

Démystifions les cryptomonnaies

Pascal Lafourcade



Zénith, Crédit Agricole
9 décembre 2025

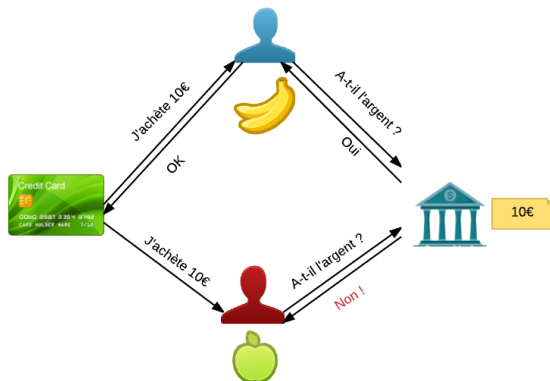
Sumériens vers 3.500 av J.C



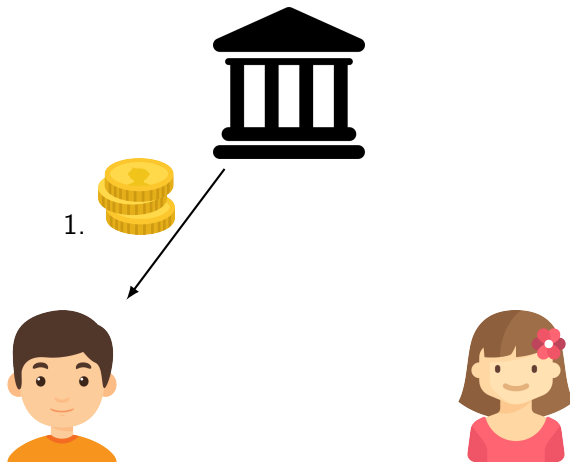
Nombreuses monnaies



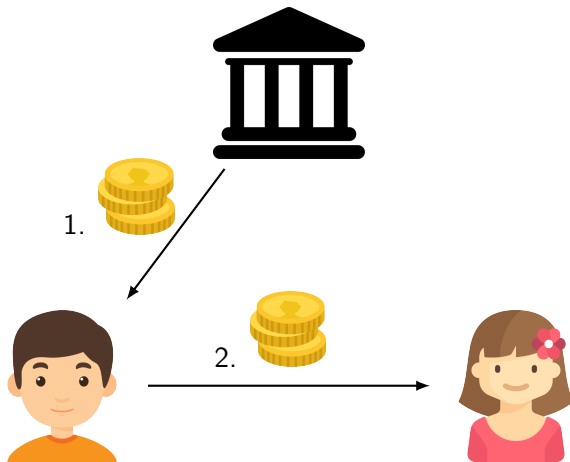
Monnaie électronique : Éviter la double dépense



