

La Blockchain : de la Cryptomonnaie au Web 3

Najah NAFFAH

Quantum Blockchain Secure

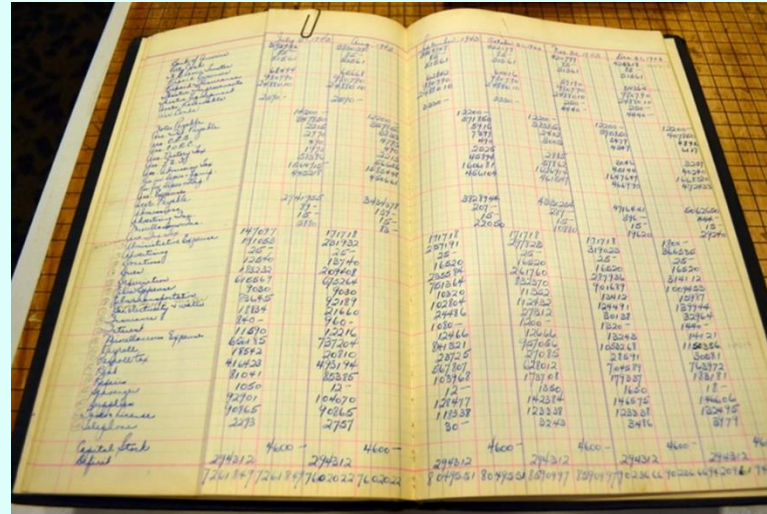
14 Novembre 2022

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 -

Qu'est ce qu'une Blockchain ?

Un Livre
Comptable



The Foundation
A Ledger
(DLT Distributed Ledger Technology)

Qu'est ce qu'une Blockchain ?

Réseaux de Nœuds "pair à pair"

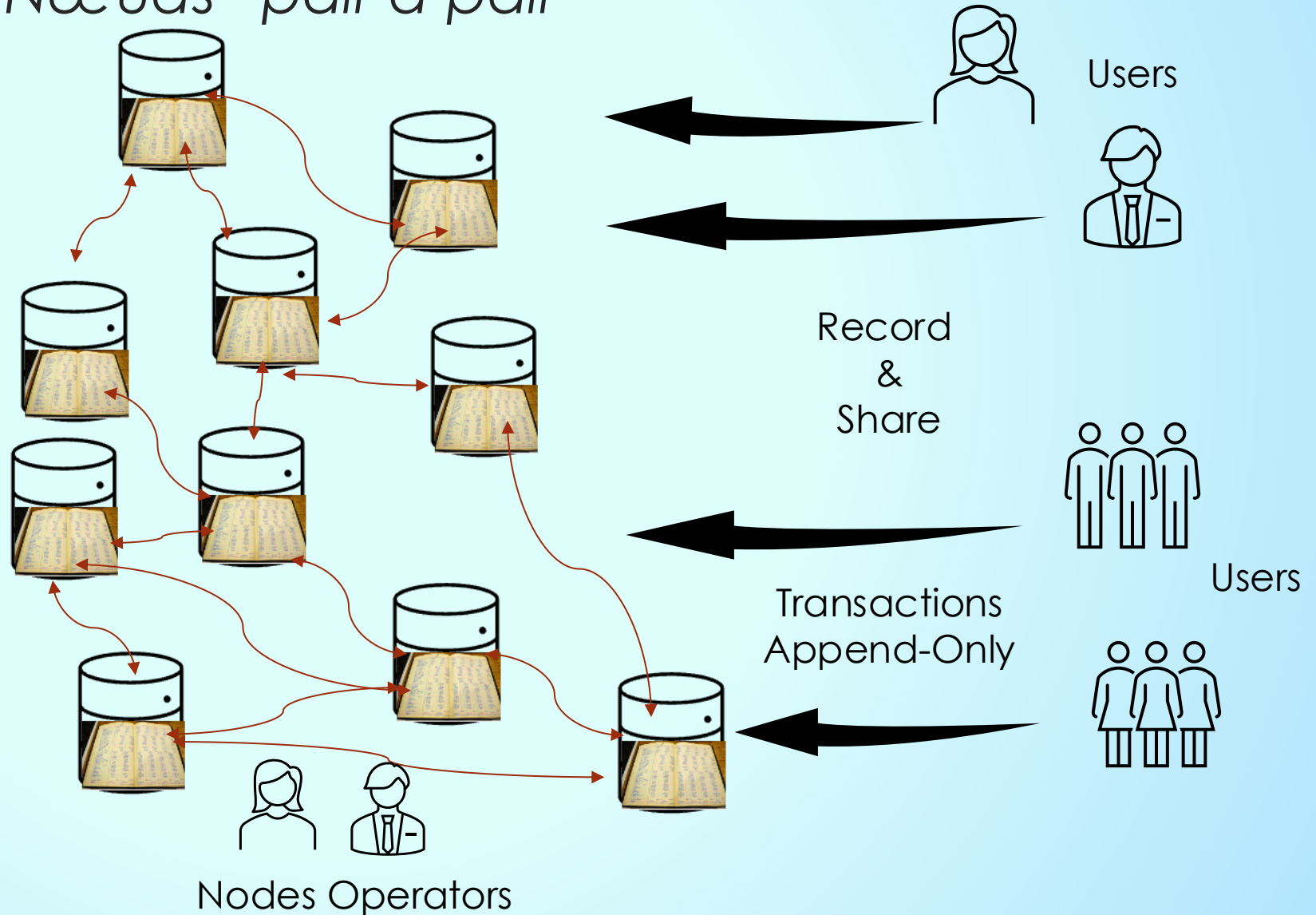
Même Copie
(tous les Nœuds)

Sans
Autorité Centrale

Sécurisé
Cryptographie

Ajout de Blocs (Tx)
(append-only)

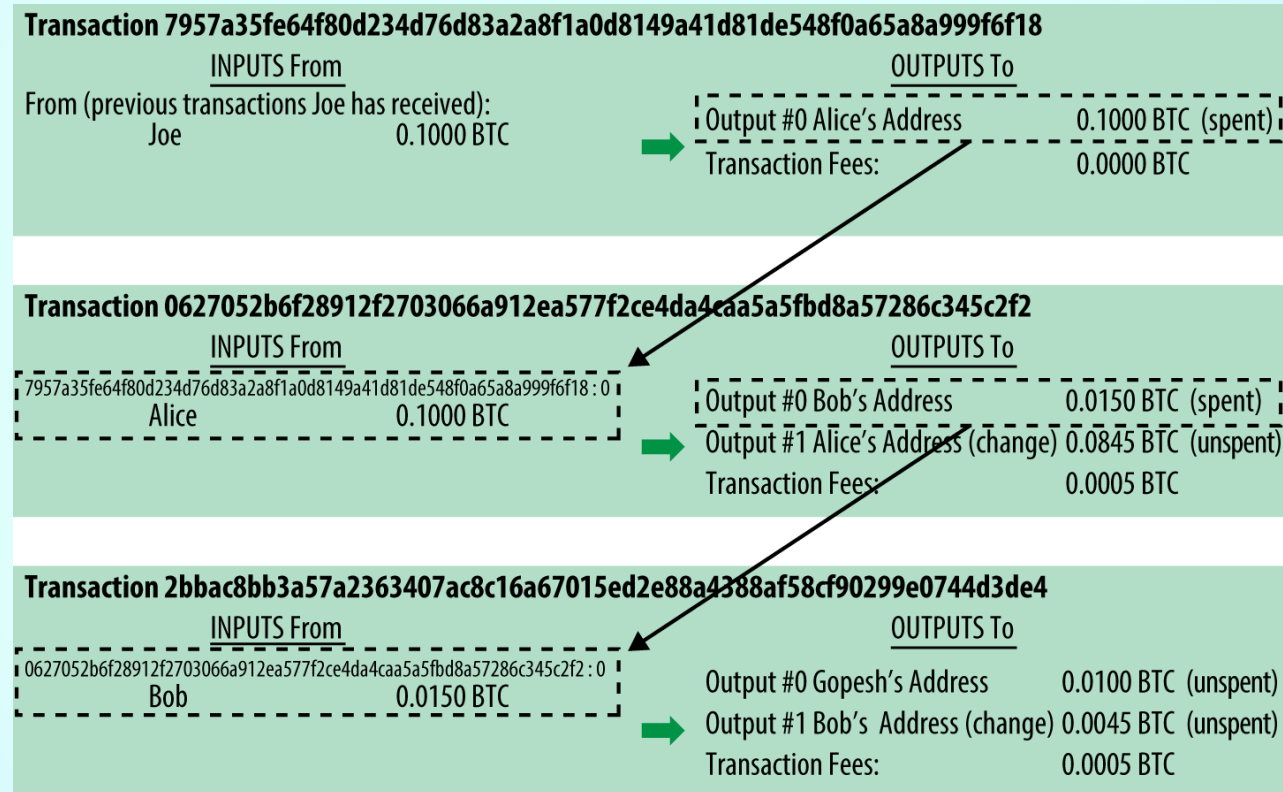
Immuable,
Transactions publiées
(non modifiables)



Nodes Operators

Contenu du Ledger

Chain of transactions: from Joe to Alice to Bob



Output of one Tx is the input of the next Tx

Buying a cup of coffee at Bob's coffee shop in Palo Alto, California.

Bob says,
"That's one-dollar-fifty,
or fifteen millibits. »
Alice choisit de payer en
BTC!



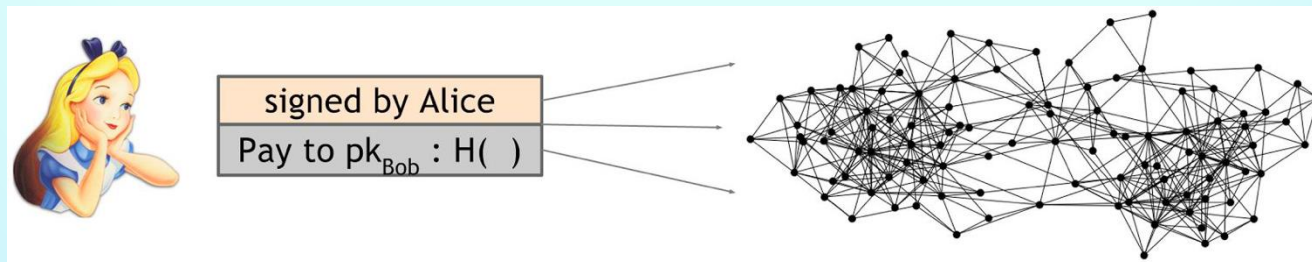
Payment request QR code
Généré par l'appareil du vendeur,
et scanné par Alice avant
d'appuyer sur Envoi
(Alice avait au préalable reçu 0,1
BTC de Joe)

A Bitcoin address: "1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA »

