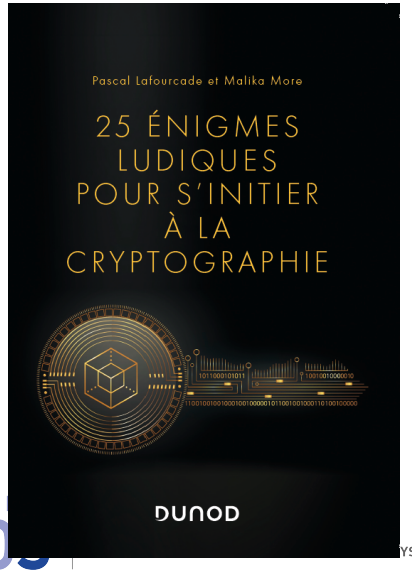
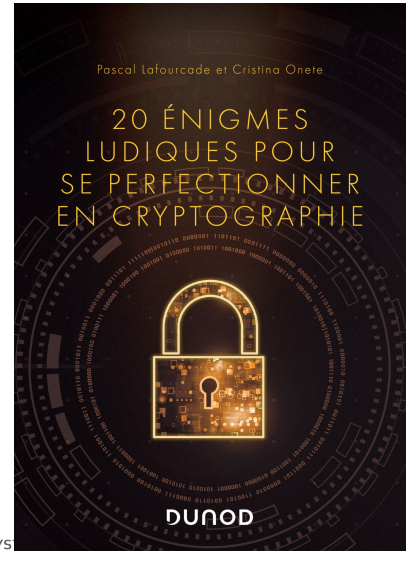

JEAN-GUILLAUME DUMAS • PASCAL LAFOURCADE
ARIANE TICHIT • SÉBASTIEN VARRETTE
LES
BLOCK CHAINS
EN 50 QUESTIONS
Comprendre le fonctionnement et les enjeux de cette technologie
DUNOD


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

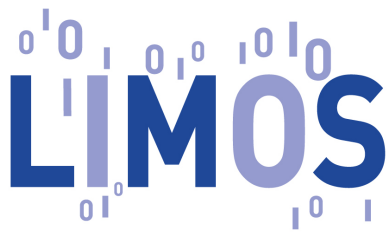

Pascal Lafourcade et Cristina Onete
20 ÉNIGMES LUDIQUES POUR SE PERFECTIONNER EN CRYPTOGRAPHIE
DUNOD


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


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

Bitcoin et la Blockchain

Pascal Lafourcade





La Défense
6 mars 2024

Sumériens vers 3.500 av J.C



Qu'est-ce que la monnaie?





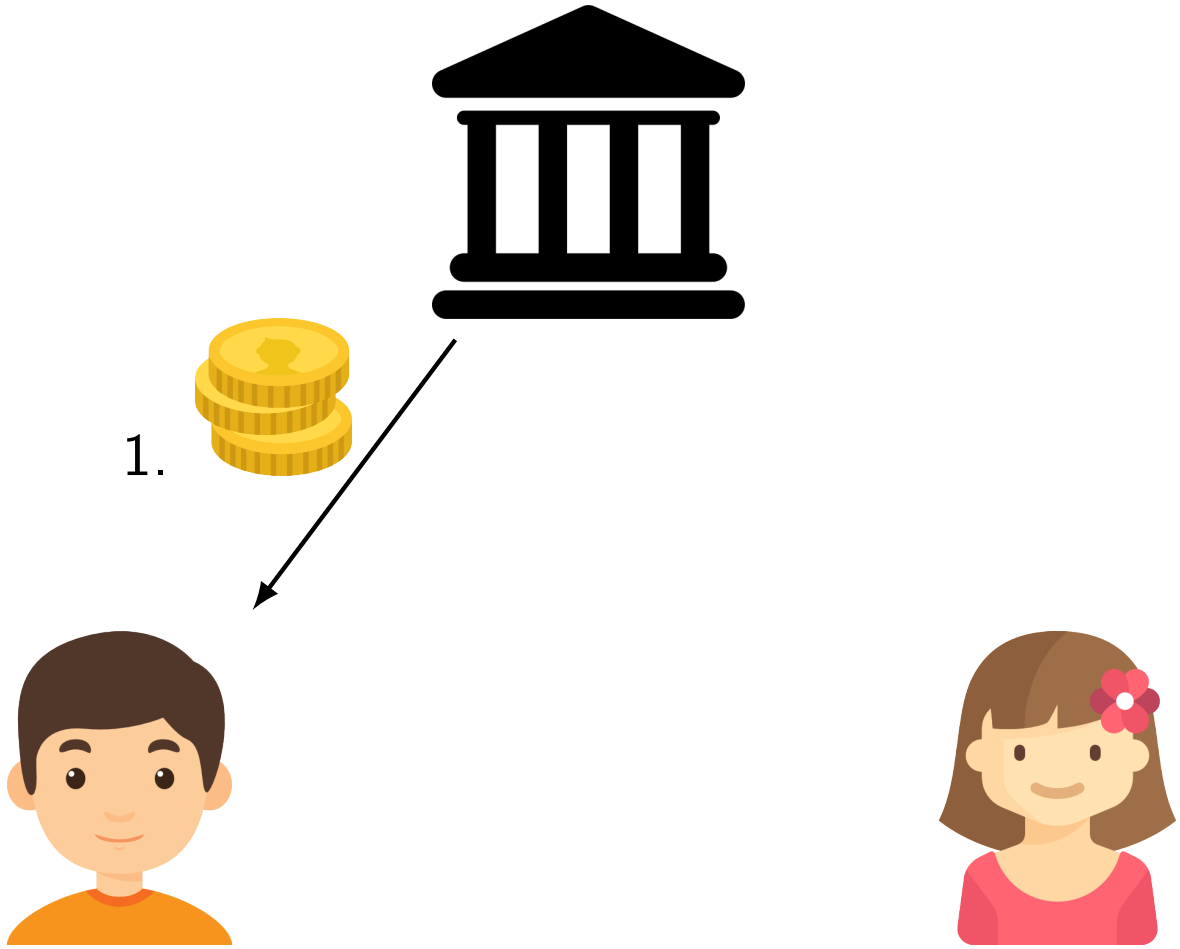


- Intermédiaire et moyens d'échanges de biens et services entre les individus
- Réserve de valeur
- Unité de compte

