

Les **BLOCK CHAINS**

EN 50 QUESTIONS

Comprendre le fonctionnement et les enjeux
de cette technologie innovante



Bitcoin et la Blockchain

Pascal Lafourcade



Caen

16 mars 2023

Sumériens vers 3.500 av J.C



Qu'est-ce que la monnaie?

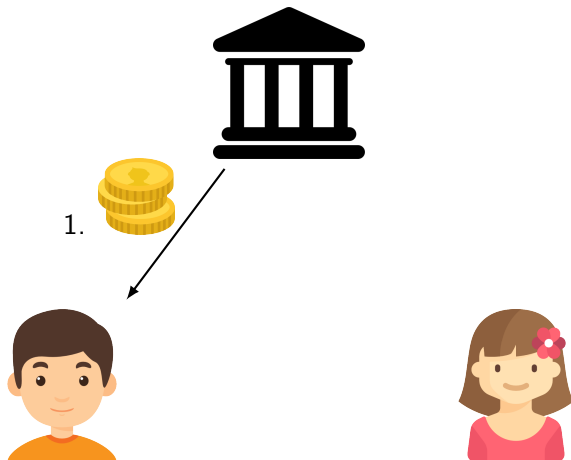


- ▶ Intermédiaire et moyens d'échanges de biens et services entre les individus
- ▶ Réserve de valeur
- ▶ Unité de compte

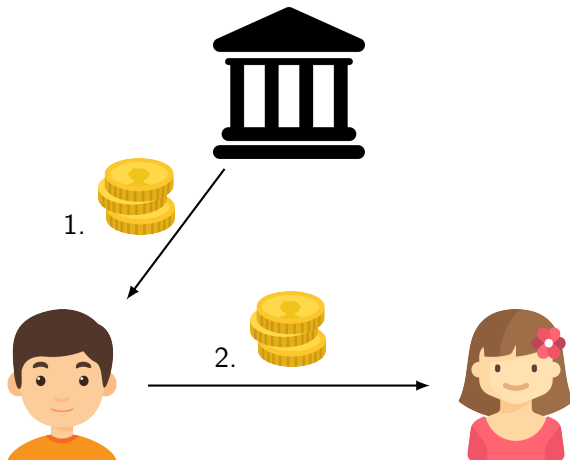
Nombreuses monnaies



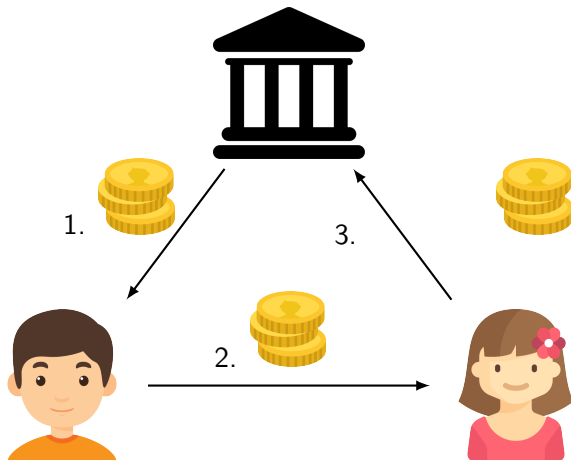
Principe : Banque centrale



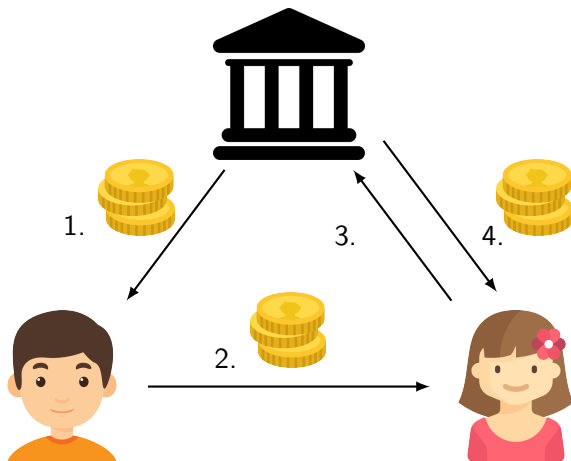
Principe : Banque centrale



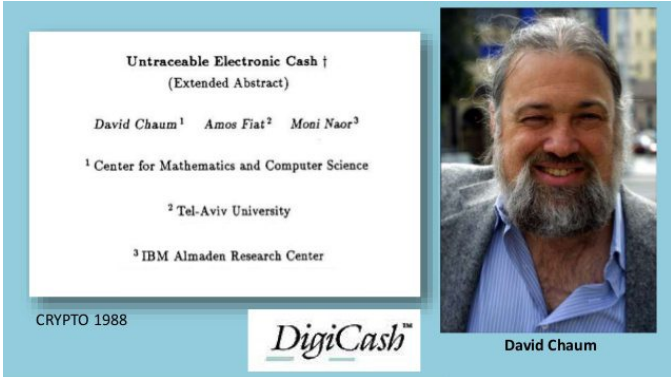
Principe : Banque centrale



Principe : Banque centrale



1988 : Digitcash



Untraceable Electronic Cash †
(Extended Abstract)

