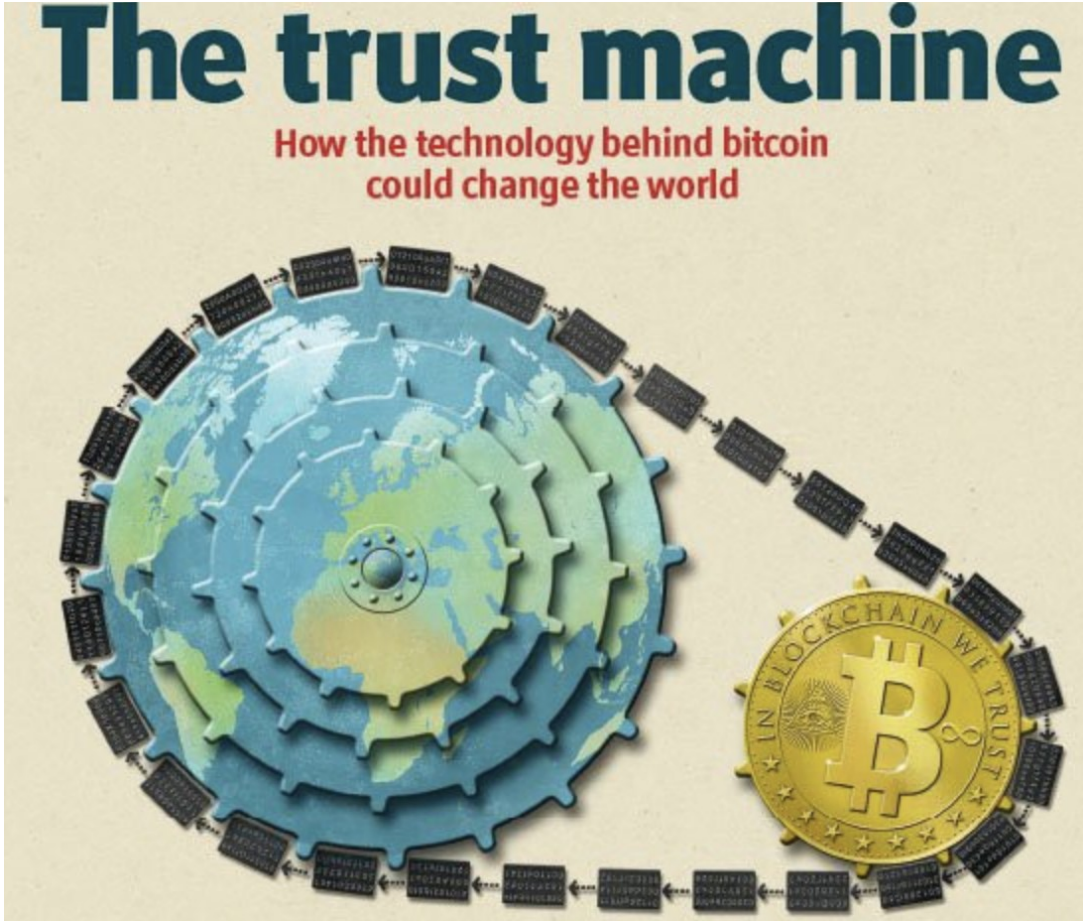

AU COEUR DES
DES BLOCKCHAINS

Blockchain épiphanie



épiphanie

nom féminin

1. Fête catholique qui commémore la manifestation de Jésus enfant aux Rois mages venus l'adorer.
   On mange la galette des Rois le jour de l'Épiphanie (jour des Rois).
2. DIDACTIQUE
   Manifestation de la divinité.
   Des épiphanies.

Commentaires

Traductions et autres définitions

fr.wikipedia.org › wiki › Épiphanie_(sentiment)

Épiphanie (sentiment) — Wikipédia

L'**épiphanie** (du grec ancien ἐπιφάνεια, epiphaneia, « manifestation, apparition soudaine ») est la compréhension soudaine de l'essence ou de la signification ...

BitConseil

Blockchain et vous ?

Une technologie mystique ?

Quelques questions :

- Qui a déjà entendu parler de Blockchain ? De Bitcoin ?
- Qui a compris ce que c'est et comment ça fonctionne ?
- Qui s'est déjà servi d'une blockchain ?

Mission Blockchain

Rendre l'impalpable intelligible...

BLOCKCHAIN - définition #1

Décentralisation & horodatage

Une blockchain : c'est une technologie de stockage et de transmission d'informations, transparente, sécurisée, horodatée et fonctionnant sans organe central de contrôle (définition de Blockchain France).

