

Bitcoin et la Blockchain

Pascal Lafourcade



Villefranche-sur-Soane
9 octobre 2024

Sumériens vers 3.500 av J.C



Qu'est-ce que la monnaie?

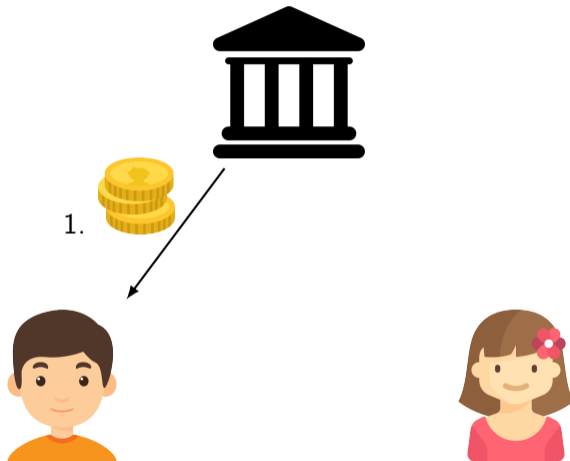


- ▶ Intermédiaire et moyens d'échanges de biens et services entre les individus
- ▶ Réserve de valeur
- ▶ Unité de compte

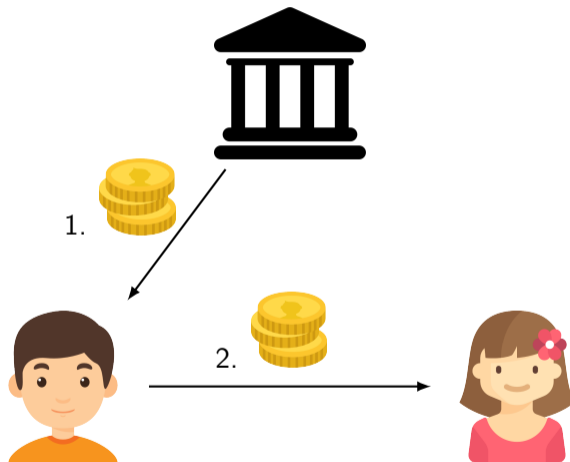
Nombreuses monnaies



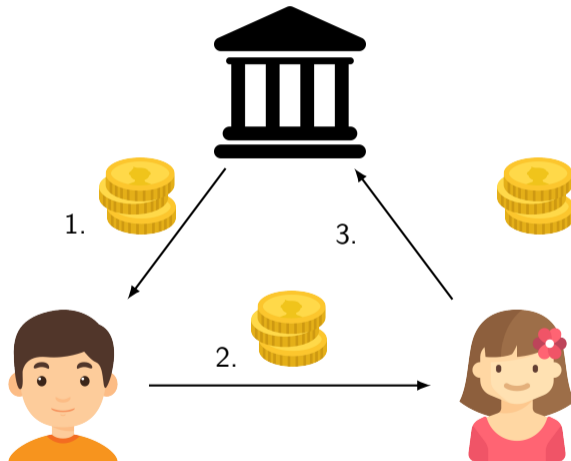
Principe : Banque centrale



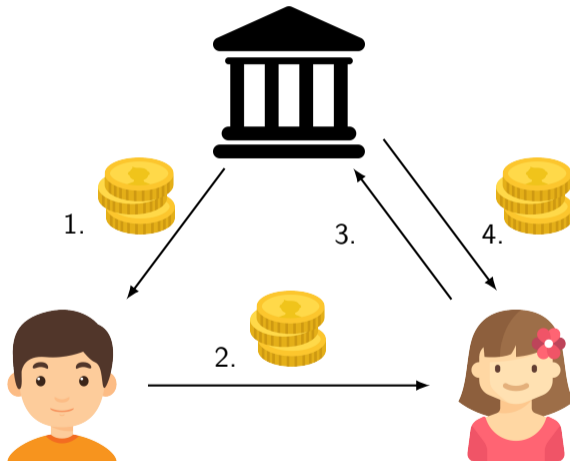
Principe : Banque centrale



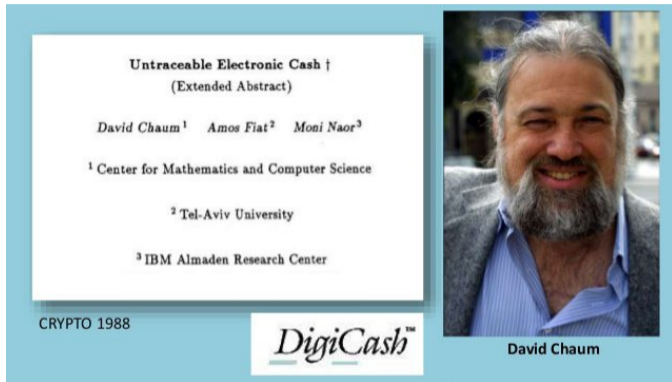
Principe : Banque centrale



Principe : Banque centrale



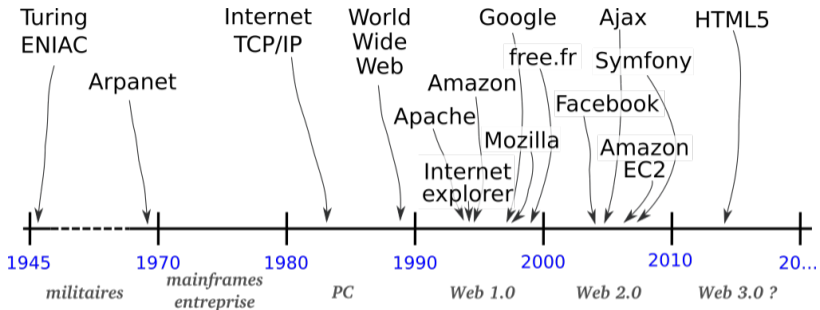
1988 : Digtcash



The image shows the title page of the paper "Untraceable Electronic Cash" and a portrait of David Chaum. The title page is white with black text, featuring the title "Untraceable Electronic Cash † (Extended Abstract)", authors "David Chaum¹ Amos Fiat² Moni Naor³", and affiliations: "¹ Center for Mathematics and Computer