citi

MACQUARIE

MERCURIA

Rabobank

MUFG

CREDIT AGRICOLE

COCH

CREDIT SUISSE

MOBI

Focus: Transportation, Identity

BLOCKCHAIN INFRASTRUCTURE

mobiNET

TECH PARTNERS

CONSENSYS

r3

IBM

MEMBERS
(20+ Financial Institutions, 140+ Companies)

HITACHI Inspire the Next

BMW

TOYOTA

HYUNDAI

HONDA

GM

Continental

SAE

accenture

Swiss Re

ZE

Pacific Gas and Electric Company

Blockchain d'Entreprise – Nouvelle Tendance –

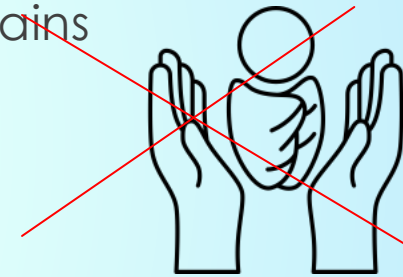
Regain d'intérêt pour la Blockchain Publique
Ethereum se positionne comme leader...

- Ecosystème Ethereum publique, en pleine **évolution et maturation**
- **Infrastructures et outils** de meilleure qualité (protocoles, architecture multiniveaux, **standardisation** de SC,...)
- Boom des applications de **DeFi** et adoption massive du concept des **NFT**

DeFi – Decentralized Finance

Decentralized & Non Custodial

- **Non-custodial** - Aucun organisation ou équipe centrale ne gère les cryptos pour le compte des utilisateurs, qui contrôlent leurs fonds en interagissant avec les divers protocoles déployés sur la ou les Blockchains

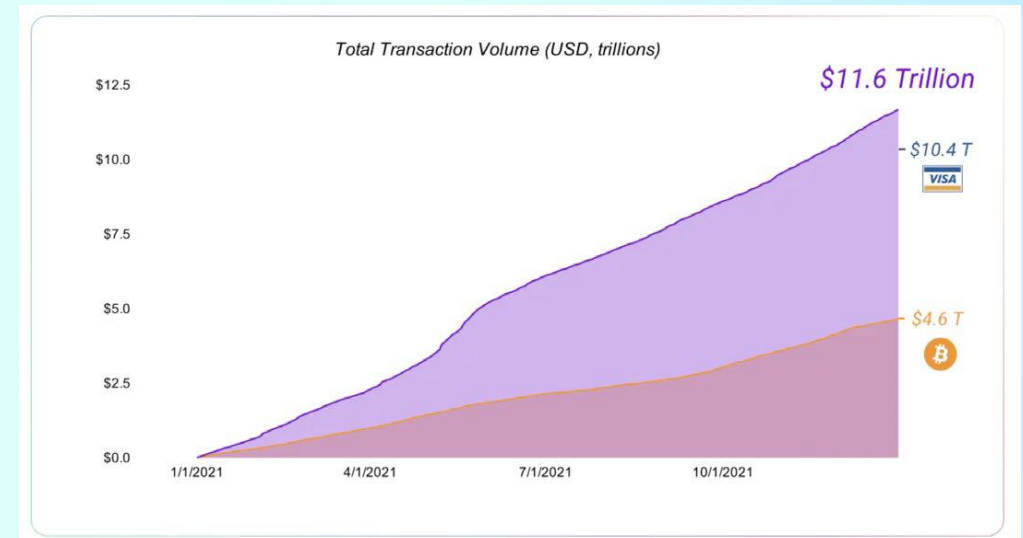


- **Decentralized** - les créateurs des protocoles ont confié les Smart Contracts (au cœur de ces protocoles) à la communauté et leurs laissent progressivement la responsabilité de faire évoluer les protocoles



La Blockchain Publique : une Chaîne de Confiance « Protocoles d'Echange et de Notarisation »

- A partir de 2020, Ethereum est devenu un socle de « *settlement* » -de confiance au niveau mondiale et sans aucune frontière:
 - Notarisation
 - Stockage
 - Echanges.



- En 2021, la blockchain Ethereum a réglé plus de \$ 11,6 mille milliards de dollars de transactions.
- Illustration de la robustesse d'Ethereum

La DeFi – Services & Risques

Services Bénéfices

- Transfert de Fonds
- Frais réduits
- Emprunt/Prêt
- DEX
- Dépôt décentralisé
- Propriété fractionnée
- Produits Dérivés
- Stablecoins
- Flash Loan
- Marketplace
- Placements non liquides

Risques

- Responsabilité utilisateur importante
- Pertes irréversibles
- Volatilité
- Risque technique
- Fraude

Les Services DeFi Populaires



- **Emprunter : Aave, Maker, Compound**
 - Emprunts instantanés de sommes importantes (apporter la preuve de remboursement par une seule transaction)
- **Prêter:** des cryptomonnaies.
 - En un seul jour, plus de \$138 million de **Flash loans** ont été émis sur Aave
 - **Flash loans** permettent aux utilisateurs d'emprunter des gros montants sans garantie à condition que l'activité on-chain avec les fonds soient profitables et exécutables en un seul bloc !
- **Change – DEX** - Uniswap permet d'échanger n'importe quel Jeton Ethereum ou gagner de l'argent on l'ajoutant à un pool de liquidités de ce Jeton
- **Token Synthétique** / Stablecoin tel que MakerDAO stablecoin DAI dont la valeur est déterminée par algorithme.
- **Porter Bitcoin sur Ethereum WBTC (Wrapped Bitcoin)**

Les taux d'intérêt varient.

Ex: prêter le DAI, le stablecoin décentralisé de Maker, pour 7,75 % sur Compound, ou l'emprunter pour 10,78 %.
Sur Aave, le prêt est à 9,59 % et l'emprunt à 17,46 %.

Top DeFi Nov. 7, 2022

- Uniswap
- AAVE
- MakerDAO
- PancakeSwap
- Curve
- THORChain
- Loopring
- 1inch
- Sushiswap
- Compound
- Gnosis
- JustLend
- Instadapp

Screeners DeFi 24H				
Mcap: \$17.96B		ROI: -3.32%		UNI dominance: 30,24%
#	Asset	Price	24H	Mcap
1	 Uniswap	\$7.19	-3.02%	\$5.43B
2	 Aave	\$87.53	-3.62%	\$1.24B
3	 Synthetix	\$2.69	+2.51%	\$825M
4	 Maker	\$834.91	-6.73%	\$816M
5	 PancakeSwa	\$4.69	-4.30%	\$680M
6	 Curve	\$0.970	-2.52%	\$549M
7	 THORChain	\$1.62	-2.31%	\$487M
8	 Loopring	\$0.326	-9.08%	\$433M
9	 1inch	\$0.641	-2.42%	\$398M
10	 DeFiChain	\$0.638	-3.01%	\$391M
11	 Amp	\$0.00486	-3.43%	\$373M
12	 SushiSwap	\$1.81	+0.77%	\$348M
13	 Compound	\$49.91	-2.14%	\$342M
14	 Gnosis	\$117.69	-2.80%	\$304M
15	 Olympus DA	\$10.04	-0.83%	\$289M

Top DeFi

23 Mars, 2023

Screeners		DeFi	24H	
Mcap: \$17.80B		ROI: +18.20%	UNI dominance: 27,09%	
#	Asset	Price	24H	Mcap
1	 Uniswap	\$6.39	+1.70%	\$4.83B
2	 Aave	\$78.73	+0.45%	\$1.13B
3	 Curve	\$0.980	-1.68%	\$755M
4	 Synthetix	\$2.73	-1.68%	\$692M
5	 PancakeSw...	\$3.78	-0.24%	\$692M
6	 Maker	\$685.12	+0.38%	\$669M
7	 Loopring	\$0.364	+4.72%	\$485M
8	 Radix	\$0.0456	+11.14%	\$456M
9	 1inch	\$0.523	-0.57%	\$439M
10	 THORChain	\$1.44	+0.64%	\$434M
11	 dYdX	\$2.60	+0.85%	\$393M
12	 DeFiChain	\$0.578	-1.17%	\$391M
13	 Injective Pr...	\$4.24	+3.52%	\$338M
14	 Compound	\$44.13	-0.03%	\$303M
15	 Gnosis	\$110.98	-0.93%	\$292M