Représentation d'une chaîne de blocs

Source : Blockchain France

BLOCKCHAIN - définition #2 : empiler des données

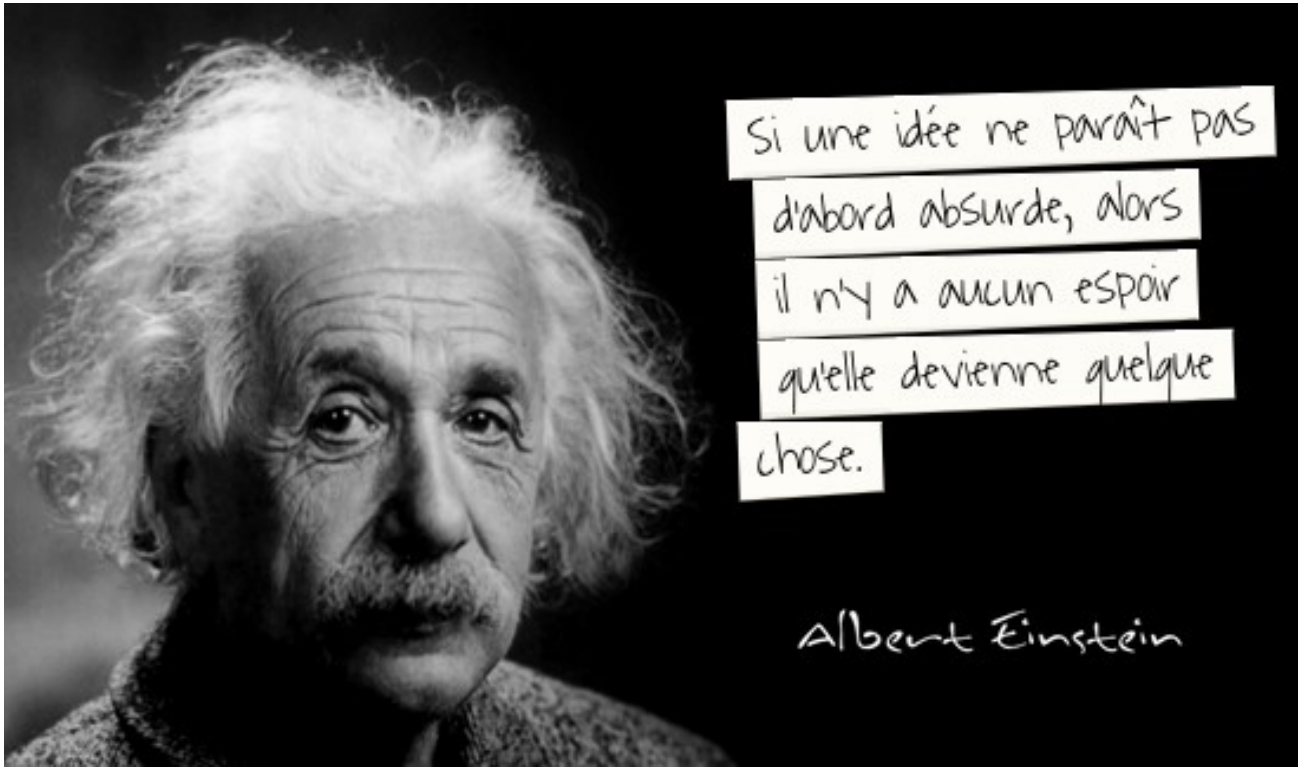
Ecrire & ne jamais effacer !

Une blockchain : c'est un **registre informatique** dans lequel tout le monde* peut écrire, mais dans lequel **PERSONNE NE PEUT RIEN EFFACER !**

BitConseil

Blockchain... mais pourquoi ?

Un concept déroutant



De l’importance des registres

Les registres font partie intégrante de notre vie

→ Outil de traçabilité

→ Utilité mémorielle

→ Instrument de gouvernance de toute organisation informationnelle

Problème actuel : les registres sont gérés par des tiers de confiance

Trusted Third Parties are Security Holes

Nick Szabo

Originally published in 2001

Introduction

Commercial security is a matter of solving the practical problems of business relationships such as privacy, integrity, protecting property, or detecting breach of contract. A security hole is any weakness that increases the risk of violating these goals. In this real world view of security, a problem does not dissapear because a designer assumes it away. The invocation or assumption in a security protocol design of a "trusted third party" (TTP) or a "trusted computing base" (TCB) controlled by a third party constitutes the introduction of a security hole into that design. The security hole will then need to be plugged by other means.

Un problème de confiance aussi vieux que l'humanité

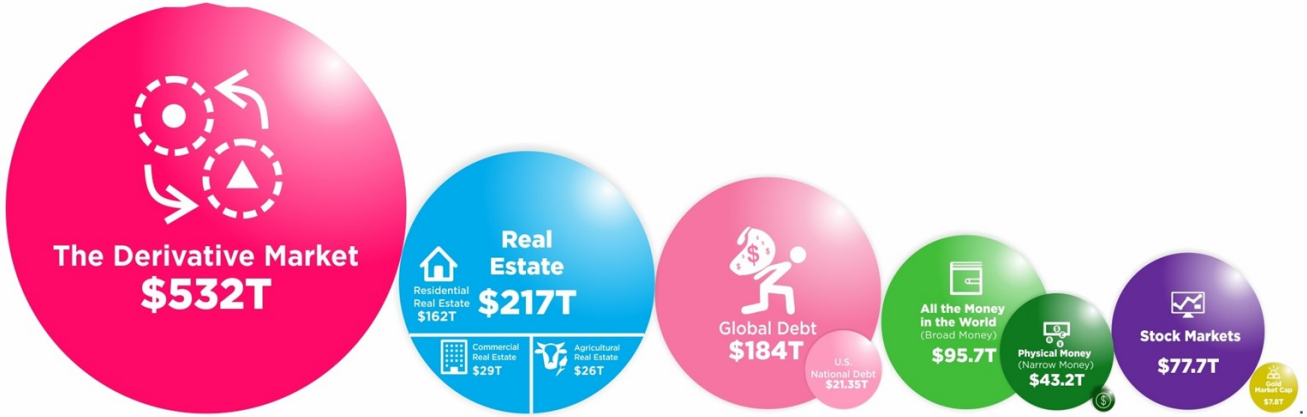
et par extension, de sécurité

Exemples de registres sensibles : les registres comptables

De l'écriture cunéiforme aux blockchains

Tablette provenant d'Uruk et datée de la période d'Uruk III (c. 3200-3000 av. J.-C.) enregistrant des distributions de bière. British Museum.

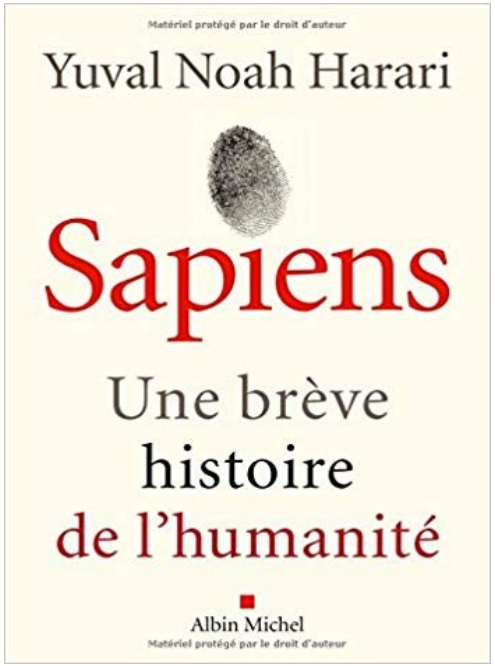
Sceau Cylindre de la période d'Uruk et datée de la période d'Uruk III (c. 3200-3000 av. J.-C.) enregistrant des distributions de bière. British Museum.