Science", "² Tel-Aviv University", and "³ IBM Almaden Research Center". Below the title page is the "CRYPTO 1988" logo and the "DigiCash™" logo. To the right is a color photograph of David Chaum, a man with a grey beard and hair, wearing a blue shirt and a grey jacket, smiling.

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

Une idée visionnaire en avance sur son temps



Crypto-monnaie

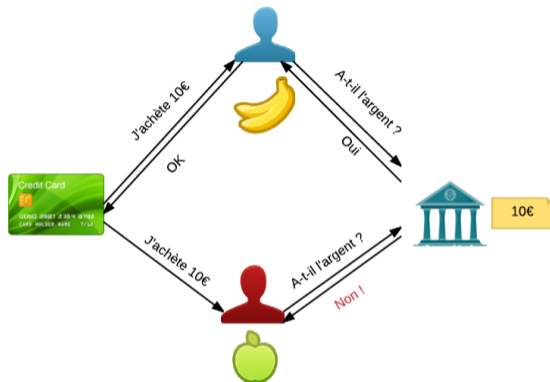
- ▶ Monnaie
 1. Intermédiaire et moyen d'échanges
 2. Réserve de valeur
 3. Unité de compte

- ▶ Crypto-monnaie : monnaie électronique, se passant d'un Tiers
 4. Respect de la vie privée
 5. Non-Falsifiable
 6. Éviter les doubles dépenses

Propriétés : Non-Falsifiable (Unforgeable)



Propriétés : Eviter la double dépense



► identification fraudeur

► “présomption d’innocence”



Propriétés : Respect de la vie privée

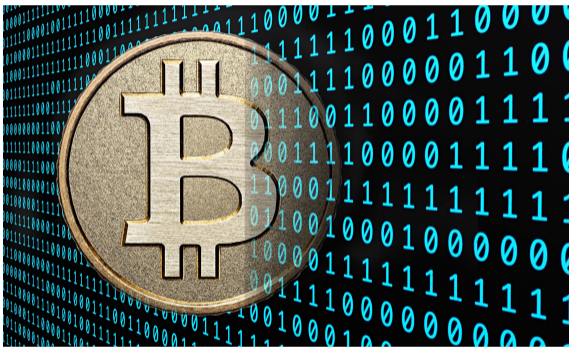
- ▶ Anonymat faible : non identification d'un acheteur
- ▶ Anonymat fort : non traçabilité d'un acheteur