David Chaum¹ Amos Fiat² Moni Naor³


¹ Center for Mathematics and Computer Science

² Tel-Aviv University

³ IBM Almaden Research Center

CRYPTO 1988

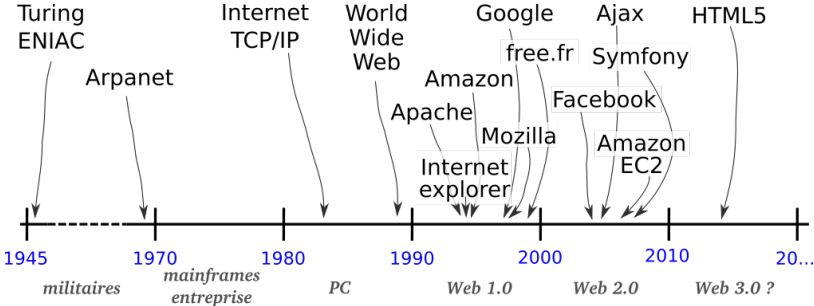
DigiCash™



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



▶ Monnaie

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

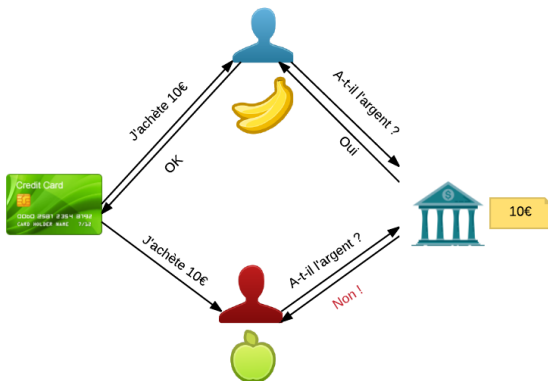
▶ Crypto-monnaie : monnaie électronique, se passant d'un Tiers

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

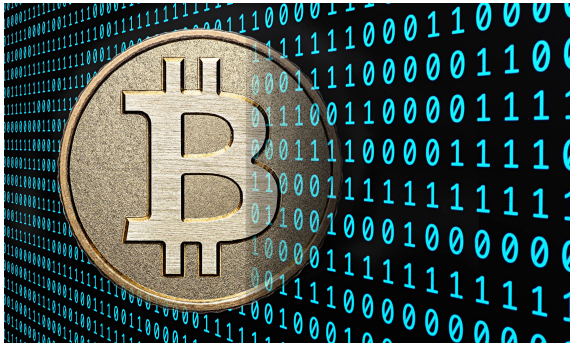
- ▶ Anonymat faible : non identification d'un acheteur
- ▶ Anonymat fort : non traçabilité d'un acheteur



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	✓	✓	✗

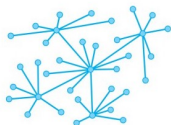
La révolution Bitcoin 2009



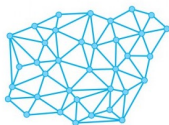
► Crypto-monnaie décentralisée et distribuée



