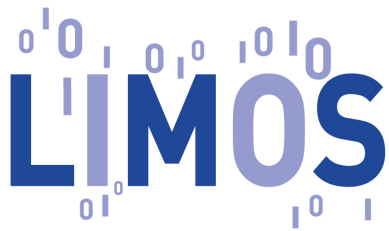
Comment fonctionne Bitcoin et la Blockchain ?

Pascal Lafourcade



Université Ouverte
Avril 2019

Plan

Plan

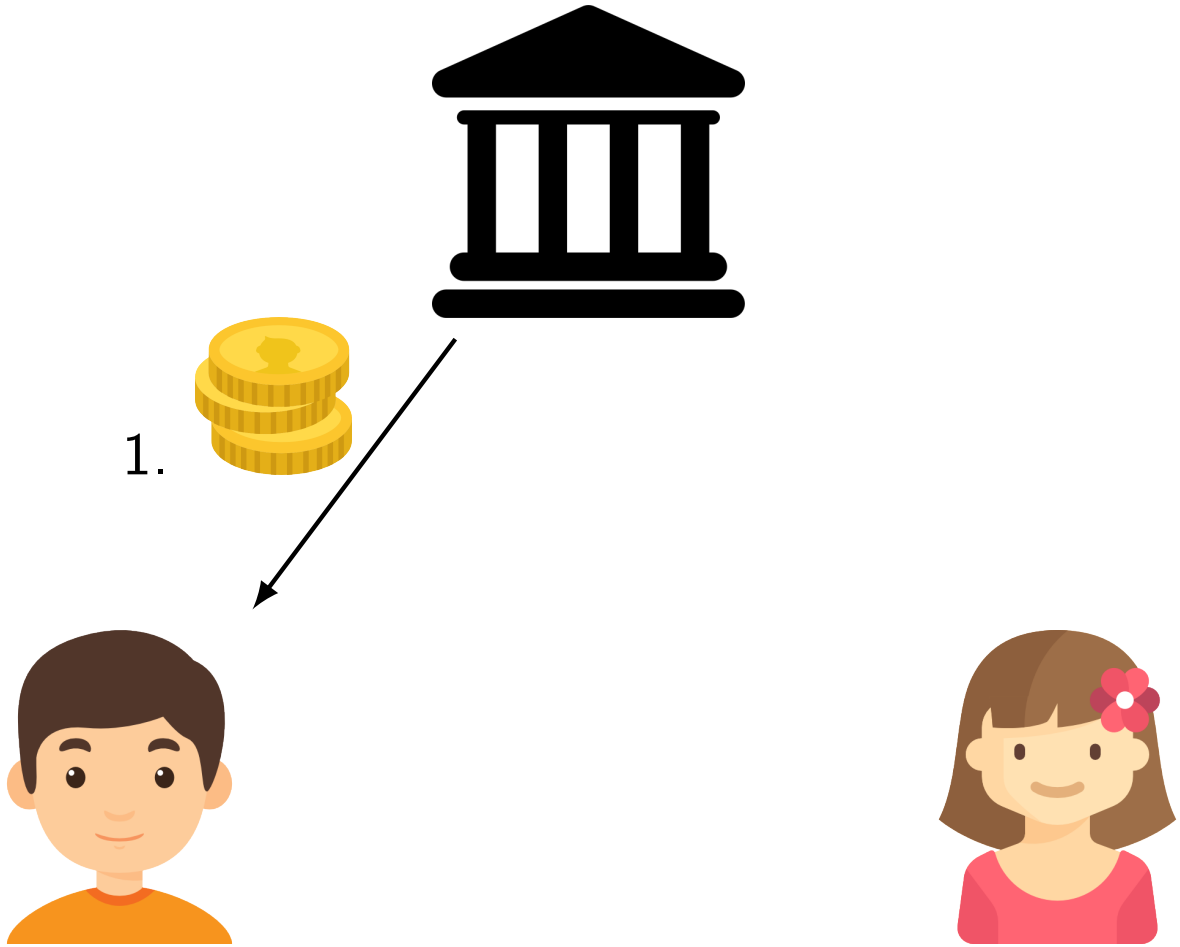
Sumériens vers 3.500 av J.C

Qu'est-ce que la monnaie?

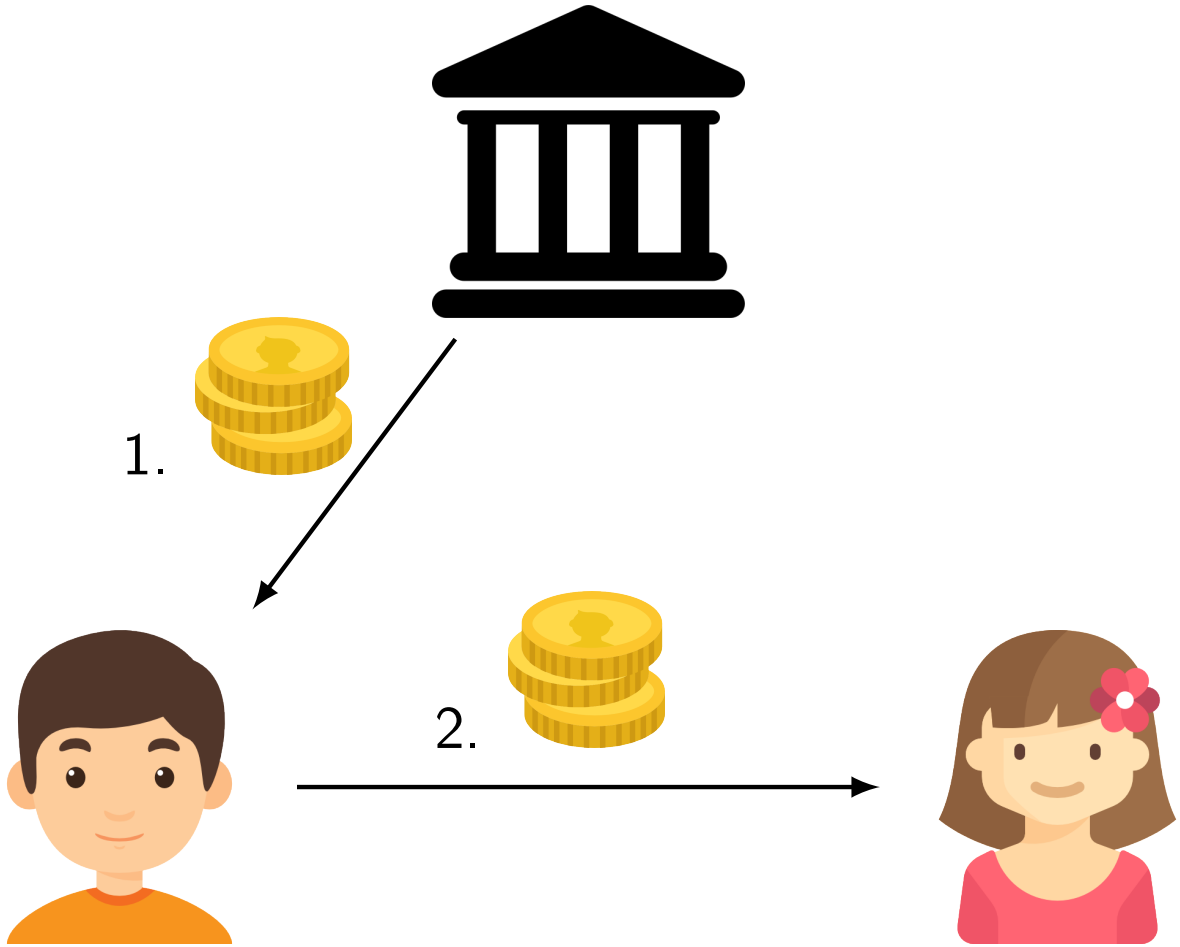
- Intermédiaire et moyens d'échanges de biens et services entre les individus
- Réserve de valeur
- Unité de compte

