

Les

BLOCK CHAINS

EN 50 QUESTIONS

Comprendre le fonctionnement et les enjeux
de cette technologie innovante



Introduction au fonctionnement de Bitcoin et de la Blockchain

Pascal Lafourcade



Tunis

18 mars 2021

Plan

Bitcoin

Altcoins

Blockchain

Conclusion

Plan

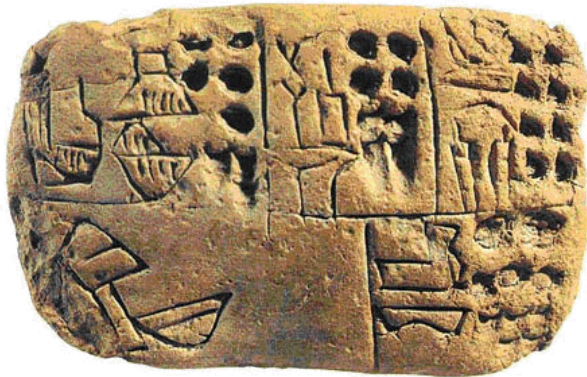
Bitcoin

Altcoins

Blockchain

Conclusion

Sumériens vers 3.500 av J.C



Qu'est-ce que la monnaie?

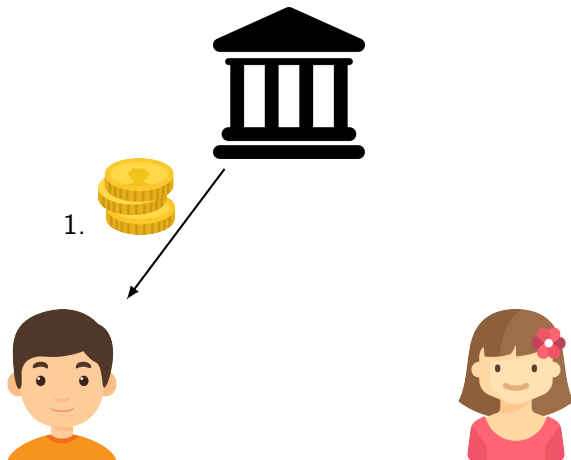


- ▶ Intermédiaire et moyens d'échanges de biens et services entre les individus
- ▶ Réserve de valeur
- ▶ Unité de compte

