Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Bitcoin et cryptomonaies

Emmanuel Benoist

Séminaire Mathématiques et Société
29 mars 2019 - Uni Neuchâtel

Computer Science Division

Bitcoin et cryptomonaies

- Un peu d'Histoire
- Vocabulaire
- Le Bitcoin
- La Blockchain
- Le Minage de Bitcoins
- Monero
- Vue d'ensemble

Un peu d'histoire

Les monnaies dans l'histoire

- **Monnaie: quelquechose que l'on peut échanger pour payer et être payé**
  - Doit avoir une valeur pour les deux parties
  - Doit être thésaurisable (vous vendez un boeuf maintenant et rachetez une vache dans deux mois)
- **Exemples de monnaies dans l'histoire**
  - Sel pour payer les légionnaires romains (d'où salaire),
  - les fèves de cacao dans l'empire Aztec,
  - certains coquillages ont même servi de monnaie.

Monnaies métalliques

- **Les métaux sont recherchés par nos sociétés humaines**
  - Le Bronze : pour faire des armes
  - L'Argent : est rare et a une belle reflexion métallique
  - L'Or: a de nombreuses propriétés exceptionnels
    Ne peut pas être oxydé, ductile, très bonne conductivité, beau
- **Ces métaux ont les propriétés recherchées pour les monnaies**
  - Peuvent être accumulées et stockées sur un long terme,
  - beaucoup de valeur pour un très petit volume (surtout l'or)
  - aura toujours une valeur dans le future (confiance) - la capacité de *"créer"* de la monnaie est très limitée.
- **La valeur de la monnaie métallique varie fortement avec le temps**
  - Découverte des mines d'argent dans l'Amérique espagnole du 16ème siècle,
  - Découverte de l'or californien change la valeur de l'or dans la seconde moitié du 19ème siècle.
- **La valeur intrinsèque du métal reste la même**

Un peu plus d'histoire

- **Les monnaies modernes étaient liées à l'or et/ou l'argent**
  - Au 19ème Siècle, le Sterling était convertible en or (Gold Standard)
  - Les pièces de 20 francs (Suisse, France, Italie, Belgique, . . . : l'Union latine) étaient en or.
    Les pièces de 1 et 5 francs étaient en argent.
  - Le dolar US est resté convertible à l'or jusqu'en 1971.
- **Actuellement: Monnaie = Confiance**
  - Le Dollar n'est plus convertible en or à taux fixe.
  - Aucune valeur tangible n'est liée à une monnaie
  - Valeur d'une monnaie = Pure Confiance dans la banque centrale
- **Valeur de la monnaie?**
  - Capacité de la banque centrale à payer des intérêts (quoi que)
  - Confiance dans la banque centrale à limiter l'inflation
  - *Inflation* = la valeur du papier que l'on garde diminue
    On peut acheter moins avec le même papier

Problèmes avec les monnaies existantes

- **Controlées par les états**
  - Les libertariens n'ont pas confiance dans l'état
  - Les traficants de drogue non plus.
- **Les état dictent les règles pour les banques centrales**
  - La Réserve fédérale ("Fed") aux USA
  - La Banque centrale européenne BCE in Europe
  - La Banque nationale suisse en Suisse
- **Les états et les banques peuvent suivre toutes les transactions électroniques**
  - Les transactions ont lieu de banque à banque
  - Clients peuvent être espionnés
  - Les banques collectent des frais
- **Si une banque fait faillite, l'argent est perdu**
  - Le client n'a pas de vrai contrôle sur son argent.

Une monnaie électronique

- **Internet est un nouveau territoire**
  - Pas relié à un pays (ou état)
  - Certaines transactions ne sont qu'électroniques (ebooks, films, licences de softwares, jeux, journaux . . .)
- **Cahier des charges pour une nouvelle monnaie**
  - Ne doit pas être contrôlée par un état
  - Doit avoir une valeur stable
  - Transactions gratuites (si possible pas de frais)
  - La monnaie ne doit pas être dépensée deux fois (trivial avec l'or, plus difficile avec des données).

Vocabulaire

Vocabulaire

- **Fonction de hashage**: fonction à sens unique
  - $z = h(x)$ est facile à calculer
  - $x = h^{-1}(z)$ est en pratique impossible à calculer
  - Exemples : MD5, SHA256,
- **Cryptographie asymétrique** Basée sur une paire de clés
  - *Clé privée* connue uniquement du propriétaire
  - *Clé publique* peut être connue de tous

  Avec la clé publique on peut encrypter, mais le décryptage se fait avec la clé privée
  Avec la clé privée on peut signer, on vérifie avec la clé publique
  Exemples: RSA, ElGamal, Courbes éliptiques.

Le Bitcoin

Le Bitcoin

- **Inventé en 2008 par "Satoshi Nakamoto"**
  - Monnaie virtuelle (Cryptocurrency) basée sur un logiciel open source
- **Bitcoin est entièrement transparent**
  - Le logiciel client est open source
  - Toutes les transactions sont publiées dans une *"Blockchain"* que tous les clients devraient downloader
  - Les validatations des transactions sont faites on-line par des volontaires qui calculent la *Blockchain*
  - Les volontaires reçoivent des nouveaux bitcoins (comme des pépites d'or). On les appelle les *"mineurs"*.

Une transaction

- **L'argent est stocké dans une "Adresse"**
  - Une *adresse* est un nombre (pas vraiment) aléatoire
  - De l'argent lui est affecté
- **Transaction**
  - Une *transaction* est lorsque de l'argent est transféré d'une adresse à une autre.
- **Toutes les transactions sont stockées dans une gigantesque "Blockchain"**
  - Contient toutes les transactions depuis la naissance des Bitcoins
  - On peut voir l'argent circuler d'une adresse à une autre
  - On peut savoir exactement combien d'argent contient chaque adresse.
  - Lorsqu'une transaction est ajoutée à la blockchain, l'argent est transféré d'une adresse à une autre.
  - Tout le monde voit toutes les transactions et les adresses.

Une Adresse (I)

- **Une adresse n'est pas un nombre aléatoire: c'est le hash d'une clé publique.**
  - L'utilisateur génère une paire de clés asymétriques (clés publique et privée)
  - La clé publique est gardée secrète.
    Comme l'argent peut rester longtemps sur une adresse donnée, il pourrait être possible de casser la clé publique si elle était connue.
  - Le hash de la clé publique est publié, c'est ce que nous appelons une *adresse*

Une Adresse (II)

- **Comment dépenser de l'argent**
  - L'utilisateur doit publier sa clé publique.
    Tout le monde peut vérifier que la clé publique correspond au hash connu (i.e. l'adresse).
  - L'utilisateur peut ensuite signer la transaction avec sa clé privée
  - Tout le monde peut (et doit) vérifier que la clé privée utilisée correspond bien à la clé publique publiée qui correspond aussi à l'adresse connue dans la blockchain.
  - La nouvelle transaction est ajoutée à la blockchain.

Une Adresse (III)

- **Usage**
  - L'utilisateur devrait dépenser tout l'argent d'une adresse en une seule fois (de manière que l'adresse ne soit plus utilisée)
  - Si l'utilisateur veut transférer moins d'argent que le total, il envoie le reste de l'argent vers une nouvelle adresse.
  - Si l'utilisateur a besoin de plus d'argent, il va regrouper plusieurs adresses
  - Pour grouper plusieurs adresses, l'utilisateur a besoin de TOUTES les clés privées.

