Bitcoins

Pascal Lafourcade

Chaire industrielle,
Confiance numérique

Clermontech 17 mai 2016
Saint Pascal

Clef symétrique

Exemples

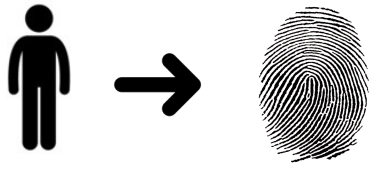
- DES
- AES

Chiffrement à clef publique

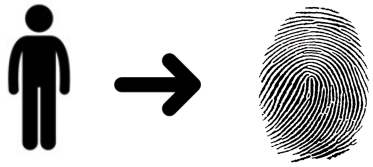
Exemples

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

Fonction de Hachage (SHA-1, SHA-3)

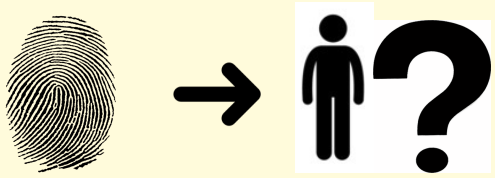


Fonction de Hachage (SHA-1, SHA-3)

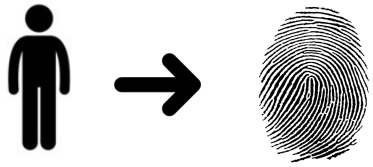


Propriétés de résitance

- Pré-image

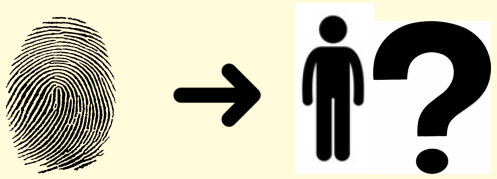


Fonction de Hachage (SHA-1, SHA-3)

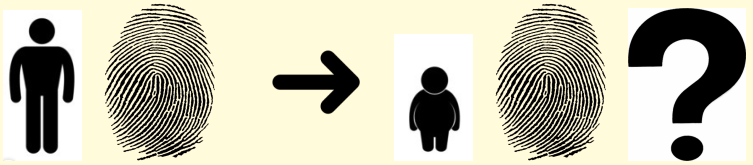


Propriétés de résitance

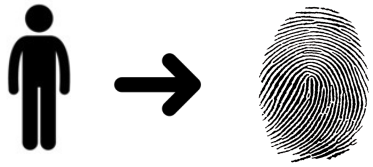
- Pré-image



- Seconde Pré-image

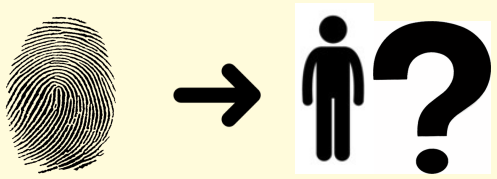


Fonction de Hachage (SHA-1, SHA-3)

