

Fonctionnement de la Blockchain

Pascal Lafourcade



24 Septembre 2020

Plan

À l'origine : Bitcoin

Un peu de cryptographie

Au coeur de Bitcoin

Altcoins

Conclusion

Plan

À l'origine : Bitcoin

Un peu de cryptographie

Au coeur de Bitcoin

Altcoins

Conclusion

Bitcoin : monnaie électronique

Créée en 2008 par Satoshi Nakamoto (1 BTC \approx 9271 euros 17 Septembre 2020)



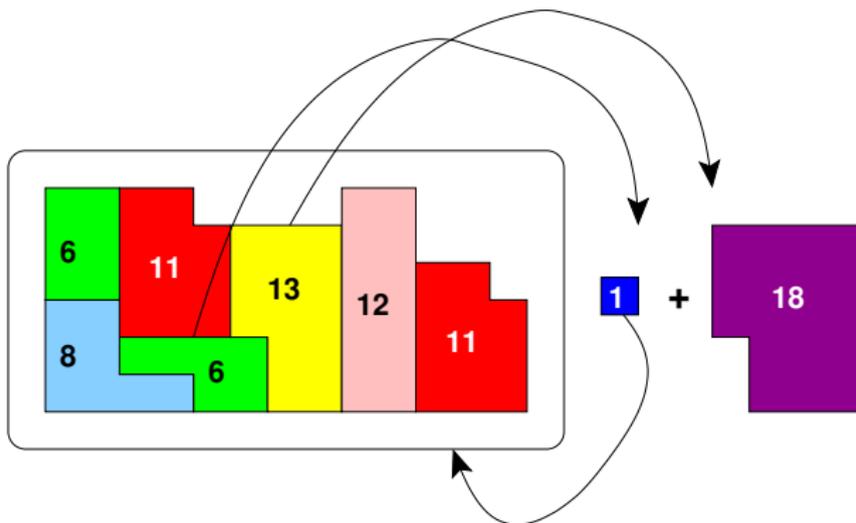
1	BTC = 1 Bitcoin	
0,01	BTC = 1 cBTC	= 1 centiBitcoin (ou bitcent)
0,001	BTC = 1 mBTC	= 1 milliBitcoin
0,000 001	BTC = 1 μ BTC	= 1 microBitcoin
0,000 000 01	BTC = 1 Satoshi	

Taux de change du bitcoin



Payer 18 BTC avec des pièces

 *Nous acceptons
Les **bitcoins***



Propriétés d'une monnaie électronique

- ▶ Non-Falsifiable (Unforgeable)



- ▶ Eviter la double dépense & identification fraudeur & "présomption d'innocence"



- ▶ Respect de la vie privée :

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



Plan

À l'origine : Bitcoin

Un peu de cryptographie

Au coeur de Bitcoin

Altcoins

Conclusion

Clef symétrique



Exemples

- ▶ DES
- ▶ AES

Chiffrement à clef publique



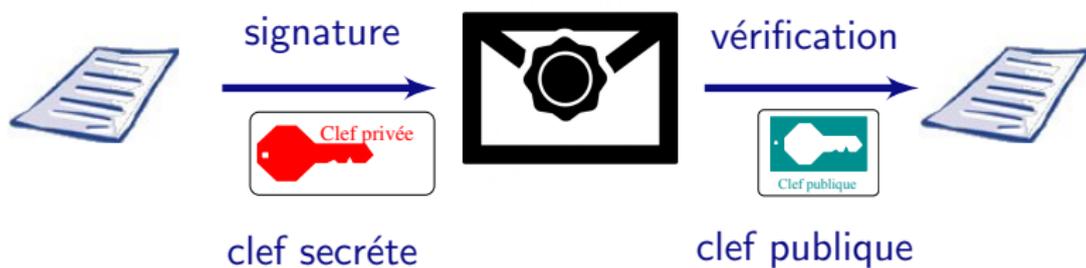
Exemples

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

Signature



Signature



$$\text{RSA: } m^d \text{ mod } n$$

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

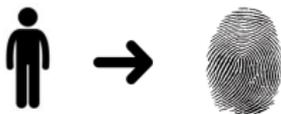
► Pré-image



► Seconde Pré-image



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



Propriétés de résistance

► Pré-image



► Seconde Pré-image



► Collision



Plan

À l'origine : Bitcoin

Un peu de cryptographie

Au coeur de Bitcoin

Altcoins

Conclusion

Bitcoins : caractéristiques

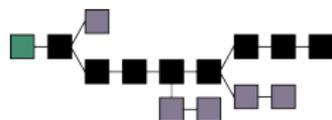
- ▶ Le nombre total de bitcoins est **fini**