Nombreuses monnaies

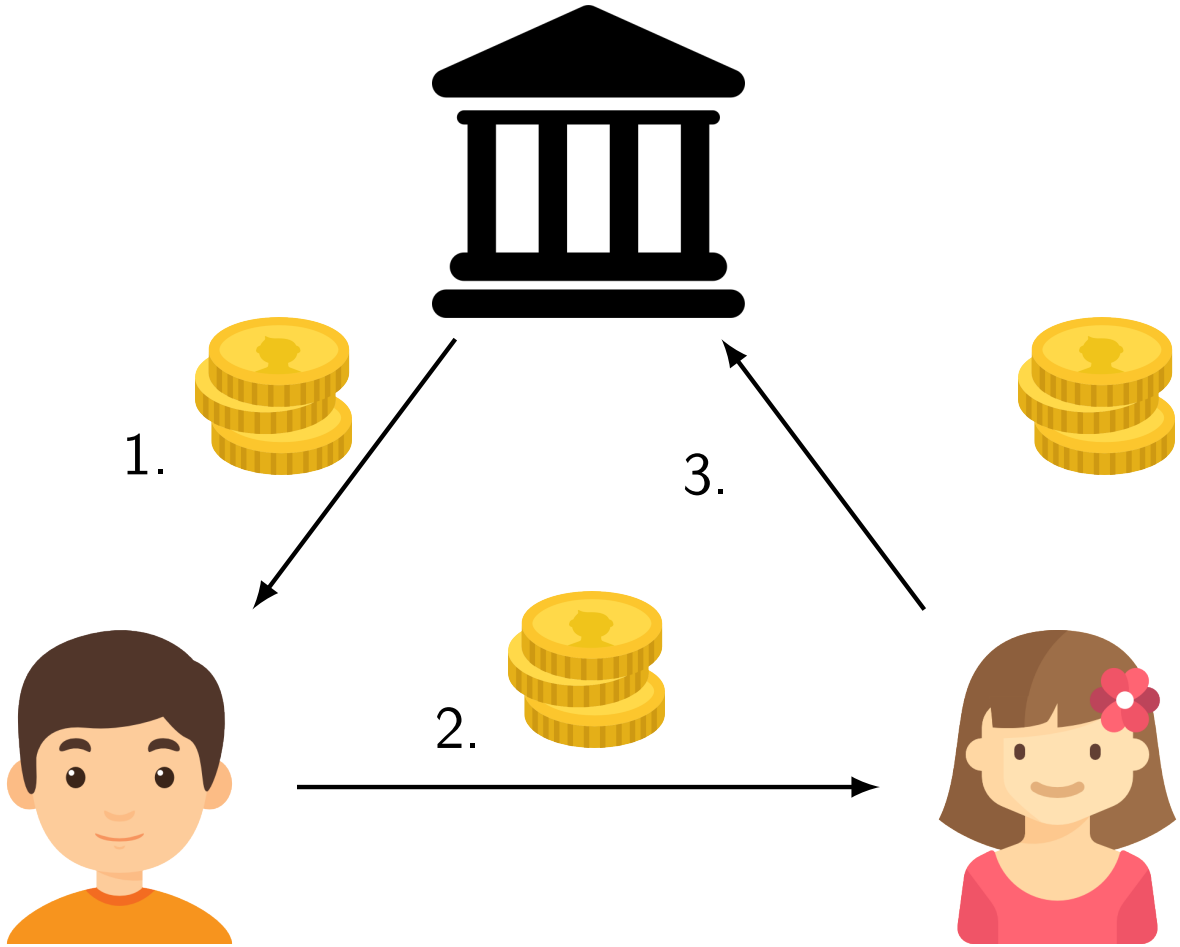
Principe : Banque centrale



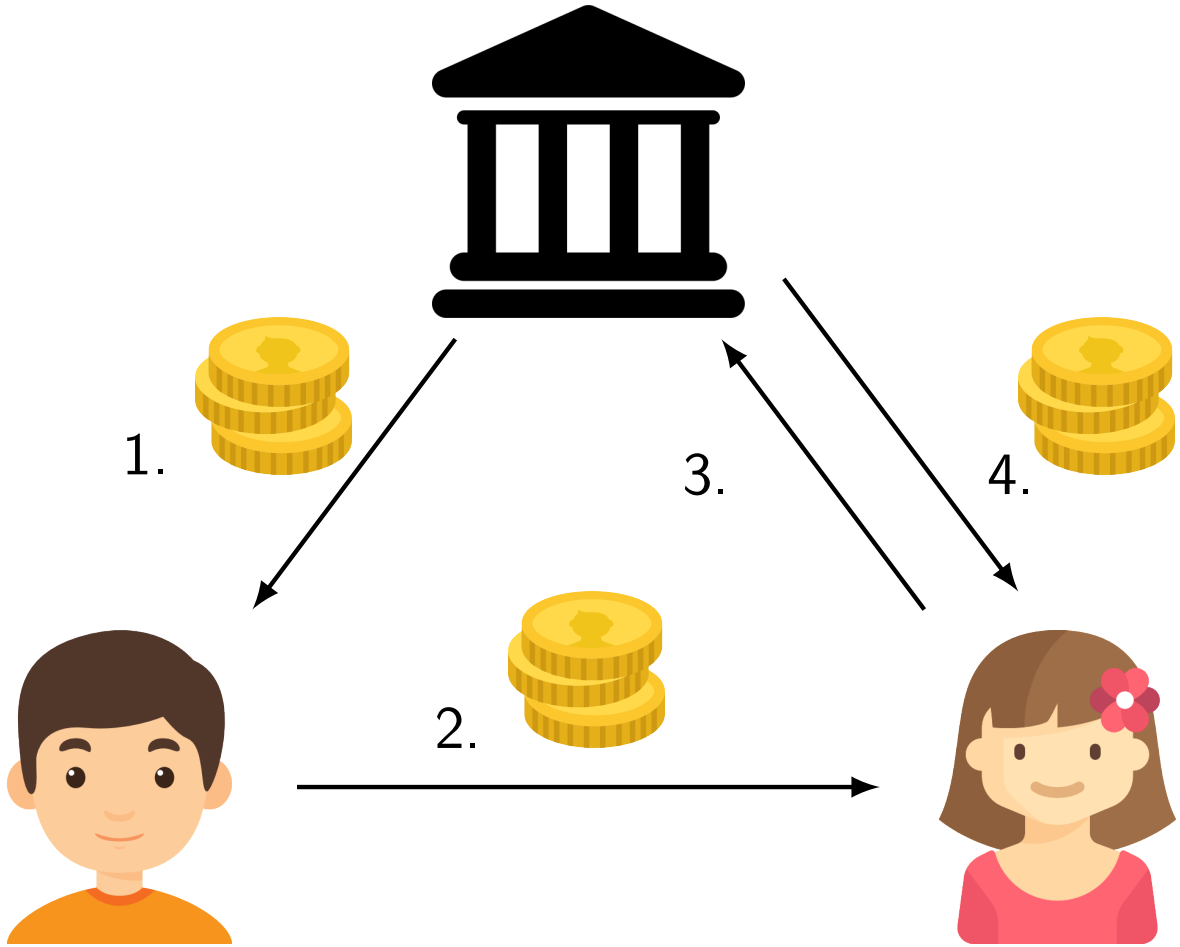
Principe : Banque centrale



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

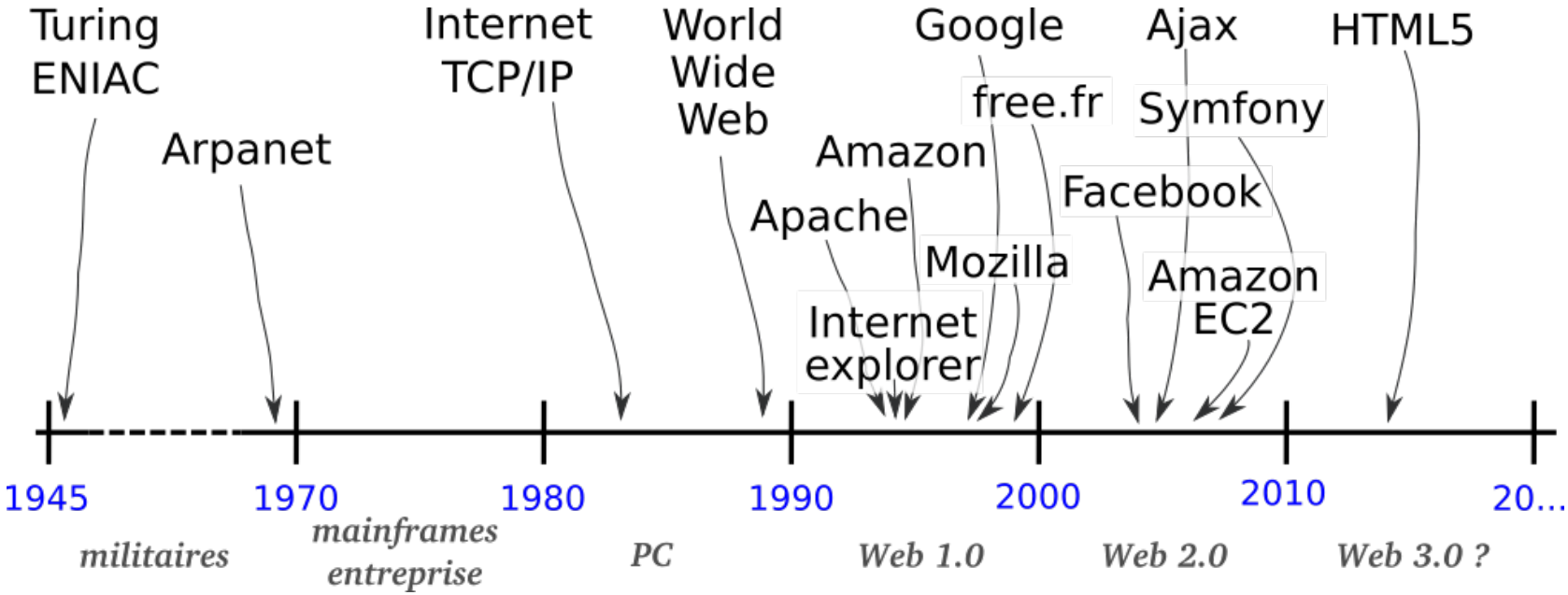
DigiCash™

David Chaum

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

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

Une idée visionnaire en avance sur son temps



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

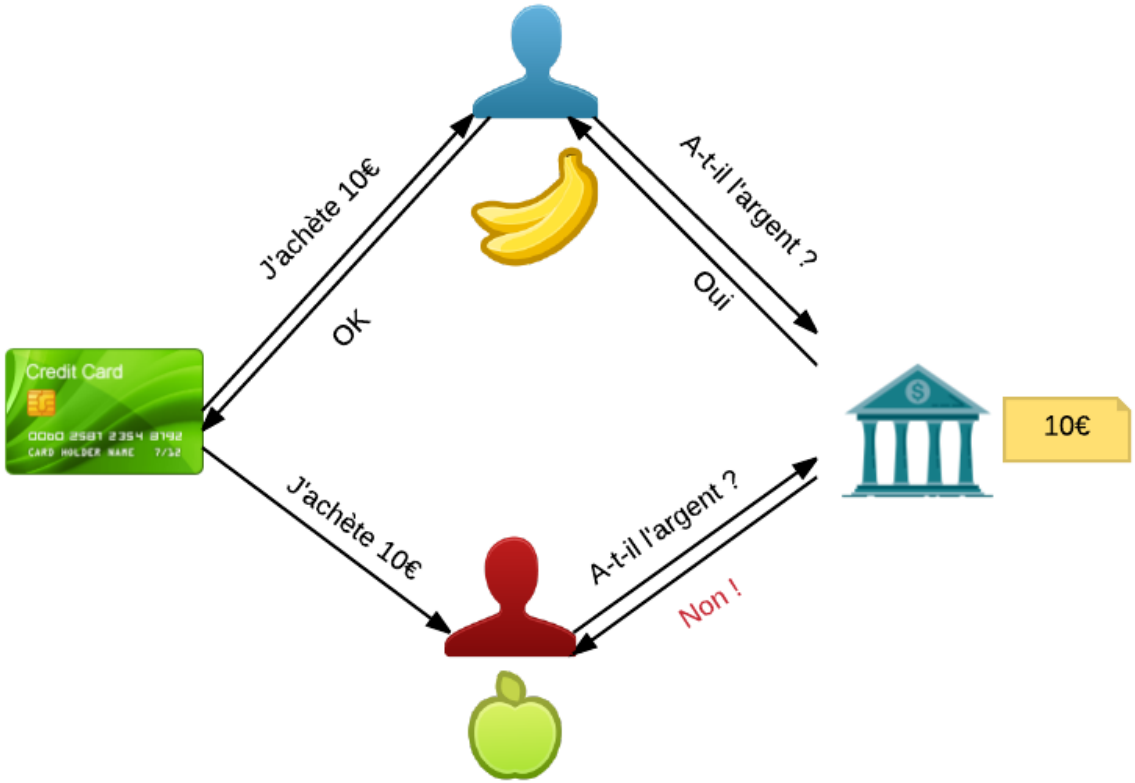
Crypto-monnaie

- 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

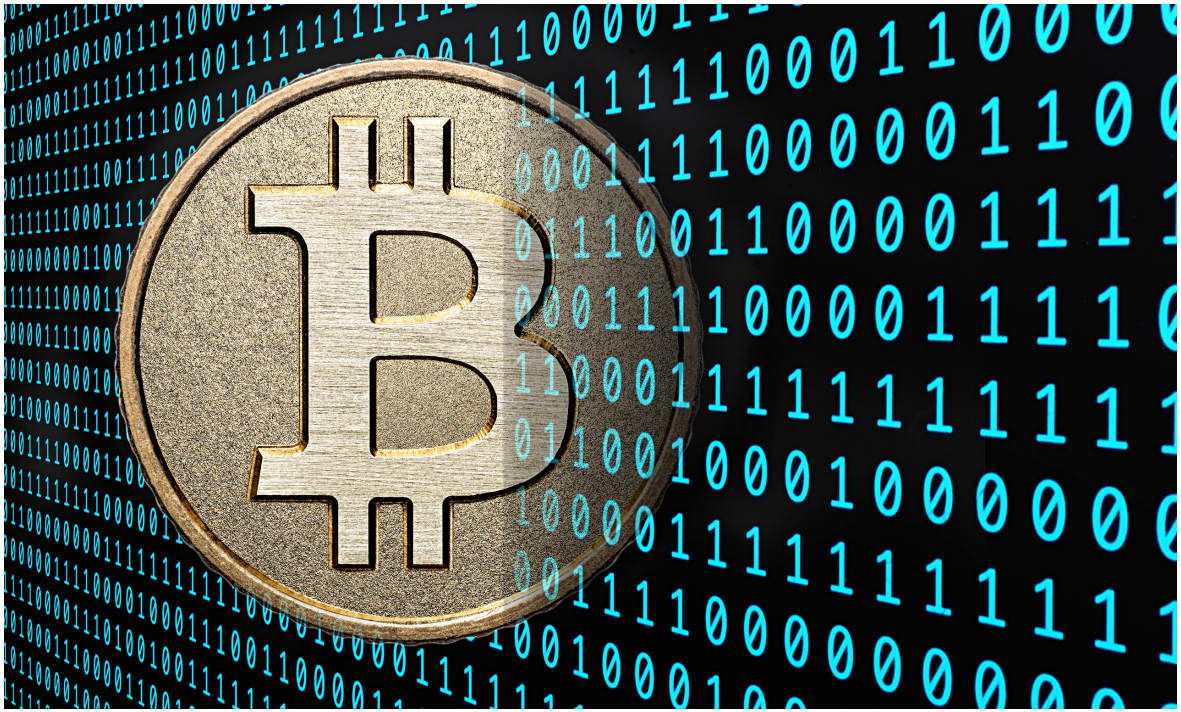
- "présemption d'innocence"

