Démystifions les cryptomonnaies

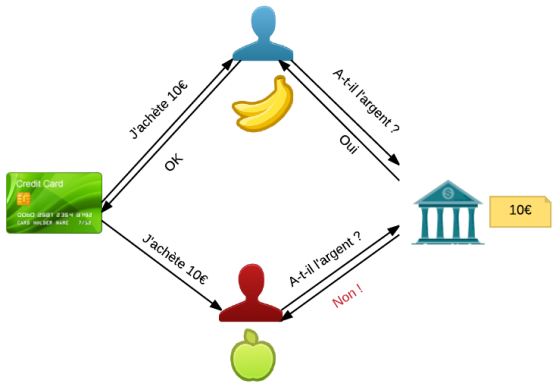
Pascal Lafourcade

Zénith, Crédit Agricole
9 décembre 2025

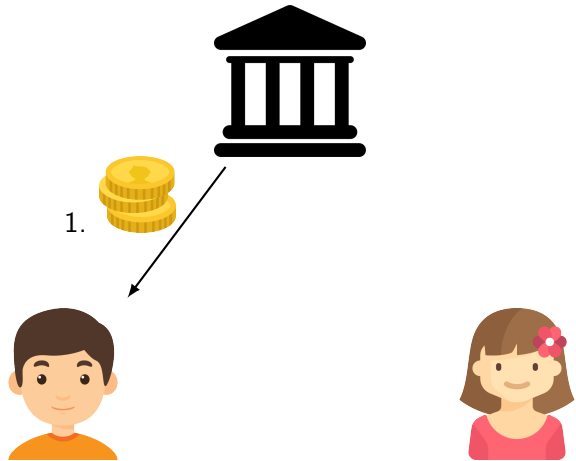
Sumériens vers 3.500 av J.C

Nombreuses monnaies

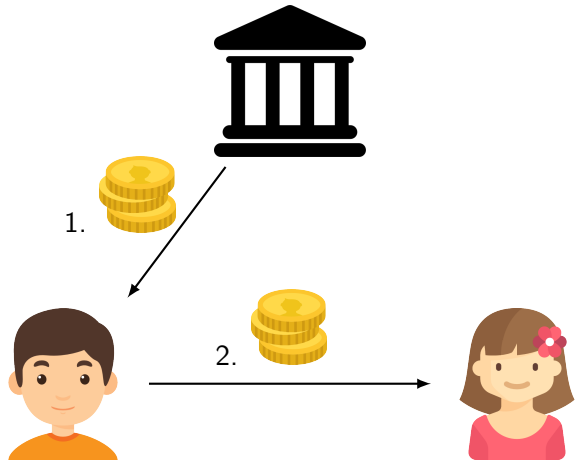
Éviter la double dépense



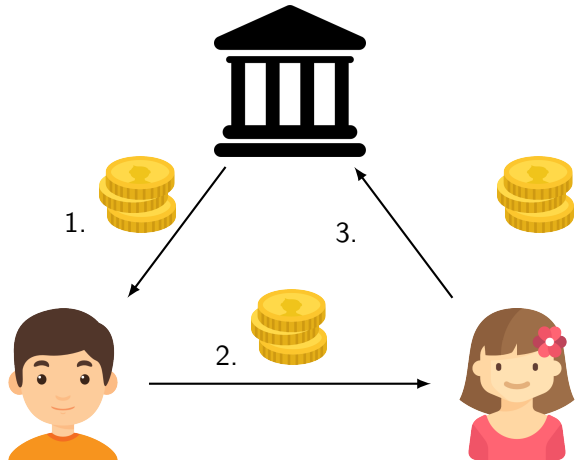
Principe : Banque centrale



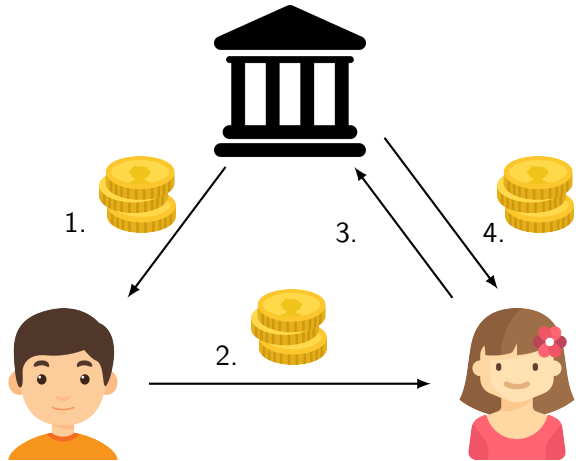
Principe : Banque centrale



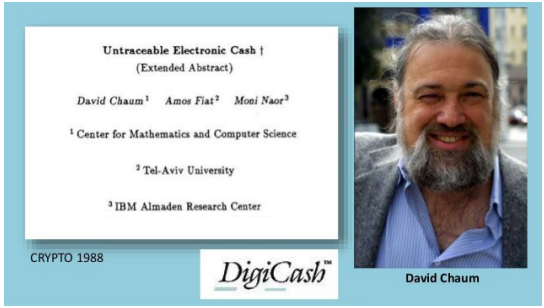
Principe : Banque centrale



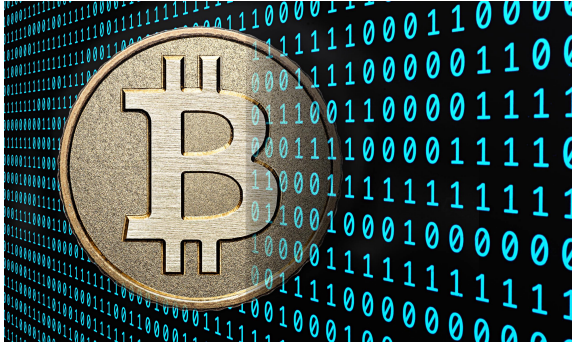
Principe : Banque centrale



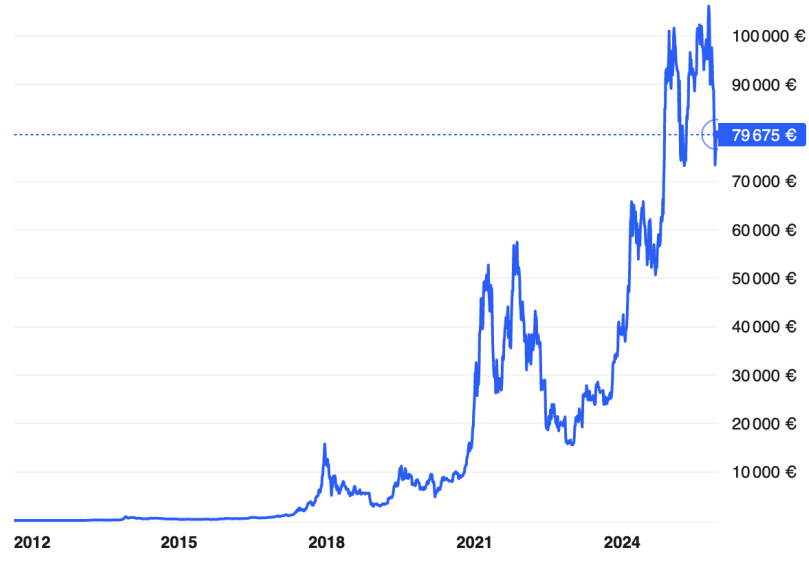
1988 : Digitcash