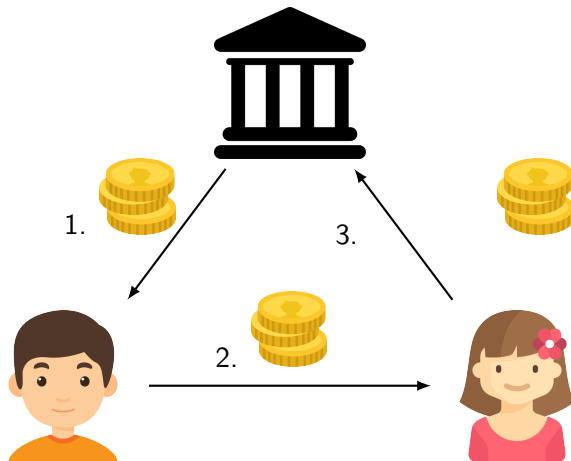
Principe : Banque centrale



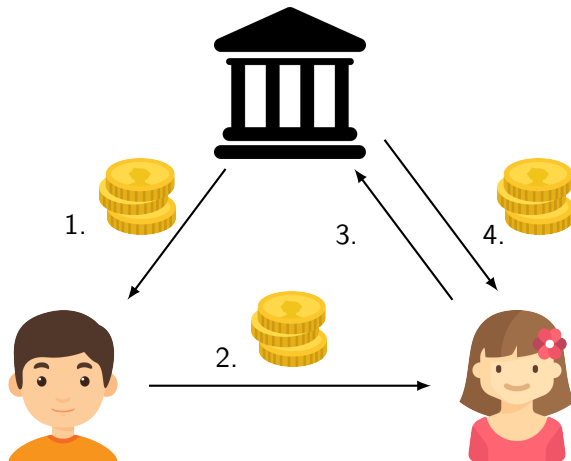
Principe : Banque centrale



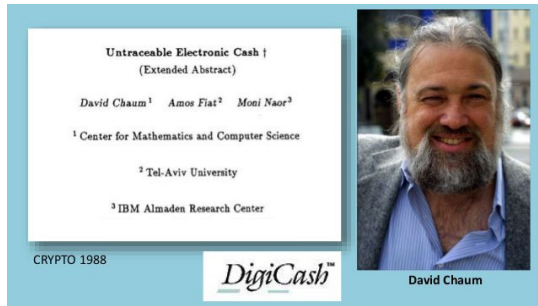
Principe : Banque centrale



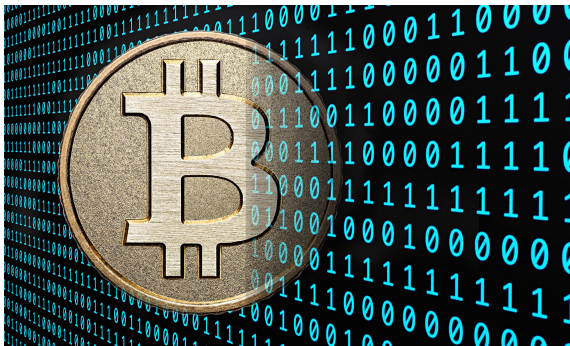
Principe : Banque centrale



1988 : Digtcash



La révolution Bitcoin 2009



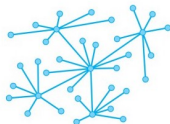
Taux de change du bitcoin 3 décembre 2025



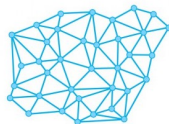
► Crypto-monnaie décentralisée et distribuée



Système centralisé



Système décentralisé



Système distribué

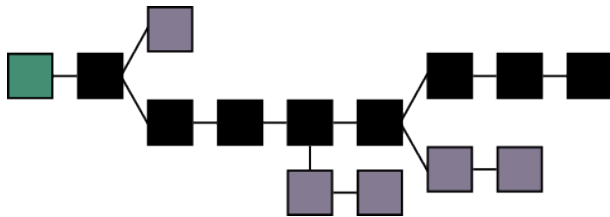


21 millions BTC

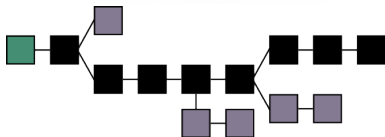
Inarrêtable car distribuée



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 ?

Les “mineurs” valident les transactions

Transactions : UTXO (Unspent transaction output)

CRÉDIT AGRICOLE ALPES PROVENCE

à rédiger exclusivement en euros €

Payez contre ce chèque Quinze Euros
non endossable sauf au profit d'une banque ou d'un établissement assimilé

A Alain

Payable en France
13 **MARIGNANE**
T: 0892 897 139 (*)
(*) 0.34 euro 10/min
N° de compte 3447 50

ASS PYRAMIDORPOINTCOM
26 BOULEVARD GEORGES CLEMENCEAU
13700 MARIGNANE

N° 00 78 Série: 00
▼ N° du chèque ▼

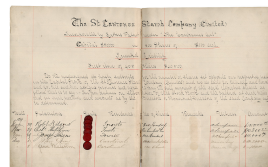
€ **15€**

A **Marignane**
Le **09/01/2006**

[Signature]
<48> Signature

⑈0078⑈0013011306908⑈034⑈50⑈

Écrivent les transactions valides sur la blockchain.