Monnaie de Pierre des îles YAP,

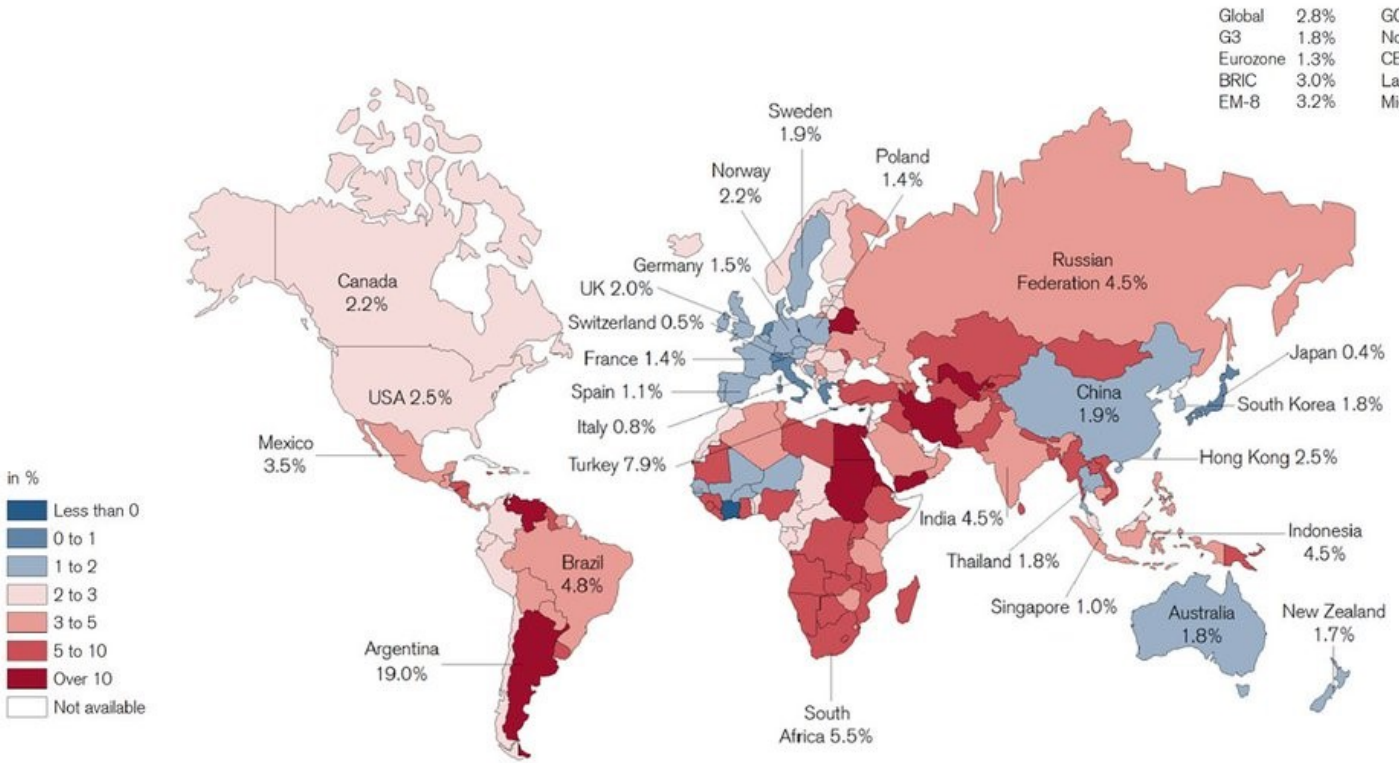
BitConseil

L’histoire chaotique de la monnaie



BitConseil

Global Economy in Detail - Forecast: Inflation in 2018 in % YoY



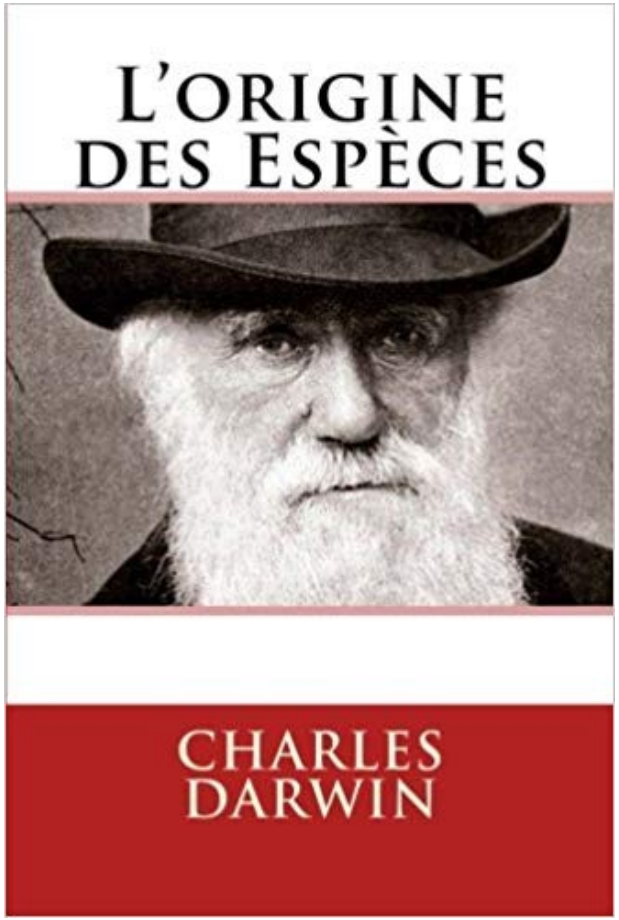
Source: IMF, Credit Suisse

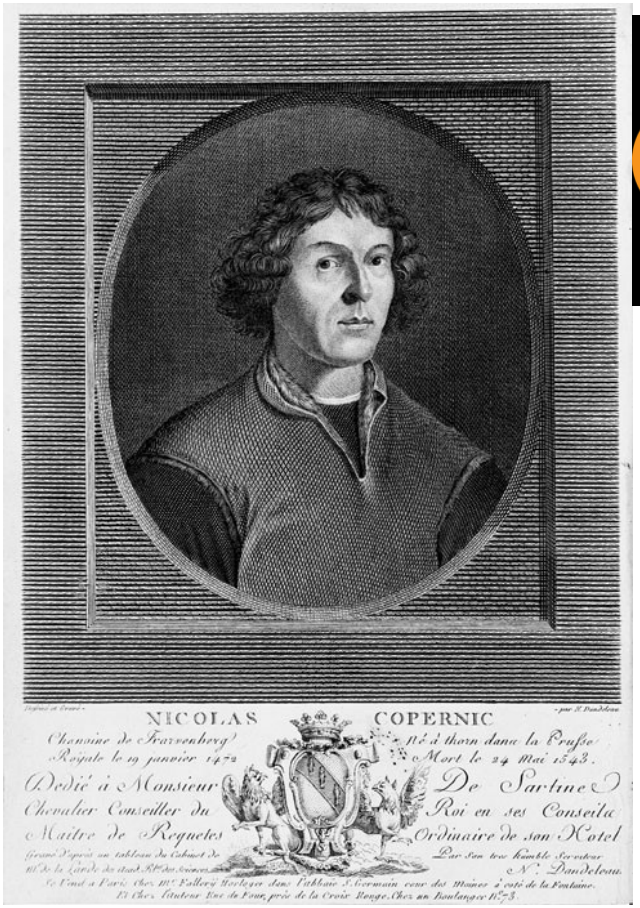
BITCOIN

https://bitcoin.org le site original, créé par Satoshi Nakamoto pour présenter Bitcoin

BitConseil