Transactions

Alice veut acheter de l'herbe à Bob

mBTC	Adresse
50	anvjuerjHH
8.7	NNjuURZZ
300	UUIODG7

Alice

Bob

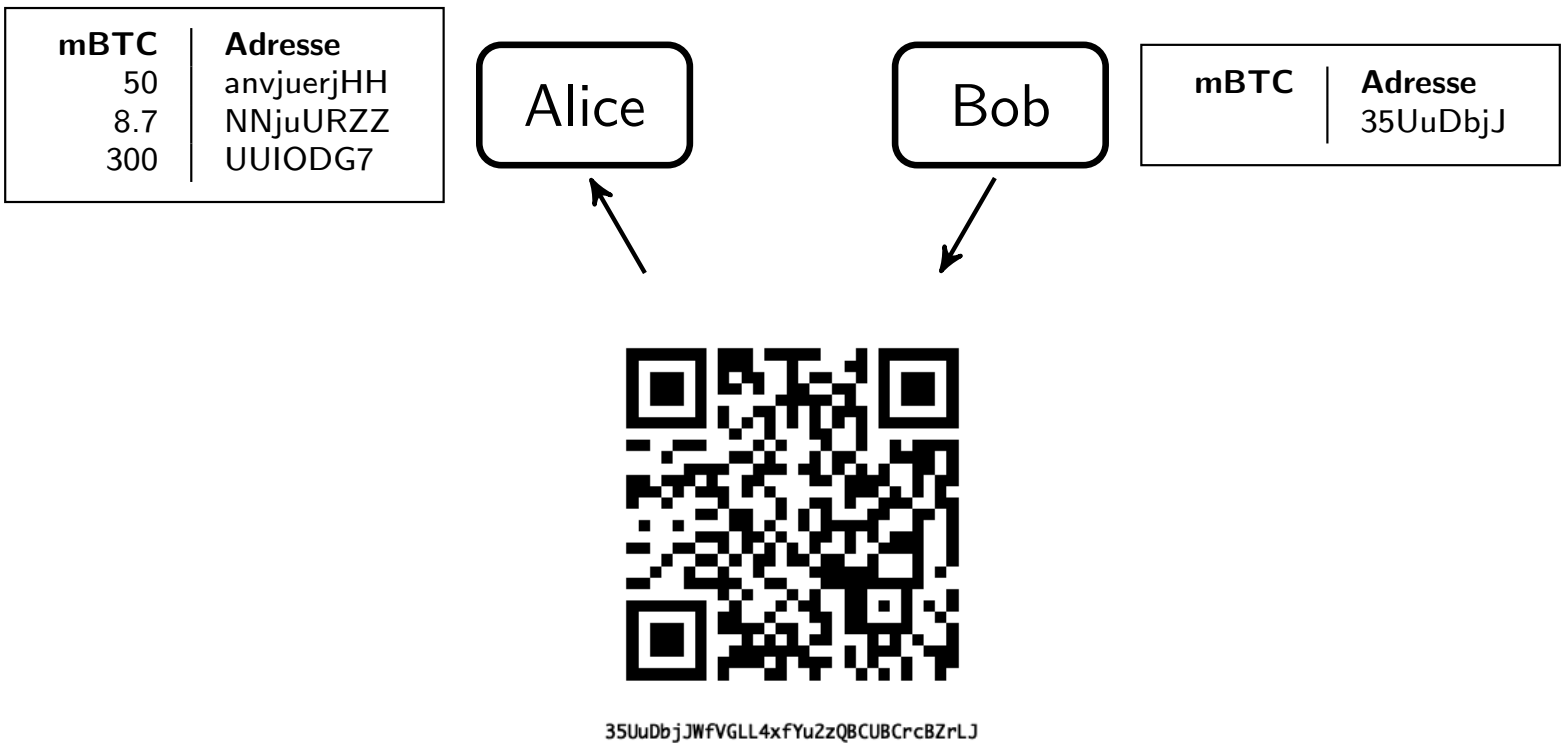
mBTC	Adresse

Transactions

Bob lui génère une adresse Bitcoin pour recevoir de l'argent

Transactions

Bob envoie un message à Alice *"Envoie BTC 0.3 à 35UuDbjJ"*



Transactions

Alice génère une nouvelle transaction depuis une de ses adresses

mBTC	Adresse
50	anvjuerjHH
8.7	NNjuURZZ
300	UUIODG7

Alice

Bob

mBTC	Adresse
	35UuDbjJ

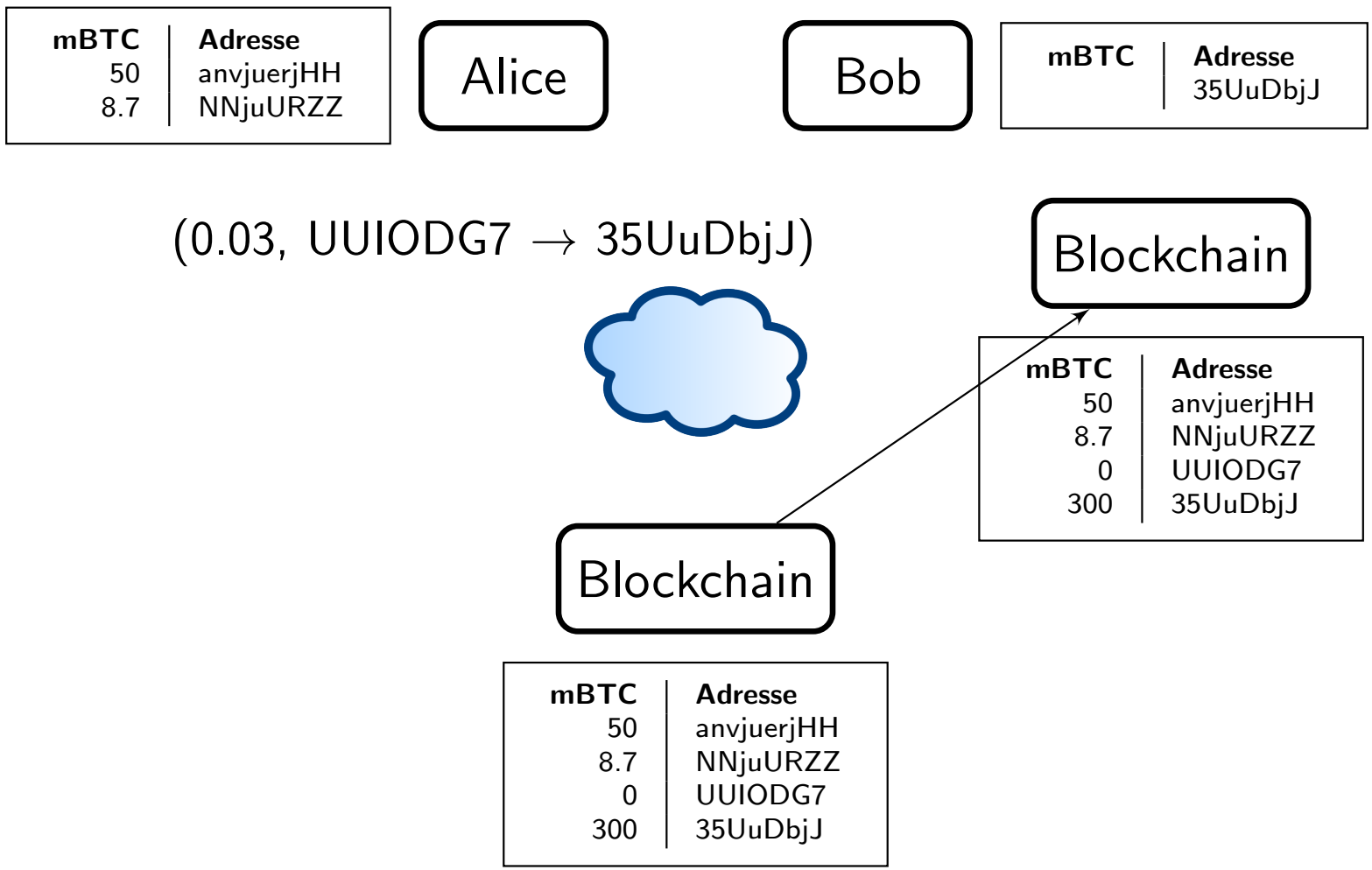
(0.03, UUIODG7 → 35UuDbjJ)