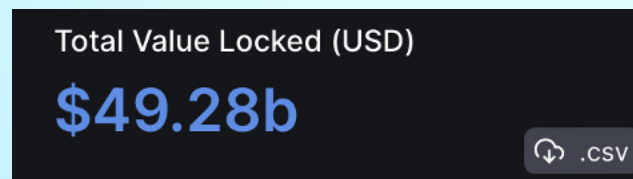
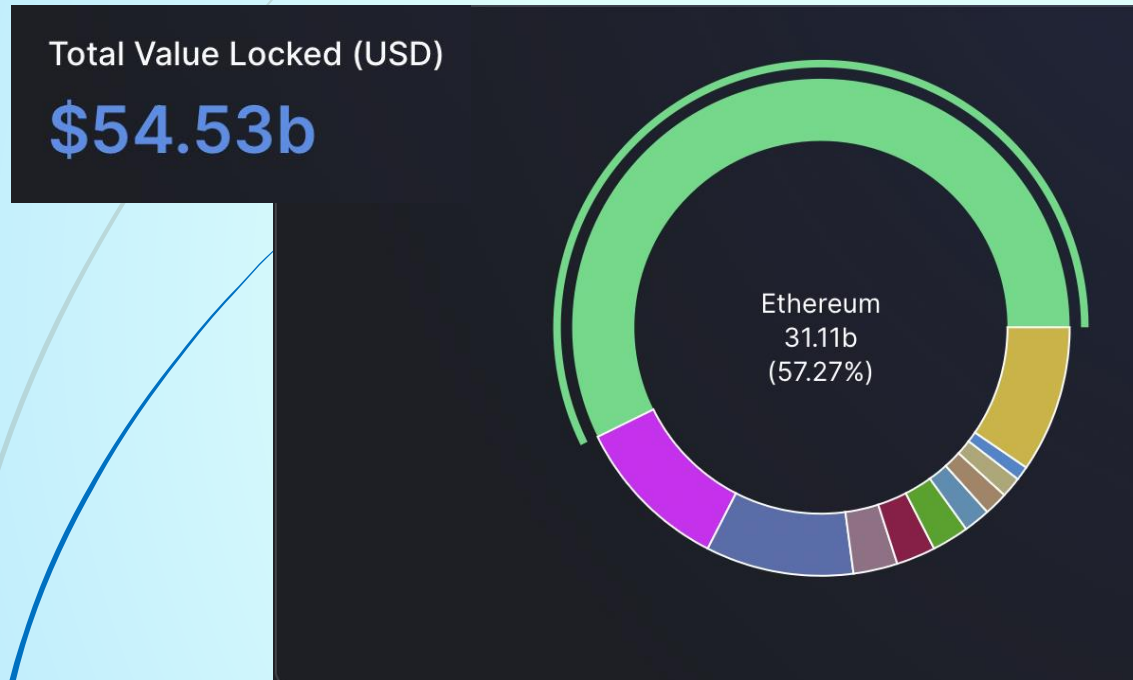
Le DeFi – quelques déboires

- Des accidents de parcours dus au non respect de la vision « décentralisé et non-custodial ».
- En examinant les protocoles et les smart contracts associés, on découvre des liens privilégiant les fondateurs avec risque de reprise du pouvoir
- Le fondateur et CEO de Curve, Michael Egorov, a repris 71% de droits de vote sur la plateforme DAO!
- **Le cas FTX**



TVL (Total Value Locked) on All Chains

Sept 16, 2022

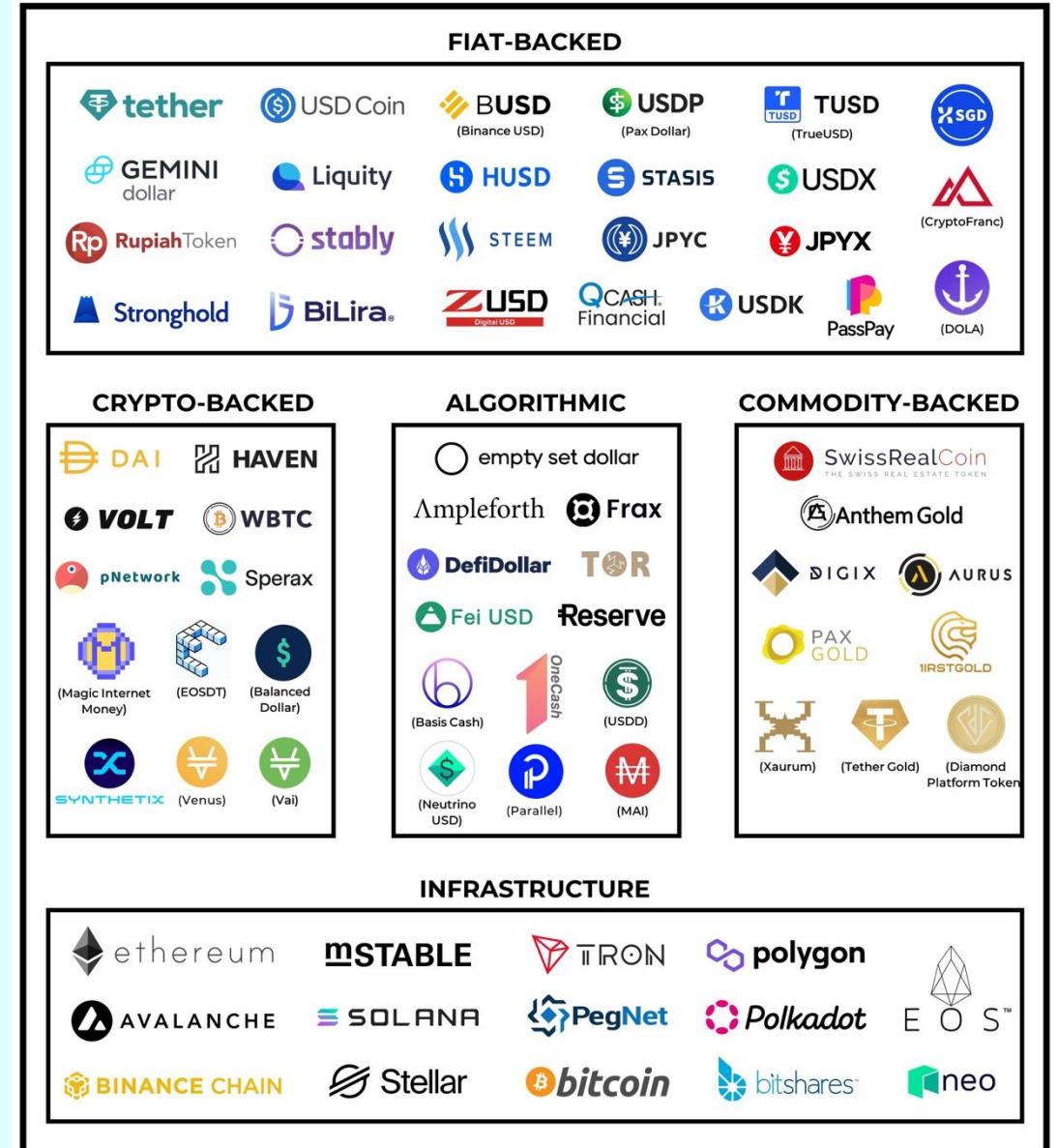


Mars 2023

1		Ethereum (ETH)	\$31.11b
2		Tron (TRON)	\$5.55b
3		BSC (BNB)	\$5.22b
4		Avalanche (AVAX)	\$1.56b
5		Polygon (MATIC)	\$1.38b
6		Solana (SOL)	\$1.31b
7		Arbitrum	\$943.47m
8		Optimism (OP)	\$837.24m
9		Cronos (CRO)	\$725.66m
10		Fantom (FTM)	\$499.03m

Les Stablecoins

- Remède à la volatilité (BTC, Ether, Binance...)
- Offrant valeur stable tout en étant décentralisé!
- Garantie 1:1 \$ ou Or.
- Transactions plus rapides et moins coûteuses.
- Top 3: Tether, USD Coin (USDC), Binance USD (BUSD),
- Dai, TrueUSD (TUSD)
- 134 Stablecoins 2/11/22
- 4 Catégories
 - Fiat backed (82%),
 - Crypto backed,
 - commodity backed,
 - Algorithmic



L'Adoption par les Banques Centrales reste incertaine !!!