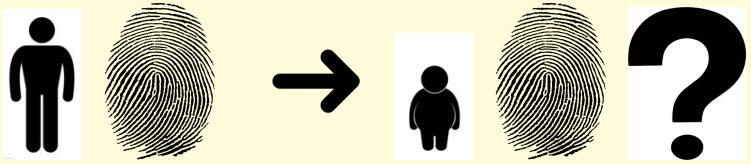


Propriétés de résitance

- Pré-image

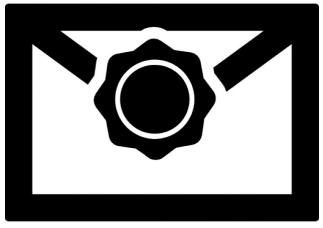


- Seconde Pré-image

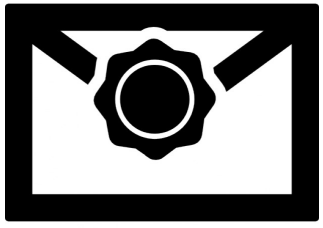


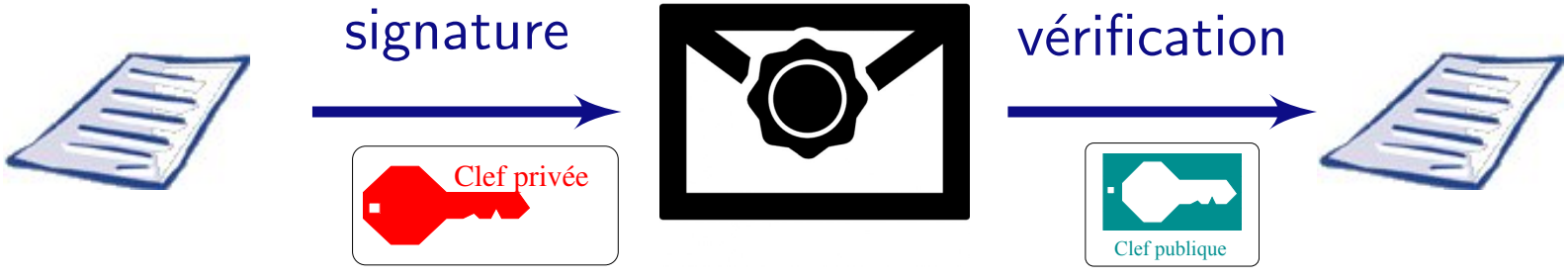
- Collision

Signature



Signature





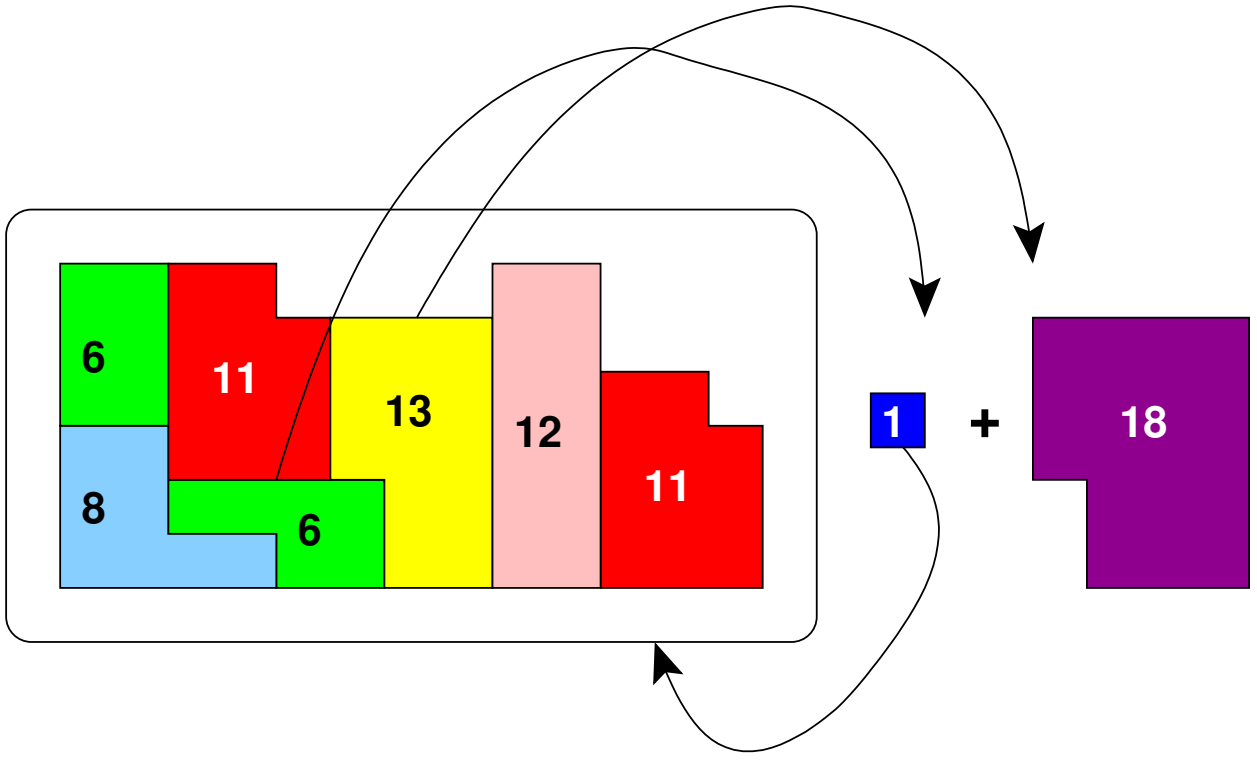
RSA: $m^d \mod n$

Bitcoin : monnaie électronique

Créée en 2008 par Satoshi Nakamoto (1 BTC $\approx$ 405 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	