Blockchain

mBTC	Adresse
50	anvjuerjHH
8.7	NNjuURZZ
0	UUIODG7
300	35UuDbjJ

Transactions

Bob met à jour sa copie de la Blockchain



Transactions

Bob vérifie qu'une transaction arrive à 35UuDbjJ

mBTC	Adresse
50	anvjuerjHH
8.7	NNjuURZZ

Alice

Bob

mBTC	Adresse
300	35UuDbjJ

Blockchain

mBTC	Adresse
50	anvjuerjHH
8.7	NNjuURZZ
0	UUIODG7
300	35UuDbjJ

Blockchain

mBTC	Adresse
50	anvjuerjHH
8.7	NNjuURZZ
0	UUIODG7
300	35UuDbjJ

Transactions

Bob envoie l'herbe

mBTC	Adresse
50	anvjuerjHH
8.7	NNjuURZZ

Alice ← Bob

mBTC	Adresse
300	35UuDbjJ

Blockchain

mBTC	Adresse
50	anvjuerjHH
8.7	NNjuURZZ
0	UUIODG7
300	35UuDbjJ

Blockchain

mBTC	Adresse
50	anvjuerjHH
8.7	NNjuURZZ
0	UUIODG7
300	35UuDbjJ

La Blockchain

Partage des Transactions

- **Toutes les transactions doivent être publiques**
  - Il n'y a pas de banque pour valider une transaction
  - C'est la tâche de la communauté
- **Chaque transaction doit être envoyée au réseau peer2peer.**
  - Le protocole transfert la transaction à tout le réseau
  - Chaque noeud doit connaitre toutes les transactions
- **Problèmes**
  - Un noeud n'est pas on-line 100% du temps
  - Un noeud peut ratter des transactions
- **Besoin d'une liste des transactions**
  - Ne peut pas être simplement une immense liste monolithique
  - Doit contenir des blocs, c'est une chaine de blocs la *blockchain*
  - Doit être validée et unique

Blockchain

- **La blockchain contient toutes les transactions depuis la création du bitcoin**
  - Sa taille est de 200GB
- **Chacun peut en avoir une copie (et devrait)**
  - Le client Satoshi (logiciel standard: Bitcoin Core) télécharge la chaine entière.
  - Il peut vérifier chaque adresse et donc pour chaque transaction indiquer si elle est valide.
  - Il peut voir si une transaction est incluse dans la blockchain

Le Minage de Bitcoins

Validation des transactions

- **Les blocs doivent être validés par quelqu'un**
  - Quelles transactions sont acceptées et lesquelles sont rejetées?
  - Impossible d'avoir une unique autorité centrale (banque centrale ou clearing agency).
- **Un partenaire du réseau va valider UN bloc**
  - Il choisit l'ensemble des transactions valides
  - Très grande responsabilité
  - Ce rôle doit être donné à un des membres du réseau au hasard: Comment produire un hasard distribué?
- **La preuve de travail "proof of work"**
  - Le validateur doit générer un "nonce" (un nombre quelconque) et l'ajouter à l'ensemble des transactions, ensuite il calcule un hash du tout.
    $hash(Transaction1 + Transaction2 + Transaction3 + ... + nonce)$
  - Le nonce est valide si le hash démarre avec X zéros en notation binaire (X doit varier pour empêcher de générer plus d'un bloc toutes les 10 minutes).

Le mining de Bitcoins

- **Un Mineur Alice choisit certaines transactions**
  - Initialement: toutes les transactions
  - Actuellement: Uniquement les transactions donnant un bonus au mineur sont sélectionnées
- **Alice ajoute une transaction vers elle-même**
  - Alice crée une nouvelle adresse vers laquelle de nouveaux bitcoins sont transférés
  - C'est la pépite du mineur
- **Le mineur doit ensuite générer une preuve de travail "proof of work"**
  - L'idée est d'avoir ainsi une méthode aléatoire de choix des responsables de la validation des blocs.
  - Sur le long terme, les pépites doivent compenser les coûts du minage.

Preuve de travail I

- **Idée comment choisir aléatoirement un partenaire?**
  - Chacun fait des calculs aléatoires et le premier à trouver un résultat satisfaisant a gagné.
- **Problème: obtenir un résultat débutant avec un nombre donné de zéros**
  - Une fonction de hashage est vue comme un générateur aléatoire
  - Pour générer des valeurs différentes, il suffit de changer la valeur à hasher: Ajouter un nonce
    Hasher une valeur avec un nonce = acheter un billet de loterie
  - Chaque hash calculé = nouvelle chance de gagner

Preuve de travail II

- **Exemple**

hash(Transaction1+Transaction2+Transaction3+"AAAAAAAAA")=AE4529EB90
hash(Transaction1+Transaction2+Transaction3+"AAAAAAAAB")=90A63BB89C
...
hash(Transaction1+Transaction2+Transaction3+"AAAAABERFP")=00301230FF
A 10 zéros au début (en forme binaire): valeur OK!!!

Deux blocs sont trouvés en parallèle

- **2 mineurs trouvent un bloc simultanément**
  - Les deux blocs entrent en compétition
  - A long terme, la blockchain la plus longue est conservée
  - Seul le premier à avoir un successeur sera conservé
- **Exemple de compétition entre blocs**
  - On a la blockchain *Chain*
  - Team A et Team B trouvent le blocs : $Block_A$ and $Block_B$
  - On a 2 blockchains:
    $Chain + Block_A$ and $Chain + Block_B$
  - Certain noeuds reçoivent l'une, d'autre l'autre.
  - Un mineur trouve un nouveau block: $Block_C$ basé sur $Chain + Block_B$
  - On a 2 blockchains:
    $Chain + Block_A$ and $Chain + Block_B + Block_C$
    La chaine la plus longue gagne.

Protection de la sphère privée

- **Les transactions sont toutes publiques**
  - La blockchain peut être downloadée par tout le monde
  - On peut utiliser des sites pour voir les transactions (`https://blockchain.info/`)
  - On voit pour une adresse les transactions entantes et sortantes
- **Besoin d'anonymat**
  - Des services sont spécialisés dans le *tumblering* (pour cacher les transactions)
  - Exemple: `https://bitlaunder.com`
  - On envoie de l'argent à une adresse, l'argent est renvoyé à une nouvelle adresse (depuis une adresse différente).
  - Les deux adresses ne sont plus liées.

Algorithmes utilisés

- **Hashage**
  - SHA256
- **Clés publiques et privées**
  - RSA
  - Multiplication de deux grands entiers vs. factorisation d'un très grand entier (modulo m).