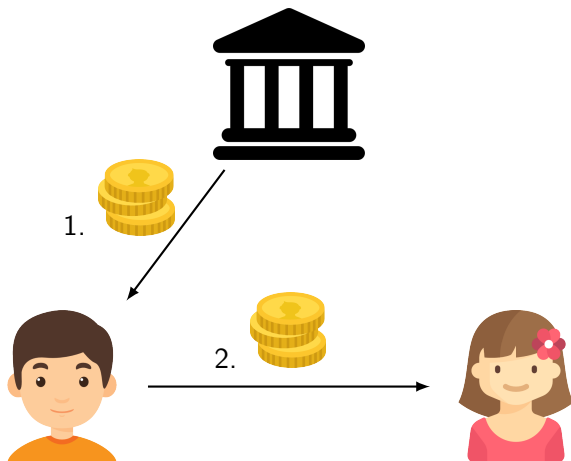
Nombreuses monnaies



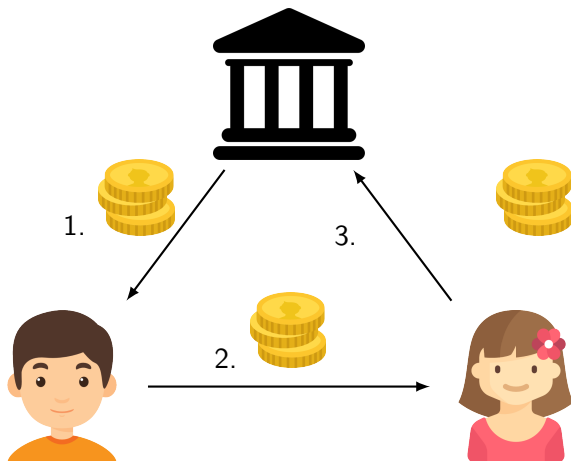
Principe : Banque centrale



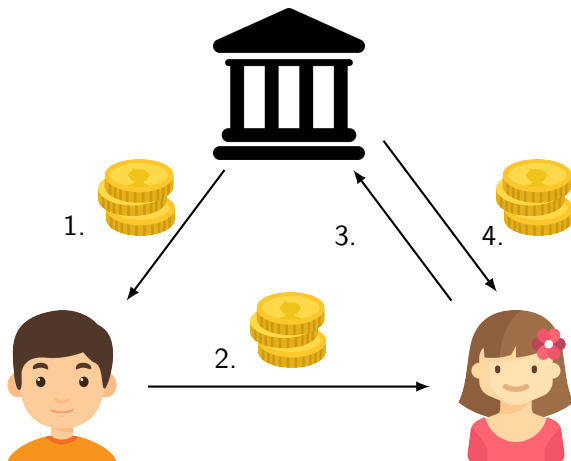
Principe : Banque centrale



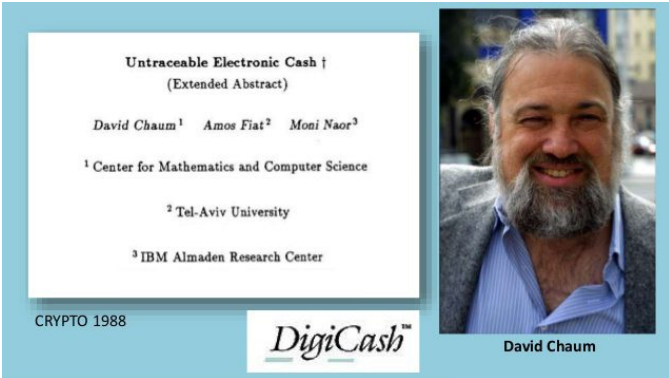
Principe : Banque centrale



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

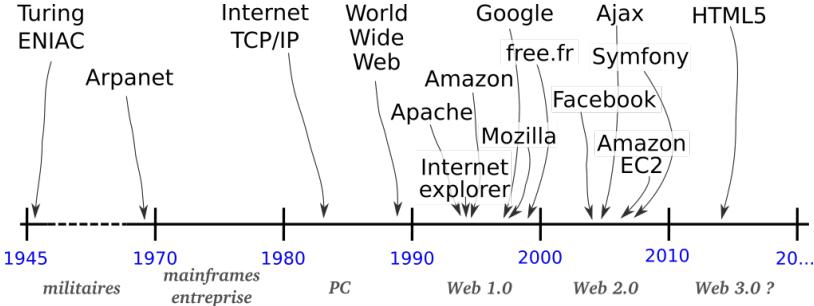
DigiCash[™]



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

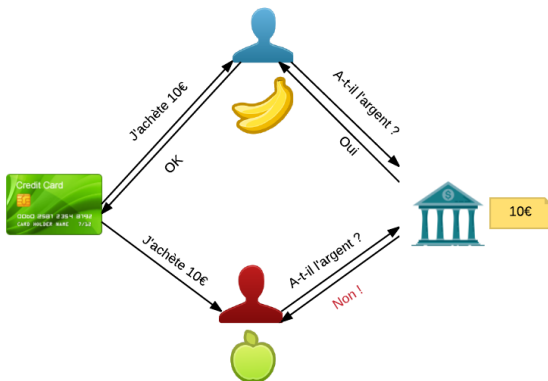
▶ Crypto-monnaie : monnaie électronique, se passant d'un Tiers

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	✓	✓	✗

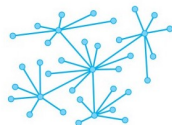
La révolution Bitcoin 2009



► Crypto-monnaie décentralisée et distribuée



Système centralisé



Système décentralisé



Système distribué

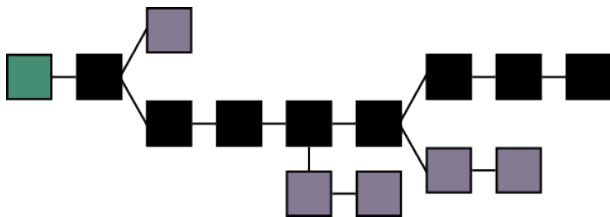


21 millions BTC

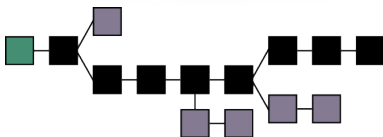
Inarrêtable car distribuée



Infalsifiable



Auditable



Bitcoin : monnaie électronique

Créée en 2008 par Satoshi Nakamoto (1 BTC \approx 945 euros)



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



Clef symétrique



Exemples

- ▶ DES
- ▶ AES

Chiffrement à clef publique



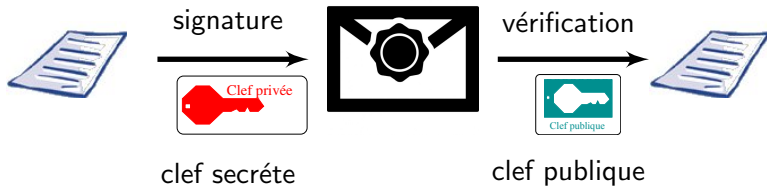
Exemples

- ▶ RSA : $c = m^e \pmod n$
- ▶ ElGamal : $c \equiv (g^r, h^r \cdot m)$

Signature

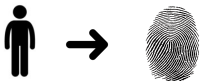


Signature



RSA: $m^d \bmod n$

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

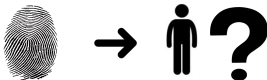


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)