Propriétés : Respect de la vie privée

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

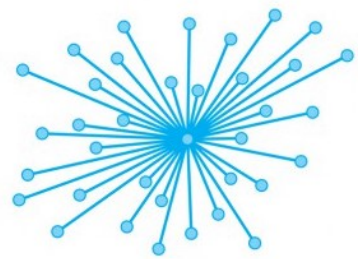
Plan

La révolution Bitcoin 2009

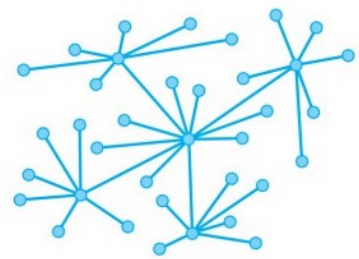


Bitcoin

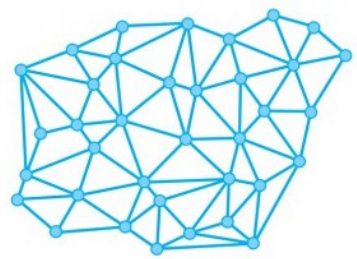
- Cryto-monnaie décentralisée et distribuée



Système centralisé



Système décentralisé

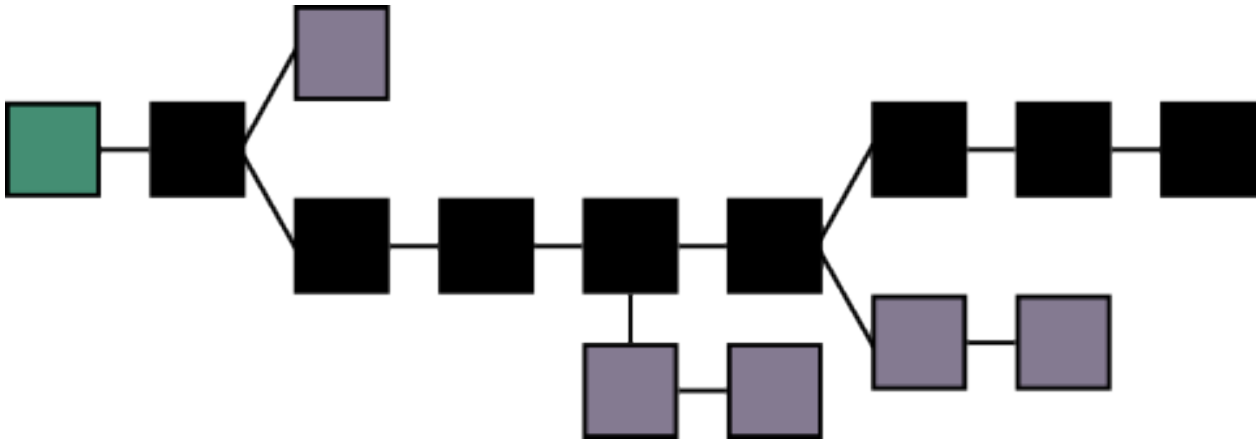


Système distribué

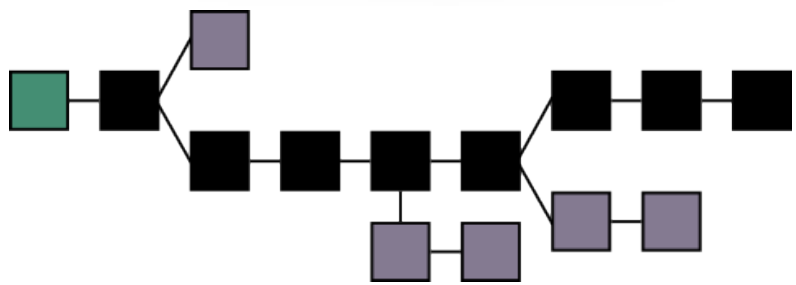
21 millions BTC

Inarrêtable car distribuée

Infalsifiable



Auditable

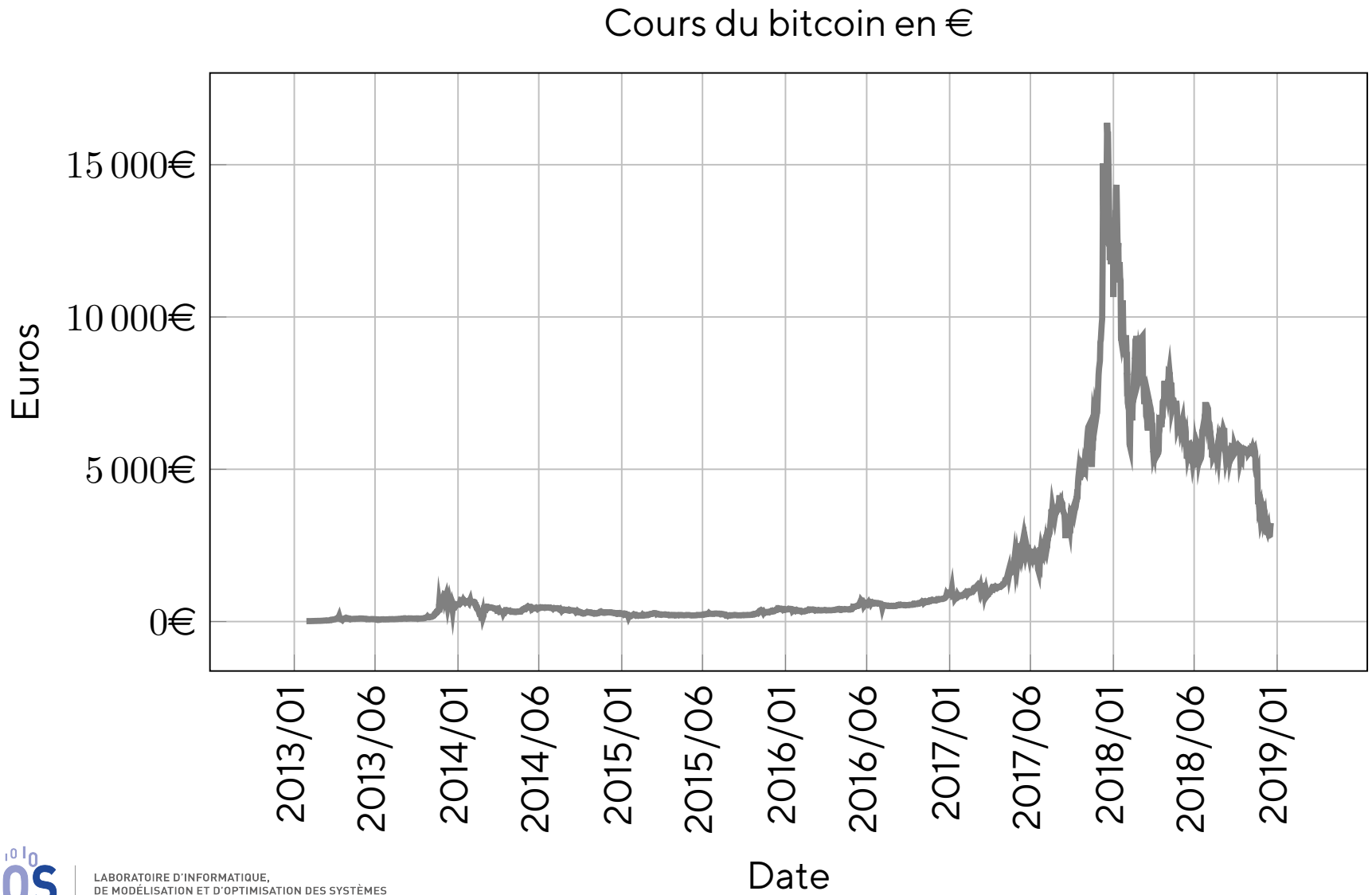


Bitcoin : monnaie électronique

Créée en 2008 par Satoshi Nakamoto (1 BTC $\approx$ 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 μBTC	= 1 microBitcoin
0,000 000 01	BTC = 1 Satoshi	

Taux de change du bitcoin



Clef symétrique

Exemples

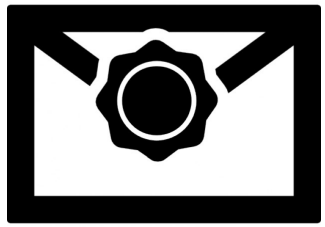
- DES
- AES

Chiffrement à clef publique

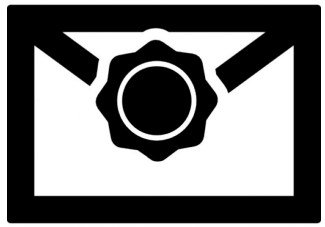
Exemples

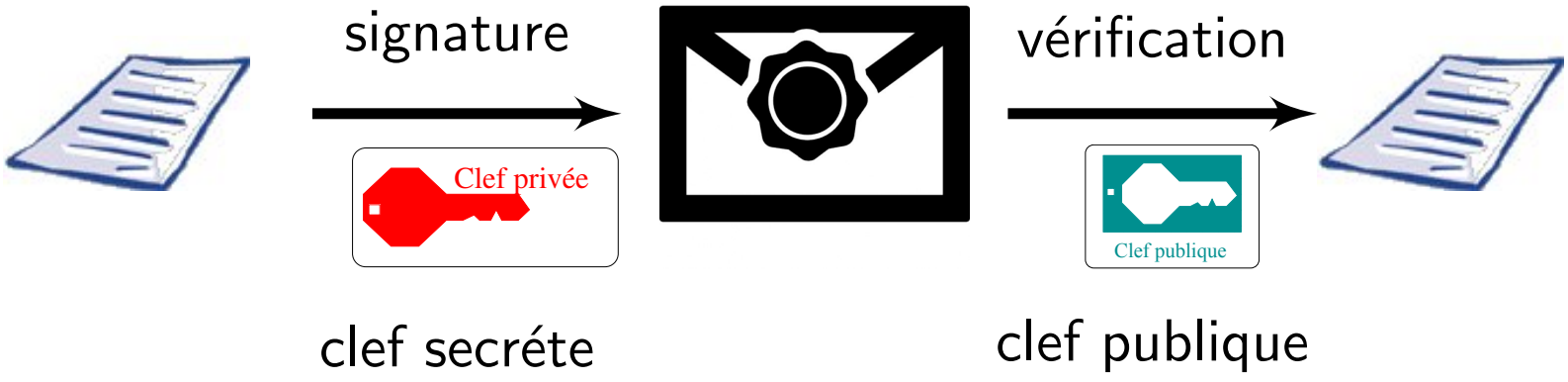
- RSA : $c = m^e \mod n$
- ElGamal : $c \equiv (g^r, h^r \cdot m)$