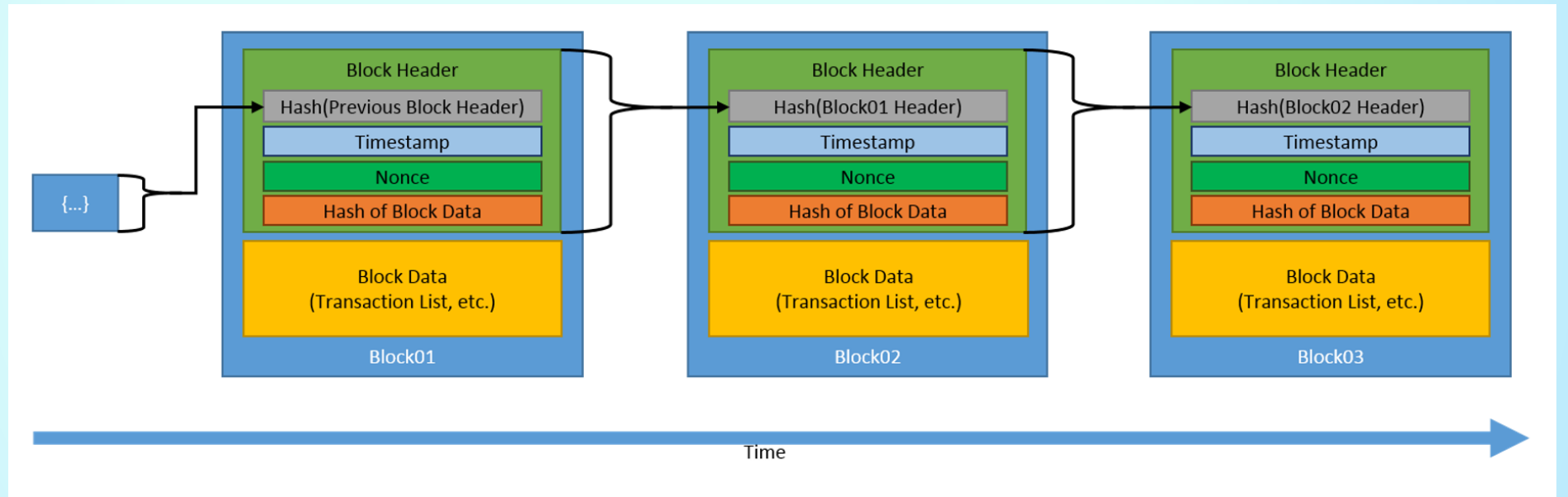
The payment amount: "0.015"

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

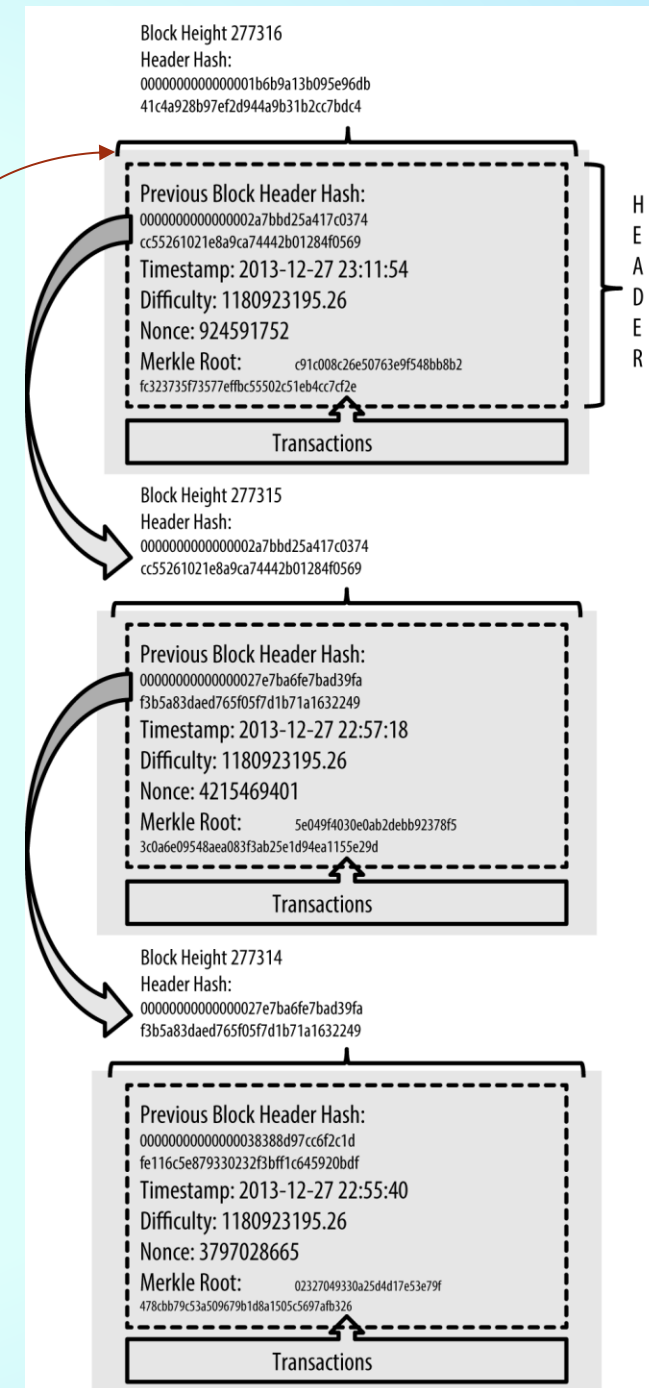
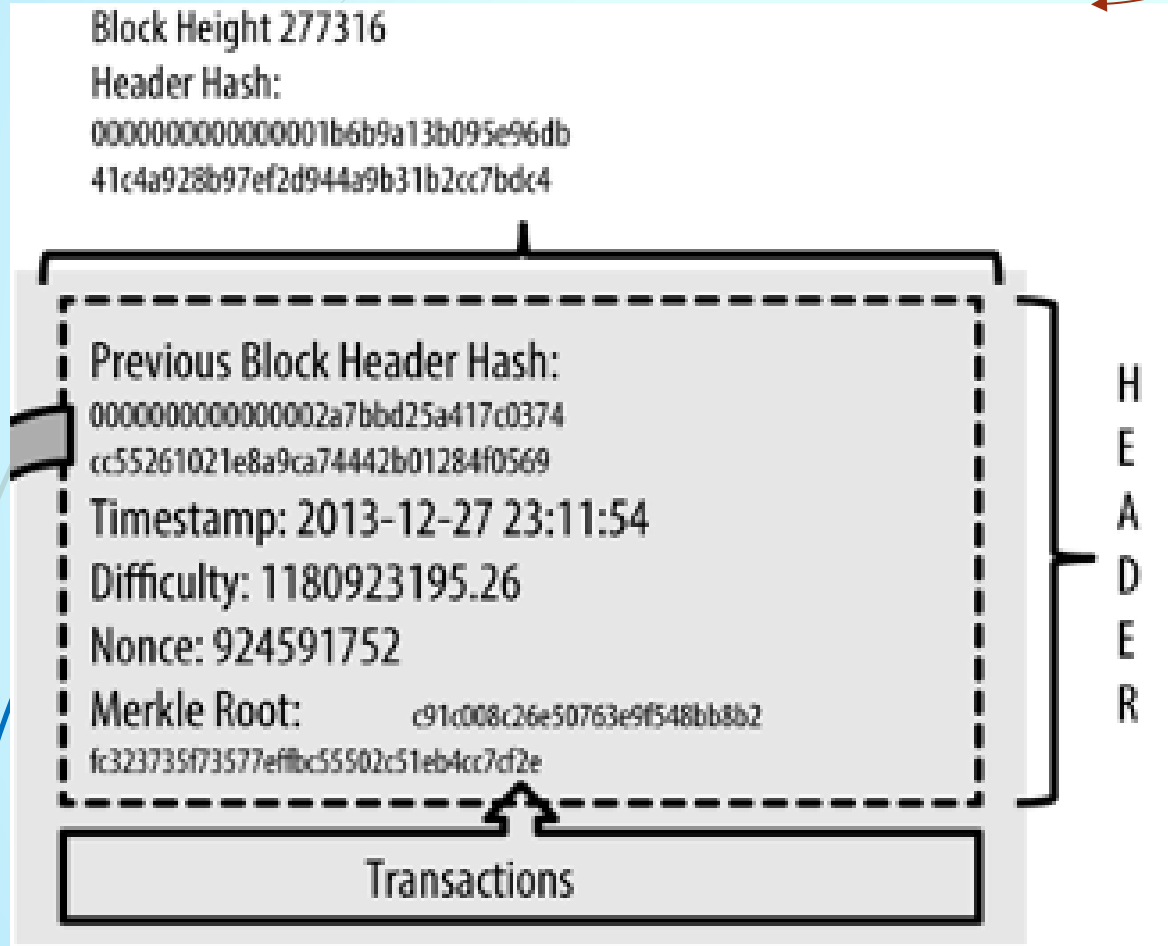
A description for the payment: "Purchase at Bob's Cafe"



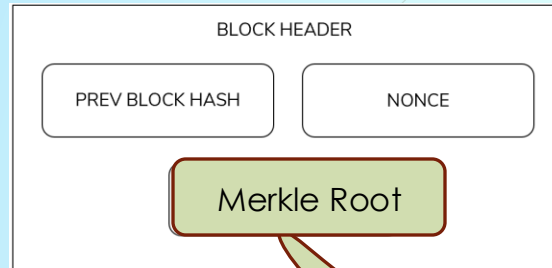
What's Inside the



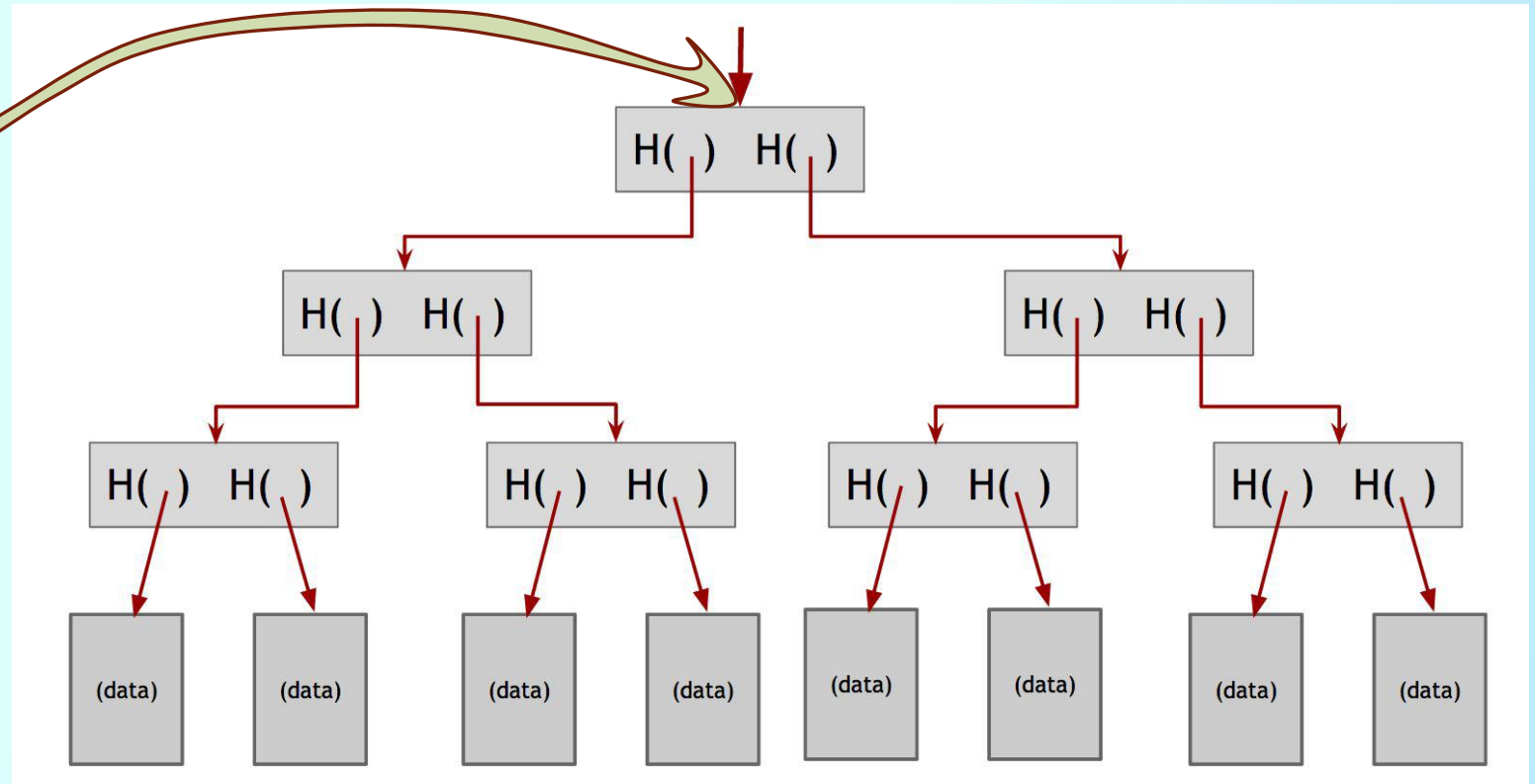
Un Zoom sur la Chaîne de Blocs



Blockchain Data Structure



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

L'Annonce de Satoshi ...