Propriétés de résistance

► Pré-image

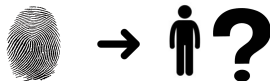


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)



Propriétés de résistance

▶ Pré-image



▶ Seconde Pré-image

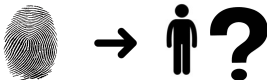


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)



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 :

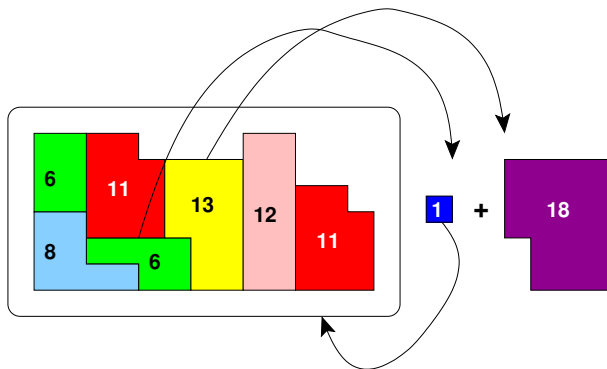
$\text{RIPEMD-160}(\text{SHA-256}(\text{ECDSA}_{pub}))$

- ▶ Toutes les transactions sont **publiques**

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



Payer 18 BTC avec des pièces



- Seuls des bitcoins possédés peuvent être dépensés

Porte-monnaie électronique

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

Où sont mes clefs privées ?

Solutions de portefeuille électronique

1. Sécurité
2. Disponibilité
3. Facilité

Solutions de portefeuille électronique

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

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



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

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

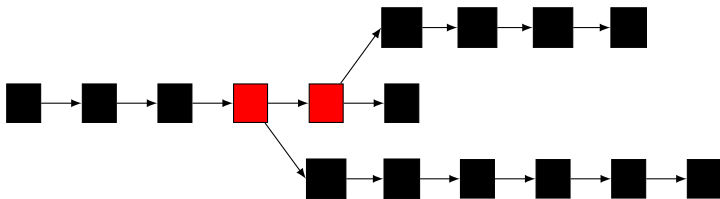
Etat de la chaîne 936127

C donne à A 1 BTC

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

Blockchain Infalsifiable

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



Hachage naïf : ASCIISUM

$$H(A, B, 3) = \text{ASCIISUM}(A, B, 3) = 65 + 66 + 51 = 132$$

dec	48	49	50	51	52	53	54	55	56	57
char	0	1	2	3	4	5	6	7	8	9
dec	65	66	67	68	69	70	71	72	73	74
char	A	B	C	D	E	F	G	H	I	J
dec	75	76	77	78	79	80	81	82	83	84
char	K	L	M	N	O	P	Q	R	S	T
dec	85	86	87	88	89	90				
char	U	V	W	X	Y	Z				

Simulateur de preuve de travail ASCII

ASCIISUM(ASCIISUM(A,B,1234, B_{i-1} ,nonce)) divisible par 3 et 5

dec	48	49	50	51	52	53	54	55	56	57
char	0	1	2	3	4	5	6	7	8	9
dec	65	66	67	68	69	70	71	72	73	74
char	A	B	C	D	E	F	G	H	I	J
dec	75	76	77	78	79	80	81	82	83	84
char	K	L	M	N	O	P	Q	R	S	T
dec	85	86	87	88	89	90				
char	U	V	W	X	Y	Z				

$$\begin{aligned} & \text{ASCIISUM}(\text{ASCIISUM}(A,B,1234,42,981)) \\ &= \text{ASCIISUM}(65+66+49+50+51+52+52+50+57+56+49) \\ &= \text{ASCIISUM}(597) = 53+57+55 = 165 \end{aligned}$$

Ensemble des 4 transactions disponibles

dec	48	49	50	51	52	53	54	55	56	57
char	0	1	2	3	4	5	6	7	8	9
dec	65	66	67	68	69	70	71	72	73	74
char	A	B	C	D	E	F	G	H	I	J
dec	75	76	77	78	79	80	81	82	83	84
char	K	L	M	N	O	P	Q	R	S	T
dec	85	86	87	88	89	90				
char	U	V	W	X	Y	Z				

Objectif de hachage :

$\text{ASCIISUM}(\text{ASCIISUM}(X, Y, \text{Montant}, B_{i-j}, \text{nonce}))$ divisible par 3 et 5