Signature



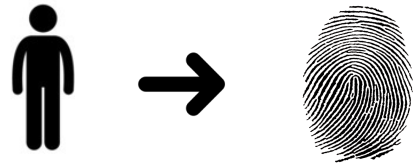
Signature



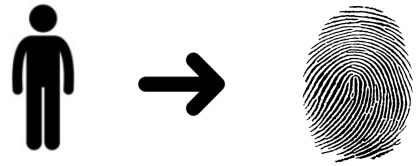


RSA: $m^d \mod n$

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

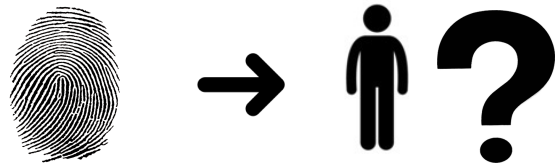


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)

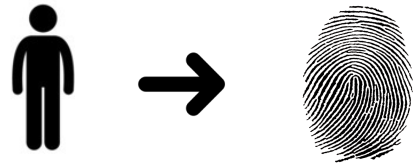


Propriétés de résitance

- Pré-image

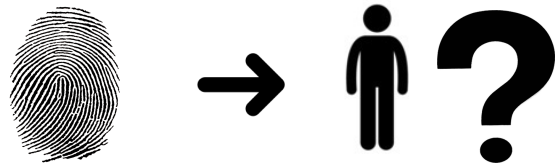


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)

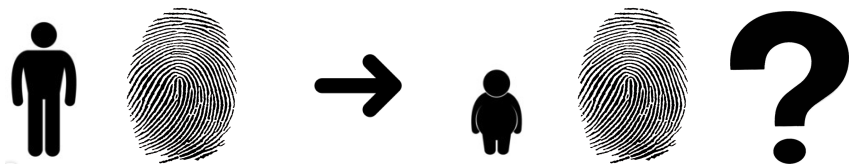


Propriétés de résitance

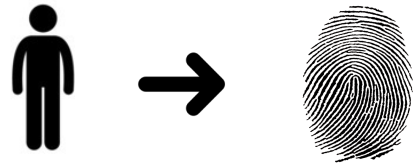
- Pré-image



- Seconde Pré-image

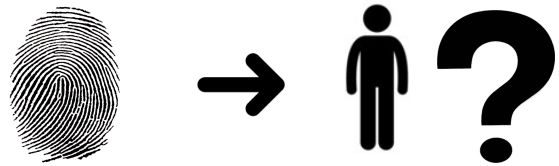


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)

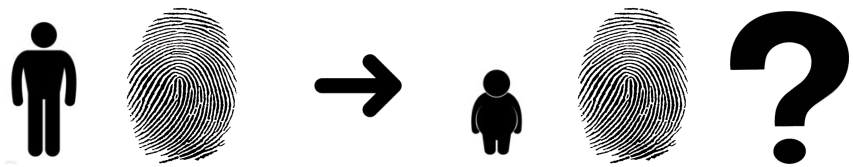


Propriétés de résitance

- Pré-image



- Seconde Pré-image



- Collision

Bitcoins : caractéristiques

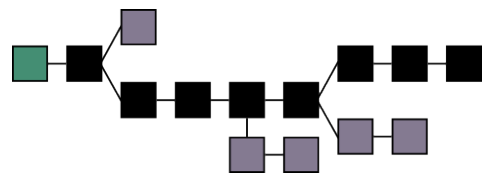
- Le nombre total de bitcoins est **fini**

  21 millions BTC

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

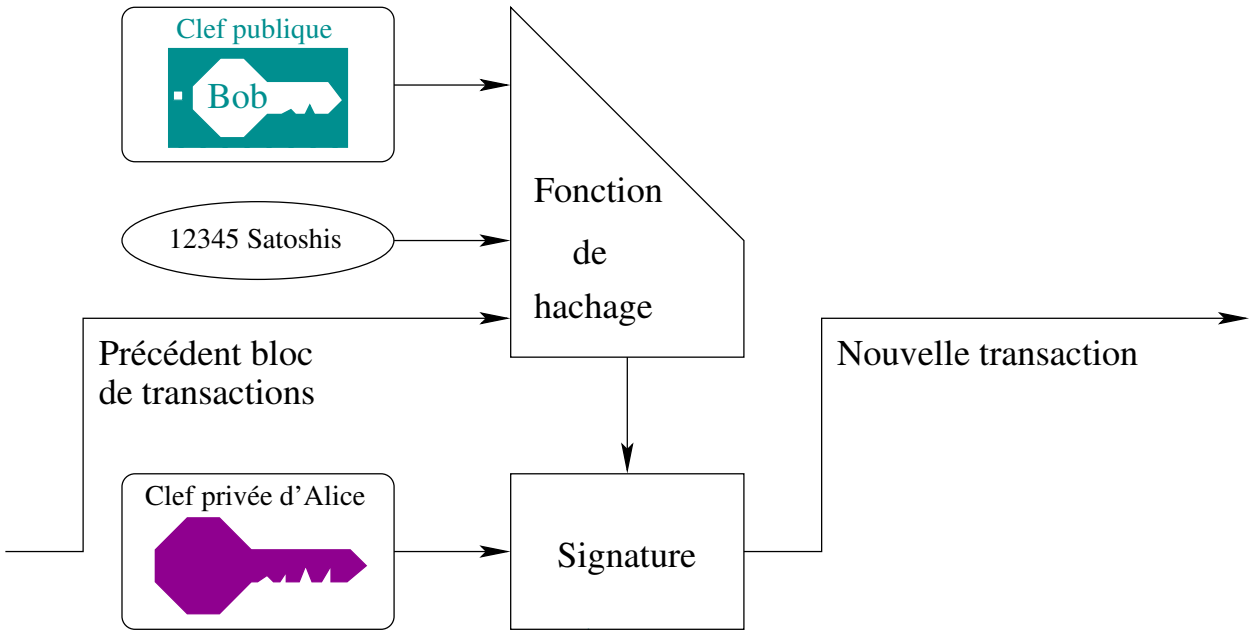
  $$\text{RIPEMD-160}(\text{SHA-256}(\text{ECDSA}_{pub}))$$

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

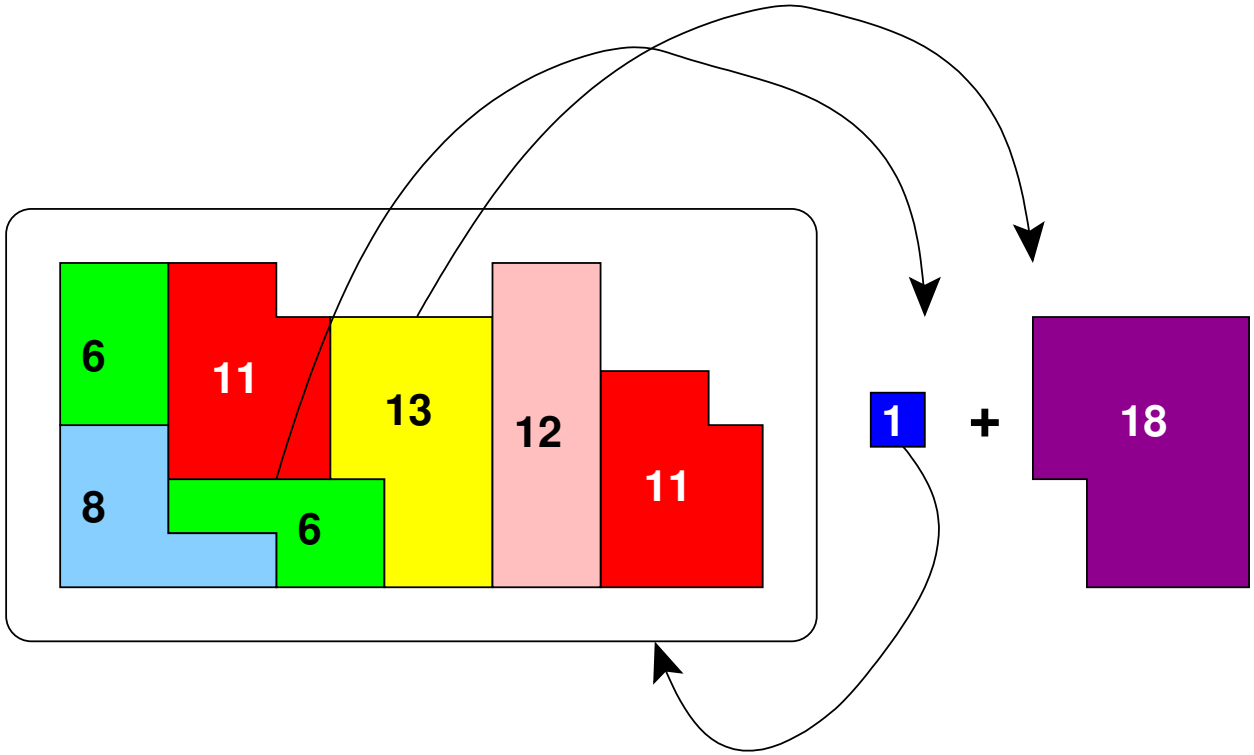


Comment faire une transaction?

