RS40 : Contrôle continu sur la Blockchain

L'objectif de ce contrôle est de vous initier aux technologies cryptographiques utilisées dans la blockchain. La structure d'un bloc de la blockchain étudiée[1] est constituée des éléments suivants (voir la Figure 1) :

1. L'empreinte numérique du block précédent[2] : Utilisation de l'algorithme de hachage sha256
2. La donnée du bloc : La transaction. Par exemple, « Bernard verse 30€ à Yves ».
3. La signature de la transaction : La personne qui réalise la transaction, Bernard, signe la transaction en utilisant ECDSA (Elliptic Curve Digital Signature Algorithm).
4. Preuve de travail : Une phrase ajoutée par un mineur pour permettre d'obtenir un résultat d'empreinte numérique du bloc[3] avec 20 zéros en hexadécimal à gauche.
5. L'empreinte numérique du bloc actuel, à savoir avec les 20 zéros.

Les mineurs vérifient si la transaction est valide avant de générer la preuve de travail :

1. L'auteur du virement, dispose-t-il de fonds suffisants ?
2. L'auteur du virement, a-t-il signé la transaction ?

Plusieurs mineurs sont en compétition pour générer la preuve de travail. Le mineur qui réussit à réaliser la preuve de travail[4] est récompensé. Tous les mineurs ajoutent le nouveau bloc valide à la blockchain.

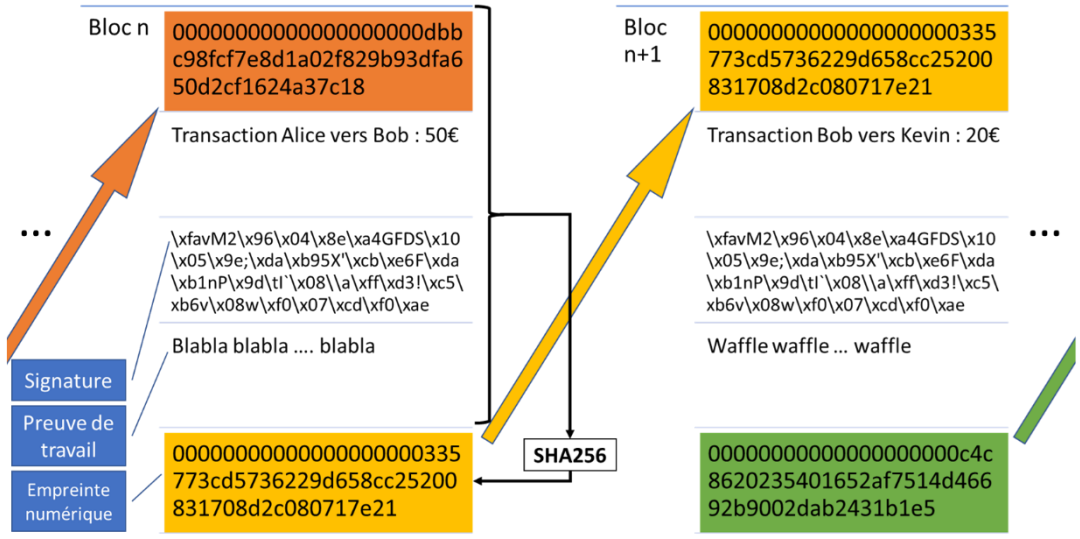

Figure 1. Exemple de contenu d'une blockchain

Les blocs sont liés entre eux en chaîne grâce aux empreintes numériques comme le montre la Figure 1. Ainsi, la moindre modification du contenu d'un bloc invalidera tous les blocs qui suivent. En effet, en plus du fait que la blockchain soit sauvegardée dans plusieurs endroits, la preuve de travail fait de sorte qu'il soit quasi-impossible de reproduire, des blocs successeurs valides sans moyens colossaux.

---

[1] La blockchain demandée sera moins complexe, à cause notamment de la simplification de la preuve de travail

[2] Ici l'empreinte numérique d'un document consiste seulement à appliquer l'algorithme SHA256 sur le document.

[3] L'empreinte numérique calculé avec SHA256 concerne seulement les 4 première parties du bloc : à savoir l'empreinte numérique du bloc précédent, la donnée du bloc, la signature de la transaction et la preuve de travail.

[4] Ajouter la phrase qui permet d'avoir une empreinte numérique avec 20 zéros en hexadécimal à gauche

1- Selon cette explication, quel est le critère de sécurité prioritaire de la blockchain, la confidentialité, la disponibilité ou l'intégrité ?

À la suite de cette brève description, nous souhaitons réaliser une blockchain personnelle pour tenir ses propres comptes.

2- Soit le code présenté dans le fichier main.py. Analysez le code et donnez les éléments qui constituent la version actuelle des blocs.
3- Quels sont les éléments manquants de la blockchain ?
4- Pour vérifier ses propres comptes, vous signez les transactions avec votre propre clé : Vous pouvez utiliser ecdsa (https://pypi.org/project/ecdsa/)[5] pour générer la paire de clés, signer et vérifier la signature de la transaction (réponse sous la forme d'un code commenté).
5- Etant donné l'absence de la signature de l'employeur, quel risque comporte cette blockchain ?
6- Vous souhaitez jouer le rôle du mineur. Il est possible d'ajouter une preuve de travail mais jusqu'à combien de zéros seriez-vous capable de réaliser ?[6] (Réponse en texte et sous la forme d'un code commenté)

[5] La librairie proposée n'est pas sécurisée mais vous pouvez l'utiliser dans ce contrôle. Il est possible de réaliser une attaque par canal auxiliaire étant donné que la multiplication dans les courbes elliptiques se réalise avec un algorithme similaire à celui de l'exponentiation rapide.
[6] Vous pouvez réaliser quelques tests pour avoir un temps voisin de 10 minutes avec votre PC.