Monnaies classiques et crypto-monnaies

	Monnaie classique		Crypto-monnaie
	Liquide	Électronique	
Moyen d'échange	✓	✓	✓
Réserve de valeur	✓	✓	✓
Unité de compte	✓	✓	✓
Création	Banque centrale	Dette	Automatique
Vie privée	✓	✗	✓
Pair à pair	✗	✗	✓
Garantie légale, stabilisation	✓	✓	✗

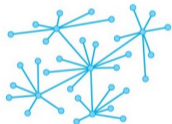
La révolution Bitcoin 2009



► Crypto-monnaie décentralisée et distribuée



Système centralisé



Système décentralisé



Système distribué

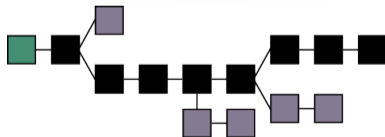


21 millions BTC

Inarrêtable car distribuée



Auditable



Bitcoin : monnaie électronique

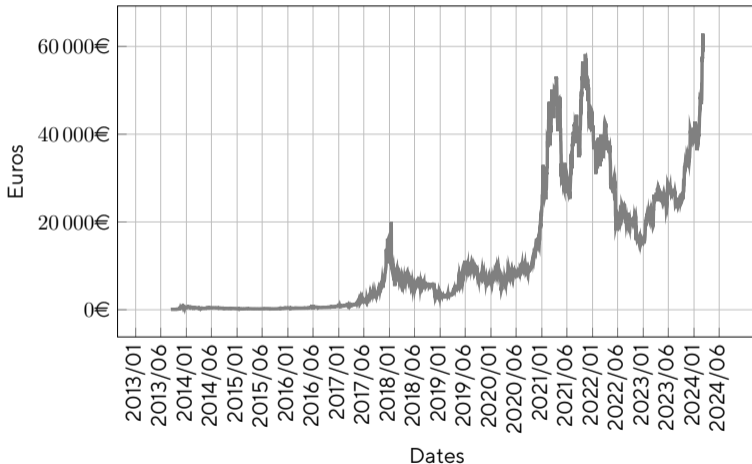
Créée en 2008 par Satoshi Nakamoto

1 BTC \approx 23 410,62 € le 15 mars 2023

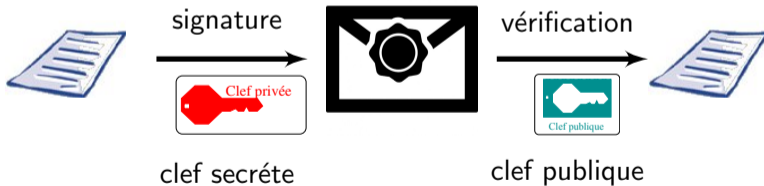


1	BTC = 1 Bitcoin	
0,01	BTC = 1 cBTC	= 1 centiBitcoin (ou bitcent)
0,001	BTC = 1 mBTC	= 1 milliBitcoin
0,000 001	BTC = 1 μ BTC	= 1 microBitcoin
0,000 000 000 000 001	BTC = 1 Satoshi	

Taux de change du bitcoin 2024



Signature



RSA: $m^d \bmod n$



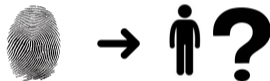
LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

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

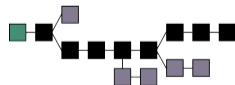
- ▶ Les transactions utilisent des **PKI**

- ▶ Numéro de compte :

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

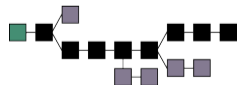
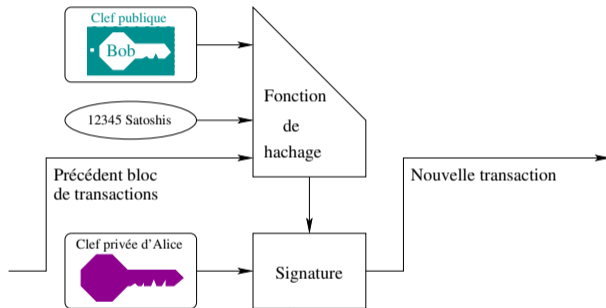
- ▶ Toutes les transactions sont **publiques**

- ▶ **Blockchain** : un système pair-à-pair qui garantit la validité des transactions