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



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

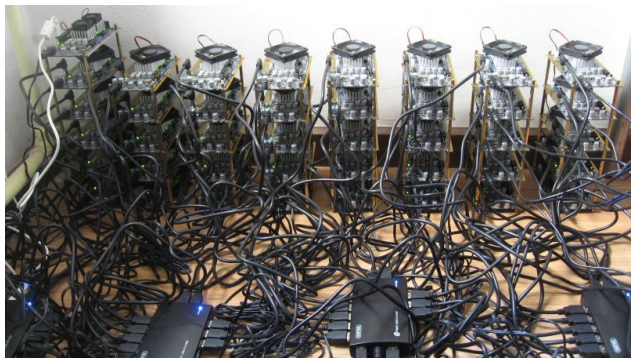
Numérique

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

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

Miner : Objectif de hachage

Cible = 0000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076

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 = 0000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076

Trouver une nombre n tel que

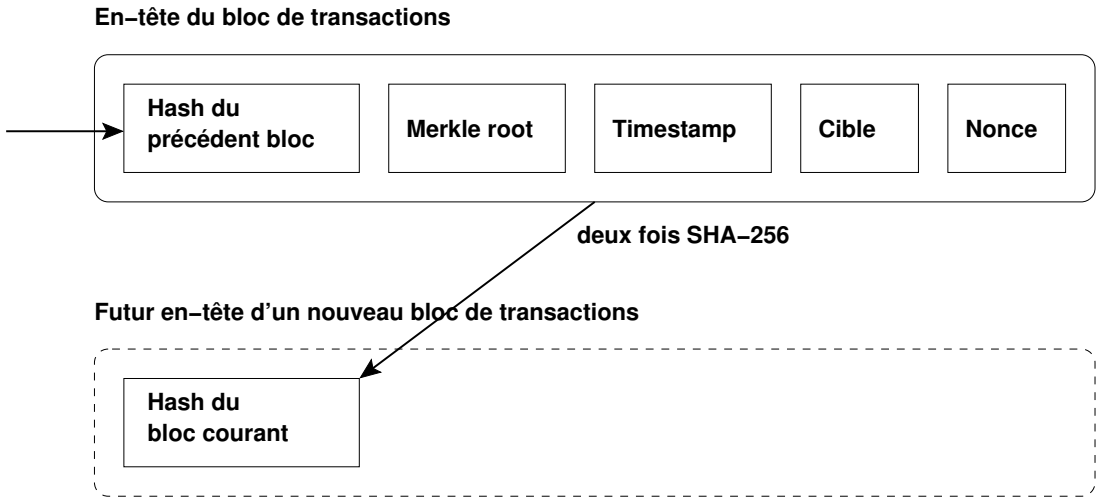
$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, n)) = x < \textit{Cible}$$

Avoir au moins 18 zéros au début de x

Stratégie : brute force

Tester toutes les valeurs possibles de n

Miner : Proof of work



Avoir un zéro de plus au début

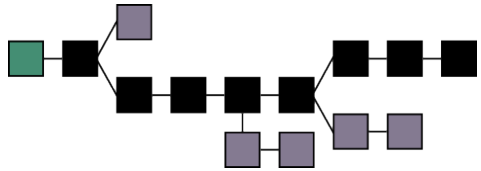
SHA-256(SHA-256(en-tête de bloc))

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

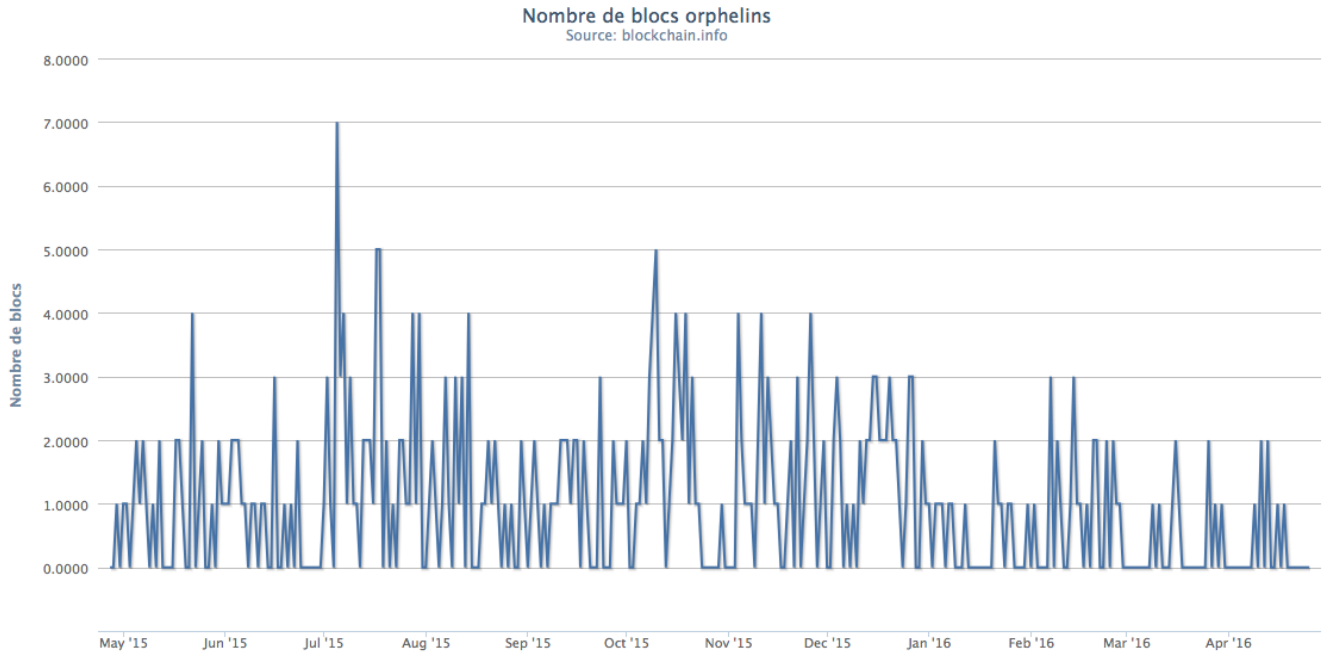
LIMOS
LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Miner = Validation des transactions

Cible: 00000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076

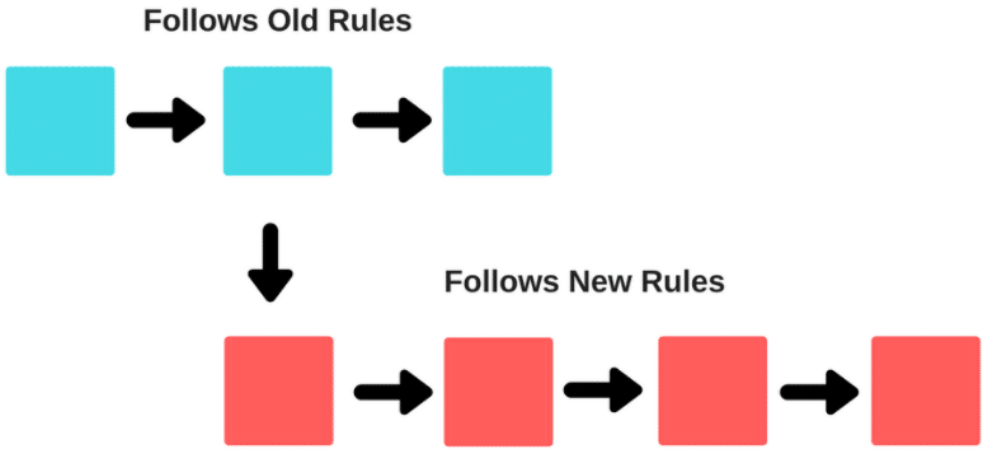


- La chaîne la plus longue persiste (attaque 51 %)
- Validation toutes les 10 minutes (6 confirmations)



LIMOS LABORAT DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Soft Fork

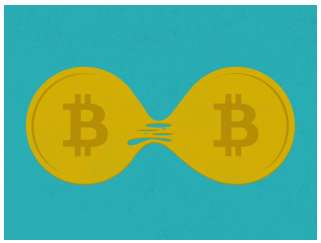


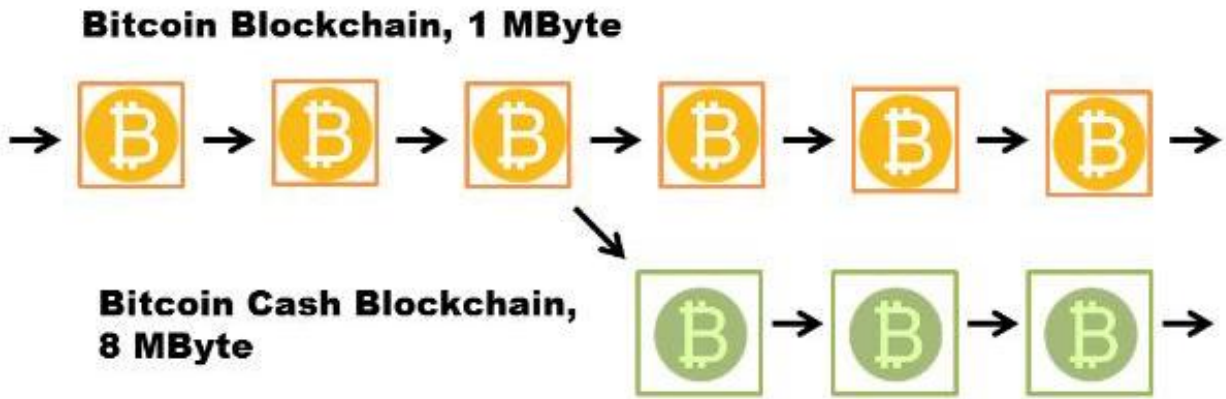
The primary difference between a soft fork and hard fork is that it is not backward compatible

Modification du code :

- Correction de bugs
- Améliorations consensuelles

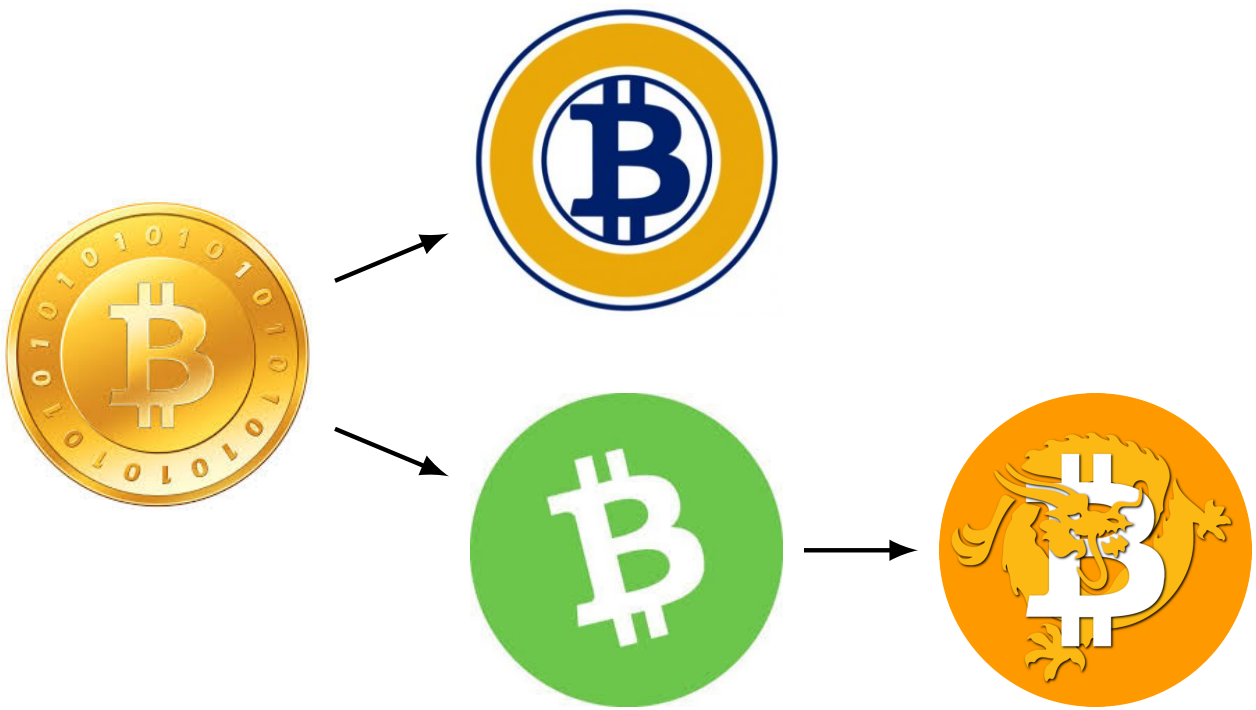
Hard Fork




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

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 ≈	5 910$
24/10/2017 :	BTG ≈	480$
25/10/2017 :	BTC ≈	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 ≈	5 910$
24/10/2017 :	BTG ≈	480$
25/10/2017 :	BTC ≈	5 380$
10/03/2019 :	BTC ≈	3 895$
	BTG ≈	12$