La révolution Bitcoin 2009

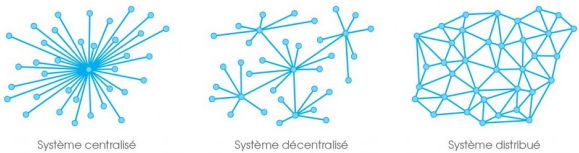


Taux de change du bitcoin 3 décembre 2025



Bitcoin

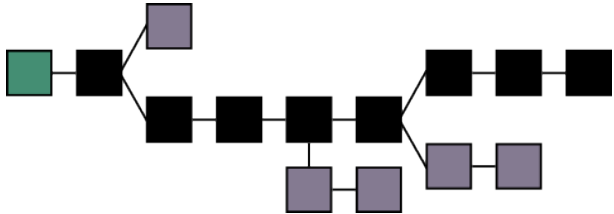
- Cryto-monnaie décentralisée et distribuée



21 millions BTC

Inarrêtable car distribuée

Infalsifiable



Auditable

Porte-monnaie électronique

- Consultation du solde
- Réalisation d'une transaction
- Gestion du stockage des pièces
- Création de nouvelles clefs de compte

Matériel

Numérique

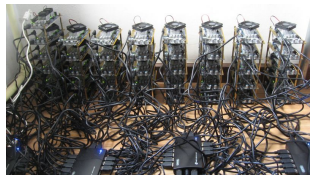
Dématérialisé

Où sont mes clefs privées ?

Miner des Bitcoins

Miner des Bitcoins

Les “*mineurs*” valident les transactions contre des bitcoins



Miner des Bitcoins

- Valider = résoudre un **objectif de hachage**
- Récompense initiale 50 BTC pour une validation
- Divisée par 2 tous les 210000 validations

$$\sum_{i=0}^{32} \frac{50}{2^i} \times 210\,000 = 21 \text{ millions BTC}$$

Miner : Objectif de hachage

Cible pour le block 816 377 (Février 2024)
0000000000000000000481940000000000000000000000000000000000000000

Trouver une nombre n tel que

$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, n)) = x < \textit{Cible}$$

Avoir au moins 18 zéros au début de x

Stratégie : brute force

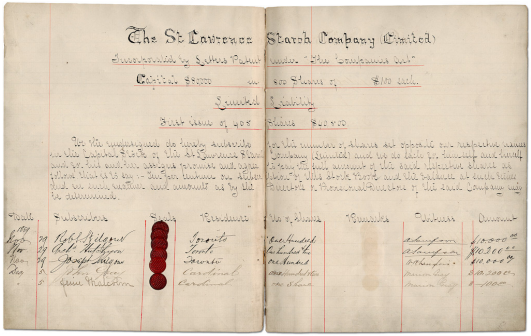
Tester toutes les valeurs possibles de n