Système centralisé



Système décentralisé



Système distribué

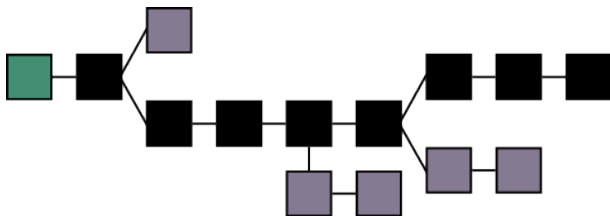


21 millions BTC

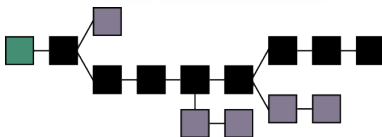
Inarrêtable car distribuée



Infalsifiable



Auditable



Bitcoin : monnaie électronique

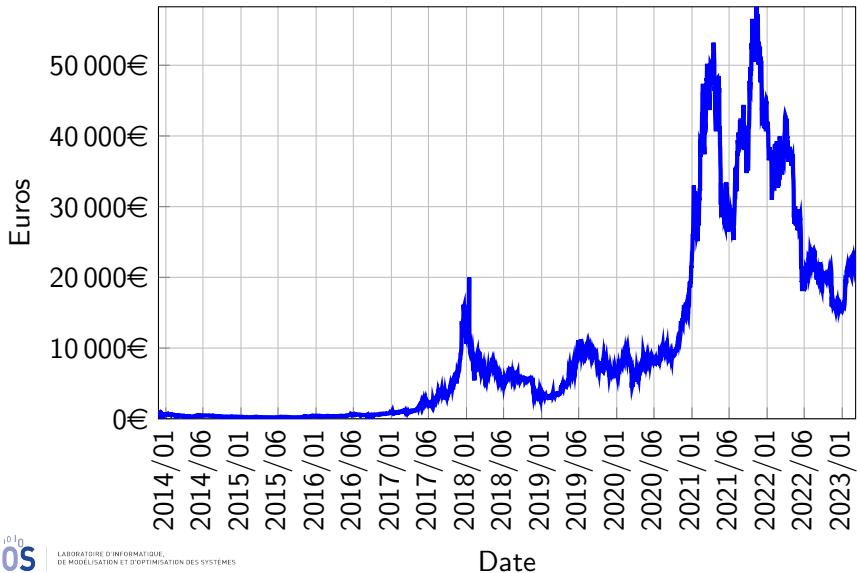
Créée en 2008 par Satoshi Nakamoto

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

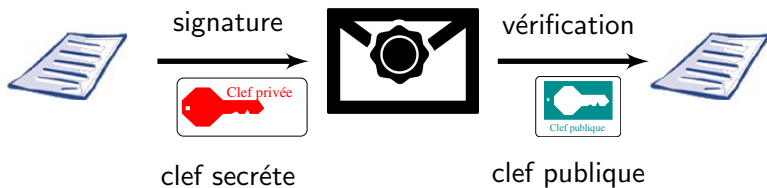


1	BTC = 1 Bitcoin	
0,01	BTC = 1 cBTC	= 1 centiBitcoin (ou bitcent)
0,001	BTC = 1 mBTC	= 1 milliBitcoin
0,000 001	BTC = 1 μ BTC	= 1 microBitcoin
0,000 000 01	BTC = 1 Satoshi	

Taux de change du bitcoin



Signature



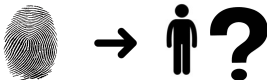
RSA: $m^d \bmod n$

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 :

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

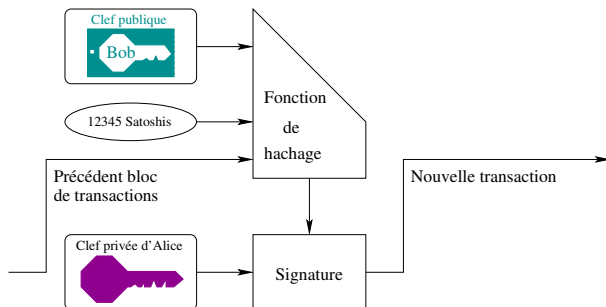
- ▶ Toutes les transactions sont **publiques**

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



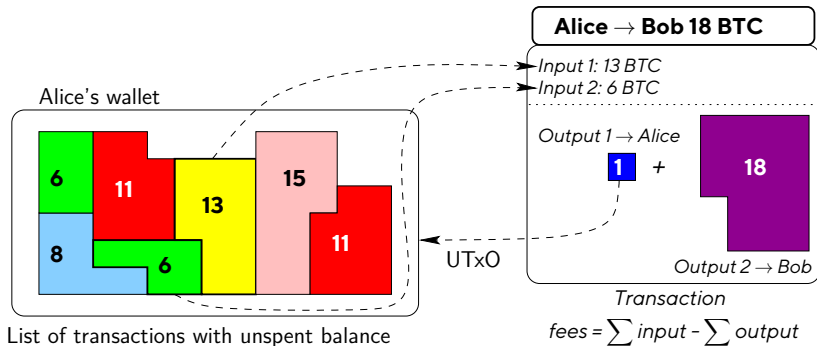
Comment faire une transaction?