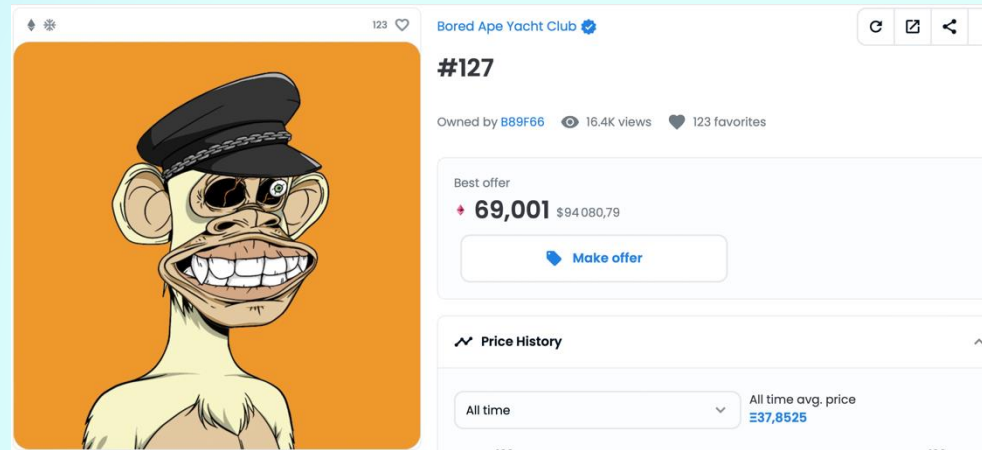
Même si tous les pays ont désormais les yeux rivés sur les CBDC et aucun pays n'ignore ce nouveau phénomène financier.

- “It is not clear how retail CBDCs will create significant added value relative to the existing solutions in Denmark,” the **Danmarks Nationalbank** stated in a CBDC-related report in June 2022.
- In July 2022, the bank (**Bank of Japan**) issued a report in which it claimed it had no plan to issue a CBDC, the “strong preference for cash and high ratio of bank account holding in Japan.”
- In August 2022, Andrés Arauz, the former general director at **Ecuador's central bank**, warned eurozone policymakers that a digital euro could potentially disrupt not only privacy but also democracy.
- After dropping its own CBDC-related project years ago, **Finland** appears to support a pan-European digital currency.

Comment démarrer dans le DeFi ?

- Obtenir un Wallet compatible Ethereum (Metamask répandu).
- Acheter le Coin du Protocole DeFi que vous voulez utiliser (ETH ou un ERC-20 coin).
- Si vous voulez utiliser le bitcoin, l'échanger avec une version Ether du Bitcoin (Wrapped BTC)
- Démarrer les activités :
 - Prêter votre crypto (best deal sur yearn.finance, ou
 - Devenir "[yield farmer](https://yieldfarming.info)" en gagnant des jetons de gouvernance (info des profits sur yieldfarming.info).
 - Placer vos fonds dans une DEX comme Uniswap, et gagner des intérêts en tant que Market Maker. (ou chez un rival Sushiswap qui fait gagner en plus des jetons de Yieldfarming..
 - Investir dans des projets « expérimentaux » à jetons volatiles (Based.Money, ou [meme coins](#), comme [\\$YAM](#), [\\$TENDIES](#), [\\$KIMCHI](#), [\\$SHRIMP](#)).

Les NFT – Collections, Arts, Haute Couture, Fidélisation, Avatar dans le Metavers,



BORED APE YACHT CLUB

Properties

- BACKGROUND**
Orange
13% have this trait
- EYES**
Crazy
4% have this trait
- FUR**
Cream
6% have this trait
- HAT**
S&m Hat
2% have this trait
- MOUTH**
Grin
7% have this trait

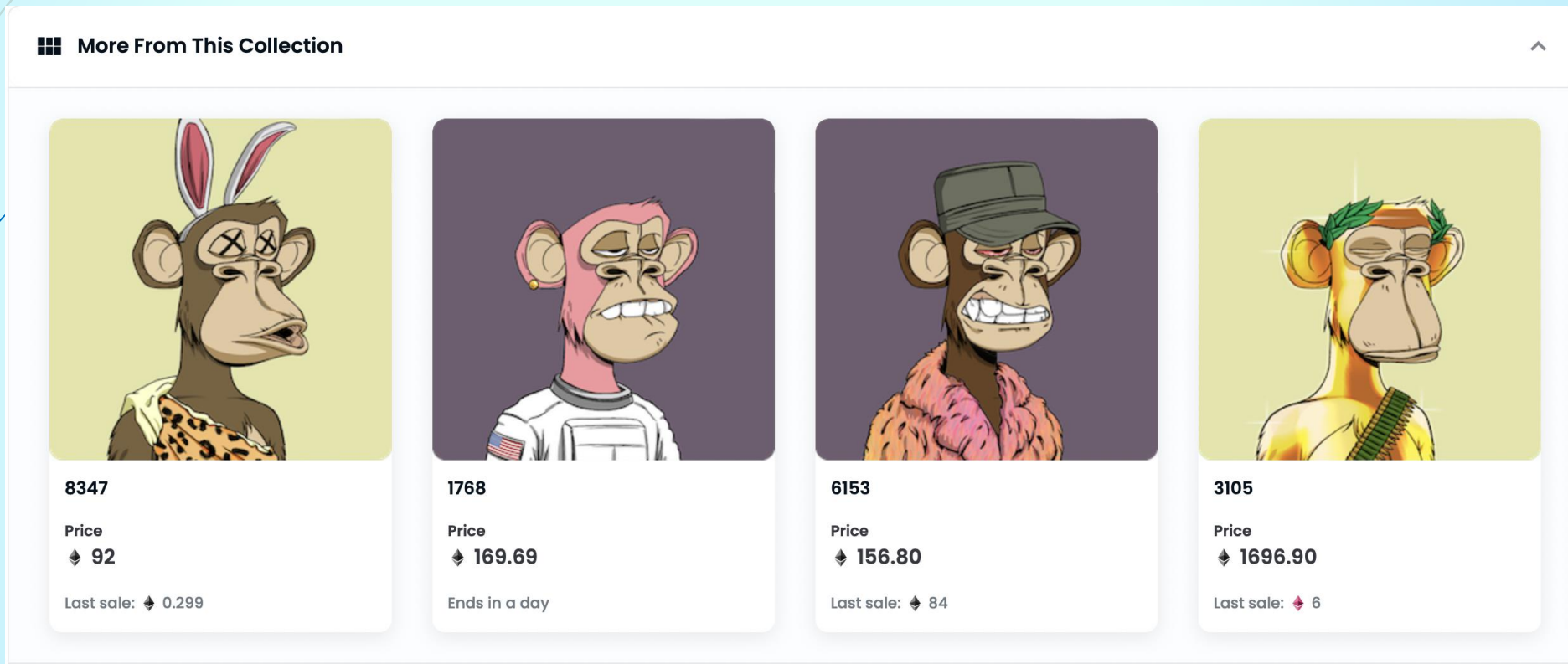
About Bored Ape Yacht Club

Details

Listings

Price	USD Price	Floor Difference	Expiration	From
69,001 WETH	\$94 080,79	7% below	about 18 hours	q
68,99 WETH	\$94 065,80	7% below	2 days	AKC_Li
67,69 WETH	\$92 293,28	9% below	about 13 hours	franklinisbored
7,93 WETH	\$10 812,32	89% below	2 days	permastic
7 WETH	\$9 544,29	91% below	1 day	La_Vermuteria