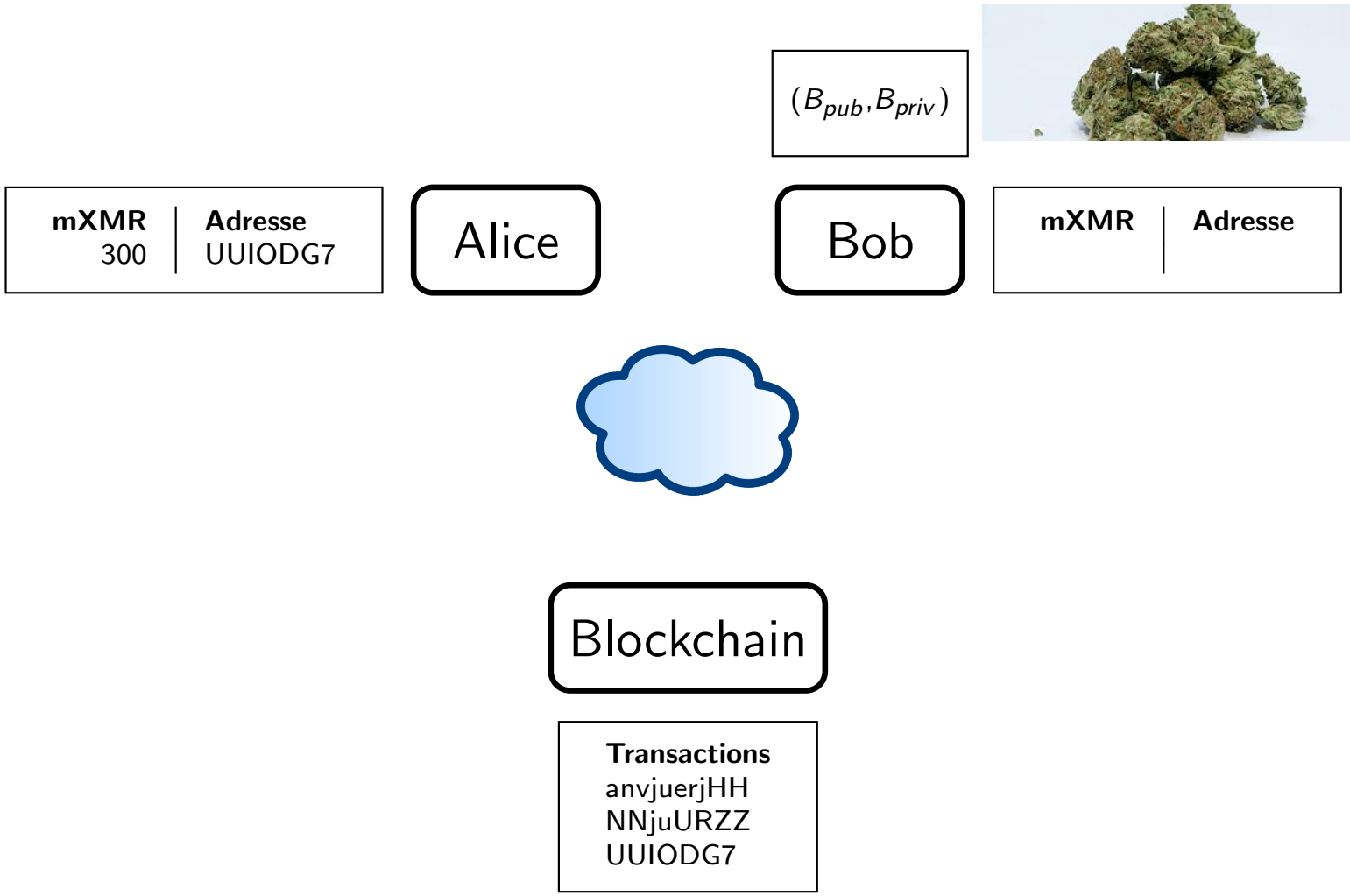
Monero

Monero

- **Une cryptomonaie faite pour protéger la sphère privée**
  - Les utilisateurs veulent garder l'anonymat sur leurs transactions,
  - Pour des actions illégales (Ransomware, Darkmarkets),
  - Pour protéger leur vie privée.
- **La blockchain reste publique**
  - Chacun peut la lire, la copier, vérifier les transactions
- **Les tranactions sont anonymes**
  - Impossible de savoir d'où vient une transaction
  - Impossible de savoir le montant d'une transaction
- **Solution**
  - Signature d'anneau (*"Ring signature"*)