Il y a 14 ans (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
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.

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**

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, l'économie et la gouvernance des organisations*

Les Garanties du réseau

building blocks pour créer des nouvelles applications

- No Double-Spend
- Immutability
- Neutrality
- Secure Timestamping
- Authorization
- Auditability
- Accounting
- Non expiration
- Integrity
- Transaction Atomicity.
- Discrete (Indivisible) Units of Value
- Quorum of Control.
- Timelock/Aging.
- Replication
- Forgery Protection
- Consistency
- Predictable Issuance

Une Comparaison avec le \$

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



Depuis le 23 avril 2011....10:29

- Après l'envoi du mail ci-dessous, Satoshi Nakamoto rejoint le 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

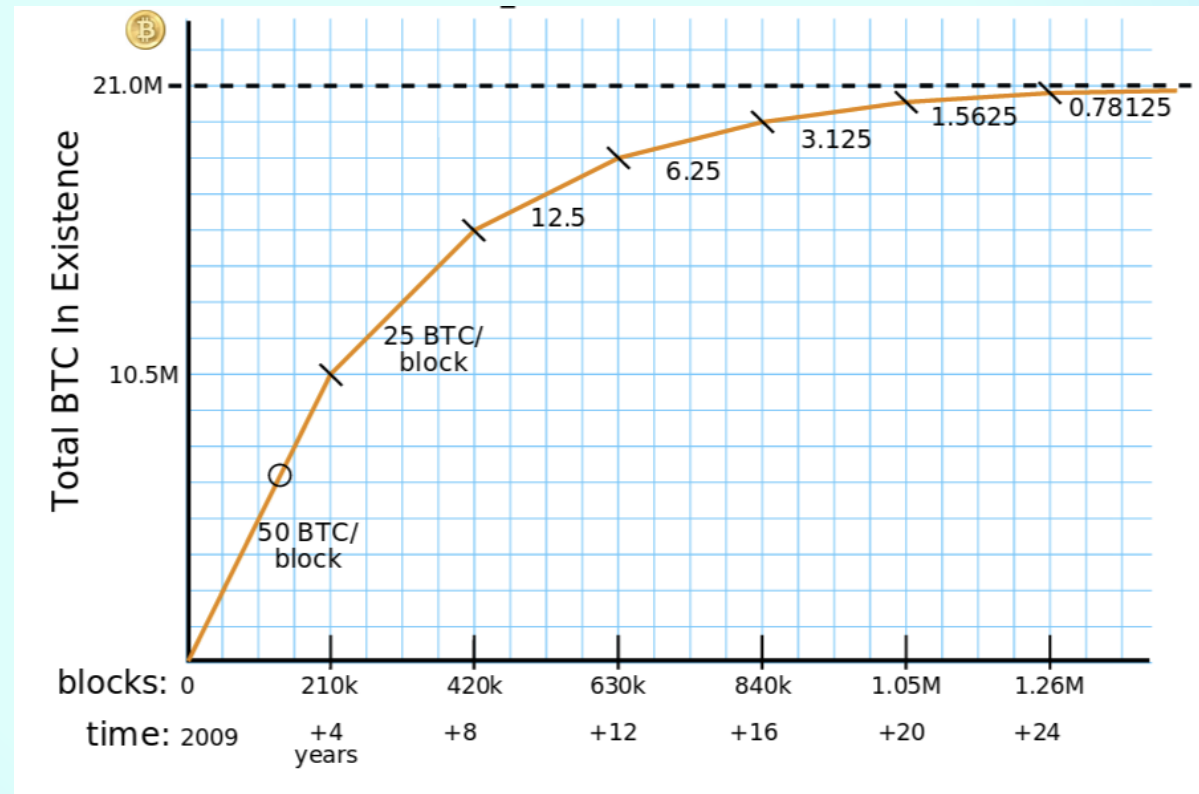
Satoshi Nakamoto satoshin@gmx.com

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.

La Courbe de Minage Génération des Bitcoins

210.000 Blocks,
50% decrease (4 years), 32 halvings)
50 – 25 – 12,5 – 6,25 – 3,125....
1/1/2009 - 50
11/2012 - 25
.....
05/2020 – 6.25
.....



In 2140, almost 21 million bitcoin, will be issued
Coinbase transaction: **Pay Jing's address 25.09094928 bitcoin**

BTC Nov 14, 2022

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

Nouveaux Bitcoins

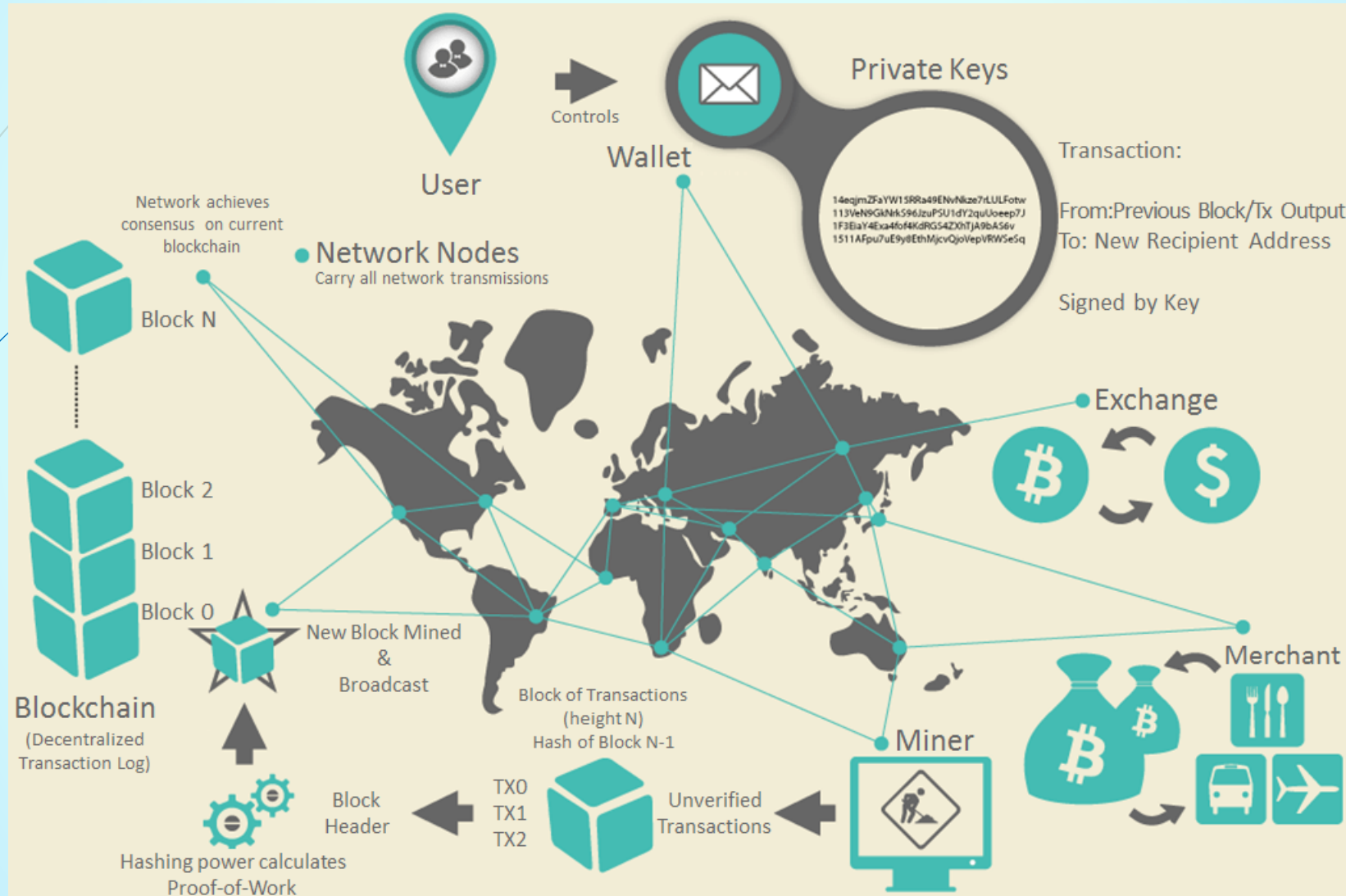
Reward Per Block	6.25+0.1264 BTC (\$106,634.75)
Reward last 24h	868.75+17.57 BTC (\$14,822,230.13)
Difficulty	36.762 T
Hashrate	251.507 Ehash/s -15.76% in 24 hours
Mining Profitability	0.0589 USD/Day for 1 THash/s
Top 100 Richest	2,898,784 BTC (\$48,477,113,897) 15.09% Total
Wealth Distribution Top 10/100/1,000/10,000 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)

Bitcoin Network Ecosystem



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

- 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



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]

Explorer

Bitcoin Rich List Oct 20, 2022

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

Les Adresses Dormantes...

	Address	Balance	% of coins	First In
1	1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF	79,957 BTC (\$1,337,145,269)	0.4163%	2011-03-01 11:26:19
2	12ib7dApVFvg82TXKycWBNpN8kFyiAN1dr wallet: 967	31,000 BTC (\$518,422,201)	0.1614%	2010-05-13 10:22:38
3	12tkqA9xSoowkzoERHmWNKsTey55YEBqkv	28,151 BTC (\$470,777,422)	0.14657%	2010-04-06 00:47:07
4	1PeizMg76Cf96nUQrYg8xuoZWLQozU5zGW	19,414 BTC (\$324,672,538)	0.10108%	2010-07-24 14:16:11
5	1F34duy2eeMz5mSrvFepVzy7Y1rBsnAyWC	10,771 BTC (\$180,118,433)	0.056077%	2011-08-09 00:14:47
6	1f1miYFQWTzdLiCBxtHHnNiW7WAWPUccr	10,009 BTC (\$167,387,487)	0.052114%	2011-05-04 04:10:49
7	1BAFWQhH9pNkz3mZDQ1tWrtKkSHVCkc3fV	10,000 BTC (\$167,233,877)	0.052066%	2011-05-04 04:01:23
8	14YK4mzJGo5NKKnmVJeuEAQftLt795Gec	10,000 BTC (\$167,233,160)	0.052066%	2011-05-04 03:40:51
9	1KbrSKrT3GeEruTuuYYUSQ35JwKbrAWJYm	10,000 BTC (\$167,232,862)	0.052065%	2011-04-03 00:18:45
10	1P1IThxBH542Gmk1kZNxyji4E4iwpvSbrt	10,000 BTC (\$167,232,796)	0.052065%	2011-05-04 03:14:27

79,957.22¹⁹⁴⁴⁸ BTC
 Balance: 1,337,145,268.76 USD

Received: 79,957.22¹⁹ BTC (437 ins) first: 2011-03-01 last: 2022-10-26

Sent: 0 BTC (0 outs) first: last:

Profit from price change: 1,337,069,797.7 USD

Unspent outputs: 437

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 au mineur qui résout l'énigme en premier, ce qui permet de produire de nouveaux bitcoins.