Hash du block précédent : 42

Alice donne à Dave 5 BTC : $A, D, 5$

Bob donne à Charlie 9 BTC : $B, C, 9$

Bob donne à Dave 7 BTC : $B, D, 7$

Charlie donne à Alice 3 BTC : $C, A, 3$

Quelques solutions

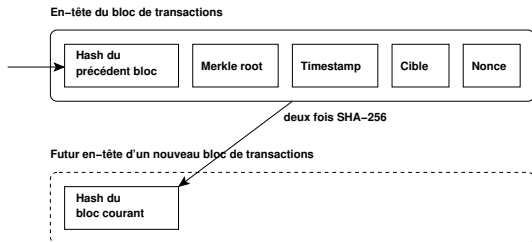
$\text{ASCIISUM}(\text{ASCIISUM}(A,D,5,42,1323)) = \text{ASCIISUM}(489) = 165$

$\text{ASCIISUM}(\text{ASCIISUM}(B,C,9,42,56)) = \text{ASCIISUM}(399) = 165$

$\text{ASCIISUM}(\text{ASCIISUM}(B,D,7,42,56)) = \text{ASCIISUM}(399) = 165$

$\text{ASCIISUM}(\text{ASCIISUM}(C,A,3,42,99)) = \text{ASCIISUM}(399) = 165$

Miner : Proof of work



Avoir un zéro de plus au début
SHA-256(SHA-256(en-tête de bloc))

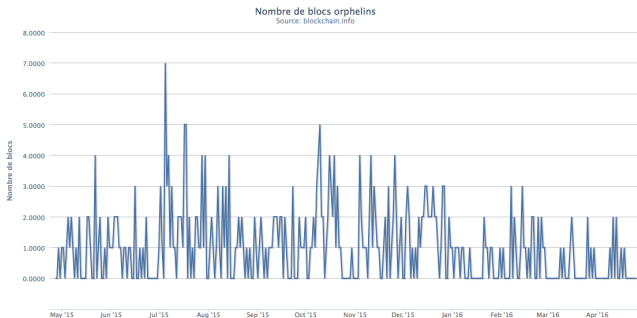
- ▶ les transactions passées (195 Go)
- ▶ les transactions à valider
- ▶ les secondes depuis 01/01/1970
- ▶ un nonce

Miner = Validation des transactions

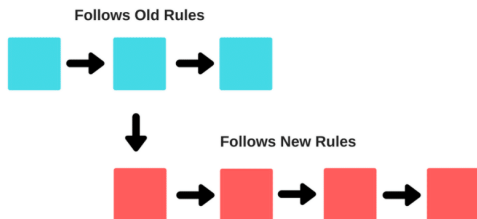
Cible: 00000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076



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



Soft Fork

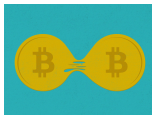


The primary difference between a soft fork and hard fork is that it is not backward compatible

Modification du code :

- ▶ Correction de bugs
- ▶ Améliorations consensuelles

Hard Fork



Bitcoin Blockchain, 1 MByte

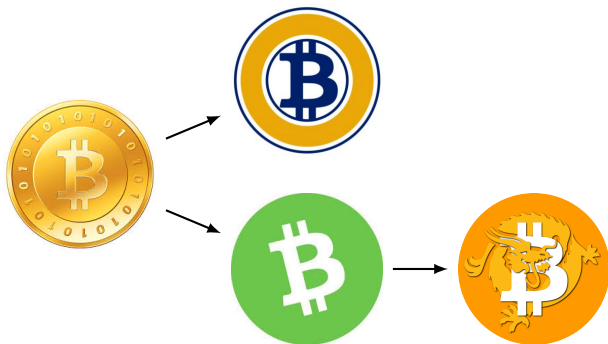


**Bitcoin Cash Blockchain,
8 MByte**



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 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	BI	Bitcoin	Monday, January 22, 2018	506980	1 BTC = 1 BI
	Bitcoinize	BTW	Bitcoin	Sunday, January 21, 2018	506050	1 BTC = 1 BTW
	Bitcoin Smart	BS	Bitcoin	Sunday, January 21, 2018	505000	1 BTC = 100 BS
	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	BU	Bitcoin	Sunday, December 31, 2017	0	1 BTC = 1 BU
	Quantum Bitcoin	QBTC	Bitcoin	Thursday, December 28, 2017	0	1 BTC = 1QBTC
	Bitcoin SegWizX v1.1	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 Gold	BGD	Bitcoin	Wednesday, December 27, 2017	504225	1 BTC = 1 BGD
	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	BTFF	Bitcoin	Tuesday, December 19, 2017	500000	1 BTC = 1 BTFF
	Bitcoin World	BTW	Bitcoin	Sunday, December 17, 2017	490777	1 BTC = 10000 BTW
	United Bitcoin	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
	Bytether	BTB	Bitcoin	Tuesday, August 01, 2017	476558	1 BTC = 1 BTB
	BitBTC	CBTC	Bitcoin	Tuesday, August 01, 2017	490888	1 BTC = 1 CBTC
	Bitcoin Cash	BCH / B	Bitcoin	Tuesday, August 01, 2017	476558	1 BTC = 1 BCH / B
	Bitcoin Cash	BCH	Bitcoin	Tuesday, August 01, 2017	476558	1 BTC = 1 BCH

Un hard fork rend-il plus riche ?