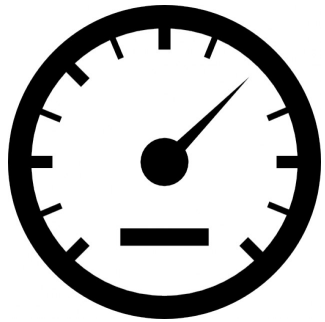
Traçable

Traçable

MONERO

ZCASH

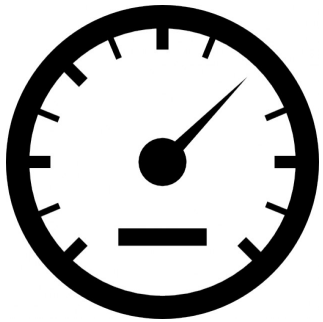
Limitations



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

Energivore

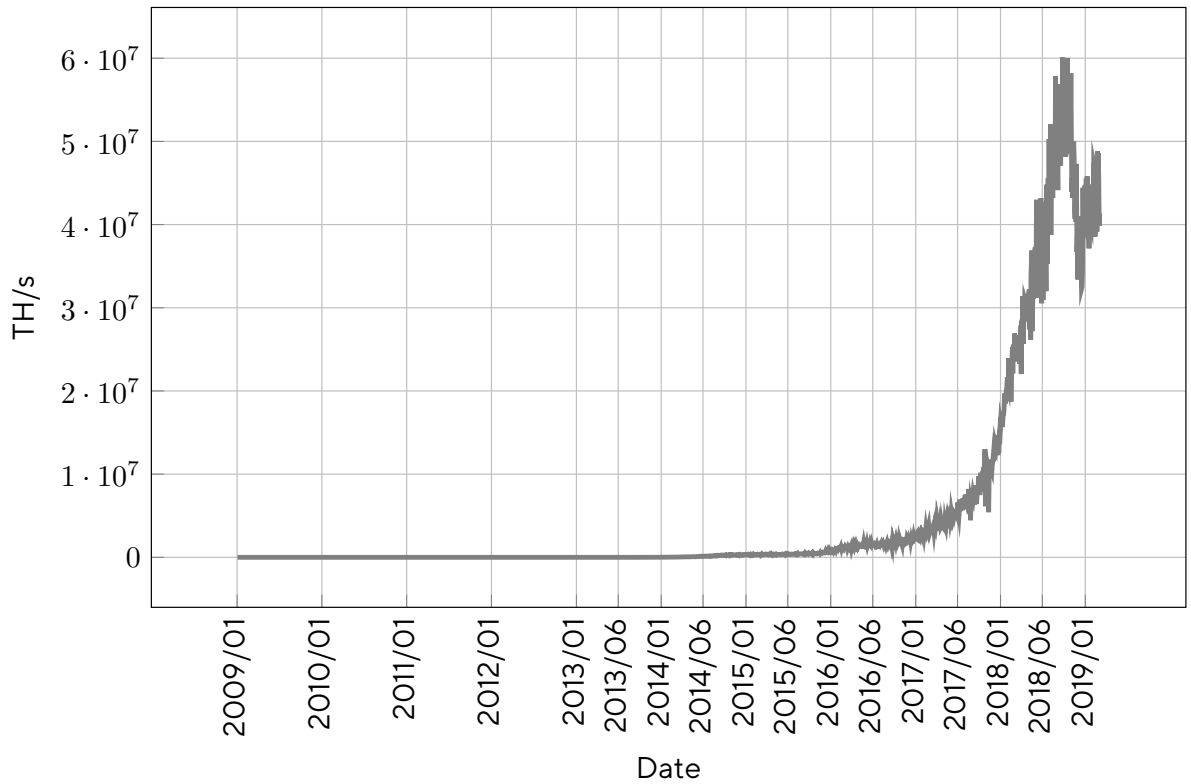
Proof of Stake

Lightning Network

Énergivore

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

Énergivore



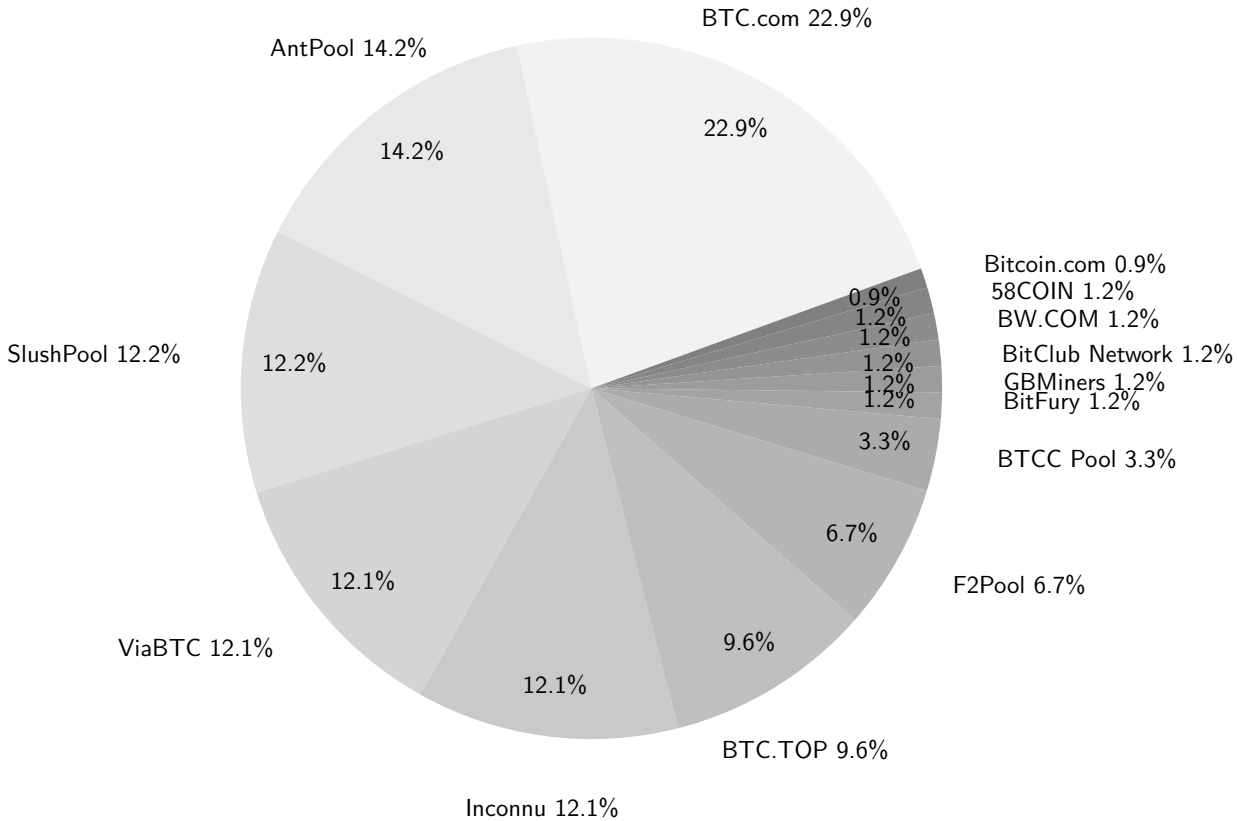
Estimation: plusieurs TWh annuels (comparable à un petit état).

Un bloc toutes les 10 minutes

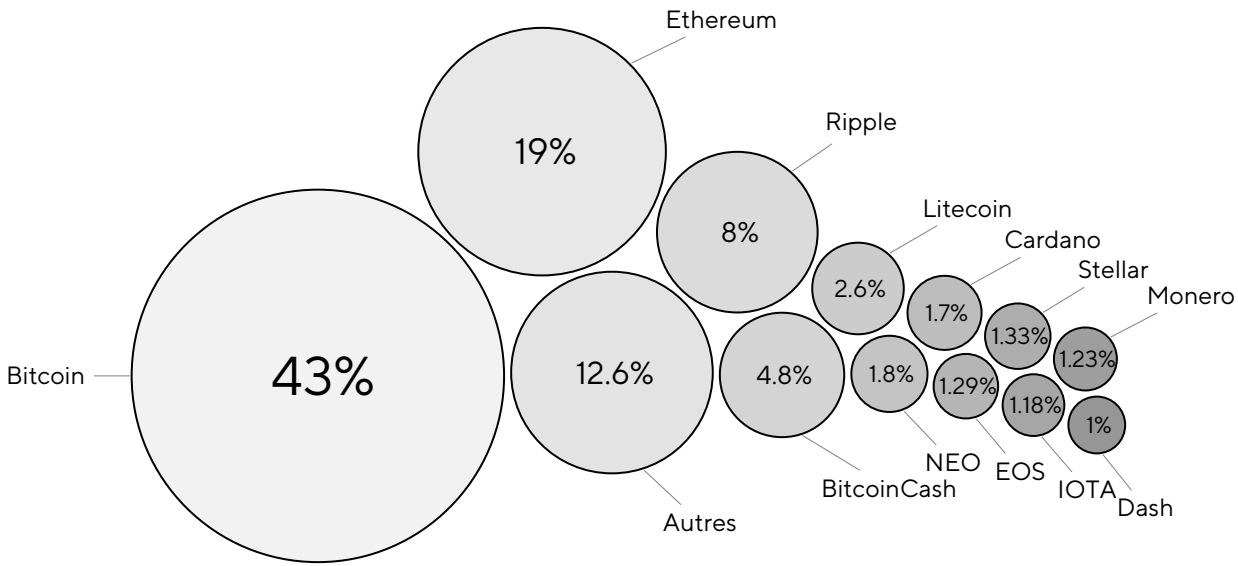
Machine	Type	Vitesse MH/s	Efficacité MH/J	Coût MH/s/€	Minage moyen Années/bloc
Core i5-2400	CPU	14	0.15	0.09	25.3 Millions
PS3	Cell	21	0.35	0.09	16.9 Millions
ATI 830	GPU	325	1.98	3.30	1.1 Millions
Ebit E11++	ASIC	44 000 000	22 200.00	8 885.00	13.6