2nd Generation Blockchains – Programmable

Smart Contract Platforms , Market Cap Aug 1,2022 \$ 342 B

- **Ethereum (59,19%)**
- BNB
- Cardano
- **Solana**
- **Polkadot**
- TRON
- **Avalanche**
- Cosmos
- Near
- **Algorand**
- VeChain, Flow, Terra Luna, Hedera (15)
- **Tezos** (18)

Screeners Smart Contract Platfo... 24H				
Mcap: \$326B		ROI: -3.74%		ETH dominance: 59,19%
#	Asset	Price	24H	Mcap
1	 Ethereum	\$1,577.73	-2.60%	\$193B
2	 BNB	\$330.02	-6.18%	\$52.89B
3	 Cardano	\$0.410	-2.80%	\$14.11B
4	 Solana	\$31.42	-12.11%	\$11.27B
5	 Polkadot	\$6.90	-2.43%	\$8.07B
6	 TRON	\$0.0623	-3.73%	\$5.75B
7	 Avalanche	\$18.23	-5.81%	\$5.46B
8	 Cosmos	\$14.22	-5.18%	\$4.08B
9	 Ethereum Cl	\$25.28	-3.38%	\$3.49B
10	 Algorand	\$0.426	-2.98%	\$3.04B
11	 NEAR Proto	\$3.08	-5.84%	\$2.52B
12	 VeChain	\$0.0260	+0.58%	\$1.89B
13	 Flow	\$1.73	-4.04%	\$1.80B
14	 Terra Luna C	\$0.000235	-4.73%	\$1.62B
15	 Hedera Hasf	\$0.0591	-4.54%	\$1.46B

Ethereum Vitalik Buterin

Blockchain (SC)
(Smartphone)



Bitcoin
(calculatrice)



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

- Né le 31 Janvier 1994, Kolomna, Moscow Oblast, Russie. (28 a)
- A Russian/Canadian computer programmer called Vitalik Buterin 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**

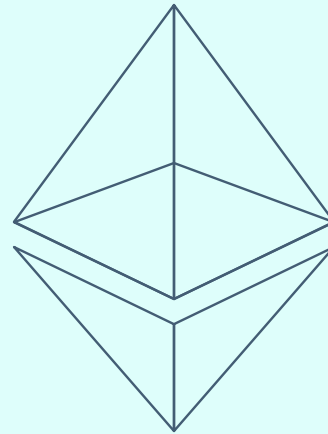
- 10x larger than second
largest blockchain community

**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**



ENTERPRISE
ETHEREUM
ALLIANCE

ERC
Standards

Fondements Technologiques

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**

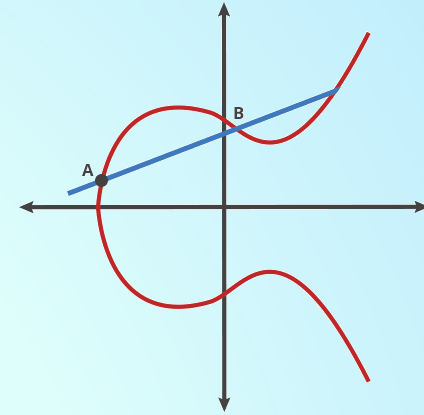
Input Text	SHA-256 Digest Value
1	0x6b86b273ff34fcea19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Hello, World!	0xdf6d6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

Asymmetric-key cryptography

- Blockchain technology uses **asymmetric-key cryptography** (also referred to as **public key cryptography**).
- Asymmetric-key cryptography uses a **pair of keys**:
 - a **public key** and a **private key** that are **mathematically related** to each other.
- The public key is **made public** *without reducing the security of the process*,
- the private key must **remain secret**
- Even though there is a relationship between the two keys, the private key **cannot efficiently be determined** based on knowledge of the public key.
- One can **encrypt with a private key** and then **decrypt with the public key**.
- Alternately, one can **encrypt with a public key** and then **decrypt with a private key**.

ECC $y^2 = x^3 + ax + b$

- ▶ An **elliptic curve cryptosystem** can be defined by:
 - ▶ picking a prime number as a maximum,
 - ▶ a curve equation
 - ▶ a public point on the curve.
- ▶ A **private key** is a number *priv*
- ▶ A **public key** is the public point **dotted with itself *priv* times.**
- ▶ Computing the private key from the public key in this kind of cryptosystem is called the **elliptic curve discrete logarithm function (the *Trapdoor Function*)**



The **secp256k1 curve** is defined by the following function, which produces an elliptic curve:

$$\{y^2 \bmod p = (x^3 + 7) \bmod p\}$$

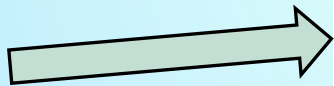
The *mod p* (modulo prime number p) indicates that this curve is over a finite field of prime order p , where $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$, a very large prime number.

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

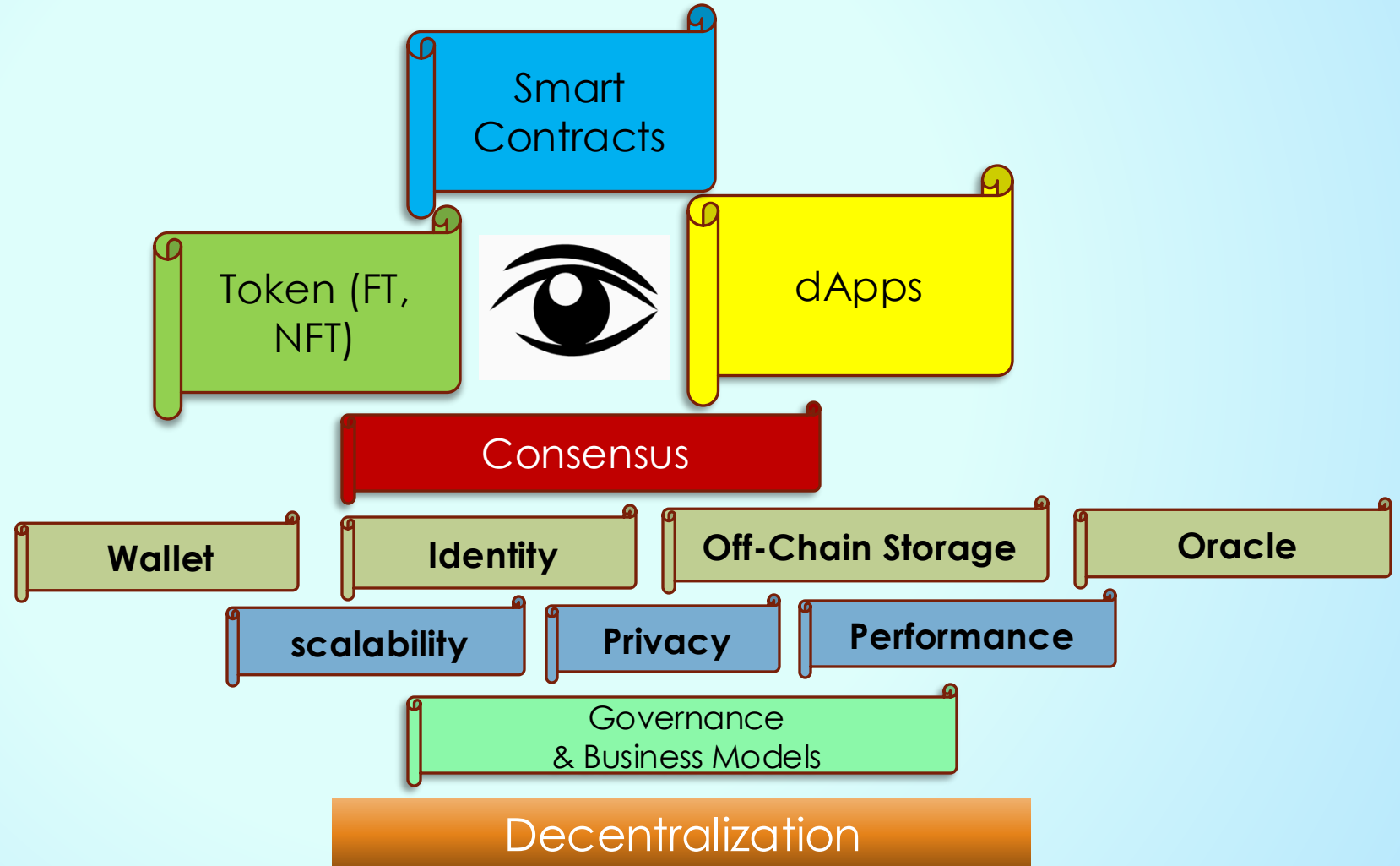
Cryptosystem	Category	Key Size	Security Parameter	Quantum Algorithm Expected to Defeat Cryptosystem	# Logical Qubits Required	# Physical Qubits Required ^a	Time Required to Break System ^b	Quantum-Resilient Replacement Strategies
AES-GCM ^c	Symmetric encryption	128 192 256	128 192 256	Grover's algorithm	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



Blocks

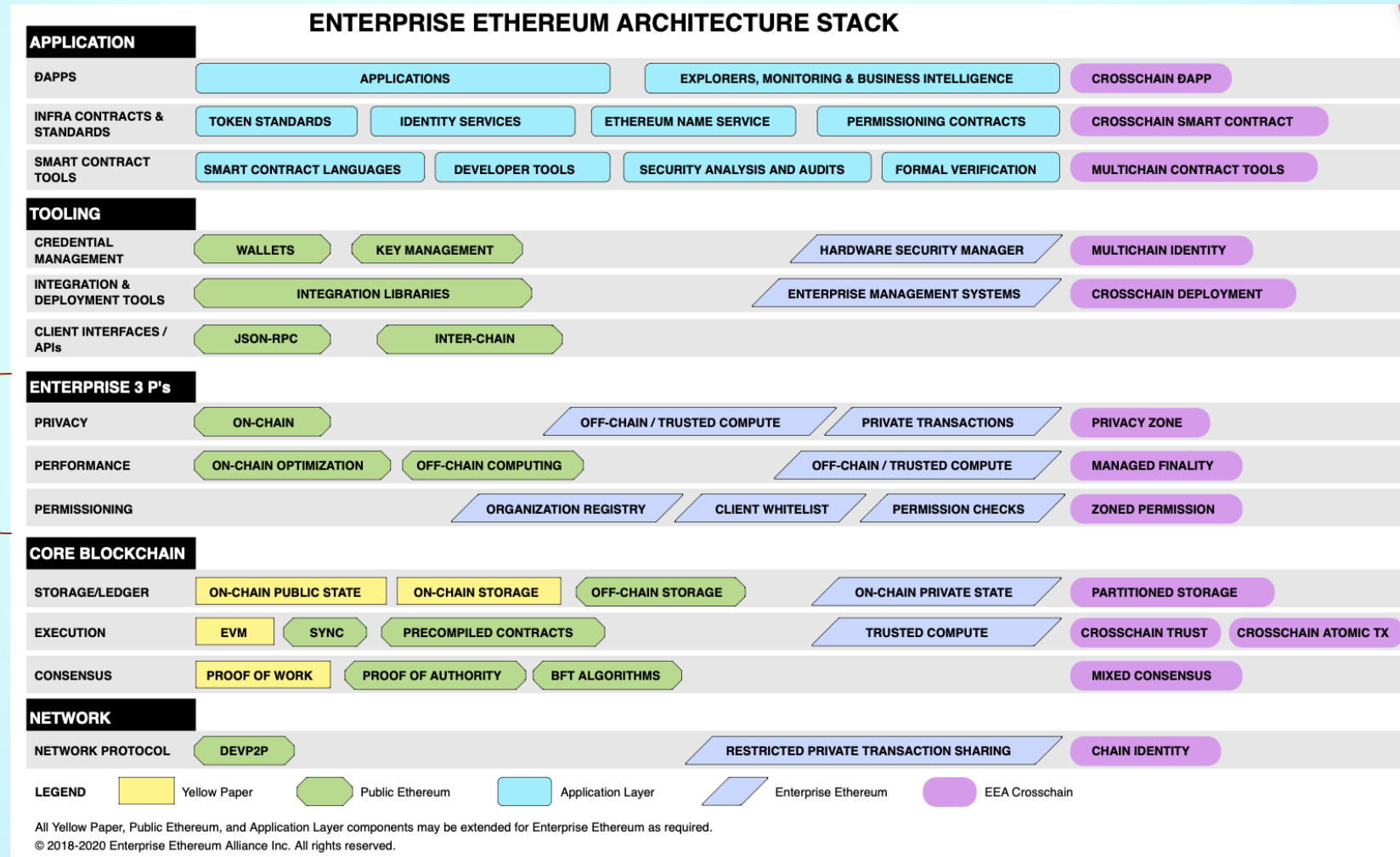
- Users submit **candidate transactions** to the blockchain network via software (desktop applications, smartphone applications, digital wallets, web services, etc.).
- The software sends these **transactions to a node or nodes** within the blockchain network.
- The chosen nodes may be **non-publishing full nodes** as well as **publishing nodes**.
- The submitted transactions are then **propagated to the other nodes** in the network
- Once a pending transaction has been distributed to nodes, it must then **wait in a queue** until it is added to the blockchain by a publishing node.
- **Transactions are added to the blockchain when a publishing node publishes a “valid” block.**

Rendre Opérationnelle une Blockchain...



