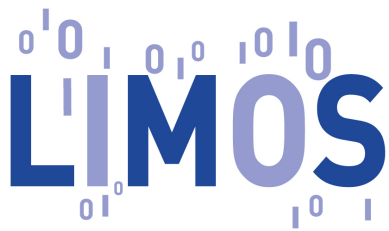

JEAN-GUILLAUME DUMAS • PASCAL LAFOURCADE
ARIANE TICHIT • SÉBASTIEN VARRETTE
LES
BLOCK CHAINS
EN 50 QUESTIONS
-
Comprendre le fonctionnement et les enjeux de cette technologie
DUNOD


JEAN-GUILLAUME DUMAS • PASCAL LAFOURCADE • ETIENNE ROUDEIX
ARIANE TICHIT • SÉBASTIEN VARRETTE
LES
NFT
EN 40 QUESTIONS
-
Des réponses claires et détaillées pour comprendre les Non Fungible Tokens
DUNOD

Bitcoin, la Blockchain et les NFT

Pascal Lafourcade



Online, le 12 mars 2023

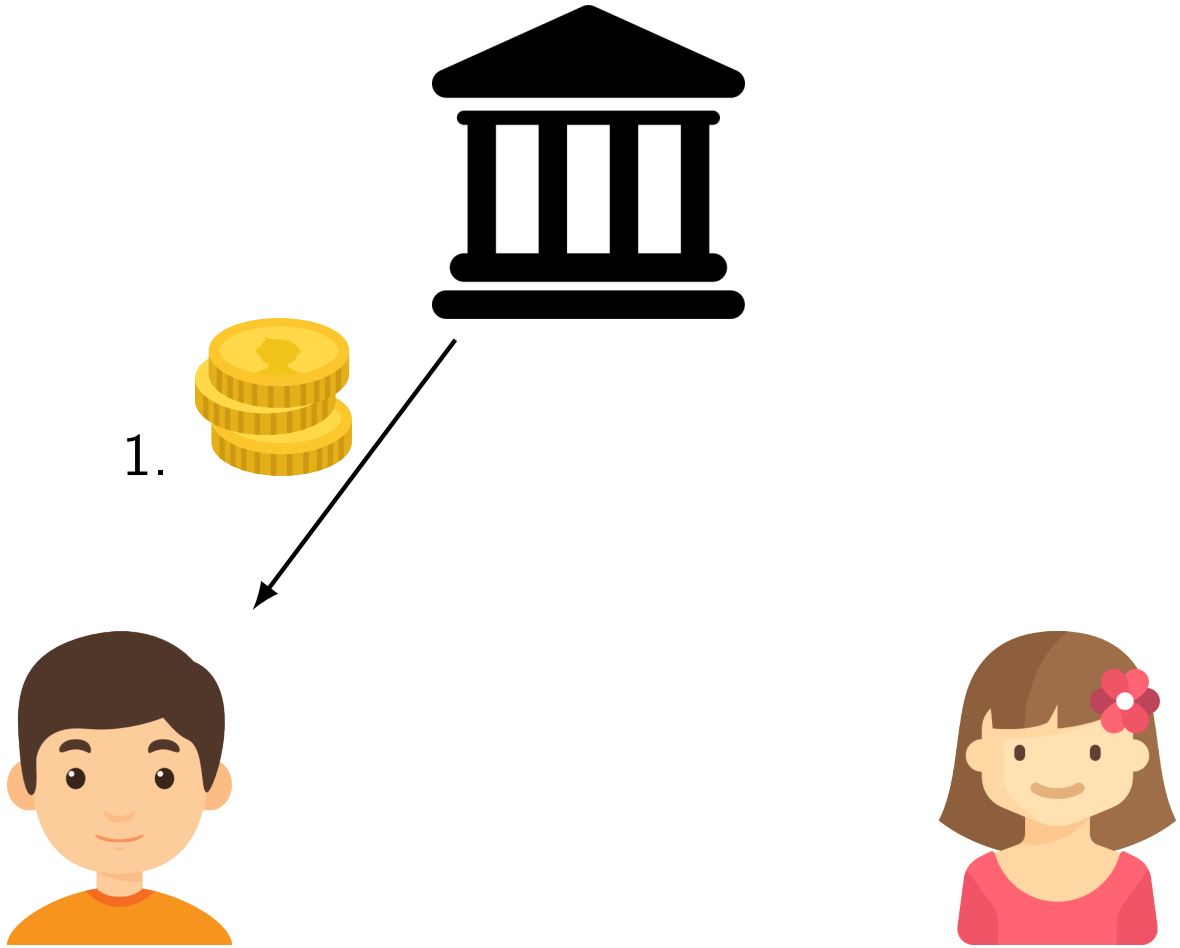
Sumériens vers 3.500 av J.C

Qu'est-ce que la monnaie?

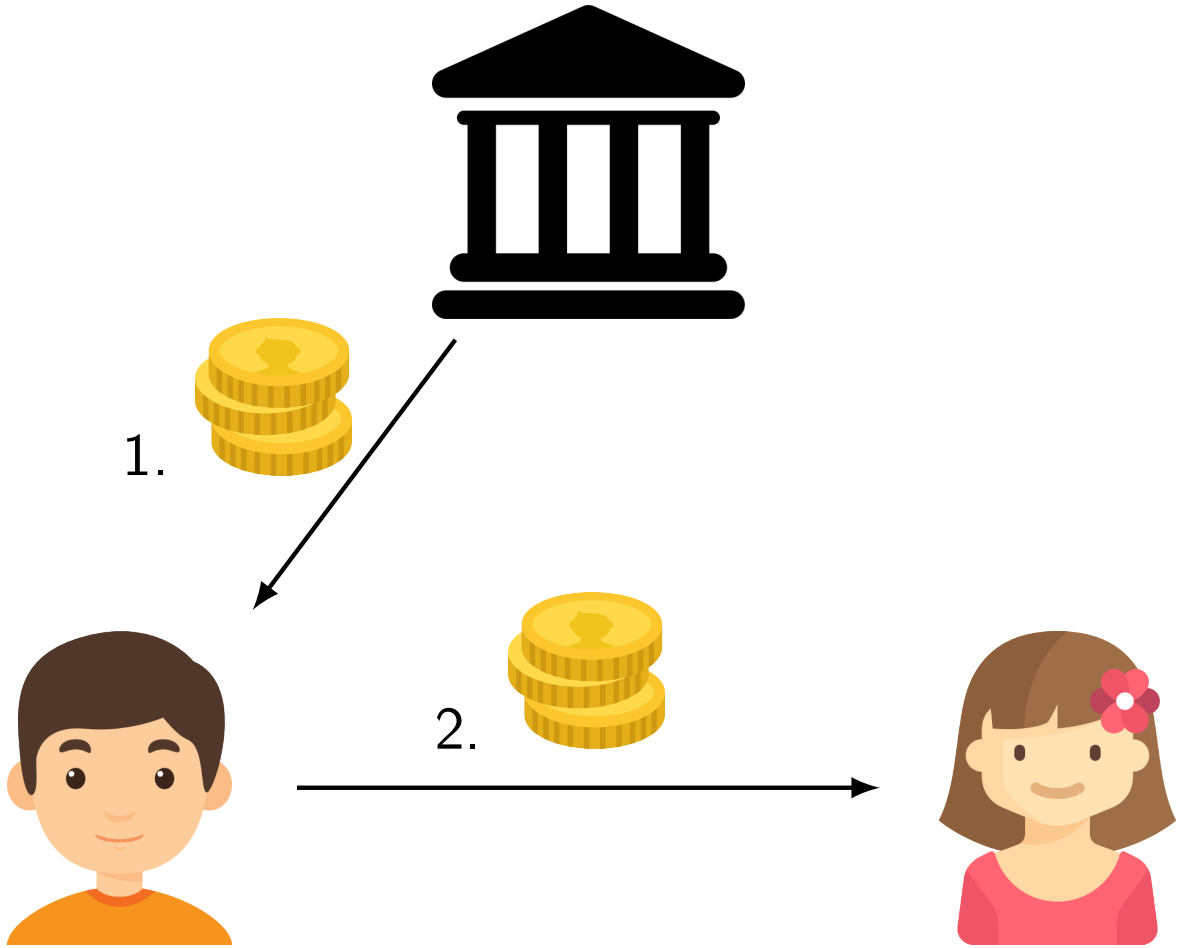
- Intermédiaire et moyens d'échanges de biens et services entre les individus
- Réserve de valeur
- Unité de compte

