Bitcoin, comment ça marche ?

Pascal Lafourcade

LIMOS

UNIVERSITÉ Clermont Auvergne

8 mars 2017

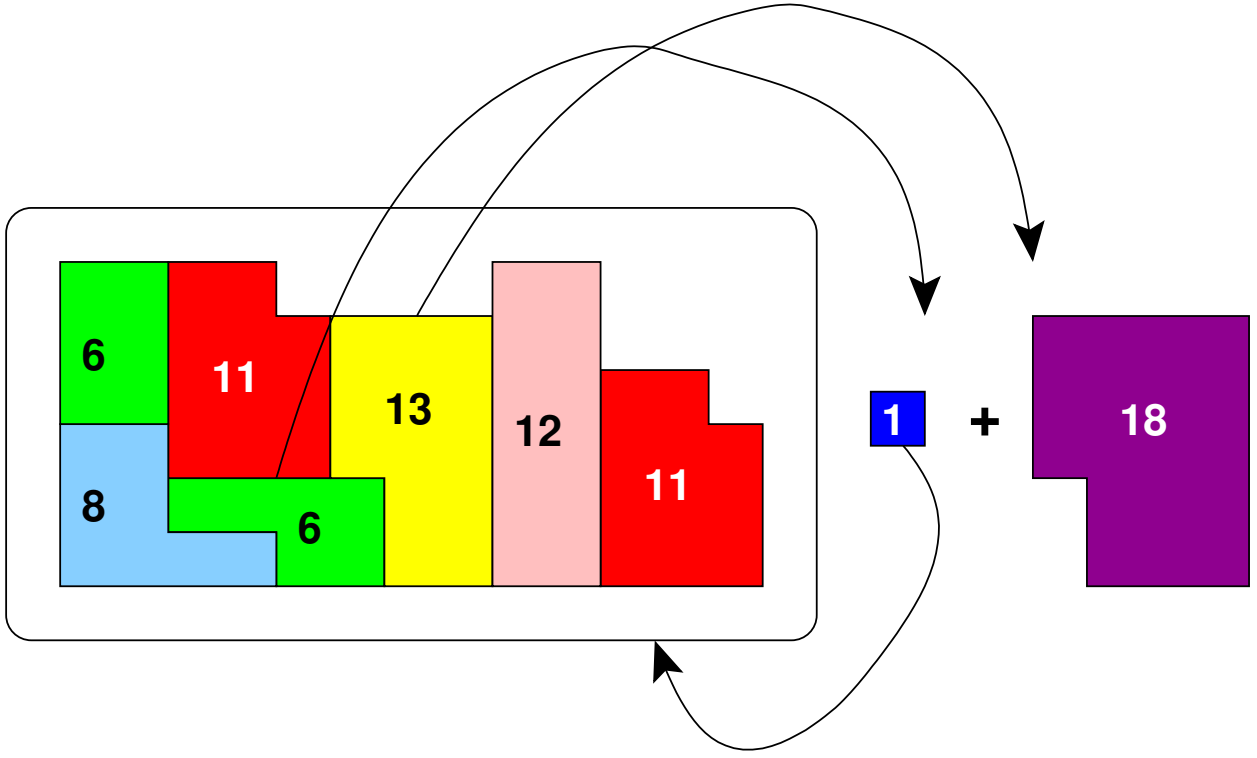
Bitcoin : monnaie électronique

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

Payer 18 BTC avec des pièces



Plan

Pré-requis

Plan

Pré-requis

Au coeur de Bitcoin

Plan

Plan

Plan

Clef symétrique

Exemples

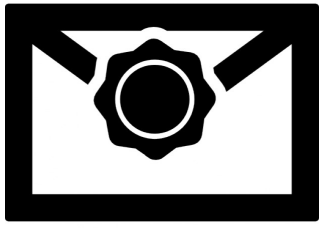
- DES
- AES

Chiffrement à clef publique

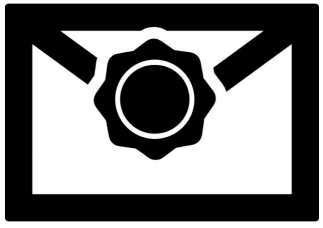
Exemples

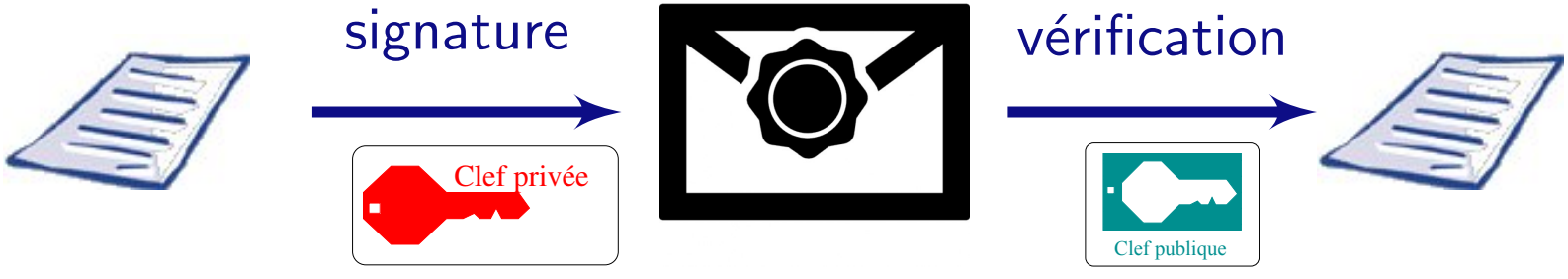
- RSA : $c = m^e \mod n$
- ElGamal : $c \equiv (g^r, h^r \cdot m)$

Signature



Signature



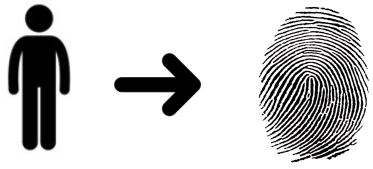


clef secréte

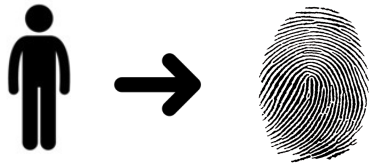
clef publique

RSA: $m^d \mod n$

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