Déployer un Stack Technologique

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



Consensus Protocols

BFT Byzantine Fault Tolerance

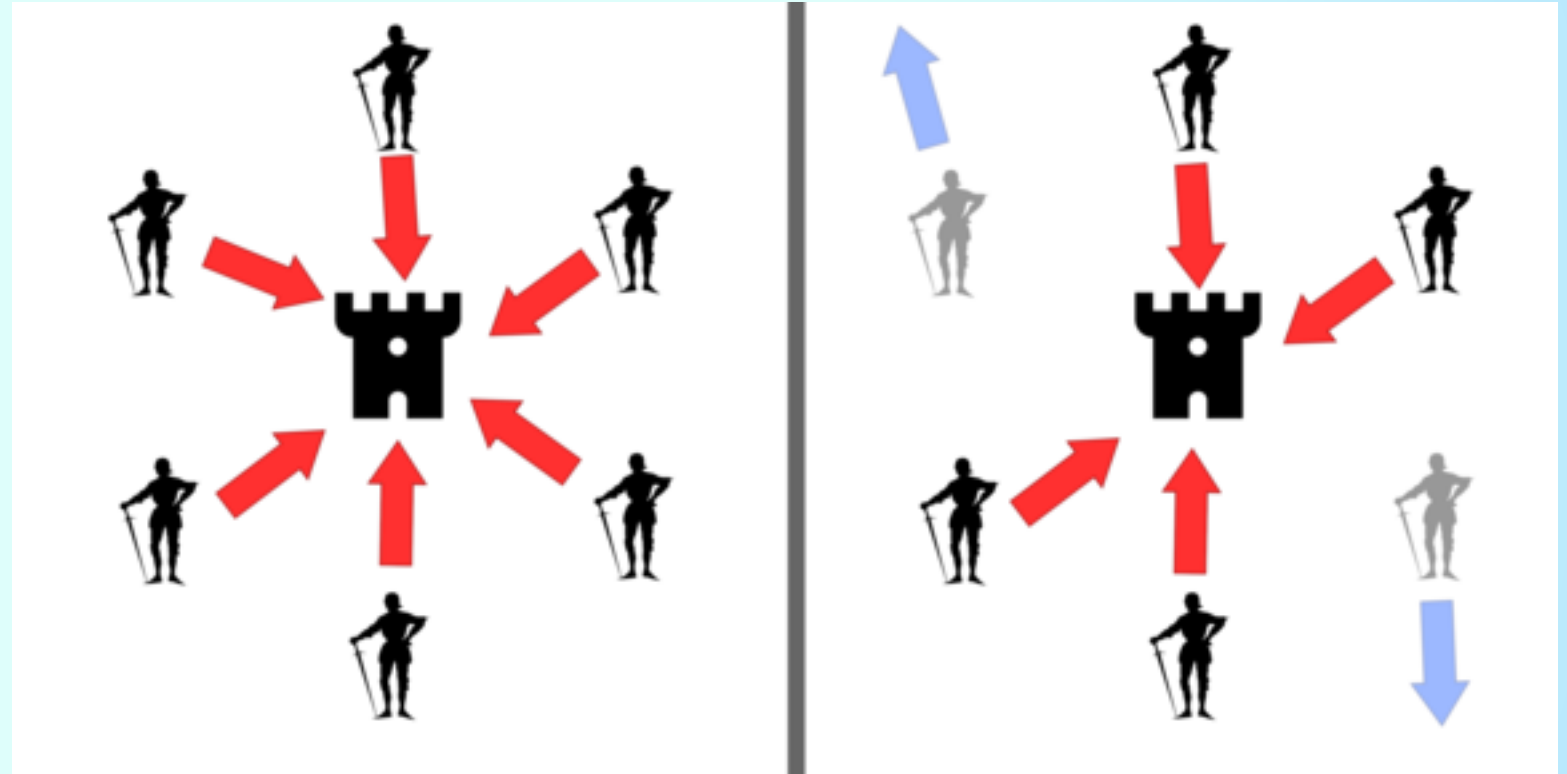


- Les généraux doivent seulement décider s'ils attaquent ou se retirent.
- Certains généraux préfèrent attaquer, d'autres se retirer et d'autres « suspects »
- Comment s'accorder sur une décision commune ?
- Le problème est compliqué par la présence de généraux traîtres qui peuvent émettre des votes 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

Proof of Work (PoW)

- Dans le modèle de **preuve de travail** (PoW), un utilisateur publie le prochain bloc en étant le premier à résoudre un puzzle (à calculs intensifs)
- La **solution de ce puzzle** est la "preuve" qu'il a effectué un travail !
- Le **puzzle** est conçu de manière à ce que sa **résolution soit difficile** mais sa **vérification soit facile**.
- Cela permet à tous les autres nœuds de **valider** facilement les blocs proposés, et de **rejeter** tout bloc incorrect
- Le puzzle, consiste à exiger que le **hash de l'entête de bloc soit inférieur à une valeur cible (la Difficulté** - cas du bitcoin).
- Pour résoudre, Les nœuds essaient des calculs successifs en **variant le nonce** dans l'entête du bloc.

PoS Ethereum

- Les valideurs sont récompensés pour avoir validé des blocs et générer des attestations
- Ils sont pénalisés s'ils n'assument pas leurs responsabilités (ex: sont offline).
- Les pénalités de l'offline sont relativement légères.
- Ainsi, si un valideur participe plus de la moitié du temps, ses récompenses seront positives.
- En revanche, si un valideur tente de compromettre la blockchain (ex: changement d'historique des données), un mécanisme de pénalité différent entre en jeu : *une partie substantielle de sa mise sera réduite (éventuellement jusqu'à la totalité de la mise) et il sera éjecté du réseau.*
- Le résultat est un risque financier énorme en cas d'échec de l'attaque d'un valideur.

Ethereum 2.0, le mécanisme de consensus PoS

- Afin de devenir un valideur, il faut déposer **32 ETH** dans le contrat de dépôt officiel Ethereum 2.0 .
- Chaque fois qu'un bloc est proposé, au moins 4 et jusqu'à 64 comités aléatoires de 128 nœuds de validation seront sélectionnés dans l'ensemble du pool de valideurs pour attester le bloc.
- La sécurité est prouvée, et il y a moins d'une chance sur mille milliards qu'un attaquant contrôlant $\frac{1}{3}$ des valideurs sur le réseau, puisse contrôler $\frac{2}{3}$ des valideurs d'un comité, pour réussir une attaque.
- Le réseau nécessitera la mise en jeu d'au moins 524 288 ETH, répartis sur 16.384 nœuds valideurs.

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 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.)

ERC 20 Scan Nov. 12, 2022

Etherscan

Eth: \$1,212.36 (-0.06%)

21 Gwei

All Filters

Search by Address / Txn Hash / Block / Token / Ens

Home

Blockchain

Tokens

Resources

More

Sign In

Token Tracker

ERC-20

ERC-20 Tokens

A total of 694,143 Token Contracts found

First

<

Page 1 of 20

>

Last

#	Token	Price	Change (%)	Volume (24H)	◄ Circulating Market Cap ?	On-Chain Market Cap ?	Holders
1	Tether USD (USDT) Tether gives you the joint benefits of open blockchain technology and traditional currency by converting your cash into a stable digital currency equivalent.	\$0.9984 0.000059 Btc 0.000824 Eth	▲ 0.34%	\$112,744,643,224.00	\$69,587,000,666.00	\$39,761,155,070.52	4,495,401
2	BNB (BNB) Binance aims to build a world-class crypto exchange, powering the future of crypto finance.	\$282.6867 0.016662 Btc 0.233171 Eth	▼ -5.89%	\$2,998,483,766.00	\$45,222,967,833.00	\$4,686,809,296.62	314,266 ▼ -0.095%
3	USD Coin (USDC) USDC is a fully collateralized US Dollar stablecoin developed by CENTRE, the open source project with Circle being the first of several forthcoming issuers.	\$1.002 0.000059 Btc 0.000826 Eth	▼ -0.13%	\$10,428,801,576.00	\$42,950,755,671.00	\$46,695,635,701.68	1,541,347 ▼ -0.307%
4	Binance USD (BUSD) Binance USD (BUSD) is a dollar-backed stablecoin issued and custodied by Paxos Trust Company, and regulated by the New York State Department of Financial Services. BUSD is available directly for sale 1:1 with USD on Paxos.com and will be listed for trading on Binance.	\$0.9991 0.000059 Btc 0.000824 Eth	▲ 0.08%	\$25,013,756,920.00	\$22,814,382,929.00	\$17,558,486,341.41	147,891 ▲ 0.147%
5	Matic Token (MATIC) Matic Network brings massive scale to Ethereum using an adapted version of Plasma with PoS based side chains.	\$0.9402 0.000055 Btc 0.000776 Eth	▲ 4.30%	\$1,760,787,813.00	\$8,212,009,471.00	\$9,402,004,786.72	506,663 ▲ 0.164%

ERC 721 Standard

- Il permet la mise en œuvre d'une API standard pour les NFT dans les Smart Contracts
- Il fournit une fonctionnalité de base pour suivre et transférer les NFT.
- Les cas d'usages couvrent les NFT détenus et négociés par les individus .
- Les NFT peuvent représenter la propriété d'actifs numériques ou physiques.
- Divers univers d'actifs sont pris en compte :
- Biens physiques - maisons, œuvres d'art uniques
- Biens de collection virtuels - photos uniques de chatons, cartes de collection.
- Actifs à "valeur négative" - prêts, charges et autres responsabilités.
- Toutes les maisons sont distinctes, et il n'y a pas deux chatons identiques.
- Les NFT sont distincts et les utilisateurs peuvent suivre la propriété de chacun d'entre eux séparément.

Quelle Blockchain Publique Choisir ?