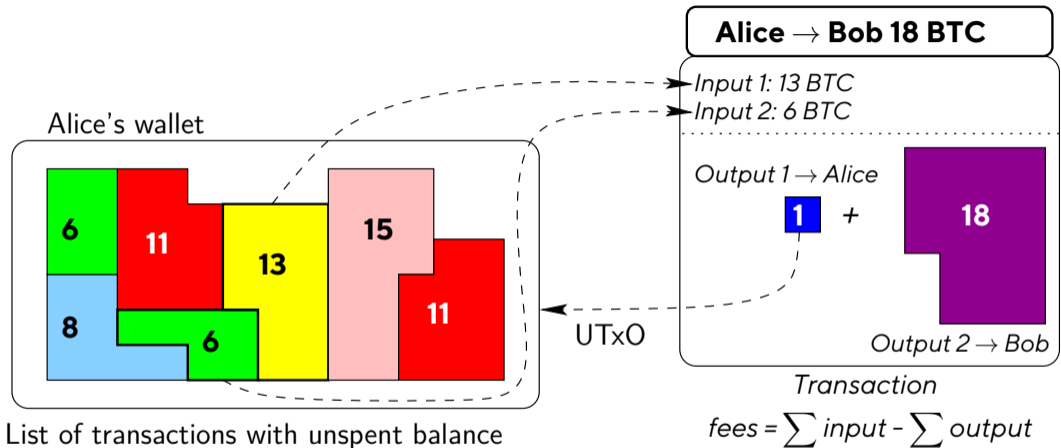
Comment faire une transaction?

