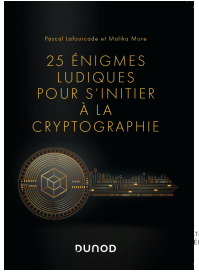
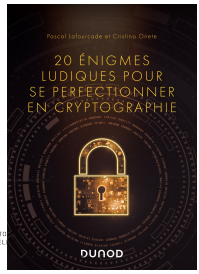

JEAN-GUILLAUME DUMAS • PASCAL LAFOURCADE
ARIANE TICHIT • SÉBASTIEN VARRETTE
LES
BLOCK CHAINS
EN 50 QUESTIONS
Comprendre le fonctionnement et les enjeux de cette technologie
DUNOD


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


Pascal Lafourcade et Malika More
25 ÉNIGMES LUDIQUES POUR S'INITIER À LA CRYPTOGRAPHIE
DUNOD


Pascal Lafourcade et Cristina Onete
20 ÉNIGMES LUDIQUES POUR SE PERFECTIONNER EN CRYPTOGRAPHIE
DUNOD


Pascal Lafourcade et Malika More
15 ÉNIGMES LUDIQUES POUR S'INITIER À LA PROGRAMMATION PYTHON
DUNOD


Pascal Lafourcade, Guesnelle De Julis et Malika More
15 ÉNIGMES LUDIQUES POUR SE PERFECTIONNER EN PROGRAMMATION PYTHON
DUNOD

Bitcoin et la Blockchain

Pascal Lafourcade

LIMOS

UNIVERSITÉ Clermont Auvergne

3A BUT, 9 septembre 2024

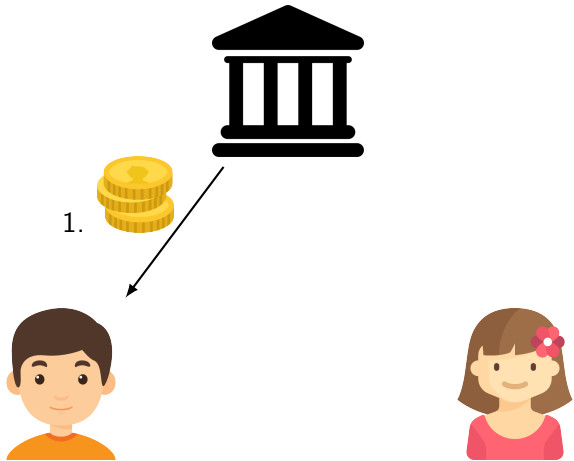
Sumériens vers 3.500 av J.C

Qu'est-ce que la monnaie?

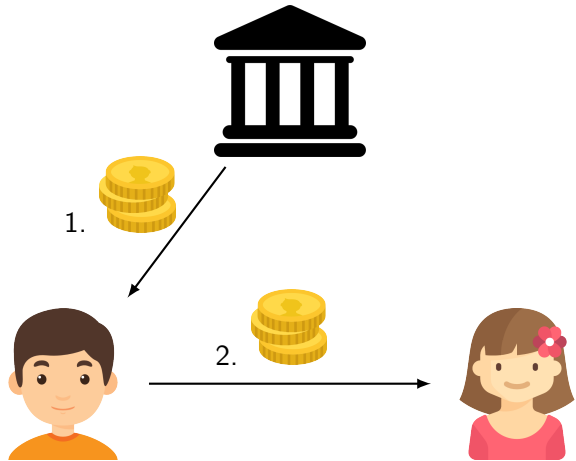
- Intermédiaire et moyens d'échanges de biens et services entre les individus
- Réserve de valeur
- Unité de compte