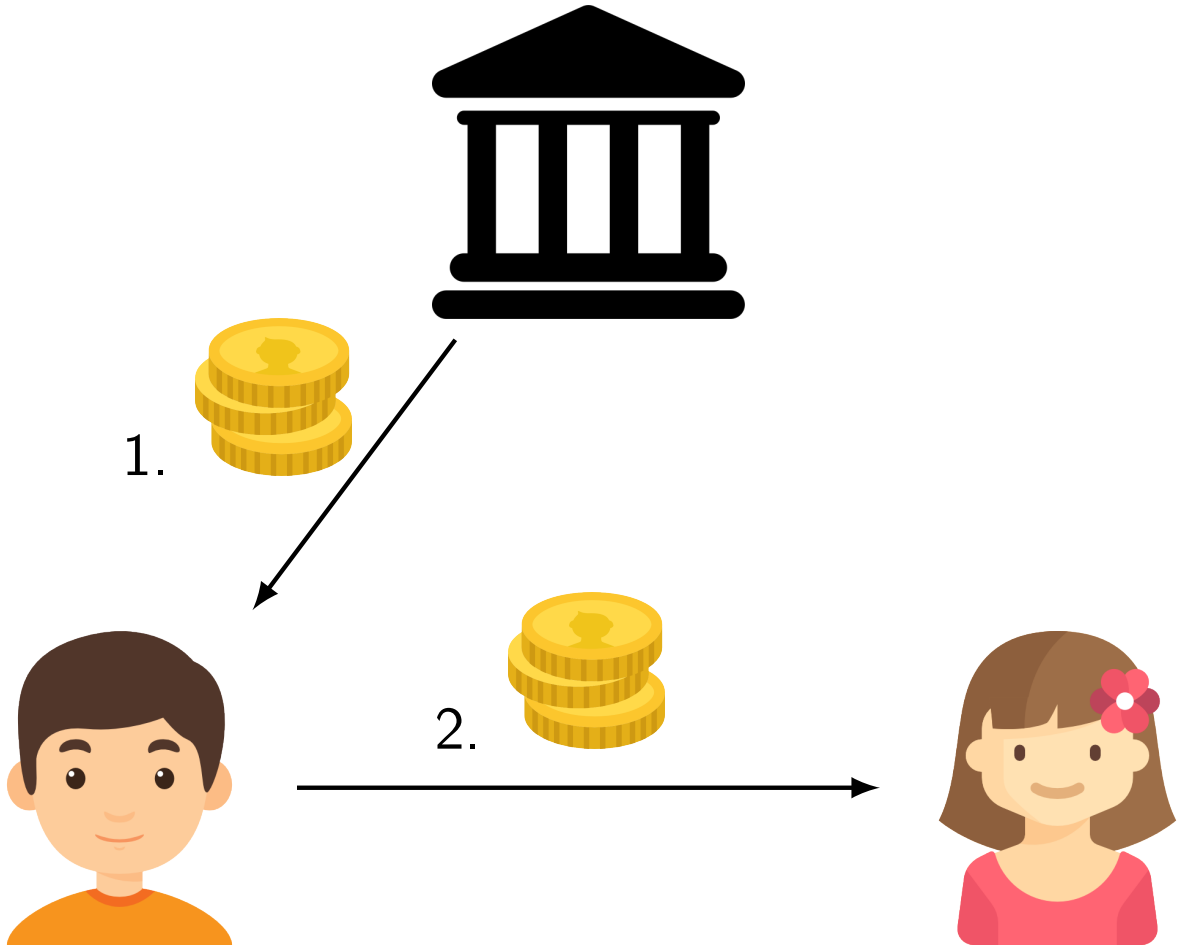
Nombreuses monnaies



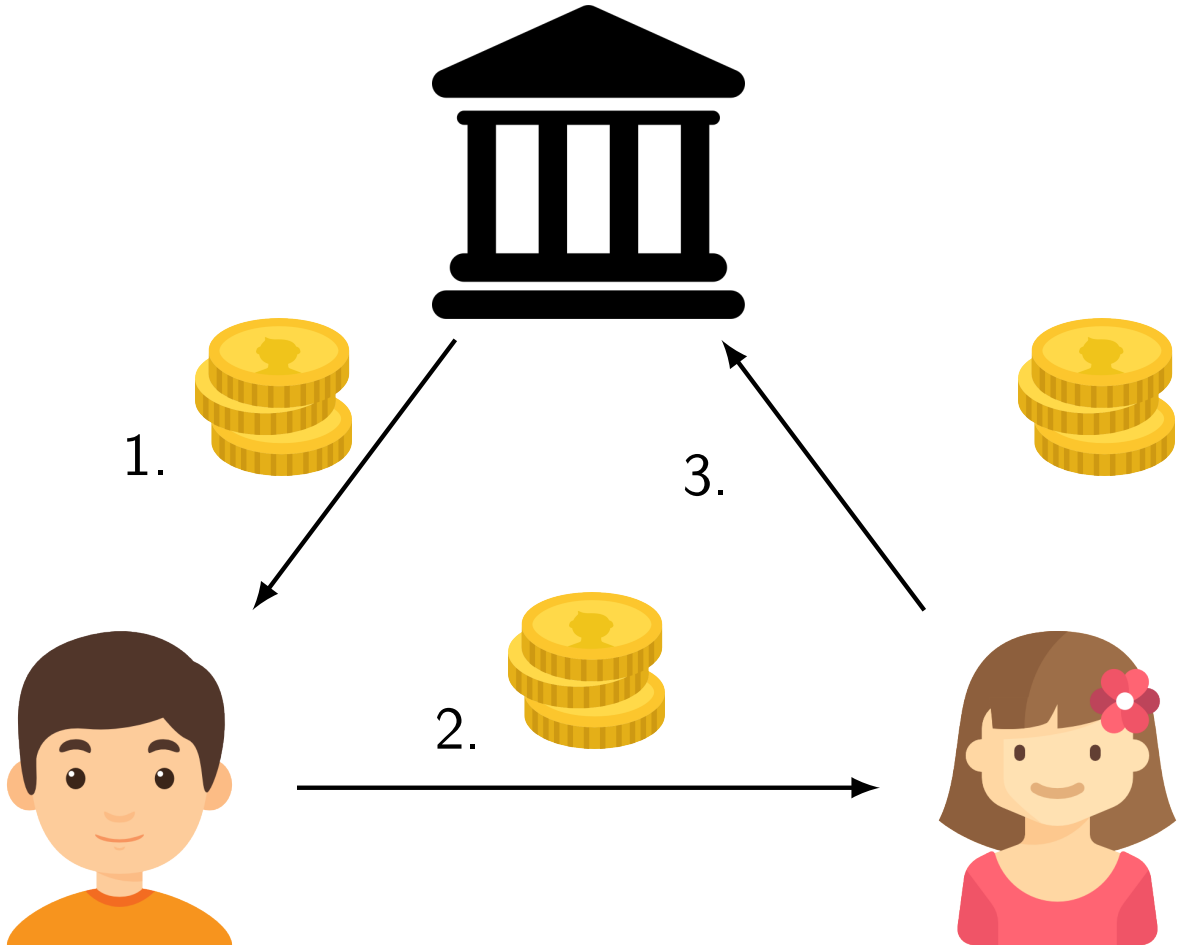
Principe : Banque centrale



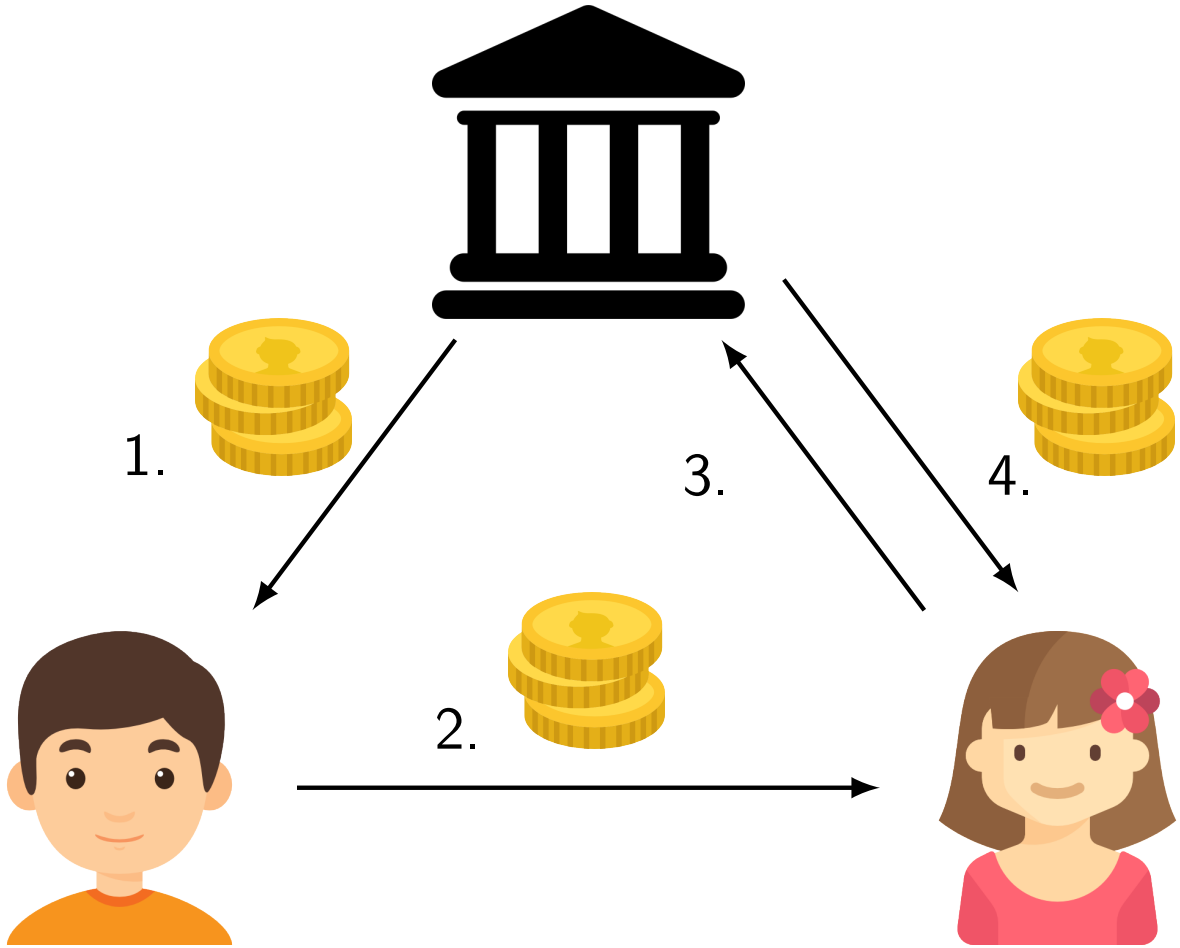
Principe : Banque centrale



Principe : Banque centrale



Principe : Banque centrale



1988 : Digitcash

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

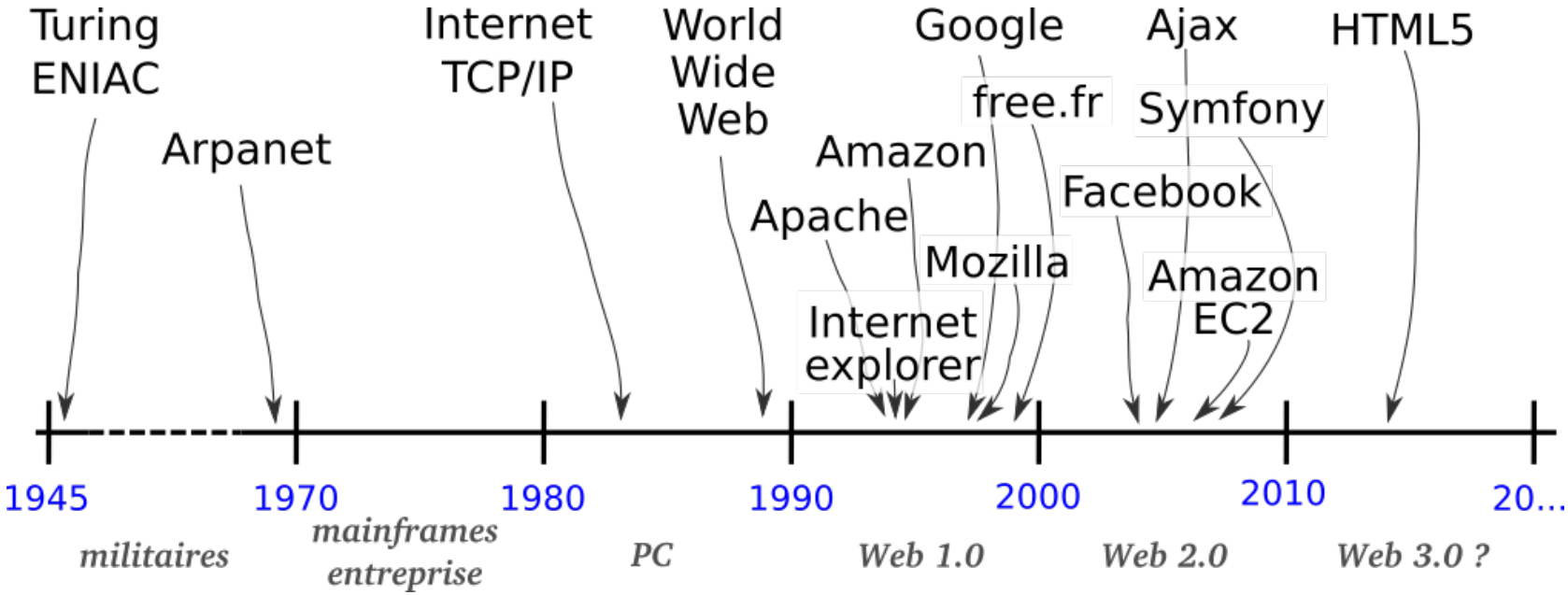
DigiCash™



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











Crypto-monnaie

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

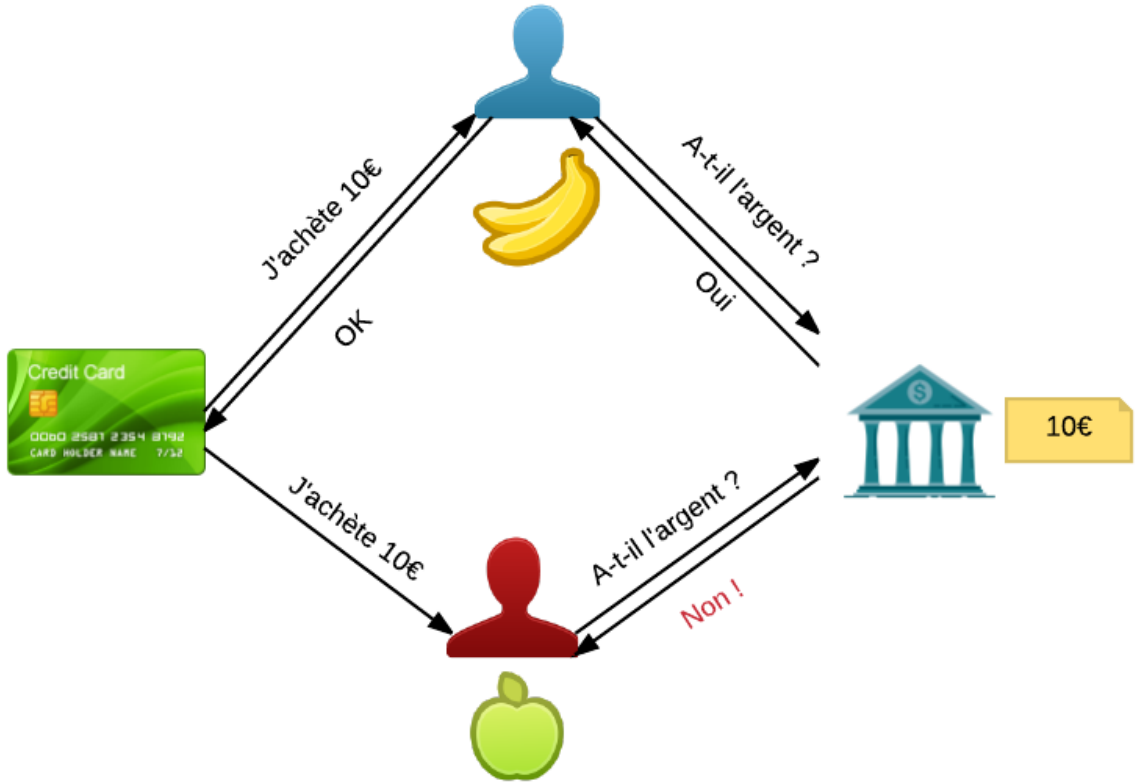
- Crypto-monnaie : monnaie électronique, se passant d'un Tiers
  4. Respect de la vie privée
  5. Non-Falsifiable
  6. Éviter les doubles dépenses

Propriétés : Non-Falsifiable (Unforgeable)





Propriétés : Eviter la double dépense



- 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



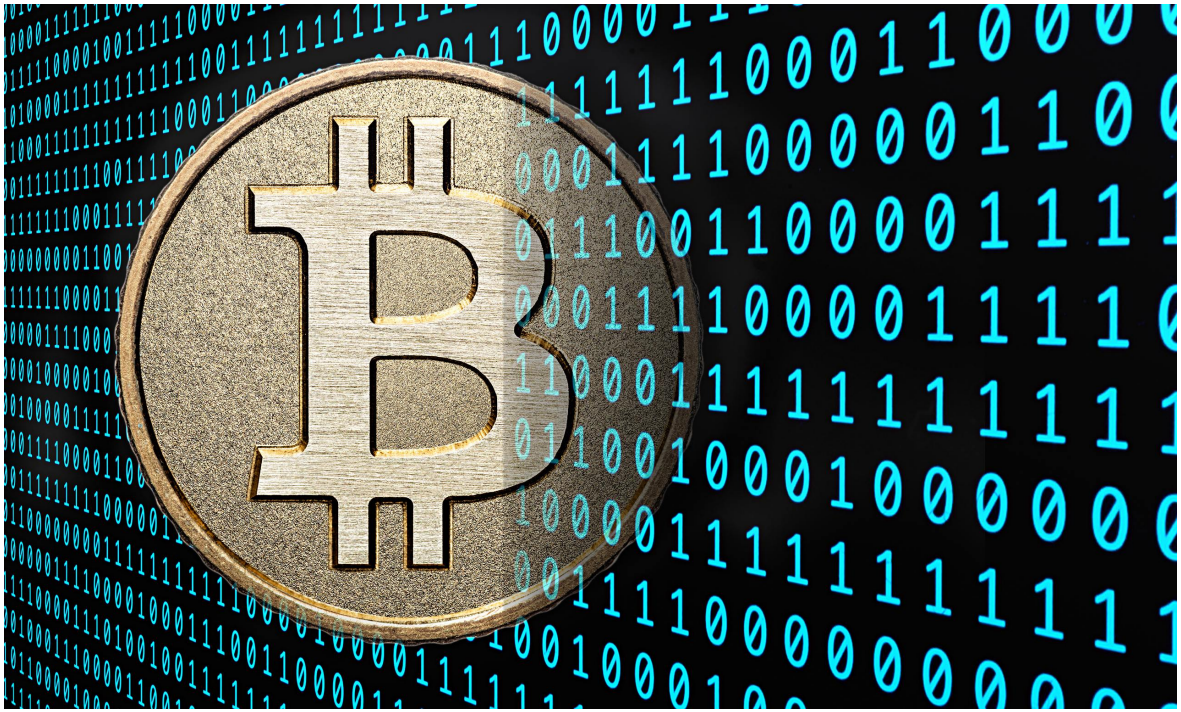




Monnaies classiques et crypto-monnaies

	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	✓	✓	✗

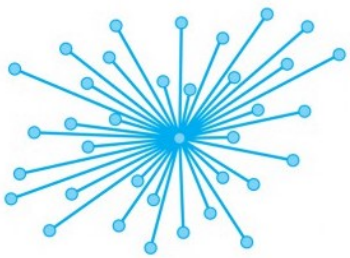
La révolution Bitcoin 2009



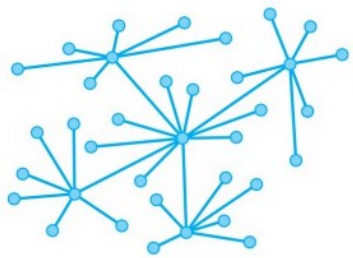


Bitcoin

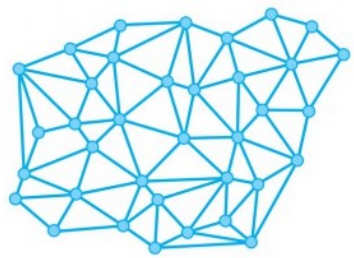
- Cryto-monnaie décentralisée et distribuée