- ▶ Instantanément : doublement du nombre de pièces (même solde dans chaque branche)
- ▶ Pouvoir d'achat a priori inchangé à l'instant de la scission (répartition dans les deux monnaies)

L'exemple de Bitcoin Gold

23/10/2017 : BTC \approx 5 910\$

24/10/2017 : BTG \approx 480\$

25/10/2017 : BTC \approx 5 380\$

Un hard fork rend-il plus riche ?

- ▶ Instantanément : doublement du nombre de pièces (même solde dans chaque branche)
- ▶ Pouvoir d'achat a priori inchangé à l'instant de la scission (répartition dans les deux monnaies)
- ▶ **Ensuite : chaque crypto-monnaie fluctue en propre**

L'exemple de Bitcoin Gold

23/10/2017 : BTC \approx 5 910\$

24/10/2017 : BTG \approx 480\$

25/10/2017 : BTC \approx 5 380\$

10/03/2019 : BTC \approx 3 895\$

BTG \approx 12\$

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

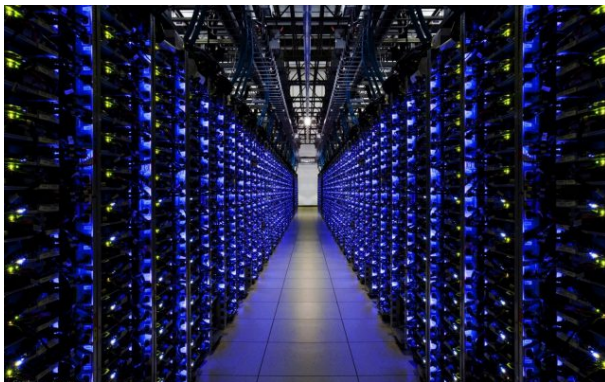


ETHEREUM

12 secondes

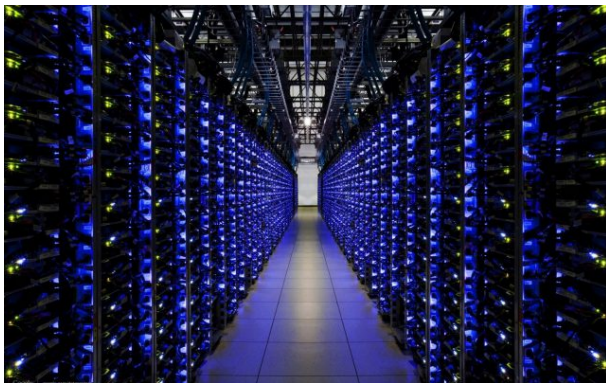
Energivore

Bitcoin 61,71 TWh/year = 6 585 585 US Houses/year

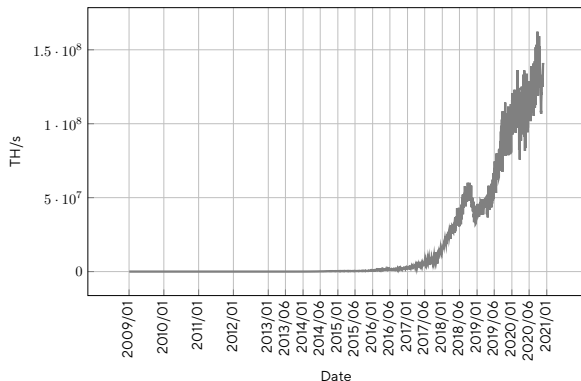


Energivore

Bitcoin 61,71 TWh/year = 6 585 585 US Houses/year



Proof of Stake
Lightning Network



Estimation: plusieurs TWh annuels (comparable à un petit état).