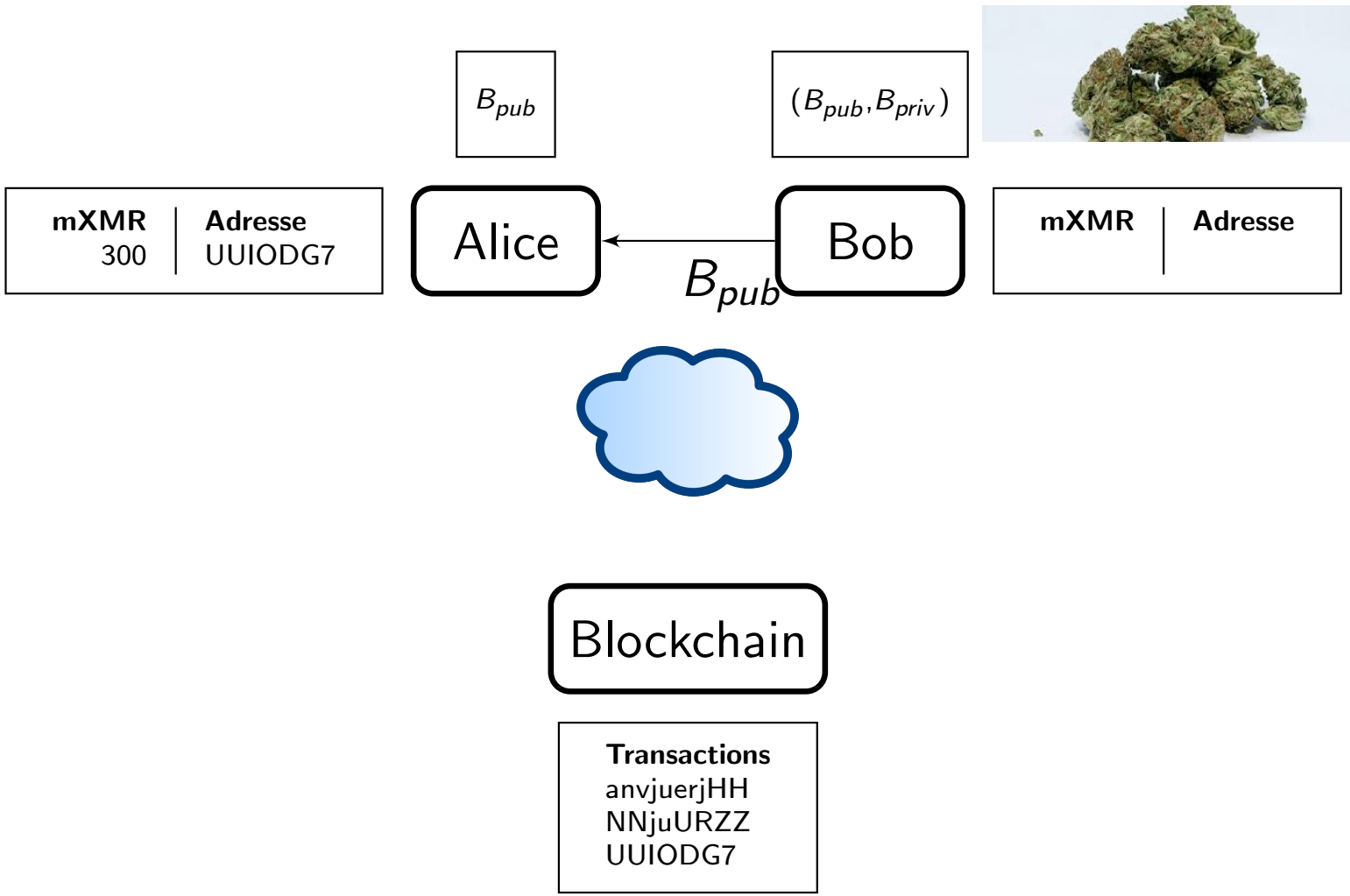
Transactions pour Monero

Alice veut acheter de l'herbe à Bob



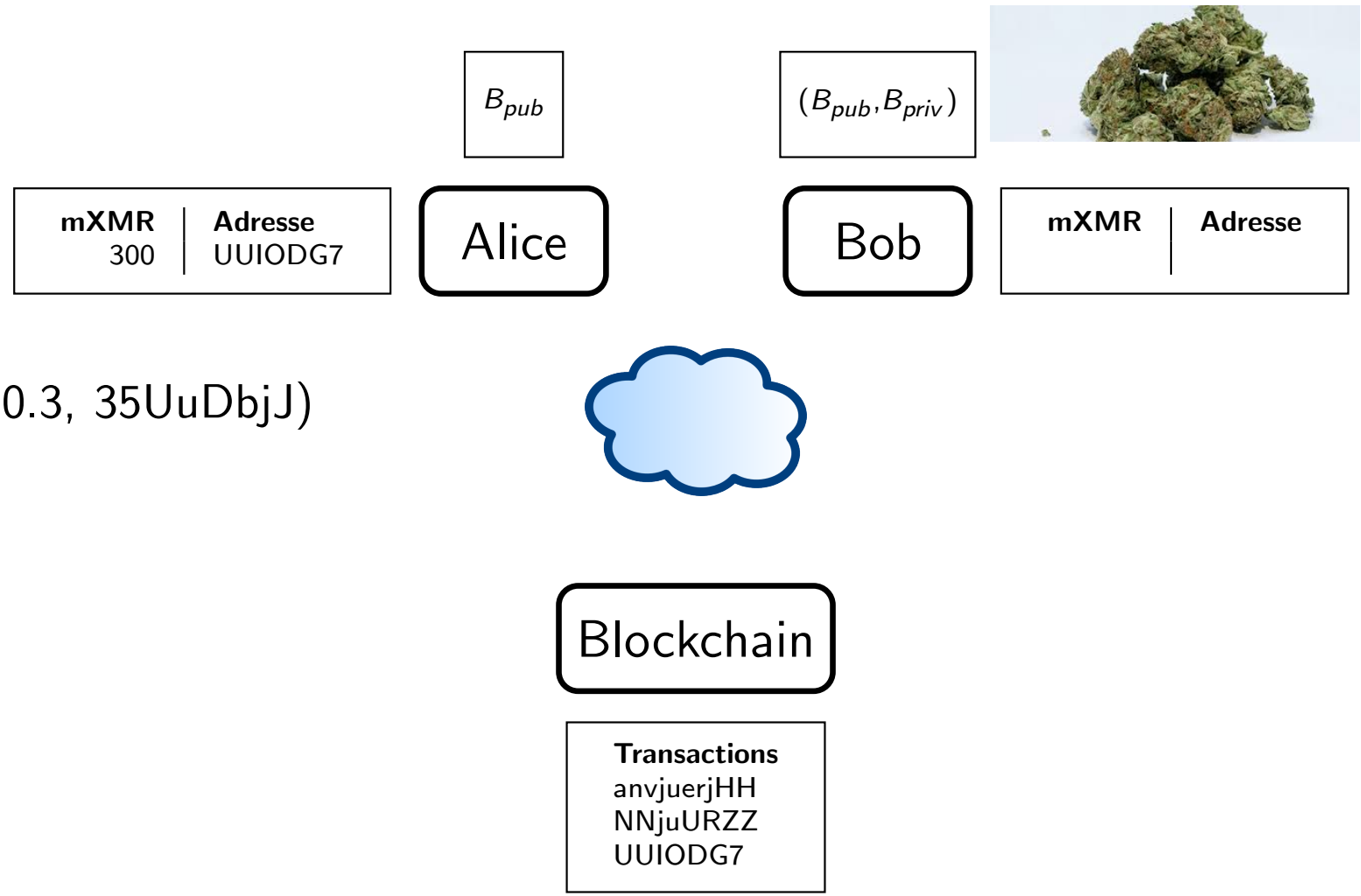
Transactions pour Monero

Bob envoie sa clé publique B_{pub} à Alice



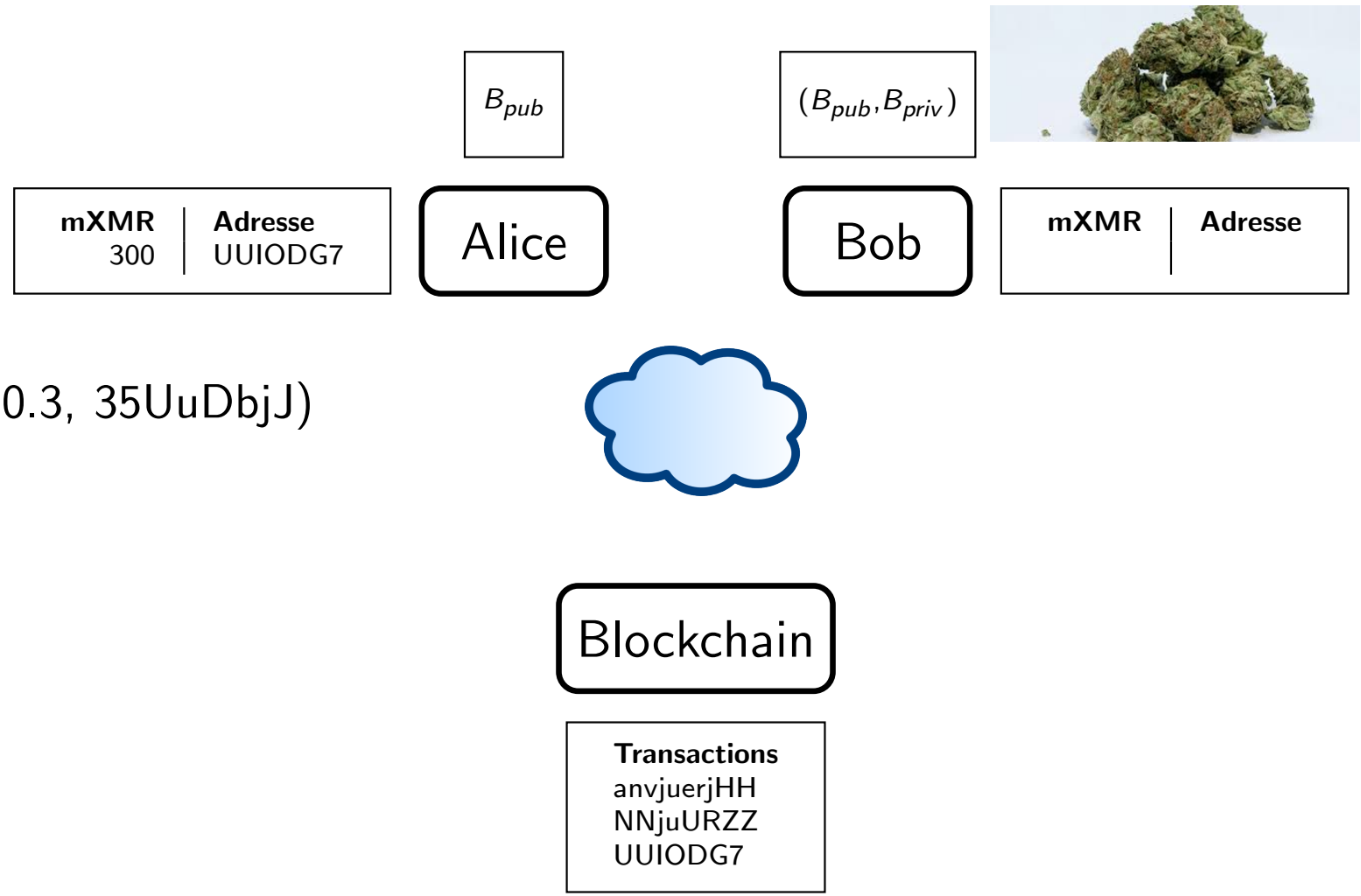
Transactions pour Monero

Alice génère une transaction à destination de B_{pub}.



