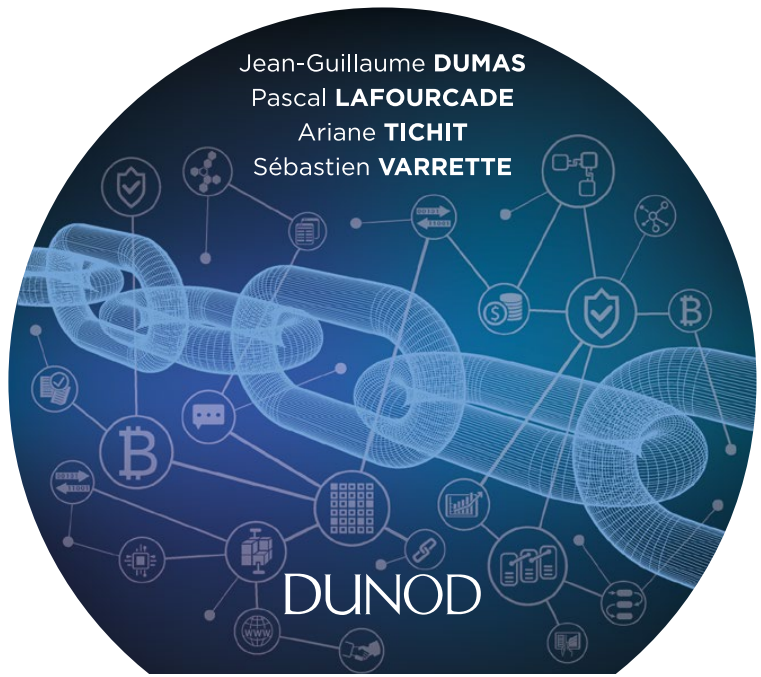
Les BLOCK CHAINS

EN 50 QUESTIONS

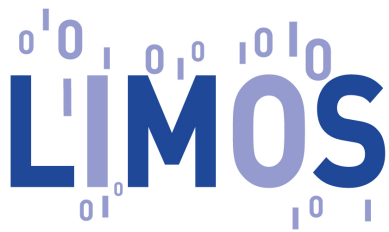
Comprendre le fonctionnement et les enjeux de cette technologie innovante



LIMOS
LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATIO

Bitcoin et la Blockchain

Pascal Lafourcade



Nice
Juin 2019

Plan

Plan

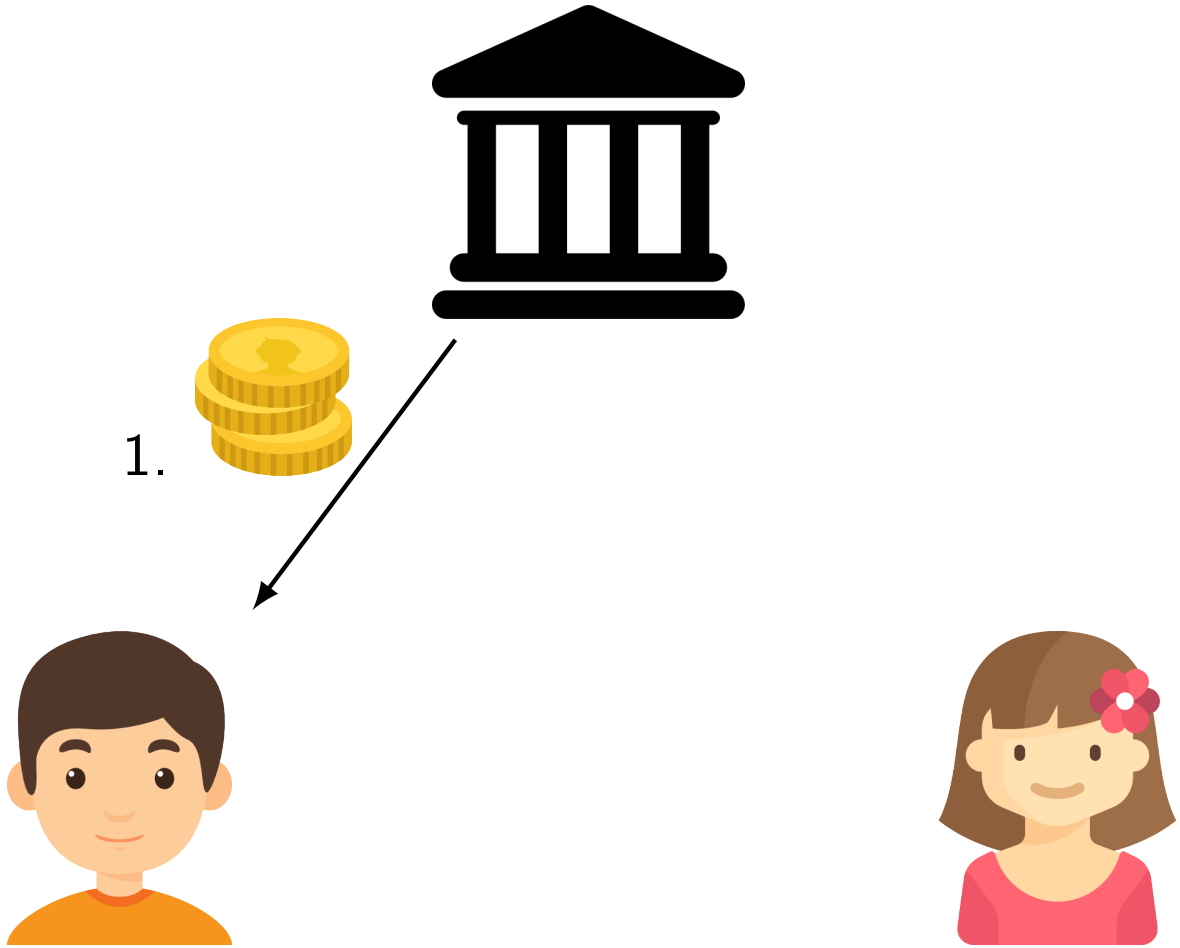
Sumériens vers 3.500 av J.C

Qu'est-ce que la monnaie?

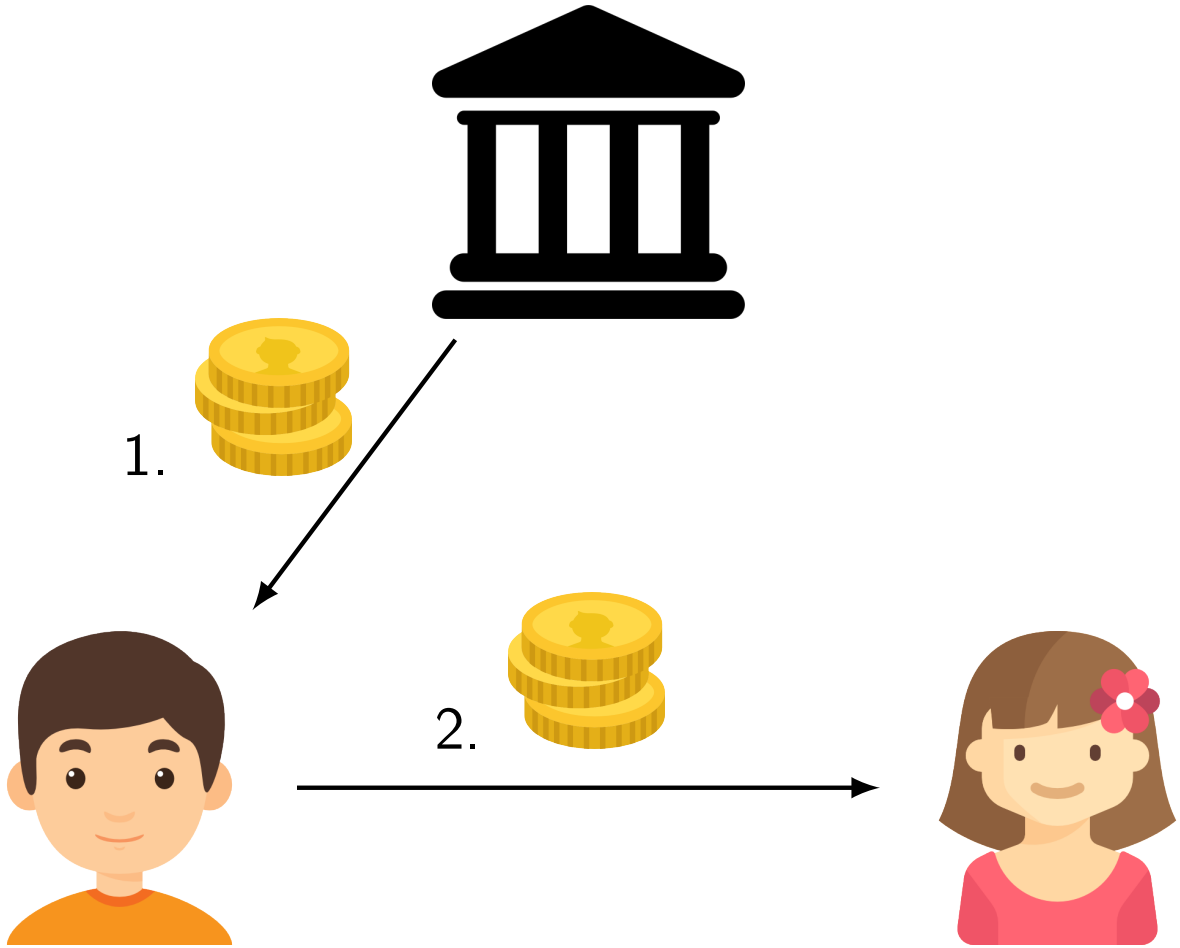
- Intermédiaire et moyens d'échanges de biens et services entre les individus
- Réserve de valeur
- Unité de compte