Des révolutions conceptuelles radicales





bitcoin

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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

BitConseil

Exemples de registres sensibles : les registres de santé

Quid du registre des demandeurs d'organes ?

Fonctionnement des blockchains

"Mal nommer les choses c'est ajouter aux malheurs du monde"

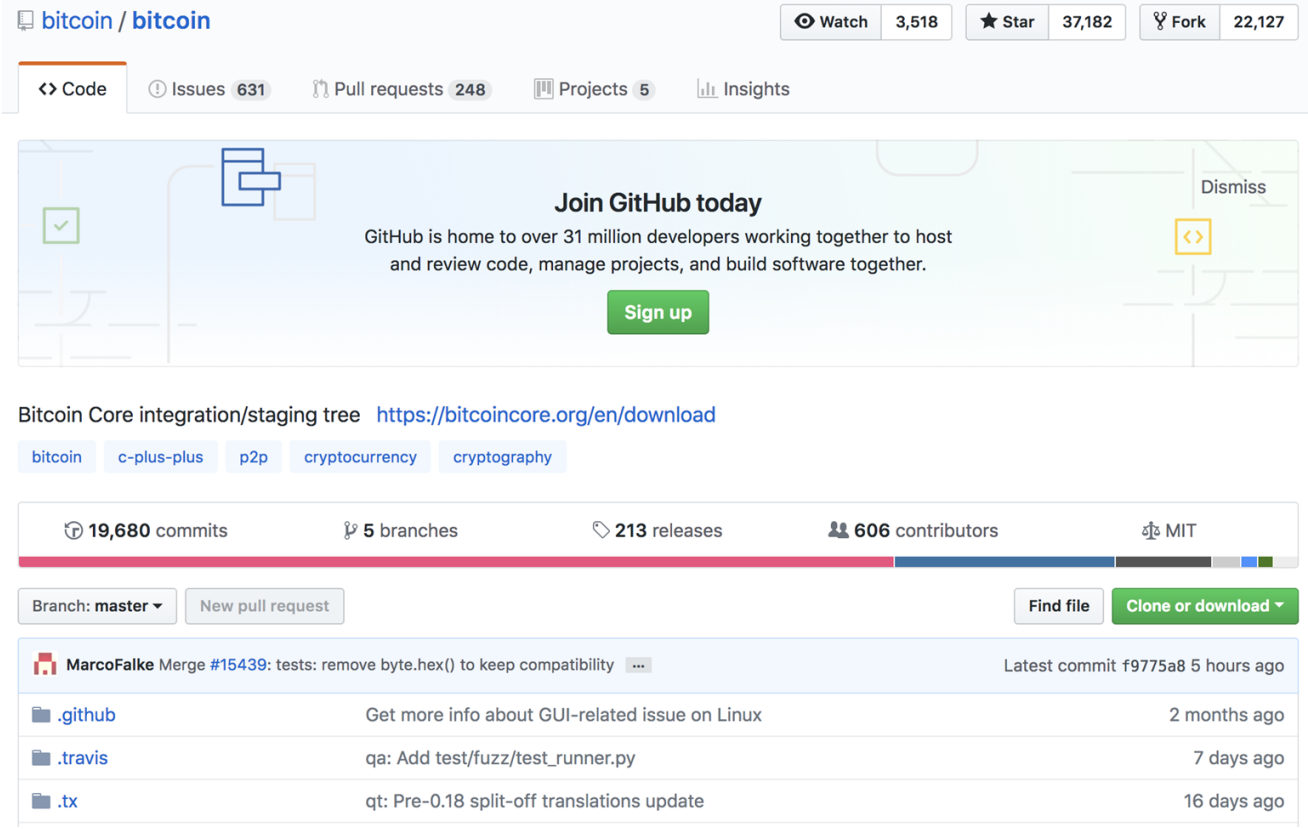
Un peu de sémantique :