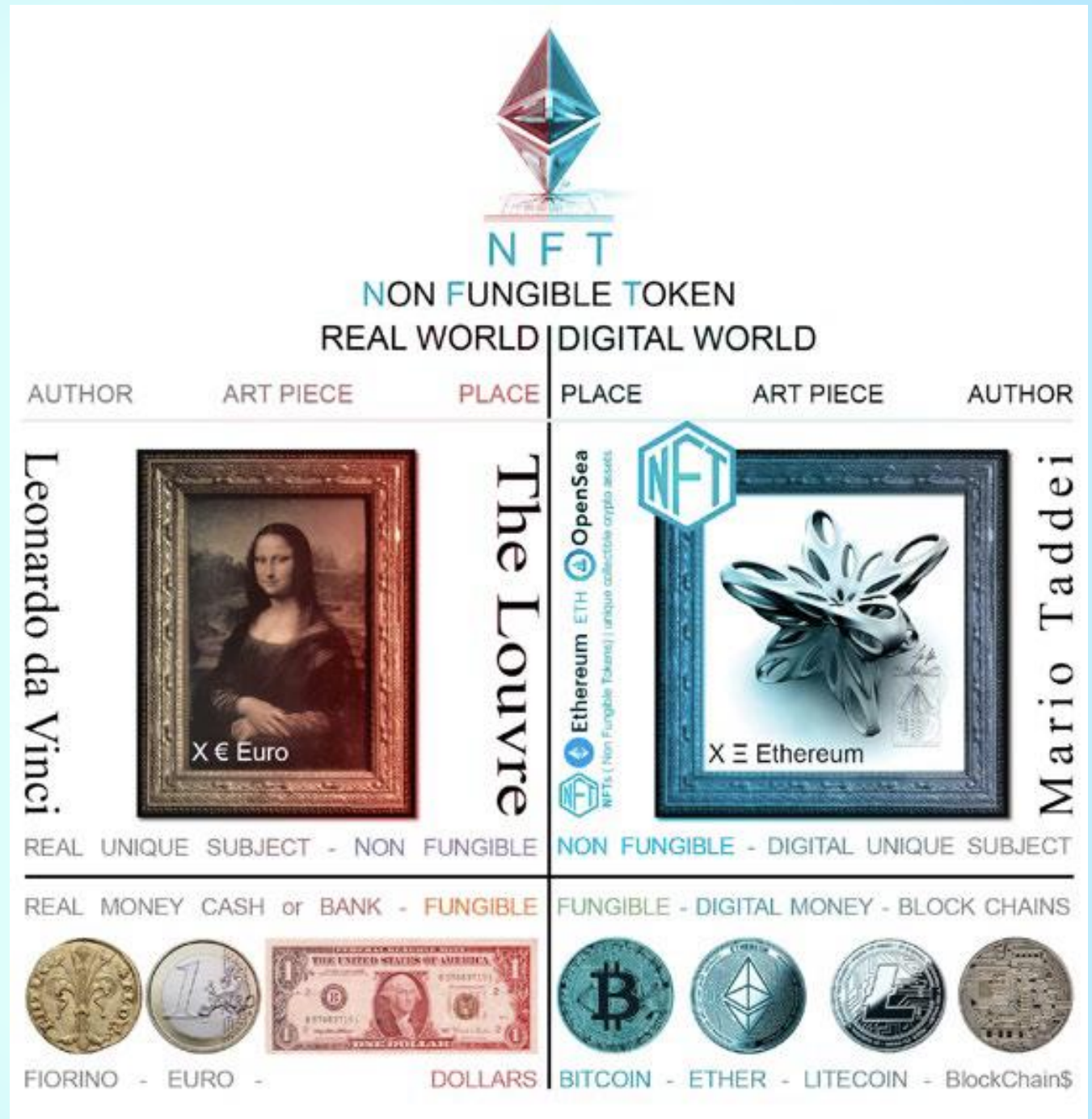
An anonymous source tipped *Bloomberg* that the Securities and Exchange Commission is currently investigating whether NFTs sold by Yuga Labs, the \$4 billion company behind the Bored Ape Yacht Club, violated security registration laws. The SEC did not deny the report.



Collection de 10.000 images

Dépenser des Millions de \$
Sur du JPEG ?
Est-ce raisonnable ?

Prenons les fondements de
la Joconde par Léonard de Vinci
Rareté
Unique
Artiste célèbre
Exposée au Louvre
Des Fans
Génère des revenus



Les NFT - A \$69 Million Mona Lisa JPEG

Beeple

Famous artist? Check.

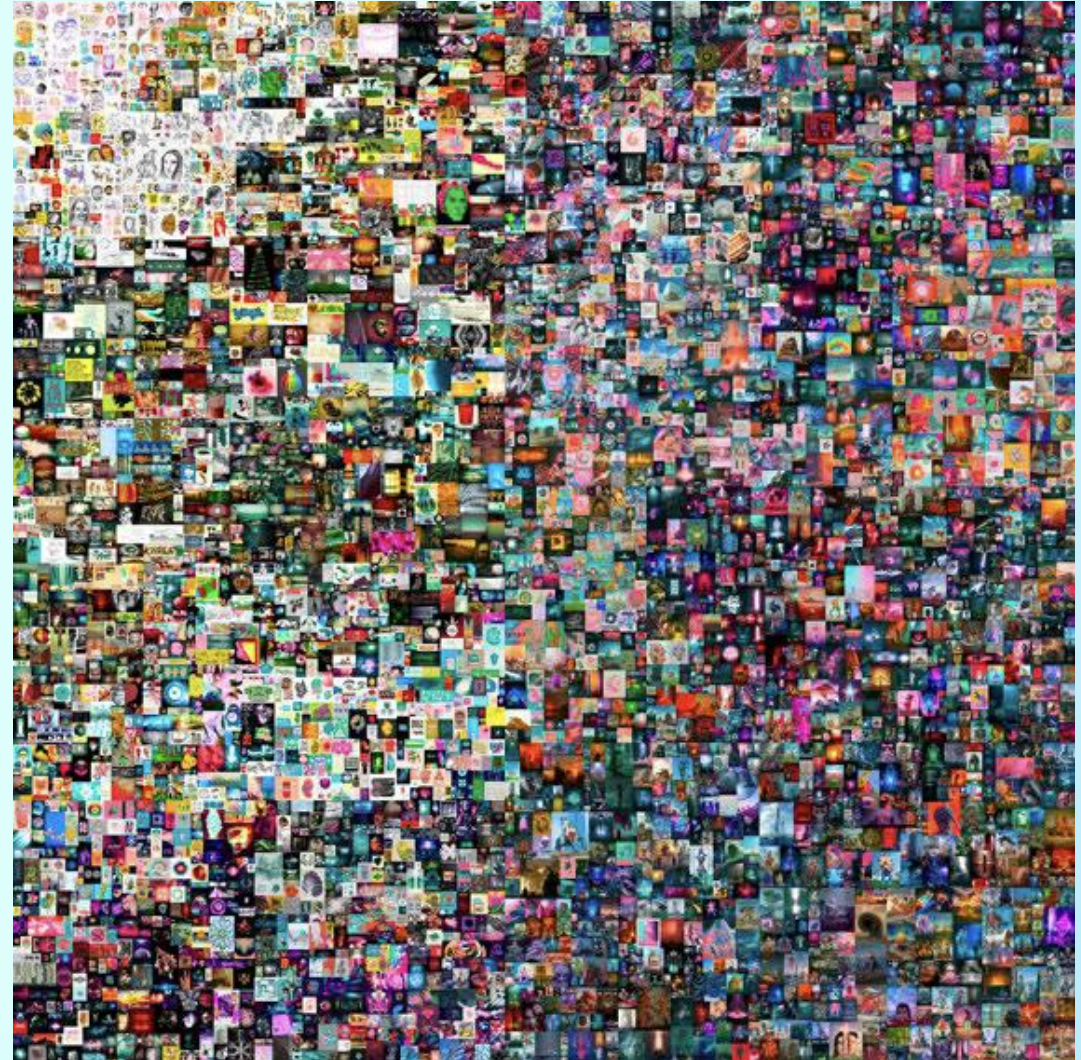
Beeple had 2.5 million followers at the time of sale.