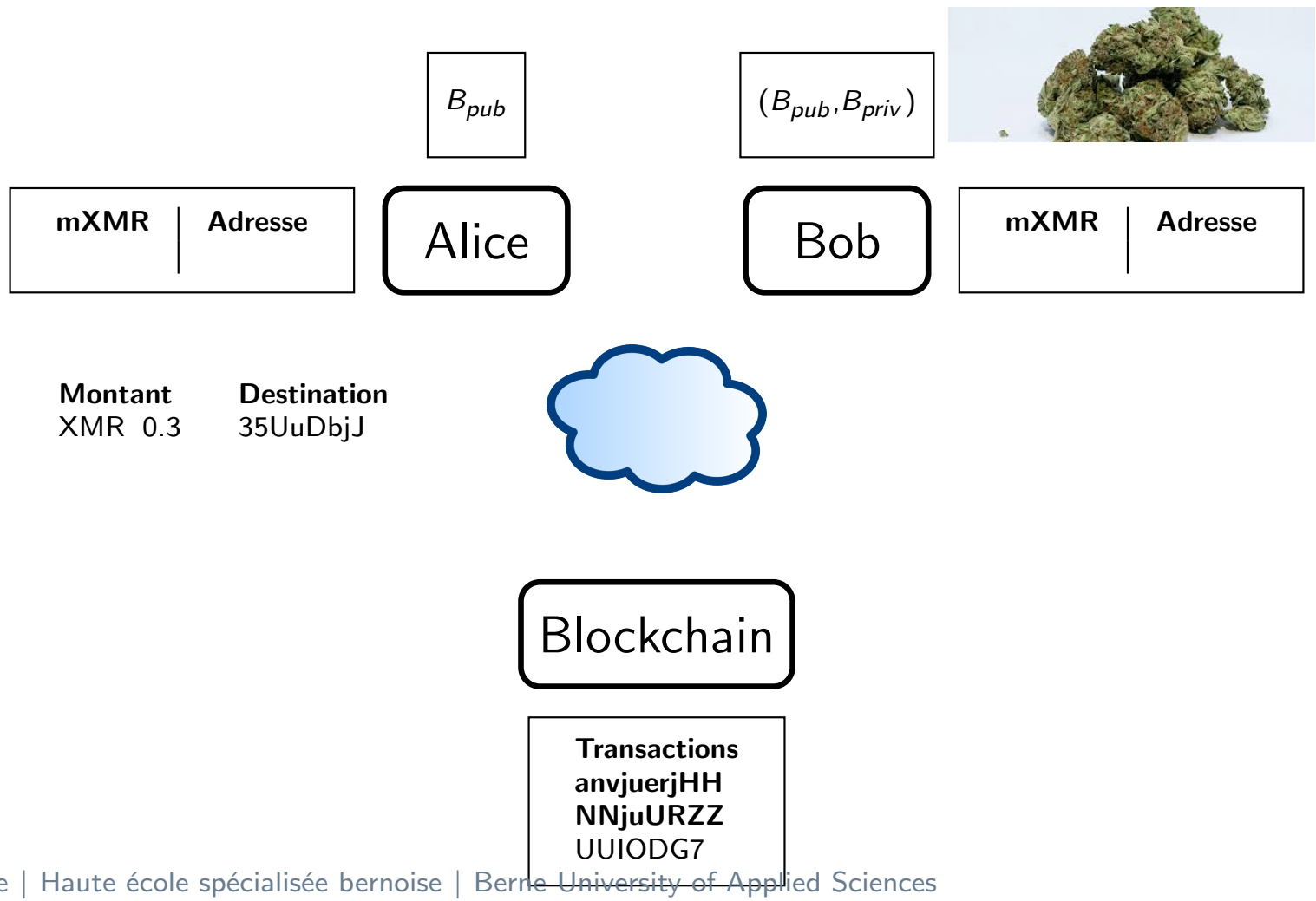
Transactions pour Monero

Alice choisit dans ses transactions, celle dont elle prend l'argent



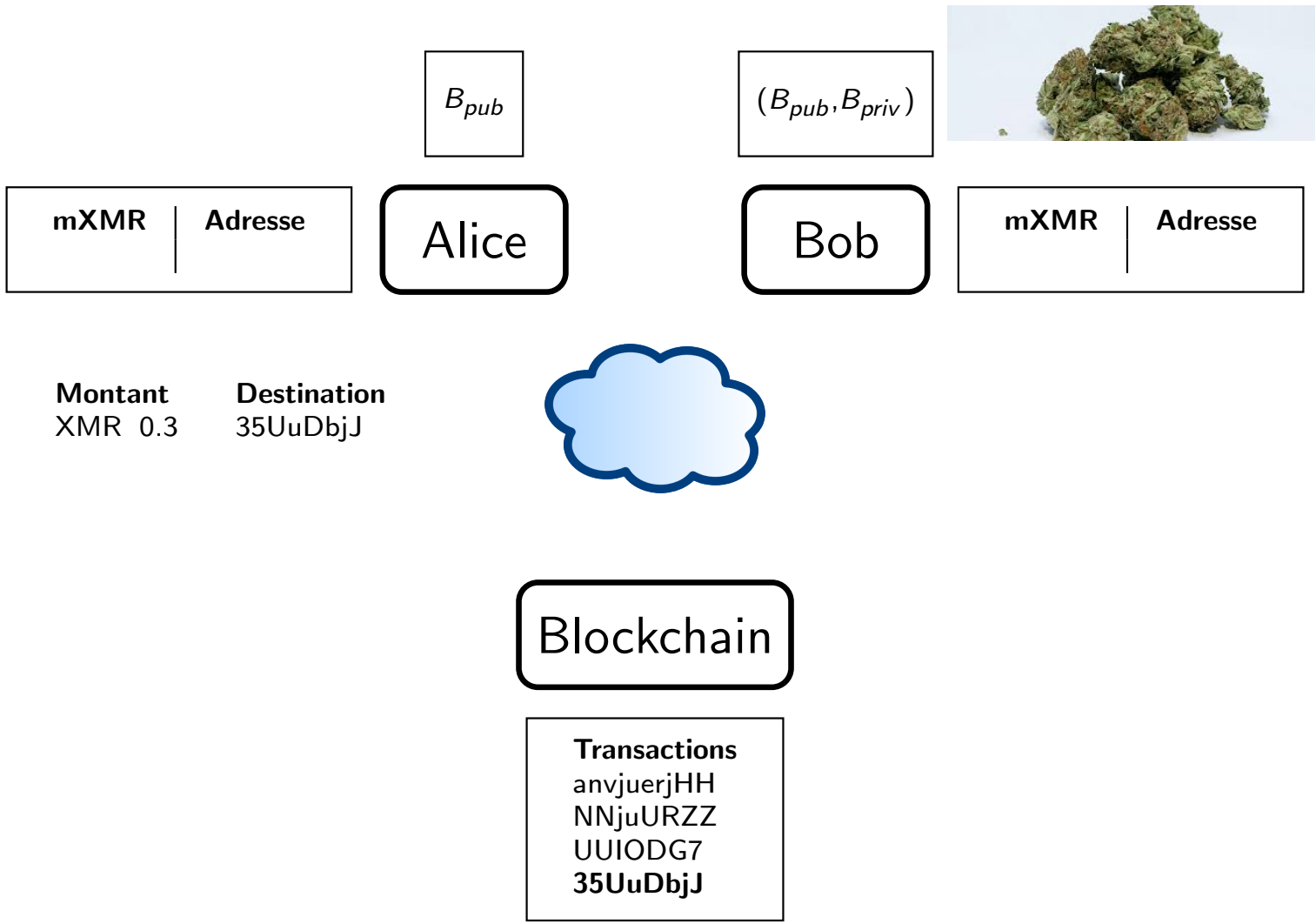
Transactions pour Monero

La transaction choisie est cachée dans un ensemble de 11 transactions (aléatoires).