Nombreuses monnaies

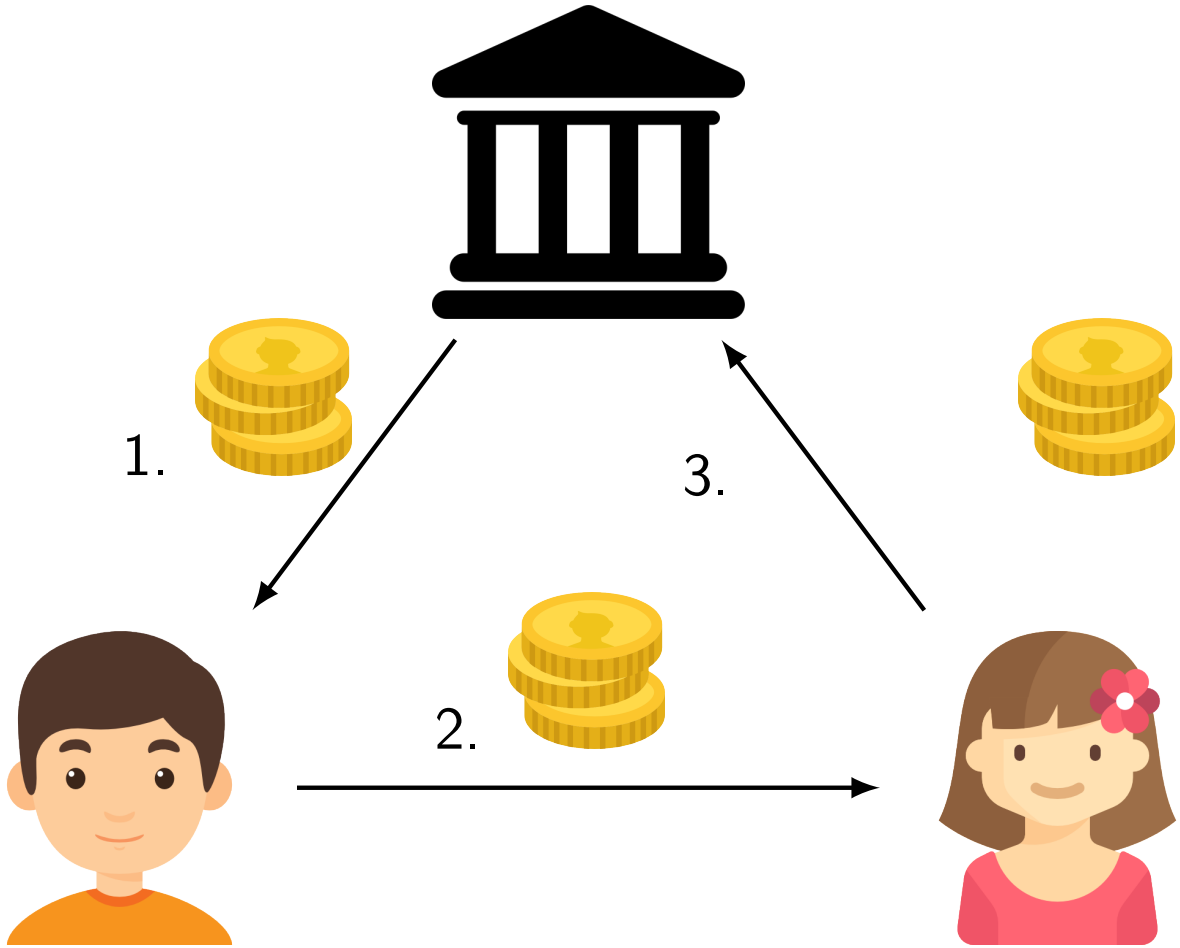
Principe : Banque centrale



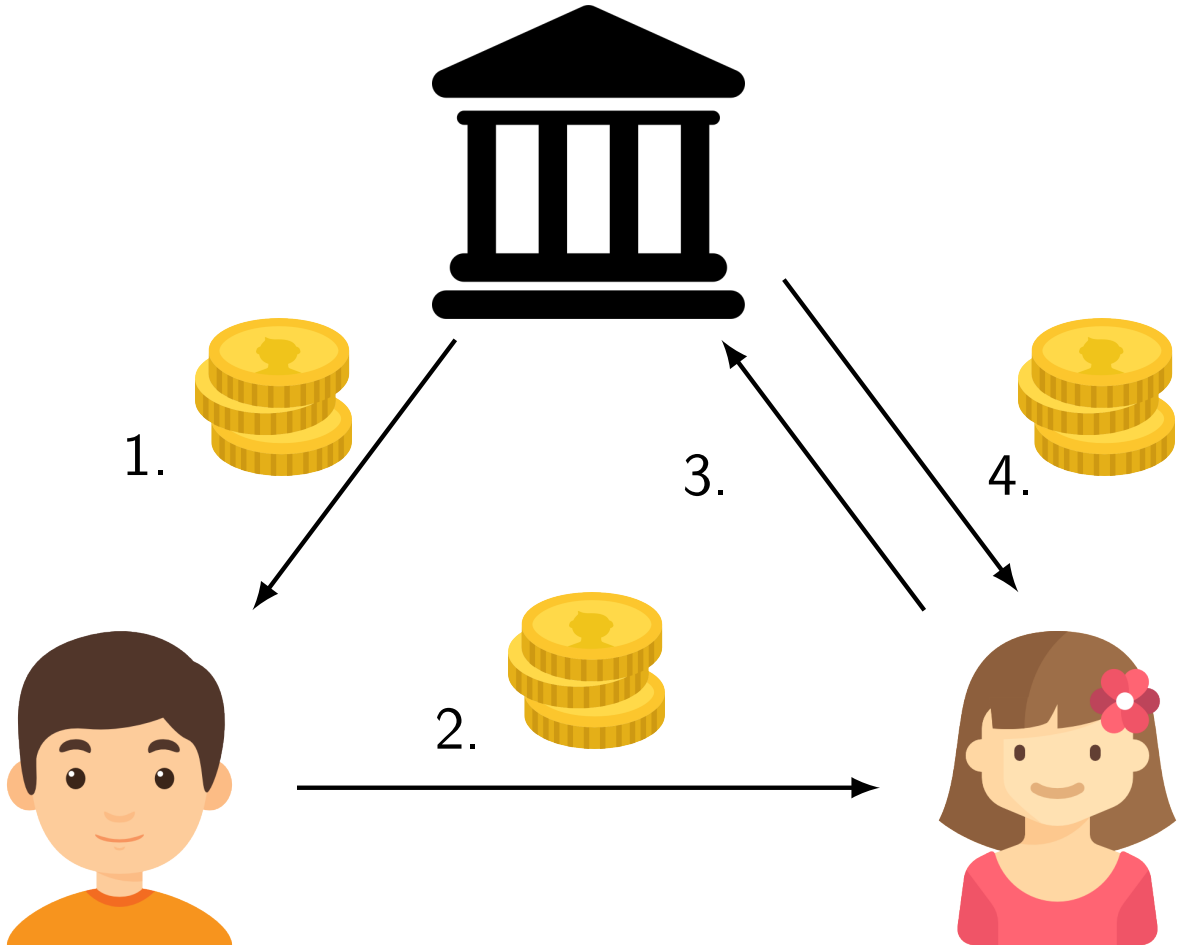
Principe : Banque centrale



Principe : Banque centrale



Principe : Banque centrale



1988 : Digitcash

Untraceable Electronic Cash †
(Extended Abstract)

David Chaum[1] *Amos Fiat*[2] *Moni Naor*[3]

[1] Center for Mathematics and Computer Science

[2] Tel-Aviv University

[3] IBM Almaden Research Center

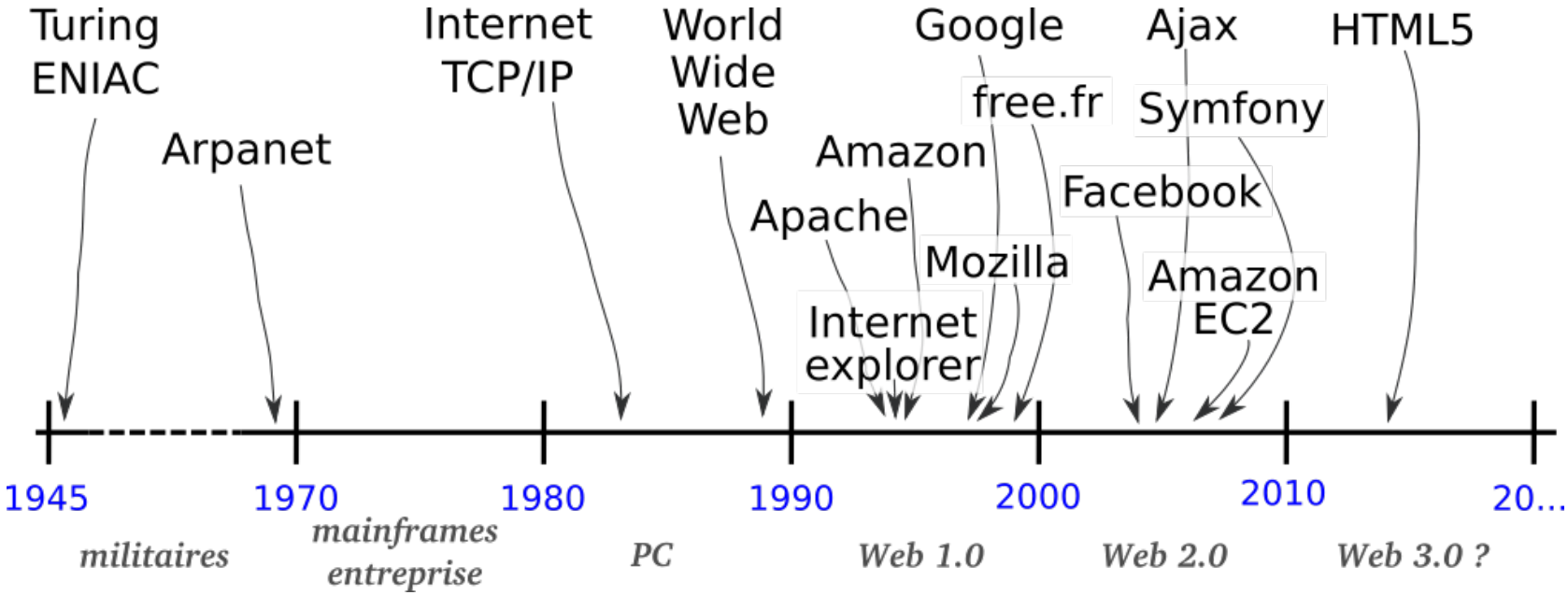
CRYPTO 1988

DigiCash™

David Chaum

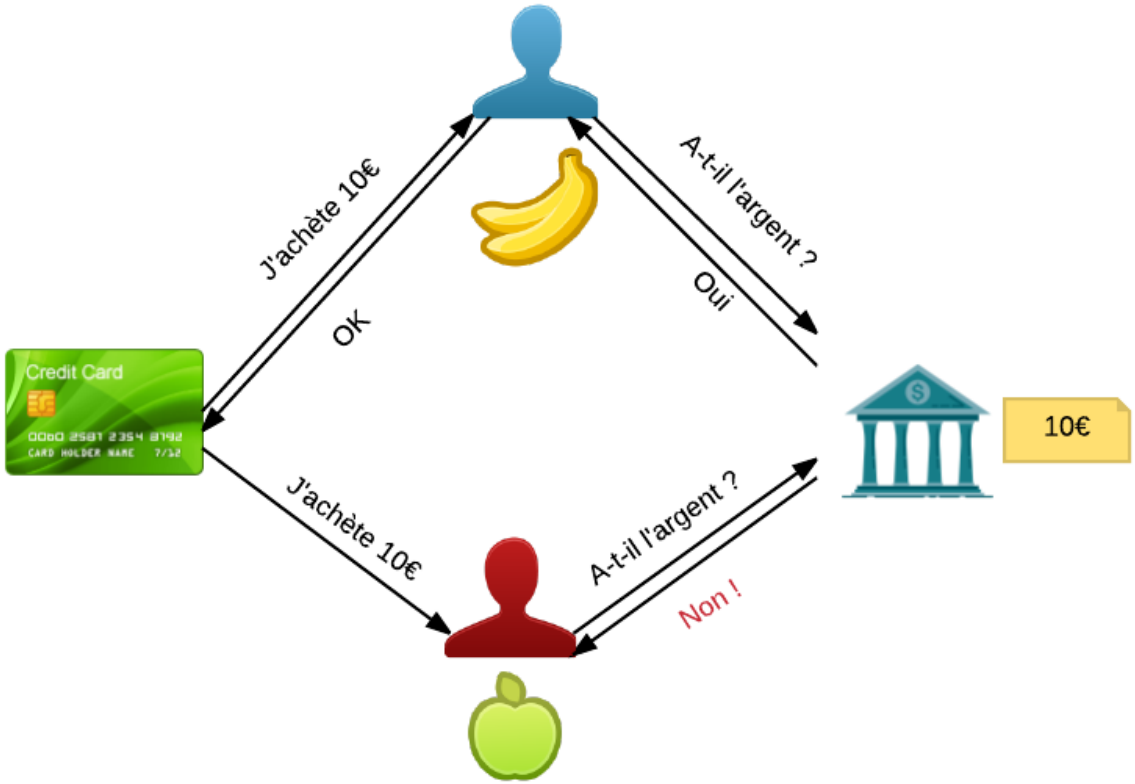
- ☺ Préserve la vie privée
- 😐 À l'aide de primitives cryptographiques
- ☹ Nécessite toujours un tiers (banque)

Une idée visionnaire en avance sur son temps



Propriétés : Non-Falsifiable (Unforgeable)