Nombreuses monnaies

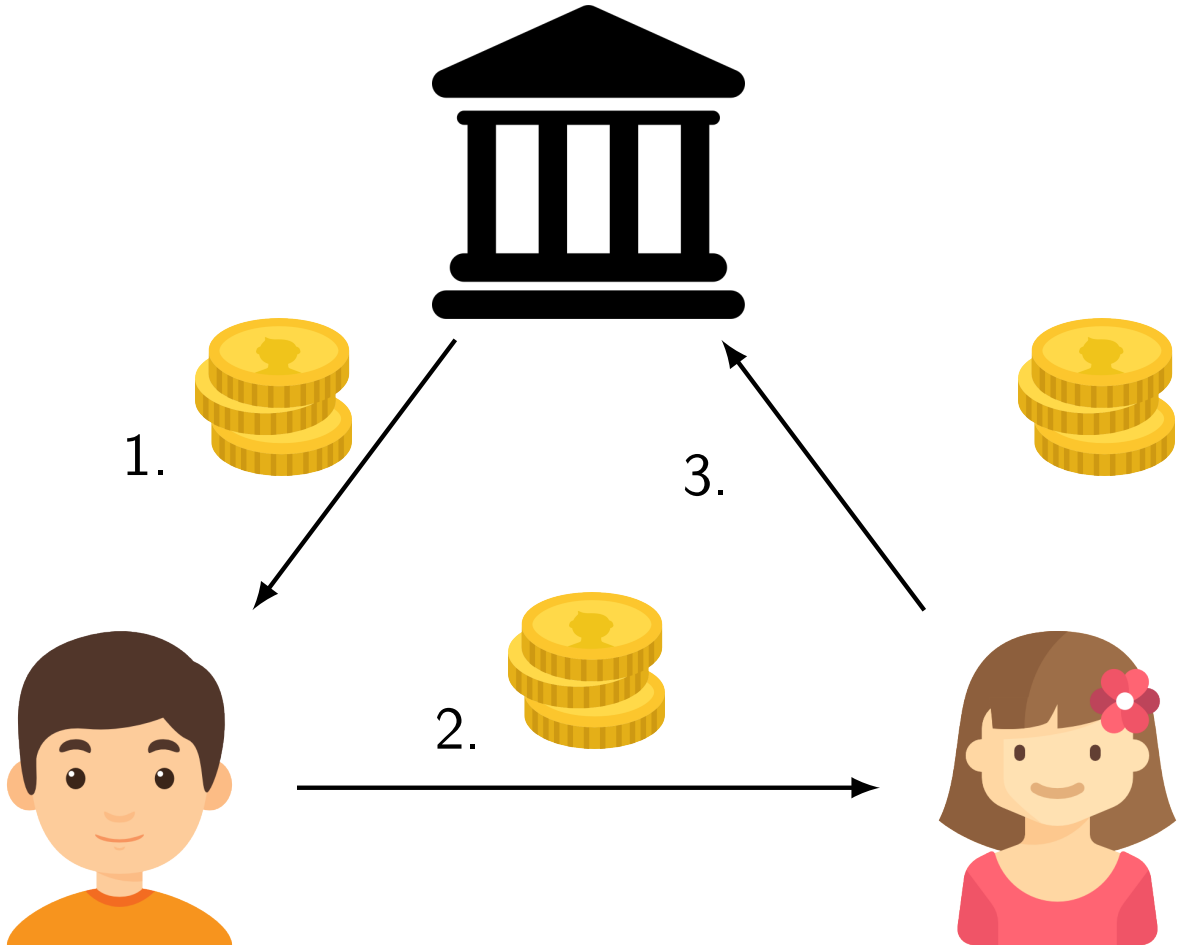
Principe : Banque centrale



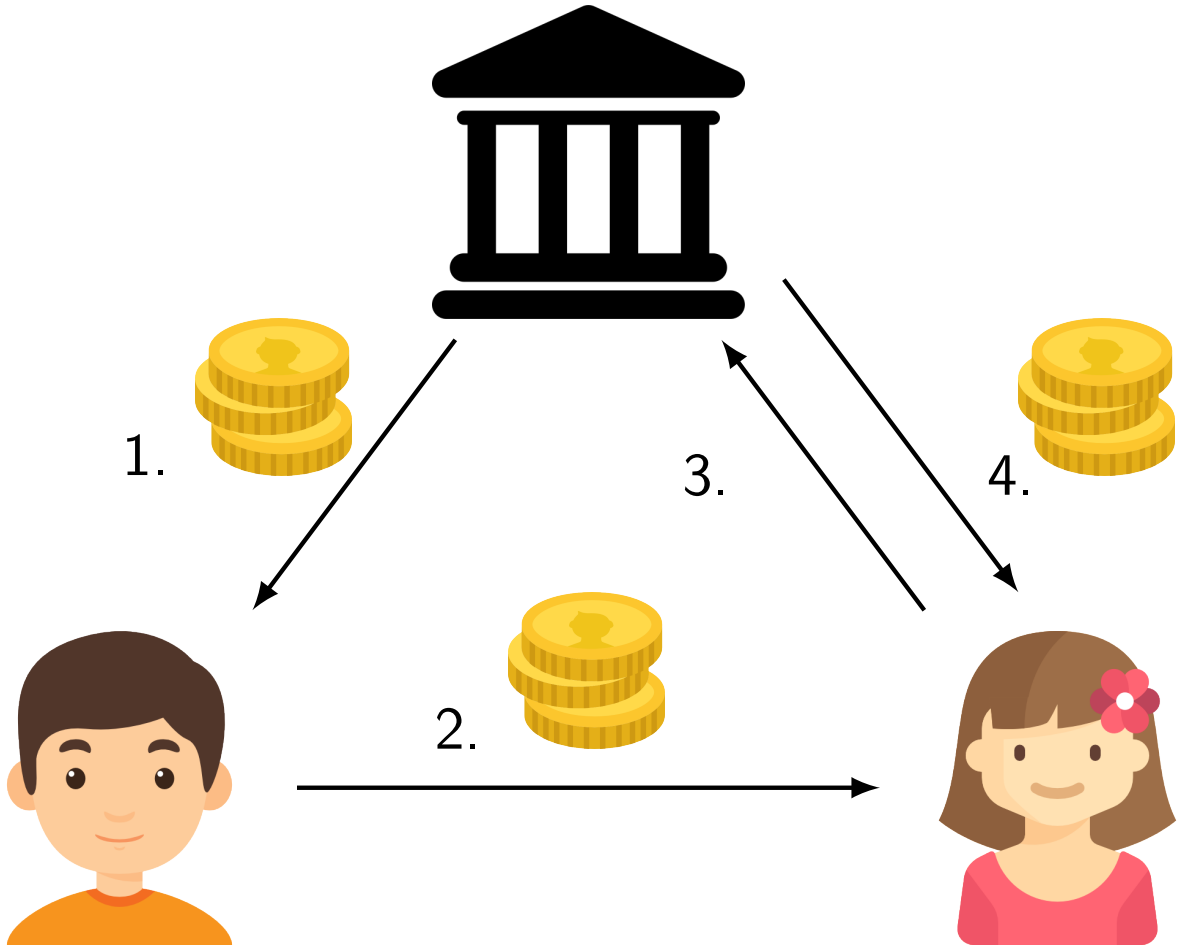
Principe : Banque centrale



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

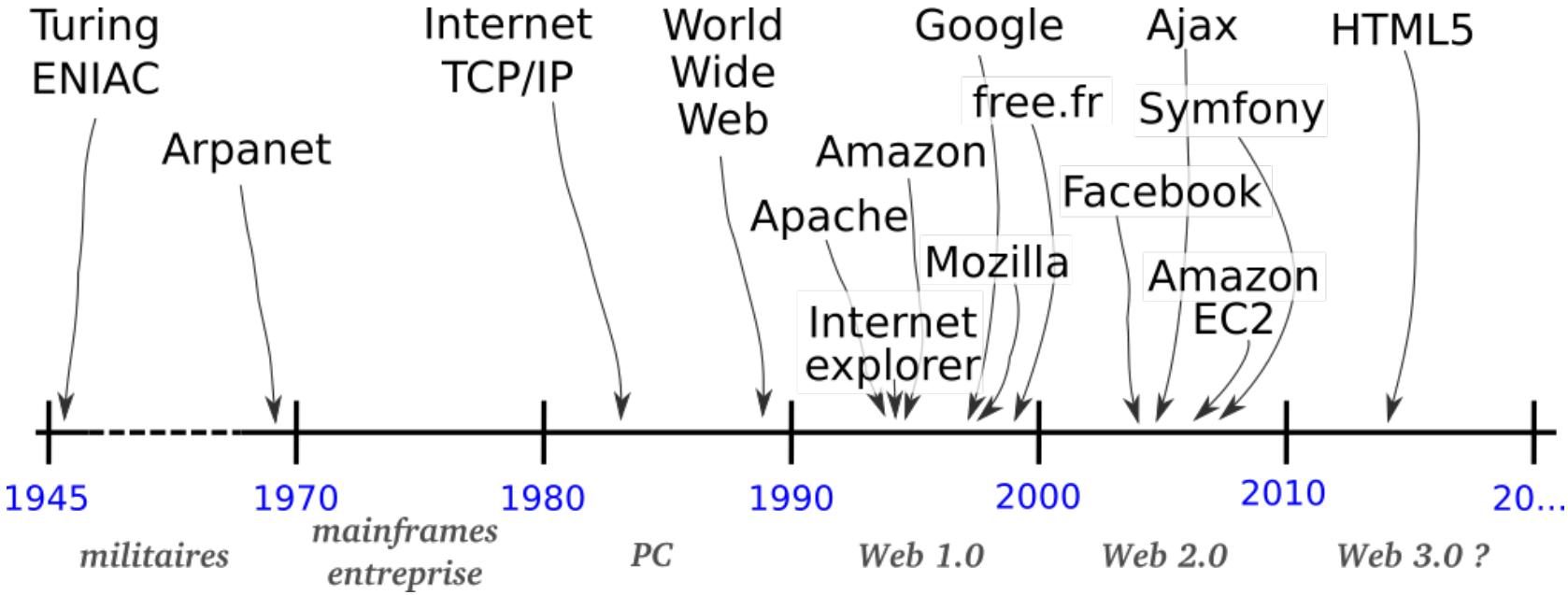
CRYPTO 1988

DigiCash™

David Chaum

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

Une idée visionnaire en avance sur son temps



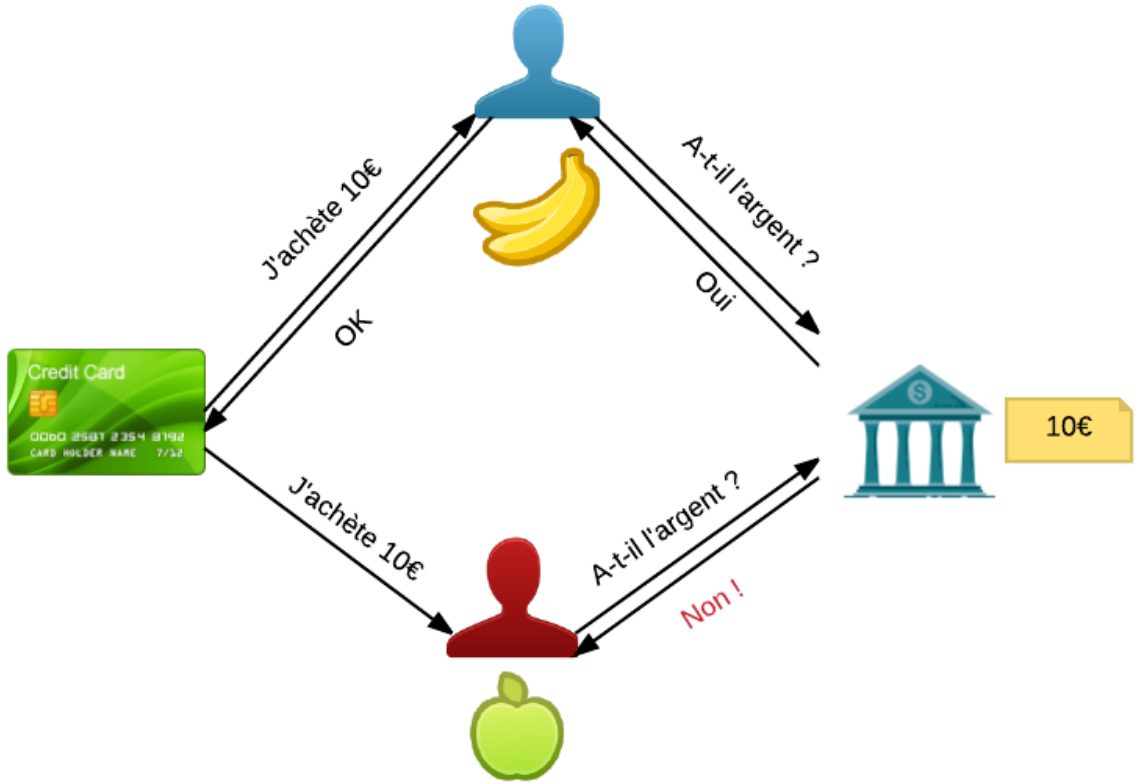
Crypto-monnaie

- 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"