Payer avec des bitcoins 18 BTC



Bitcoins : caractéristiques

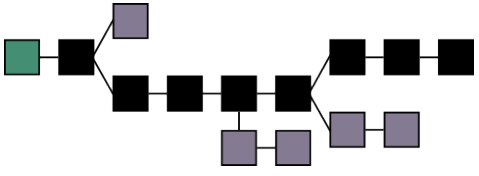
- Le nombre total de bitcoins est **fini**

  21 millions BTC

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

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

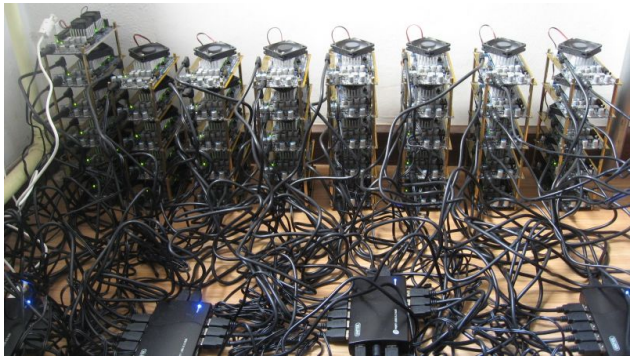
- Toutes les transactions sont **publiques**
- **Blockchain** : un système pair-à-pair qui garantit la validité des transactions