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

Fermes de mineurs



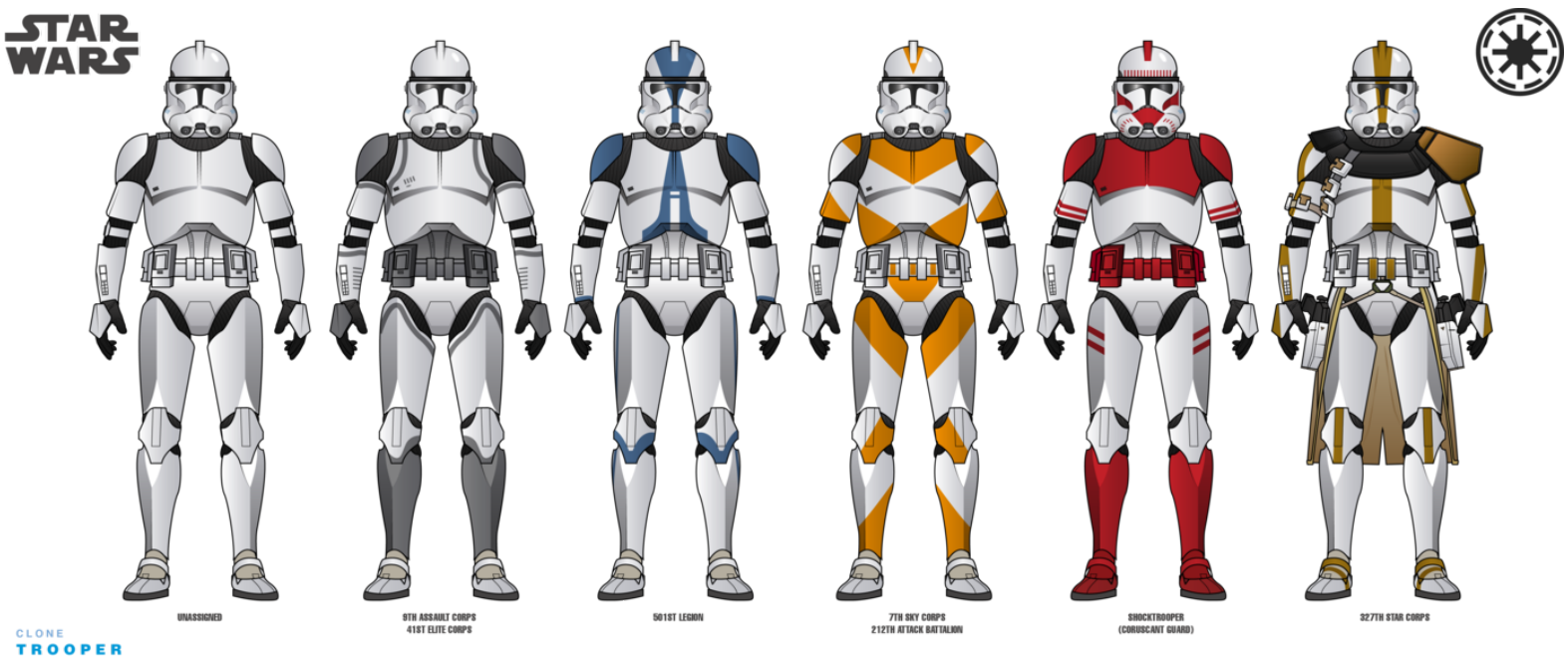
Diversité monétaire



Autres crypto-monnaies

Classification I : Pourris

Classification II : Clones de Bitcoin

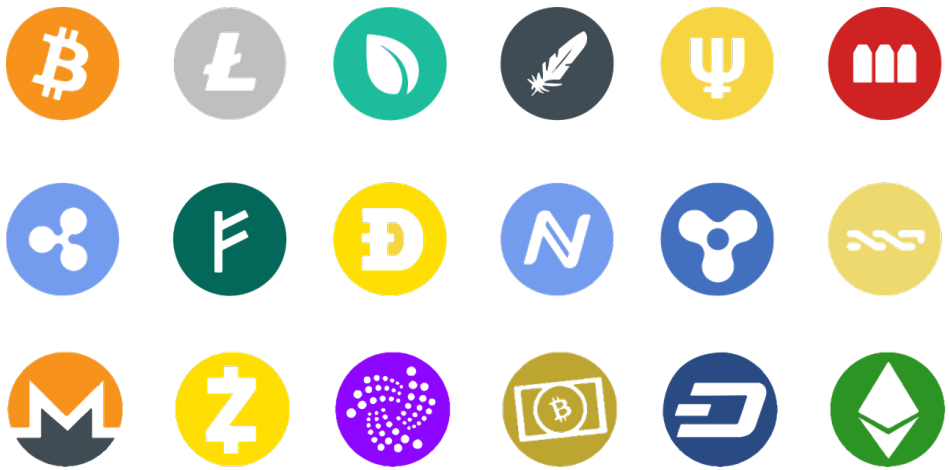


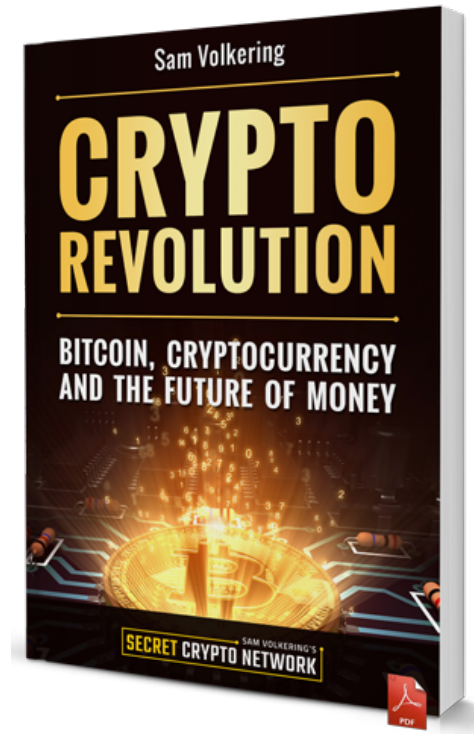
Classification III : Plus utile

Classification IV : Autres preuves de travail

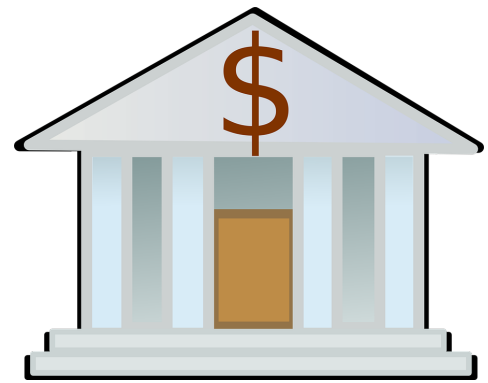
ethereum

Pluriculture des créations monétaires



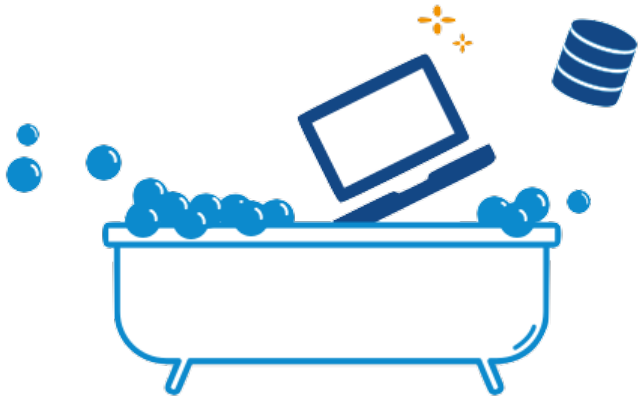


Qui s'approprie ces nouvelles monnnaies ?



Un exemple : ĞI

Freins



Bitcoin : Crypto-monnaie dématérialisée décentralisée

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

Bitcoin : Crypto-monnaie dématérialisée décentralisée

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

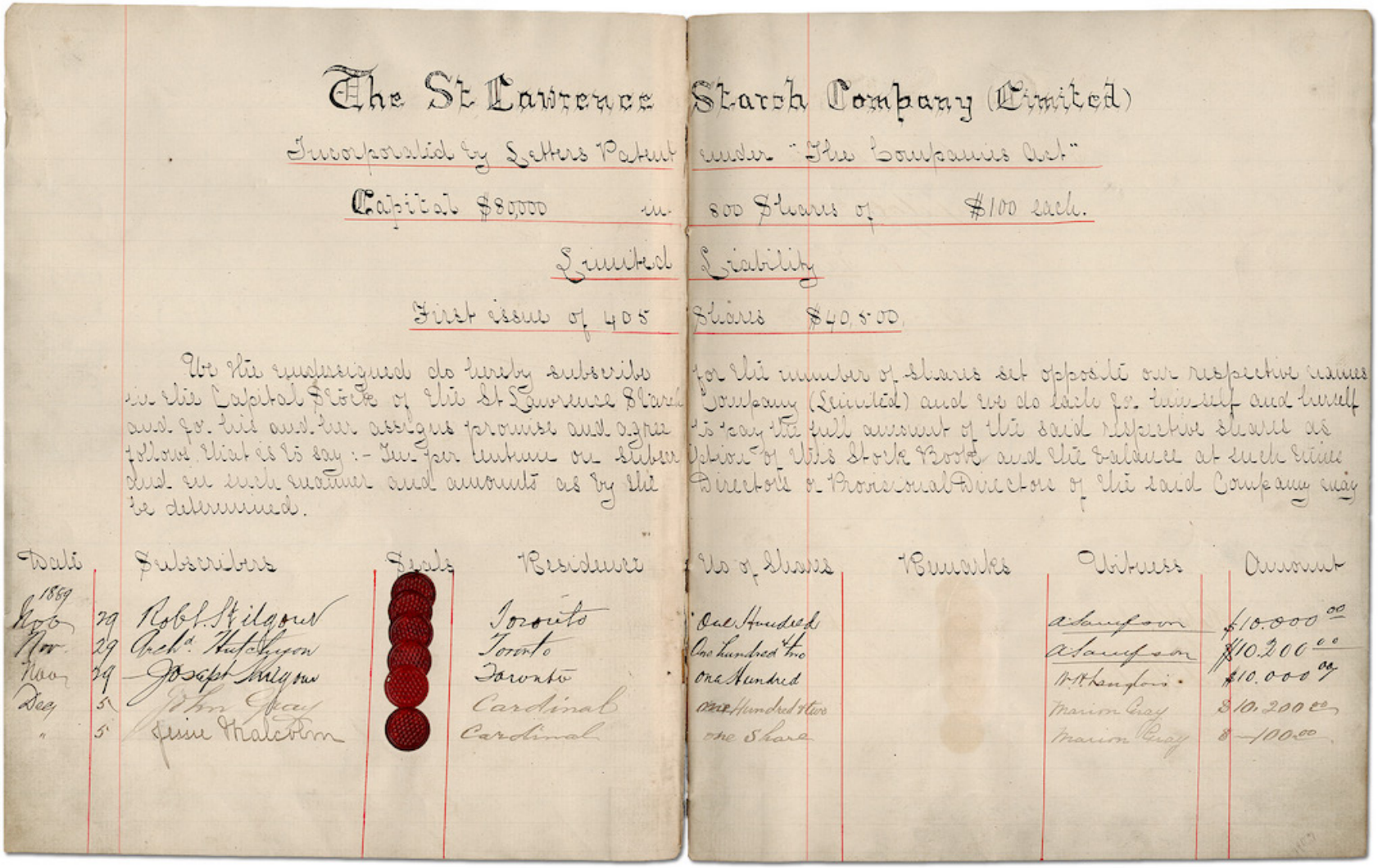


- Perte ou vol de la clef secrète = irréversible
- Monnaie anonyme et traçable



Plan

Blockchain



The St Lawrence Starch Company (Limited)

Incorporated by Letters Patent under "The Companies Act"