Propriétés : Eviter la double dépense



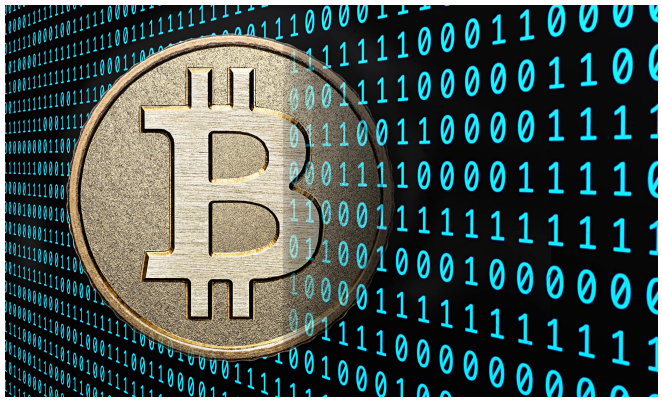
- identifiation fraudeur

- "présemption d'innocence"

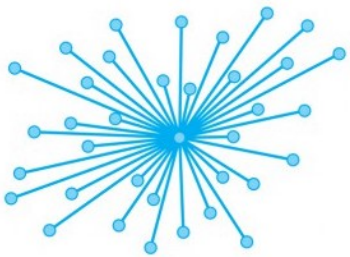
Propriétés : Respect de la vie privée

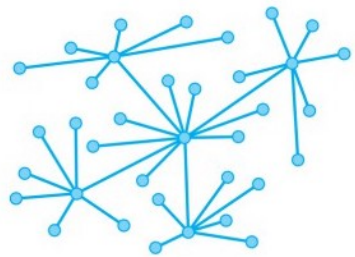
- Anonymat faible : non identification d'un acheteur
- Anonymat fort : non traçabilité d'un acheteur

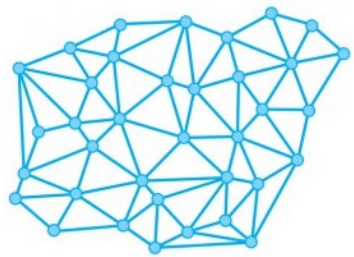
La révolution Bitcoin 2009



- Cryto-monnaie décentralisée et distribuée


Système centralisé


Système décentralisé


Système distribué

21 millions BTC

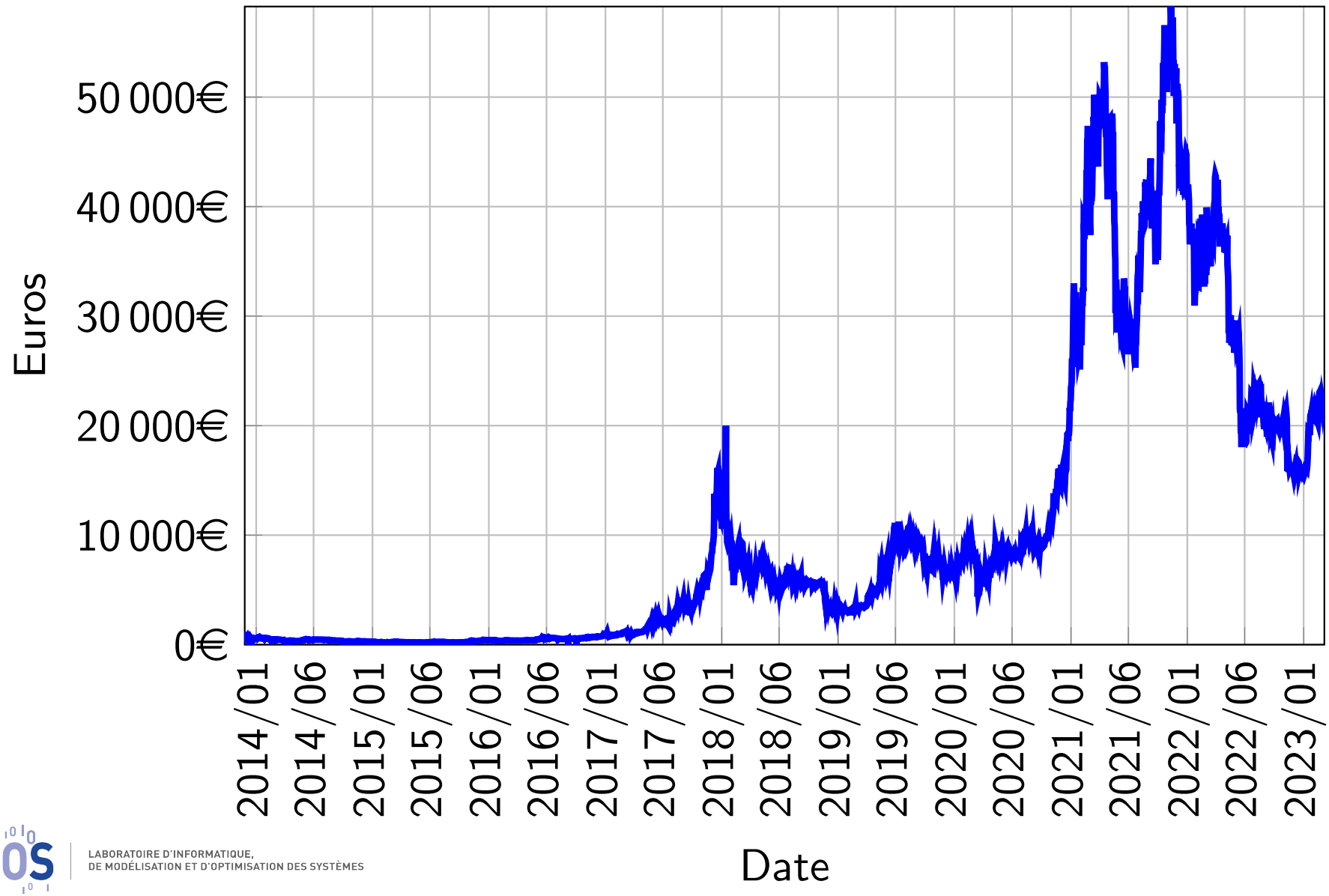
Bitcoin : monnaie électronique

Créée par Satoshi Nakamoto

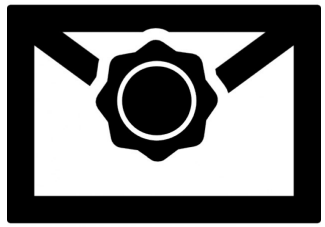
1 BTC $\approx$ 25 411,62 € le 9 avril 2023

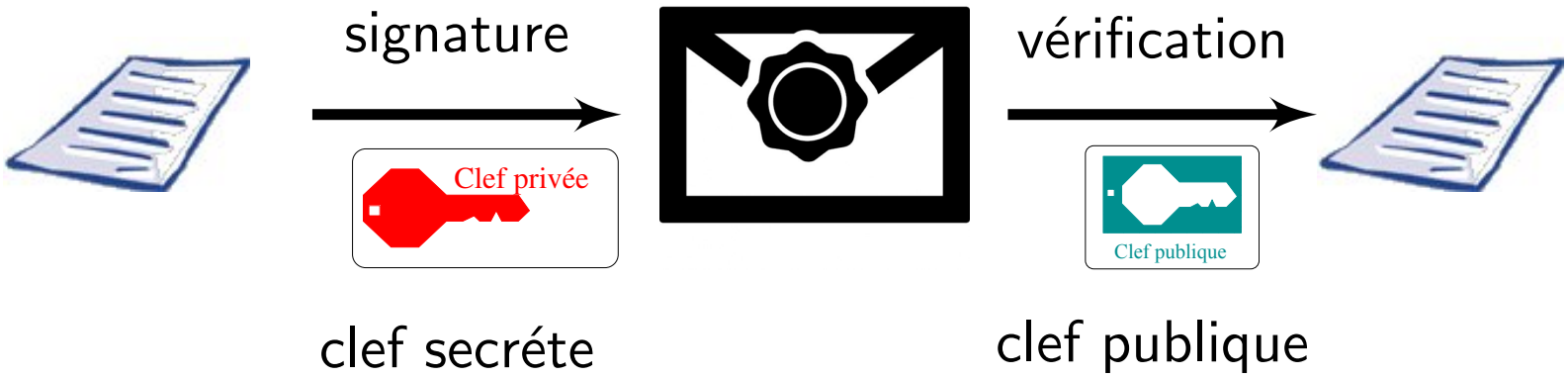
1	BTC = 1 Bitcoin	
0,01	BTC = 1 cBTC	= 1 centiBitcoin (ou bitcent)
0,001	BTC = 1 mBTC	= 1 milliBitcoin
0,000 001	BTC = 1 μBTC	= 1 microBitcoin
0,000 000 01	BTC = 1 Satoshi	

Taux de change du bitcoin



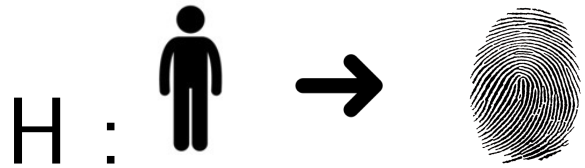
Signature





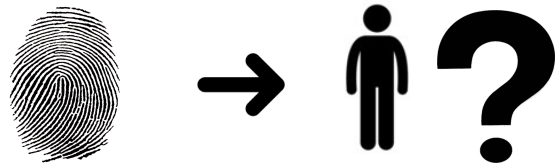
RSA: $m^d \mod n$

Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)

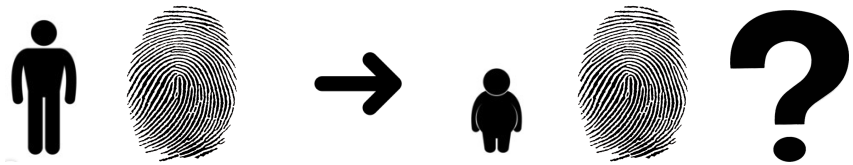


Propriétés de résistance

- Pré-image

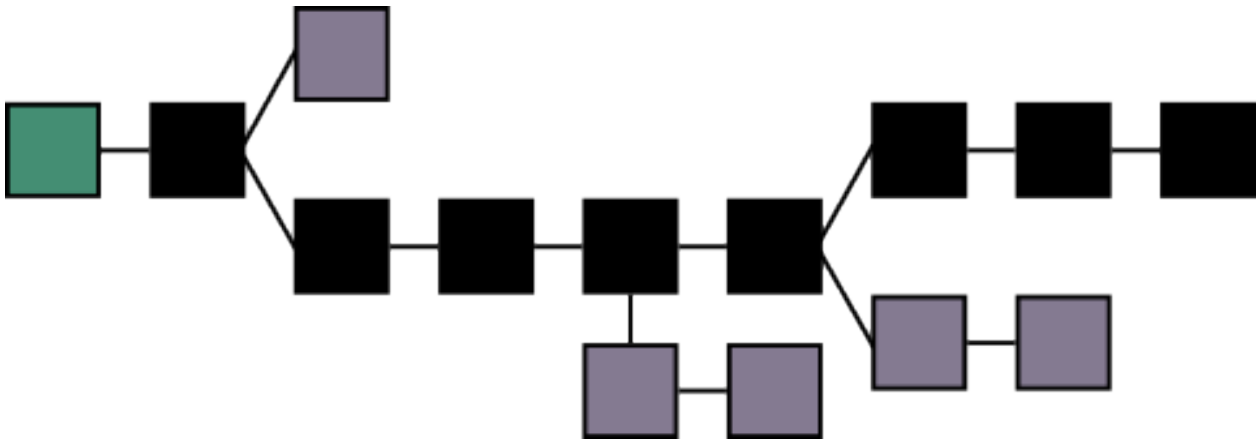


- Seconde Pré-image

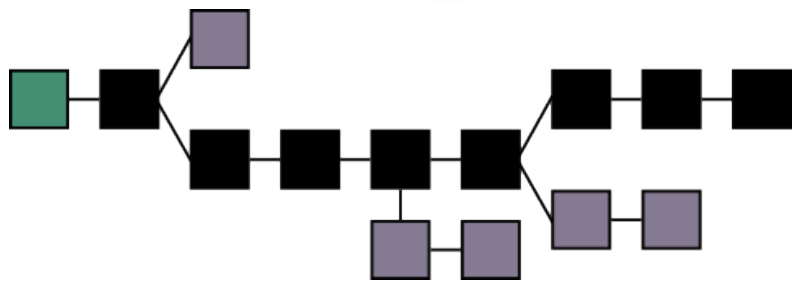


- Collision

Infalsifiable : Chaîne de blocs



Auditable



LIMOS
LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Inarrêtable car distribuée