Parmi les critères de Comparaison Coef. Nakamoto

- Couverture Géographique
- Nombre des Nœuds
- Programmabilité/SC Librairie
- Equipe de Développeurs
- Historique et Roadmap
- Scalabilité
- Sécurité (résistance attaques)
- dApps (nombre, diversité)
- Wallets
- Nakamoto Coef:
 - Un critère qui dépend
 - Nombre de mineurs
 - Nombre de Nœuds
 - Les développeurs
 - La gouvernance
 - Le nombre d'utilisateurs
 - La distribution d'adresses

BCN	Launch	Token	Consensus	Language	Speed	Blocktime	Finality
Algorand	June2019	ALGO	Pure POS	TEAL	+1000	<5 sec	
Avalanche	Sept2020	AVAX	POS	Go, Solidity,..	+4500	<3 sec	
Cardano	July2020	ADA	POS	Haskell, Plutus	1000 (Hydra)	20 sec	
Cosmos	March 2019	ATOM	POS	Agoric Ethermint	1000s	1 sec	
Flow	Sept 2020	FLOW	POS	Cadence	TBA	TBA	
Harmony	June 2020	ONE	Effective POS	Solidity Vyper	+200000	5 sec	
Hedera Hashgraph	Feb 2020	HBAR	POS	Various & Solidity	10000	<5 sec	
Near	May 2020	NEAR	Threshold POS	Rust, Assembly script,...	+1000	TBA	
Polkadot	May 2020	DOT	POS	Ink!	TBA	6 sec	
Solana	March 2020	SOL	POH, POS	C, C++, Move, Rust	50000	< 1 sec	

Les Blockchains d'Entreprise

Pourquoi une Blockchain au Service des Entreprises



Collaborer en toute confiance avec ses partenaires

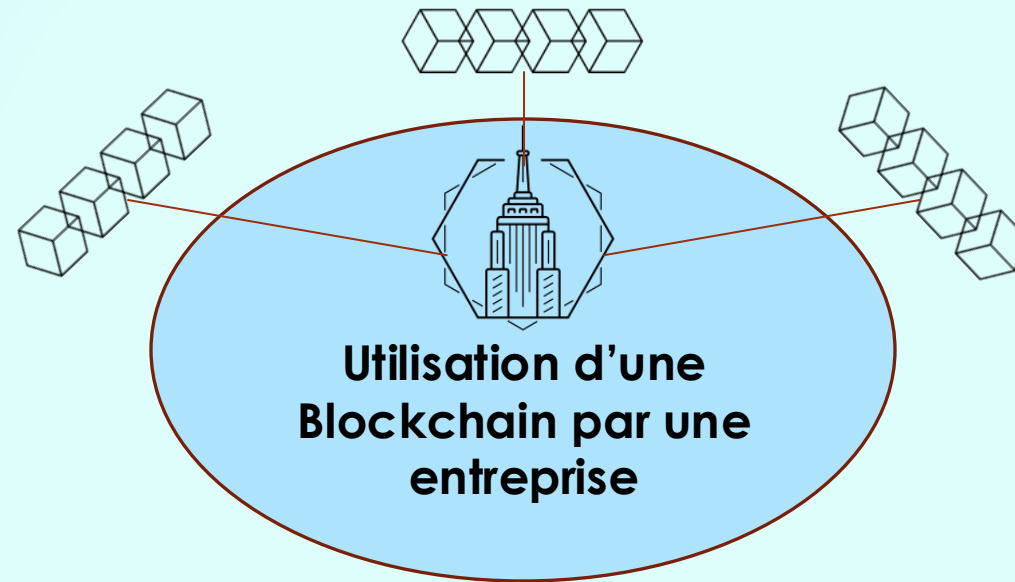
Compléter les solutions existantes par un nouveau **socle de confiance**



Fournir à ses clients ou administrés des services de confiance

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

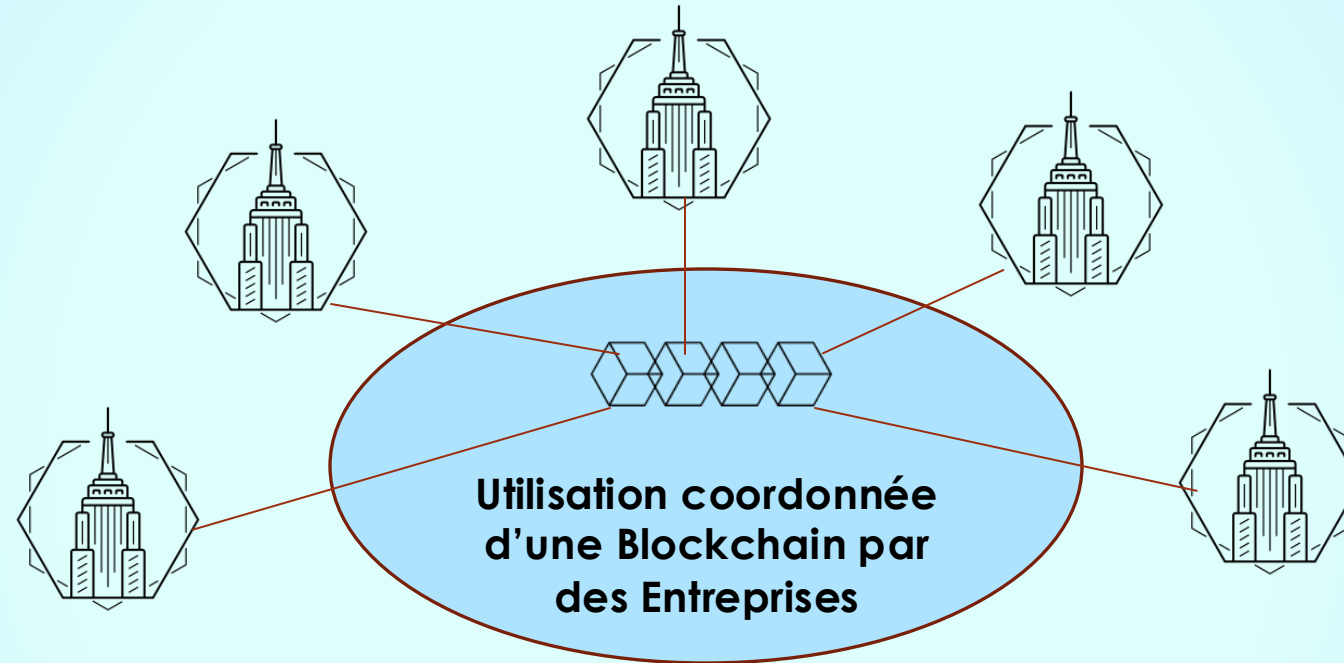
Blockchain d'Entreprise – Ciblage 1



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



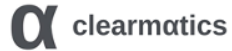
Processus Métier Multi-acteurs

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

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

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 | EF CCP | BAYER | INCM | NOVARTIS | janssen | Roche | AstraZeneca | ICSI

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 | SANBILO | BANCO BPM | BPER: cdp | MONTE DEI PASCHI DI SIENA | Allianz | Bank | Santander Consumer Bank | FINECO BANK | MEDIABANCA | 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 | G | MERCURIA | Rabobank | CREDIT AGRICOLE | Shell | MUFG | KOCH | 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 | HONDA | TOYOTA | HYUNDAI | GM | GROUPE RENAULT | 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**

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

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**



Illustrations des risques



- **FTX** had been one of the largest and most visible cryptocurrency exchanges, backed by high-profile partnerships with athletes, teams, and sports leagues.
- The company was valued at \$32 billion in January 2022, when it raised an additional \$1.8 billion.
- The U.S. Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) are both now investigating FTX, according to a *Bloomberg* report, for wrongdoing regarding how it managed customers' money ahead of the liquidity crunch.
- Alameda had \$14.6 billion of assets as of June 30, according to a private document CoinDesk reviewed. Much of it is the FTT token issued by FTX, another Bankman-Fried company.
- "It's fascinating to see that the majority of the net equity in the Alameda business is actually FTX's own centrally controlled and printed-out-of-thin-air token,"
- Other significant assets on the balance sheet include \$3.37 billion of "crypto held" and large amounts of the Solana blockchain's native token: \$292 million of "unlocked SOL," \$863 million of "locked SOL" and \$41 million of "SOL collateral »

Les Stabelcoins

- ❖ 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

Le cas Tether:

Il y a environ 24 milliards de dollars de Tether, la principale monnaie stable libellée en dollars américains, en circulation. Tether affirme que ses jetons sont entièrement garantis par les réserves de liquidités du dollar américain. Mais les réponses à ces affirmations se trouvent derrière des portes fermées, et la société a précédemment admis que ces jetons n'étaient à un moment donné garantis qu'à 74 % par le dollar américain. La société fait actuellement l'objet d'une enquête du procureur général de New York.