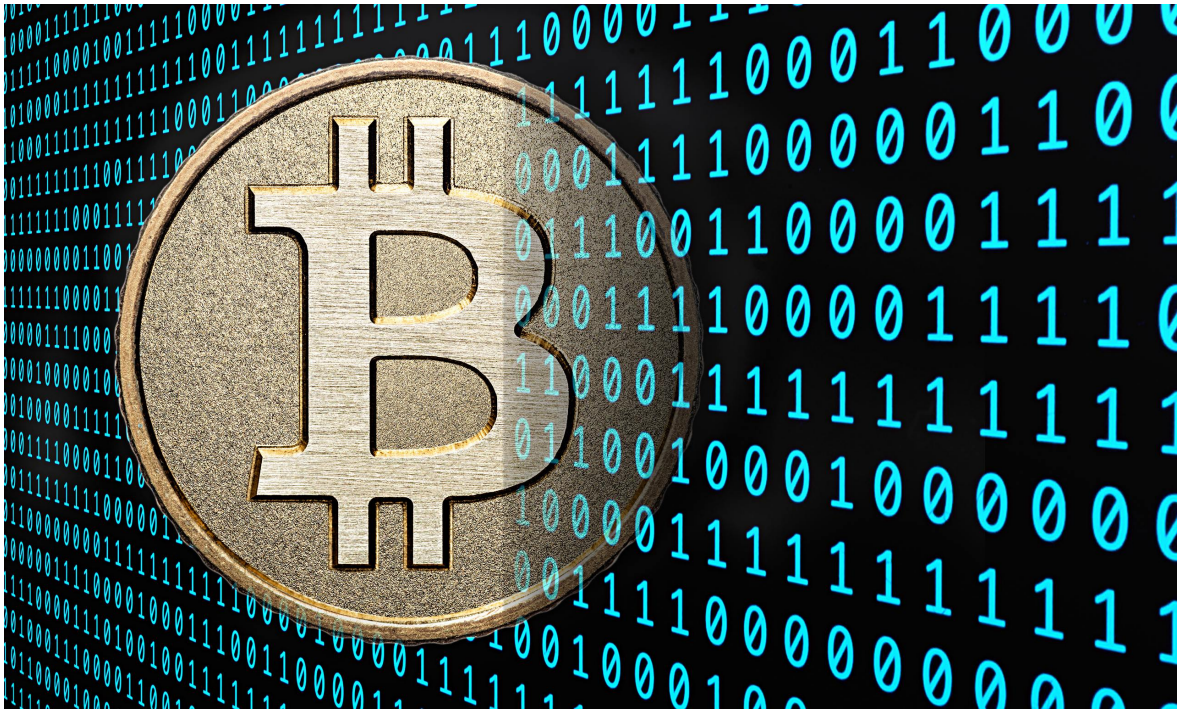
Propriétés : Respect de la vie privée

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

Monnaies classiques et crypto-monnaies

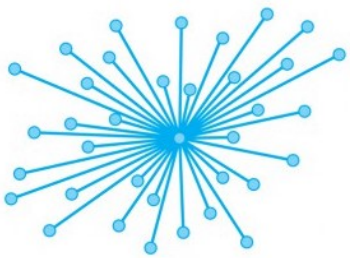
	Monnaie classique		Crypto-monnaie
	Liquide	Électronique	
Moyen d'échange	✓	✓	✓
Réserve de valeur	✓	✓	✓
Unité de compte	✓	✓	✓
Création	Banque centrale	Dette	Automatique
Vie privée	✓	✗	✓
Pair à pair	✗	✗	✓
Garantie légale, stabilisation	✓	✓	✗

La révolution Bitcoin 2009

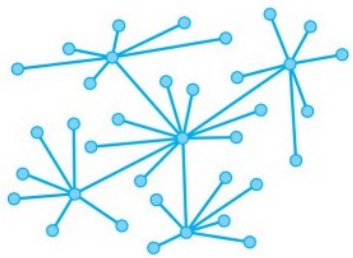


Bitcoin

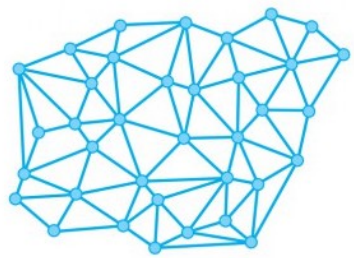
- Cryto-monnaie décentralisée et distribuée