Proof-of-rarity? Check.

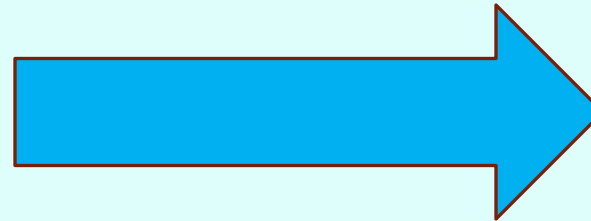
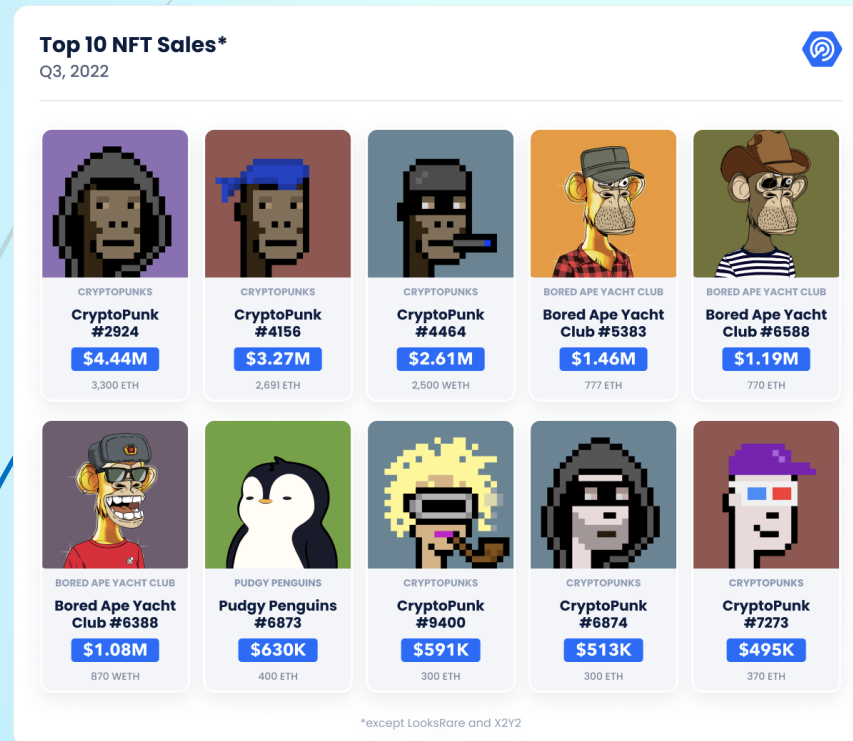
It will be incredibly difficult to replicate as the mural represents the culmination of 14 years' worth of daily dedication.

Novel backstory? Check.

It wasn't stolen, but it made history as the first major NFT art piece auctioned through Christie's, and the sticker price itself (\$69 million) contributes to the art's rarity.

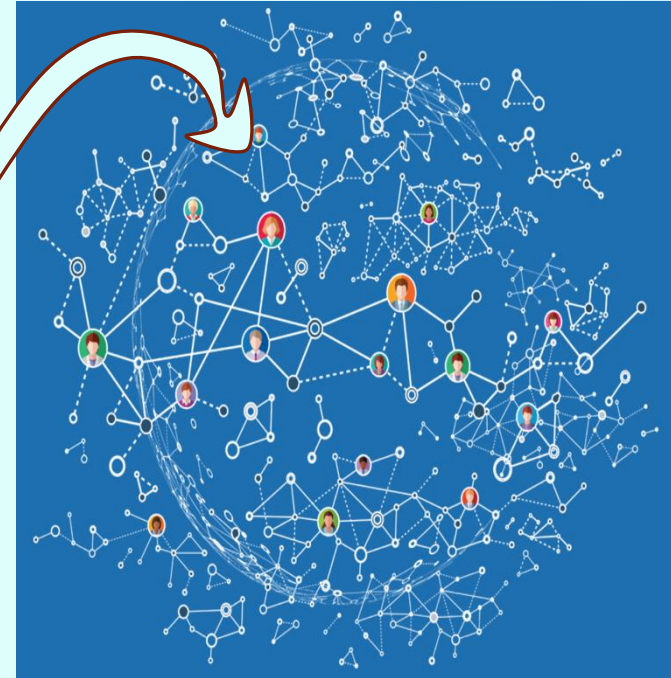
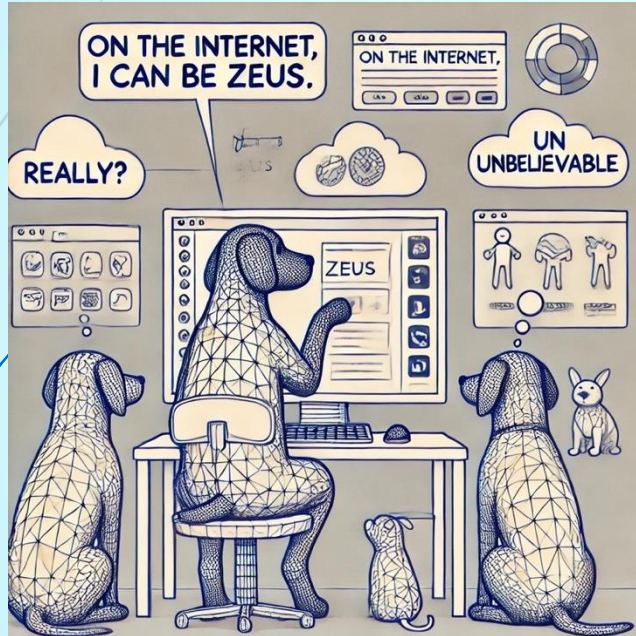


Les Entreprises ayant adopté les NFT...



- Salesforce
- Adidas
- Lamborghini
- Coca-Cola
- Nike
- Louis Vuitton
- Samsung
- McDonald's
- Ray-Ban

L'Identité Numérique



- Anonymat
- Fake News
- Manipulation
- Menace des démocraties

Le Problème actuel – La dépendance des géants du Net



Collecteur des Données*
Monétisation des Données

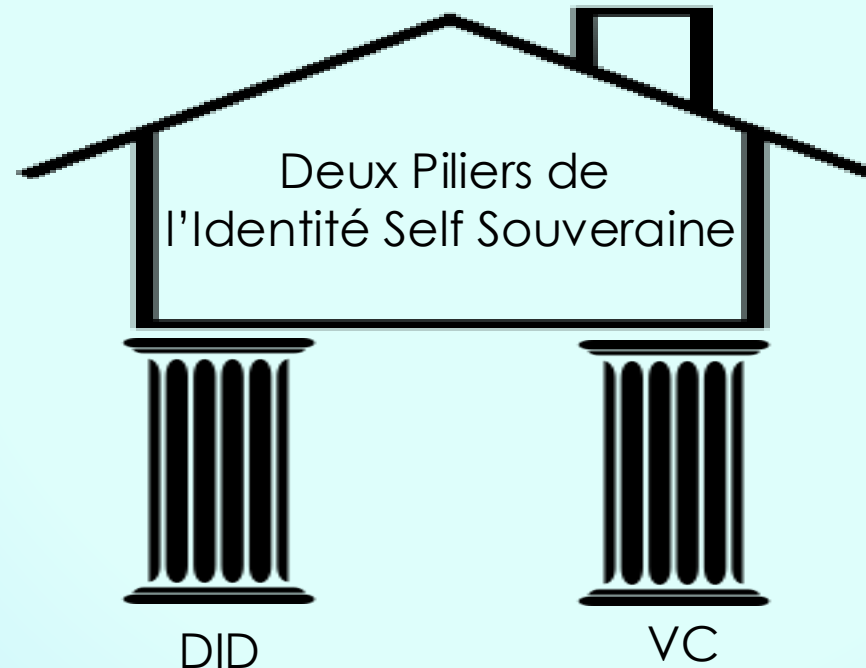
+

**Ils nous attribuent
des Identités numériques
"traçabilité
et collecte de données"**

* Nous sommes responsables

L'Identité Self-Souveraine (SSI)