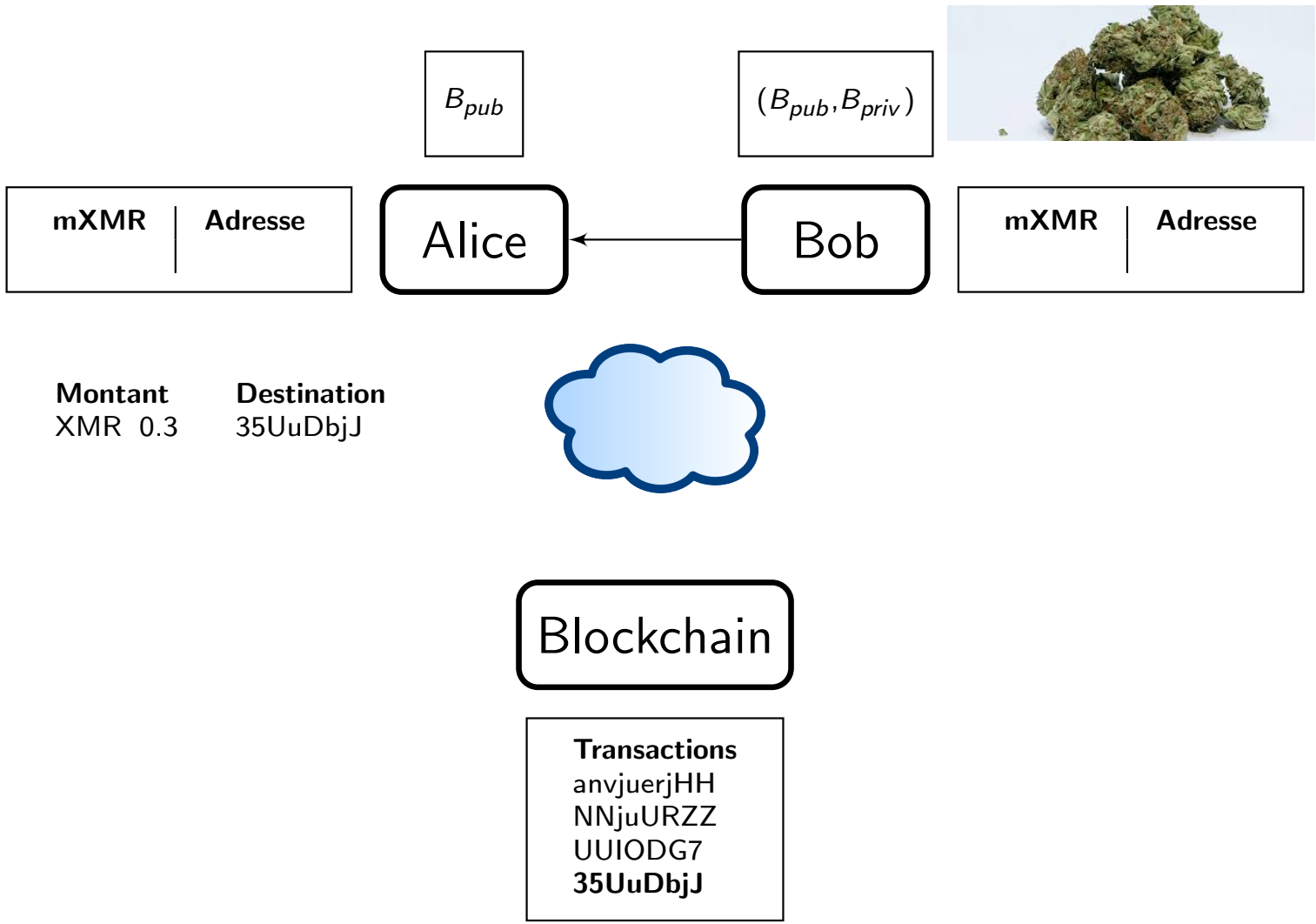
Transactions pour Monero

Alice signe l'anneau des 11 transactions



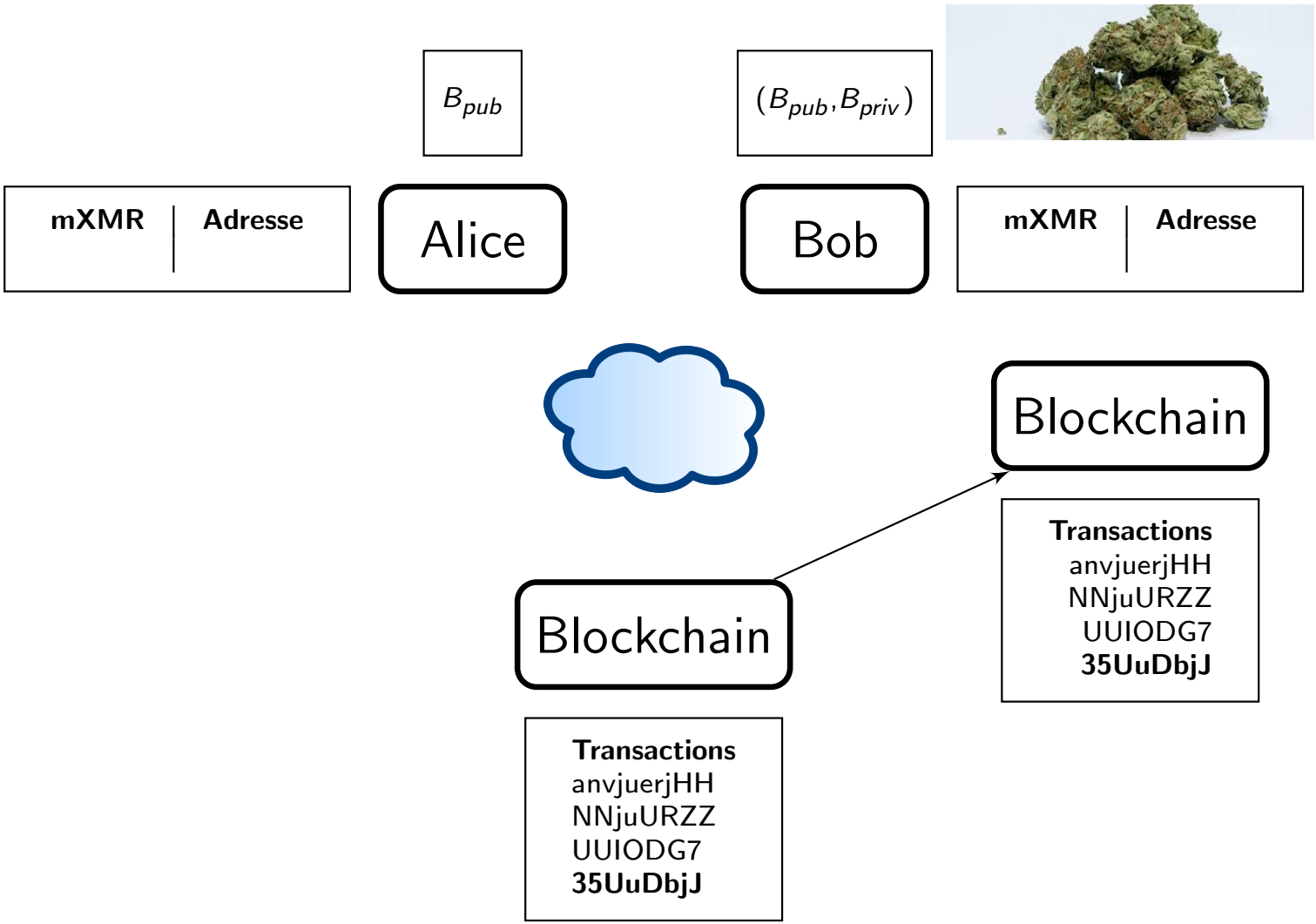
Transactions pour Monero

Alice envoie la nouvelle transaction sur la blockchain



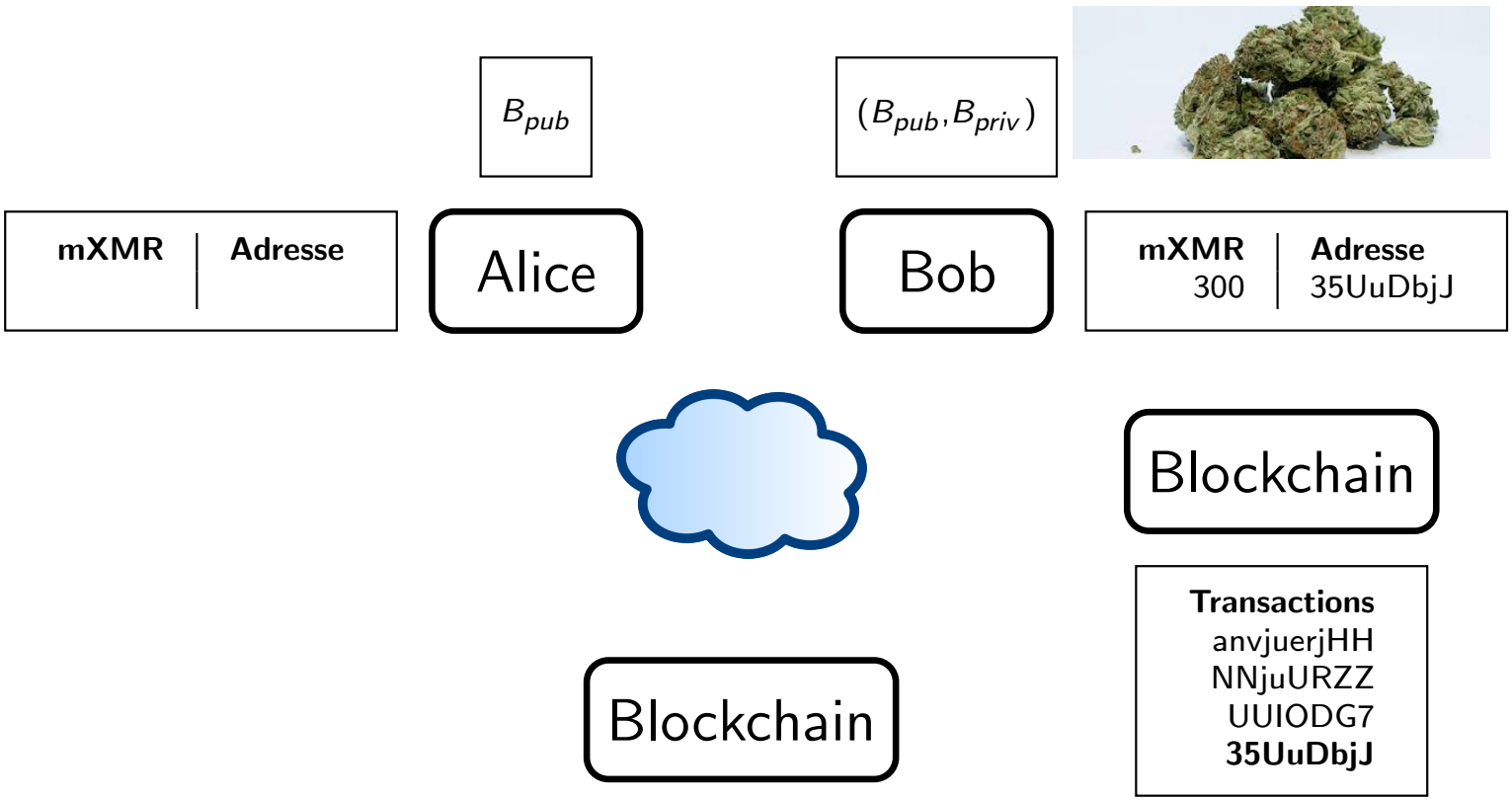
Transactions pour Monero

Bob met à jour sa copie de la Blockchain



Transactions pour Monero

Bob vérifie qu'une transaction arrive bien à destination de B_{priv}, et son montant. (Il est le seul à pouvoir le faire)



Transactions pour Monero

Bob envoie l'herbe

mXMR	Adresse

Alice

Bob

mXMR	Adresse
300	35UuDbjJ

Blockchain

Transactions
anvjuerjHH
NNjuURZZ
UUIODG7
35UuDbjJ

Blockchain

Transactions
anvjuerjHH
NNjuURZZ
UUIODG7
35UuDbjJ

Algorithmes utilisés par Monero

- **Hashage**
  - Pour la proof of work : CryptoNight (utilisant CryptoNote)
  - Difficile pour les “application-specific integrated circuits” (ASIC)
- **Signature de cercle**
  - Schema de signature MLSAG (Liu, Wei et Wong)
- **Cryptographie asymétrique (clés publiques et privées)**
  - Courbes éliptiques (multiplication par un scalaire est triviale, division difficile).

Vue d'ensemble

Cryptomonnaies [1]

- **Bitcoin BTC (71 milliards de USD)**
  - Première et plus grosse monnaie, très utilisée sur le Darknet,
  - Fonction de Hashage: SHA256