FIAT-BACKED



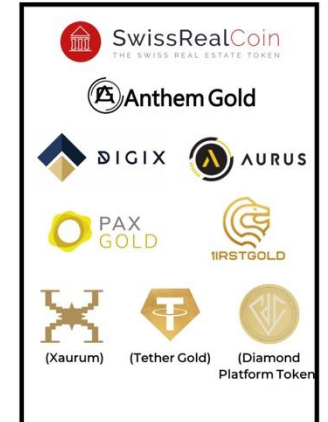
CRYPTO-BACKED



ALGORITHMIC



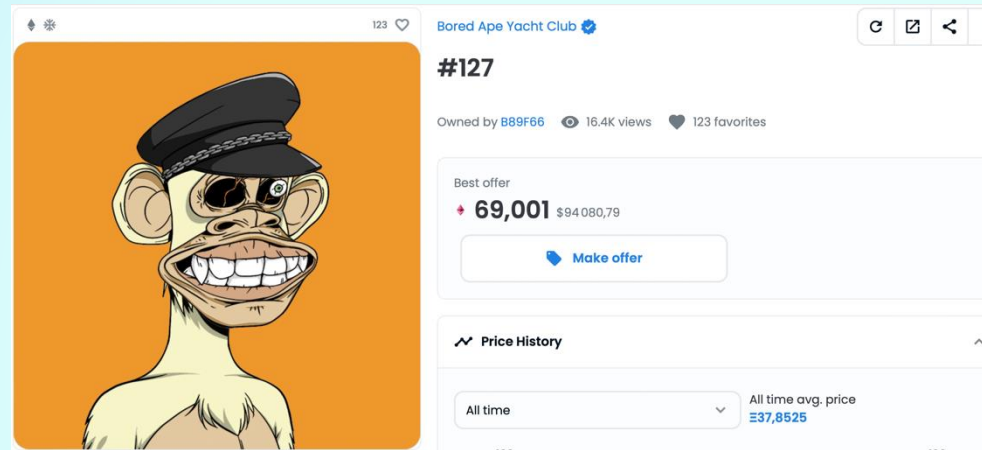
COMMODITY-BACKED



INFRASTRUCTURE



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

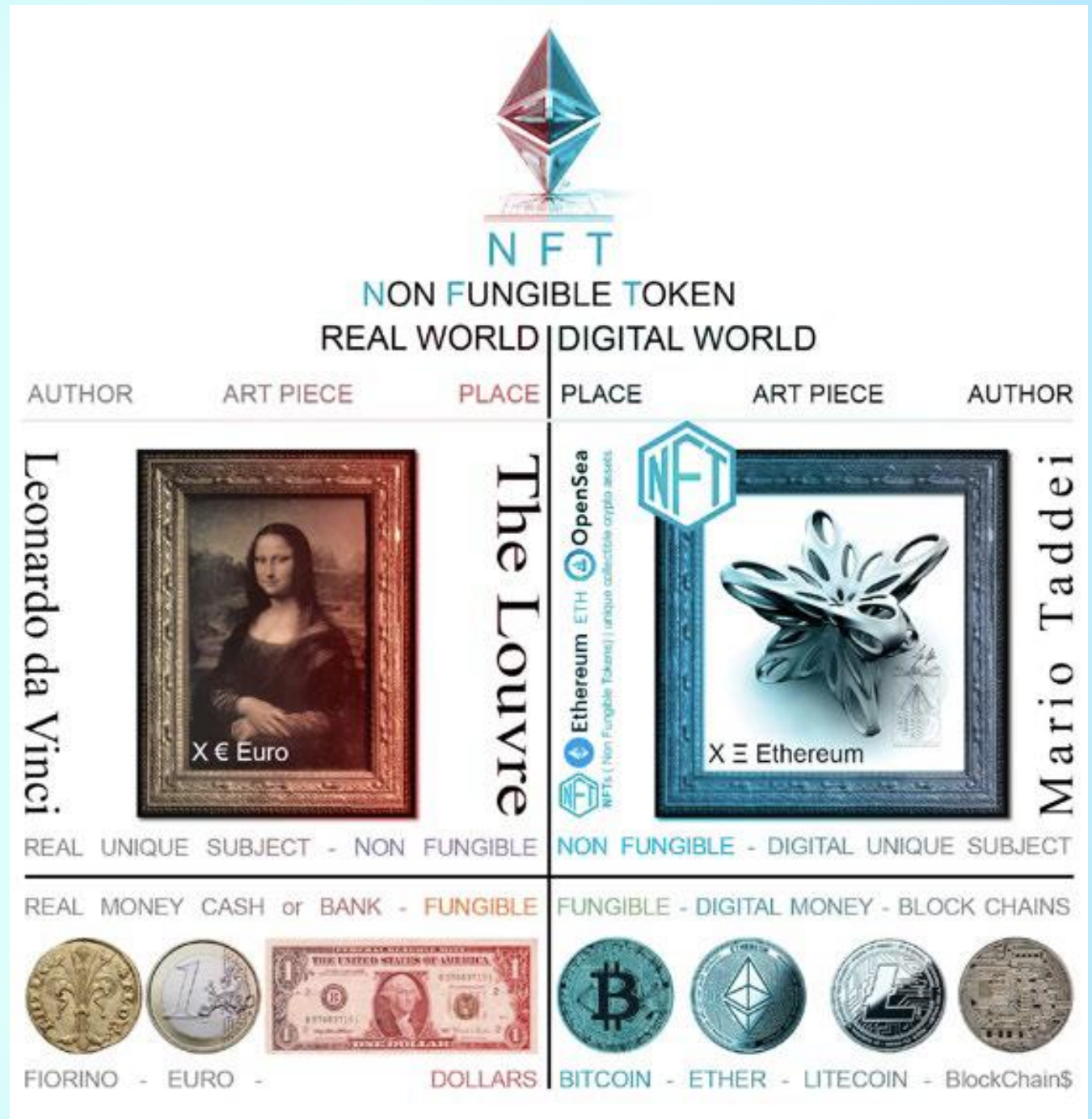
Details

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

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.

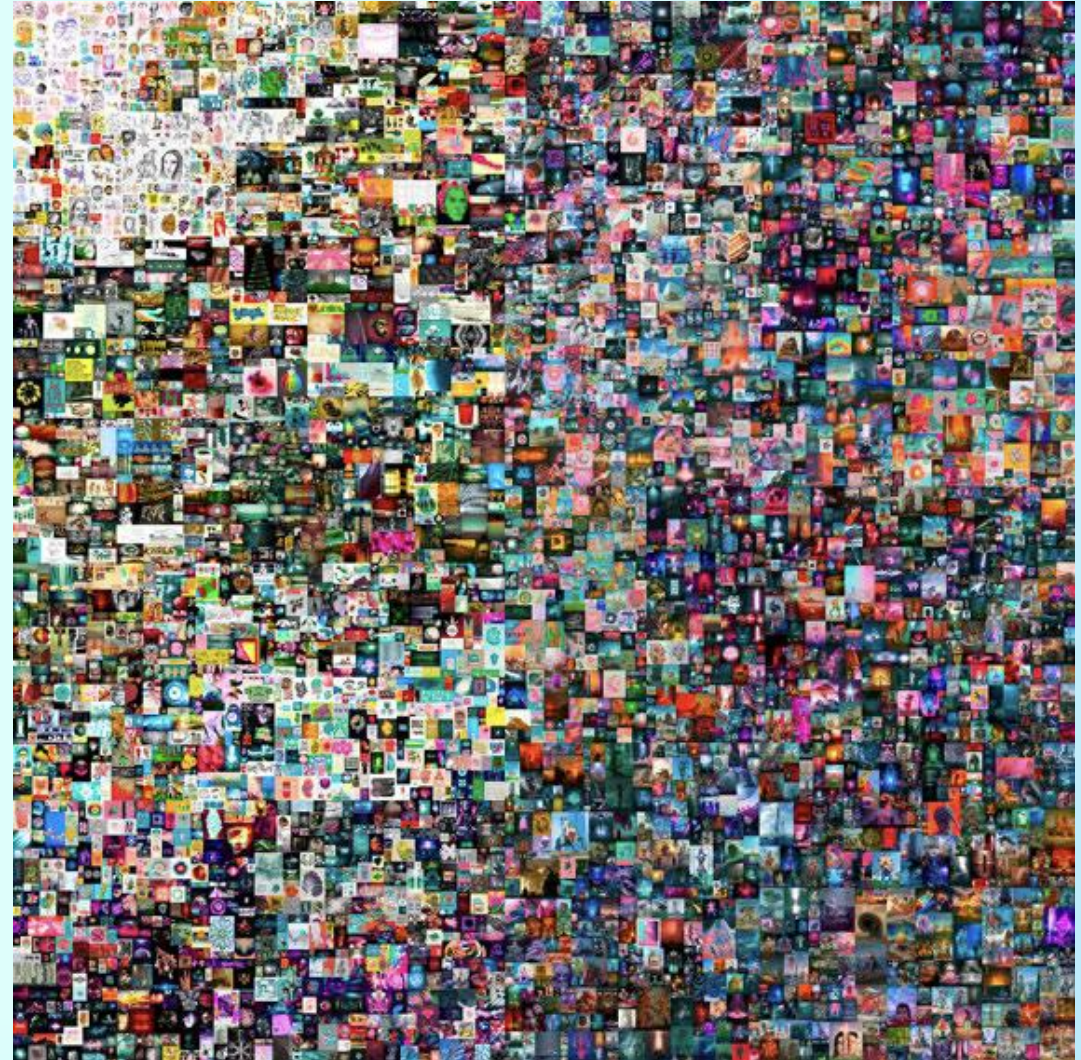
Beeple had 2.5 million followers at the time of sale.

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.

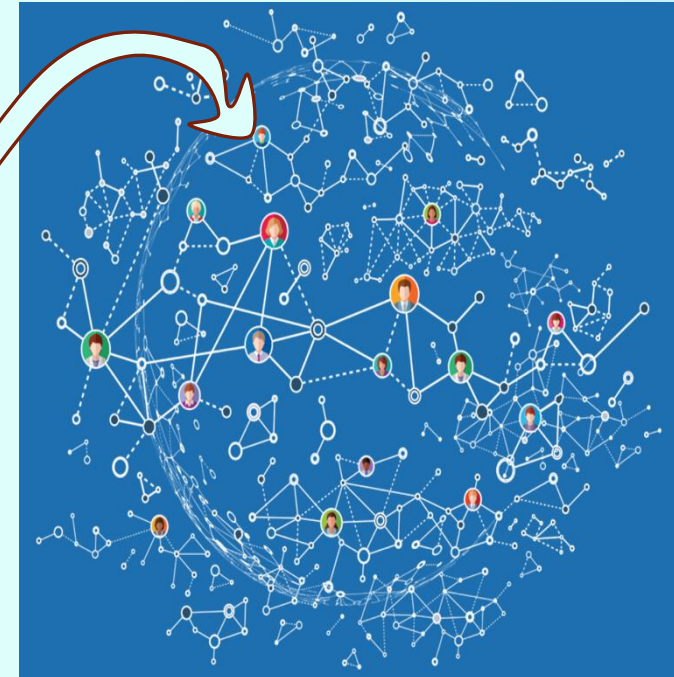
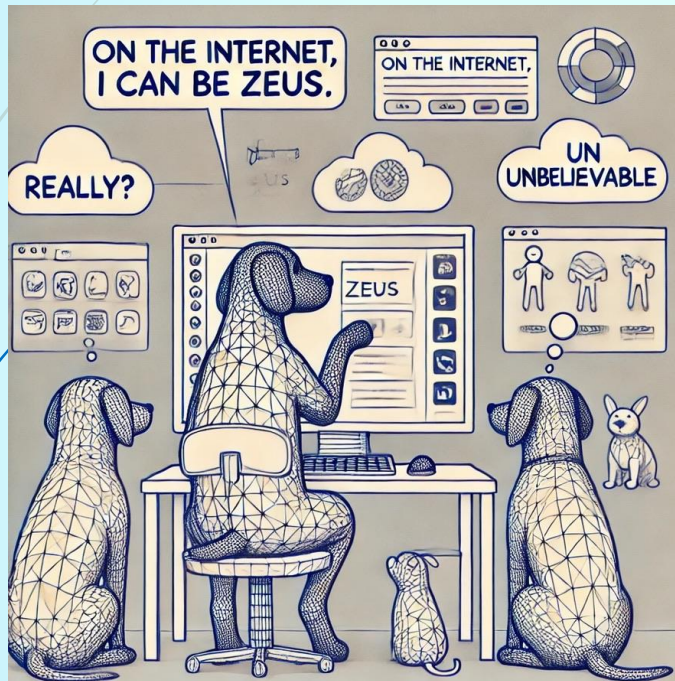


Régulation MiCA *Markets in Crypto-Assets* ("MiCA")

Un encadrement européen des marchés de cryptoactifs

- MiCA couvre plusieurs domaines dont :
 - L'offre au public et l'admission aux négociations de jetons ;
 - L'offre au public et l'admission aux négociations de jetons de valeur stable (stablecoins) ;
 - La fourniture de services sur cryptoactifs par des prestataires ;
 - La prévention des abus de marché sur cryptoactifs.
- Ce règlement a vocation à remplacer les cadres nationaux, dont celui introduit par la loi PACTE du 22 mai 2019 en France définissant un régime spécifique pour les offres au public de jetons (ICO) et les prestataires de services sur actifs numériques (PSAN).
- Les prestataires agréés MiCA pourront bénéficier du passeport européen et fournir leurs services dans tous les pays de l'UE.
- Les jetons non fongibles (NFT) seront exclus du champ d'application du règlement MiCA