- Attribuer des Identificateurs Universels aux personnes physiques et morales, aux objets, aux données ...(DID)
- Y associer des attestations vérifiables (VC)

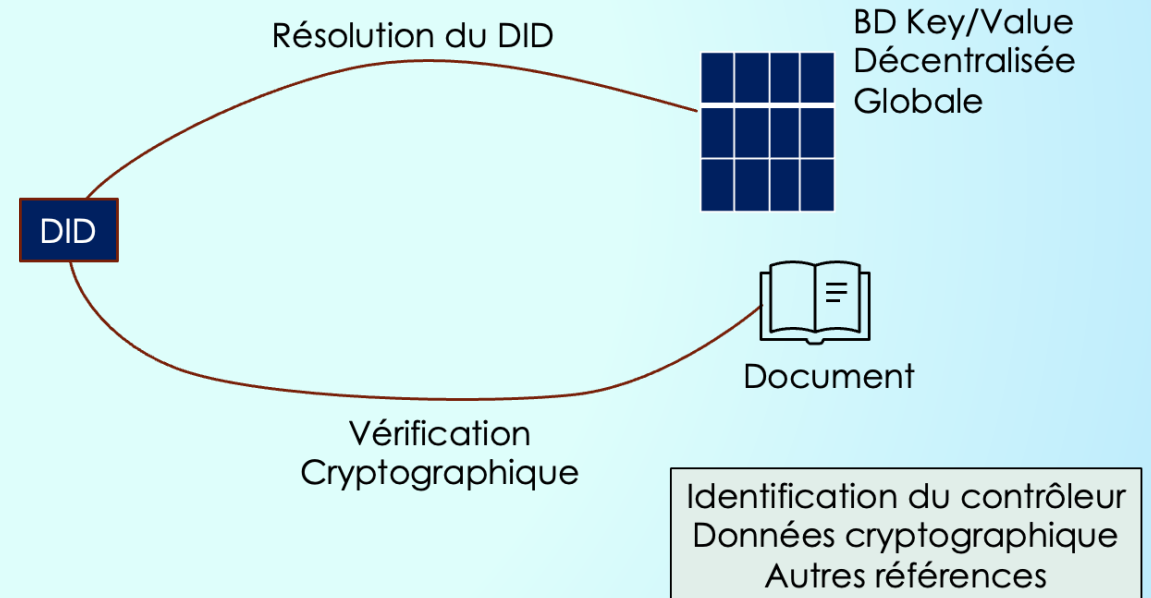


SSI: Self Sovereign Identity

Les DID ancrés sur la Blockchain

**Nouveau Type d'identificateur
Permettant la création d'une identité décentralisée**

Scheme
did:example:123456789abcdefghijk
DID Method DID Method Specific String

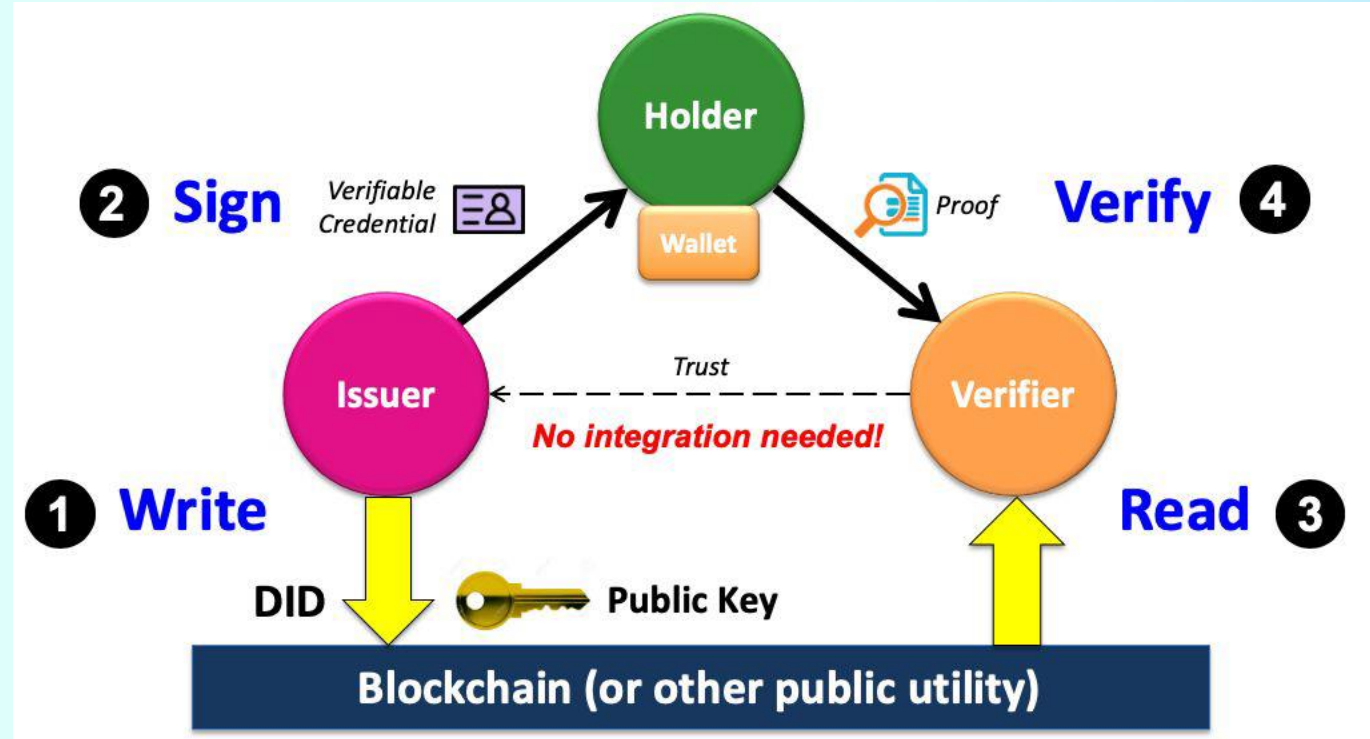
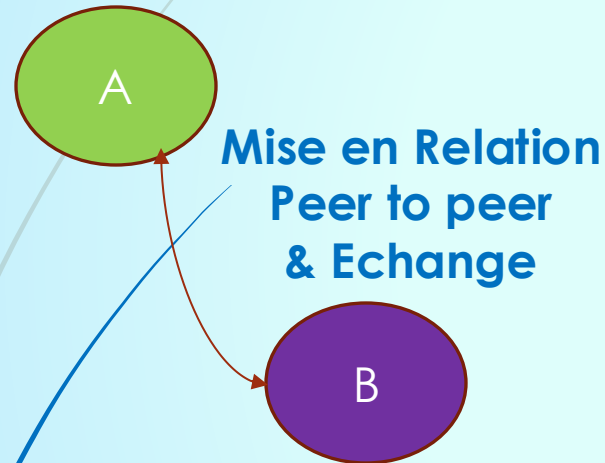


Decentralized Identifiers (DID)

Principales Caractéristiques

- **Simple à générer**
- **Décentralisé** – sans intermédiaire
- **Persistant**
- **Vérifiable** - par cryptographie
- **Traductible/Solvable**: pointe sur des metadata

DID : Divers Modèles de Confiance





Welcome to the Web 3 World



Web1

- Open source internet protocols from the 70s and 80s, including TCP, IP, SMTP and HTTP.
- Designed in the spirit of openness and inclusiveness.
- Anyone could build on top of them without anyone's permission.



Web2

- Open source is hard to monetize.
- Web2's business model depended on building proprietary, closed protocols on top of the Internet's open ones.
- Several of these companies are now the most valuable in history, and while we use them for free, we have to place trust in models that sell user data and opaque code.



Web3

- Like Web1, open source protocols, but collectively owned through cryptoeconomics.
- Independent of traditional organizations, code executed as written.
- Values open source software, user ownership of data, and permissionless access.
- Creates a shared sense of identity and collaboration.