Système centralisé



Système décentralisé



Système distribué



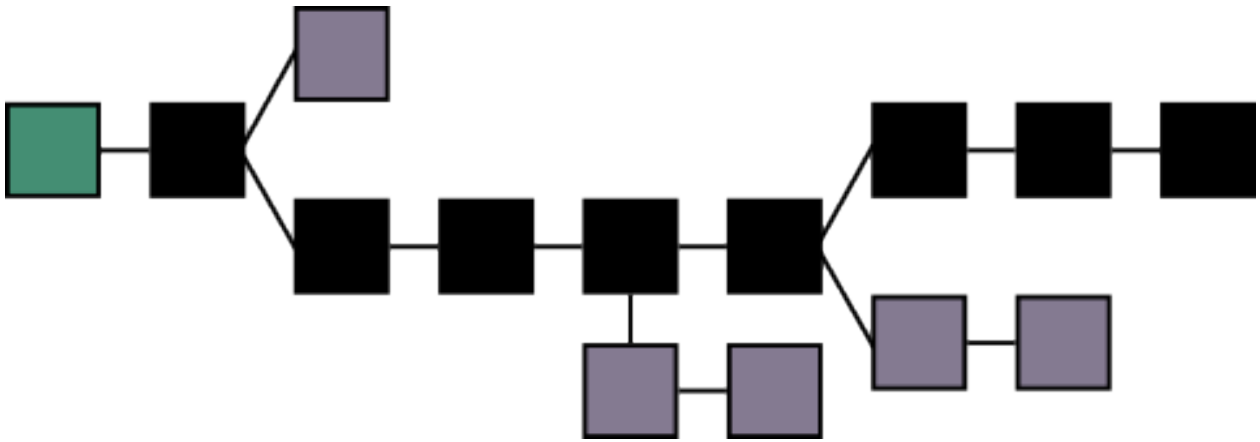


21 millions BTC

Inarrêtable car distribuée

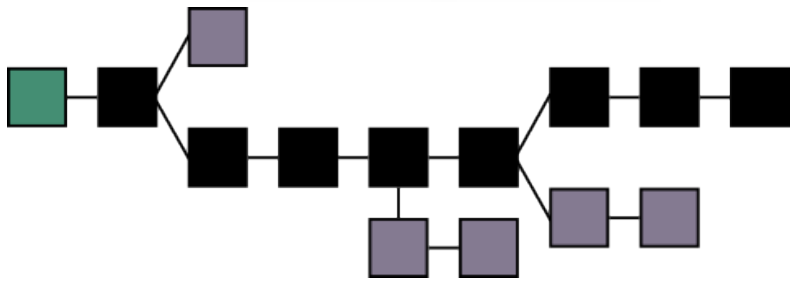


Infalsifiable



Auditable





Bitcoin : monnaie électronique

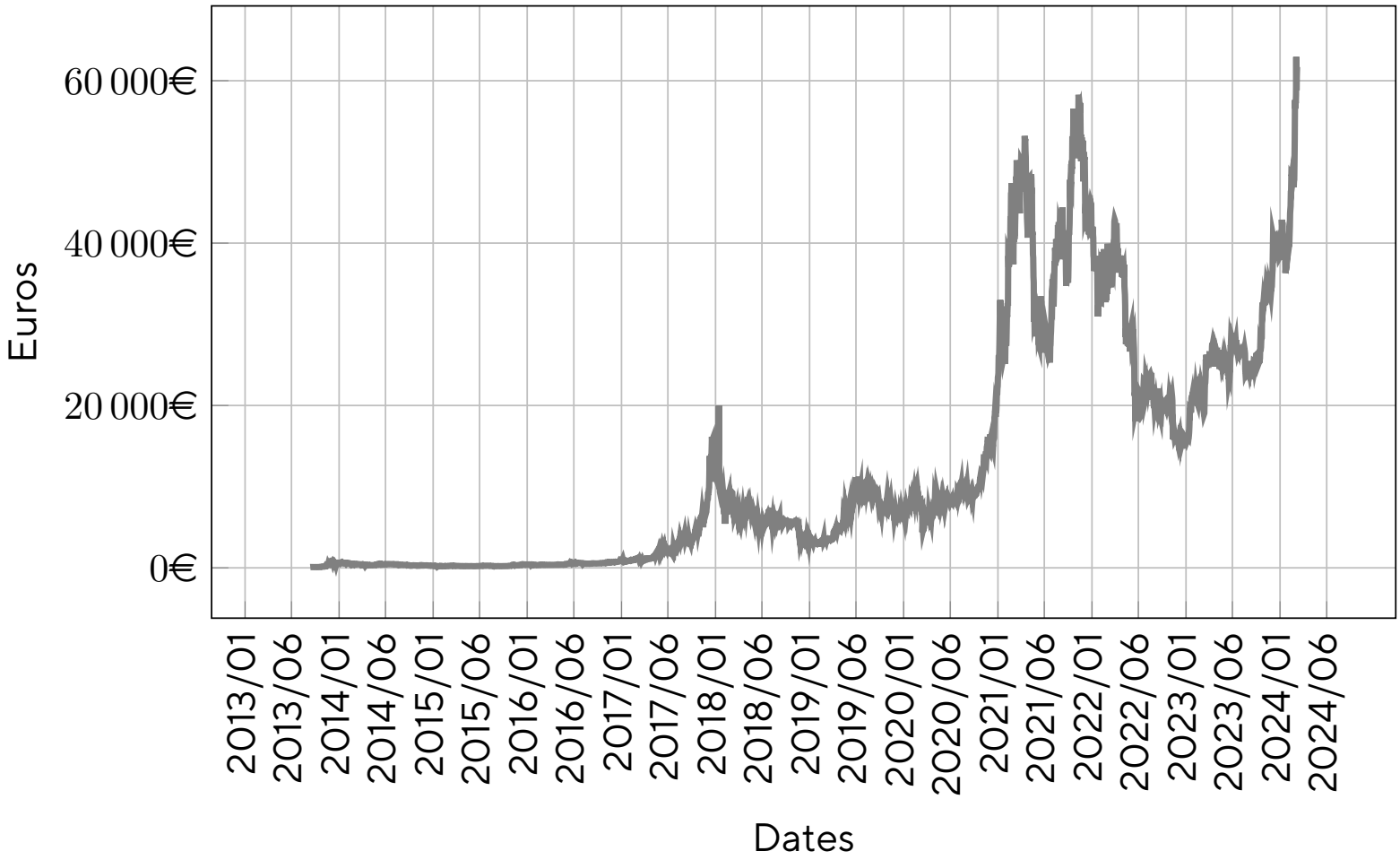
Créée en 2008 par Satoshi Nakamoto

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

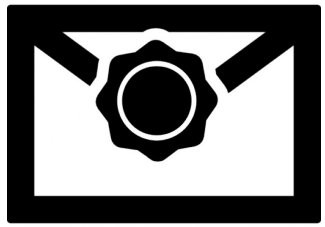


1	BTC = 1 Bitcoin	
$0,01$	BTC = 1 cBTC	= 1 centiBitcoin (ou bitcent)
$0,001$	BTC = 1 mBTC	= 1 milliBitcoin
$0,000\,001$	BTC = 1 μBTC	= 1 microBitcoin
$0,000\,000\,01$	BTC = 1 Satoshi	

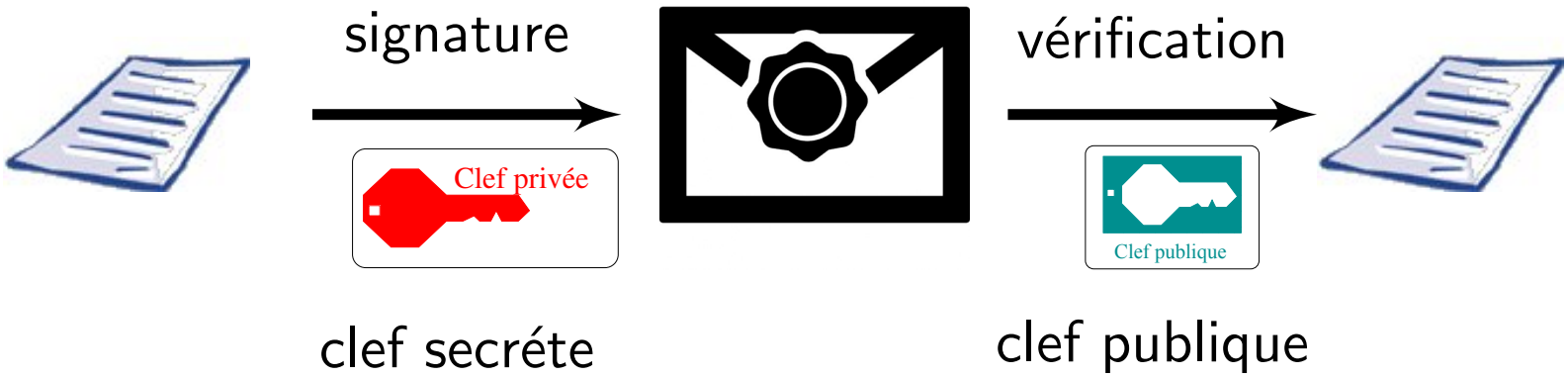
Taux de change du bitcoin 2024



Signature

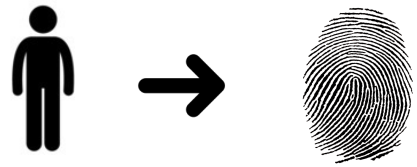






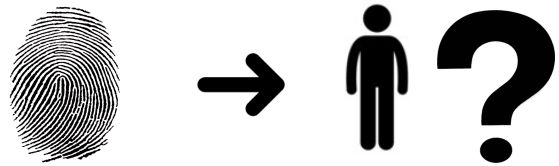
RSA: $m^d \mod n$

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

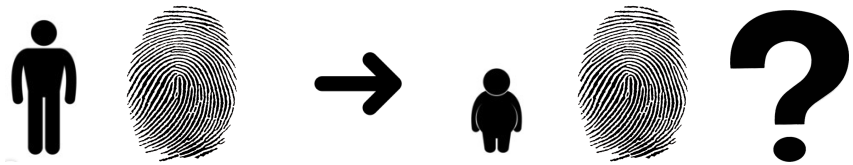


Propriétés de résistance

- Pré-image



- Seconde Pré-image



- Collision



Bitcoins : caractéristiques

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

  21 millions BTC

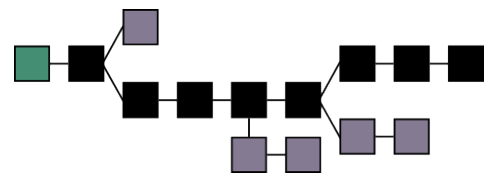


- Les transactions utilisent des **PKI**
- Numéro de compte :

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

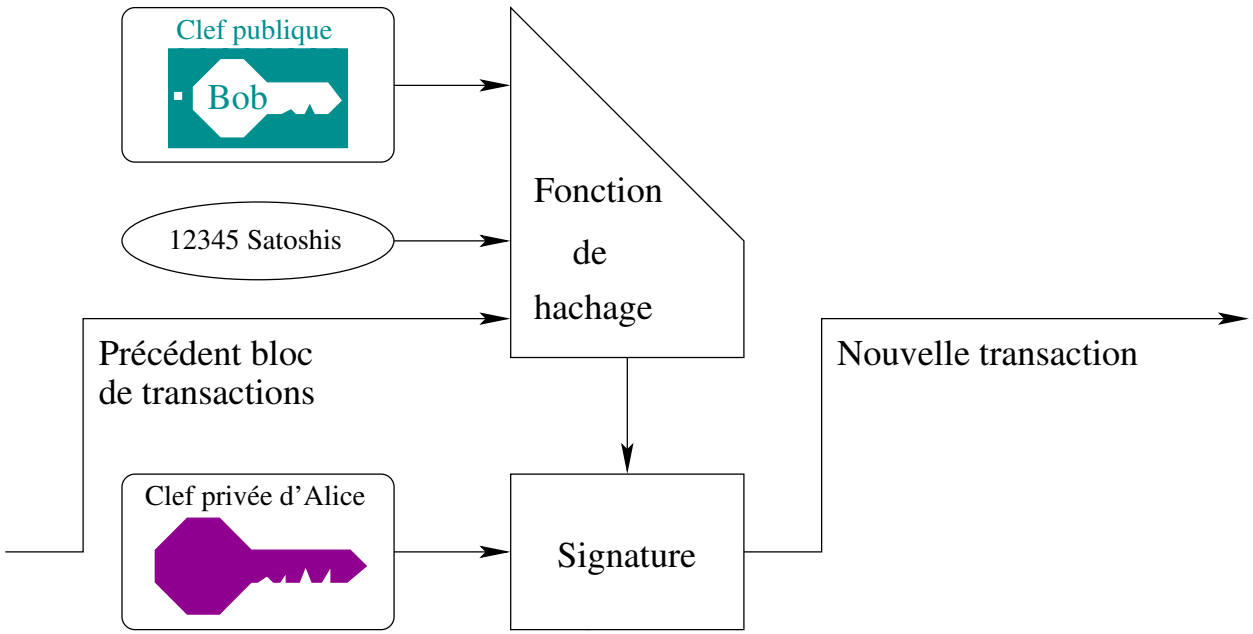


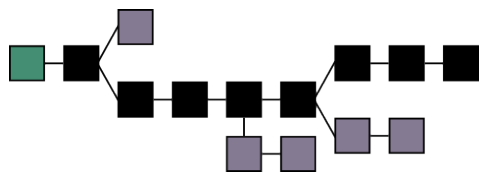
- Toutes les transactions sont **publiques**
- **Blockchain** : un système pair-à-pair qui garantit la validité des transactions



Comment faire une transaction?

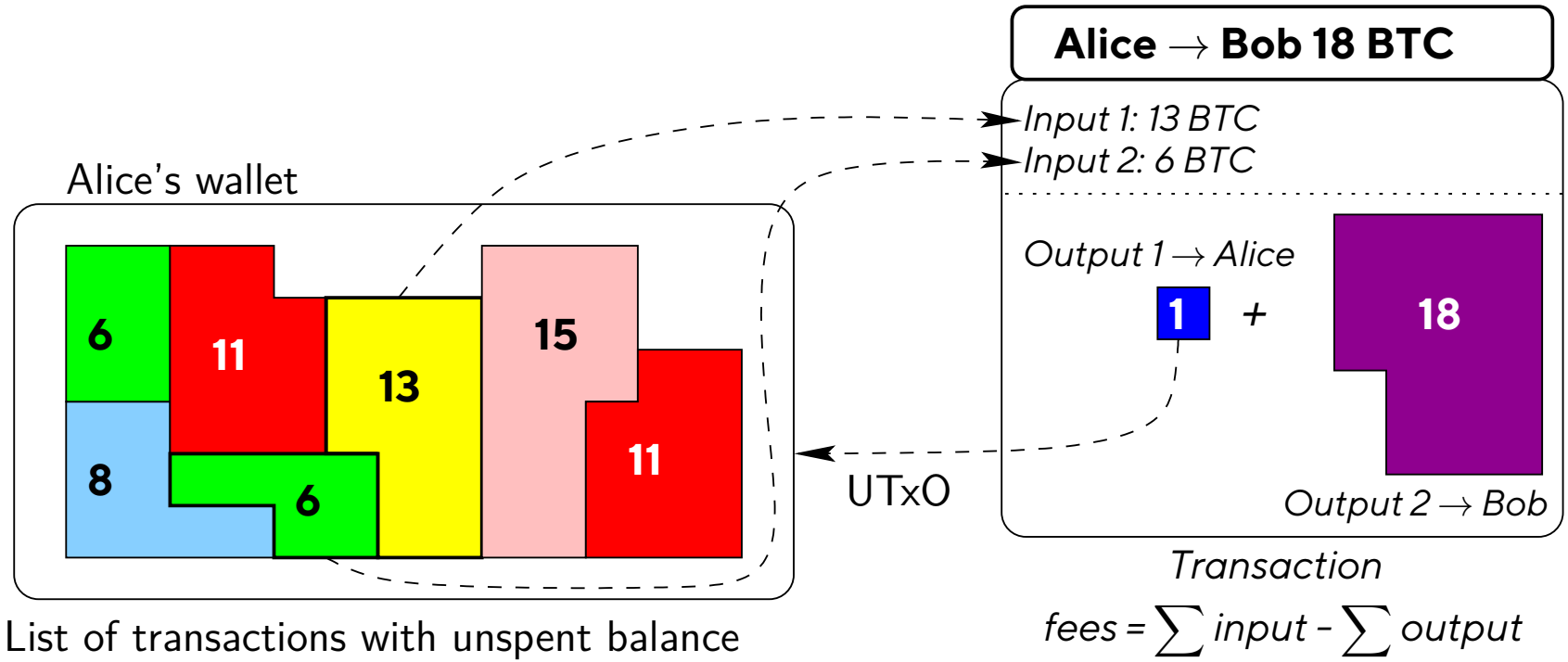
Alice donne 12345 Satochis ($\approx 5c$) à Bob.