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

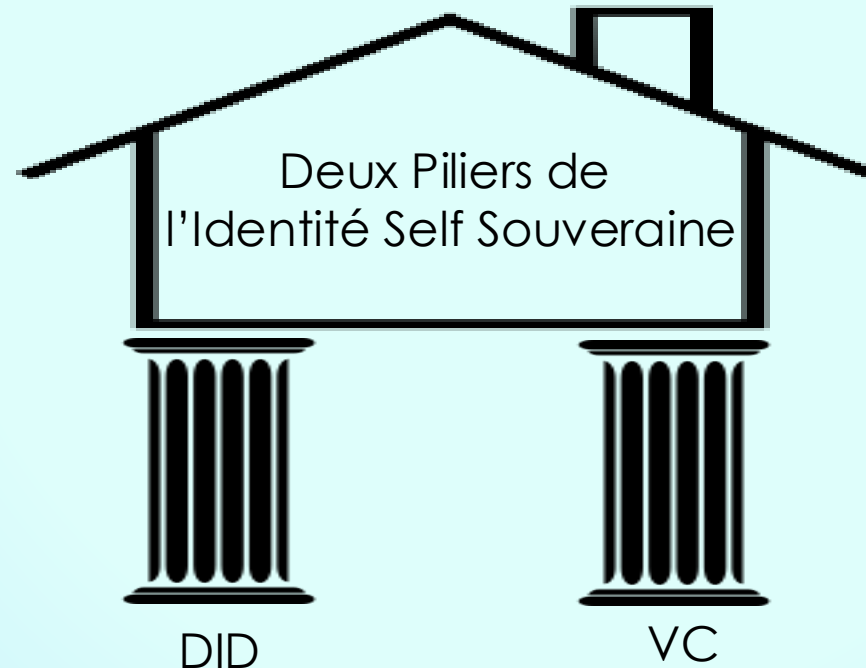
+

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

* Nous sommes responsables

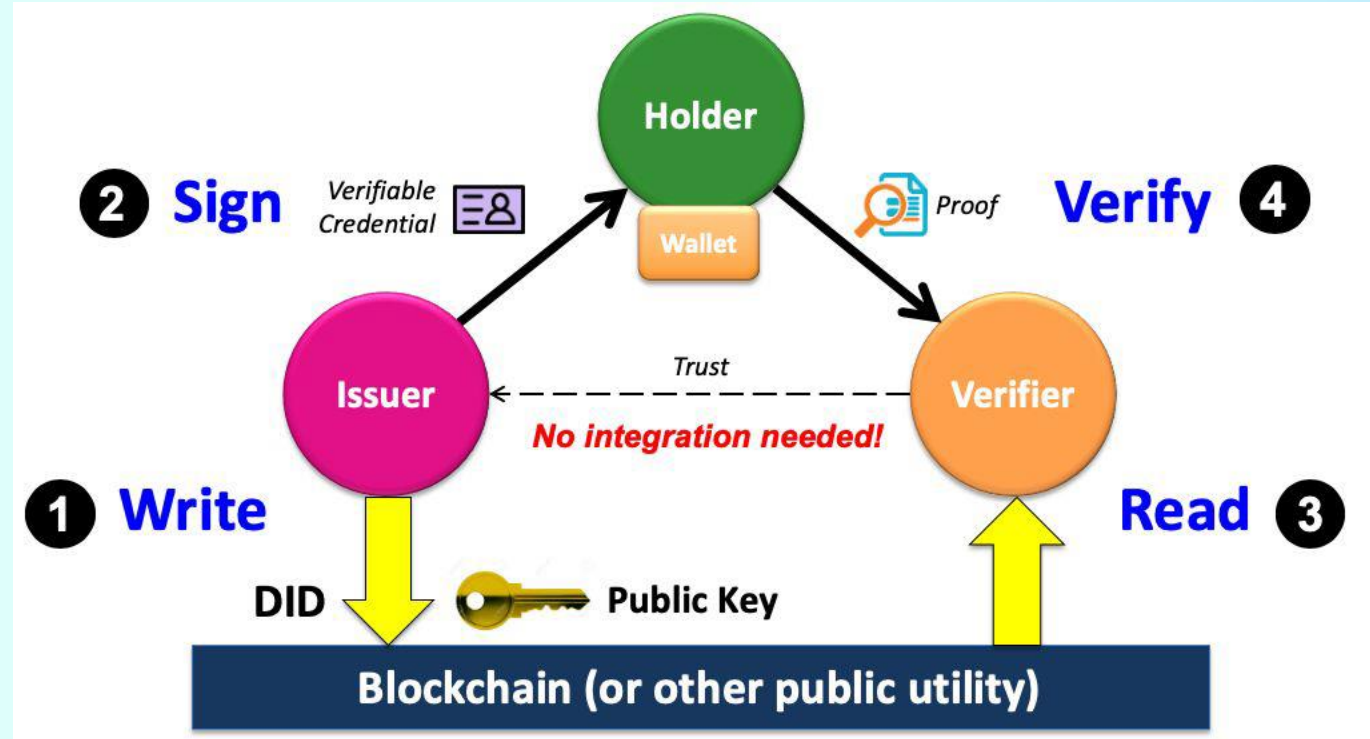
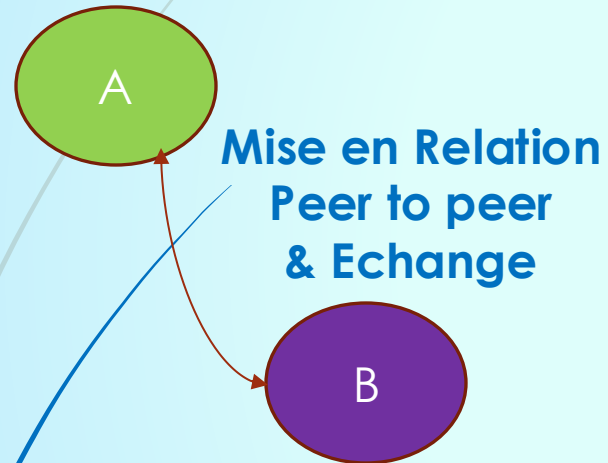
L'Identité Self-Souveraine (SSI)

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



SSI: Self Sovereign Identity

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

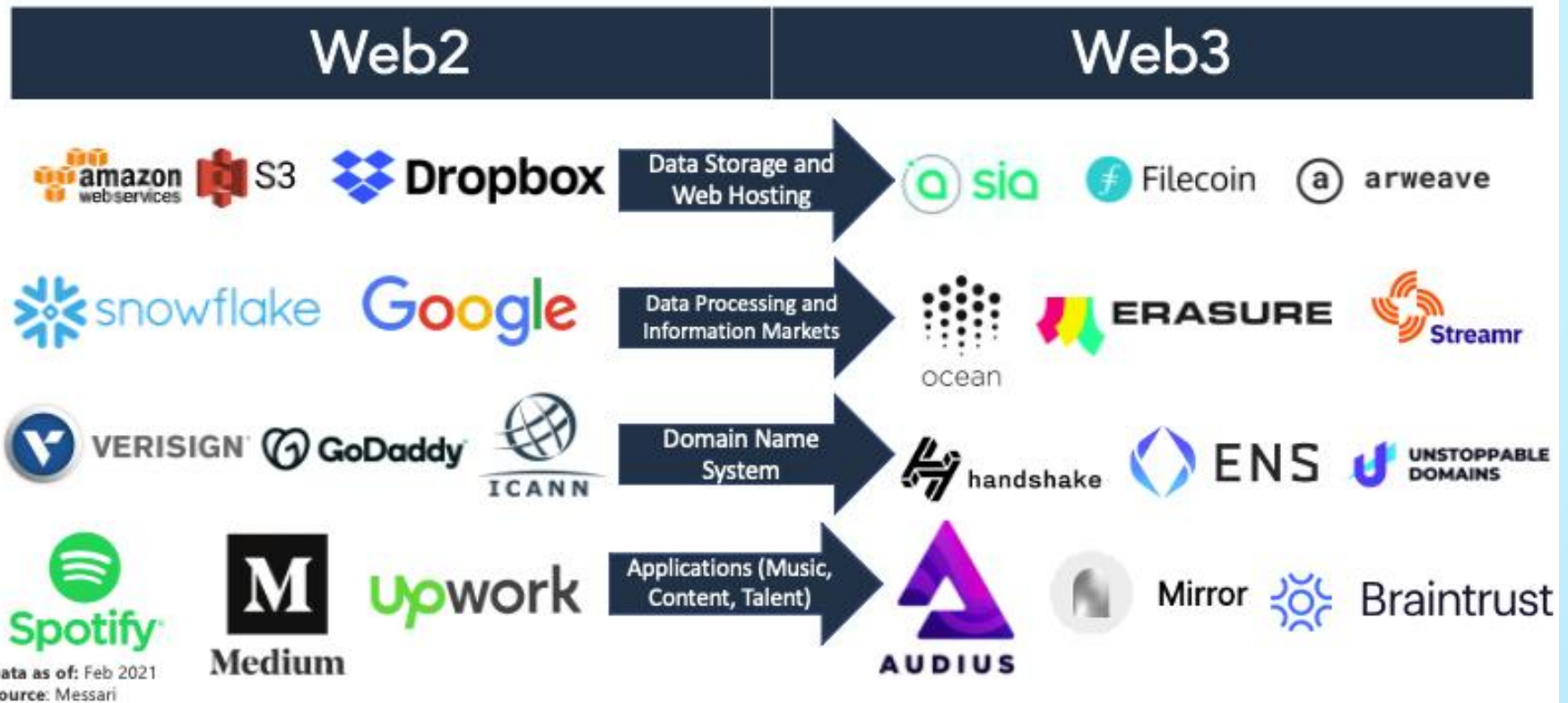
- Like Web1, open source protocols, but collectively owned through cryptoeconomics.
- Independent of traditional organizations, code executed as written.
- Values open source software, user ownership of data, and permissionless access.
- Creates a shared sense of identity and collaboration.

Web 2 vs. Web 3

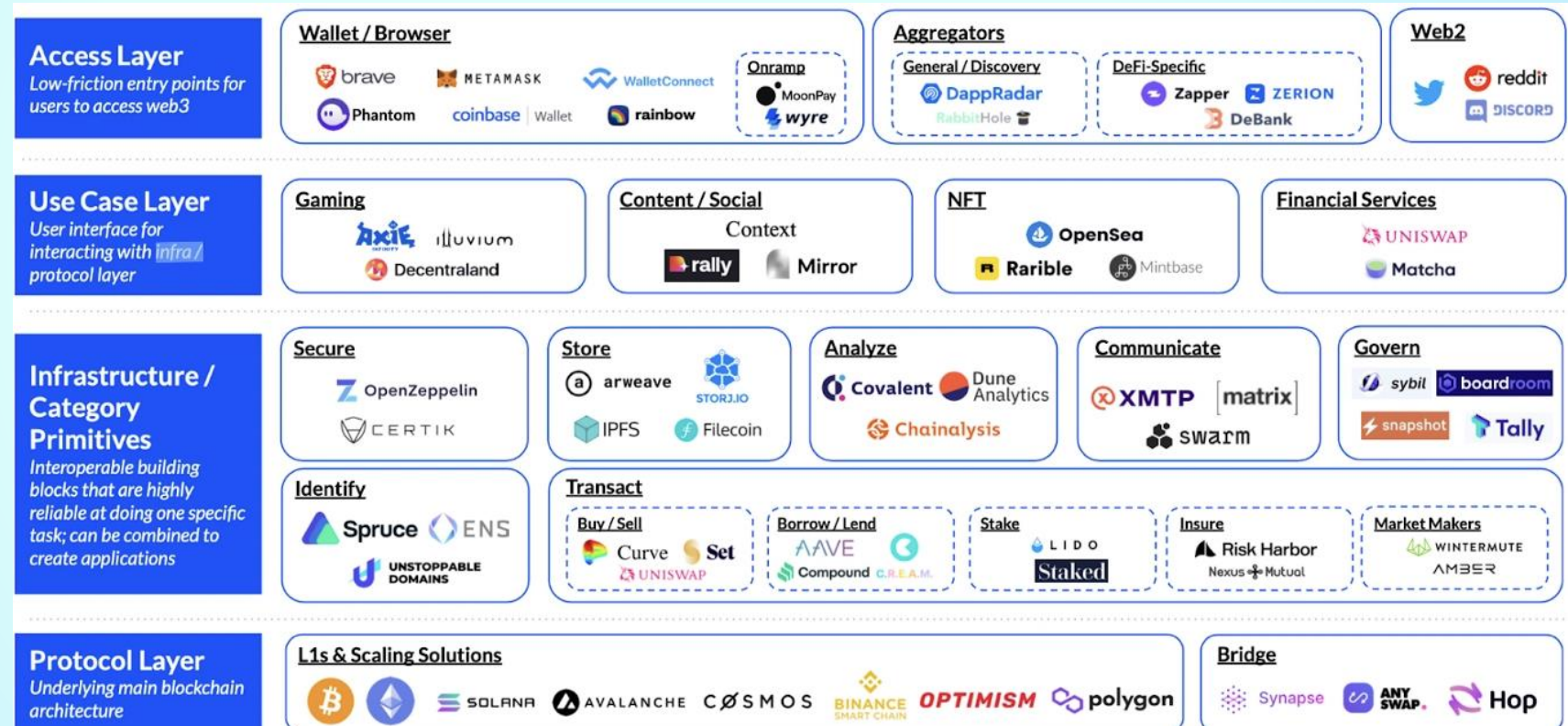
MESSARI

Web2 Companies Vs. Web3 Protocols

Web3 protocols aiming to replace or compete with web2 companies



Web 3 Stack – An illustration



Perspectives et Conclusions

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
The Metaverse

2022
beyond