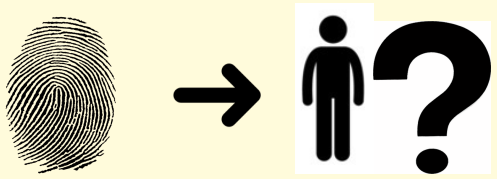


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)

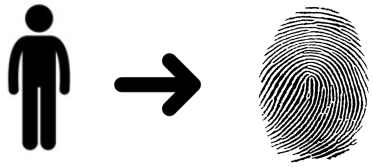


Propriétés de résitance

- Pré-image

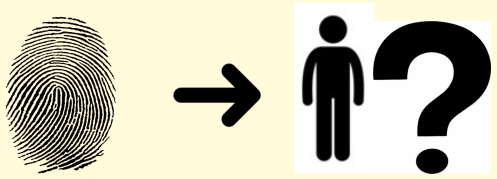


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)

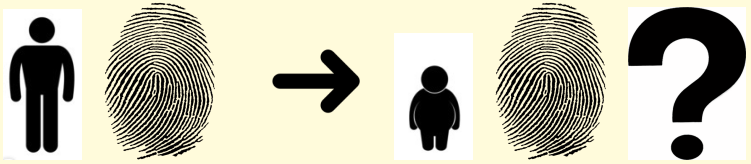


Propriétés de résitance

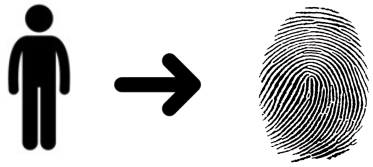
- Pré-image



- Seconde Pré-image

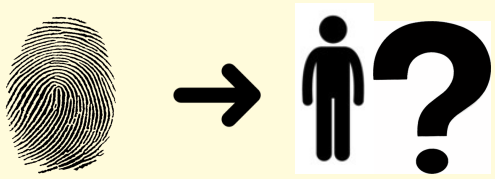


Fonction de Hachage (RIPEMD-160, SHA-256, SHA-3)

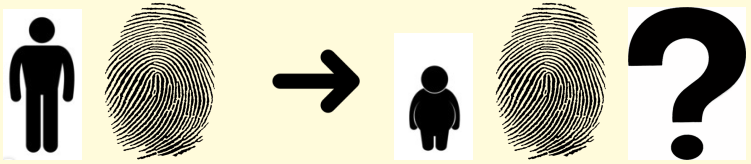


Propriétés de résitance

- Pré-image



- Seconde Pré-image



- Collision

Propriétés d'une monnaie électronique

- Non-Falsifiable (Unforgeable)

- Eviter la double dépense & identifiation fraudeur & "présemption d'innocence"