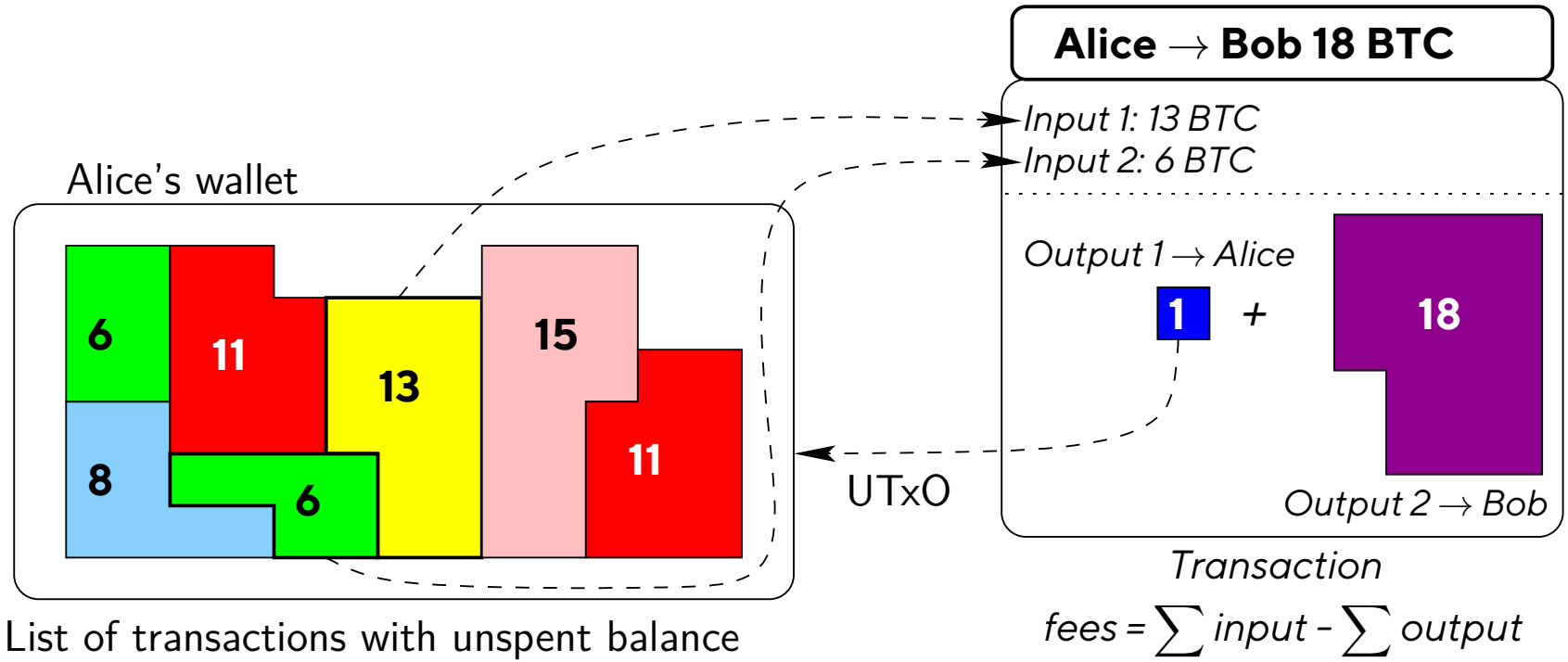


Unspent Transaction Output UTXO

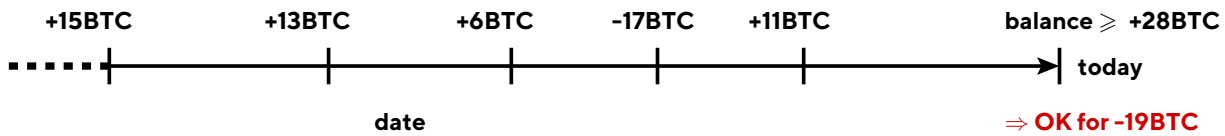
Pay 18 BTC with coins



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 ?

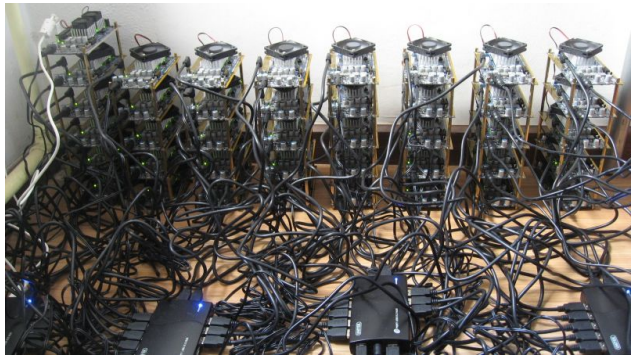
Miner des Bitcoins



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

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





Principe de la Blockchain

Etat de la chaîne 424210 A donne à B 3 BTC

🖨(A,B,3,424210)=458237

Etat de la chaîne 458237 C donne à B 9 BTC

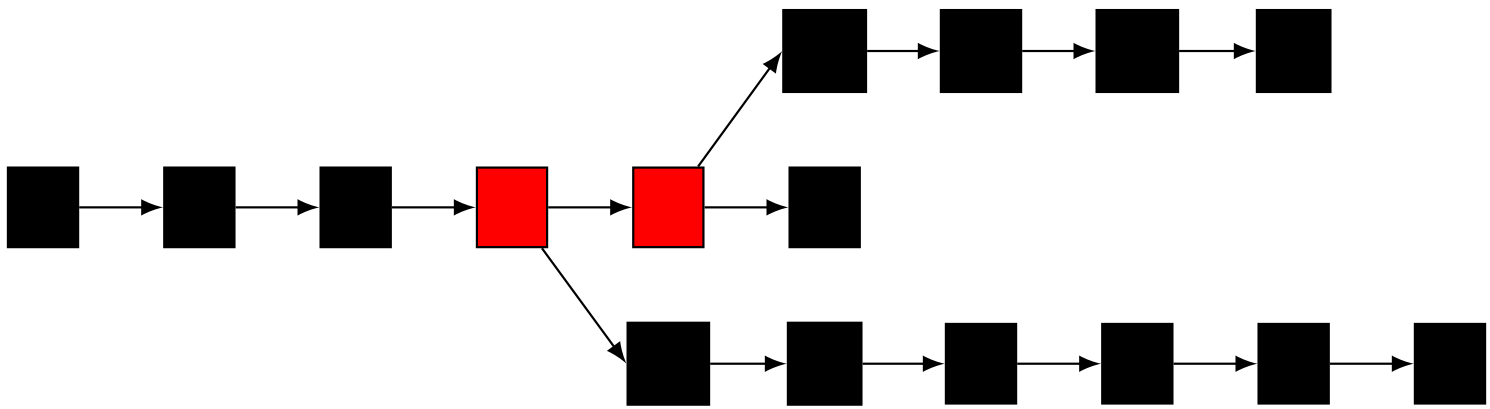
🖨(C,B,9,458237)=936127

Etat de la chaîne 936127 C donne à A 1 BTC

🖨(C,A,1,936127)=458237

Blockchain Infalsifiable

$$
\begin{aligned}
& \text{🖨}(C, A, 1, \text{🖨}(C, B, 9, \text{🖨}(A, B, 3, 424210))) \\
= \; & \text{🖨}(C, A, 1, \text{🖨}(C, B, 9, 458237)) \\
= \; & \text{🖨}(C, A, 1, 936127) \\
= \; & 458237
\end{aligned}
$$



Miner : Objectif de hachage

Cible pour le block 816 377 (Février 2024)

0000000000000000000481940000000000000000000000000000000000



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)
0000000000000000000481940000000000000000000000000000000000



Trouver une nombre n tel que

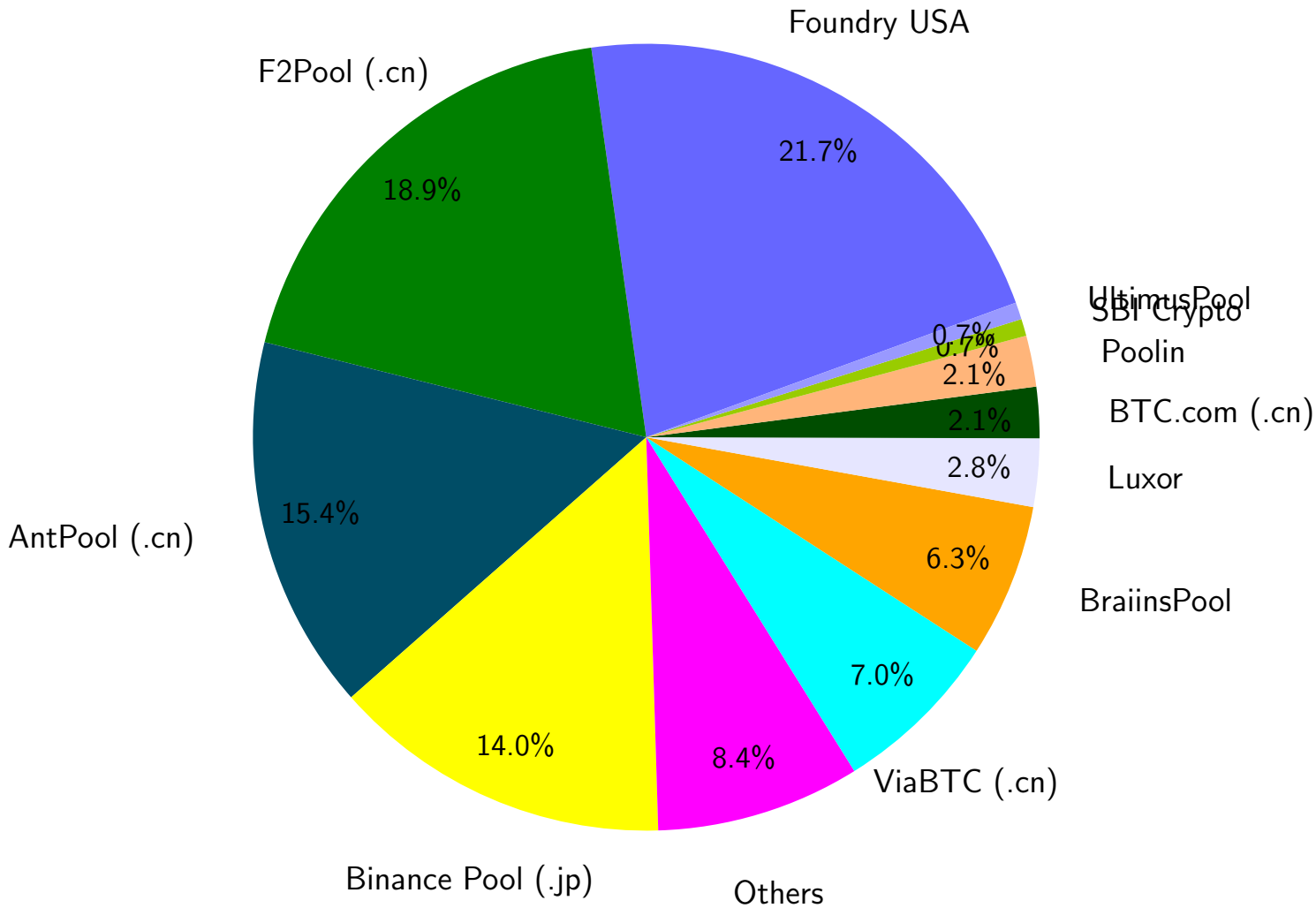
$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, n)) = x < \textit{Cible}$$

Avoir au moins 18 zéros au début de x

Stratégie : brute force

Tester toutes les valeurs possibles de n

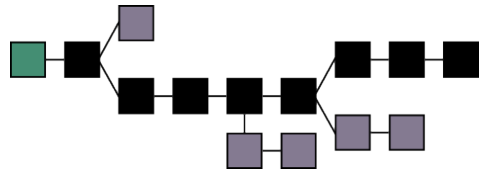
Fermes de mineurs: partagent les récompenses



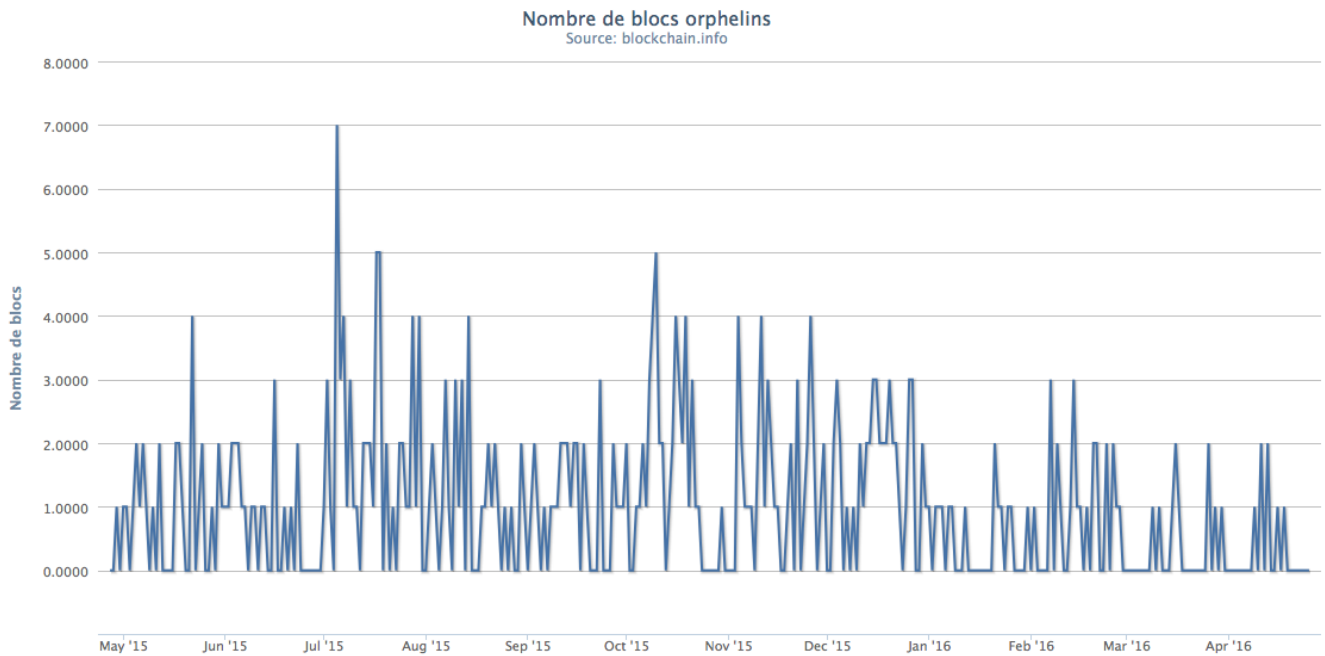
Miner = Validation des transactions

Cible: 00000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076

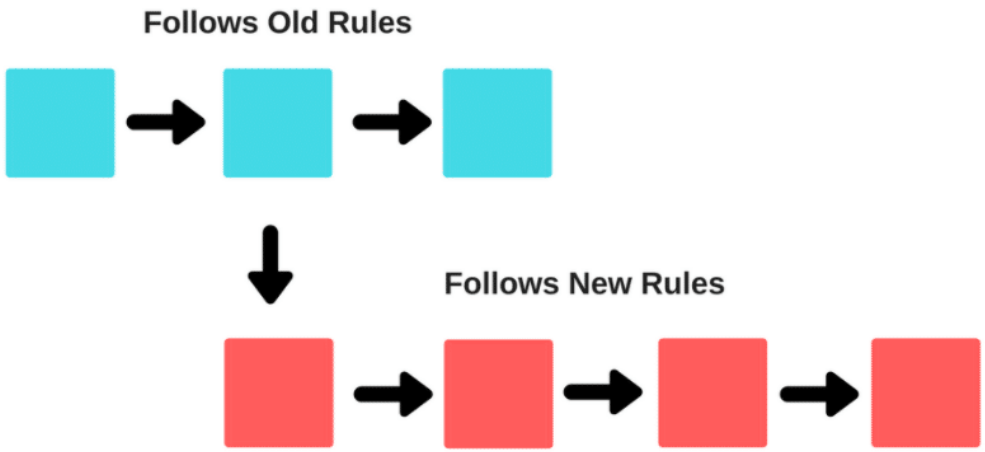
Re-évaluée tous les blocs à partir des 2016 blocs passéss