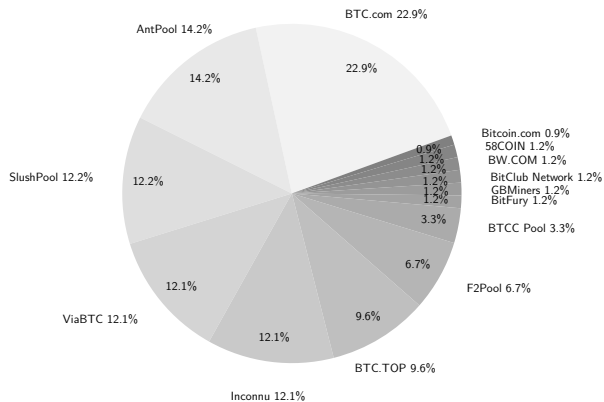
Un bloc toutes les 10 minutes

Machine	Type	Vitesse MH/s	Efficacité MH/J	Coût MH/s/€	Minage moyen Années/bloc
Core i5-2400	CPU	14	0.15	0.09	25.3 Millions
PS3	Cell	21	0.35	0.09	16.9 Millions
ATI 830	GPU	325	1.98	3.30	1.1 Millions
Ebit E11++	ASIC	44 000 000	22 200.00	8 885.00	13.6

- ▶ Cible : 74 zéros initiaux, $\frac{1}{2^{74}}$ chances de miner
- ▶ 44 000 000 MH/s = $4.4 \cdot 10^{13}$ H/s $\approx 2^{45.3}$ H/s
- ▶ $2^{28.7} \approx 4.3 \cdot 10^8$ s $\approx 5\,000$ jours \approx **13.6 années** de calcul d'un Ebit E11++
- ▶ Réseau mondial \approx **700 000 E11**



Fermes de mineurs



Plan

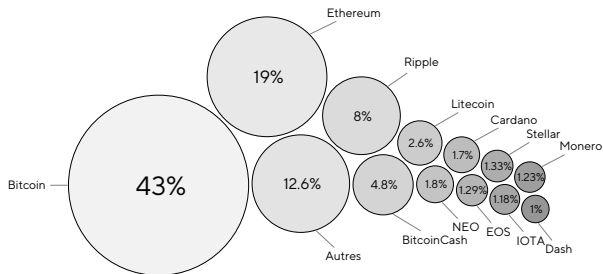
Bitcoin

Altcoins

Blockchain

Conclusion

Diversité monétaire



Autres crypto-monnaies



Classification I : Pourris



Classification II : Clones de Bitcoin

STAR
WARS



UNARMED

CLONE
TROOPER



6TH MANDALAY CORPS
66TH LEGION CORPS



501ST LEGION



75th INFANTRY
51ST AIRBORNE DIVISION



99TH TROOPER
COMMANDO BRIGADE



82ND AIRBORNE CORPS



Classification III : Plus utile



Classification IV : Autres preuves de travail

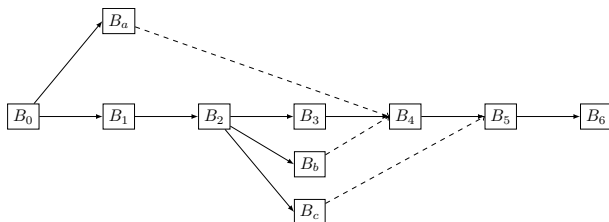


Unité	wei
wei	1 wei
Kwei (babbage)	10^3 wei
Mwei (lovelace)	10^6 wei
Gwei (shannon)	10^9 wei
microether (szabo)	10^{12} wei
milliether (finney)	10^{15} wei
ether	10^{18} wei



Vitesse : 12 secondes

Récompenser les oncles



B_4 reçoit $3 \times \left(1 + \frac{2}{32}\right) = 3.185$ ethers

B_b reçoit $\frac{7}{8} \times 3 = 2.625$ ethers, B_a reçoit $\frac{5}{8} \times 3 = 1.875$ ethers

Peercoin : Âge des pièces

Pour 10 pièces

Jours	0	1	2	...
Âge	10	10	20	...

Après V 0.3 :

- ▶ Attendre 30 jours
- ▶ Maximum 90 jours



Peercoin : Âge des pièces

Pour 10 pièces

Jours	0	1	2	...
Âge	10	10	20	...



Après V 0.3 :

- ▶ Attendre 30 jours
- ▶ Maximum 90 jours

Objectif de hachage

$$H < C \times A \times \frac{1}{2^{32 \times D}}$$

- ▶ C : Nombre de pièces
- ▶ A : Âge jour des pièces
- ▶ D : Difficulté

Scalability ?

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

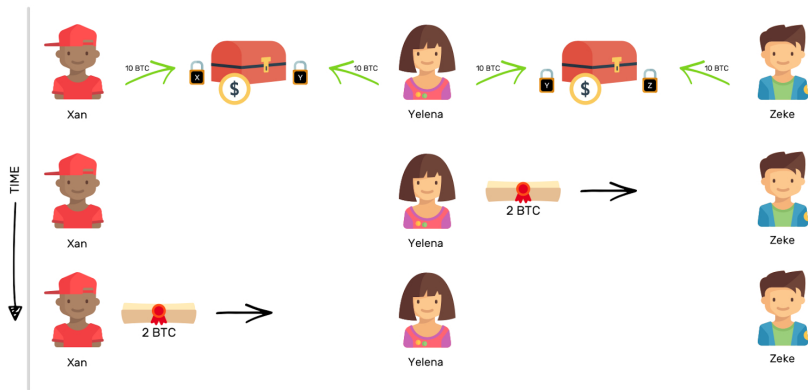
Scalability ?