- Respect de la vie privée :
  - Anonymat faible : non identification d'un acheteur
  - Anonymat fort : non traçabilité d'un acheteur

Plan

Bitcoins : caractéristiques

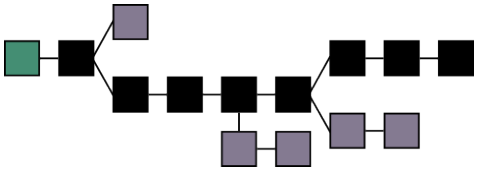
- Le nombre total de bitcoins est **fini**

  21 millions BTC

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

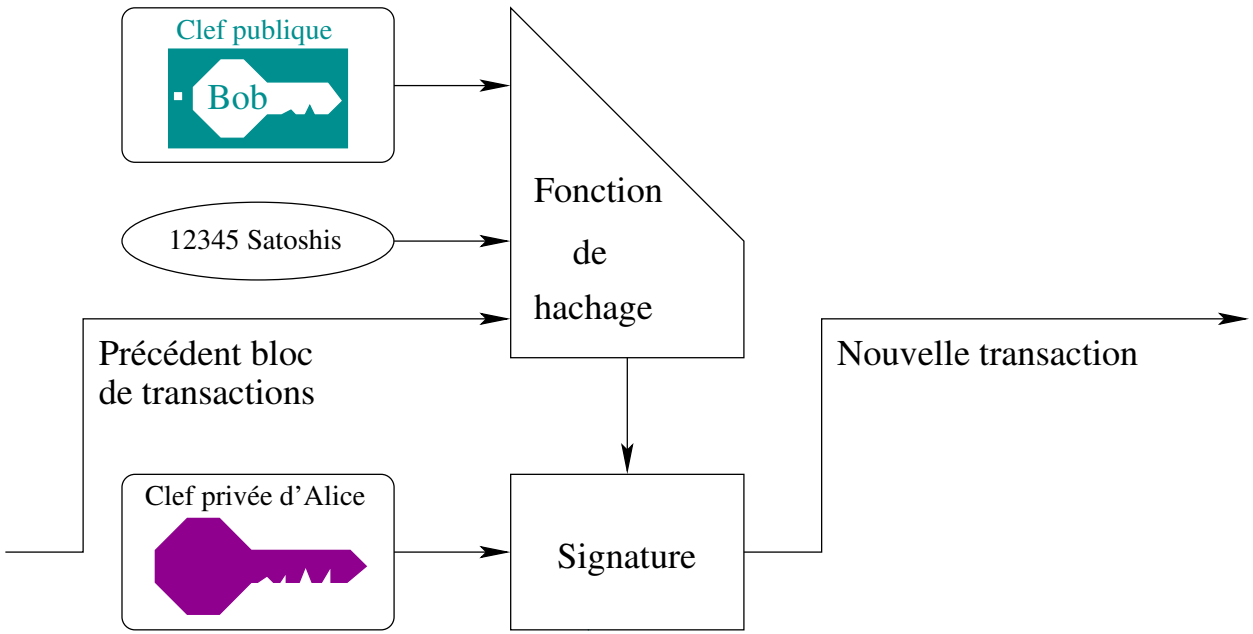
  $$\text{RIPEMD-160}(\text{SHA-256}(\text{ECDSA}_{pub}))$$