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

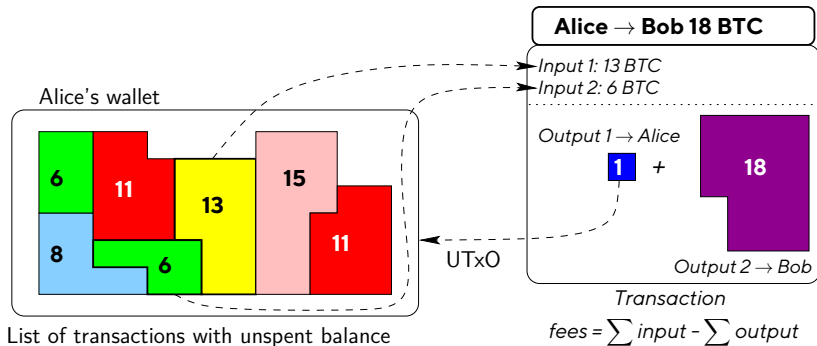


Unspent Transaction Output UTXO

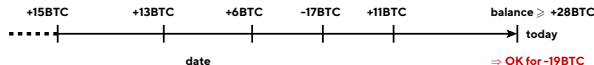
Pay 18 BTC with coins



Pay 18 BTC with coins



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



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

$$\text{SHA256}(A, B, 3, 424210) = 458237$$

Etat de la chaîne 458237

C donne à B 9 BTC

$$\text{SHA256}(C, B, 9, 458237) = 936127$$

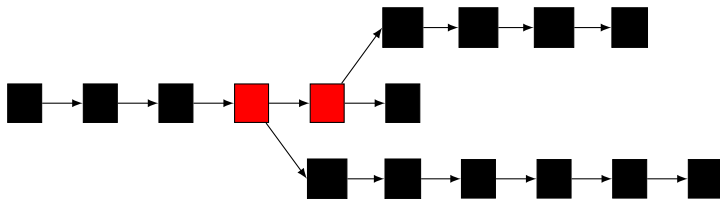
Etat de la chaîne 936127

C donne à A 1 BTC

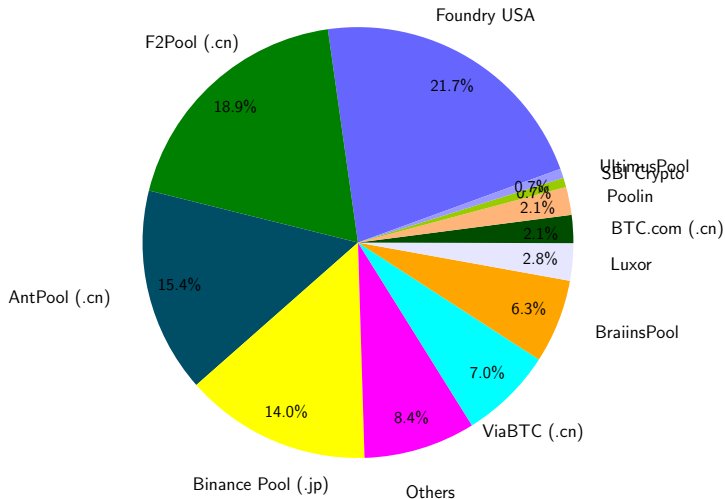
$$\text{SHA256}(C, A, 1, 936127) = 458237$$

Blockchain Infalsifiable

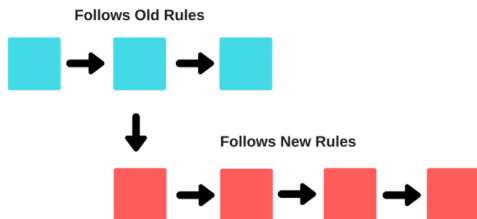
$$\begin{aligned} & \text{SHA256}(C, A, 1, \text{SHA256}(C, B, 9, \text{SHA256}(A, B, 3, 424210))) \\ = & \text{SHA256}(C, A, 1, \text{SHA256}(C, B, 9, 458237)) \\ = & \text{SHA256}(C, A, 1, 936127) \\ = & 458237 \end{aligned}$$



Fermes de mineurs: partagent les récompenses



Soft Fork

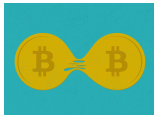


The primary difference between a soft fork and hard fork is that it is not backward compatible

Modification du code :