Système centralisé



Système décentralisé

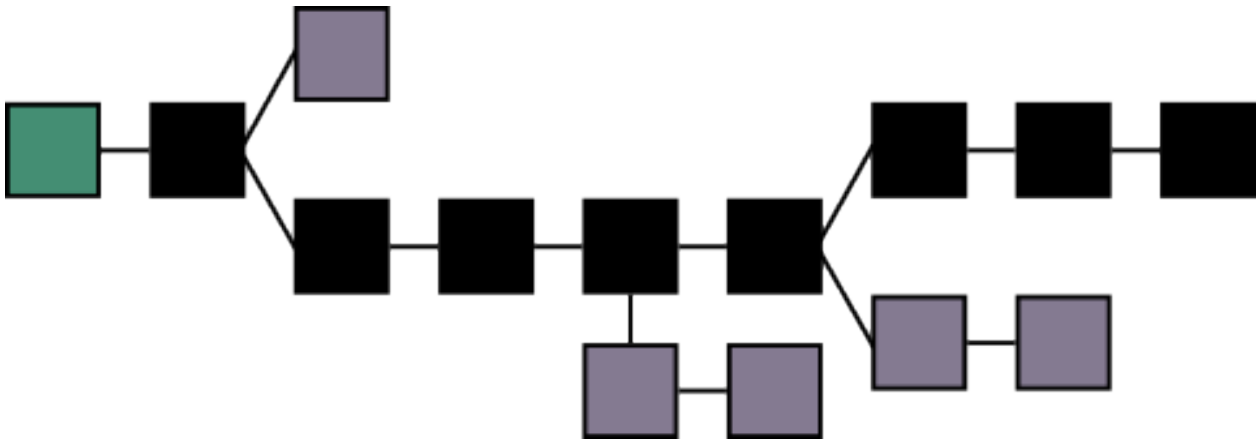


Système distribué

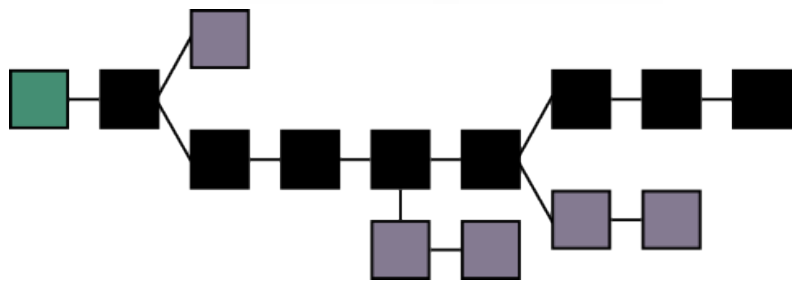
21 millions BTC

Inarrêtable car distribuée

Infalsifiable



Auditable

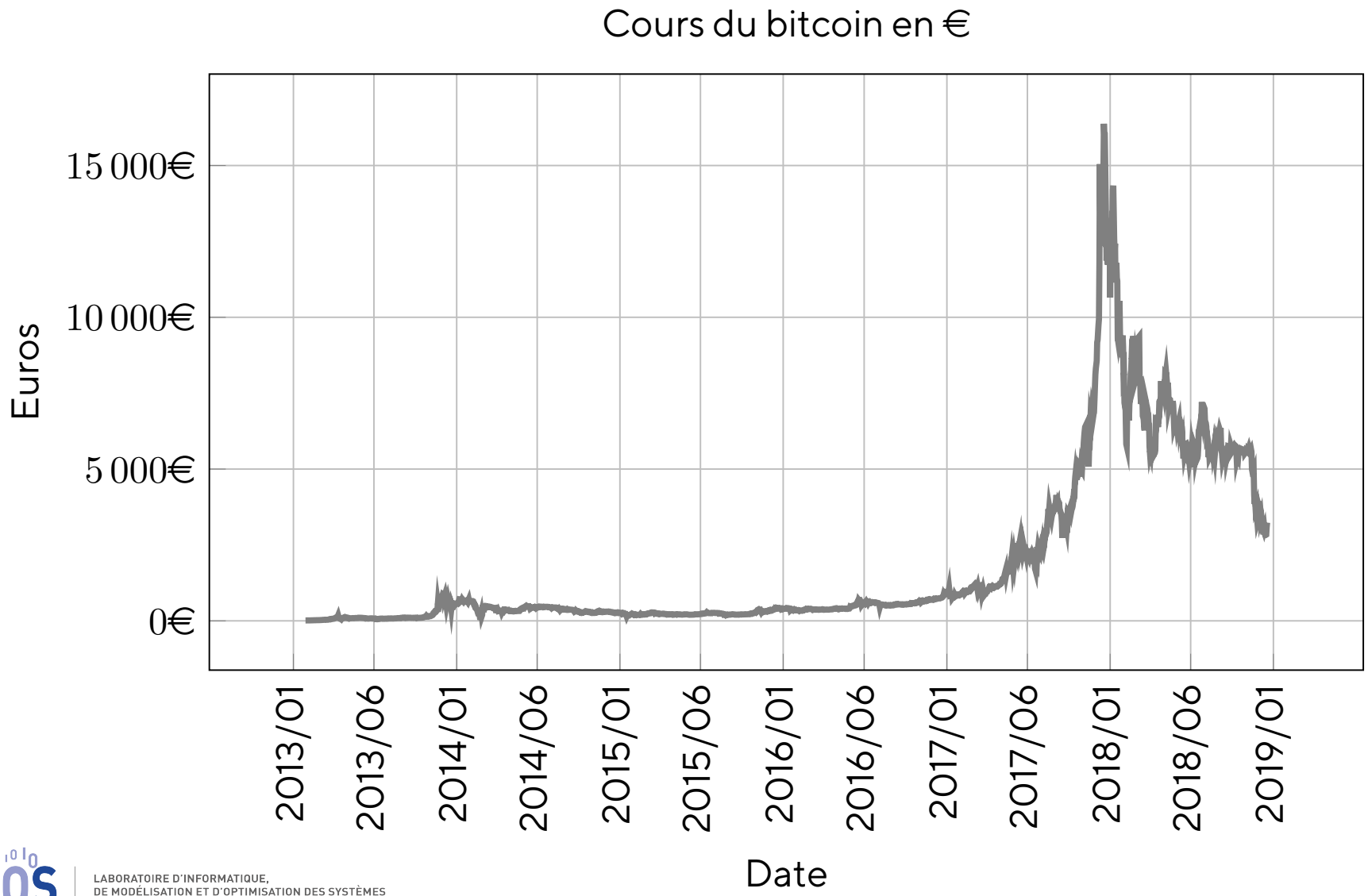


Bitcoin : monnaie électronique

Créée en 2008 par Satoshi Nakamoto (1 BTC $\approx$ 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

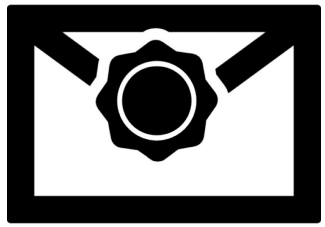
- DES
- AES

Chiffrement à clef publique

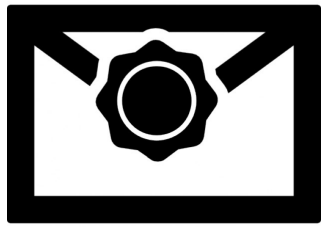
Exemples

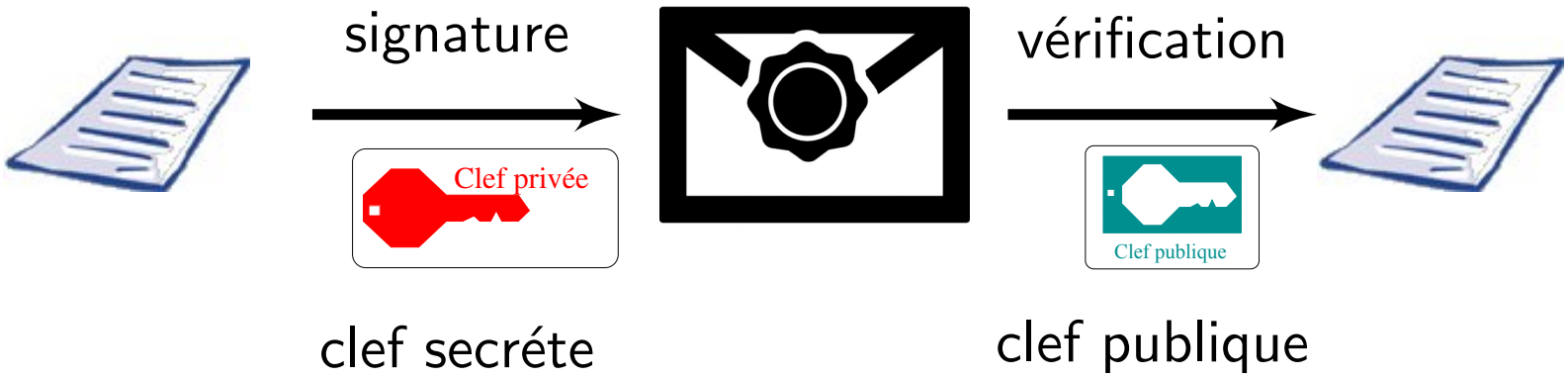
- RSA : $c = m^e \mod n$
- ElGamal : $c \equiv (g^r, h^r \cdot m)$

Signature



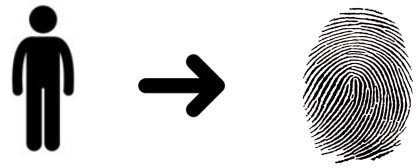
Signature



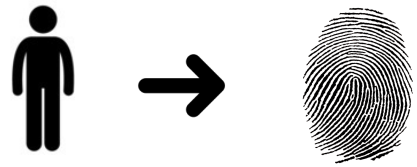


RSA: $m^d \mod n$

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

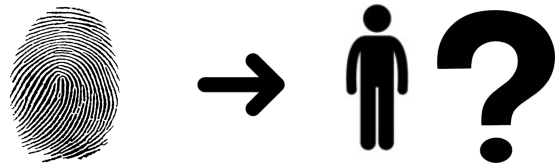


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)

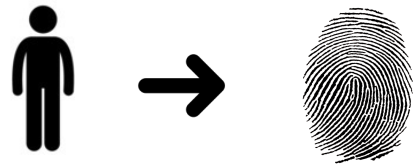


Propriétés de résistance

- Pré-image

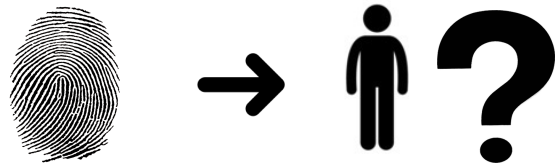


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)

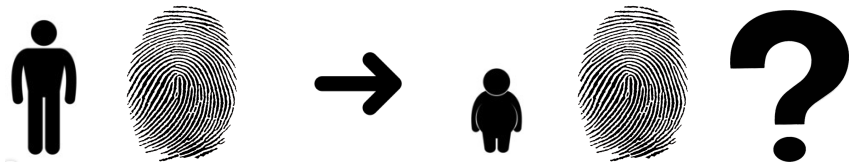


Propriétés de résistance

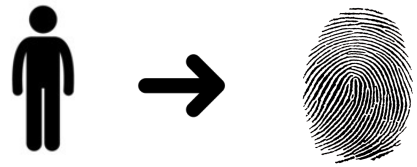
- Pré-image



- Seconde Pré-image

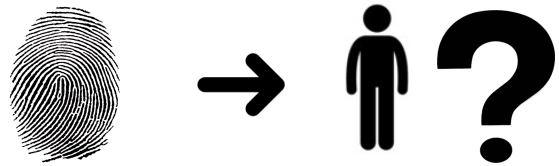


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)

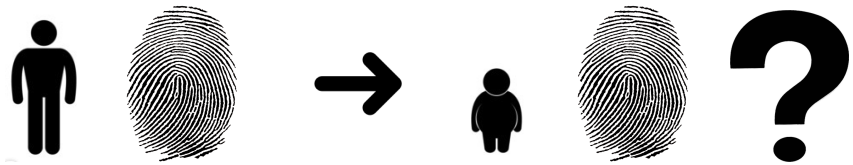


Propriétés de résistance

- Pré-image



- Seconde Pré-image



- Collision

Bitcoins : caractéristiques

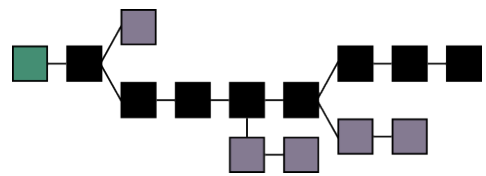
- Le nombre total de bitcoins est **fini**

  21 millions BTC

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

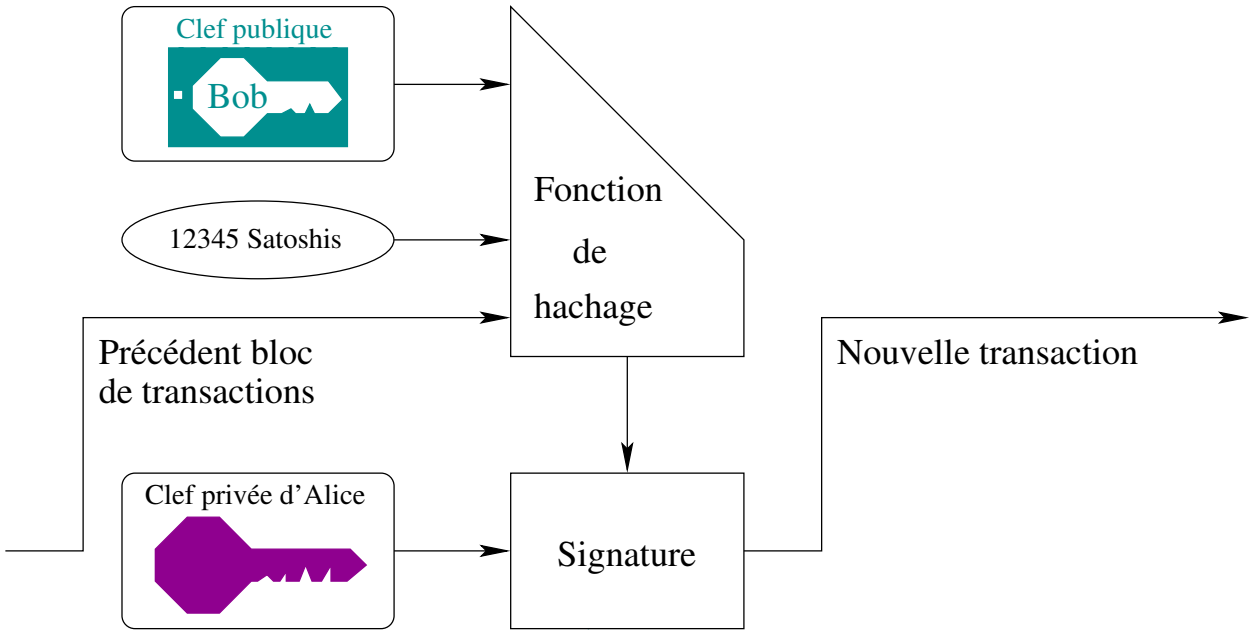
  $$\text{RIPEMD-160}(\text{SHA-256}(\text{ECDSA}_{pub}))$$

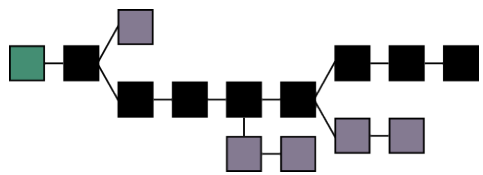
- Toutes les transactions sont **publiques**
- **Blockchain** : un système pair-à-pair qui garantit la validité des transactions



Comment faire une transaction?