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

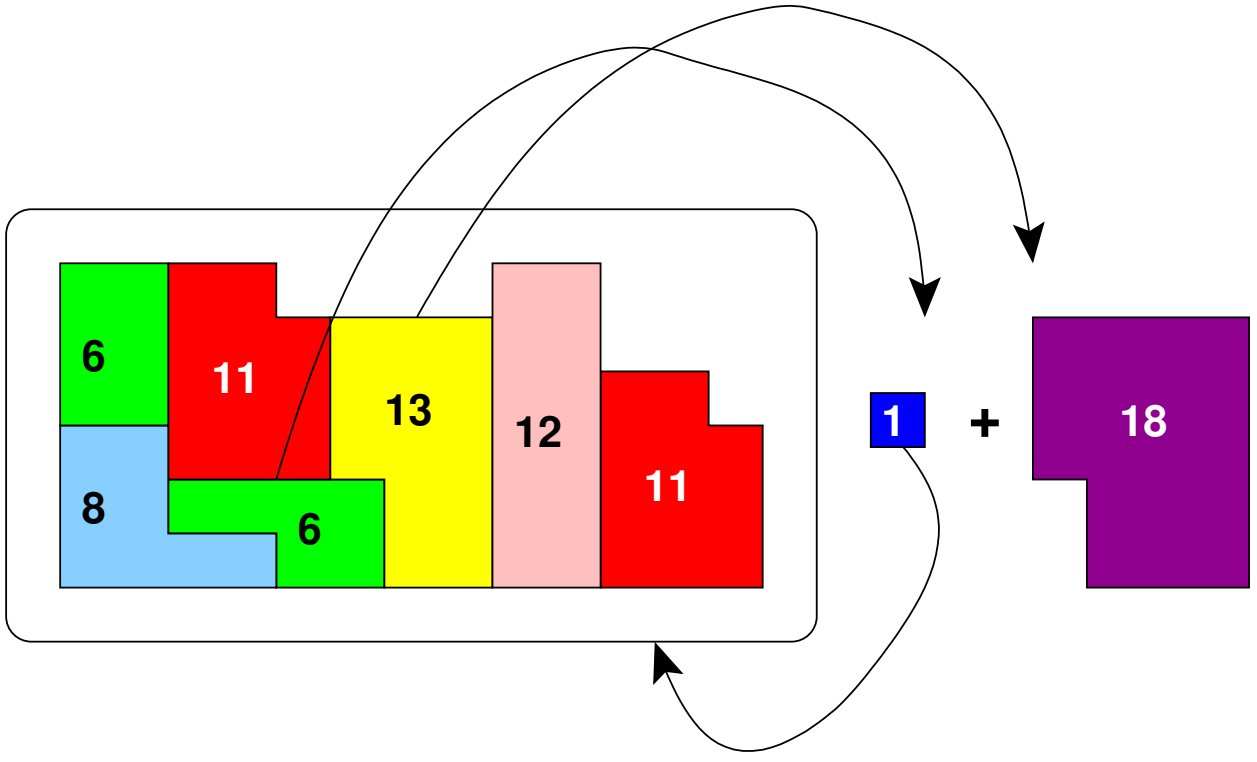


Comment faire une transaction?

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



Payer 18 BTC avec des pièces

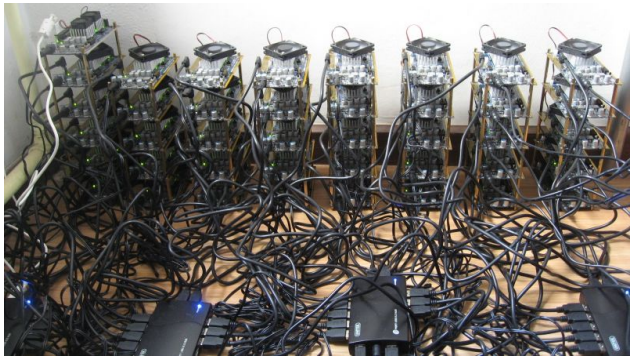


- Seuls des bitcoins possédés peuvent être dépensés

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 un 0 plus de au début de x

Miner : Objectif de hachage

Cible = 0000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076

Trouver une nombre n tel que

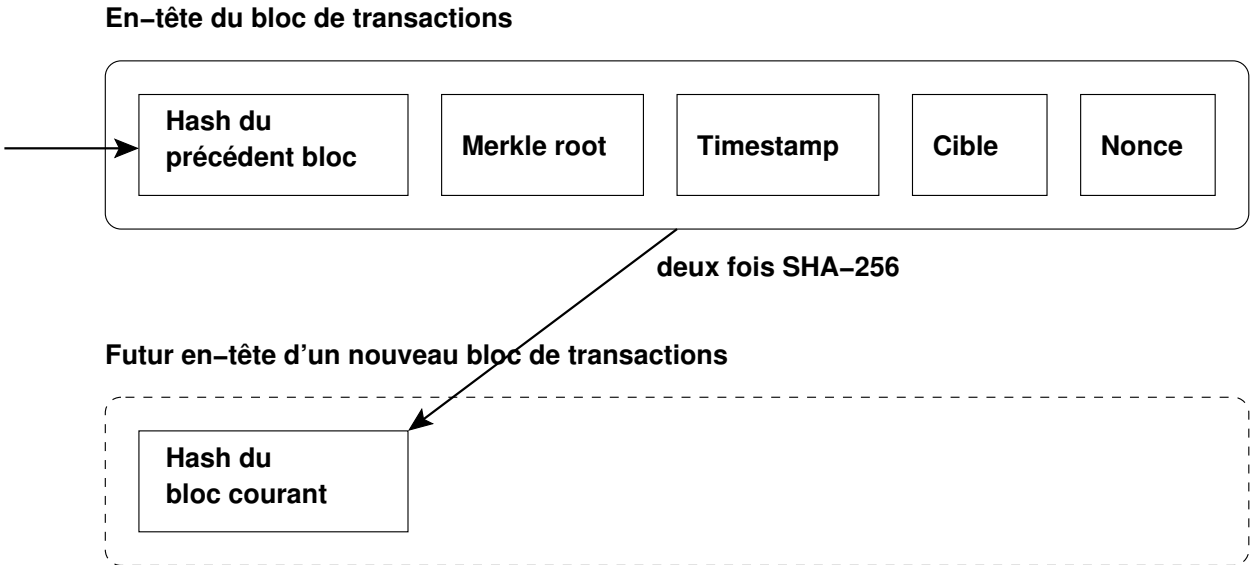
$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, n)) = x < \textit{Cible}$$