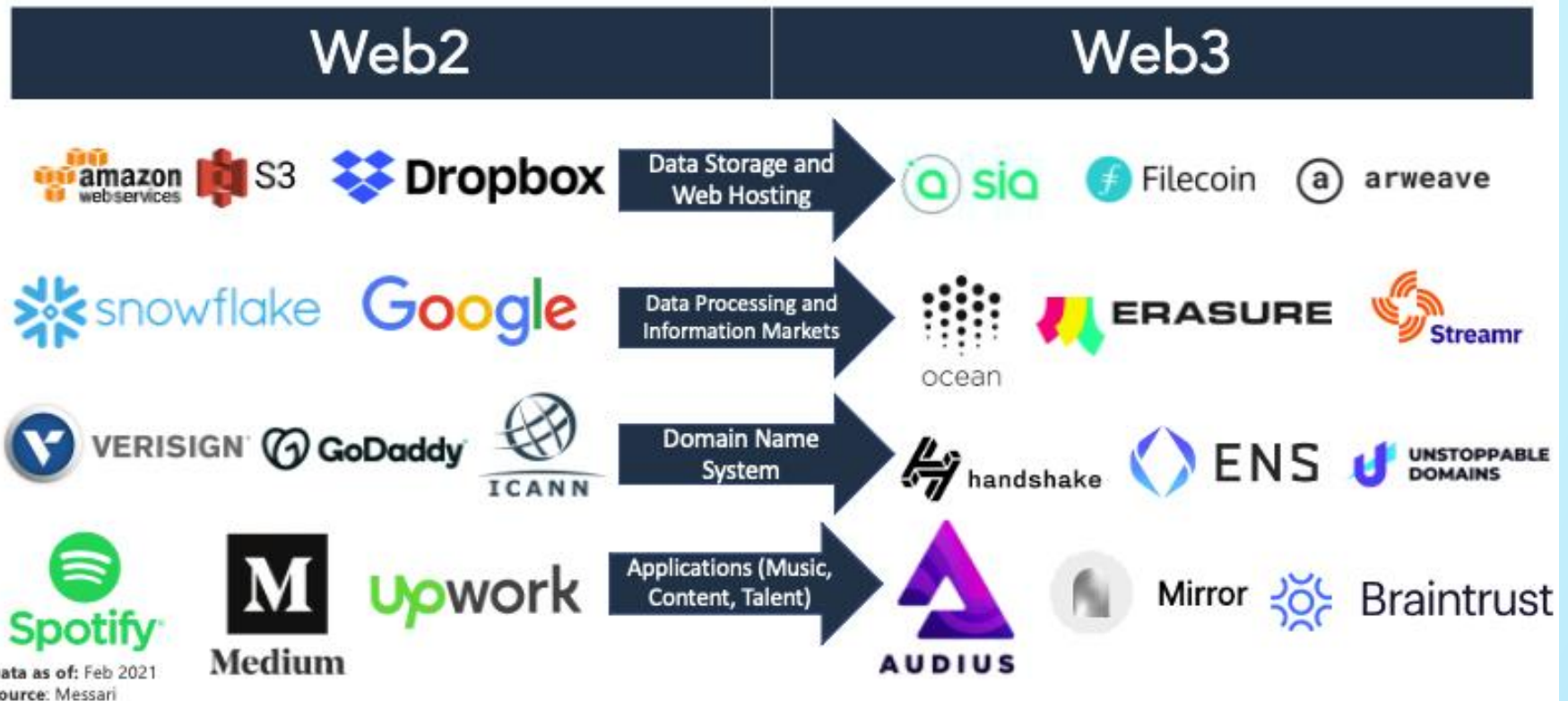
Rendre
À l'utilisateur
Une autonomie
Et une
Maîtrise
Et contrôle
De ses Données
Et des ses
Actifs
Numériques

Web 2 vs. Web 3

MESSARI

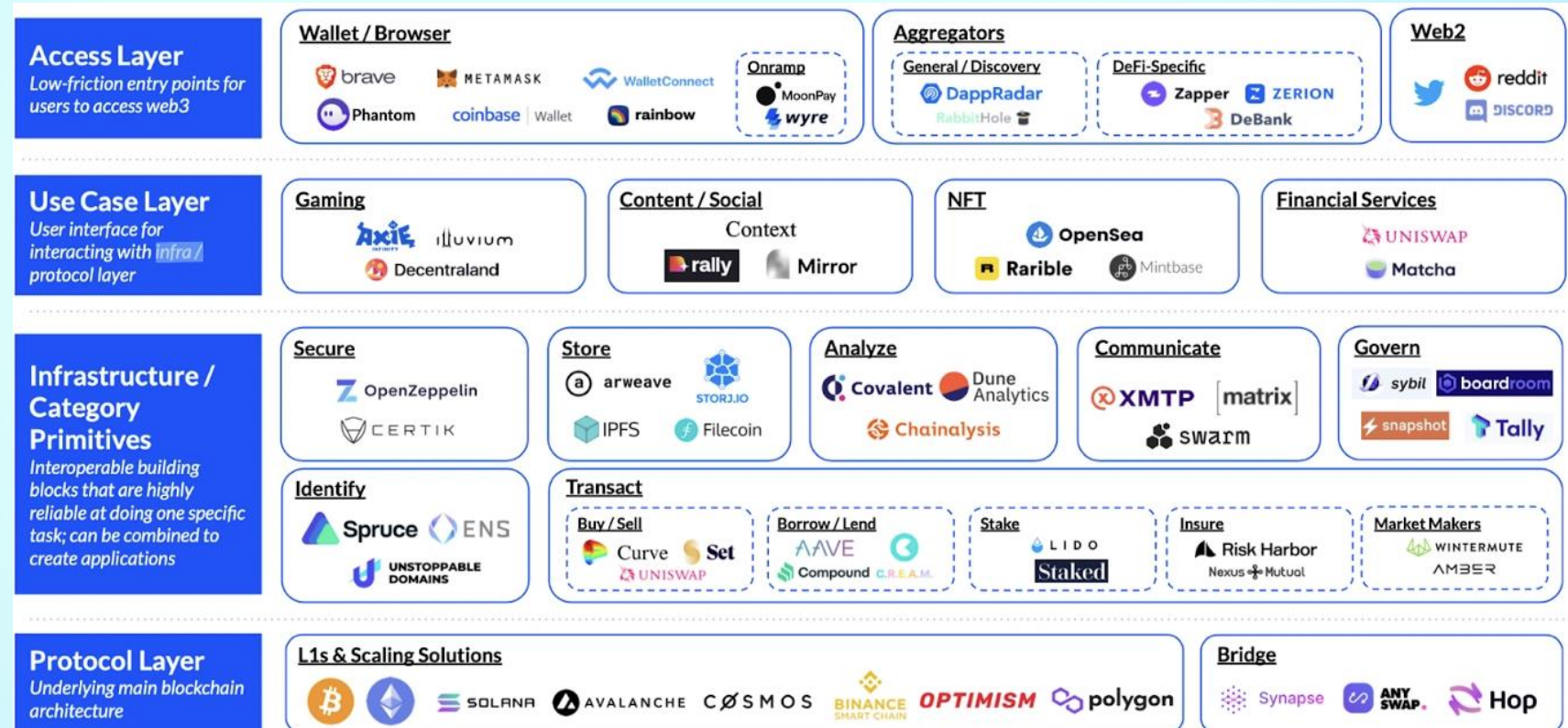
Web2 Companies Vs. Web3 Protocols

Web3 protocols aiming to replace or compete with web2 companies



Data as of: Feb 2021
Source: Messari

Web 3 Stack – An illustration



Acteurs Types du Web 3

- Chainlink
- Filecoin
- Arweave
- The Graph
- Golem
- Audius

Google Cloud and Coinbase announced a new, long-term strategic partnership to better serve the growing Web3 ecosystem and its developers.