Bitcoins : caractéristiques

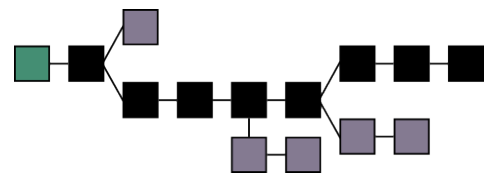
- Le nombre total de bitcoins est **fini**

  21 millions BTC

- Numéro de compte :

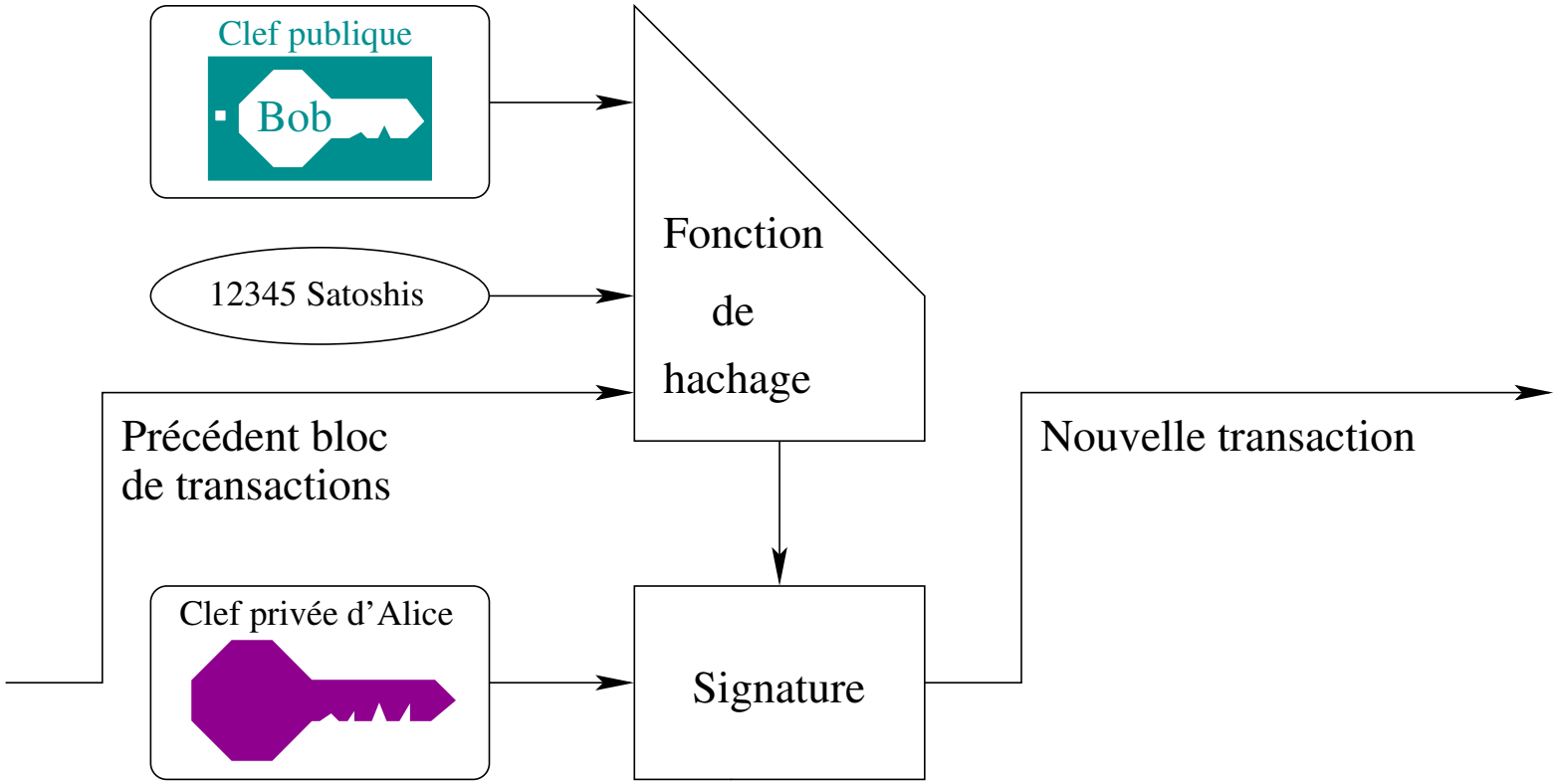
  $$\text{RIPEMD-160}(\text{SHA-256}(\text{ECDSA}_{pub}))$$

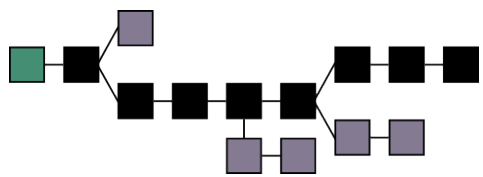
- Toutes les transactions sont **publiques**
- **Blockchain** : un système pair-à-pair qui garantit la validité des transactions



Comment faire une transaction?

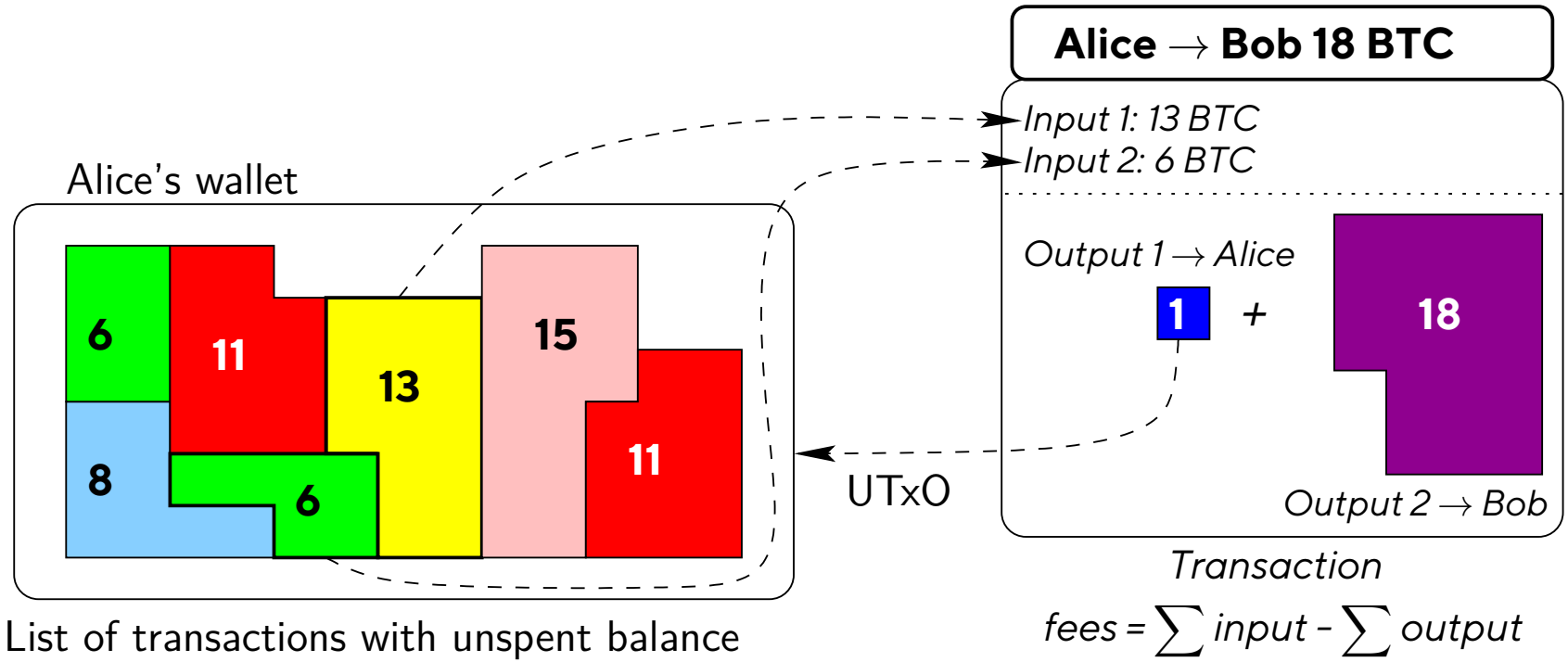
Alice donne 12345 Satochis ($\approx 5c$) à Bob.