Nombreuses monnaies

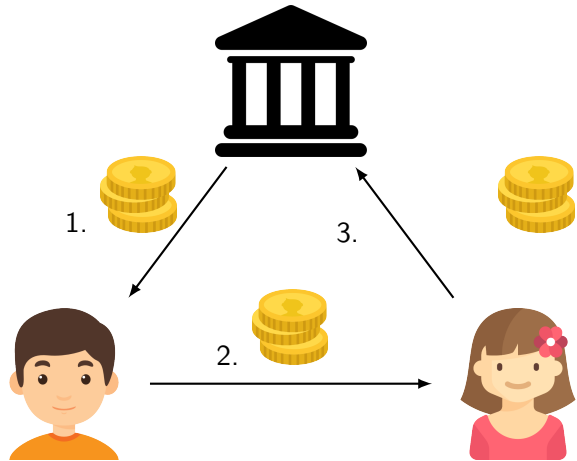
Principe : Banque centrale



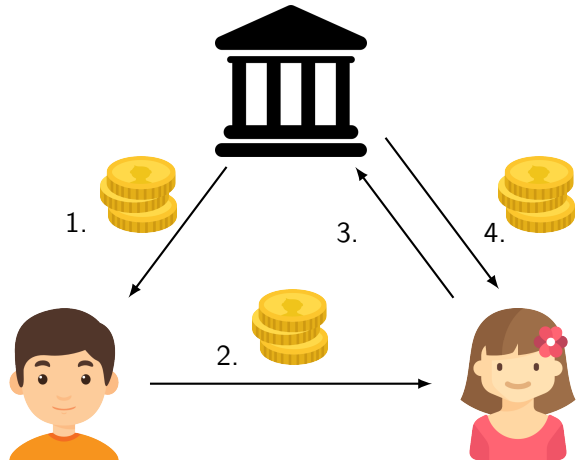
Principe : Banque centrale



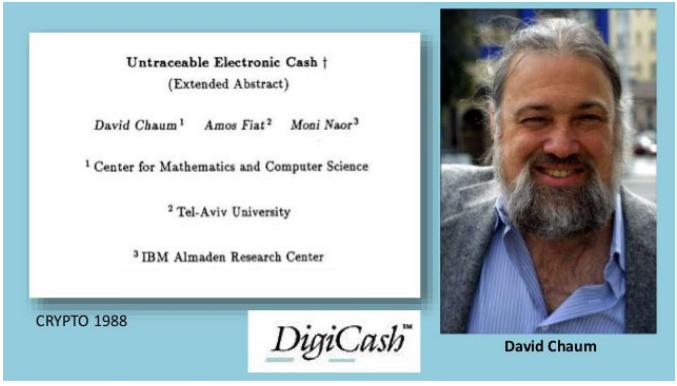
Principe : Banque centrale



Principe : Banque centrale



1988 : Digitcash

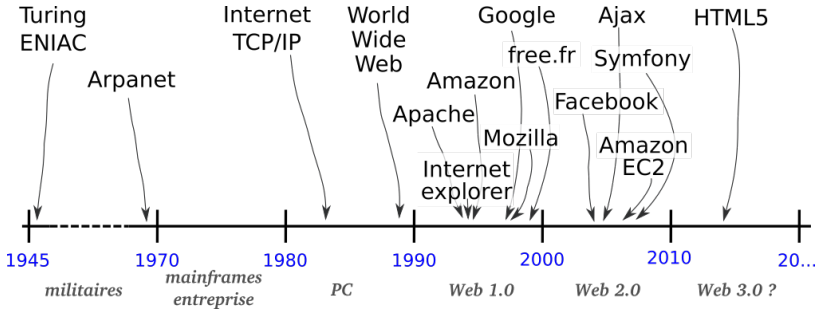


☺ Préserve la vie privée

😐 À l'aide de primitives cryptographiques

☹ Nécessite toujours un tiers (banque)