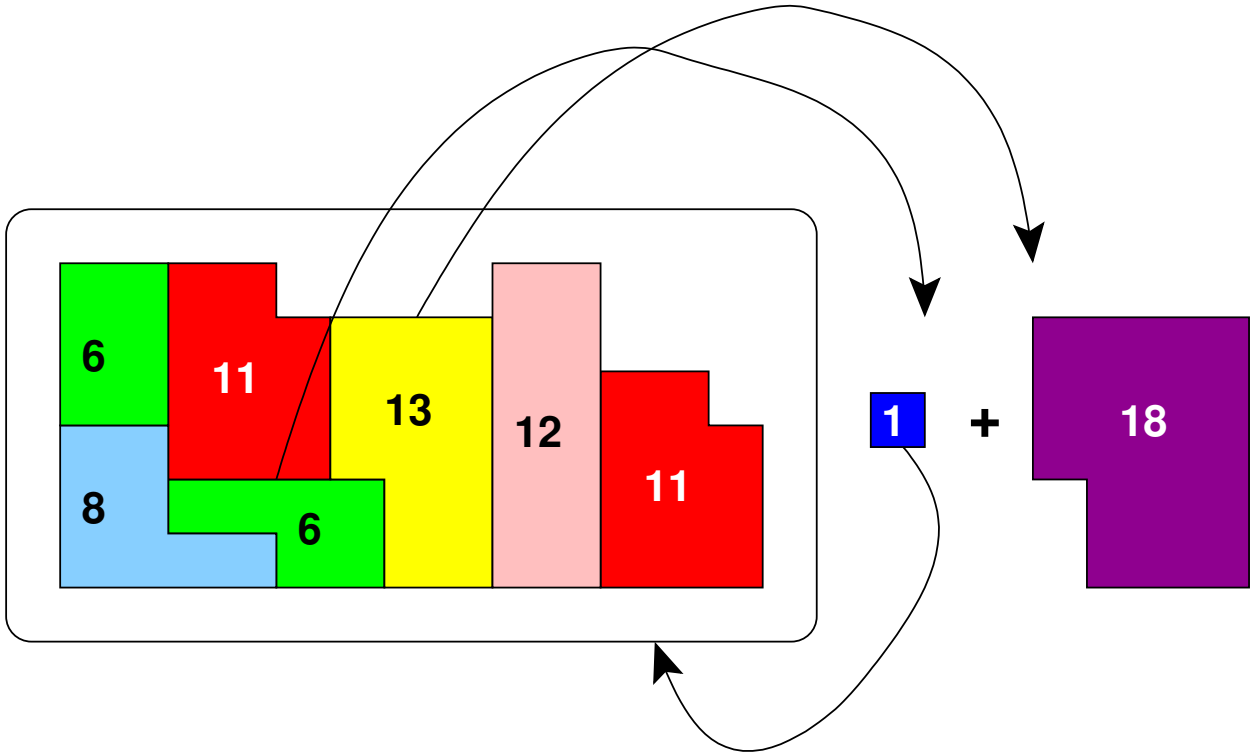
Alice donne 12345 Satochis ($\approx 5c$) à Bob.





Unspent Transaction Output UTXO

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

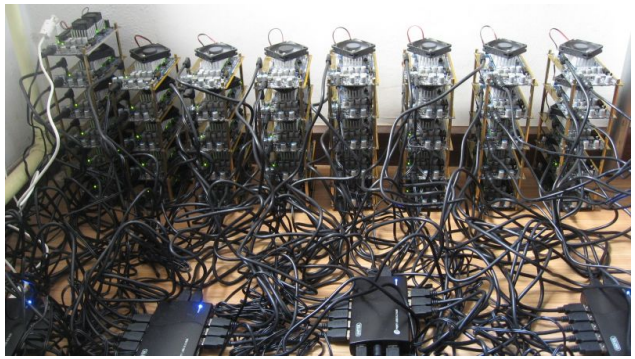
Numérique

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

🖨(A,B,3,424210)=458237

Etat de la chaîne 458237 C donne à B 9 BTC

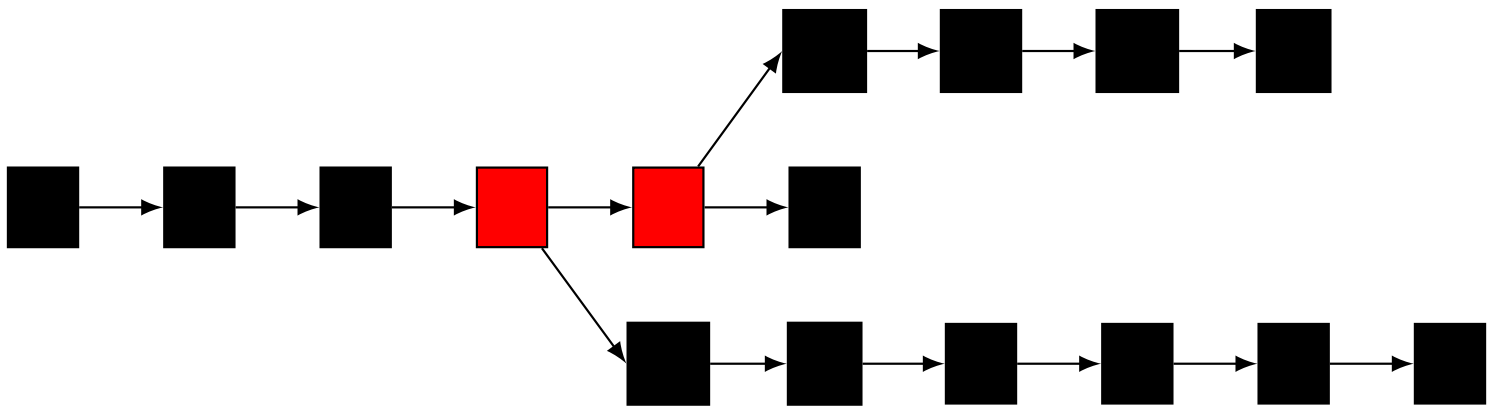
🖨(C,B,9,458237)=936127

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 = 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

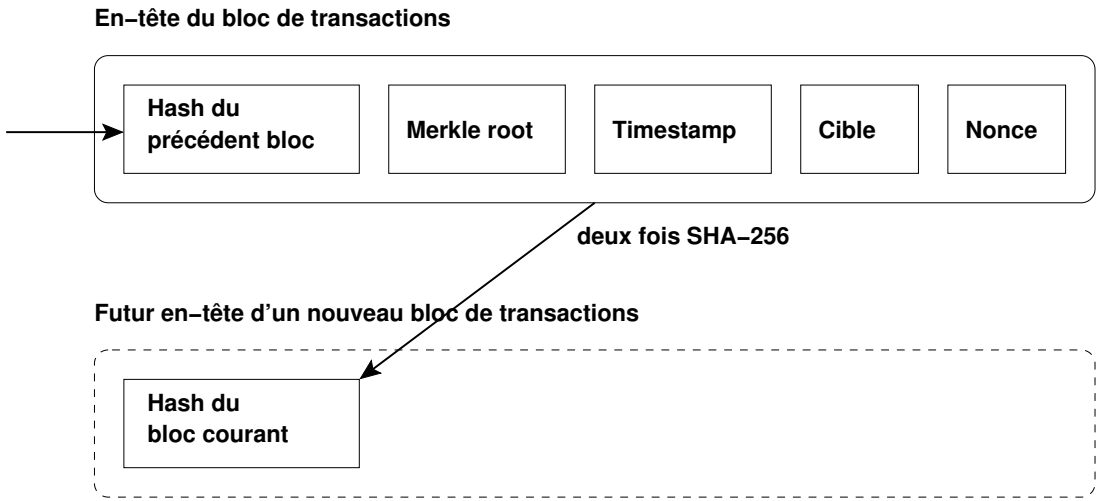
$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, n)) = x < \textit{Cible}$$

Avoir au moins 18 zéros au début de x

Stratégie : brute force

Tester toutes les valeurs possibles de n

Miner : Proof of work



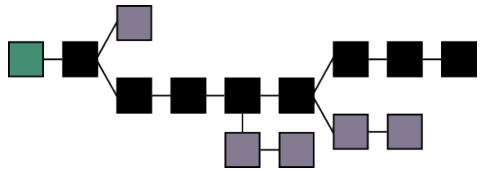
Avoir un zéro de plus au début

SHA-256(SHA-256(en-tête de bloc))

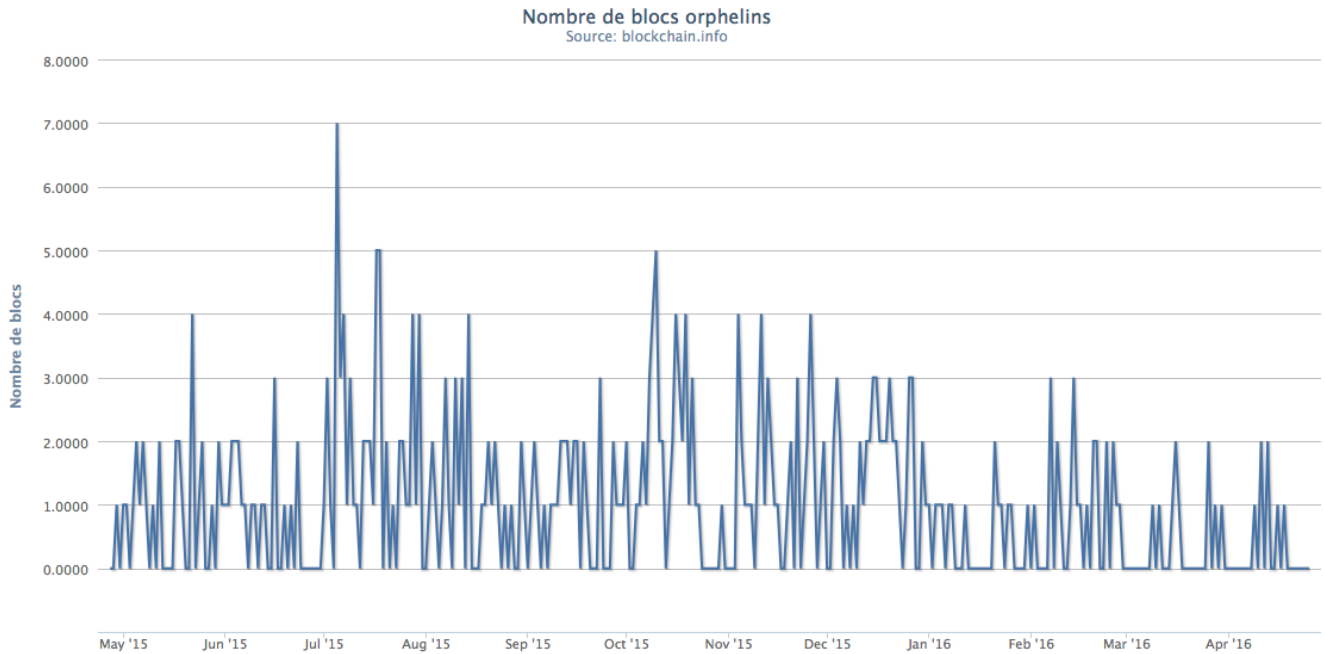
- les transactions passées (195 Go)
- les transactions à valider
- les secondes depuis 01/01/1970
- un nonce