Le protocole Bitcoin

La blockchain de Bitcoin

Les blockchains

Le protocole Bitcoin sur GitHub



BitConseil

LES PRÉCURSEURS DE BITCOIN

A l'origine des systèmes d'échange de valeur distribués : le protocole Bitcoin

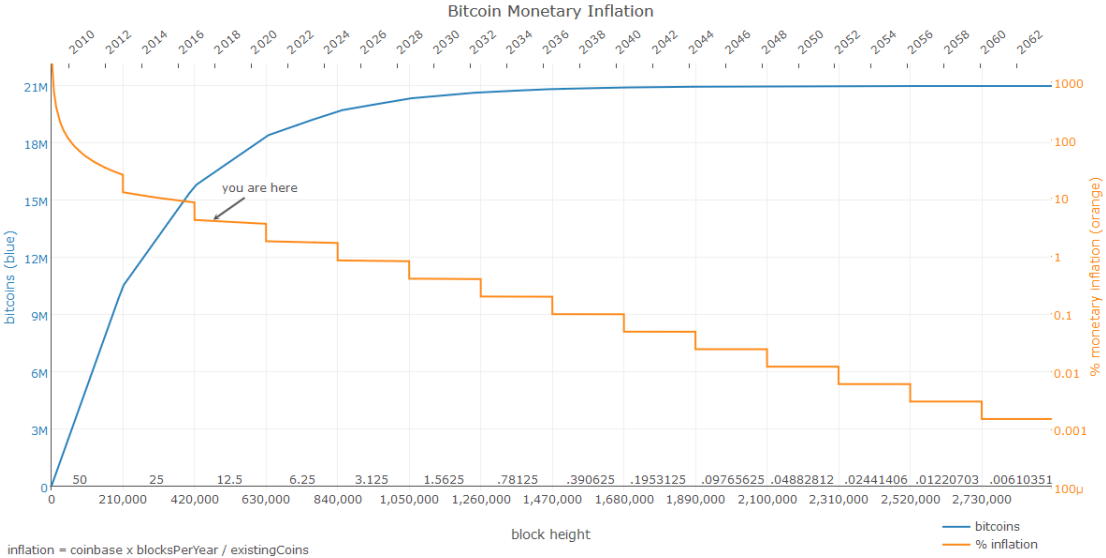
« **Si j'ai vu plus loin, c'est que j'étais juché sur les épaules de géants**. »
Isaac Newton, 1675

Bitcoin repose sur de nombreux concepts scientifiques éprouvés :

- 1977 : Chiffrement asymétrique (RSA).
- 1979 : Merkle Tree Compression mechanism de Ralph Merkle.
- 1990 : Digicash de David Chaum, première monnaie cryptographique (centralisée).
- 1992 : Cryptographie par courbe elliptiques (ECDSA).
- 1994 : Première description des Smart-Contracts par Nick Szabo.
- 1997 : Hashcash de Adam Back, un système de preuve de travail.
- 1999 / 2000 : Napster puis Gnutella, premières plateformes de partage de fichiers en pair à pair.
- 1998 - 2005 : Bitgold, et Rpow de Nick Szabo et Hal Finney

L'ÉMISSION INITIALE DES BITCOINS

La fonction de production des bitcoins

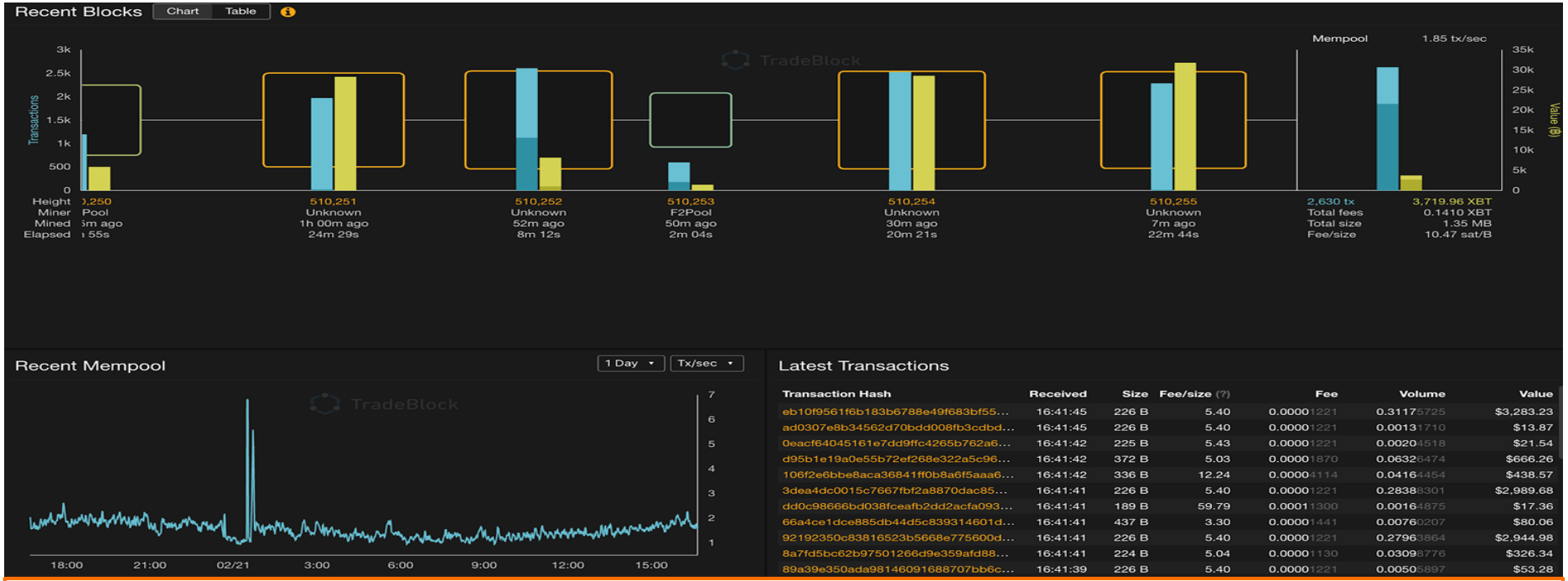


La fameuse courbe d'émission des bitcoins (en bleu) qui tend vers un maximum de 21 millions de bitcoins produits (16,8 millions de bitcoins sont actuellement en circulation) et le taux d'inflation (en orange) qui à terme sera nul. (environ 4% à l'heure actuelle : 12,5 bitcoins créés toutes les 10 minutes).