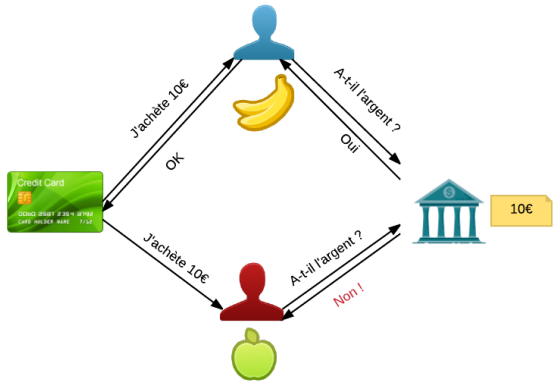
Une idée visionnaire en avance sur son temps



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

Propriétés : Non-Falsifiable (Unforgeable)

Propriétés : Eviter la double dépense

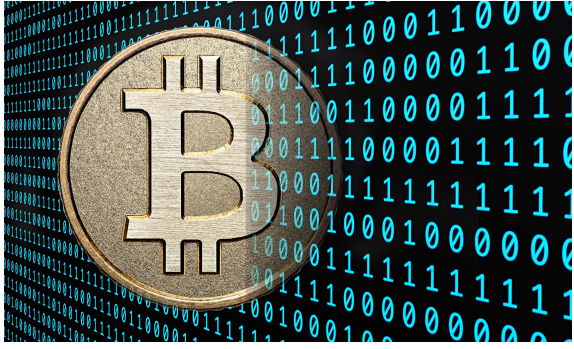


- identifiation fraudeur
- "présemption d'innocence"

Propriétés : Respect de la vie privée

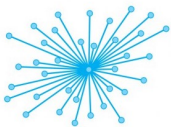
- Anonymat faible : non identification d'un acheteur
- Anonymat fort : non traçabilité d'un acheteur

La révolution Bitcoin 2009

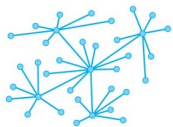


Bitcoin

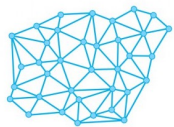
- Cryto-monnaie décentralisée et distribuée



Système centralisé



Système décentralisé

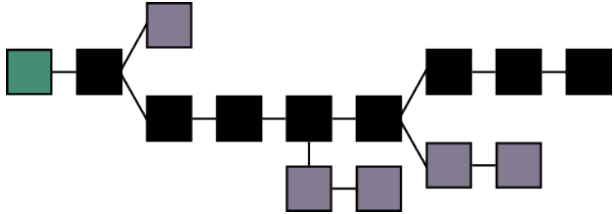


Système distribué

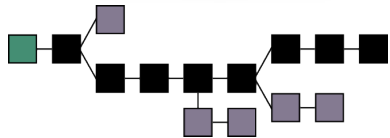
21 millions BTC

Inarrêtable car distribuée

Infalsifiable



Auditable



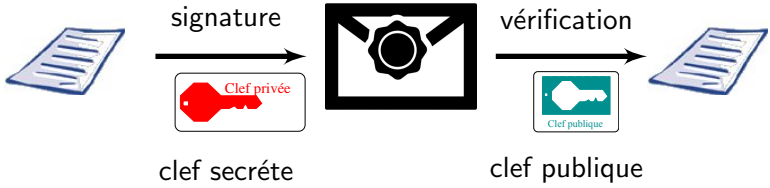
Bitcoin : monnaie électronique

Créée en 2008 par Satoshi Nakamoto

1 BTC $\approx$ 81 03023 euros € le 4 mars 2025

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	

Signature



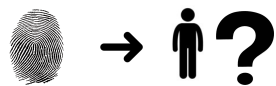
RSA: $m^d \mod n$

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

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

Propriétés de résistance

- Pré-image



- Seconde Pré-image

- Collision

Bitcoins : caractéristiques

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

  21 millions BTC

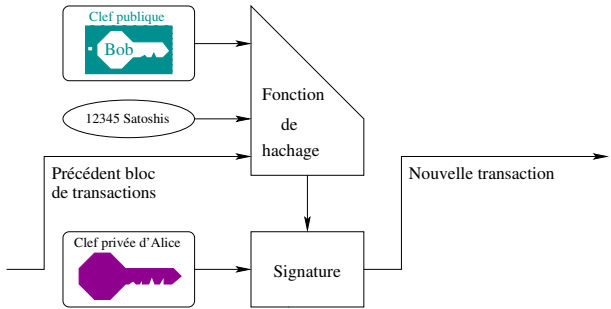
- Les transactions utilisent des **PKI**
- Numéro de compte :