Avoir un 0 plus de au début de x

Stratégie : brute force

Tester toutes les valeurs possibles de n

Miner : Proof of work



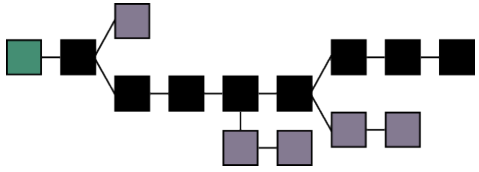
Avoir un zéro de plus au début

SHA-256(SHA-256(en-tête de bloc))

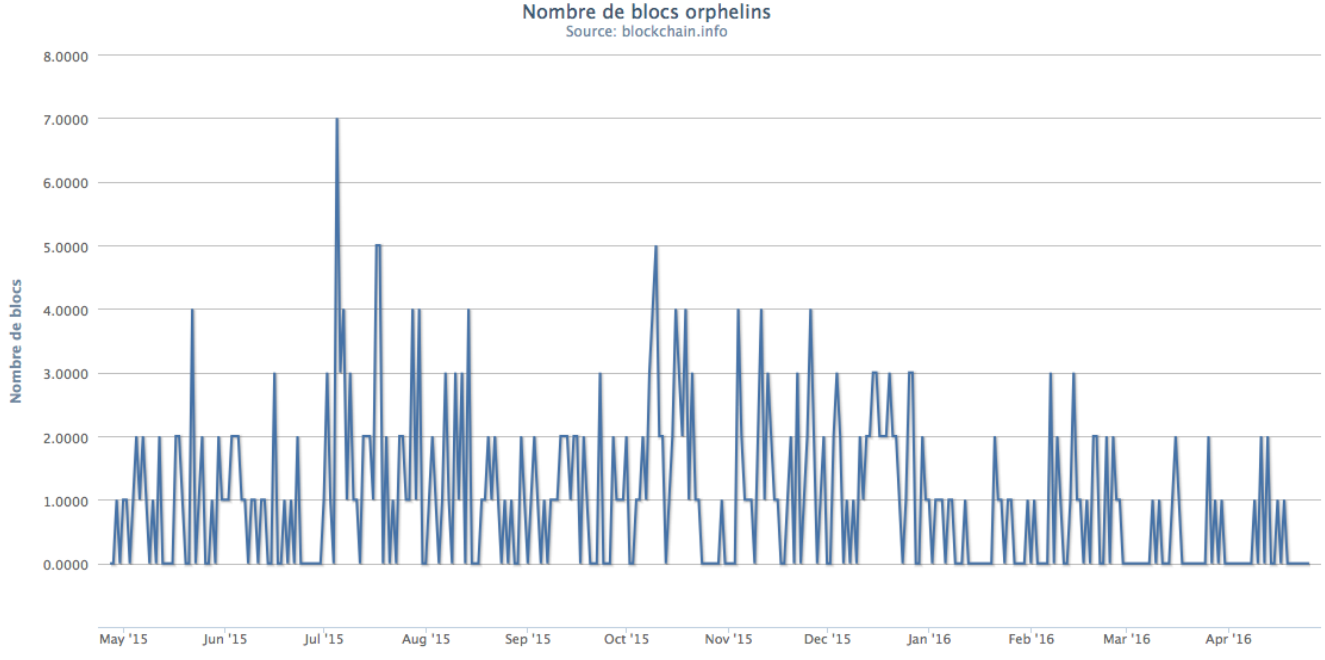
- les transactions passées (95 Go)
- les transactions à valider
- les secondes depuis 01/01/1970
- un nonce
- etc ...

Miner = Validation des transactions

Cible: 00000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076



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



Plan

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

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 = difficle + energivore



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



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 ?