- ▶ Correction de bugs
- ▶ Améliorations consensuelles

Hard Fork



Bitcoin Blockchain, 1 MByte

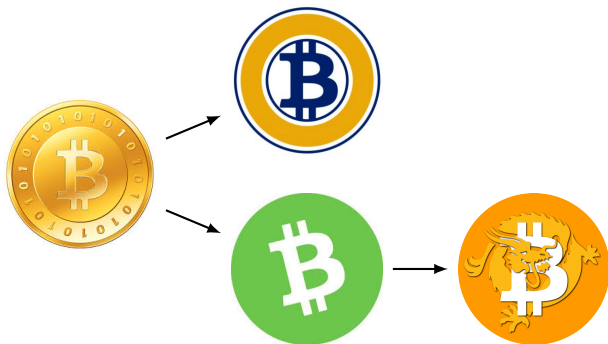


**Bitcoin Cash Blockchain,
8 MByte**



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 BZX = 1 BTC = 1 BZX
	Minc Bitcoin	MBC	Bitcoin	Wednesday, May 30, 2018	525000	1 BTC = 10000 MBC
	Classic Bitcoin	CBTC	Bitcoin	Sunday, April 01, 2018	516305	1 BTC = 10000 CBTC
	Bitcoin Life	BTCL	Bitcoin	Tuesday, January 30, 2018	0	1 BTC = 1 BTCL
	Bitcoin Atom	BGA	Bitcoin	Wednesday, January 24, 2018	508886	1 BTC = 1 BGA
	Bitcoin Interest	BCI	Bitcoin	Monday, January 22, 2018	506980	1 BTC = 1 BCI
	Bitcoinize	BTV	Bitcoin	Sunday, January 21, 2018	506050	1 BTC = 1 BTV
	Bitcoin Smart	BCS	Bitcoin	Sunday, January 21, 2018	505000	1 BTC = 100 BCS
	Bitcoin Prochain	BTR	Bitcoin	Wednesday, January 10, 2018	0	1 BTC = 1 BTR
	Bitcoin Private	BTCP	Bitcoin	Monday, January 07, 2018	0	1 BTC = 200 = 1 BTCP
	Bitcoin AB	BTA	Bitcoin	Monday, January 01, 2018	0	1 BTC = 1 BTA
	Bitcoin Pizza	BPK	Bitcoin	Monday, January 01, 2018	504888	1 BTC = 1 BPK
	BitcoinBay	BCB	Bitcoin	Sunday, December 31, 2017	501808	1 BTC = 100 BCB
	Bitcoin Oro	BDO	Bitcoin	Sunday, December 31, 2017	501940	1 BTC = 1 BDO
	Bitcoin Uranium	BUU	Bitcoin	Sunday, December 31, 2017	0	1 BTC = 1 BUU
	Quantum Bitcoin	QBTC	Bitcoin	Thursday, December 28, 2017	0	1 BTC = 1QBTC
	Bitcoin SegWizX v11	BZX	Bitcoin	Thursday, December 28, 2017	504401	1 BTC = 1 BZX
	Bitcoin Flu	BFI	Bitcoin	Wednesday, December 27, 2017	504225	1 BTC = 1000 BFI
	Bitcoin God	GOD	Bitcoin	Wednesday, December 27, 2017	504225	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 = 0.75N
	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	490777	1 BTC = 10000 BTW
	UnleashBitcoin	UB	Bitcoin	Tuesday, December 12, 2017	480777	1 BTC = 1 UB
	Bitcoin Hut	BTH	Bitcoin	Tuesday, December 12, 2017	480648	1 BTC = 100 BTH
	BitcoinK	BCK	Bitcoin	Tuesday, December 12, 2017	480688	1 BTC = 10000 BCK
	Super Bitcoin	SBTC	Bitcoin	Tuesday, December 12, 2017	480688	1 BTC = 1 SBTC
	Bitcoin Silver	BTSL	Bitcoin	Friday, December 01, 2017	0	1 BTC = 1 BTSL
	Bitcoin Nano	BTN	Bitcoin	Friday, December 01, 2017	501888	1 BTC = 1000 BTN
	Bitcoin Diamond	BDD	Bitcoin	Friday, November 24, 2017	490886	1 BTC = 10 BDD
	Bitcoin	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
	Byether	BT4	Bitcoin	Tuesday, August 01, 2017	476558	1 BTC = 1 BT4
	OH BTC	OBTC	Bitcoin	Tuesday, August 01, 2017	490888	1 BTC = 1 OBTC
	Bitcoin Cash	BCH / B	Bitcoin	Tuesday, August 01, 2017	476558	1 BTC = 1 BQHC / B
	Bitcoin Cash	BCH	Bitcoin	Tuesday, August 01, 2017	476558	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