Traçable

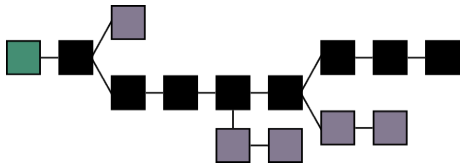
MONERO

ZCASH

Blockchain

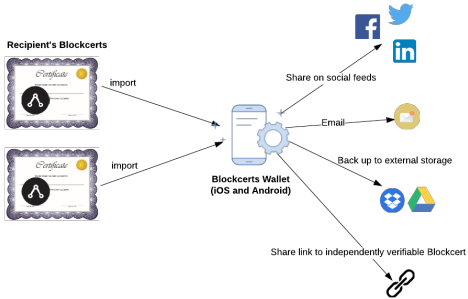


Tiennent à jour le registre distribué

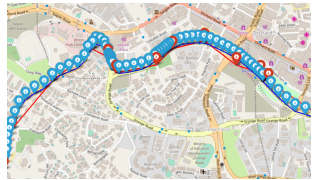


Inarrêtable, Infalsifiable, Auditable

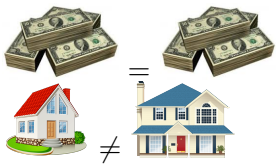
Blockchain Application : MIT Diploma



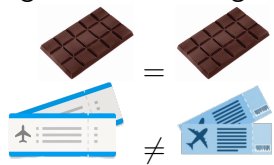
EcoMobiCoin: Proof of Behavior

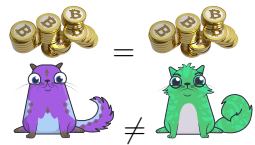


Fungible vs Non-fungible Tokens



Fongible = interchangeable



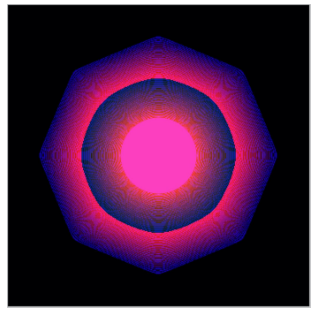


Non-fongible = individuel

Critère	Fongible	Non-Fongible
Interchangeabilité	interchangeable.	non interchangeable, chacun représentant un unique actif.
Divisibilité	divisible en petites parts	Non divisible
Transfert de valeur	dépend du nombre de jetons possédés.	La valeur de l'actif unique représenté par un NFT

Quand a été créé le premier NFT ?

Quantum, mai 2014



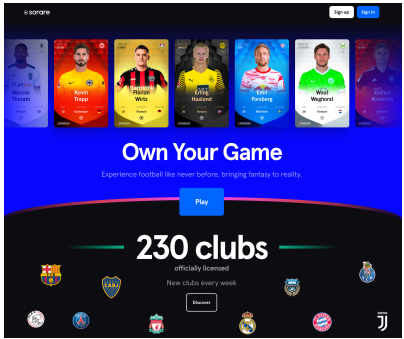
Artiste new-yorkais Kevin McCoy

Premier certificat de propriété numérique déposé sur Namecoin.org
Le 10 juin 2021, vendue aux enchères pour $1,472$ million $

NFT in Card Games and Sport

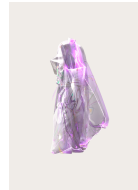
Sorare (Panini like)

- Fantasy Football: stats. d'après les footballeurs réels
- Cartes Sorare comme tokens SOR (ERC-721)
- 150 millions € entre jan. & oct. 2021

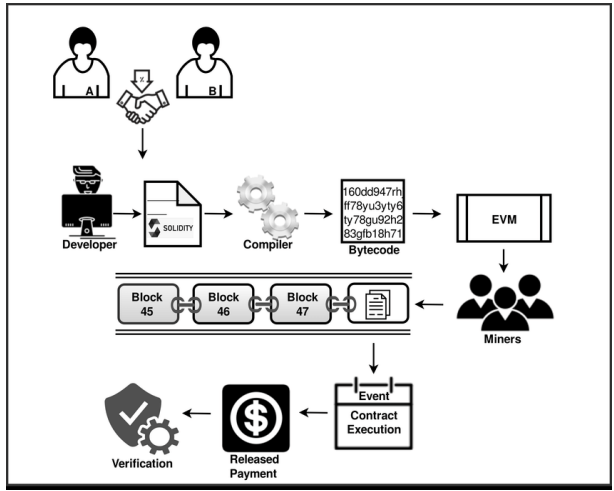


Sneakers virtuels : Cryptokickers

Garderobe dans le Métavers : The Fabricant



Smart Contract



Buisness : en 3 étapes

1. Alice achète 100 pommes à 5 $ à un producteur

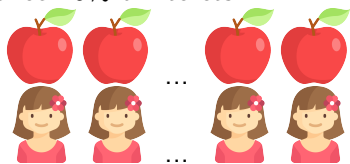
2. Alice vend chaque pomme 6 $

3. Alice gagne 100 $

Ce qu'Alice a besoin



1. Cash : 500 $ $\Rightarrow$ Banque avec 10% d'intêrets



2. 100 acheterur pour 100 pommes




3. Alice gagne seulement 50 $ et la Banque gagne 50 $

Flash Loans / Emprunts Flash

Smart Contract

Tout s'effectue dans un seul bloc de transactions !

