

Bitcoin et la Blockchain

Pascal Lafourcade
Université Clermont Auvergne



Campus Cyber
7 novembre 2023

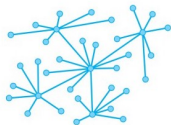
La révolution Bitcoin 2009



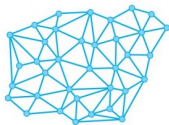
► Crypto-monnaie décentralisée et distribuée



Système centralisé



Système décentralisé



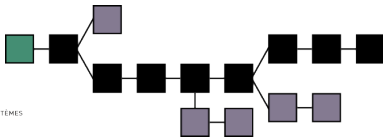
Système distribué



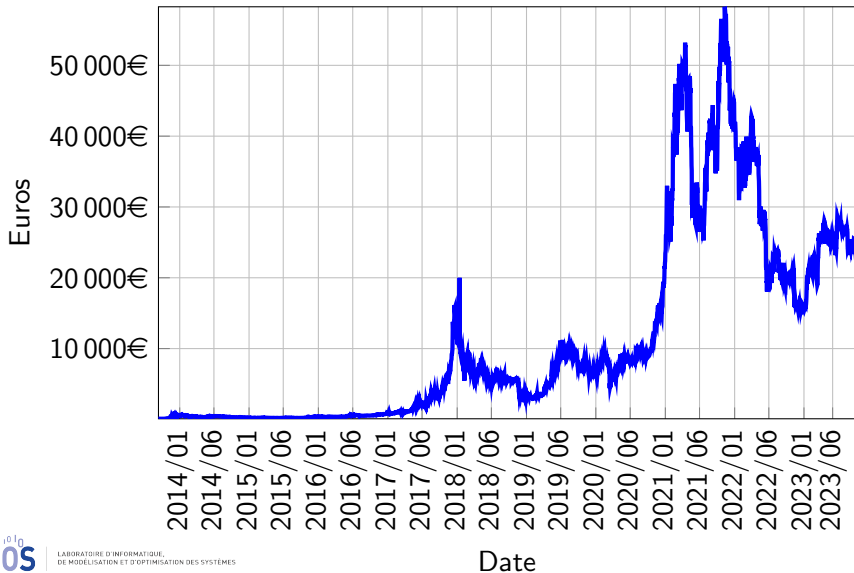
21 millions BTC

► Inarrêtable car distribuée

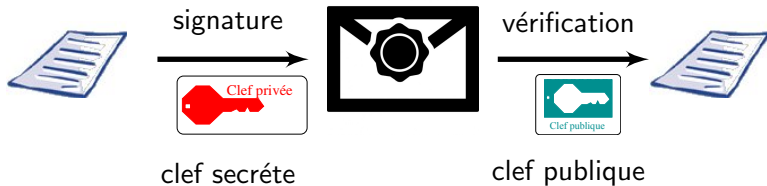
► Infalsifiable et auditable



Taux de change du bitcoin

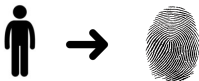


Signature



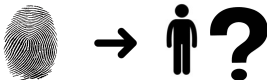
RSA: $m^d \bmod n$

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



Propriétés de résistance

▶ Pré-image



▶ Seconde Pré-image



▶ Collision



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 = 00000000000000000000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076



Trouver une nombre n tel que

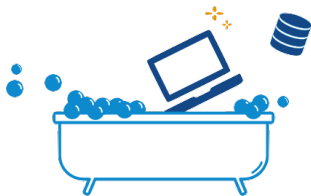
$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, n)) = x < \text{Cible}$$

Avoir au moins 18 zéros au début de x


Stratégie : brute force

Tester toutes les valeurs possibles de n

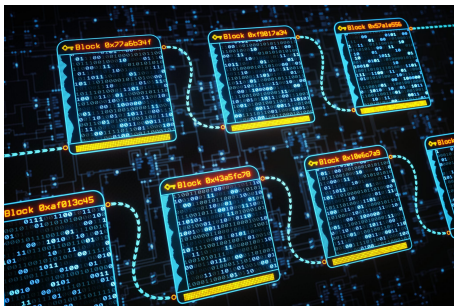
Freins



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 time 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 time as the Board of 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	Robt Kilgus Chas. Nicholson Joseph Wilson John Gray Sam. Halperin		Toronto Toronto Toronto Cardinal Cardinal	One Hundred One Hundred Two One Hundred One Hundred Six One Share		Thompson Thompson Thompson Main Bay Main Bay	\$10,000.00 \$10,200.00 \$10,000.00 \$10,200.00 \$100.00

Blockchain

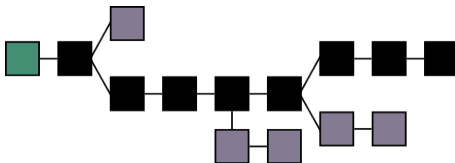


Registre distribué, sécurisé, infalsifiable

Mineurs valident des transactions

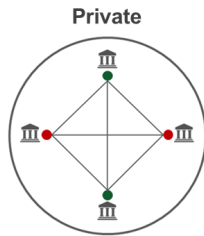
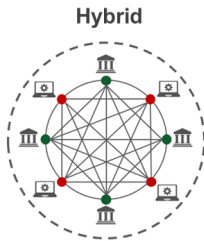
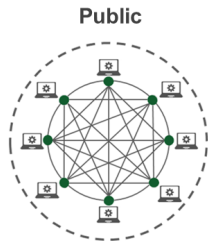


Tiennent à jour le registre distribué

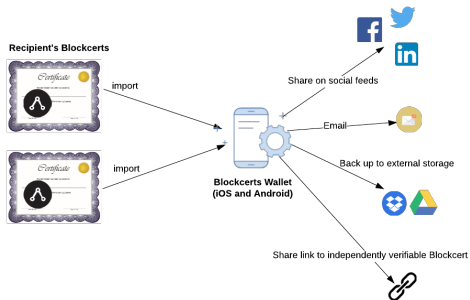


Inarrêtable, Infalsifiable, Auditable

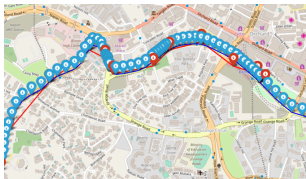
Blockchain Privée vs Publique



Blockchain Application : MIT Diploma



EcoMobiCoin: Proof of Behavior



Choses à retenir

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

Merci pour votre attention

Questions ?



pascal.lafourcade@uca.fr