21 millions BTC

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

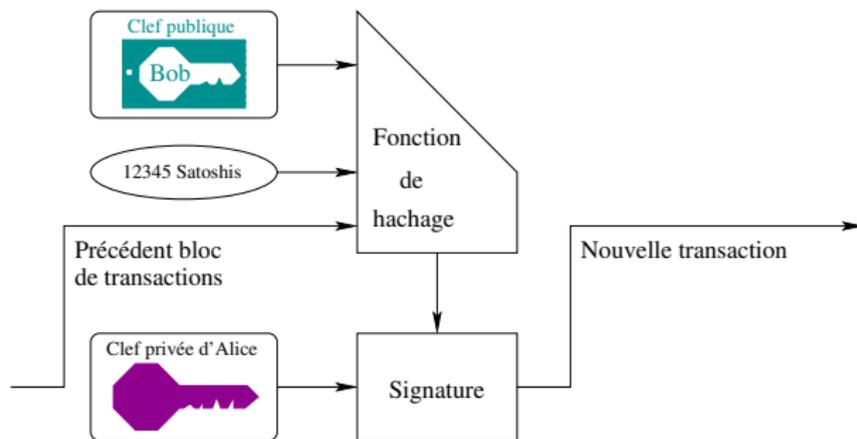
$\text{RIPEMD-160}(\text{SHA-256}(\text{ECDSA}_{pub}))$

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

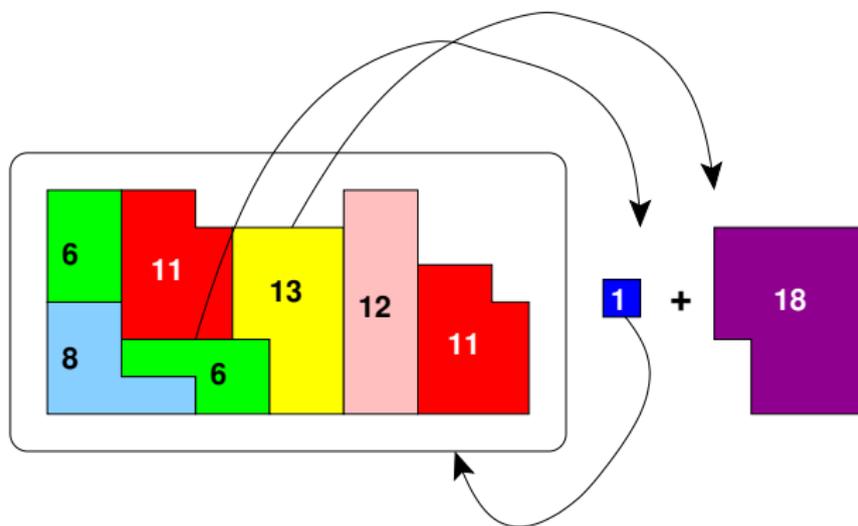


Comment faire une transaction?

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



Payer 18 BTC avec des pièces



- Seuls des bitcoins possédés peuvent être dépensés

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 = 00000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076



Trouver un nombre n tel que

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

Avoir un 0 plus de au début de x

Miner : Objectif de hachage

Cible = 00000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076



Trouver un nombre n tel que

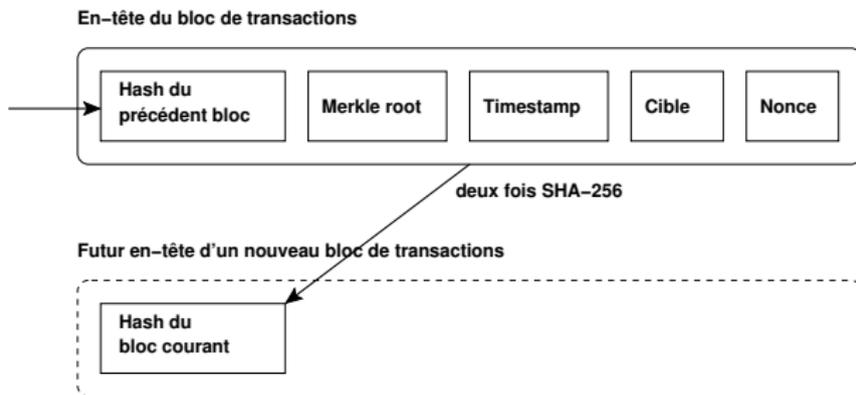
$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, n)) = x < \text{Cible}$$