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

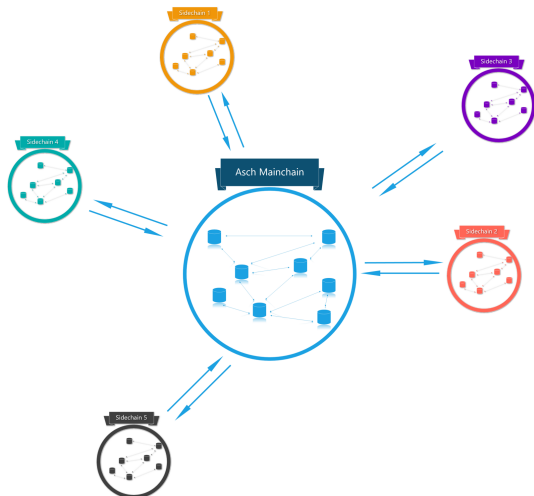
Solutions:

- ▶ Extend the block size
- ▶ Decrease the block interval
- ▶ Reduce the number of transactions on the chain :
 1. State Channel (BitcoinJ, Lightning Network, Rrainden Network, Sprites, REvive, Rapido, Duplex Micropayment Channel, Channel Factory ...)
 2. Side Chain (Pegged Sidechain, Minimal Viable Plasma, Plasma Cash)

State Channel : Lightning Network



Side Chain Idea



Limitations:

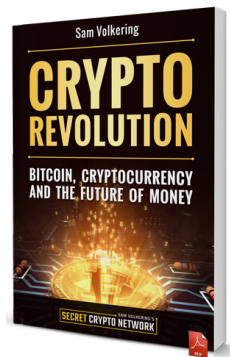
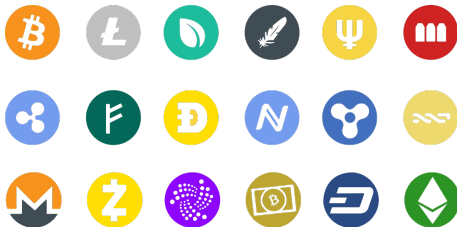
State Channel

- ▶ Intermediate amount or failure
- ▶ Continuous internet connection
- ▶ Solution uses watchtowers (energy consumption)

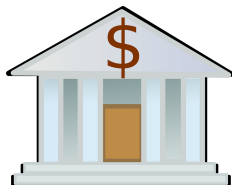
Side Chain

- ▶ Massive withdraw implies congestion on the main chain

Pluriculture des créations monétaires



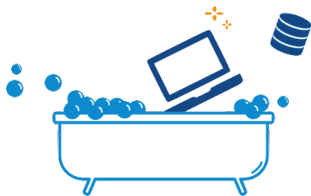
Qui s'approprie ces nouvelles monnaies ?



Un exemple : Ğ1



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



Plan


Bitcoin

Altcoins

Blockchain

Conclusion

Blockchain

The St Lawrence				Starb 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 Starb 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 rate as the Board of 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 rate as the Board of Directors of the said Company may be determined.</p>			
Trade	Subscribers	Shares	Residence	No of Shares	Remarks	Witness	Amount
1899 Sept 11th Nov 29 Dec 5	Robt Kilgus Chas. Nicholson Joseph Wilson John Gray Samuel Halperin		Toronto Toronto Toronto Cardinal Cardinal	one Hundred one hundred two one hundred one hundred two one share		Atkinson Atkinson Atkinson Mainway Mainway	\$10,000.00 \$10,200.00 \$10,000.00 \$10,200.00 \$100.00

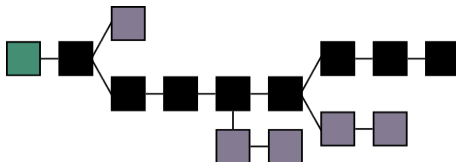
Blockchain



Registre distribué, sécurisé, infalsifiable

Fondamentaux d'une blockchain

- ▶ Registre distribué
 - ⇒ tous les participants ont une copie
- ▶ Protocole de consensus
 - ⚠ instant t , quelle est la copie officielle ?
- ▶ Crypto-monnaie
 - 👍 incitation à participer