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



Soft Fork

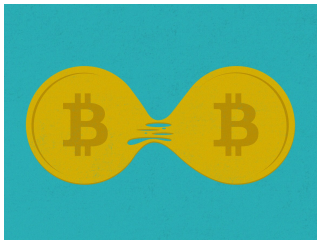


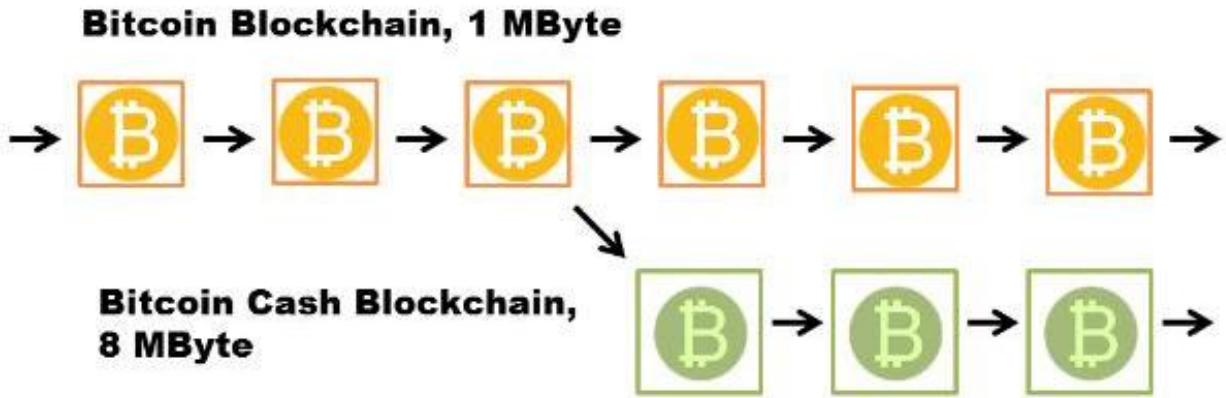
The primary difference between a soft fork and hard fork is that it is not backward compatible

Modification du code :

- Correction de bugs
- Améliorations consensuelles

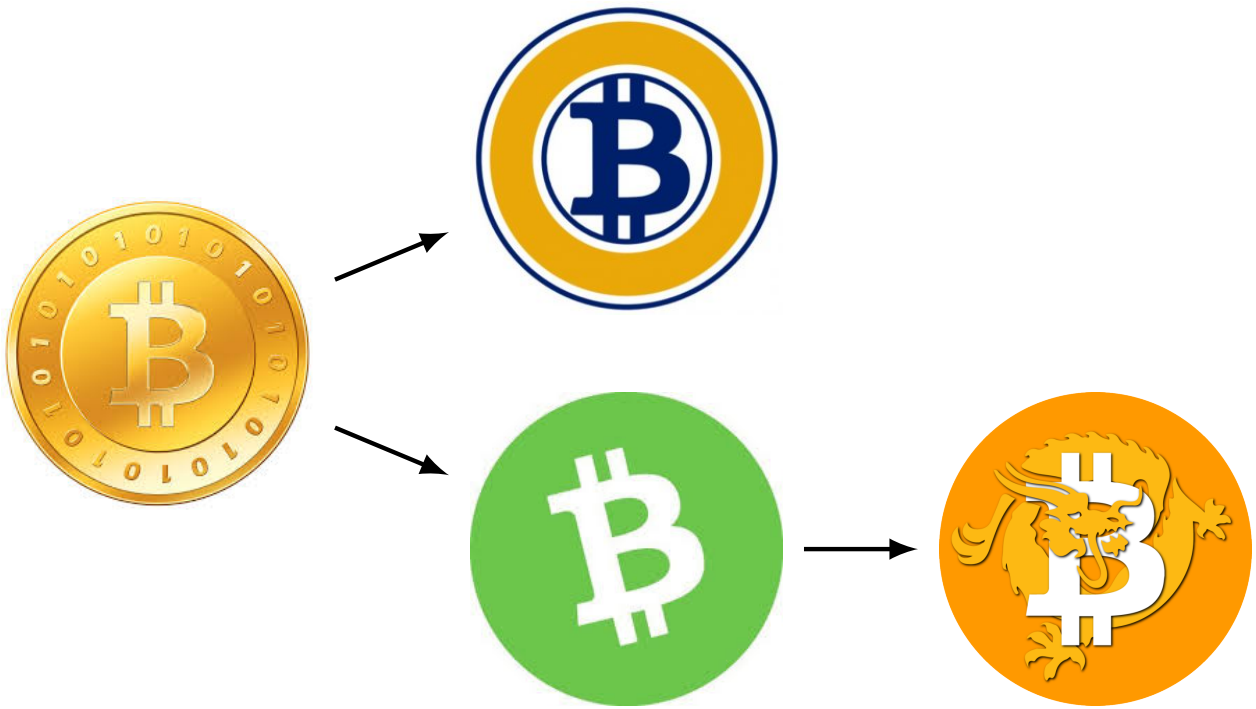
Hard Fork




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)



Hard Fork History

Logo	Fork Name	Fork Symbol	Blockchain	Fork Date	Fork Block	Coin Distribution
	Bitcoin Zero	BZX	Bitcoin	Sunday, September 30, 2018	0	1 HXX : 1 BTC = 1 BZX
	Micro Bitcoin	MBC	Bitcoin	Wednesday, May 30, 2018	525000	1 BTC = 10000 MBC
	ClassicBitcoin	CBTC	Bitcoin	Sunday, April 01, 2018	516095	1 BTC = 10000 CBTC
	Bitcoin Lite	BTCL	Bitcoin	Tuesday, January 30, 2018	0	1 BTC = 1 BTCL
	Bitcoin Atom	BCA	Bitcoin	Wednesday, January 24, 2018	505888	1 BTC = 1 BCA
	Bitcoin Interest	BCI	Bitcoin	Monday, January 22, 2018	505083	1 BTC = 1 BCI
	BitVote	BTV	Bitcoin	Sunday, January 21, 2018	505050	1 BTC = 1 BTV
	Bitcoin Smart	BCS	Bitcoin	Sunday, January 21, 2018	505050	1 BTC = 100 BCS
	Bitcoin Rhodium	BTR	Bitcoin	Wednesday, January 10, 2018	0	1 BTC = 1 BTR
	Bitcoin Private	BTCP	Bitcoin	Monday, January 01, 2018	0	1 BTC/ZCL = 1 BTCP
	Bitcoin All	BTA	Bitcoin	Monday, January 01, 2018	0	1 BTC = 1 BTA
	Bitcoin Pizza	BPA	Bitcoin	Monday, January 01, 2018	501888	1 BTC = 1 BPA
	BitcoinBoy	BCB	Bitcoin	Sunday, December 31, 2017	501888	1 BTC = 100 BCB
	Bitcoin Ore	BCO	Bitcoin	Sunday, December 31, 2017	501949	1 BTC = 1 BCO
	Bitcoin Uranium	BUM	Bitcoin	Sunday, December 31, 2017	0	1 BTC = 1 BUM
	Quantum Bitcoin	QBTC	Bitcoin	Thursday, December 28, 2017	0	1 BTC = 1QBTC
	Bitcoin SegWit2X x11	B2X	Bitcoin	Thursday, December 28, 2017	501451	1 BTC = 1 B2X
	Bitcoin File	BIFI	Bitcoin	Wednesday, December 27, 2017	501225	1 BTC = 1000 BIFI
	Bitcoin God	GOD	Bitcoin	Wednesday, December 27, 2017	501225	1 BTC = 1 GOD
	Bitcoin Top	BTT	Bitcoin	Tuesday, December 26, 2017	501118	1 BTC = 1 BTT

Logo	Fork Name	Fork Symbol	Blockchain	Fork Date	Fork Block	Coin Distribution
	Bitcoin New	BTN	Bitcoin	Monday, December 25, 2017	501000	1 BTC = BTN
	Lightning Bitcoin	LBTC	Bitcoin	Tuesday, December 19, 2017	499999	1 BTC = 1 LBTC
	Bitcoin Stake	BTCS	Bitcoin	Tuesday, December 19, 2017	499999	1 BTC = 100 BTCS
	Bitcoin Faith	BTF	Bitcoin	Tuesday, December 19, 2017	500000	1 BTC = 1 BTF
	Bitcoin World	BTW	Bitcoin	Sunday, December 17, 2017	499777	1 BTC = 10000 BTW
	UnitedBitcoin	UB	Bitcoin	Tuesday, December 12, 2017	498777	1 BTC = 1 UB
	Bitcoin Hot	BTH	Bitcoin	Tuesday, December 12, 2017	498848	1 BTC = 100 BTH
	BitcoinX	BCX	Bitcoin	Tuesday, December 12, 2017	498888	1 BTC = 10000 BCX
	Super Bitcoin	SBTC	Bitcoin	Tuesday, December 12, 2017	498888	1 BTC = 1 SBTC
	Bitcoin Silver	BTSI	Bitcoin	Friday, December 01, 2017	0	1 BTC = 1 BTSI
	Bitcoin Nano	BTN	Bitcoin	Friday, December 01, 2017	501888	1 BTC = 1000 BTN
	Bitcoin Diamond	BCD	Bitcoin	Friday, November 24, 2017	495866	1 BTC = 10 BCD
	Bitcore	BTX	Bitcoin	Thursday, November 02, 2017	0	1 BTC = 0.5 BTX
	Bitcoin Gold	BTG	Bitcoin	Tuesday, October 10, 2017	491407	1 BTC = 1 BTG
	Bytether	BTH	Bitcoin	Tuesday, August 01, 2017	478558	1 BTC = 1 BTH
	Oil BTC	OBTC	Bitcoin	Tuesday, August 01, 2017	498888	1 BTC = 1 OBTC
	Bitcoin Clashic	BCHC / B	Bitcoin	Tuesday, August 01, 2017	478558	1 BTC = 1 BCHC / B
	Bitcoin Cash	BCH	Bitcoin	Tuesday, August 01, 2017	478559	1 BTC = 1 BCH