Miner des Bitcoins



Miner des Bitcoins



Les “*mineurs*” valident, écrivent les transactions et créent 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

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





Cible pour le block 926 895 (7 décembre 2025)

$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, n)) < 149301205959700$$

Stratégie : brute force

Tester toutes les valeurs possibles de n

Traçable

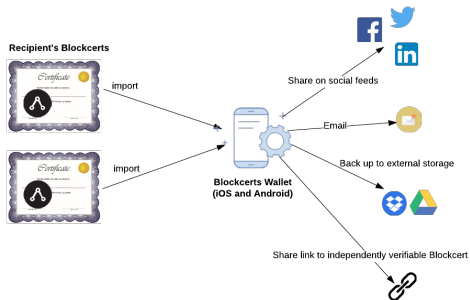


MONERO

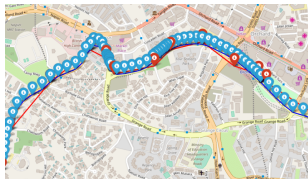


CASH

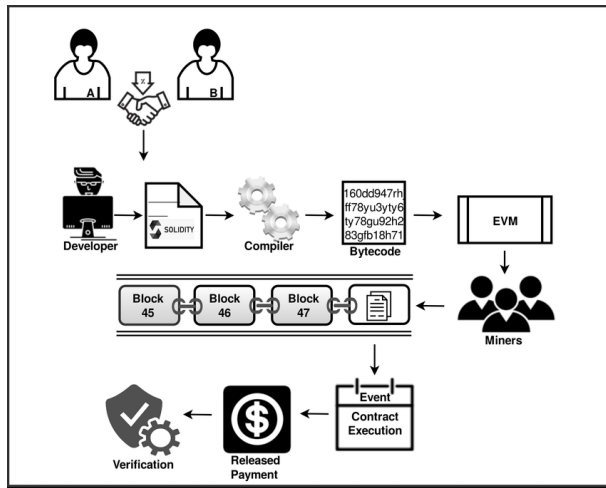
Blockchain Application : MIT Diploma



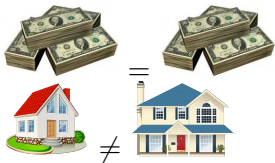
EcoMobiCoin: Proof of Behavior



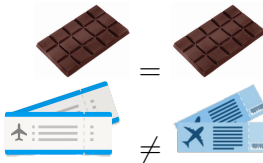
Smart Contract



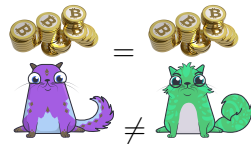
Fungible vs Non-fungible Tokens (NFT)



Fongible = interchangeable

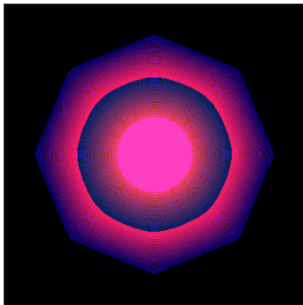


Non-fongible = individuel



Quand a été créé le premier NFT ?

Quantum, mai 2014



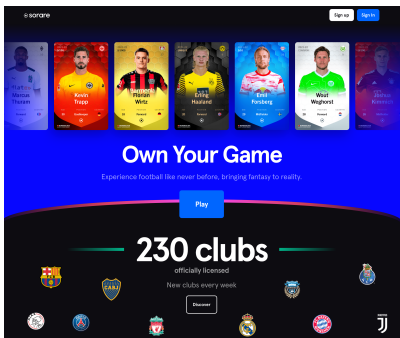
Kevin McCoy

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

Applications des NFT

Sorare (Panini like)

- ▶ Stats d'après les footballeurs réels
- ▶ Cartes Sorare comme tokens SOR (ERC-721)



Sneakers virtuels Cryptokickers



Garderobe virtuelle The Fabricant



Buisness : en 3 étapes



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



2. Alice vend chaque pomme 6 \$

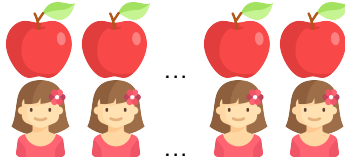


3. Alice gagne 100 \$

Ce qu'Alice a besoin



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



2. 100 acheteurs pour 100 pommes



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

Flash Loans / Emprunts Flash



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

Stablecoins garantis

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

UST de Terra un stablecoin algorithmique



1 UST contre 1 dollar de LUNA

Malgré 2 milliards de dollars de Bitcoin de réserve pour la fondation LUNA.

Faillite de FTX la 2nd place de marché en 2022



Fermée en 10 jours, en novembre 2022

Que s'est-il passé ?

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

Merci pour votre attention

Questions ?