Source : https://bashco.github.io/Bitcoin_Monetary_Inflation/

Bitcoin et la 1ère blockchain de l'histoire

Visualisation de la blockchain de Bitcoin avec un explorateur de blocs



En pratique la blockchain de Bitcoin c'est un grand livre de compte qui contient l'historique complet de toutes les transactions qui ont été émises sur le réseau Bitcoin.

BitConseil

LE RÉSEAU BITCOIN

La blockchain de Bitcoin, un registre comptable mondialement distribué

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Thu Jan 31 2019 20:51:19 GMT+0100 (heure normale d'Europe centrale).

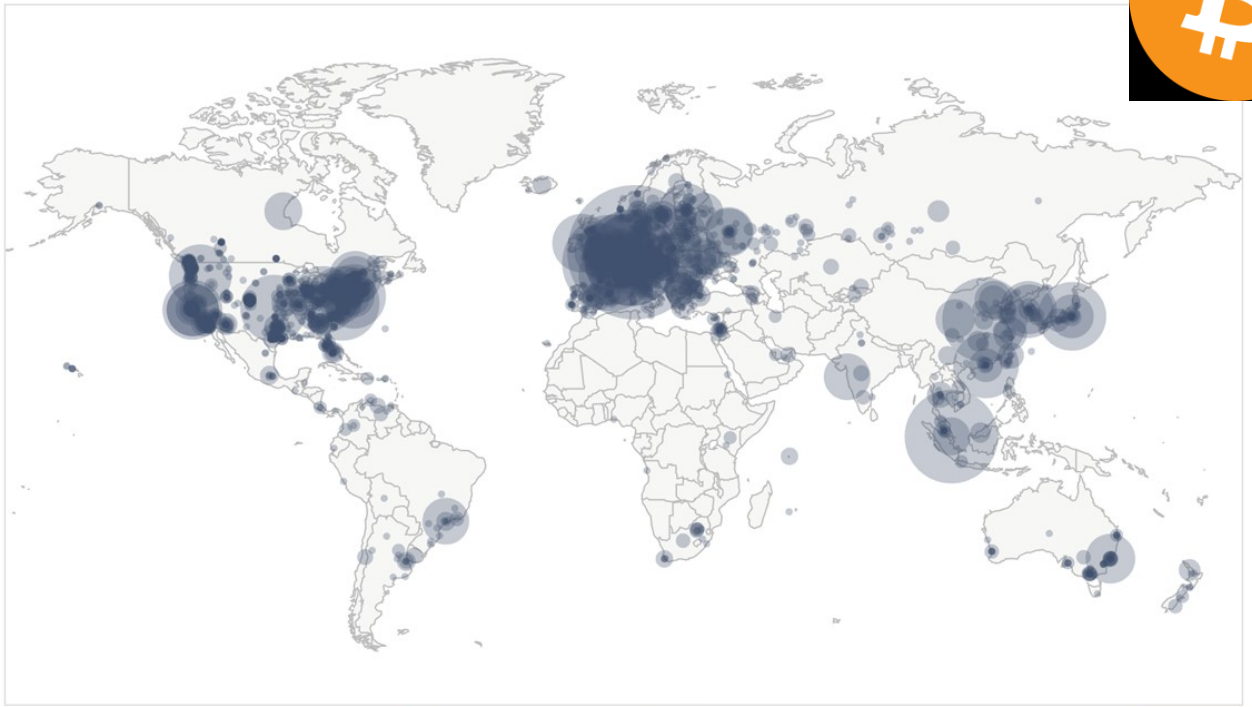
10322 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2531 (24.52%)
2	Germany	1967 (19.06%)
3	France	697 (6.75%)
4	Netherlands	518 (5.02%)
5	Canada	393 (3.81%)
6	China	388 (3.76%)
7	United Kingdom	358 (3.47%)
8	Singapore	326 (3.16%)
9	Russian Federation	266 (2.58%)
10	Japan	250 (2.42%)

More (101) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

BitConseil

BITCOIN & LA PREUVE DE TRAVAIL

Le mining

$$\frac{\sum_{i=0}^{32} 210000 \lfloor \frac{50.10^8}{2^i} \rfloor}{10^8}$$

La fameuse fonction de production des bitcoins

BitConseil

PRINCIPES DE FONCTIONNEMENT TECHNIQUE

Présentation d'une machine dédiée au minage de crypto-monnaies (Ethereum)

BitConseil

REGISTRES DISTRIBUÉS & CONSENSUS

Un consensus est un ensemble de règles publiques qui met tout le monde d'accord.

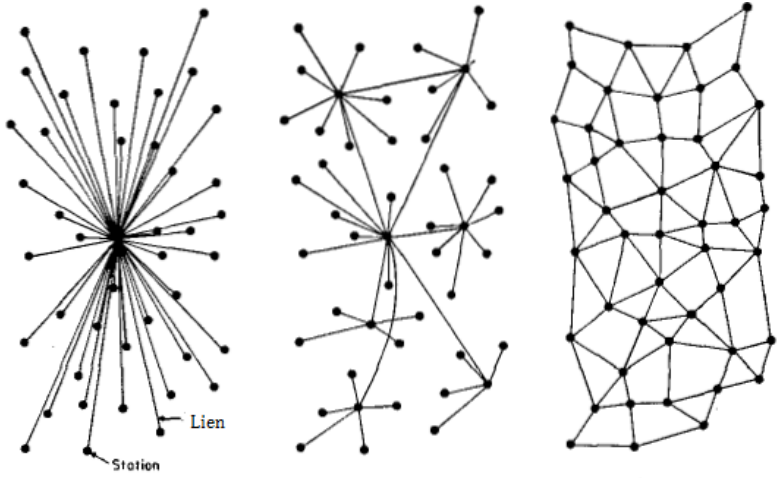


Fig. 1—(a) Centralisé (b) Décentralisé (c) Réseaux distribués

Le concept le plus important à comprendre au sujet du Bitcoin: Le CONSENSUS

Un sujet multi facette, complexe et passionnant. Essayer de comprendre Bitcoin, c'est un peu comme rentrer dans un labyrinthe. À chaque détour vous ne savez pas sur quoi vous allez tomber. Peut-être sur un cul de sac ou peut-être sur une chose inattendue. Si vous êtes d'une nature curieuse, c'est un sujet fascinant qui est fait pour vous car il implique de nombreux domaines: informatique, cryptographie, politique, économie, finance, sociologie. Tout y passe et pour envisager l'impact du Bitcoin sur notre société, il est nécessaire de faire le lien entre tous ces aspects. Pour le profane, il est difficile de savoir par quel bout l'aborder sans faire fausse route. Quelle est donc la meilleure façon d'aborder ce sujet ?