Miner = Validation des transactions

Cible: 00000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076



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

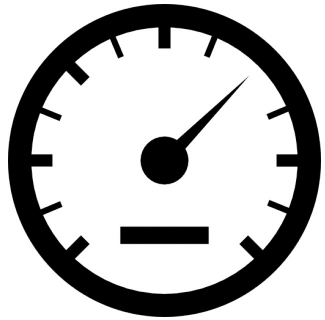


Traçable

Traçable

Snark

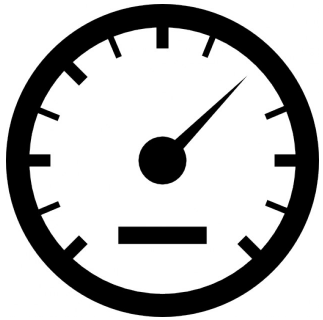
Limitations



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

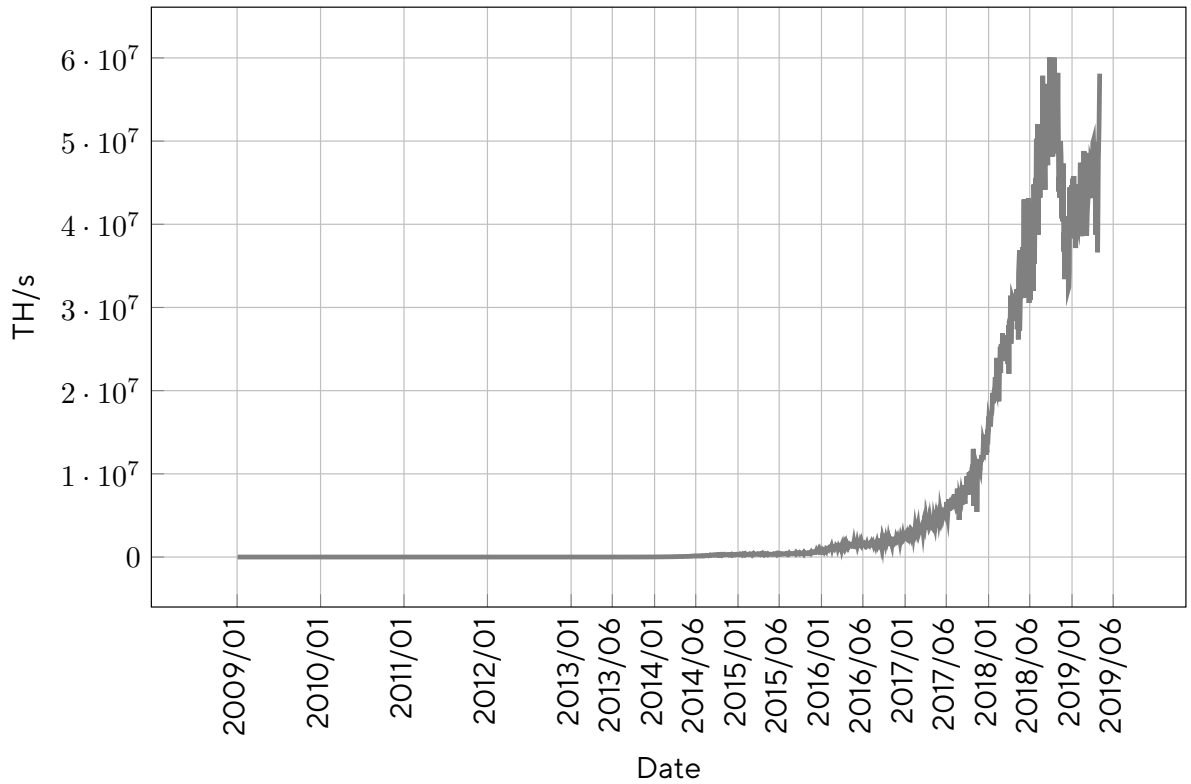
Energivore

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

Proof of Stake

Lightning Network

Énergivore



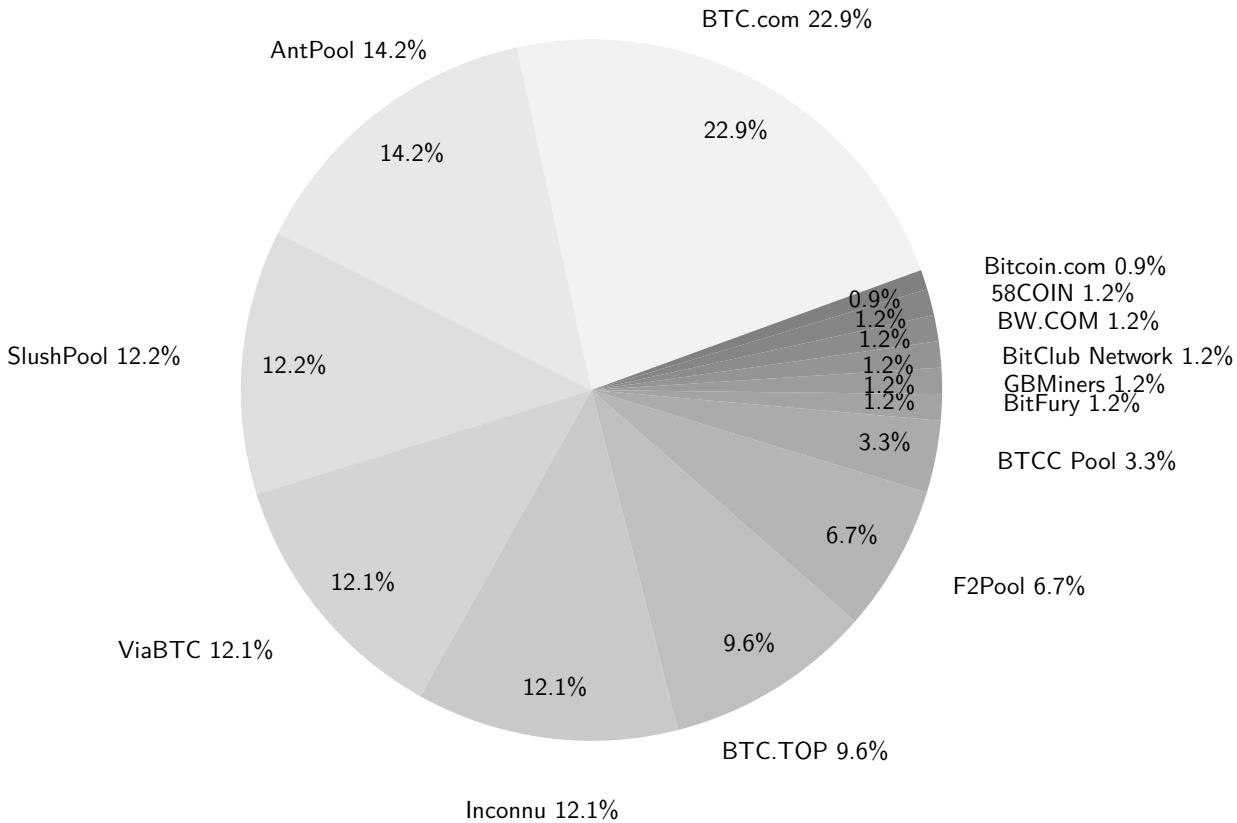
Estimation: plusieurs TWh annuels (comparable à un petit état).

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

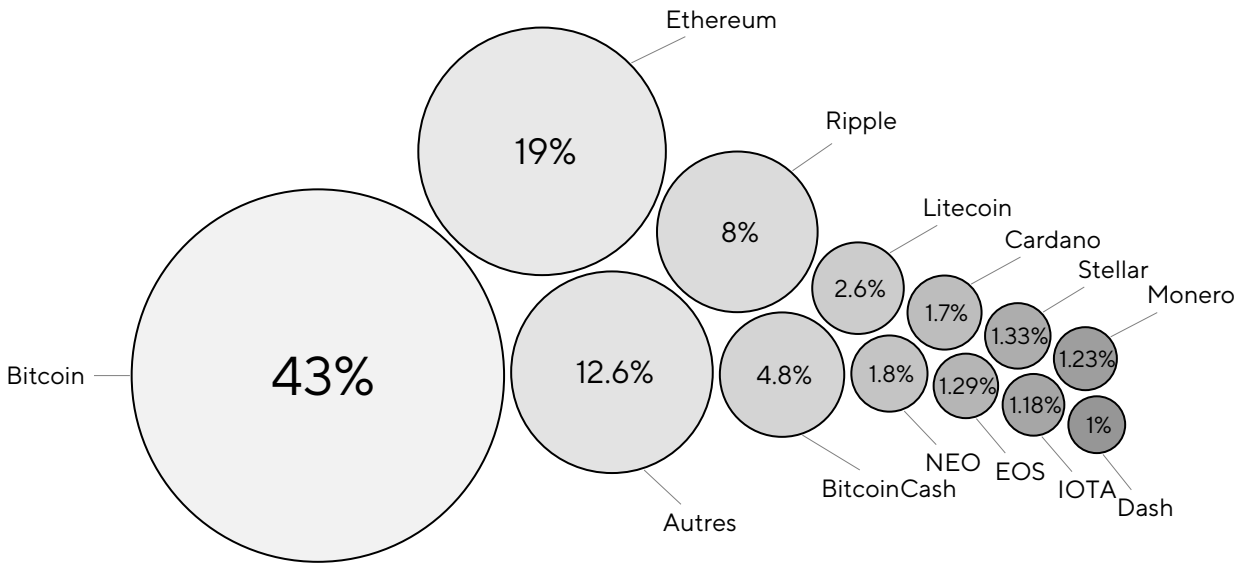
- Cible : 74 zéros initiaux, $\frac{1}{2^{74}}$ chances de miner
- $44\,000\,000$ MH/s $= 4.4\,10^{13}$ H/s $\approx 2^{45.3}$ H/s
- $2^{28.7} \approx 4.3\,10^{8}$ s $\approx 5\,000$ jours ≈ 13.6 années de calcul d'un Ebit E11++
- Réseau mondial $\approx 700\,000$ E11