Miner des Bitcoins

Miner des Bitcoins

Les "*mineurs*" valident les transactions contre des bitcoins



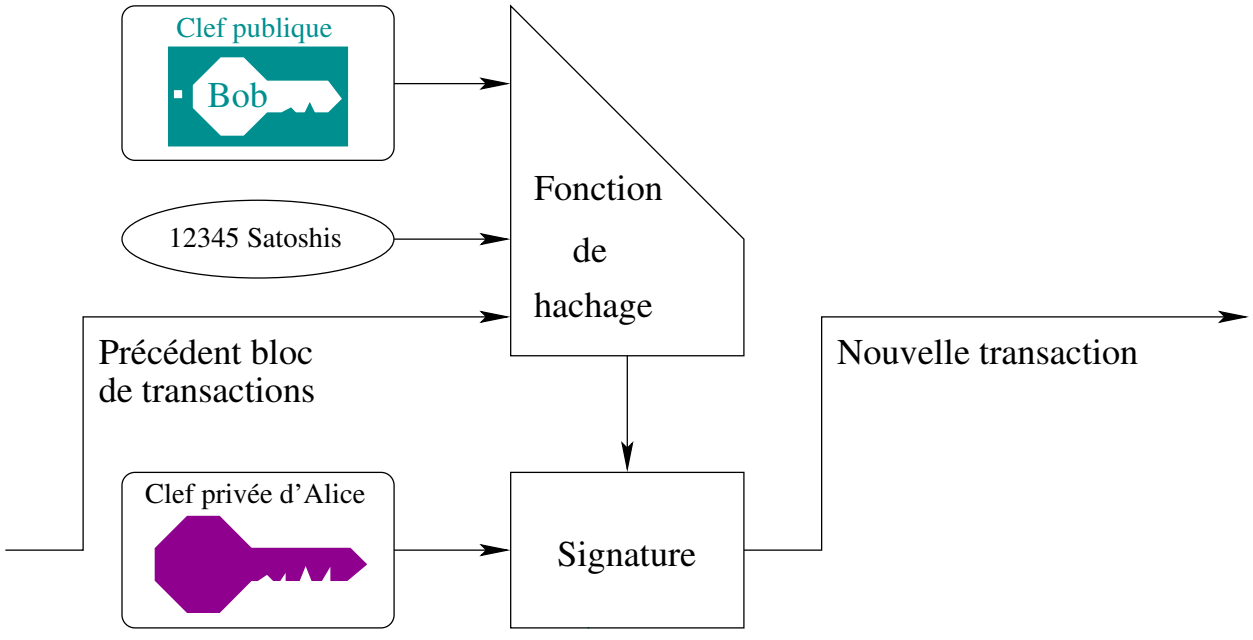
Miner des Bitcoins

- Valider = résoudre un **objectif de hachage**
- Récompense initiale 50 BTC pour une validation
- Divisée par 2 tous les 210000 validations

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

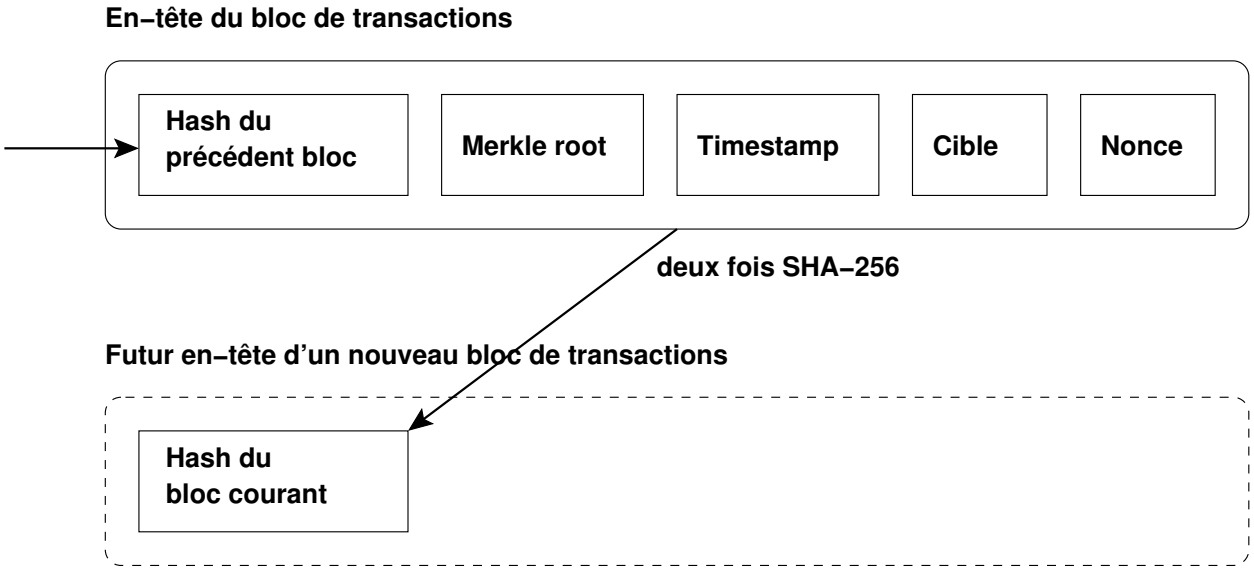
Bitcoins : Fonctionnement

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



- Seuls des bitcoins possédés peuvent être dépensés

Bitcoins : Objectif de hachage (Proof of work)