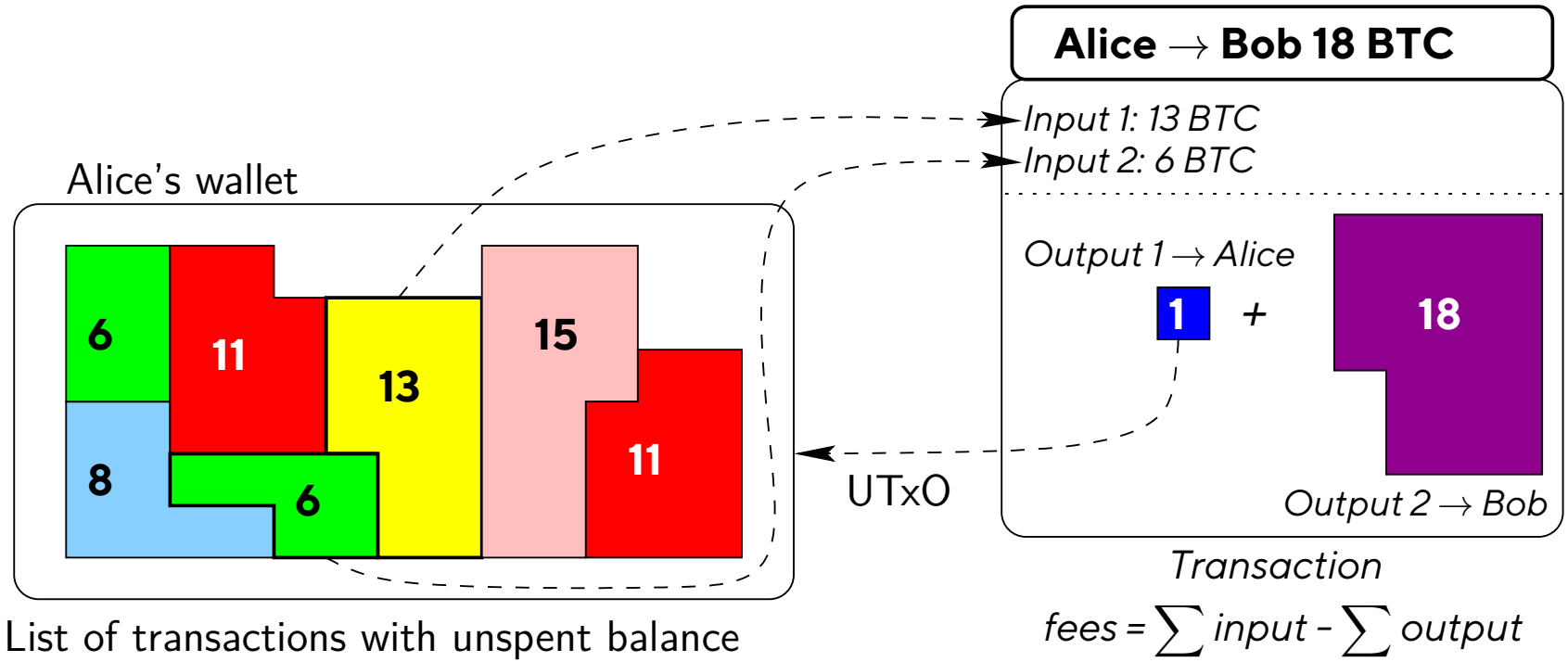


Unspent Transaction Output UTXO

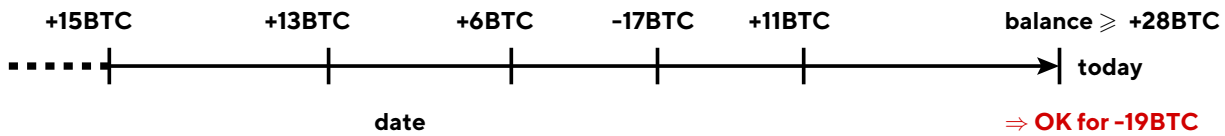
Pay 18 BTC with coins



Pay 18 BTC with coins



- Seul les bitcoins possédés peuvent être dépensés, UTXO (Unspent transaction output)



LIMOS LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Porte-monnaie électronique

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

1. Sécurité
2. Disponibilité
3. Facilité

Matériel

Numérique

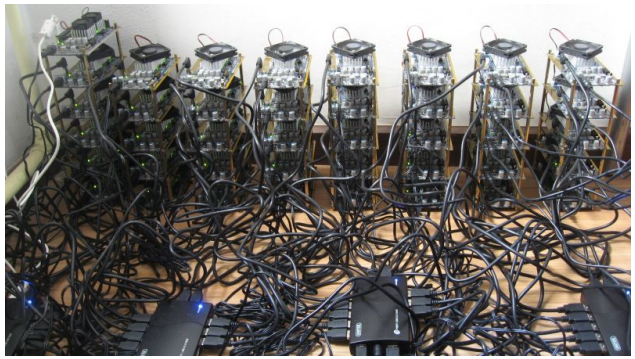
Dématérialisé

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 = 0000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076

Trouver une nombre n tel que

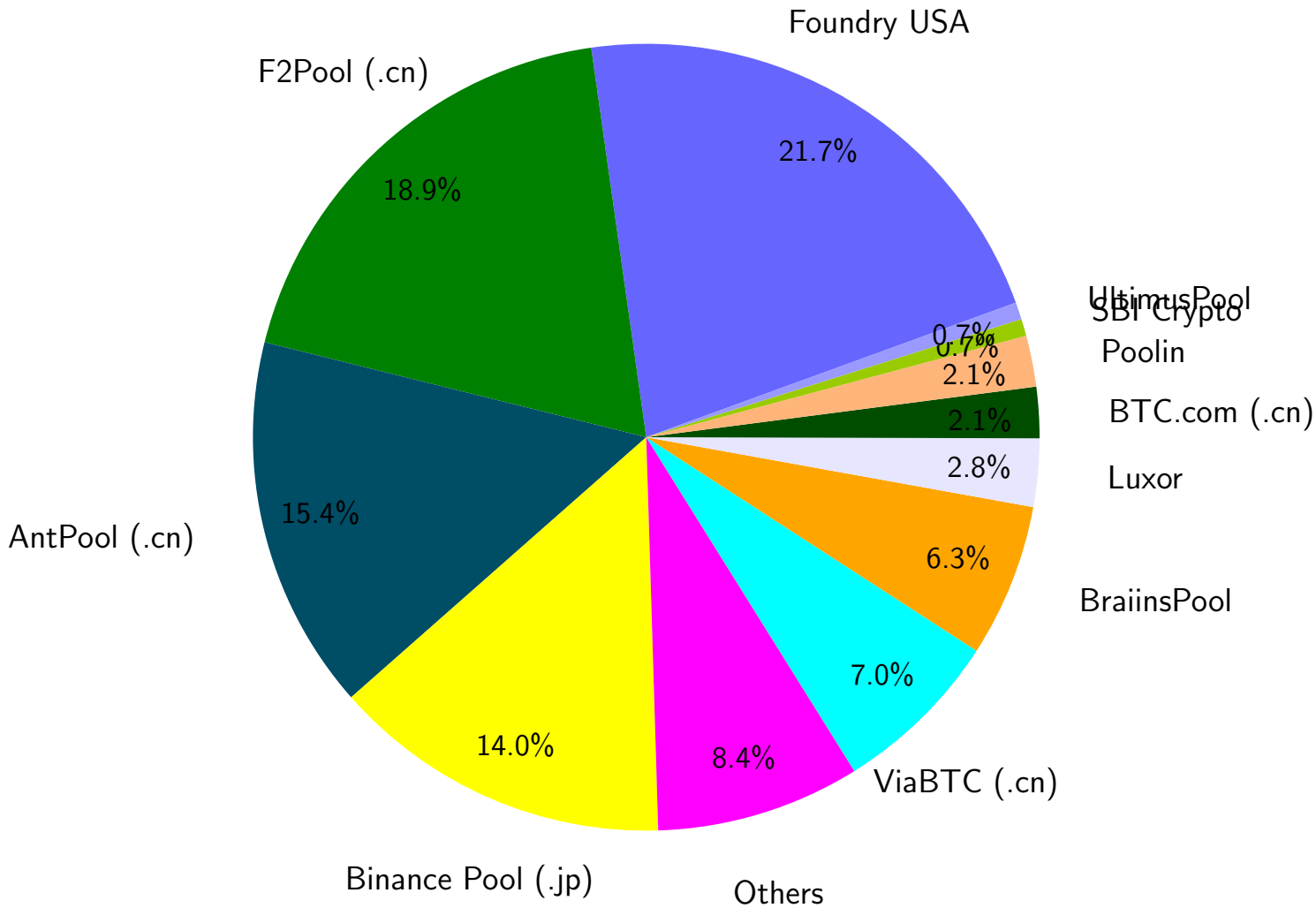
$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, n)) = x < \textit{Cible}$$