Fermes de mineurs



Plan

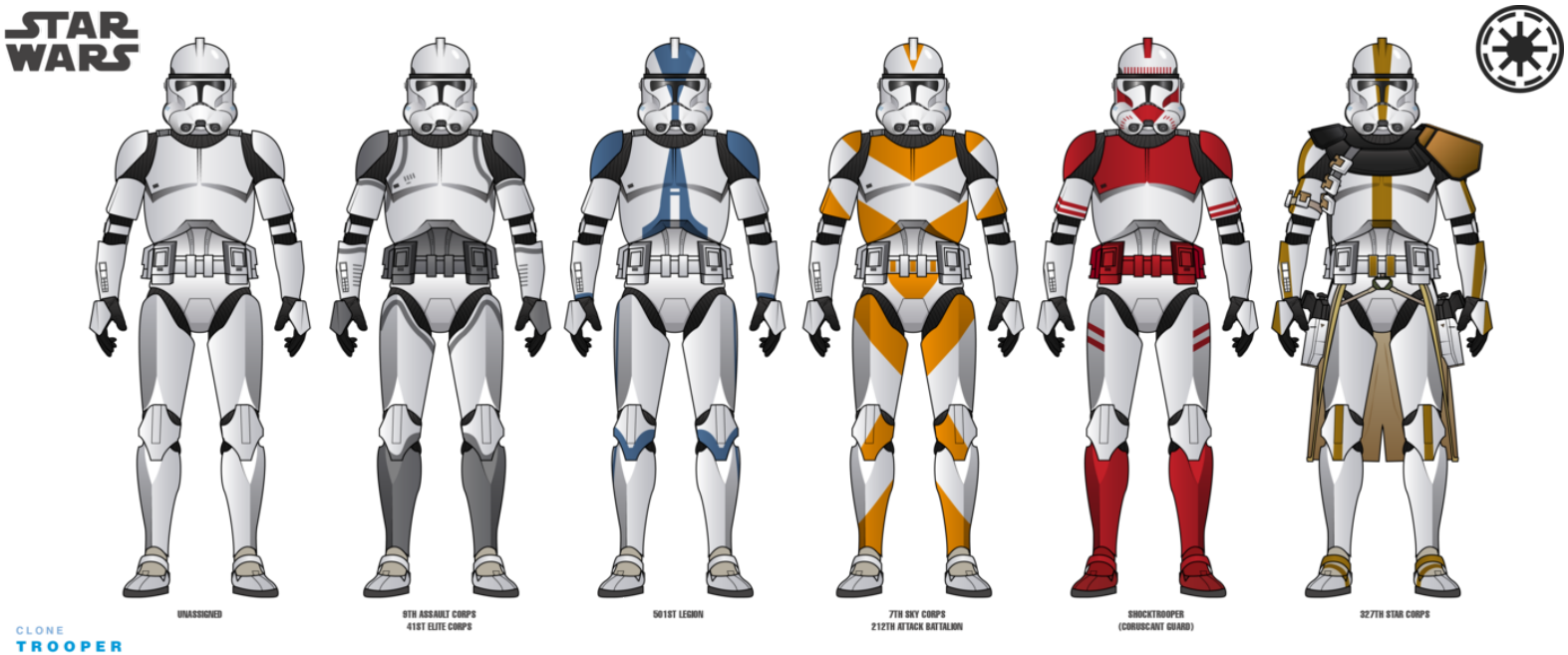
Diversité monétaire



Autres crypto-monnaies

Classification I : Pourris

Classification II : Clones de Bitcoin



Classification III : Plus utile

Classification IV : Autres preuves de travail

ethereum

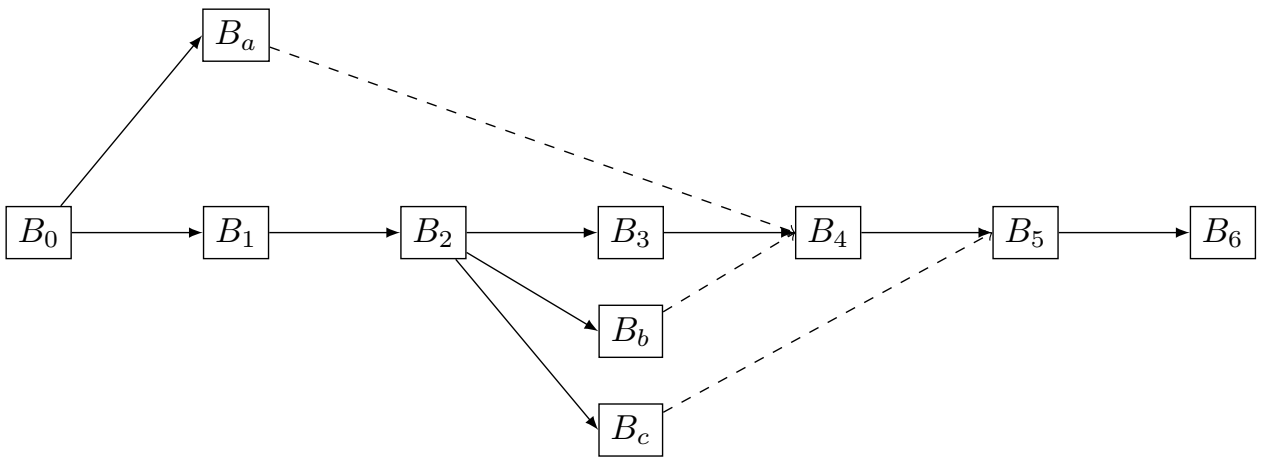
Etherum

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

ethereum

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

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

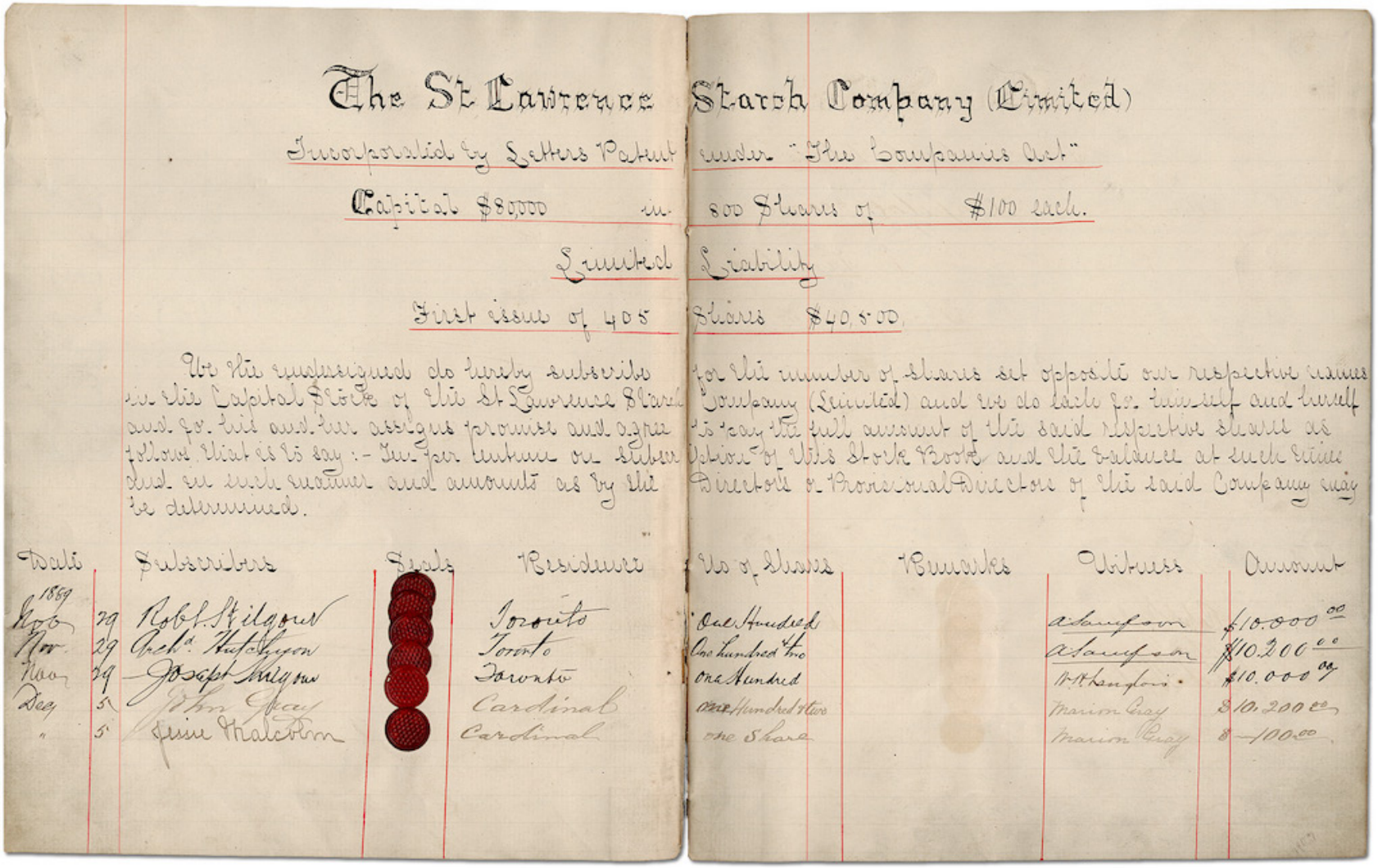


- Perte ou vol de la clef secrète = irréversible
- Monnaie anonyme et traçable



Plan

Blockchain



The St Lawrence Starch Company (Limited)

Incorporated by Letters Patent under "The Companies Act."

Capital $80000 in 800 Shares of $100 each.