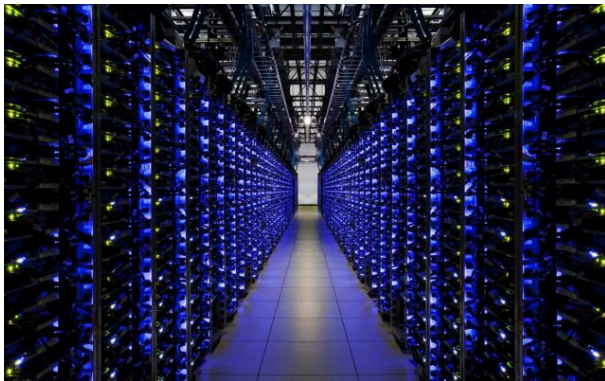


Lightning Network



ETHEREUM

12 secondes

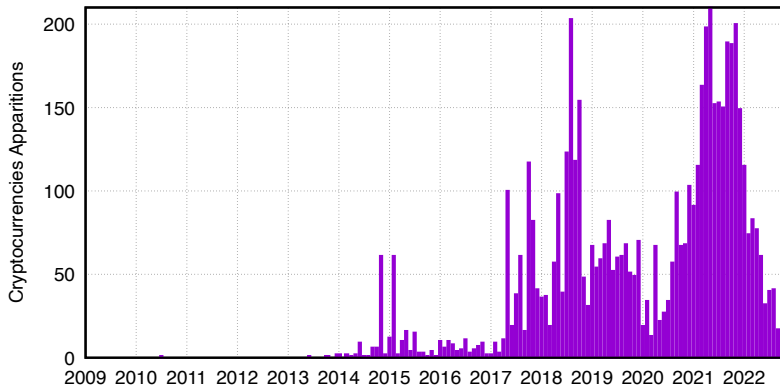


Proof of Stake Lightning Network

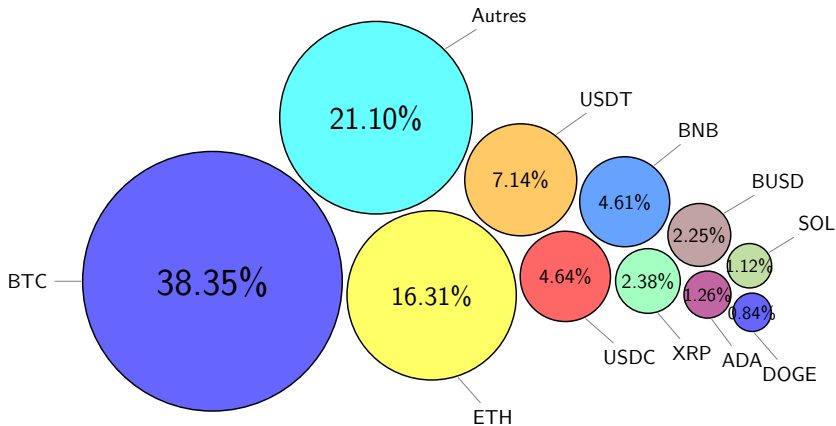
Autres crypto-monnaies



Autres crypto-monnaies



Diversité monétaire



Classification I : Pourris



Classification II : Clones de Bitcoin

STAR
WARS



STANDARD

CLONE
TROOPER



67th AIRSPEEDER CORPS
67th AIRSPEEDER CORPS



101ST RECON



75th SKY CORPS
51ST AIRBORNE DIVISION



99th ASSTLTROOPER
(COMMERCIAL BRAND)



82ND AIRSPEEDER CORPS



Classification III : Plus utile



Classification IV : Autres preuves de travail



Passage à l'échelle ?

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

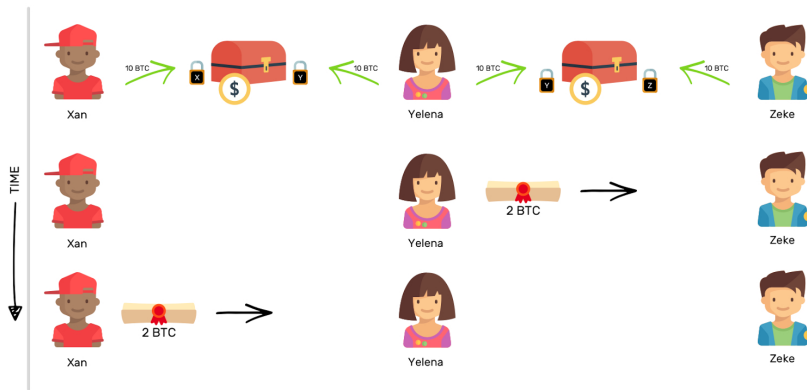
Passage à l'échelle ?

- ▶ 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

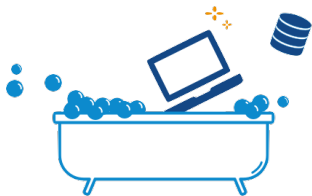
State Channel : Lightning Network



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



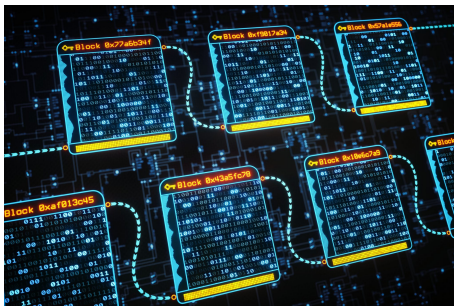
- ▶ Perte ou vol de la clef secrète = irréversible
- ▶ Monnaie anonyme et traçable