Avoir au moins 18 zéros au début de x

Stratégie : brute force

Tester toutes les valeurs possibles de n

Fermes de mineurs: partagent les récompenses

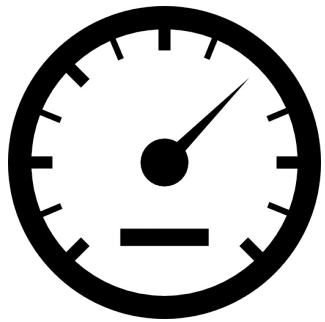


Traçable

Traçable

Snark

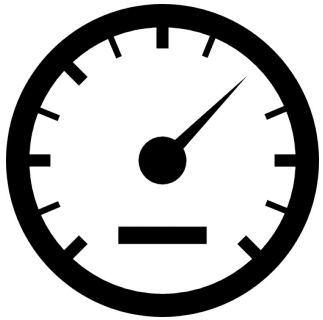
Limitations



10 minutes = 1 block

Taille des transactions 1 Mo

Limitations



10 minutes = 1 block

Taille des transactions 1 Mo

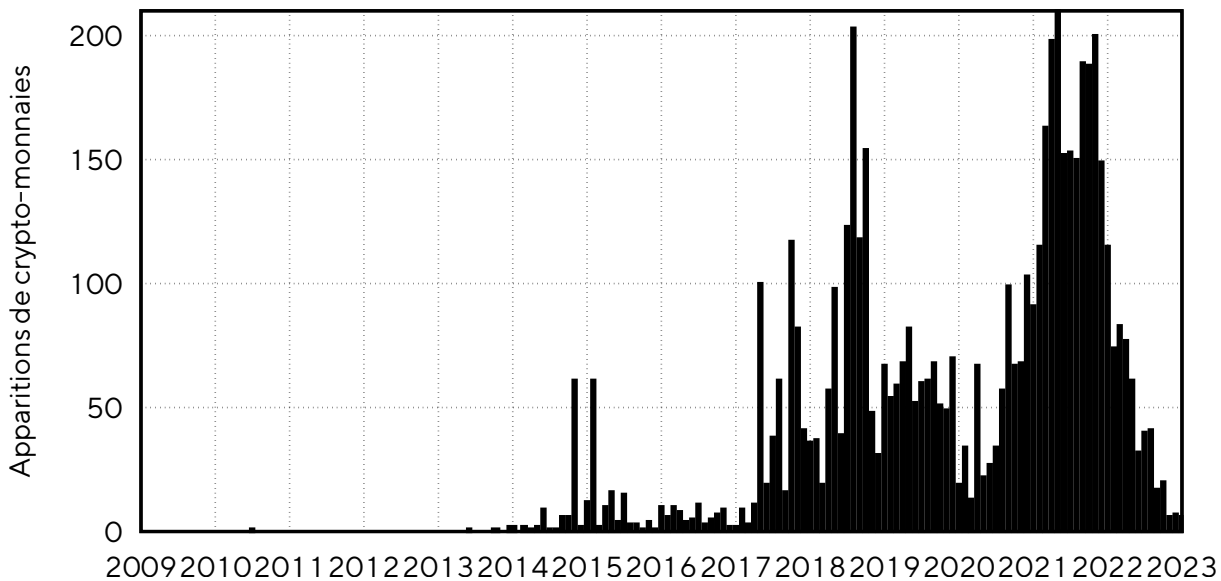
Lightning Network

12 secondes

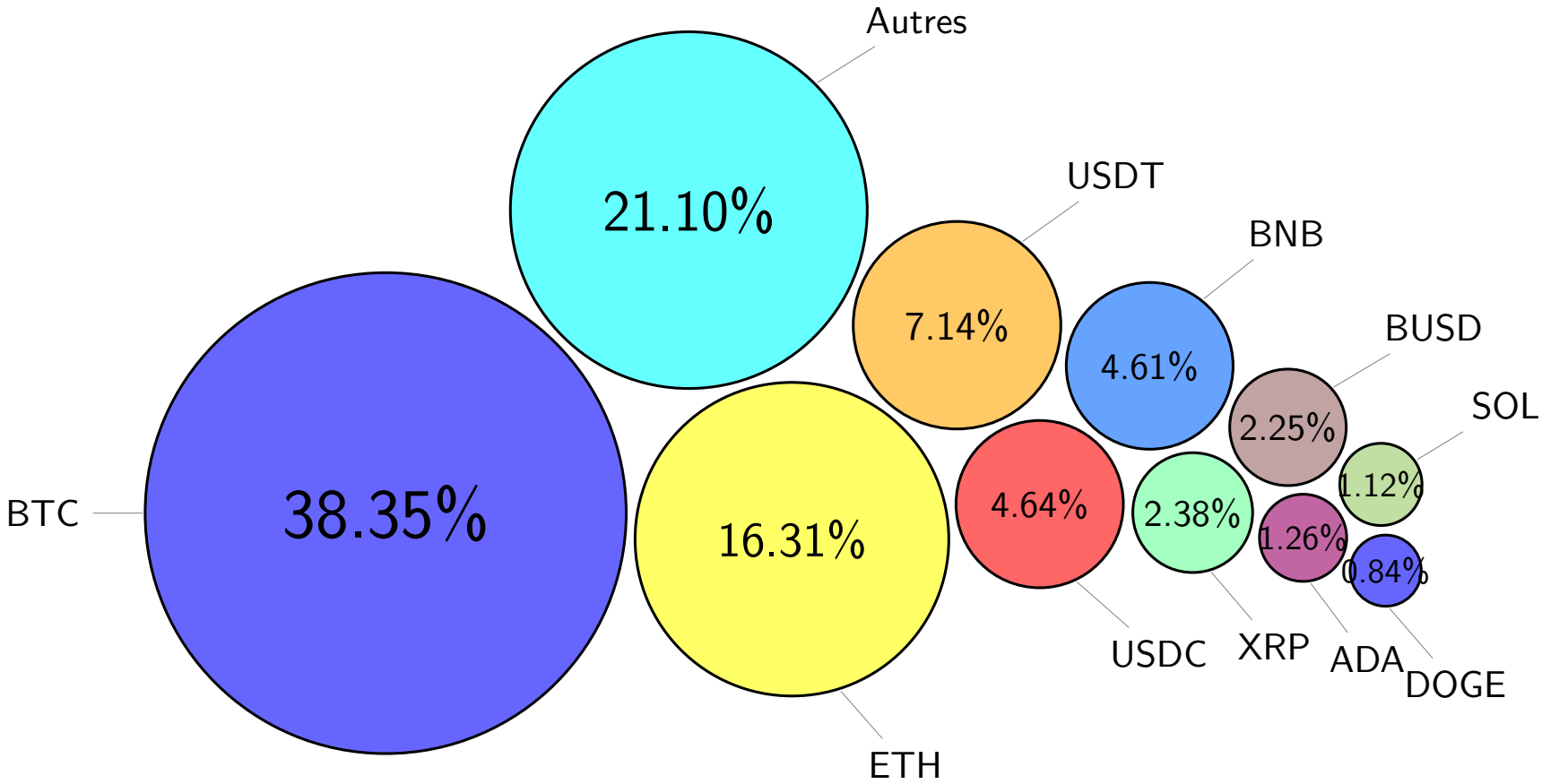
Energivore

Proof of Stake
Lightning Network

Autres crypto-monnaies

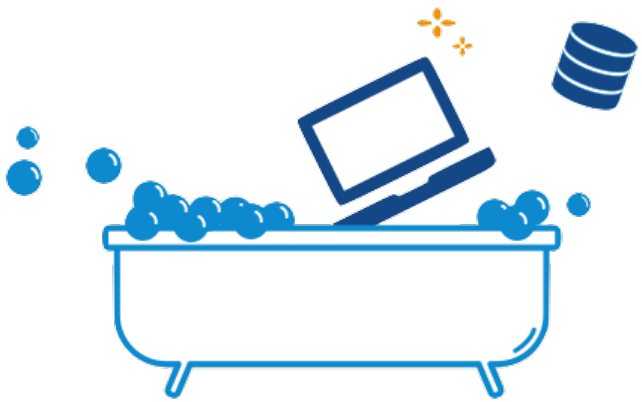


Diversité monétaire



Qui s'approprie ces nouvelles monnnaies ?

Freins

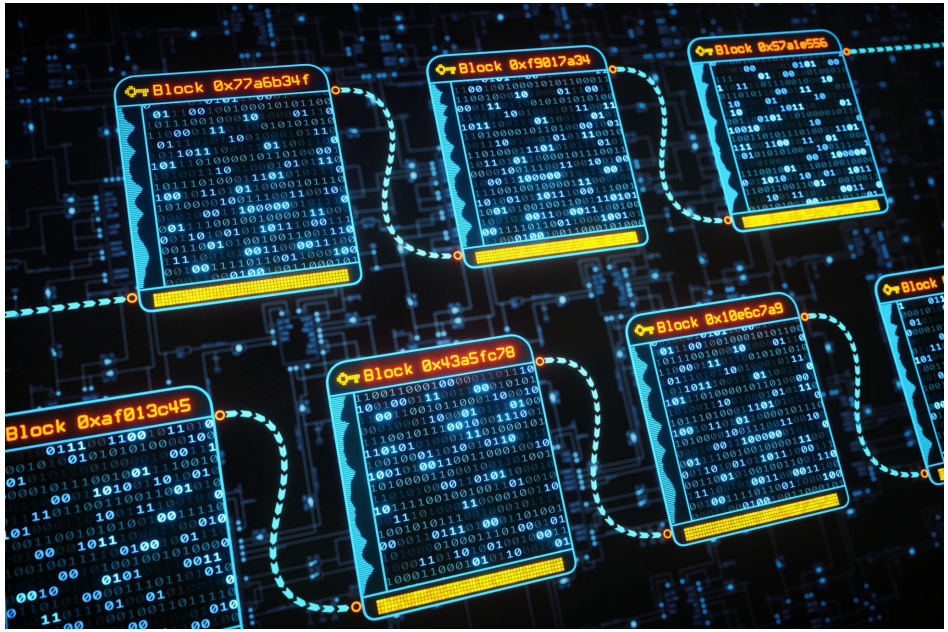


Bitcoin : Crypto-monnaie dématérialisée décentralisée

- Preuve de travail = Objectif de Hachage
- Création de la monnaie = récompense aux mineurs
- Miner = difficile + energivore