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

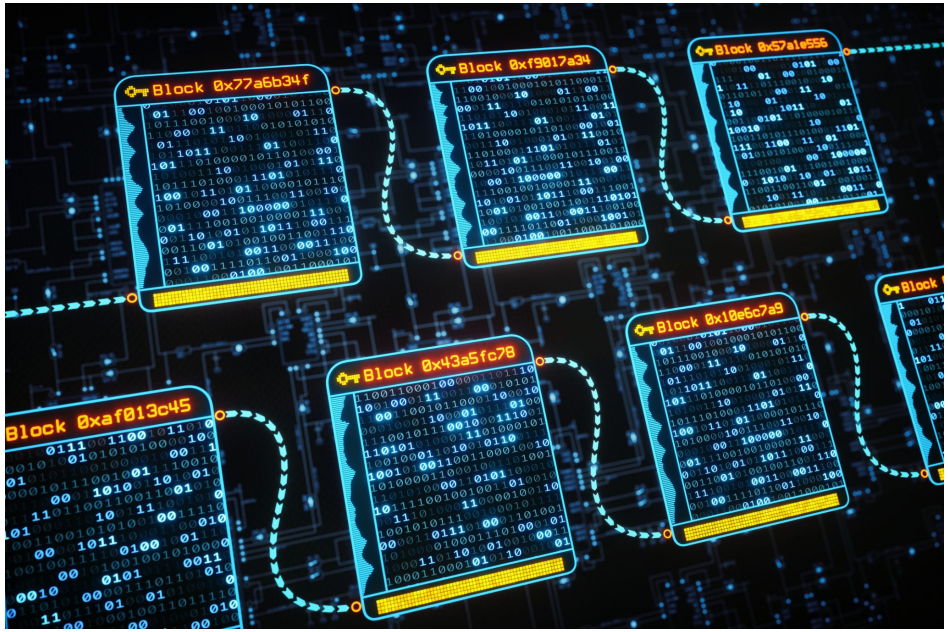
Limited Liability

First issue of 405 Shares $40,500

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 and severally promise and agree to pay the full amount of the said respective shares as follows that is to say:- Ten per centum on Stock Book and the balance at such time Directors or Provisional Directors of the said Company may be determined.

Date 1869		Subscribers	Seals	Residence	No of Shares	Remarks	Witness	Amount
Nov	29	Robt Stilgoe		Toronto	One Hundred		adamson	$10.000 00
Nov	29	Robt Hutchison		Toronto	One Hundred & two		adamson	$10.200 00
Nov	29	Joseph Stilgoe		Toronto	one Hundred		W.H. Langford	$10.000 00
Dec	5	Wm Gray		Cardinal	one Hundred & two		Marion Gray	$10.200 00
"	5	Jesse Malcolm		Cardinal	one Share		Marion Gray	$ 100.00

Blockchain



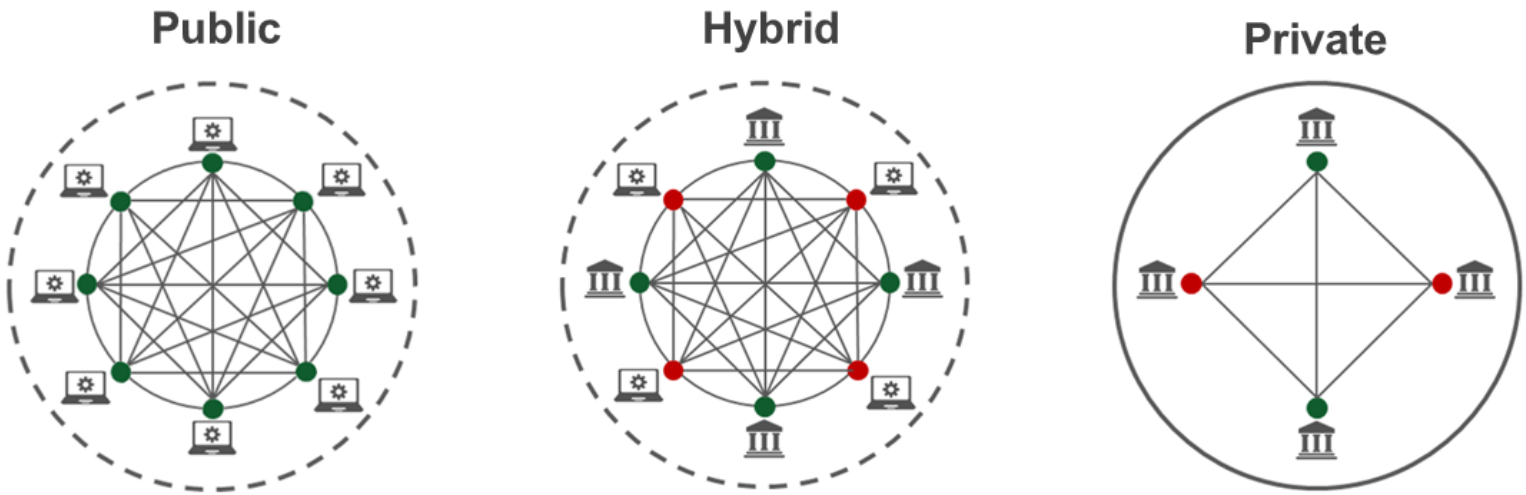
Registre distribué, sécurisé, infalsifiable

Mineurs valident des transactions

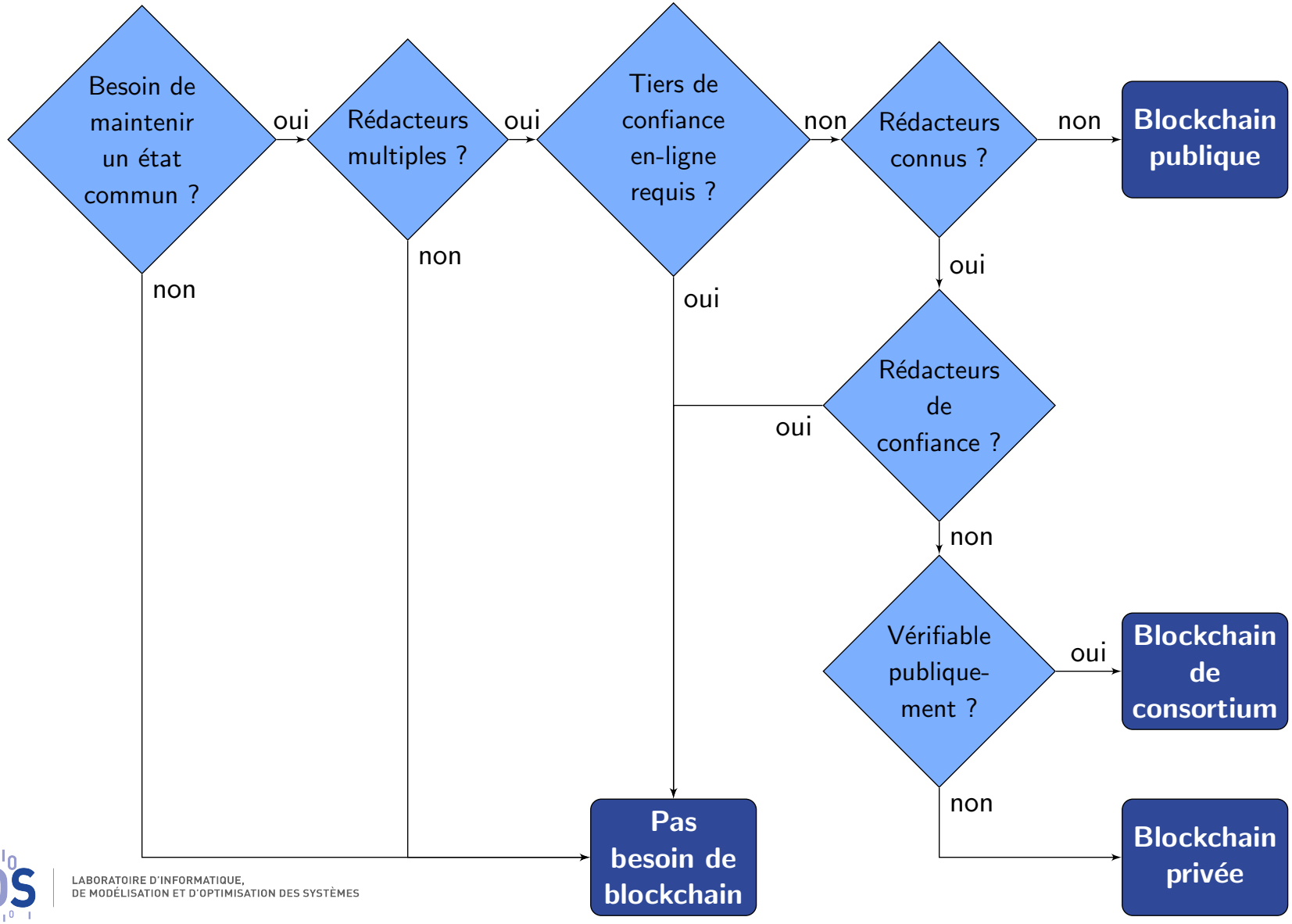
Tiennent à jour le registre distribué

Décision des mineurs

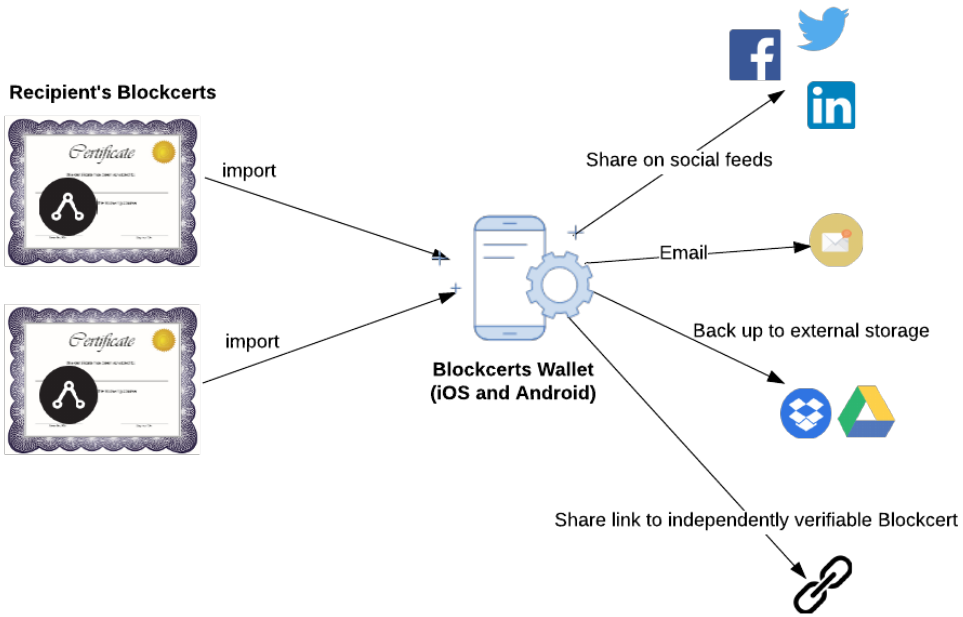
Blockchain Privée vs Publique



Ai-je besoin d'une blockchain ?



Blockchain Application : MIT Diploma



Blockchain Applications

BlockchainyourIP

E-commerce

E-voting

E-Health

...

Merci pour votre attention

Questions ?

pascal.lafourcade@uca.fr

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