Blockchain

The St Lawrence				Starob Company (Limited)			
Incorporated by Letters Patent				under "The Companies Act"			
Capital \$8000 in				800 Shares of \$100 each.			
Limited				Liability			
First issue of 405				Shares \$40500			
<p>We the undersigned do hereby subscribe in the Capital Stock of the St Lawrence Starob and Co. Ltd and do assign promise and agree to pay the full amount of the said respective shares as shown by this stock book and the balance at such time and in such manner and amount as by the Directors & Provisional Directors of the said Company may be determined.</p>				<p>for the number of shares set opposite our respective names Company (Limited) and we do each for himself and himself to pay the full amount of the said respective shares as shown by this stock book and the balance at such time and in such manner and amount as by the Directors & Provisional Directors of the said Company may be determined.</p>			
Totals	Subscribers	Shares	Residence	No of Shares	Remarks	Witness	Amount
1899 Sept 11th Nov 29 Dec 5	29 Robt Kilgus 29 Chas. Nicholson 29 Joseph Wilson 5 Wm. Gray 5 Sam. Halperin		Toronto Toronto Toronto Cardinal Cardinal	One Hundred One Hundred Two One Hundred One One Hundred Six One Share		Wm. Gray Wm. Gray Wm. Gray Wm. Gray Wm. Gray	\$10,000.00 \$10,200.00 \$10,000.00 \$10,200.00 \$100.00

Blockchain

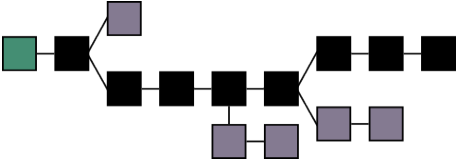


Registre distribué, sécurisé, infalsifiable

Mineurs valident des transactions



Tiennent à jour le registre distribué

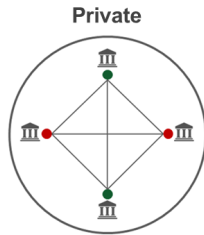
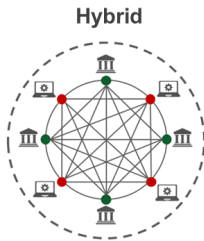
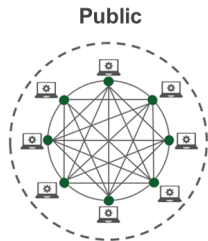


Inarrêtable, Infalsifiable, Auditable

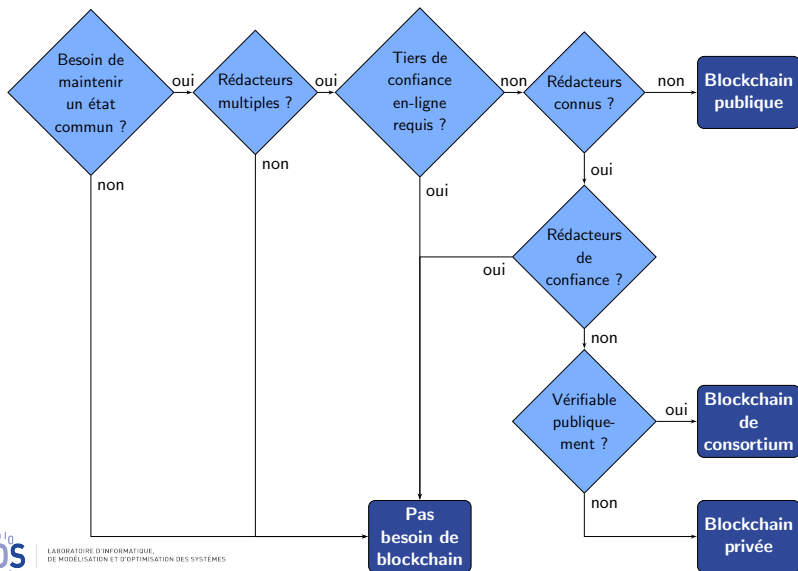
Décision des mineurs



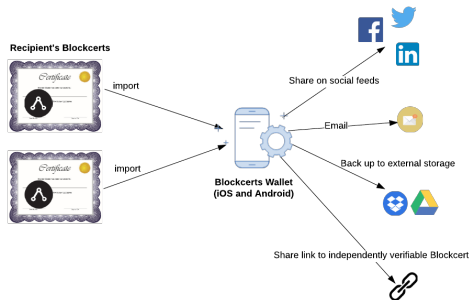
Blockchain Privée vs Publique



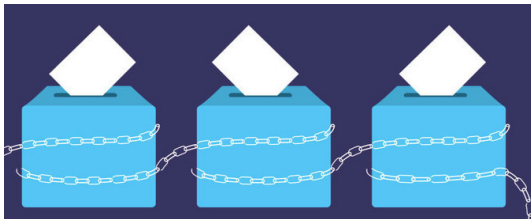
Ai-je besoin d'une blockchain ?