Traçable



Traçable

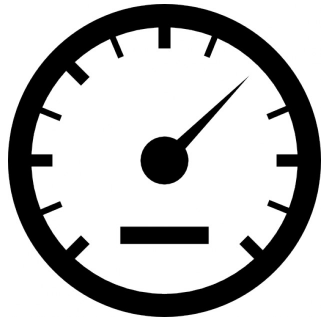






Snark

Limitations

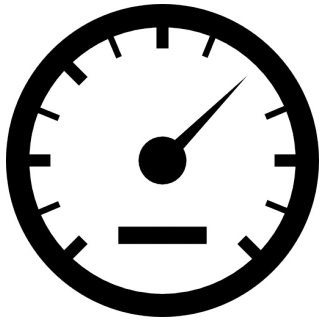


10 minutes = 1 block



Taille des transactions 1 Mo

Limitations



10 minutes = 1 block



Taille des transactions 1 Mo



Lightning Network

ETHEREUM

12 secondes

Energivore

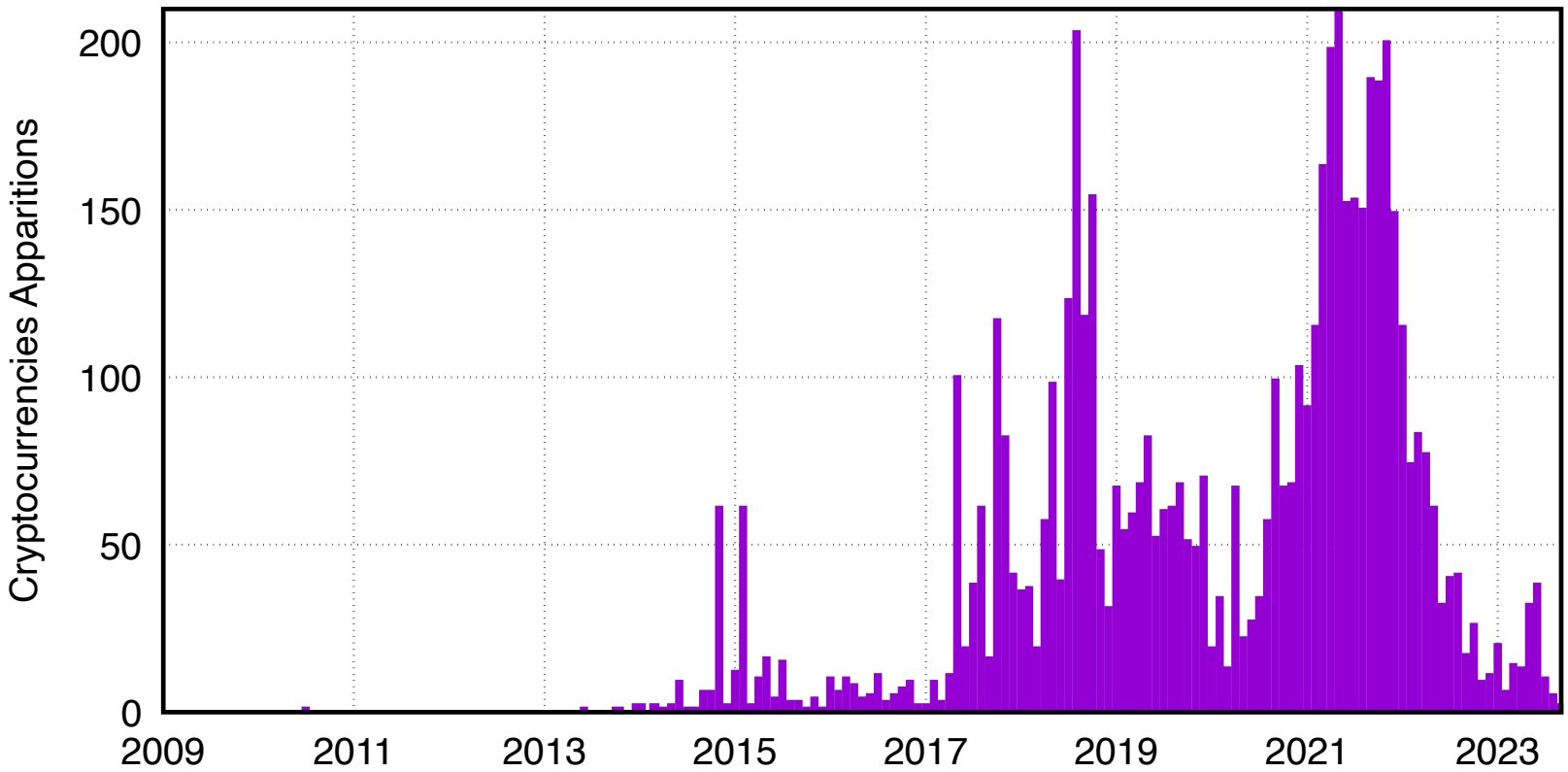


Proof of Stake
Lightning Network

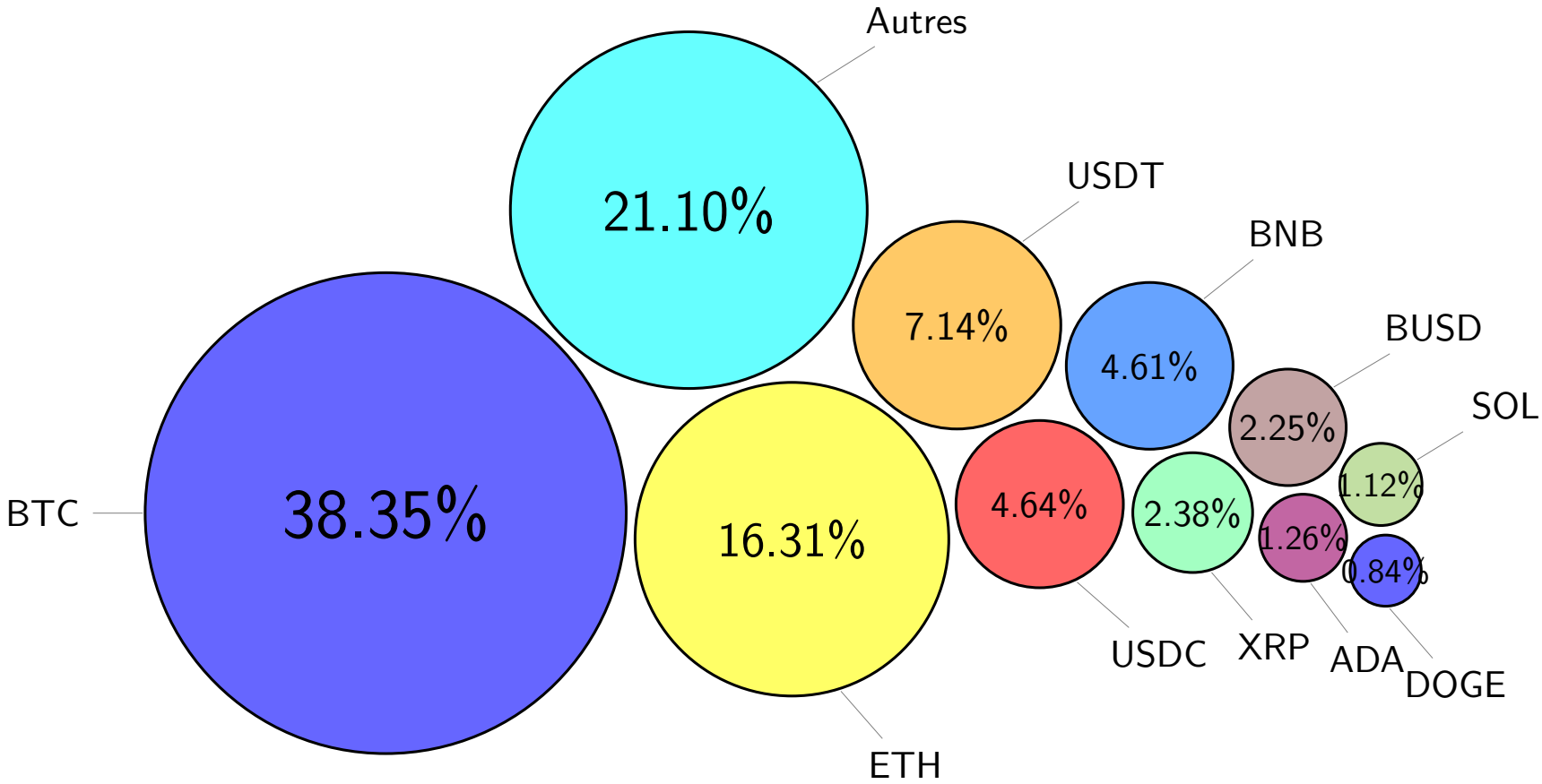
Autres crypto-monnaies



Autres crypto-monnaies



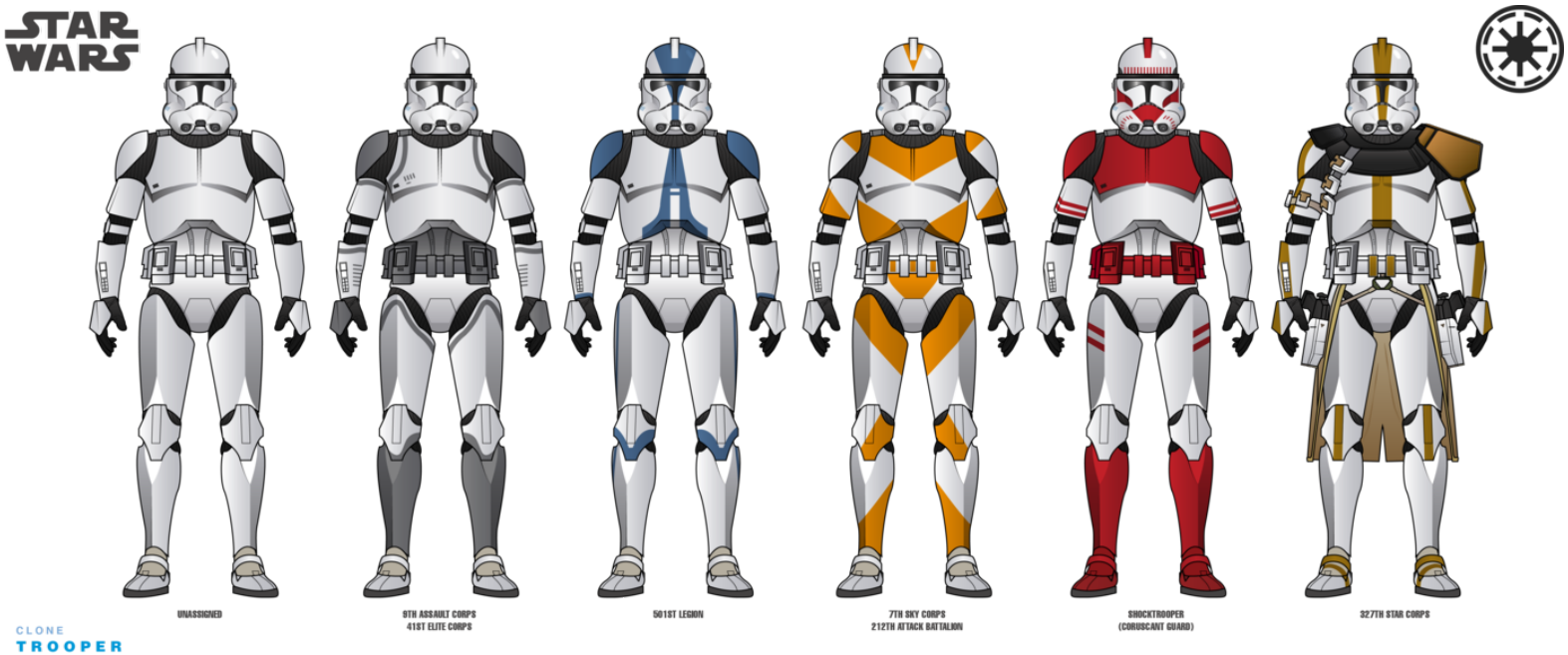
Diversité monétaire



Classification I : Pourris



Classification II : Clones de Bitcoin



Classification III : Plus utile











Classification IV : Autres preuves de travail







ethereum



helium

Passage à l'échelle ?

- Bitcoin 3-4 transactions / seconde
- Etherum 15 transactions / seconde
- VISA 65 000 transactions / seconde

Passage à l'échelle ?

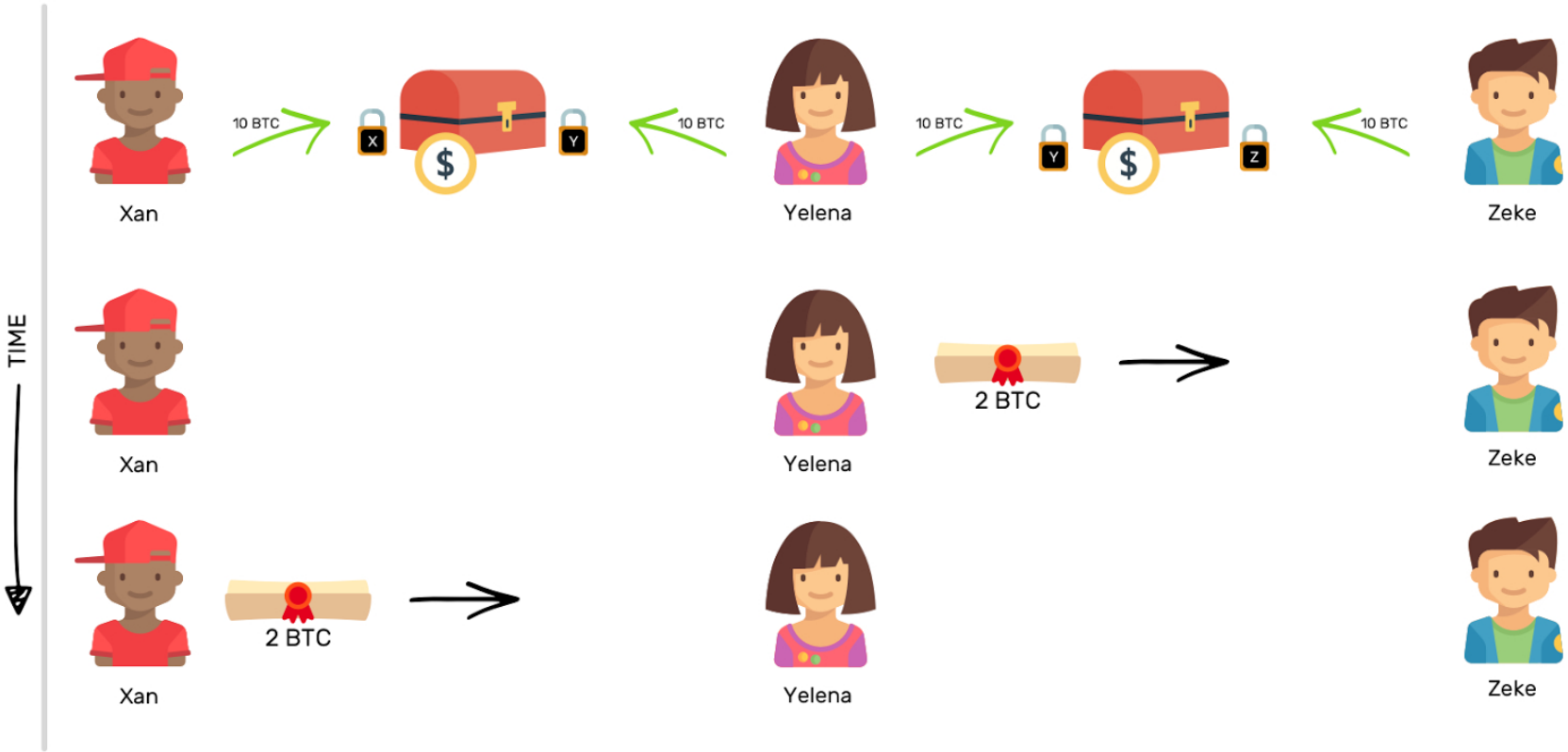
- Bitcoin 3-4 transactions / seconde
- Etherum 15 transactions / seconde
- VISA 65 000 transactions / seconde

Solutions :

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

State Channel : Lightning Network





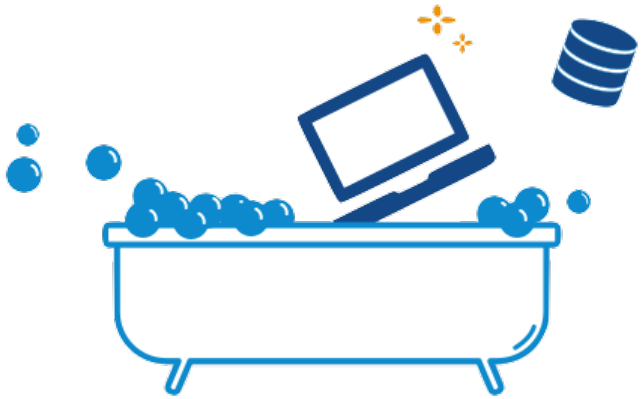
Qui s'approprie ces nouvelles monnnaies ?







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







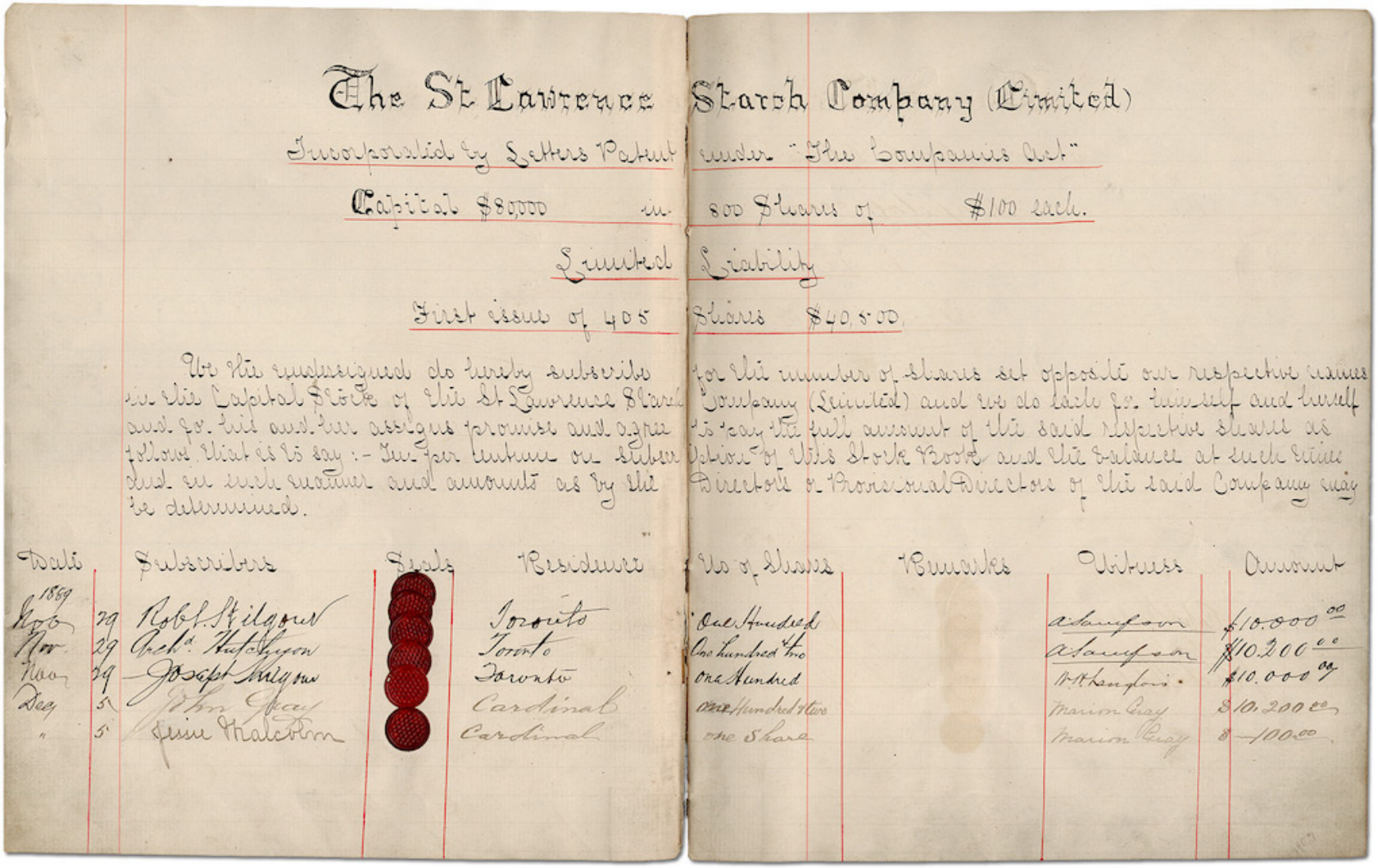
- Perte ou vol de la clef secrète = irréversible
- Monnaie anonyme et traçable







Blockchain



The St Lawrence Starch Company (Limited)

Incorporated by Letters Patent under "The Companies Act."