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

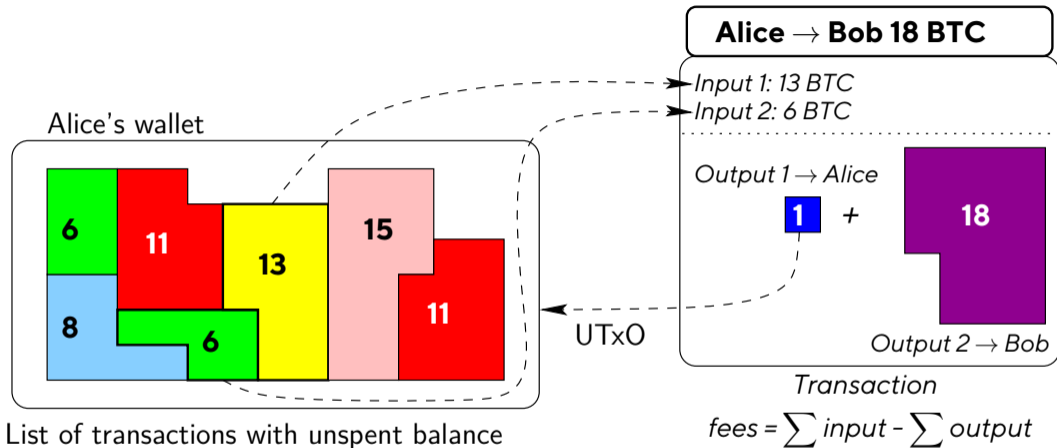


Unspent Transaction Output UTXO

Pay 18 BTC with coins



Pay 18 BTC with coins



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

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

Miner des Bitcoins



Miner des Bitcoins



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



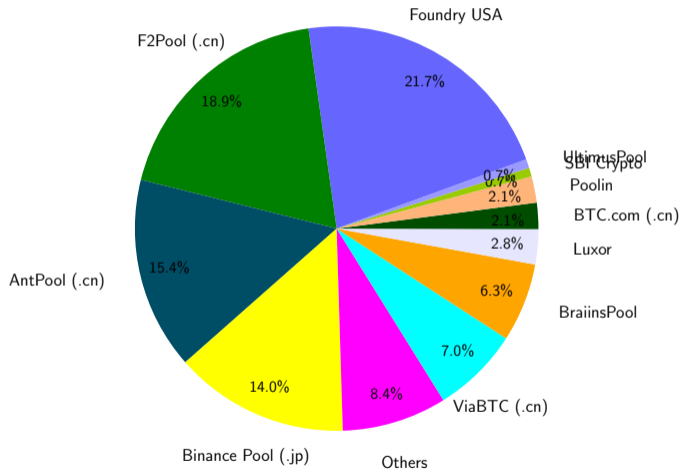
Miner des Bitcoins

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

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



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

LIMOS

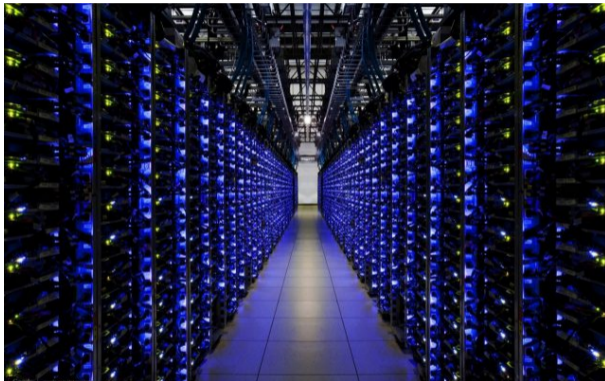
LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES



ETHEREUM

12 secondes

Energivore



Proof of Stake
Lightning Network

LIMOS

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

Passage à l'échelle ?

- ▶ Bitcoin 3-4 transactions / seconde
- ▶ Ethereum 15 transactions / seconde
- ▶ VISA 65 000 transactions / seconde

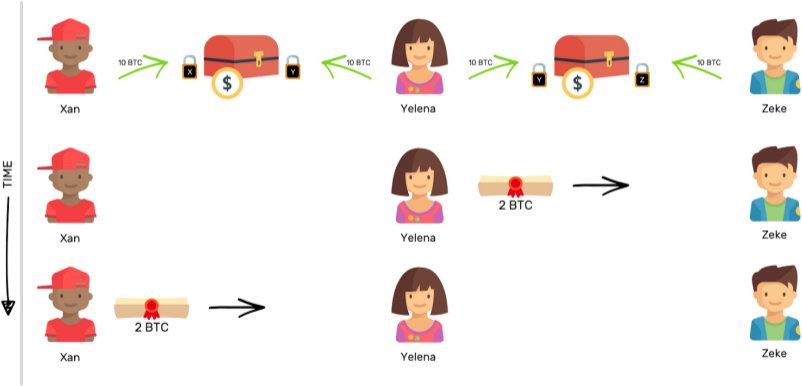
Passage à l'échelle ?

- ▶ Bitcoin 3-4 transactions / seconde
- ▶ Ethereum 15 transactions / seconde
- ▶ VISA 65 000 transactions / seconde

Solutions :

- ▶ Augementer la taille des blocs
- ▶ Diminuer le temps entre blocs
- ▶ Réduire le nombre de transactions sur la chaîne

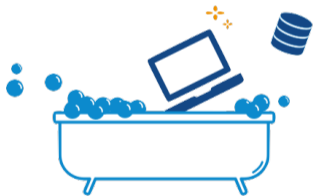
State Channel : Lightning Network



Qui s'approprie ces nouvelles monnaies ?



Freins



Bitcoin : Crypto-monnaie dématérialisée décentralisée

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



Bitcoin : Crypto-monnaie dématérialisée décentralisée

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



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



The St Lawrence Starch Company (Limited)

Incorporated by Letters Patent under "The Companies Act"

Capital \$80000 in 800 Shares of \$100 each.

Liability

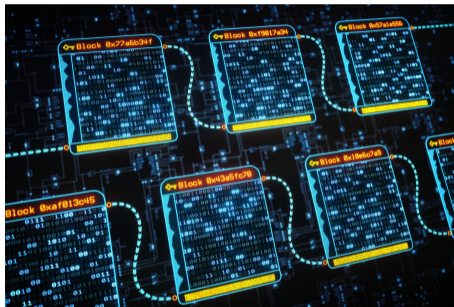
First issue of 405 Shares \$40,500.

We the undersigned do hereby subscribe in the Capital Stock of the St Lawrence Starch and Co. Ltd and our assigns promise and agree to pay the full amount of the said respective shares as shown in this Book and the balance at such time and in such manner and amount as by the Directors or Provisional Directors of the said Company may be determined.

for the number of shares set opposite our respective names in this Book and we do each for himself and himself to pay the full amount of the said respective shares as shown in this Book and the balance at such time and in such manner and amount as by the Directors or Provisional Directors of the said Company may be determined.