Blockchain Application : MIT Diploma



Blockchain Applications : Verify Your Vote, DABSTERS



Properties

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

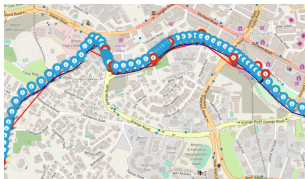
Blockchain Applications : Auction



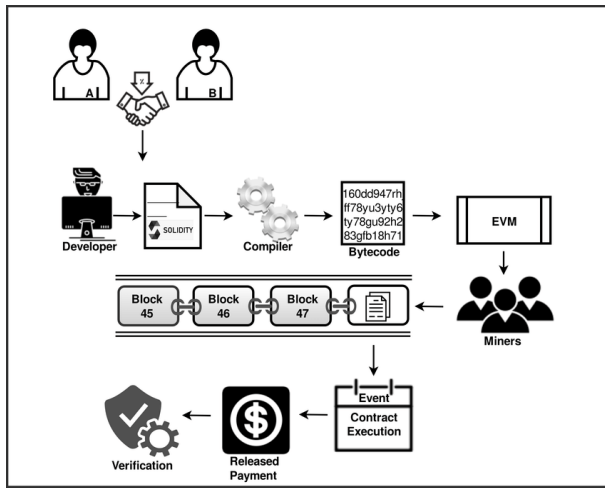
Properties

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

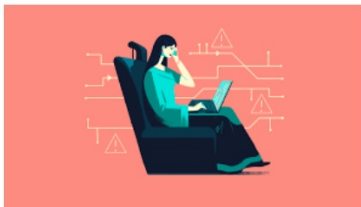
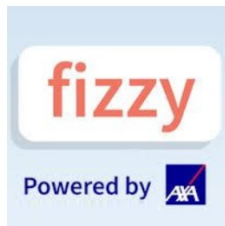
EcoMobiCoin: Proof of Behavior



Smart Contract

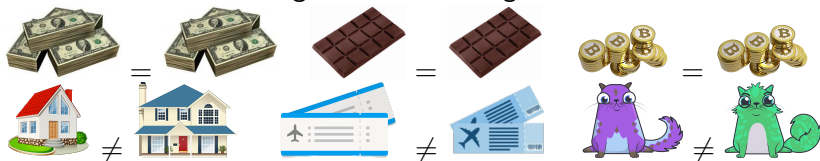


Smart Contract



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, ©beeple-crap.com



Everydays: the First 5000 Days, detail, Shockin', Beeple, ©beeple-crap.com



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



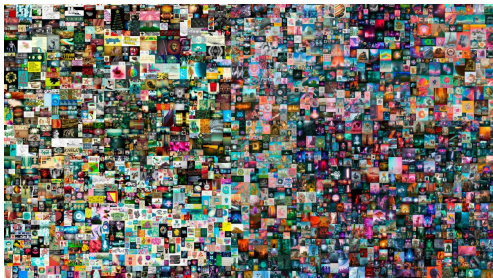
Everydays: the First 5000 Days, detail, Canine's Got, Beeple, ©beeple-crap.com



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



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



#1353978 (Gén. 15) :



#1812662 (Gén. 4) :



#2011210 : offspring (Gén.

16)

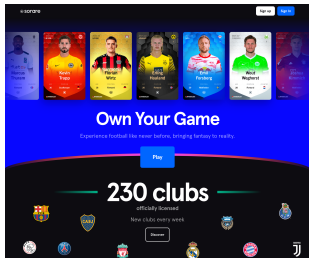


- ▶ Projet démarré en 2017 par Axiom Zen
 - ▶ Créatures uniques pouvant être échangées, collectionnées, avec reproduction (gérée par contrat intelligent) !
 - ▶ Ensemble de 512 bits :
 - ▶ 256 bits de gènes (couleur, yeux, queue, etc.) dominant ou récessifs
 - ▶ 256 bits pour la date de naissance, l'identité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

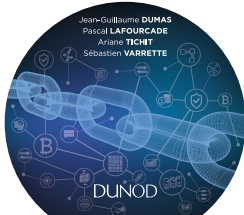
Merci pour votre attention

Questions ?

Les
**BLOCK
CHAINS**

EN 50 QUESTIONS

Comprendre le fonctionnement et les enjeux
de cette technologie innovante



pascal.lafourcade@uca.fr