- Perte ou vol de la clef secrète = irréversible
- Monnaie anonyme et traçable

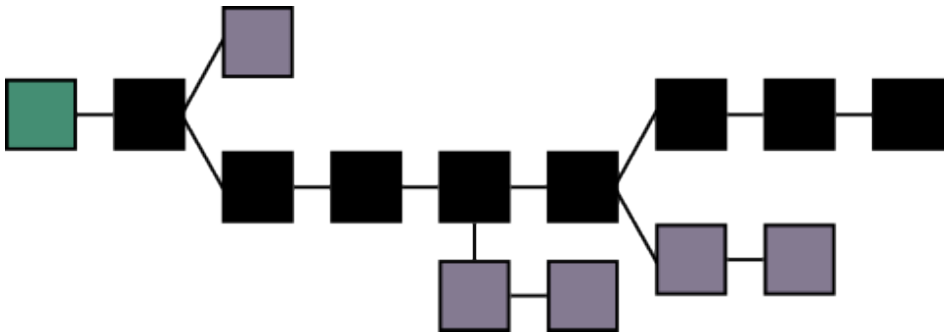
Blockchain



Registre distribué, sécurisé, infalsifiable

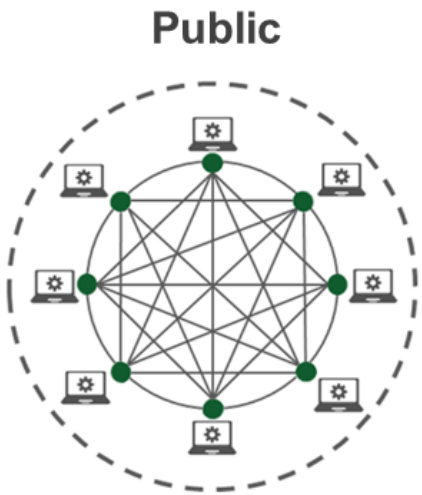
Mineurs valident des transactions

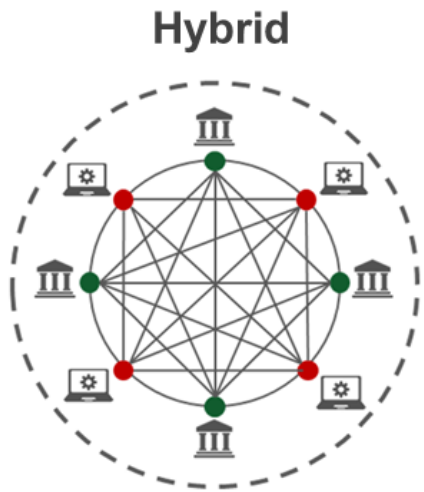
Tiennent à jour le registre distribué

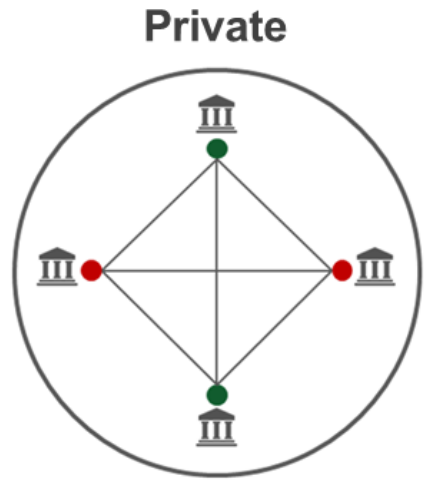


Inarrêtable, Infalsifiable, Auditable

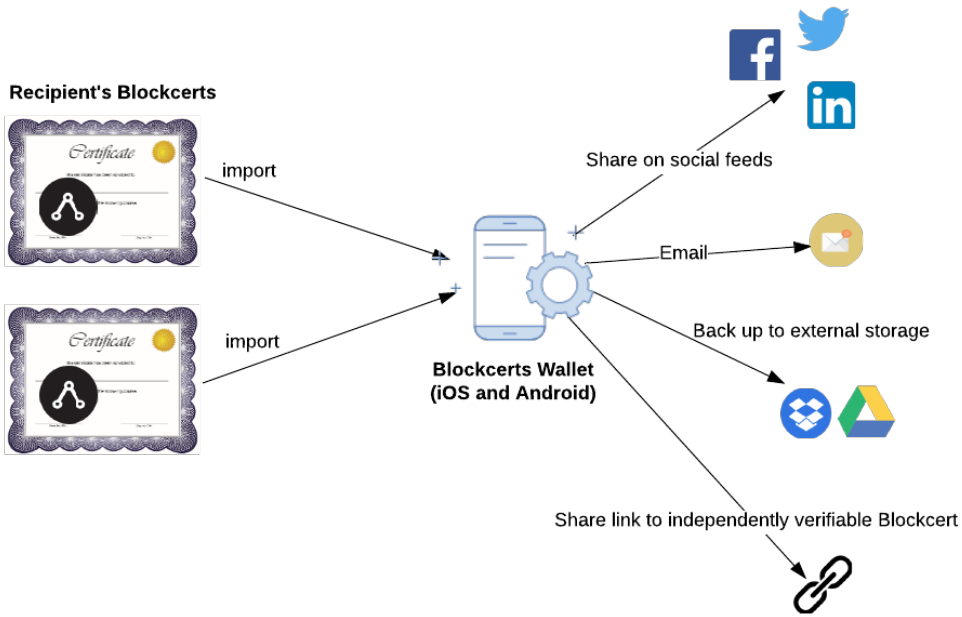
Blockchain Privée vs Publique



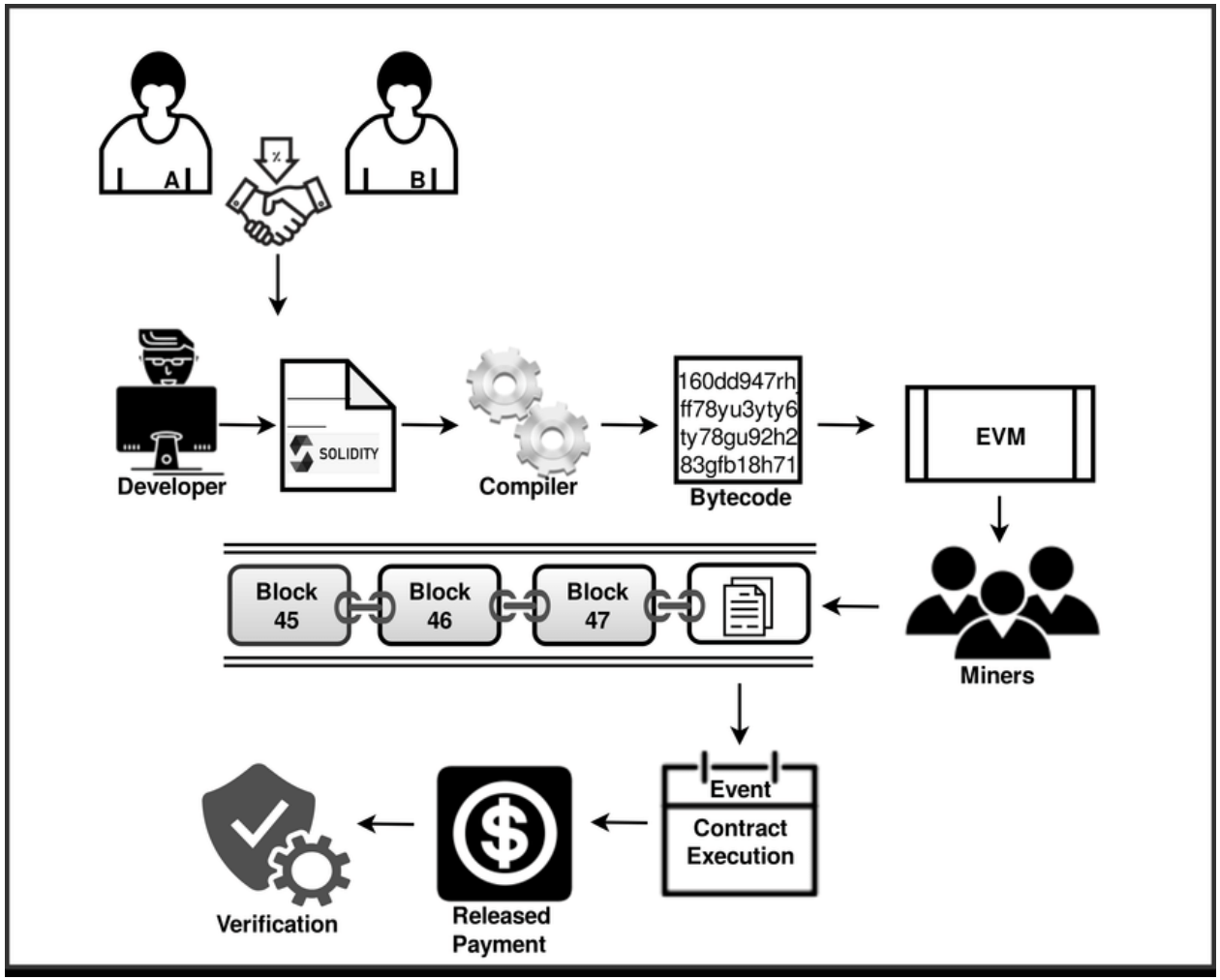




Blockchain Application : MIT Diploma

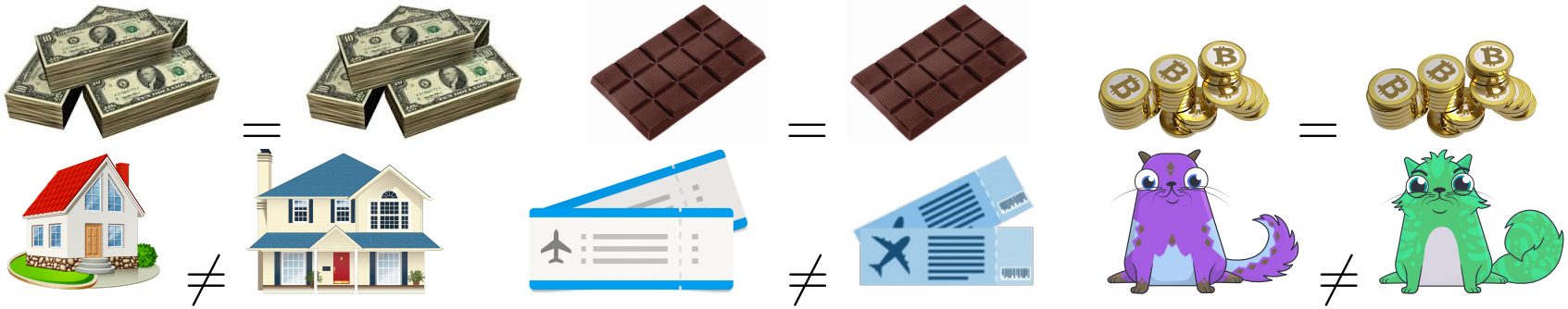


Smart Contract



Fungible vs Non-fungible Tokens

Fongible = interchangeable



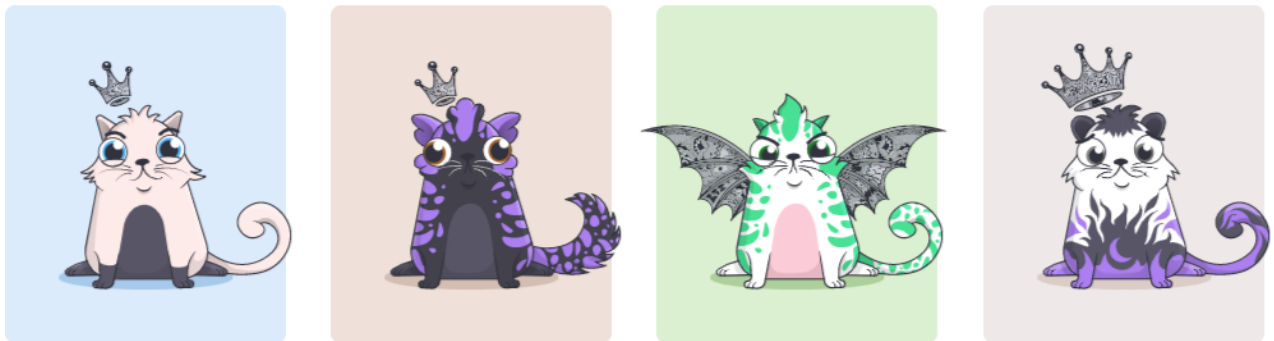
Non-fongible = individuel

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

Non-fungible Tokens (NFT)

Definition

Un jeton non-fongible (NFT) est une unité de données unique et non-interchangeable, enregistrée sur un registre distribué.



⇨Représente de manière unique des fichiers (image, vidéo, ...)

⇨Certificat d'Authenticité : la propriété prouvée & vérifiée

⚠Copies ne sont pas restreintes au possesseur du NFT
(peuvent être copiées et partagées comme tout autre fichier)

Everydays

Everydays: the First 5000 Days = Œuvre digitale créée par Beeple

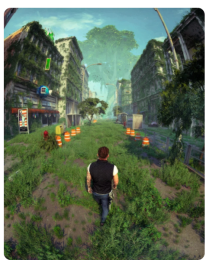
- Collage de 5427 images digitales créées par M. Winkelmann pour sa série Everydays
- Le NFT associé vendu pour 69.3 millions via Christie's en 2021

Everydays: the First 5000 Days, detail, *Happy Birthday*, Beeple, ©beeple-crap.com

Everydays: the First 5000 Days, detail, *Shitshow*, Beeple, ©beeple-crap.com

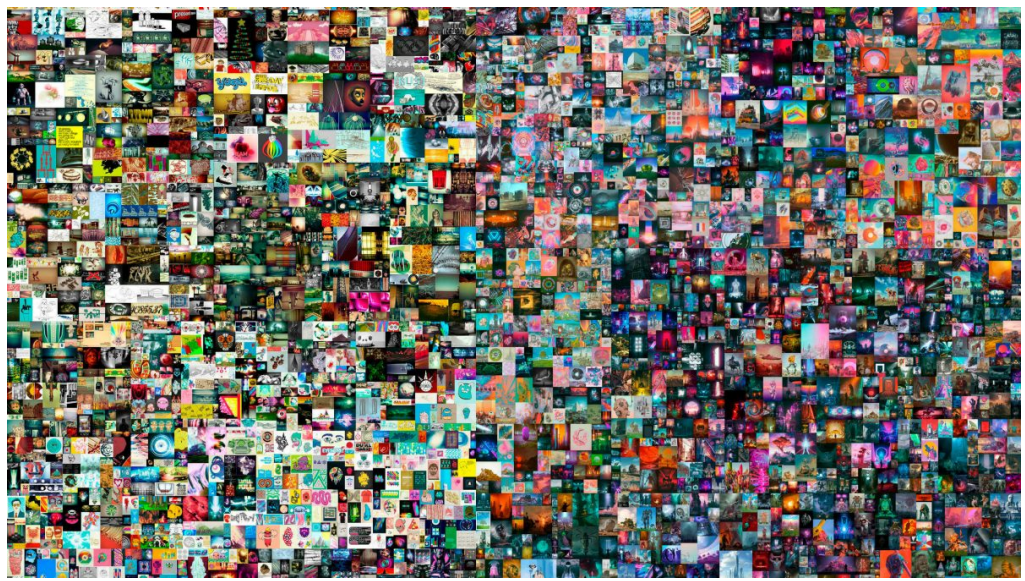
Everydays: the First 5000 Days, detail, *Jong*, Beeple, ©beeple-crap.com

Everydays: the First 5000 Days, detail, *Carefree Goat*, Beeple, ©beeple-crap.com



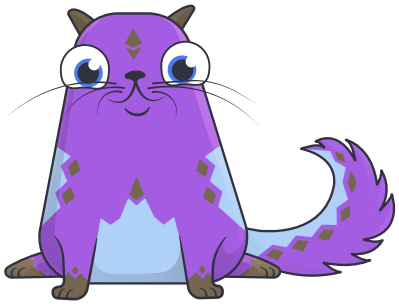
Everydays: the First 5000 Days, detail, *Natural Reboot*, Beeple, ©beeple-crap.com

Everydays: the First 5000 Days, detail, *Worst Case*, Beeple, ©beeple-crap.com



CryptoKitties www.cryptokitties.co

#1353978 (Gén. 15) :



#1812662 (Gén. 4) :