Screeners		Web3	24H	
Mcap: \$14.13B		ROI: -4.34%	LINK dominance: 28,97%	
#	Asset	Price	24H	▼ Mcap
1	Chainlink	\$8.37	-1.35%	\$4.09B
2	Filecoin	\$5.73	-8.44%	\$1.81B
3	Theta Netwc	\$1.20	-6.72%	\$1.20B
4	Arweave	\$13.95	-9.26%	\$699M
5	The Graph	\$0.0892	-6.16%	\$659M
6	Helium	\$3.90	-5.17%	\$516M
7	Basic Attenti	\$0.330	+0.29%	\$492M
8	BitDAO	\$0.408	-4.32%	\$440M
9	Stacks	\$0.317	-4.14%	\$426M
10	Ethereum Ni	\$16.37	-5.68%	\$422M
11	Mask Netwo	\$4.43	-8.67%	\$299M
12	Render Token	\$0.932	-2.87%	\$280M
13	Golem	\$0.275	-2.67%	\$275M
14	Livepeer	\$9.96	-4.26%	\$249M
15	Audius	\$0.218	-5.59%	\$201M

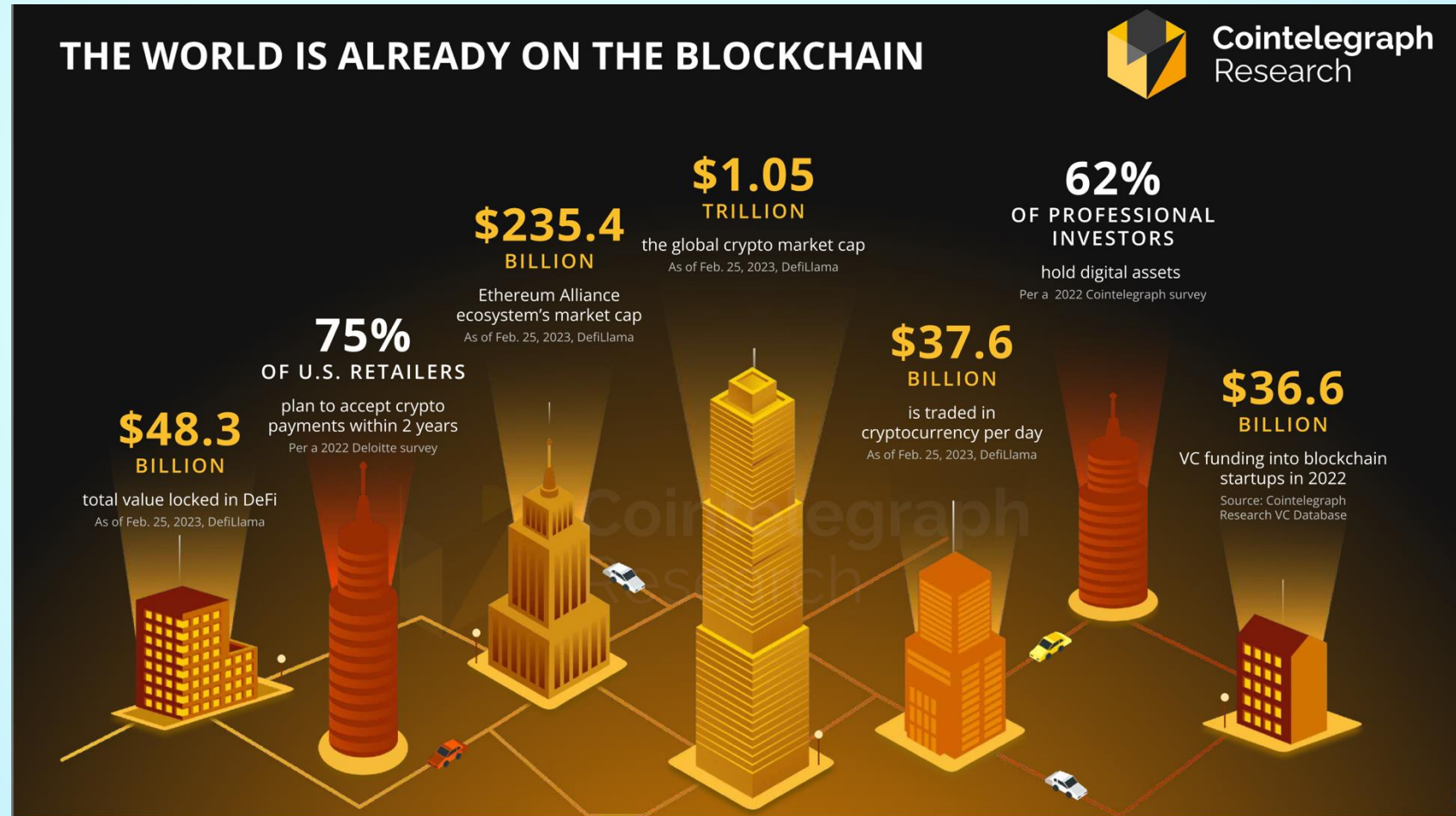
Perspectives

Rappel Bitcoin Primer – A retenir

Bitcoin – le réseau ... bitcoin – La monnaie

- Le *Bitcoin* est le premier **réseau distribué de règlement des paiements**, non permissionné (sans autorisation), pair à pair, fondé sur le consensus, et résistant à la censure
- Le *bitcoin* (BTC), l'actif natif de la blockchain *Bitcoin*, est la première monnaie numérique au monde **sans banque centrale ni administrateur**.
- Souvent qualifiés d'or numérique, les bitcoins suivent une **politique monétaire prévisible et stable** qui fonctionne de manière autonome, ce qui leurs confère des propriétés idéales de réserve de valeur.
- Pour sécuriser son réseau, le Bitcoin utilise un mécanisme de consensus connu sous le nom de **Proof-of-Work (PoW)** pour résoudre le "problème de double dépense".
- Le PoW exige des participants (mineurs) qu'ils apportent leur puissance de calcul pour résoudre des **puzzles mathématiques** afin d'ajouter un nouveau bloc à la blockchain.
- Les *bitcoins* sont **attribués (donc minés)** au mineur qui résout l'énigme en premier, ce qui permet de produire de nouveaux bitcoins.

February 25, 2023



Blockchain Use...

KEY HIGHLIGHTS: BLOCKCHAIN USE IS EVIDENT ACROSS ALL SECTORS



MAJOR BRANDS IN WEB3 ARE AMONG THE FIRST BRANDS TO START OPERATING IN THE METAVERSE AND WEB3



FASHION

	Created the Collezione Genesi NFT collection		Already selling NFTs at their virtual fashion shows in the metaverse
	Launched a charity organization with crypto payment options for their customers		Developed the Aura Blockchain Consortium, the world's first global luxury blockchain
	Released special skins for the game		Utilizing the Hedera protocol, Mars-Wrigley plans to expand into the metaverse and offer limited edition NFT T-shirts

SPORTS

	Top football leagues have launched their tokens. Manchester United has onboarded Tezos as its official Web3 and training kit partner
	The daily trading volume on the NBA Top Shot marketplace reached \$45.7 million in February 2021

Bitcoin's Utility and Discounted Price based on Network Fundamentals and Adoption

Year	2022	2023	2024	2025
Total potential	\$86,935,404,472,056	\$97,414,698,237,177	\$109,238,354,310,555	\$122,590,159,746,060
Transaction Value Processing	\$3,546,338,091,754	\$9,242,914,402,103	\$22,430,813,952,226	\$47,700,150,209,938
Circulating tokens	\$19,030,000	\$19,360,000	\$19,690,000	\$19,850,000
Network Monetary Base Necessary	\$584,868,786,674	\$1,524,358,927,949	\$3,699,332,269,208	\$7,866,799,006,649
Utility price	\$30,734	\$78,738	\$187,879	\$396,312
Discounted price	\$30,734	\$60,567	\$111,171	\$180,388

La Technologie de la Blockchain est dans un
stade naissant dans un cycle de 20 ou 50 ans de
maturation

Evolution permanente vers plus de performance,
plus de privacy et de l'interopérabilité

Horizons applicatifs sans limites

Certains comparent la **blockchain d'aujourd'hui**
au la vague Internet en 1995

Internet

Diffusion de l'information
Librement et sans Frontière

Cryptomonnaie
Monnaie Libre
& Sans Frontière

2009

Blockchain
Internet of Values

2015 - 2021

Web 3
NFT World
Univers Multiples

2022
beyond