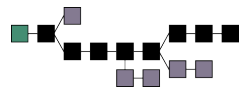
  $$\text{RIPEMD-160}(\text{SHA-256}(\text{ECDSA}_{pub}))$$

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

Comment faire une transaction?

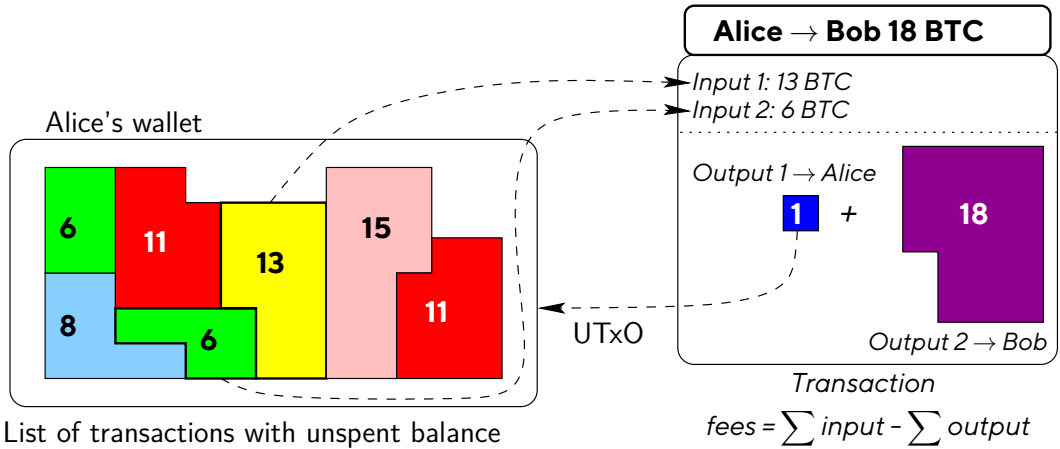
Alice donne 12345 Satochis ($\approx 5c$) à Bob.





Unspent Transaction Output UTXO

Pay 18 BTC with coins



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

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

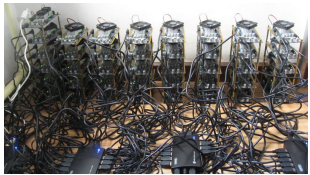
LIMOS LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

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

Miner : Objectif de hachage

Cible pour le block 816 377 (Février 2024)
0000000000000000000481940000000000000000000000000000000000000000

Trouver une nombre n tel que

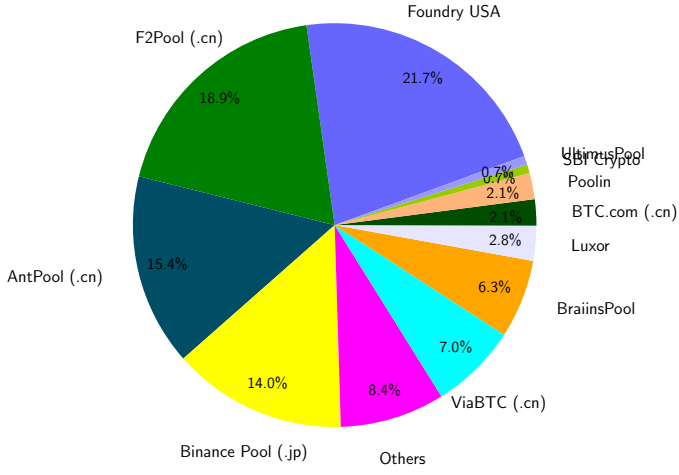
$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, n)) = x < \textit{Cible}$$