Capital $80,000 in 800 Shares of $100 each.

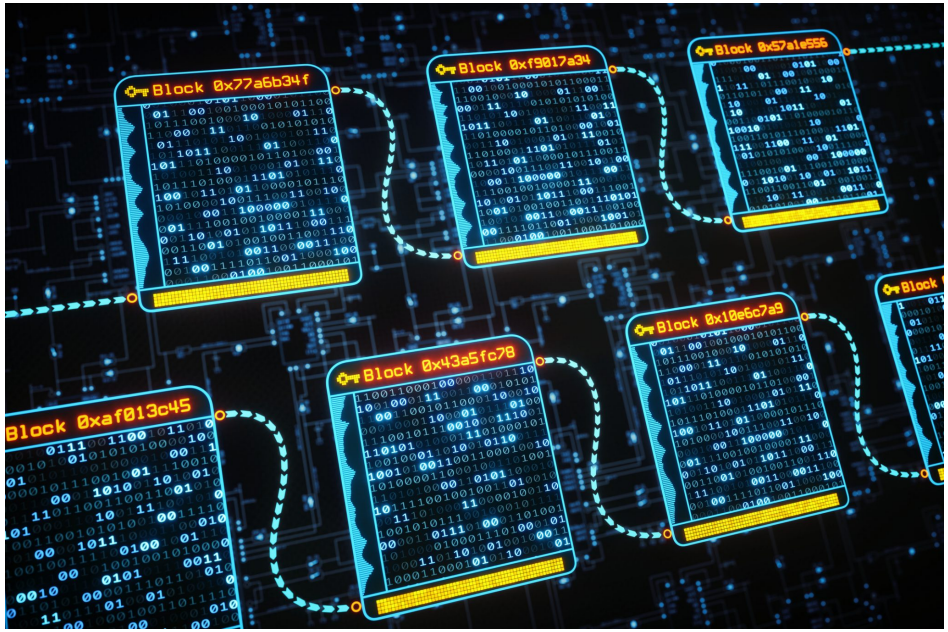
Limited Liability

First issue of 405 Shares $40,500.00

We the undersigned do hereby subscribe for the Capital Stock of the St Lawrence Starch Co. for the number of shares set opposite our respective names and do further agree to take the said shares and pay for the same 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
1869								
Nov	29	Robt Stilgoe		Toronto	One Hundred		a Sampson	$10.000 00
Nov	29	Archd Hutchison		Toronto	One Hundred & two		a Sampson	$10.200 00
Nov	29	Joseph Stilgoe		Toronto	One Hundred		W.H. Langton	$10.000 00
Dec	5	John Gray		Cardinal	one Hundred & two		Marion Gray	$10.200 00
"	5	Jesse Malcolm		Cardinal	one Share		Marion Gray	$ 100.00

Blockchain

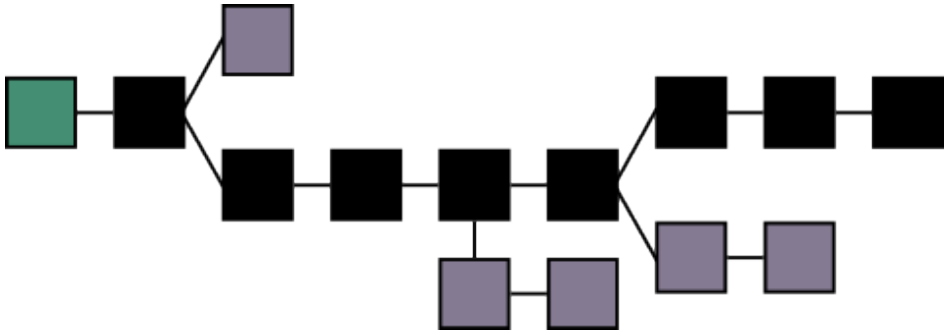


Registre distribué, sécurisé, infalsifiable

Mineurs valident des transactions



Tiennent à jour le registre distribué

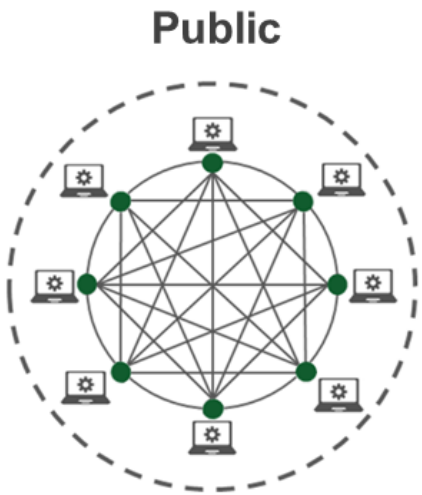


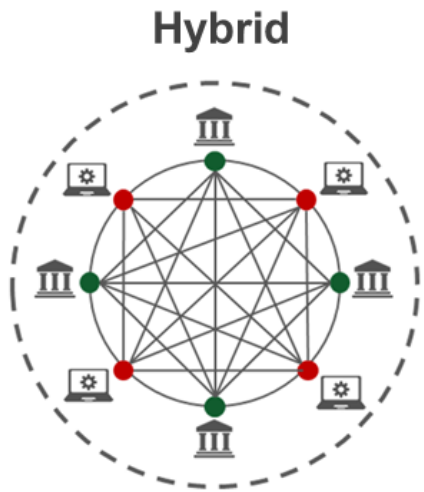
Inarrêtable, Infalsifiable, Auditable

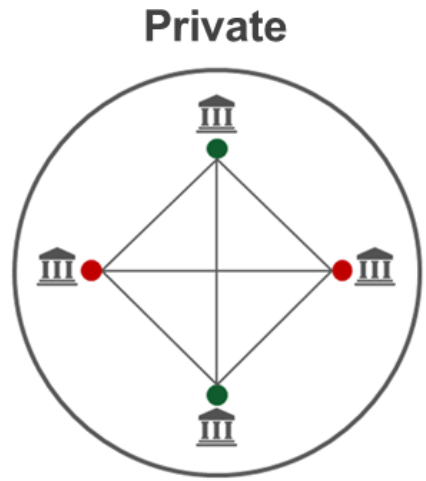
Décision des mineurs



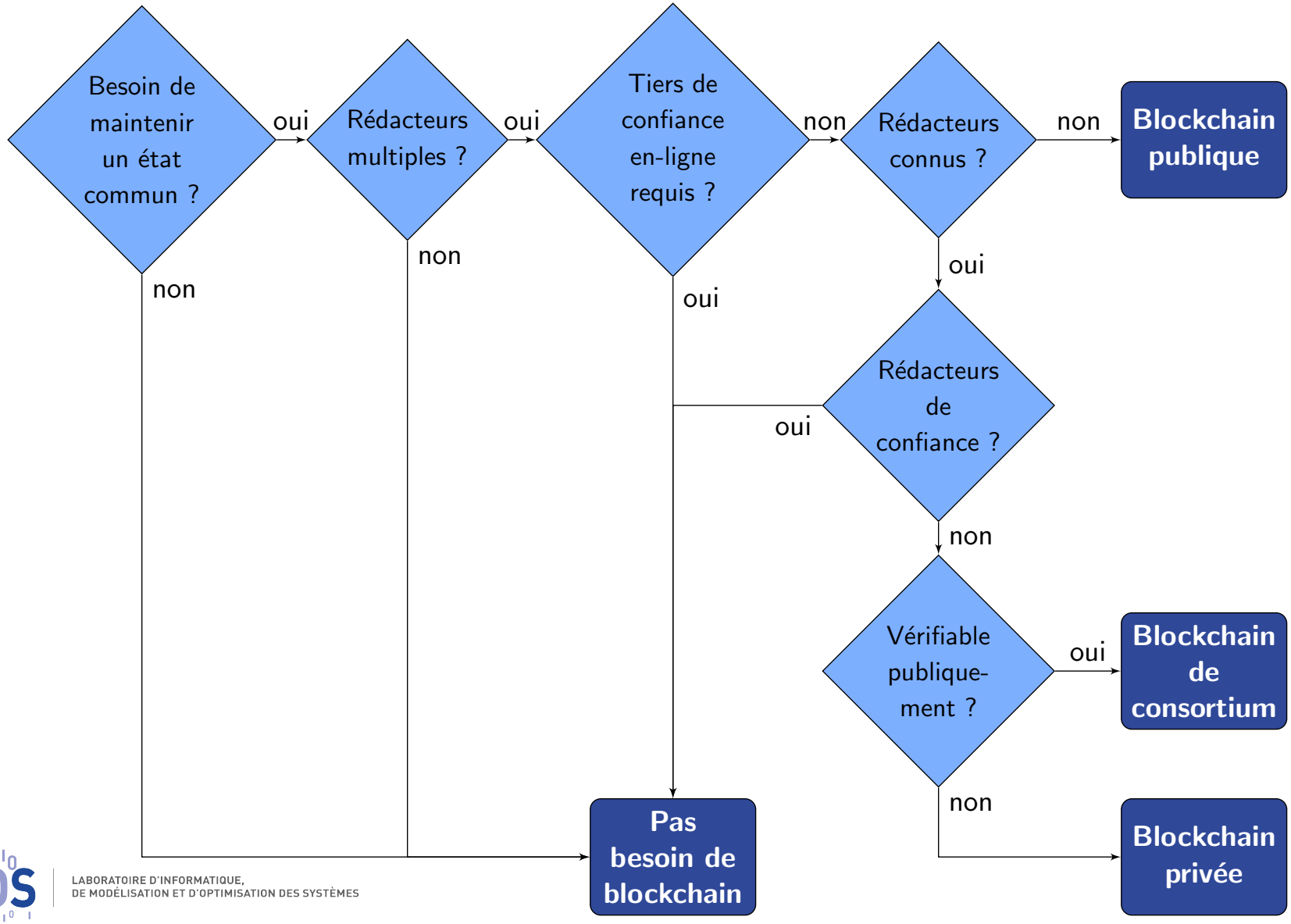
Blockchain Privée vs Publique



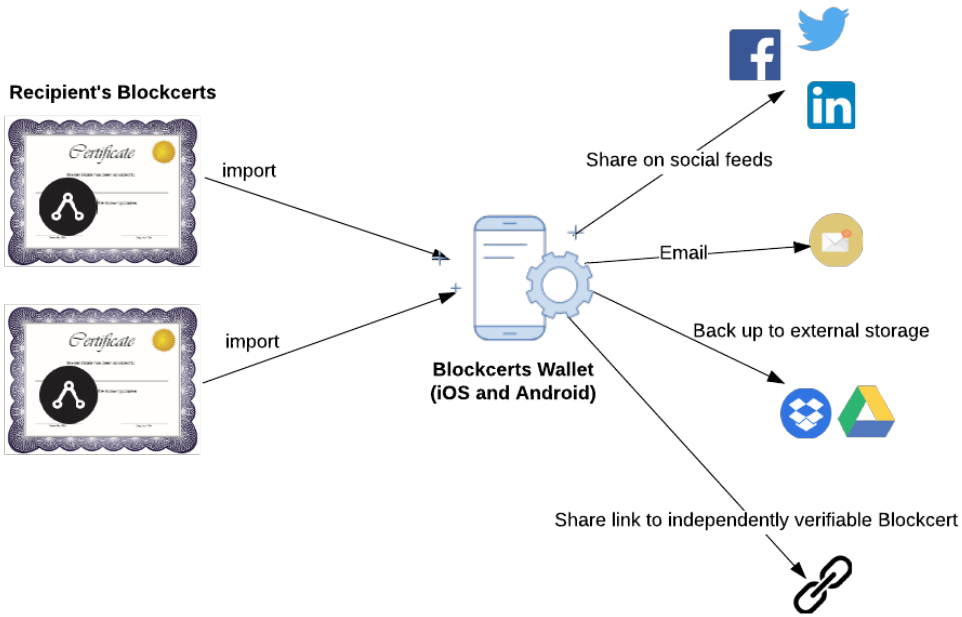




Ai-je besoin d'une blockchain ?