- **Ethereum ETH (14 milliards de USD)**
  - Permet les "smart contracts" avec un langage Turing complet, qui s'executent dans des machines virtuelles.
- **XRP (12 milliards de USD)**
  - Fonction de hashage: scrypt (requière beaucoup plus de mémoire).
- **Bitcoin Cash BCH (3 milliards de USD)**
  - Hard Fork de Bitcoin, juillet 2017
  - Taille des blocs passe de 1MB à 8MB
- **...**
- **Monero (900 millions de USD)**
  - Très orienté protection de la sphère privée
  - Ni les montants, ni les destinataires ne sont connus.

[1] `https://coinmarketcap.com/all/views/all/`

Conclusion

- **Les monnaies actuelles sont toutes basées sur la confiance (fin de l'étalon or en 1971)**
  - Pourquoi avoir plus confiance dans un état (ou une banque centrale indépendante) que dans un algorithme ?
- **Actuellement beaucoup de cryptomonnaies**
  - Différents algorithmes de cryptages (proof of work, cryptographie à clé publique, ring signature, . . .)
  - De nombreuses vont échouer
- **Différents écarts entre les blocs**
  - 10 minutes pour BTC : $\frac{1}{2}$h pour valider une transaction
  - 14 à 15 secondes pour ETH : possible pour acheter son pain.
- **Irremplaçables dans le Darkweb**
  - Bitcoin, Bitcoincash
  - Monero
  - Dash

Questions?

- Contact: emmanuel.benoist@bfh.ch
- Web : https://www.benoist.ch