JAK TRAN Follow

Apr 25, 2018 · 10 min read

BitConseil

Le compromis à trouver entre décentralisation et performance

Gouvernance et coûts de traitement des écritures

Systèmes centralisés

- Hiérarchie mieux définie
- Moins coûteux
- Plus rapide

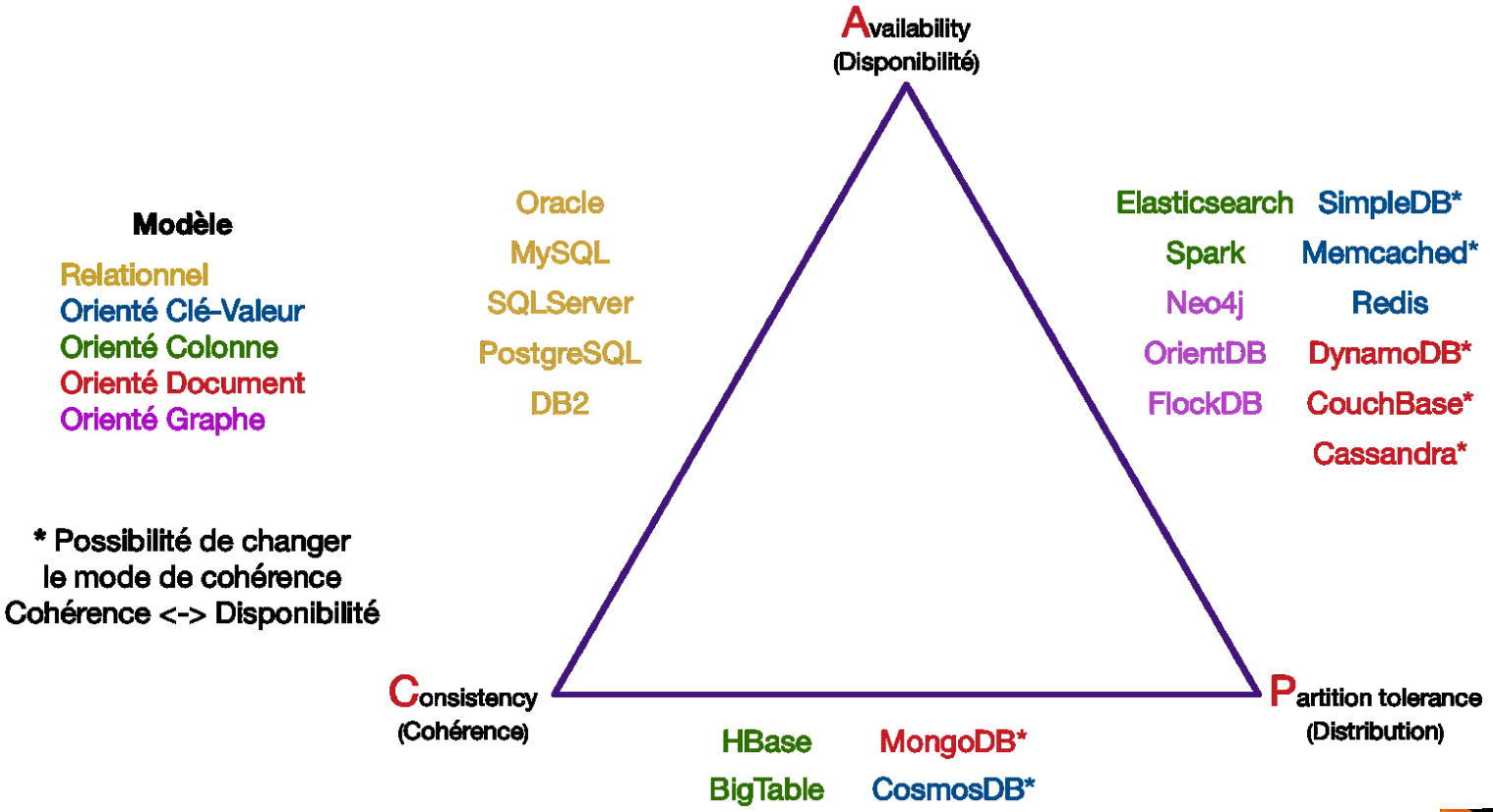
Systèmes décentralisés

- Plus robustes
- Moins corruptibles
- Gouvernance plus complexe

BitConseil

Le trilemme des blockchains

Le théorème CAP



BitConseil

LES BLOCKCHAINS DE CONSORTIUM & LES BLOCKCHAINS PRIVÉES

Différents modèles de gouvernance / différentes hiérarchies

Blockchain publique

Blockchain de consortium

Blockchain privée

Registre classique

Source : Bank for International Settlements, “Cryptocurrencies : looking beyond the hype”, 2018.

LIBRA

BitConseil

La preuve de travail et ses alternatives

Consensus

Le consensus n'est pas un terme propre aux cryptomonnaies, mais il est un élément essentiel au bon fonctionnement de tout système. Le consensus est la vérité admise par les participants au système. Cela ne veut pas dire que le consensus est la vérité absolue ou qu'il est incontestable, mais c'est la réalité sur laquelle s'accordent les participants au système. Dans le sport par exemple, c'est l'arbitre qui crée le consensus en cas de désaccord. Dans le monde judiciaire, c'est le juge. Dans le monde des cryptomonnaies, divers algorithmes, commençant par "Proof of XXXXX" permettent de parvenir au consensus sur une blockchain. La force d'une blockchain est dès lors de parvenir systématiquement, efficacement et de manière décentralisée à un consensus : on parle de **"protocole de consensus"** ou de **"mécanisme de consensus"**.