Avoir un zéro de plus au début

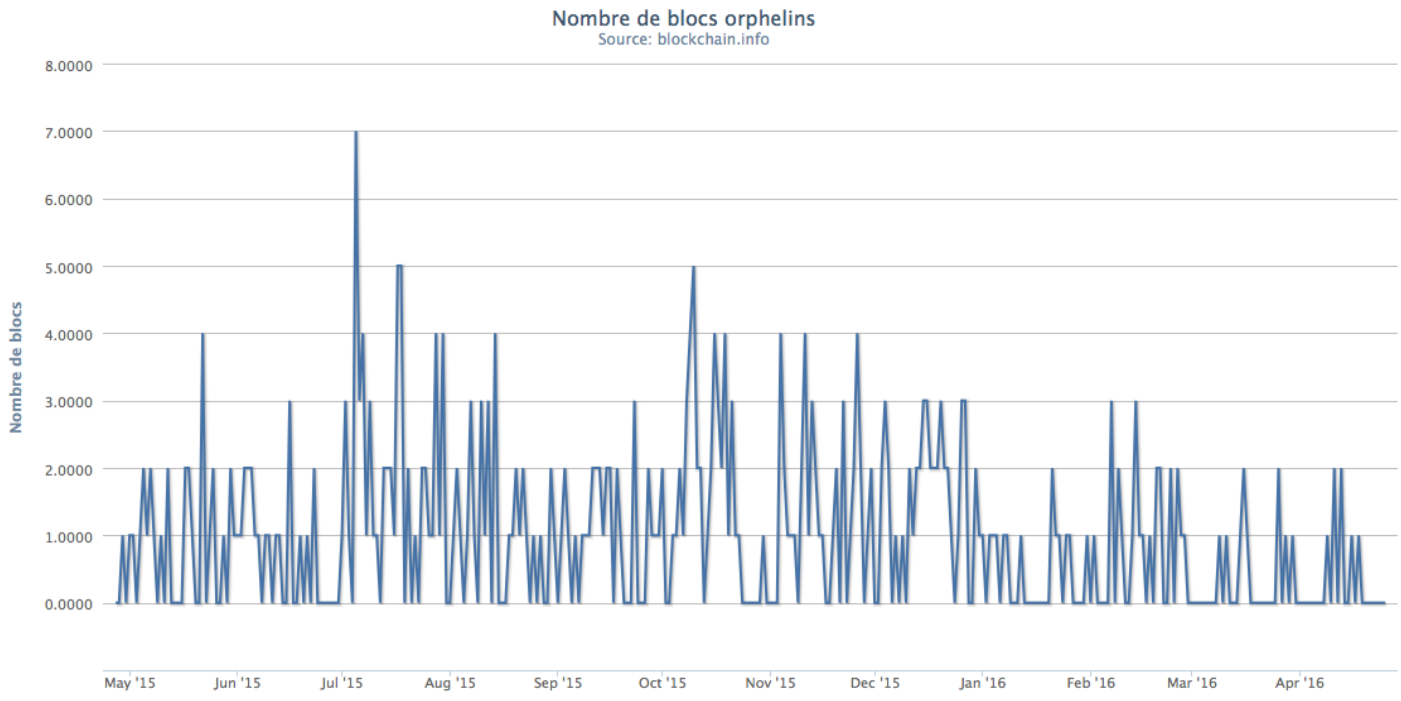
SHA-256(SHA-256(en-tête de bloc))

- les transactions passées (65 Go)
- les transactions à valider
- les secondes depuis 01/01/1970
- un nonce
- etc ...

Bitcoins : Validation des transactions

000000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076

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



Autres crypto-monnaies > 112

Chaîne de Cunningham

$1 \leq i < n, p_{i+1} = ap_i + b$ pour des premiers entre eux fixés a, b

Séminaire Confiance numérique

Jordi Herrera, Universitat Autonòma de Barcelona (UAB)

Is bitcoin a suitable research topic?

`http://confiance-numerique.clermont-universite.fr`

Merci pour votre attention.

Questions ?