1. Alice fait un prêt à la Banque de 500 $
2. Alice achète 100 pommes au producteur
3. Alice vend 1 pomme à 6 $ à B_1

⋮

4.
5. Alice vend 1 pomme à 6 $ à B_100
6. Alice rend 500 $ + 50 $ à la Banque

Alice gagne 50 $.

Stable Coins Centralisés

Stablecoins garantis (Collateralized)

USDT ou USDC = réserve d'actifs tangibles ($>$ 100 M \$).

TrueUSD (TUSD), USD Tether (USDT), USD Circle (USDC), Binance USD (BUSD)
Tether Euro, Euro-L (Lugh), Diem

Stablecoins algorithmique

Gérer par des algorithmes et smart contracts TerraUSD (UST)

Société Générale : EUR CoinVertible (EURCV) en avril 2023 sur Ethereum

Stable Coins Décentralisés

Stablecoins garantis (Collateralized)

17 Décembre 2017 Dai avec MakerDAO, des smart-contrats sur Ethereum comme base le Dollard.

Stablecoins algorithmique

sUSD

Exemples : USD Coin de Circle (USDC), Binance USD (BUSD), Tether (USDT) et DAI.
Les deux plus importantes capitalisations indexées sur l'or sont Tether Gold (XAUt) et Pax de Paxos.

UST de Terra un stablecoin algorithmique

TerraUSD Price Chart, May 1-May 20, 2022

1 UST contre 1 dollar de LUNA

Malgrè 2 milliards de dollars de Bitcoin de rérve pour la fondation LUNA.

Faillite de FTX

THE WALL STREET JOURNAL.

DOW JONES | News Corp — WEDNESDAY, DECEMBER 14, 2022 - VOL. CCLXXX NO. 140 — WSJ.com — ★★★★ $5.00

FTX Founder Is Charged With Fraud

What's News

Business & Finance

FTX founder Bankman-Fried oversaw "one of the biggest financial frauds in American history," a top federal prosecutor said in charging that the former chief executive stole billions of dollars from the crypto-currency exchange's customers while misleading investors and lenders. A1, A6

◆ Consumer prices rose in November at the slowest 12-month pace since December 2021, closing out a

Indictment comes as SEC and CFTC file lawsuits and new chief testifies at hearing

FTX founder Sam Bankman-Fried oversaw "one of the biggest financial frauds in American history," a top federal prosecutor said in charging that the former chief executive stole billions of dollars from the cryptocurrency exchange's customers while misleading investors and lenders.

By Corinne Ramey, James Fanelli and Vicky Ge Huang

An indictment by the U.S. at-

FTX était la 2nd place de marché
Fermée en 10 jours, en novembre 2022

How it happends ?

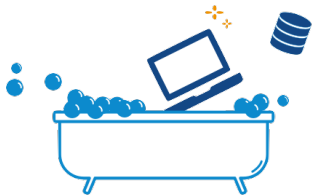
Sam Bankman-Fried a vendu plusieurs millions en une seule fois !

"One of the biggest financial frauds in American history"

MiCa (Market in Crypto Assets) Janvier 2025 en Europe

Encadrer les émissions et les services sur crypto-actifs
PSAN : Prestataire de Service sur Actifs Numériques de la loi Pacte.
(Société Générale Forge, Deblock, GOing et Hexarq)
PSAN $\Rightarrow$ PSCA : Prestataire de Services sur Crypto-Actifs

5 Choses à retenir



- La révolution Blockchain est en marche
- Un formidable outil
- Systèmes décentralisés
- De nombreuses applications mais bien comprendre les limites
- La cryptographie est au centre de la sécurité

Merci pour votre attention

Questions ?