Avoir un 0 plus de au début de x

Stratégie : brute force

Tester toutes les valeurs possibles de n

Miner : Proof of work

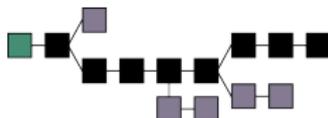


Avoir un zéro de plus au début
 $\text{SHA-256}(\text{SHA-256}(\text{en-tête de bloc}))$

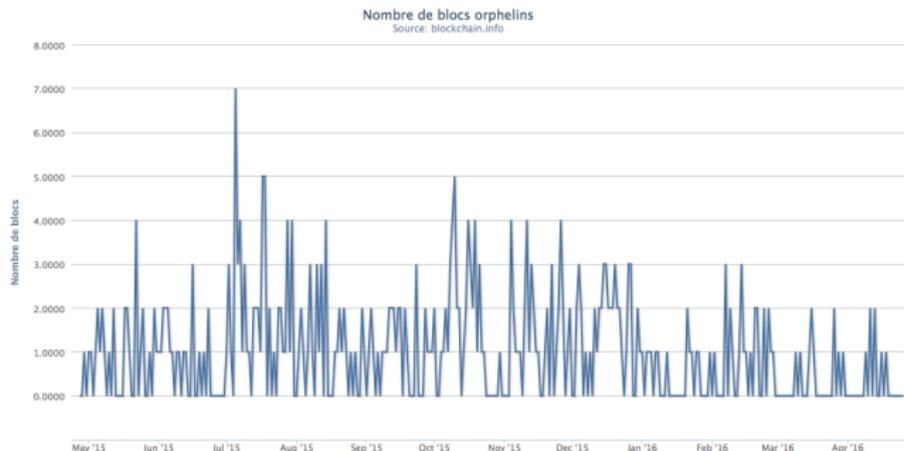
- ▶ les transactions passées (95 Go)
- ▶ les transactions à valider
- ▶ les secondes depuis 01/01/1970
- ▶ un nonce
- ▶ etc ...

Miner = Validation des transactions

Cible: 00000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076



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



Plan

À l'origine : Bitcoin

Un peu de cryptographie

Au coeur de Bitcoin

Altcoins

Conclusion

Autres crypto-monnaies



Classification des Altcoins

1. "Pourris coins"
2. Clônes de Bitcoin
3. Minage plus utiles, moins énergivores
4. Non-basés sur la preuve de travail
 - ▶ Proof of Stake (Peercoin)
 - ▶ Proof of Retreivability (Permacoin)
 - ▶ Proof of Capacity (Burstcoin)
 - ▶ Proof of Space (SpaceMint)



Plan

À l'origine : Bitcoin

Un peu de cryptographie

Au coeur de Bitcoin

Altcoins

Conclusion

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



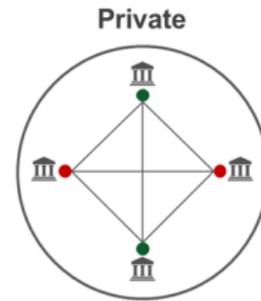
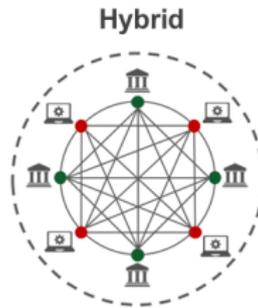
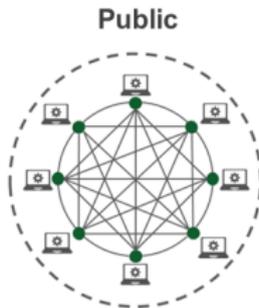
- ▶ Perte ou vol de la clef secrète = irréversible
- ▶ Monnaie anonyme et traçable



BlockChain

Registre sécurisé

- ▶ Distribué
- ▶ Infalsifiable
- ▶ Auditable
- ▶ Décentralisé



Merci pour votre attention

Questions

Les
**BLOCK
CHAINS**

EN 50 QUESTIONS

Comprendre le fonctionnement et les enjeux
de cette technologie innovante