Avoir au moins 18 zéros au début de x

Stratégie : brute force

Tester toutes les valeurs possibles de n

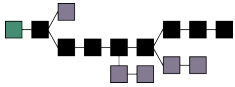
Fermes de mineurs: partagent les récompenses



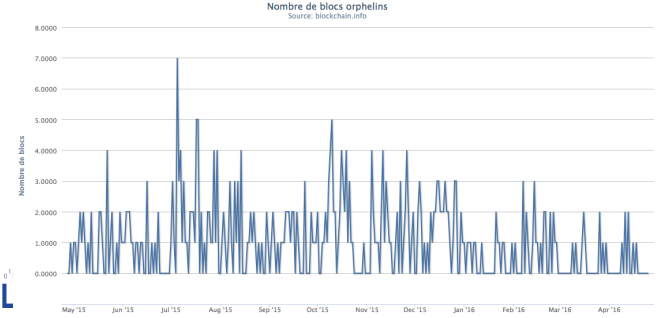
Miner = Validation des transactions

Cible: 0000000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076

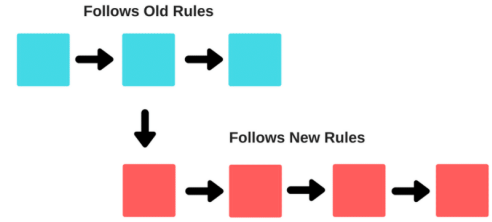
Re-évaluée tous les blocs à partir des 2016 blocs passéss



- La chaîne la plus longue persiste (attaque 51 %)
- Validation toutes les 10 minutes (6 confirmations)



Soft Fork

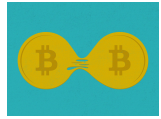


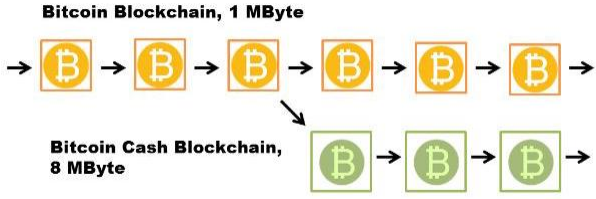
The primary difference between a soft fork and hard fork is that it is not backward compatible

Modification du code :

- Correction de bugs
- Améliorations consensuelles

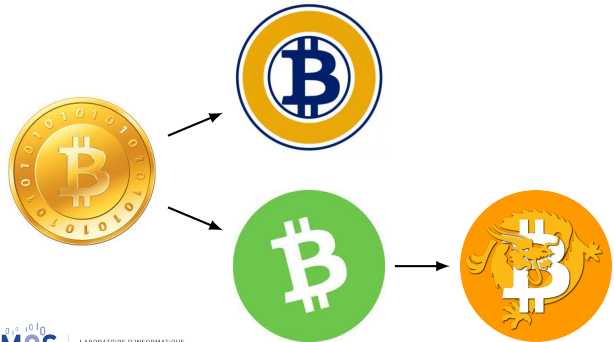
Hard Fork




Bitcoin Blockchain, 1 MByte
Bitcoin Cash Blockchain,
8 MByte

Hard Fork History

- Bitcoin Cash for Bitcoin (1 August 2017 at block 478558)
- Bitcoin Gold for Bitcoin (24 October 2017 at block 491407)
- Bitcoin SV (Satoshi Version) for Bitcoin Cash (15 November 2018 at block 556766)



Traçable

Traçable

MONERO

ZCASH

Snark

Limitations

10 minutes = 1 block

Taille des transactions 1 Mo

Limitations

10 minutes = 1 block

Taille des transactions 1 Mo

Lightning Network

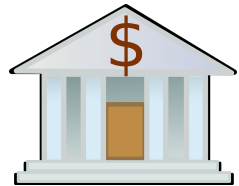
12 secondes

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

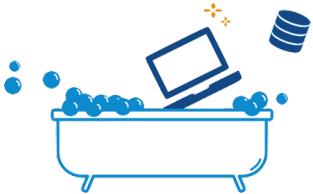
Energivore

Proof of Stake
Lightning Network

Qui s'approprie ces nouvelles monnnaies ?