	PoW		PoS	DPoS	PoET	PBFT et variantes
	BTC	*ETH*				
Matériel spécifique	ASIC	GPU	-	-	SGX	-
Type de blockchain	Publique (permissionless)		Publique et privée	Publique (permissionless)	Publique et privée	Privée (permissioned)
Finalité de transaction	Probabiliste		Probabiliste	Probabiliste	Probabiliste	Immédiate
Débit de transaction	Faible		Élevé	Élevé	Moyen	Élevé
Coin/Token nécessaire ?	Oui		Oui	Oui	Non	Non
Coût de participation ?	Oui		Oui	Oui	Non	Non
Consommation énergétique ?	Oui		Non	Non	Non	Non
Scalabilité du réseau	Élevée		Élevée	Élevée	Élevée	Faible
Modèle de confiance	Sans confiance		Sans confiance	Sans confiance	Sans confiance	Semi-confiance
Tolérance aux fautes byzantines et à la compromission	<=25%		Dépend de l'algorithme spécifique utilisé	Dépend de l'algorithme spécifique utilisé	Inconnu	<=33%
Niveau de sécurité	Très élevé		Faible	Élevé	Inconnu	Moyen
Niveau de décentralisation	Moyen		Élevé	Très élevé	Moyen	Faible

Tableau comparatif des principaux mécanismes de consensus

BitConseil

Bitcoin Astronomy

By Dhruv Bansal | September 13, 2019 | Bitcoin, Bitcoin Astronomy, Blockchain, Space

Money: The Hidden Force Behind the Star Wars Universe

by **Maciej Cepnik** 7 months ago

BitConseil

La Blockchain de Bitcoin est déjà dans l'espace

50+ BLOCKCHAIN
REAL WORLD USES CASES

THE INTERNET OF BLOCKCHAIN FOUNDATION

MATTEO GIANPIETRO ZAGO

BitConseil

woleet

Products Features Pricing Resources Log in Free Trial

The proof system for modern companies

Secure your sensitive data flows by creating Bitcoin-based **proofs of existence, electronic signatures and seals**.

Try Woleet Sign

Try Woleet API

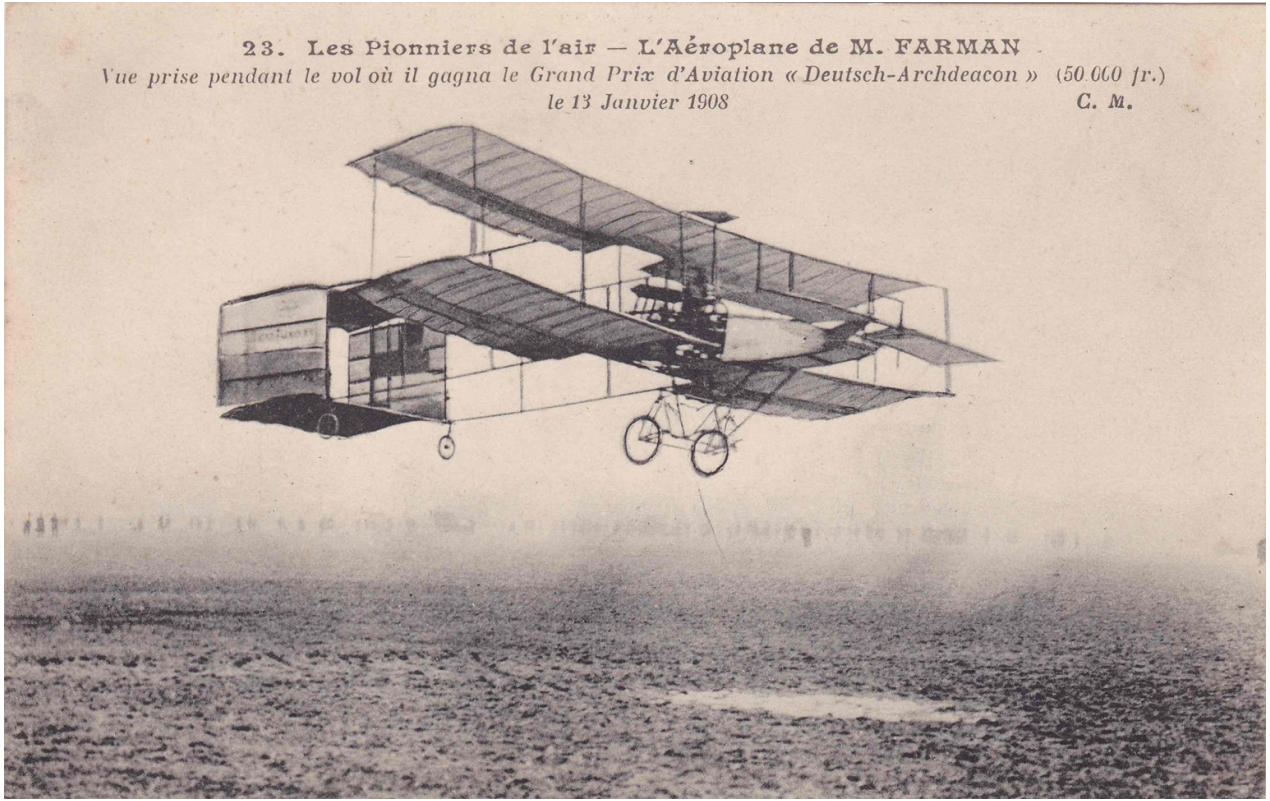
SECURING DATA FOR LEADING COMPANIES WORLDWIDE

DANONE acciona EDF SERVIER AlmavivA KERING

BitConseil

Le temps des pionniers des blockchains

Un système encore expérimental mais prometteur



BitConseil

CONCLUSION : QUI LIBRA, VERRA !

De nombreux cas d'usages à explorer et un marché immense à conquérir

BitConseil