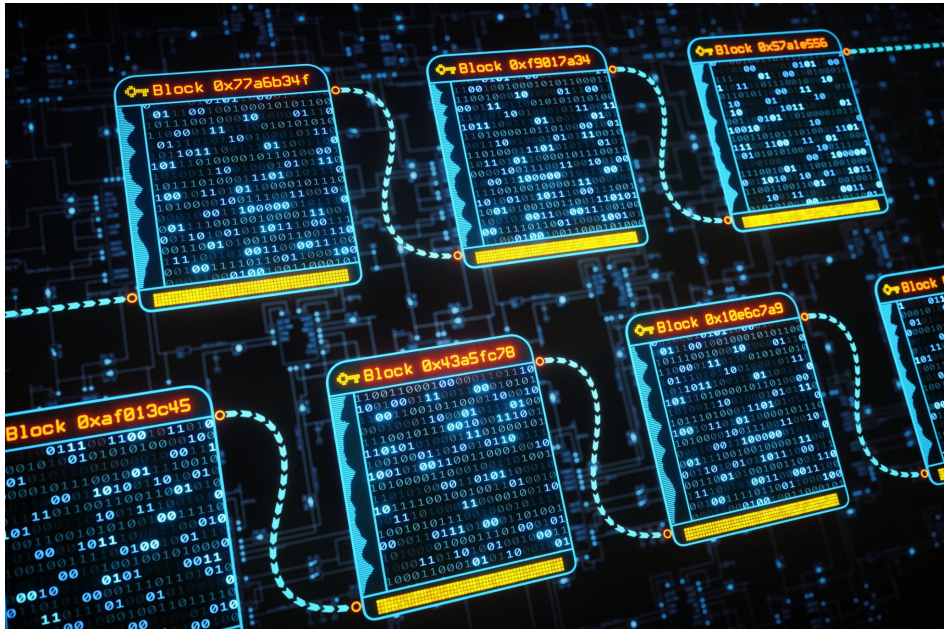
Limited Liability

First issue of 405 Shares $40500

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 pay the full amount of the said respective shares as called for by the Stock Books and the By-laws at such time or times as the 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		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

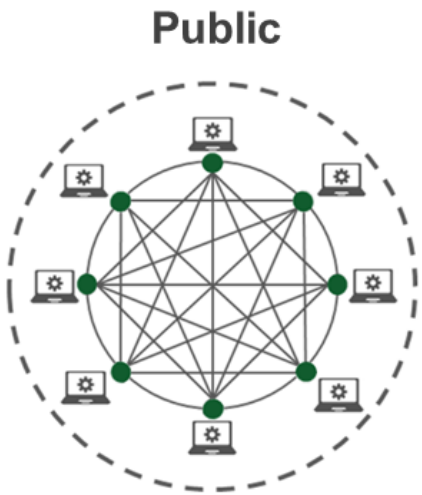


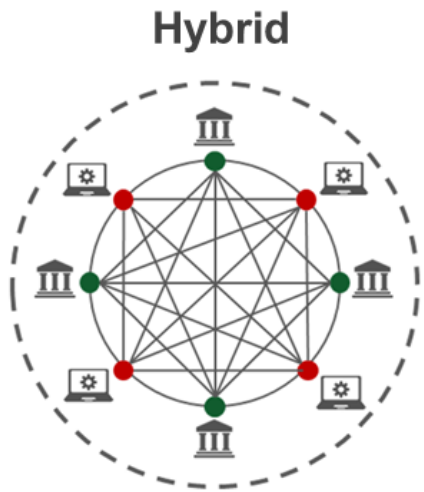
Registre distribué, sécurisé, infalsifiable

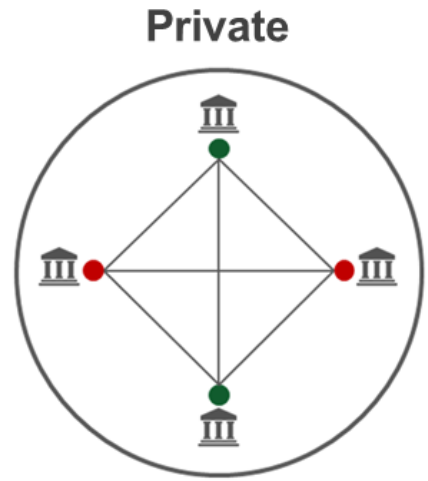
Mineurs valident des transactions

Tiennent à jour le registre distribué

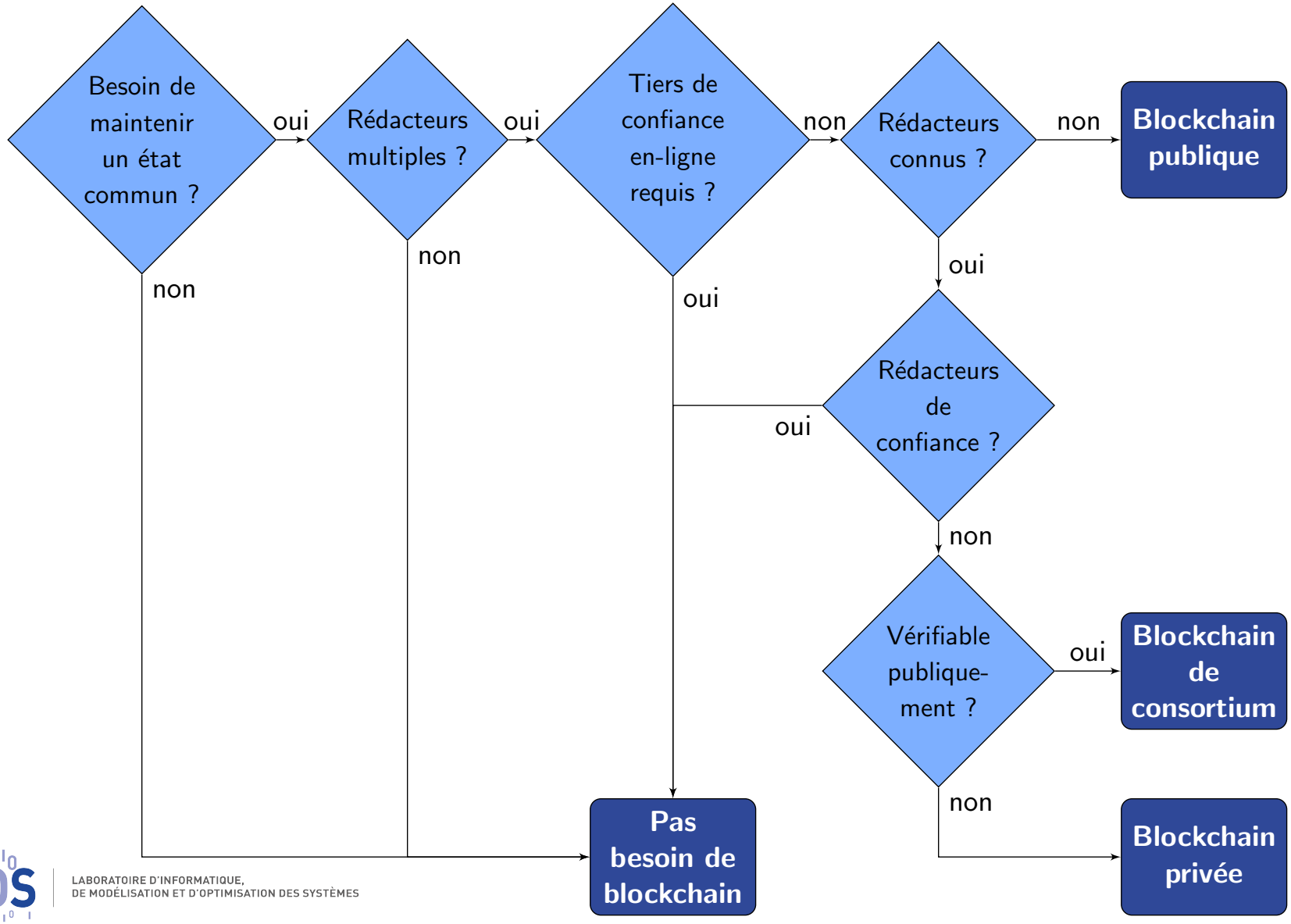
Blockchain Privée vs Publique



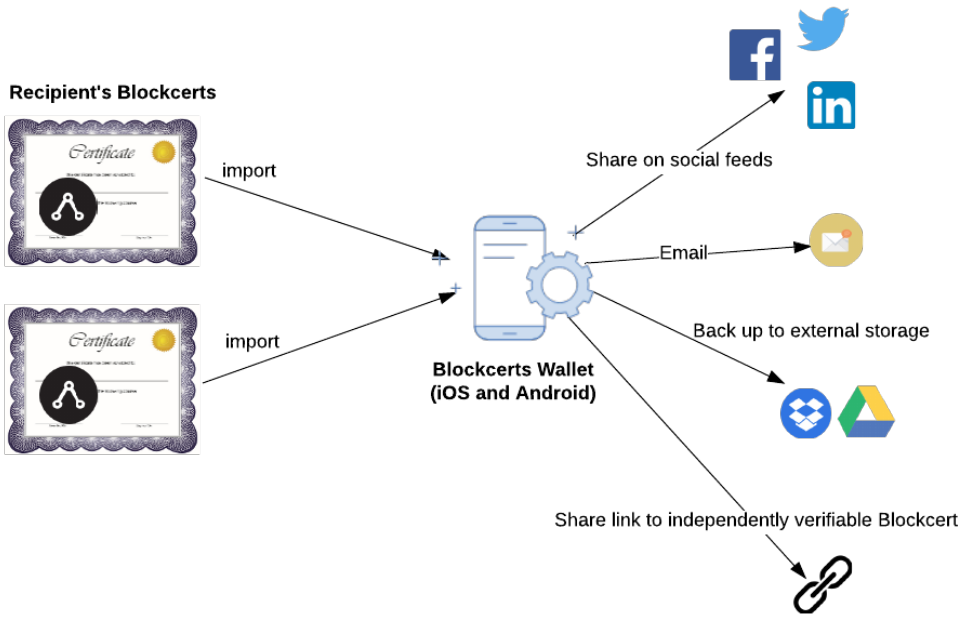




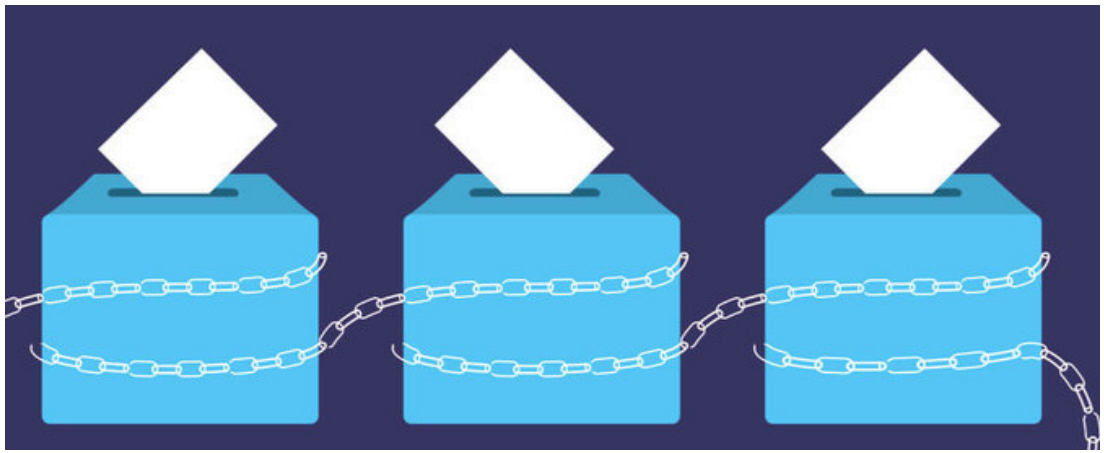
Ai-je besoin d'une blockchain ?



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 ...

Blockchain Applications

Certificates (Laposte, EDF ...)

E-commerce

E-Health

...

Plan

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

Collaborations possibles ...

Merci pour votre attention

Questions ?

pascal.lafourcade@uca.fr

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