Freins



Bitcoin : Crypto-monnaie dématérialisée décentralisée

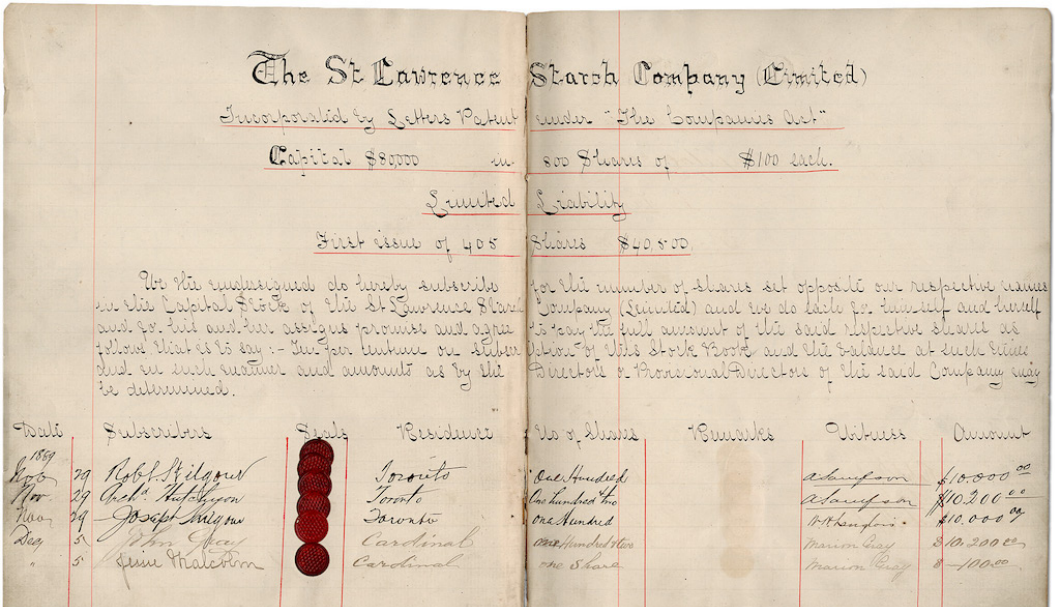
- Preuve de travail = Objectif de Hachage
- Création de la monnaie = récompense aux mineurs
- Miner = difficile + energivore

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



The St Lawrence Starch Company (Limited)

Incorporated by Letters Patent under "The Companies Act"

Capital $80000 in 800 Shares of $100 each.

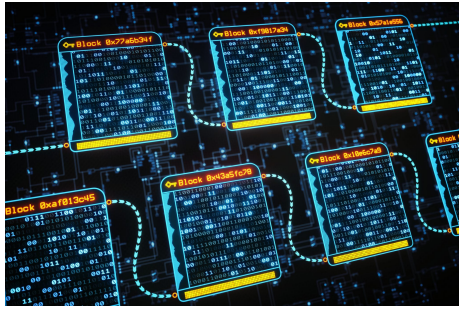
Limited Liability

First issue of 405 Shares $40500

We the undersigned do hereby subscribe for the Capital Stock of the St Lawrence Starch Company for the amounts set opposite our respective names and we do hereby for ourself and ourself severally agree to pay the full amount of the said respective shares as ordered by the Stock Book and the Directors at such times and in such manner and amounts as by the Directors or Provisional Directors of the said Company may be determined.