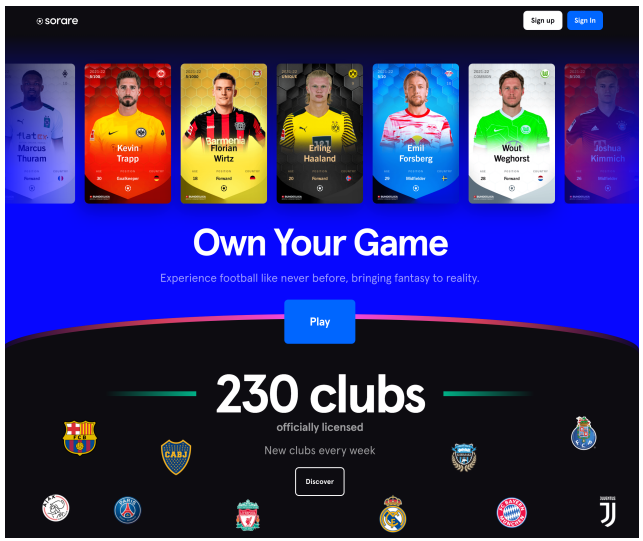
#2011210 : (Gén. 16)

- Projet démarré en 2017 par Axiom Zen
  - Créatures uniques pouvant être échangées, collectionnées, avec reproduction (gérée par contrat intelligent) !
  - Ensemble de 512 bits :
    - 256 bits de gènes (couleur, yeux, queue, etc.) dominant ou récessifs
    - 256 bits pour la date de naissance, l'identité des parents, une information de fertilité
  - Une blockchain est requise pour le NFT associé :
    - Certifie la propriété du Cryptokitty
    - Contrôle l'évolution du génôme (création, reproduction, vente, etc.)
  - Génération d'image associée par une application "off-chain"

NFT in Card Games and Sport

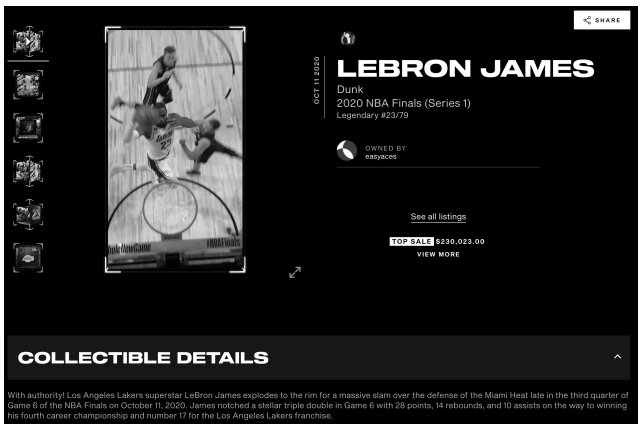
Sorare (Panini like)

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



NBA Top Shot

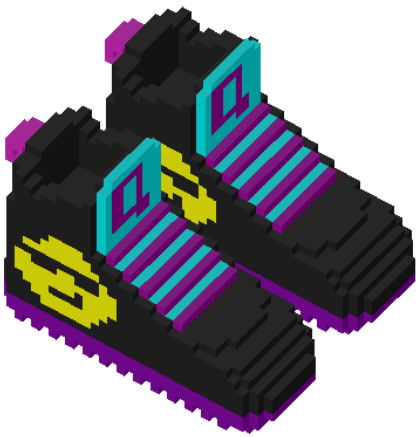
- Blockchain Flow
- "Moments" vidéo (dunk, block etc.) distribués par la NBA



NFT dans la mode et les paris

Sneakers virtuels :

Cryptokickers



Garderobe dans le Métavers :

The Fabricant

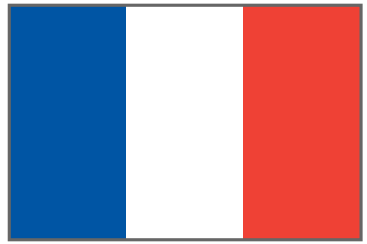
Casino virtuel géré par une DAO :

Monkey Bet

Courses de chevaux virtuels :

Atized.Run

Réglementation en France



La loi PACTE mai 2019

Définition d'un actif numérique :

Toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement.

- Taxe de 30%

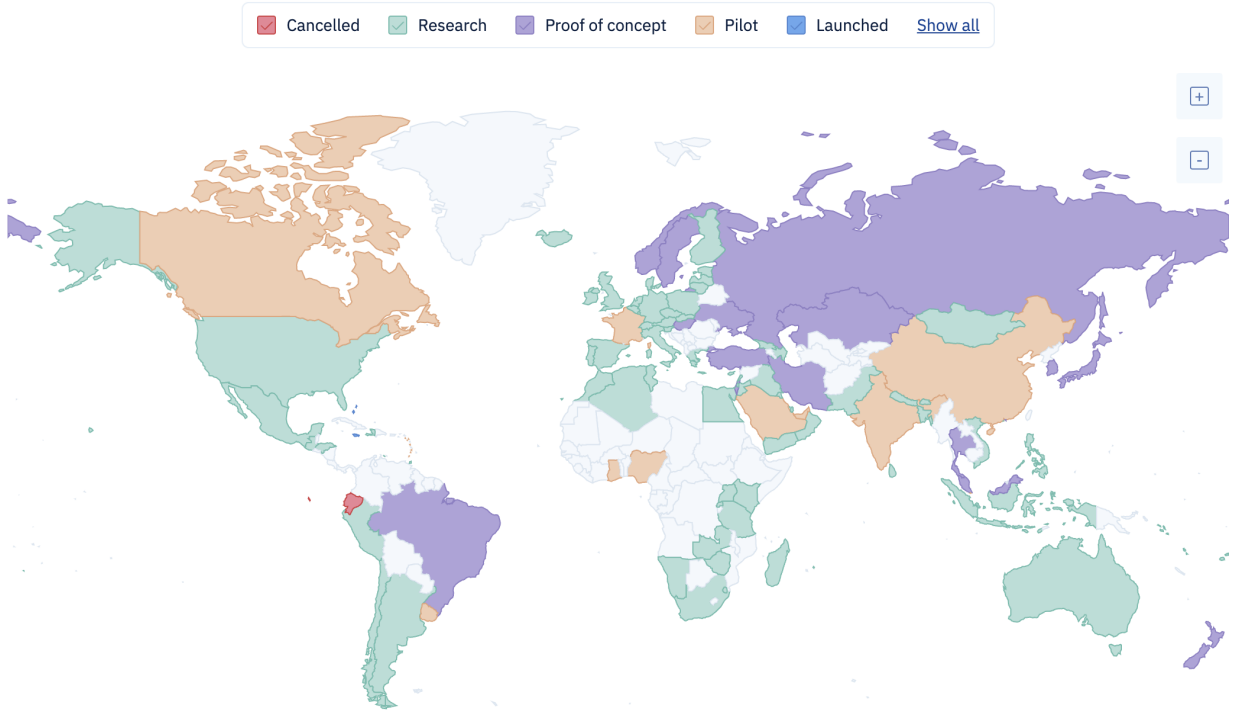
Réglementation en Europe

La **loi MiCAR**

Définition des actifs cryptographiques :

Représentation numérique de la valeur ou des droits qui peuvent être transmis et stockés électroniquement à l'aide d'une technologie de registre distribué ou similaire.

CBDC : Central Bank Digital Currencies



https://cbdctracker.org

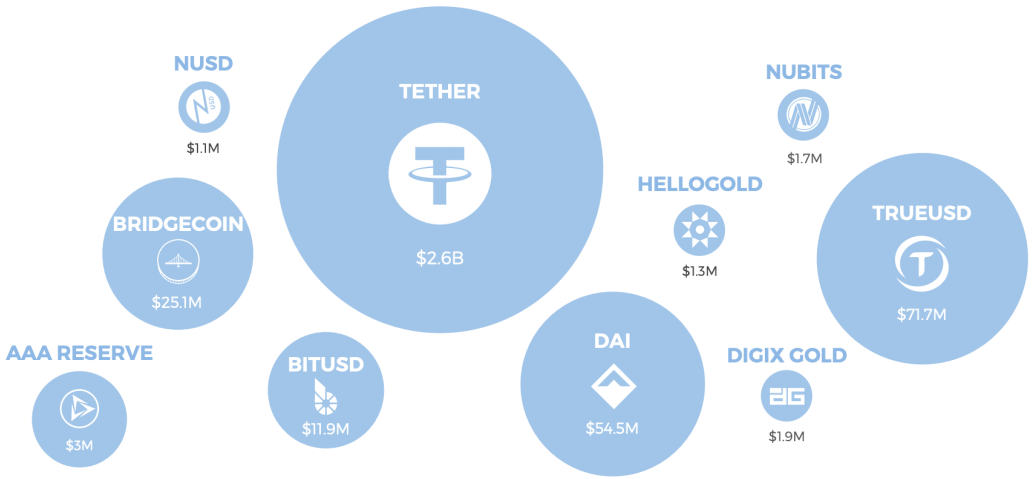
- CBDC ne sont pas des crypto-monnaies !
- Utilisent la technologie Blockchain !

Chine : e-CNY, Europe : EUROChaîne, Amérique : FEDCoin

Stable Coins

Éviter la volatilité avec les avantages de la blockchain !

- 1 USDT, 1 USDC ou 1 BUSD valent tous 1 dollar.
- 1 EURT vaut 1 euro.



Techniquement

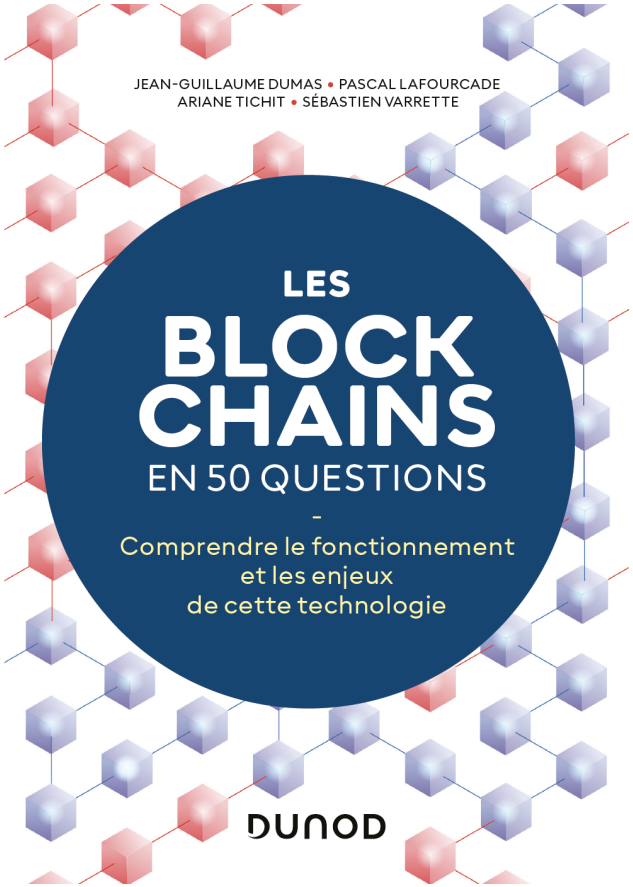
- Jetons classiques (ERC-20)
- Exemple : Tether

3 Choses à retenir

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

Merci pour votre attention

Questions ?



pascal.lafourcade@uca.fr