Date	Subscribers	Shares	Residence	No of Shares	Remarks	Witness	Amount
1859 Apr 29	Robt. Kilgour		Toronto	One Hundred		Adams	\$10,000 ⁰⁰
Apr 29	Chas. Hutchison		Toronto	One Hundred		Adams	\$10,200 ⁰⁰
May 29	Joseph Milne		Toronto	One Hundred		H. H. Hamilton	\$10,000 ⁰⁰
May 5	John Gray		Cardinal	One Hundred		Marion Gray	\$10,200 ⁰⁰
" 5	James Macleod		Cardinal	One Share		Marion Gray	\$-100 ⁰⁰

Blockchain

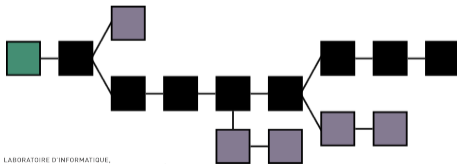


Registre distribué, sécurisé, infalsifiable

Mineurs valident des transactions



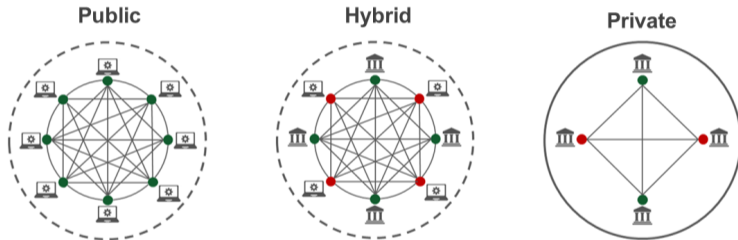
Tiennent à jour le registre distribué



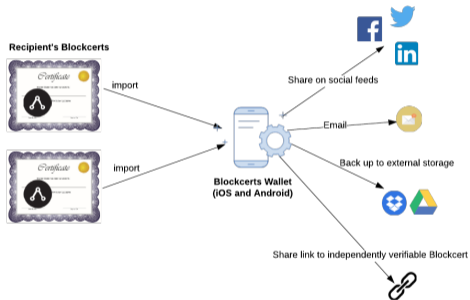
Décision des mineurs



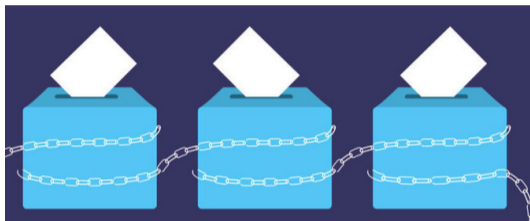
Blockchain Privée vs Publique



Blockchain Application : MIT Diploma



Blockchain Applications : Verify Your Vote, DABSTERS



Properties

Universal Verifiability, Individual Verifiability, Privacy, Receipt-Freeness, Prevent Double Vote, Vote and Go, ...

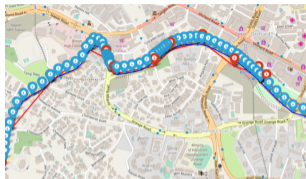
Blockchain Applications : Auction



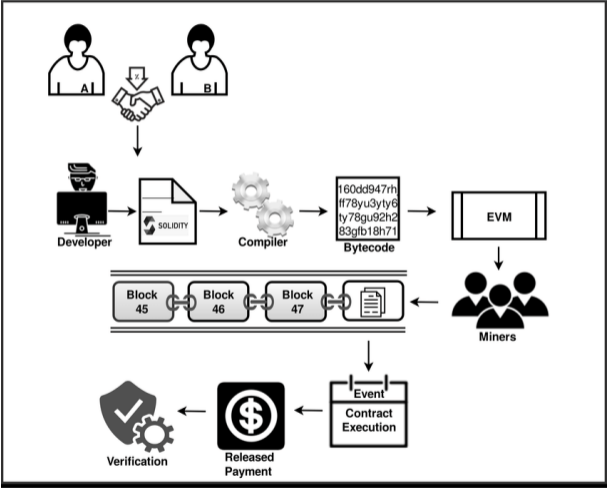
Properties

Universal Verifiability, Individual Verifiability, Privacy, Receipt-Freeness, Prevent Double Spending, Non-Repudiation ...