Date	Subscribers	Seals	Residence	No of Shares	Remarks	Witness	Amount
1859 Nov 29	Robt Kilgour		Toronto	One Hundred		A Langton	$10.000.00
Nov 29	Robt Kilgour		Toronto	One hundred two		A Langton	$10.200.00
Nov 29	Joseph Kilgour		Toronto	One Hundred		A Langton	$10.000.00
Dec 5	Wm Gray		Cardinal	One Hundred three		Marion Gray	$10.200.00
" 5	Jesse Malcolm		Cardinal	one Share		Marion Gray	$ 100.00

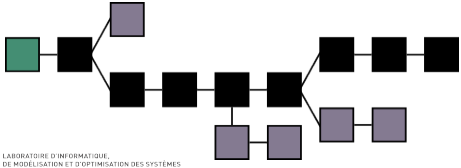
Blockchain



Registre distribué, sécurisé, infalsifiable

Mineurs valident des transactions

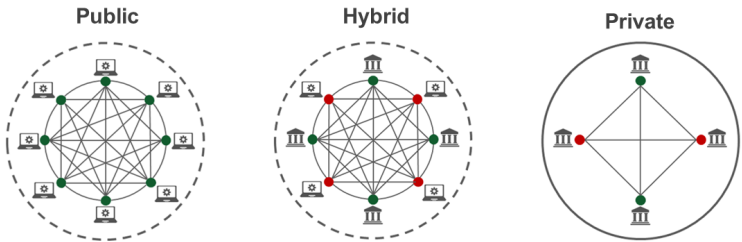
Tiennent à jour le registre distribué



Inarrêtable, Infalsifiable, Auditable

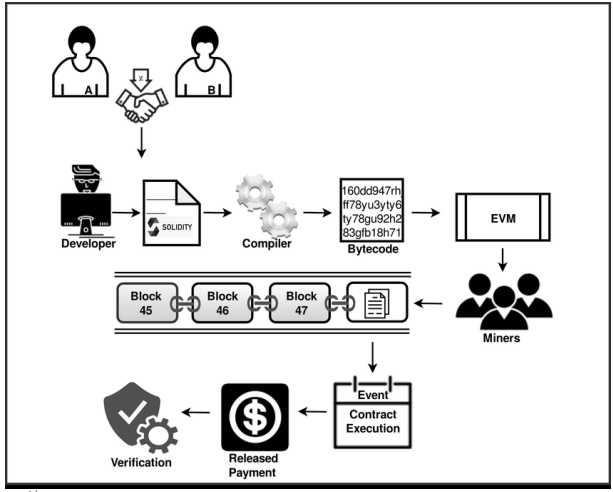
Décision des mineurs

Blockchain Privée vs Publique

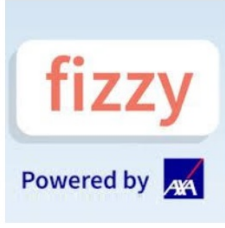


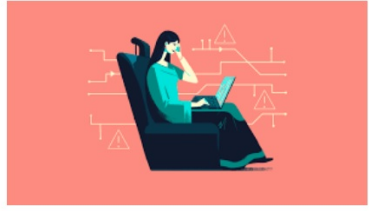
EcoMobiCoin: Proof of Behavior

Smart Contract

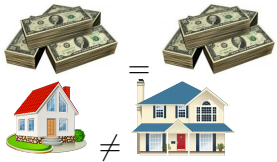


Smart Contract

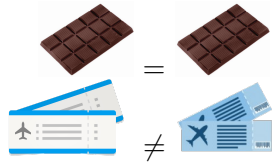




Fungible vs Non-fungible Tokens



Fongible = interchangeable



Non-fongible = individuel

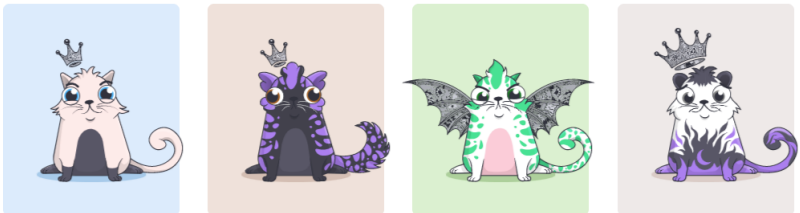
Critère	Fongible	Non-Fongible
Interchangeabilité	interchangeable.	non interchangeable, chacun représentant un unique actif.
Divisibilité	divisible en petites parts	Non divisible
Transfert de valeur	dépend du nombre de jetons possédés.	La valeur de l'actif unique représenté par un NFT