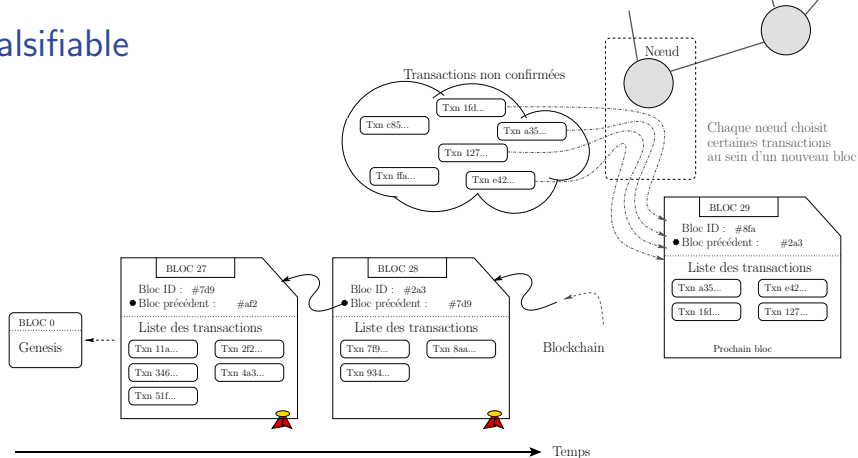
Inarrêtable, Infalsifiable, Auditable

Mineurs valident des transactions



Tiennent à jour le registre distribué

Infalsifiable



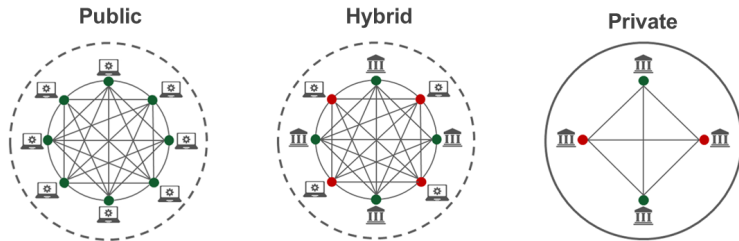
- ▶ Un résumé de chaque bloc de transaction est ajouté à chaque nouveau bloc de transactions
- ▶ **La copie** valide est sélectionnée aléatoirement & uniformément

En cas de doute, seule **la plus longue chaîne** persiste

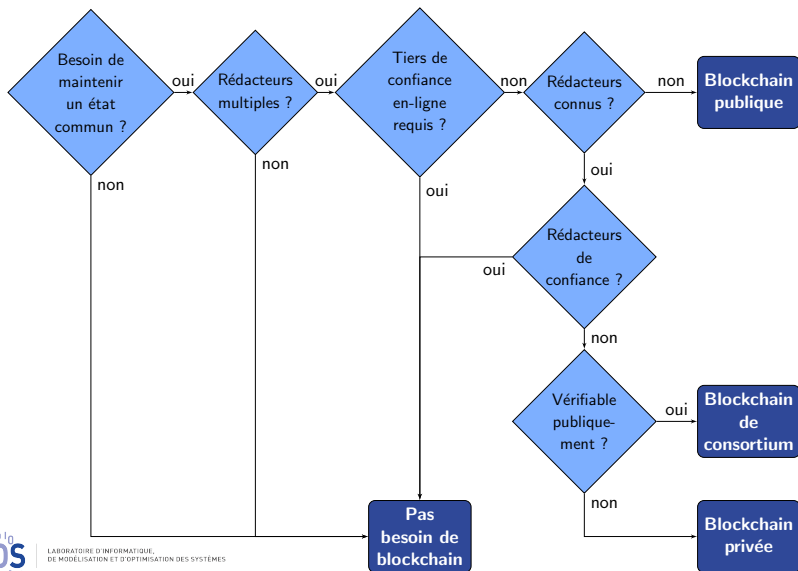
Décision des mineurs



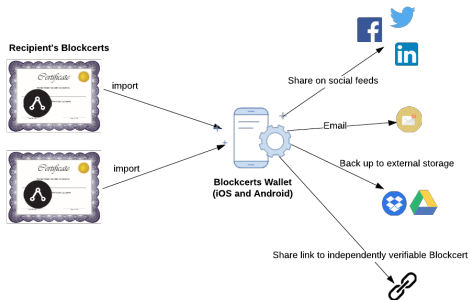
Blockchain Privée vs Publique



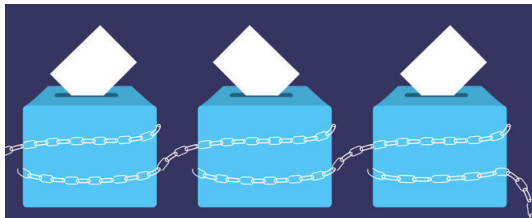
Ai-je besoin d'une blockchain ?



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 ...



Certificates (Laposte, EDF ...)

E-commerce

E-Health

...

Plan

Bitcoin

Altcoins

Blockchain

Conclusion

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