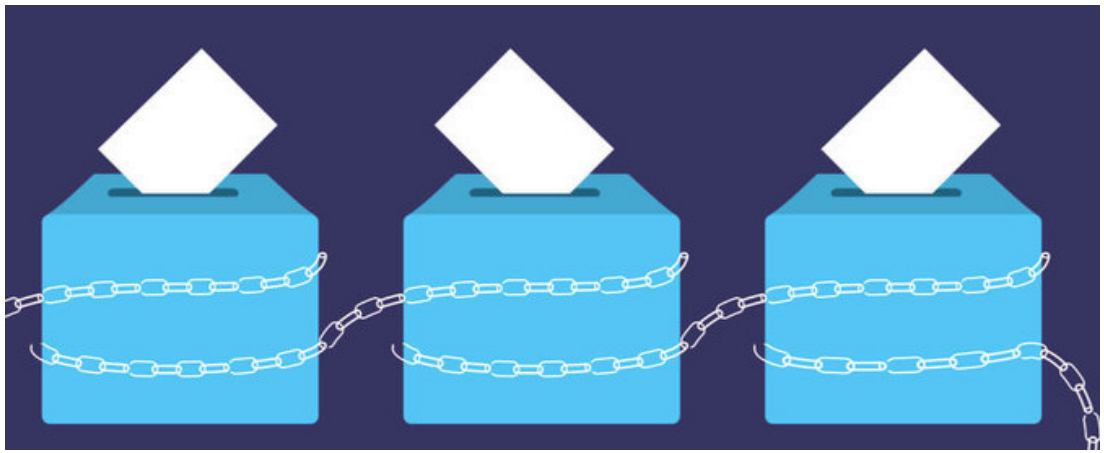


Blockchain Application : MIT Diploma





Blockchain Applications : Verify Your Vote, DABSTERS



Properties

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

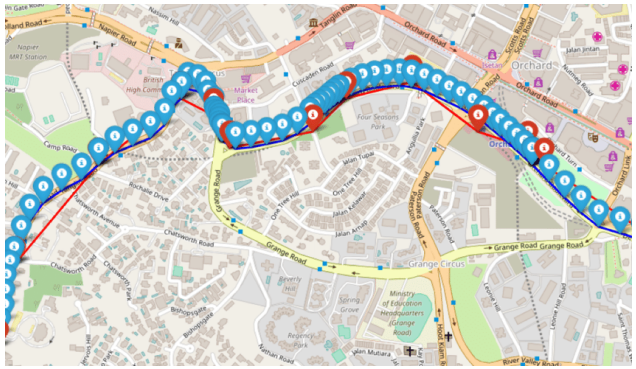
Blockchain Applications : Auction



Properties

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

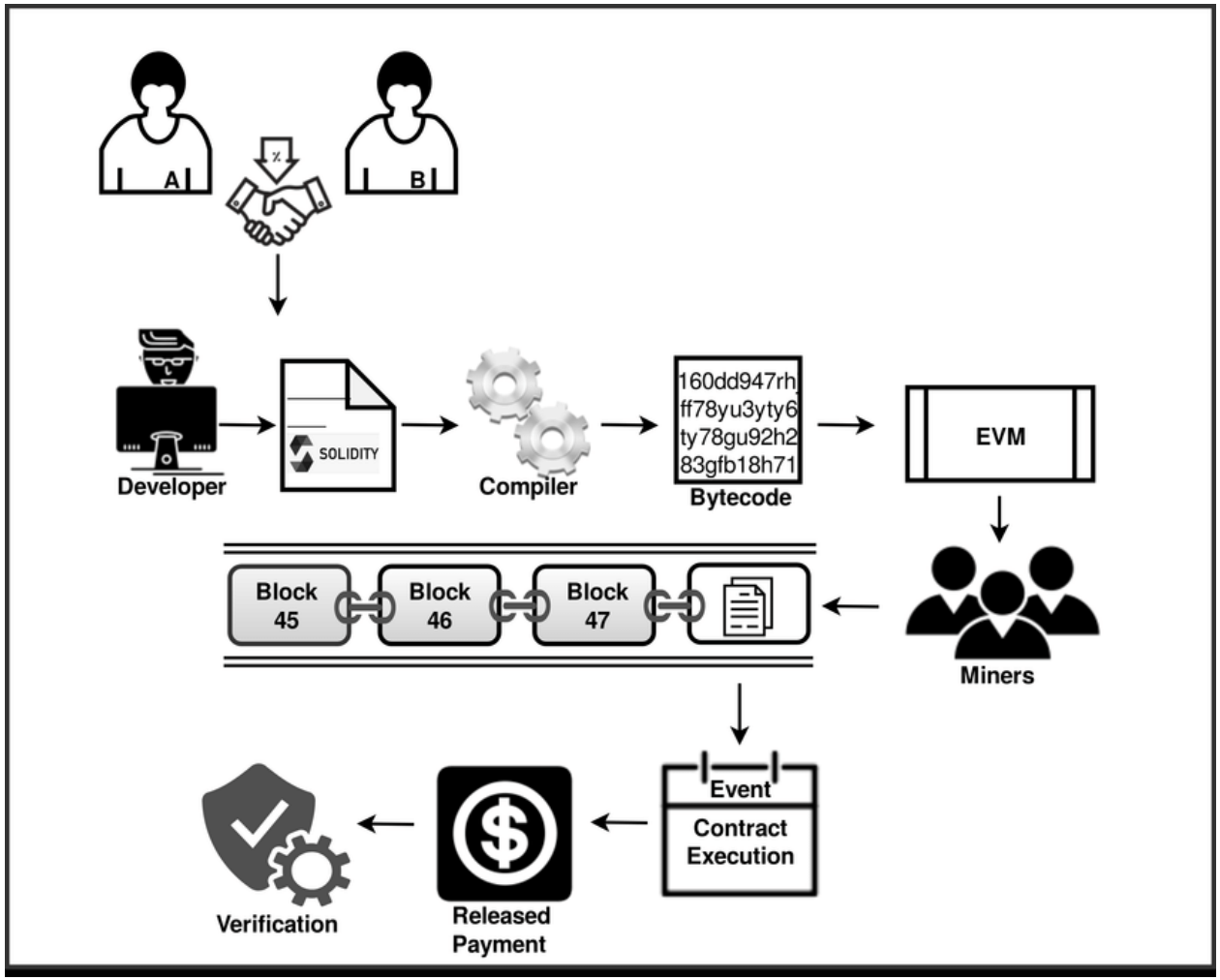
EcoMobiCoin: Proof of Behavior







Smart Contract



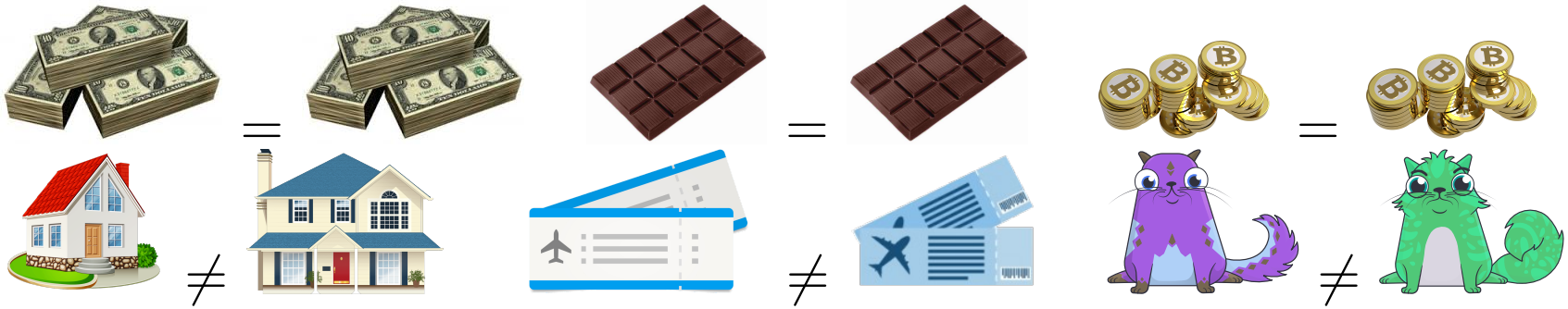
Smart Contract





Fungible vs Non-fungible Tokens

Fongible = interchangeable



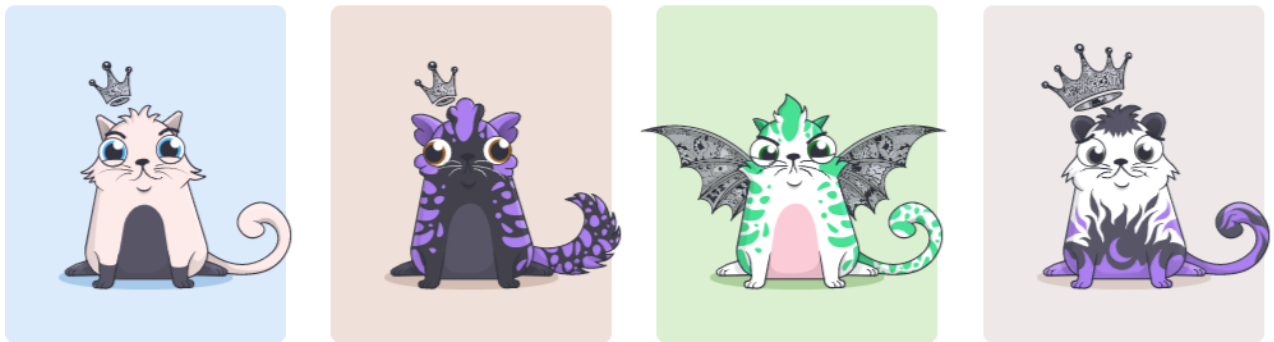
Non-fongible = individuel

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.



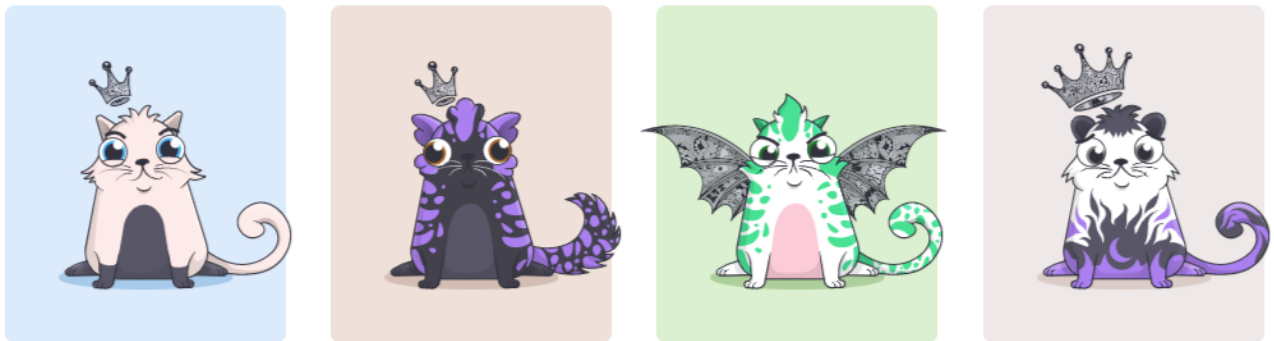
⇨Représente de manière unique des fichiers (image, vidéo, ...)

⇨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, ©beeple-crap.com



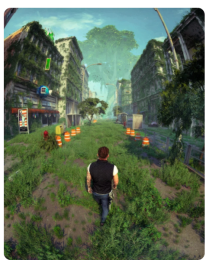
Everydays: the First 5000 Days, detail, *Shitshow*, Beeple, ©beeple-crap.com



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



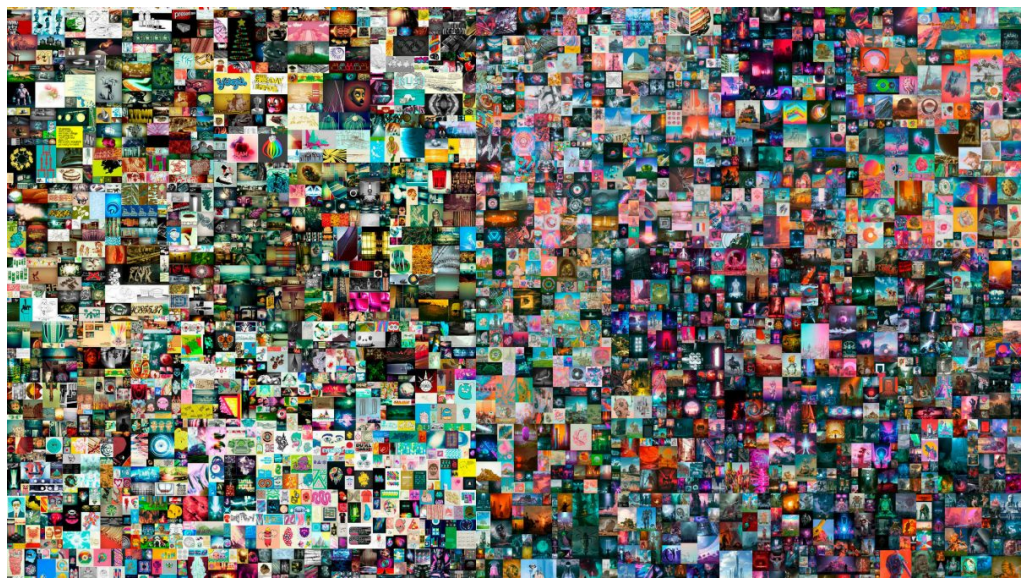
Everydays: the First 5000 Days, detail, *Carefree Goat*, Beeple, ©beeple-crap.com



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



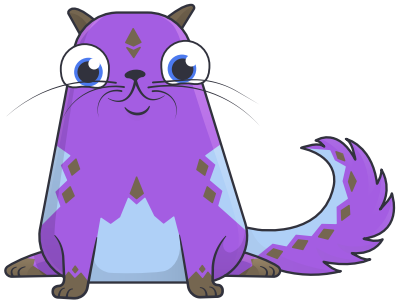
Everydays: the First 5000 Days, detail, *Worst Case*, Beeple, ©beeple-crap.com



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

CryptoKitties www.cryptokitties.co

#1353978 (Gén. 15) :



#1812662 (Gén. 4) :



#2011210 : offspring (Gén. 16)

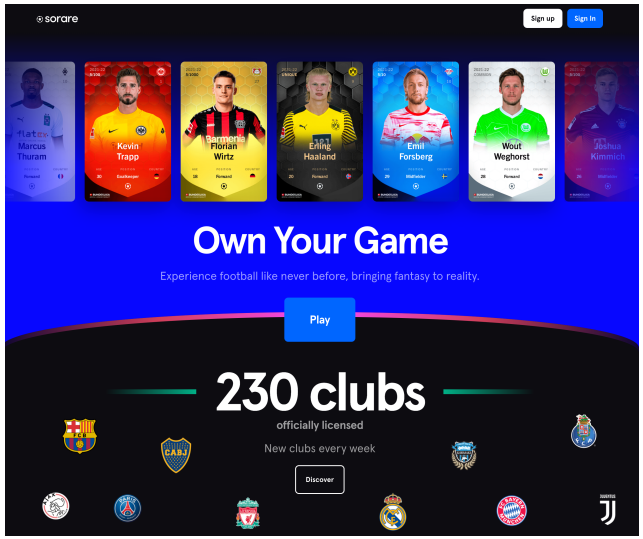


- Projet démarré en 2017 par Axiom Zen
  - Créatures uniques pouvant être échangées, collectionnées, avec reproduction (gérée par contrat intelligent) !
  - Ensemble de 512 bits :
    - 256 bits de gènes (couleur, yeux, queue, etc.) dominant ou récessifs
    - 256 bits pour la date de naissance, l'identité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

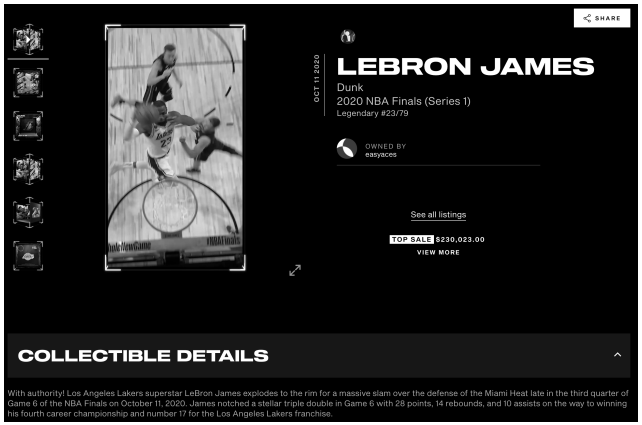
Sorare (Panini like)

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



NBA Top Shot

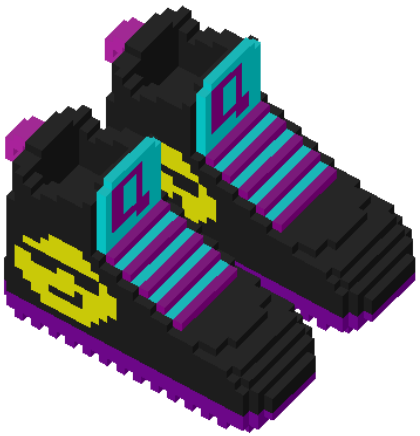
- Blockchain Flow
- "Moments" vidéo (dunk, block etc.) distribués par la NBA



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

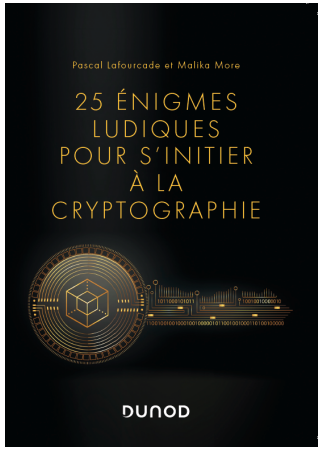
- La révolution Blockchain est en marche
- Un formidable outil
- Systèmes décentralisés
- De nombreuses applications mais bien comprendre les limites
- La cryptographie est au centre de la sécurité

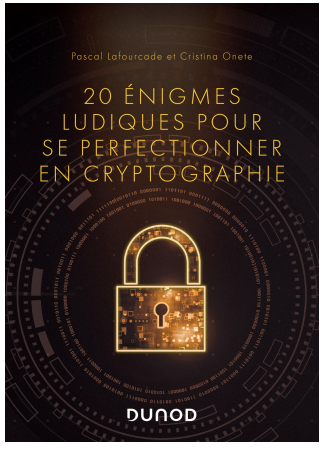
Merci pour votre attention

Questions ?













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

pascal.lafourcade@uca.fr