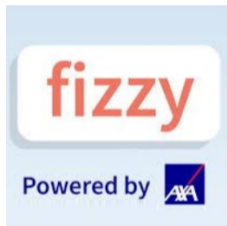
EcoMobiCoin: Proof of Behavior



Smart Contract

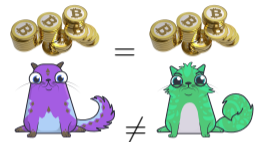
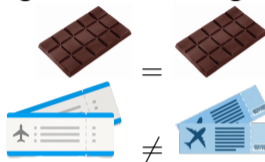
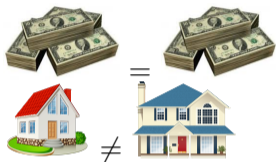


Smart Contract



Fungible vs Non-fungible Tokens

Fongible = interchangeable



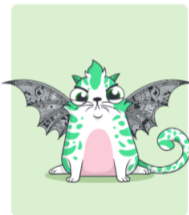
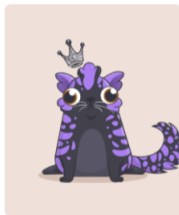
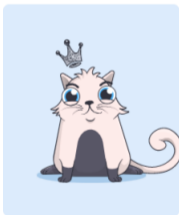
Non-fongible = individuel

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

Non-fungible Tokens (NFT)

Definition

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



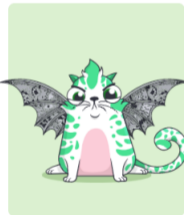
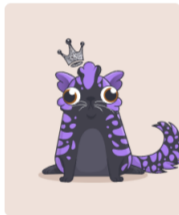
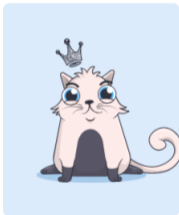
⇒ Représente de manière **unique** des fichiers (image, vidéo, ...)

⇒ **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, ...)

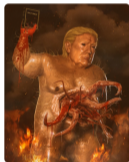
⇒ **Certificat** d'Authenticité : la propriété **prouvée & vérifiée**

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

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, ©beep-crap.com



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



Everydays: the First 5000 Days, detail, Jang, Beeple, ©beep-crap.com



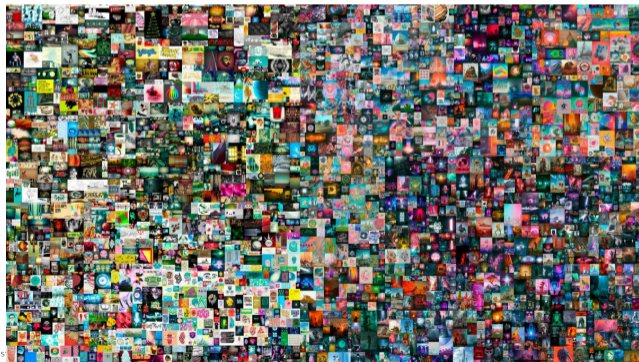
Everydays: the First 5000 Days, detail, Carefree Goat, Beeple, ©beep-crap.com



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



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



JE
HISATION DES S

#1353978 (Gén. 15) :



#1812662 (Gén. 4) :



#2011210 : offspring (Gén. 16)

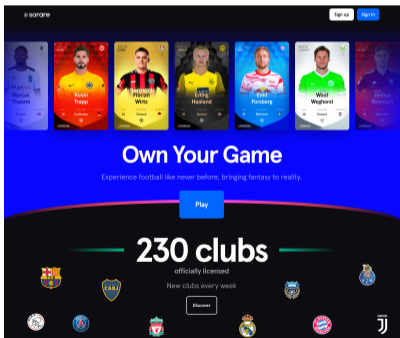


- ▶ Projet démarré en 2017 par Axiom Zen
 - ▶ Créatures uniques pouvant être échangées, collectionnées, avec reproduction (gérée par contrat intelligent) !
 - ▶ Ensemble de 512 bits :
 - ▶ 256 bits de gènes (couleur, yeux, queue, etc.) dominant ou récessifs
 - ▶ 256 bits pour la date de naissance, l'identité des parents, une information de fertilité
 - ▶ Une blockchain est requise pour le NFT 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

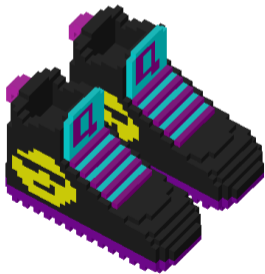
- ▶ Blockchain Flow
- ▶ "Moments" vidéo (dunk, block etc.) distribués par la NBA



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



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 ?