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

Non-fungible Tokens (NFT)

Definition

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



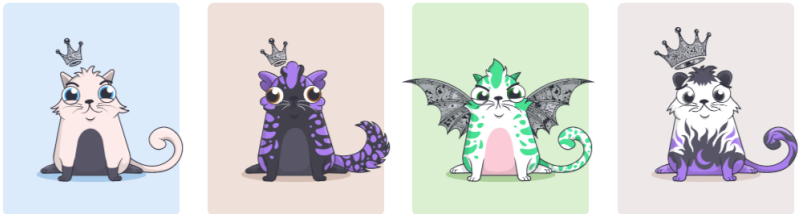
⇨Représente de manière unique des fichiers (image, vidéo, ...)

⇨Certificat d'Authenticité : la propriété prouvée & vérifiée

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)

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

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

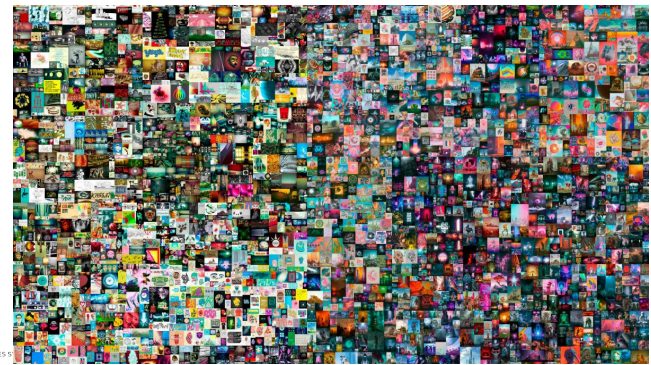
Everydays: the First 5000 Days, detail, *Shitshow*, Beeple, ©beeple-crap.com

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) :

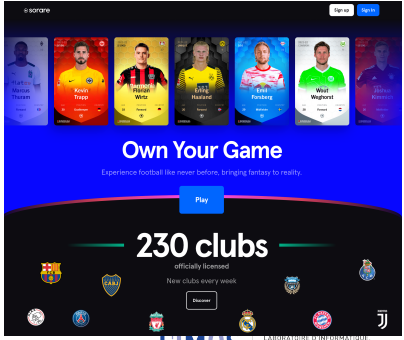
#2011210 : offspring (Gén. 16)

- 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 asocié :
    - 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

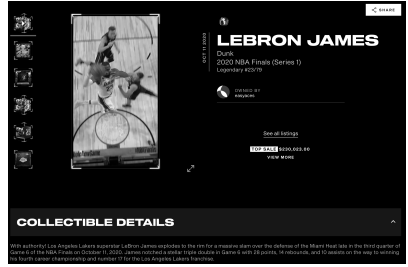
Sorare (Panini like)

- 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

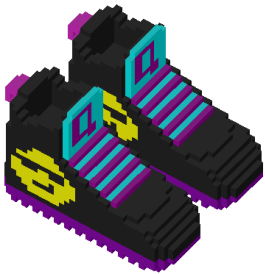


LIMOS
LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

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 :

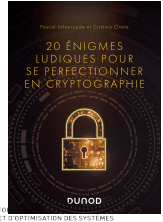
Atized.Run

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 ?



LIMOS
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES