Découverte

Fonctionnement de la blockchain

Rédigé par

David ROUMANET
Professeur BTS SIO

Changement

Date	Révision

Sommaire

A Introduction..... .1
A.1 Présentation..... .1
A.2 Prérequis..... .1
B Fonctionnement d'une blockchain..... .2
B.1 Hachage dans la blockchain..... .2
B.2 Notion de bloc..... .3
B.3 Chaîne de bloc..... .4
B.4 Distribution..... .5
B.5 Les tokens..... .6
B.6 Transactions..... .8
C Usages de la chaîne de blocs..... .9
C.1 Autres usages..... .9
C.2 NFT..... .9

Nomenclature :

- **Assimiler** : cours pur. Explication théorique et détaillée (globalement supérieur à 4 pages).
- **Décoder** : fiche de cours, généralement inférieure à 5 pages.
- **Découvrir** : Travaux dirigés. Faisable sans matériel.
- **Explorer** : Travaux pratiques. Nécessite du matériel ou des logiciels.
- **Mission** : Projet encadré ou partie d'un projet.
- **Voyager** : Projet en autonomie totale. Environnement ouvert : Vous êtes le capitaine !

A Introduction

La blockchain est arrivée en même temps que le Bitcoin, une monnaie numérique basée sur la cryptographie.

La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés. [Wikipédia]

L'intérêt de la blockchain n'est pas seulement lié à la monnaie, mais peut-être utilisé de manière différente, pour forcer l'intégrité et l'authentification de messages historisés.

A.1 Présentation

Cette rapide découverte sur la blockchain ou chaîne de blocs a pour objectif de montrer sur quels algorithmes et méthodes s'appuient les blockchains et pourquoi elles sont si fiables.

Une blockchain (du terme original en anglais), ou chaîne de blocs (du Journal officiel de la République française), est une technologie de stockage et de transmission d'informations sans autorité centrale. [Wikipédia]

A.2 Prérequis

Il sera plus simple de comprendre cette découverte si vous avez déjà quelques notions :

- Hachage, MD5, SHA-1, etc.
- Clé publique et clé privée

Ce cours s'appuie sur les outils proposés par Anders BROWNWORTH. Ce dernier a fait un ensemble d'outils permettant de parfaitement comprendre une blockchain et a également enregistré des vidéos, présentes sur son site web https://andersbrownworth.com/

B Fonctionnement d'une blockchain

La blockchain doit son nom aux éléments qui la constitue :

- Des blocs de données
- Des liens entre les blocs

Nous allons donc nous intéresser au contenu d'un bloc de données et nous assurer de son intégrité.

B.1 Hachage dans la blockchain

C'est par la fonction de hachage d'une donnée que l'on peut s'assurer qu'elle ne sera pas modifiée. Ainsi, la fonction de hachage délivre une chaîne de caractère de taille fixe, mais de valeur très variable, pour chaque donnée saisie.

Testez la fonction SHA-256 présente sur le site https://andersbrownworth.com/blockchain/hash

Trouvez-vous le même résultat que cette image pour le texte "Bonjour le monde !" ?

Que se passe-t-il si vous ajoutez un [espace] à la fin de la phrase ? De même si vous remplacez le B majuscule par une minuscule ?

Comme on peut le constater, une fonction de hachage fournit un résultat unique pour chaque donnée et ce résultat diffère énormément, même si les données diffèrent peu.

Combien de caractères contient le résultat du hachage ? Combien cela fait-il d'octet ?

Combien de possibilités existent ?

B.2 Notion de bloc

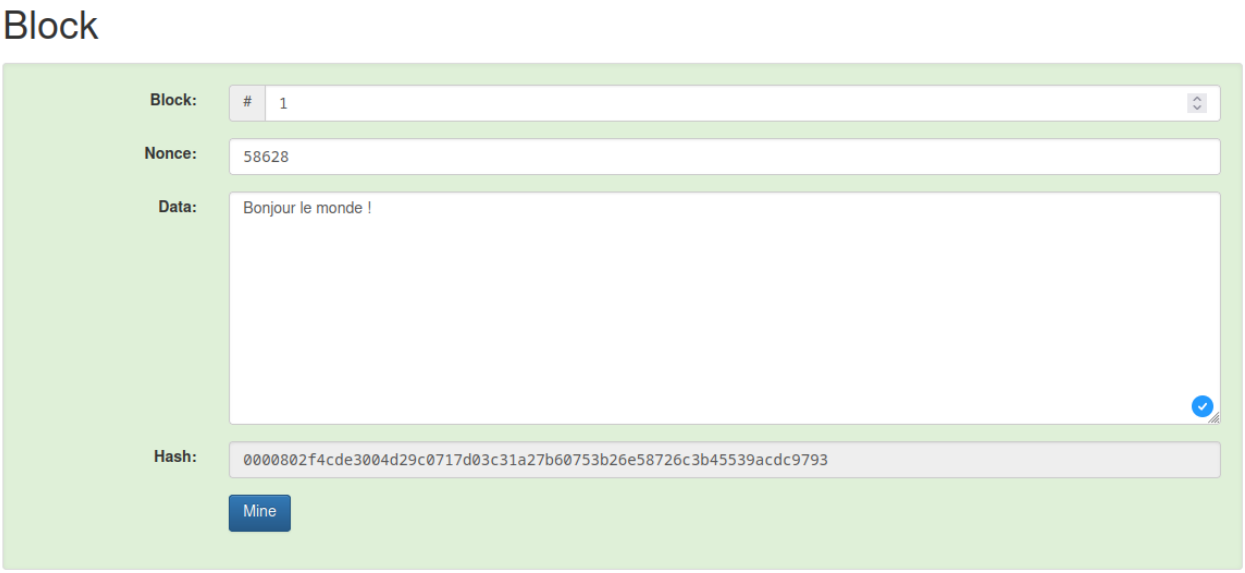
Maintenant que nous savons comment fonctionne la fonction de hachage, nous allons pouvoir l'utiliser d'une manière spécifique.

Les données que nous voulons sécuriser (non répudiation et intégrité) serons écrites dans un bloc. Ce bloc portera un numéro unique d'identification.

Enfin – et c'est là la particularité de la chaîne de bloc – le résultat du hachage du bloc doit commencer par 0000.

Pour permettre cela, on ajoute au bloc un numéro appelé "nonce" (un nombre unique sur 4 octets), qui permet de faire varier le résultat du hachage avec les données. C'est l'action de rechercher un nombre validant la condition, qu'on appelle "miner".

Essayez avec l'application d'exemple https://andersbrownworth.com/blockchain/block :



Une fois que le hachage est validé (vous avez cliqué [Mine] et l'application a trouvé un nonce qui valide le bloc), essayez de modifier les données.

Que se passe-t-il ? Pourquoi ?

Revalidez le bloc et modifiez ensuite le numéro du bloc : que se passe-t-il à nouveau ?

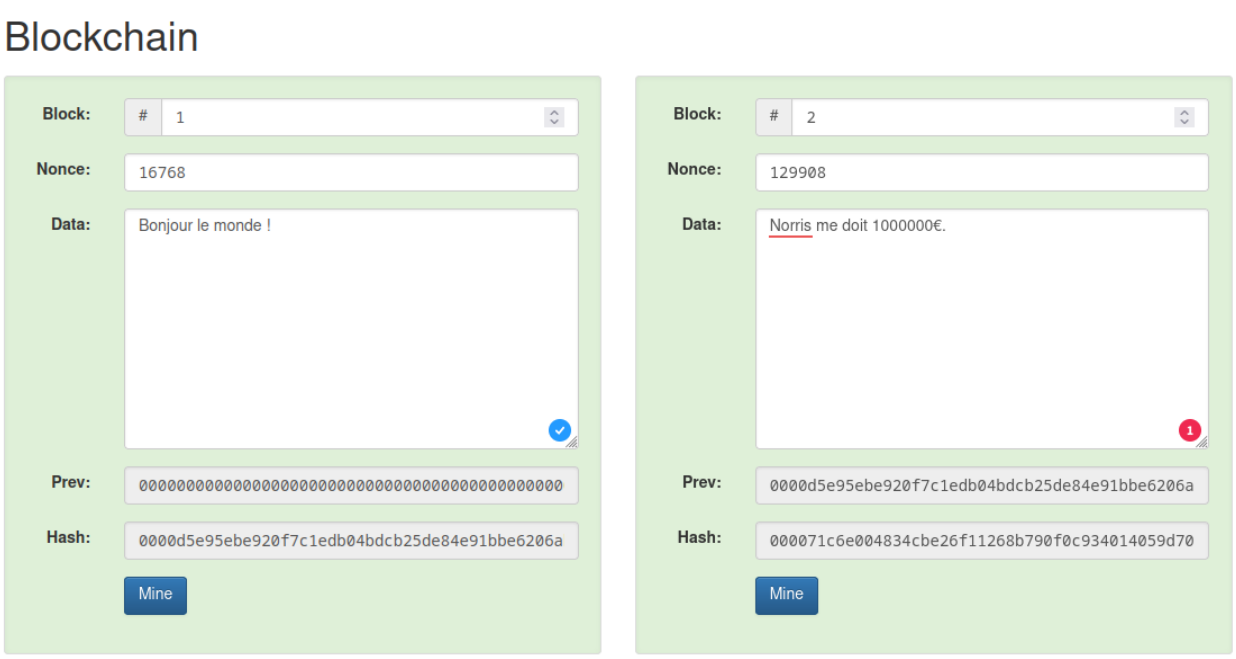
Ainsi, le hachage doit toujours être recalculé, Quel que soit le champ modifié. Désormais, nous allons lier les blocs entre eux pour créer une chaîne de bloc.

B.3 Chaîne de bloc

Nous avons donc des blocs qui nécessitent un calcul pour être validés (avoir un hachage commençant par 0000) mais les blocs sont indépendants. Chaque bloc peut contenir quelques opérations financières, donc changer une transaction implique de recalculer le nonce du bloc (calcul coûteux en temps).

Nous allons maintenant stocker dans nos données, le résultat du hachage du bloc précédent (sauf pour le premier bloc).

Testez l'exemple proposé dans le bloc https://andersbrownworth.com/blockchain/blockchain :



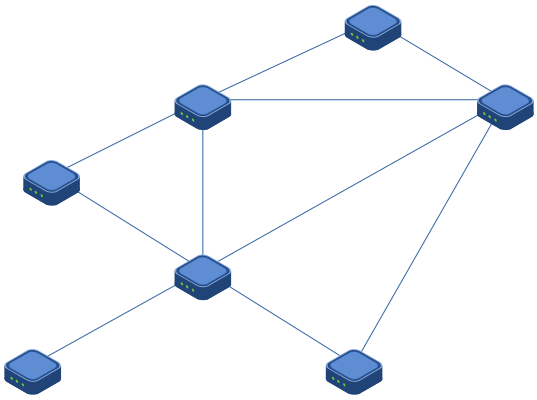
Cette fois, un changement dans le premier bloc rendra toute la chaîne, fausse, car le résultat du hachage du bloc 2 tient compte du bloc 1. Il faut donc recalculer les nonces de tous les blocs à partir du bloc modifié : cela peut prendre beaucoup de temps.

De plus, le bloc modifié est rapidement identifiable

Cependant, rien n'empêche un individu d'effectuer ce travail pour rendre la chaîne valide, c'est pourquoi, un autre mécanisme est présent dans le système de la blockchain.

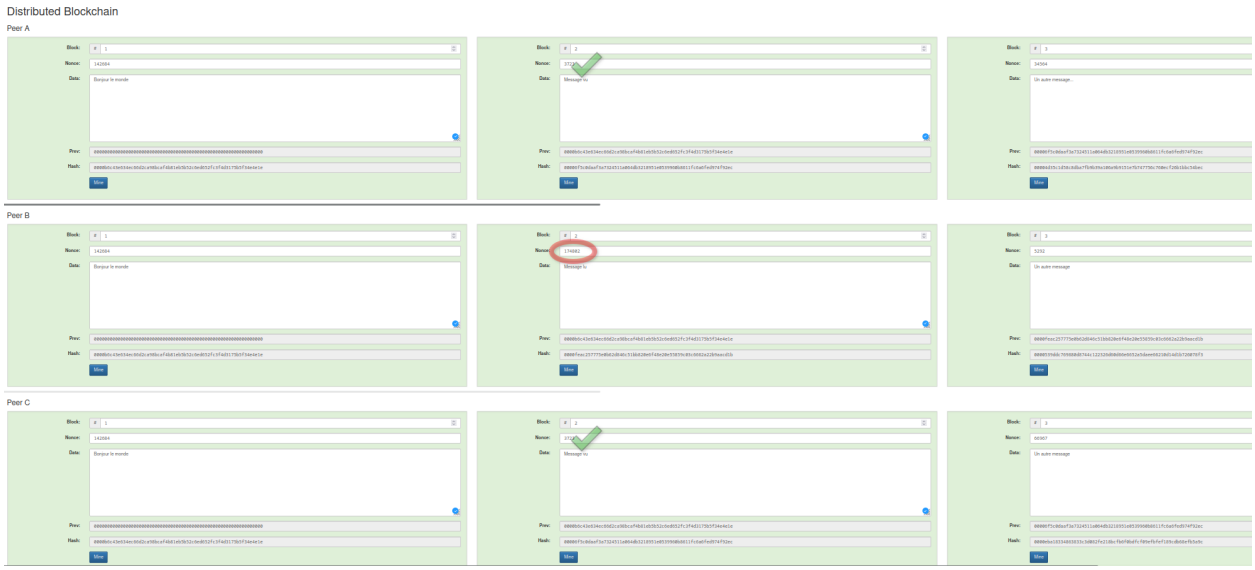
B.4 Distribution

La chaîne de bloc est donc re-calculable, au prix d'un effort de plus en plus conséquent, alors que la chaîne s'allonge. Cependant, chaque nœud participant au réseau, effectue les mêmes calculs et chaque nœud dispose des mêmes informations. Lorsqu'un bloc doit être clos, tous les nœuds recherchent le nonce de clôture et le premier qui le trouve, l'annonce à tous les autres.



Ainsi, il y a une élection pour valider les résultats, et la majorité des nœuds doivent avoir un résultat identique pour valider une nouvelle chaîne de blocs.

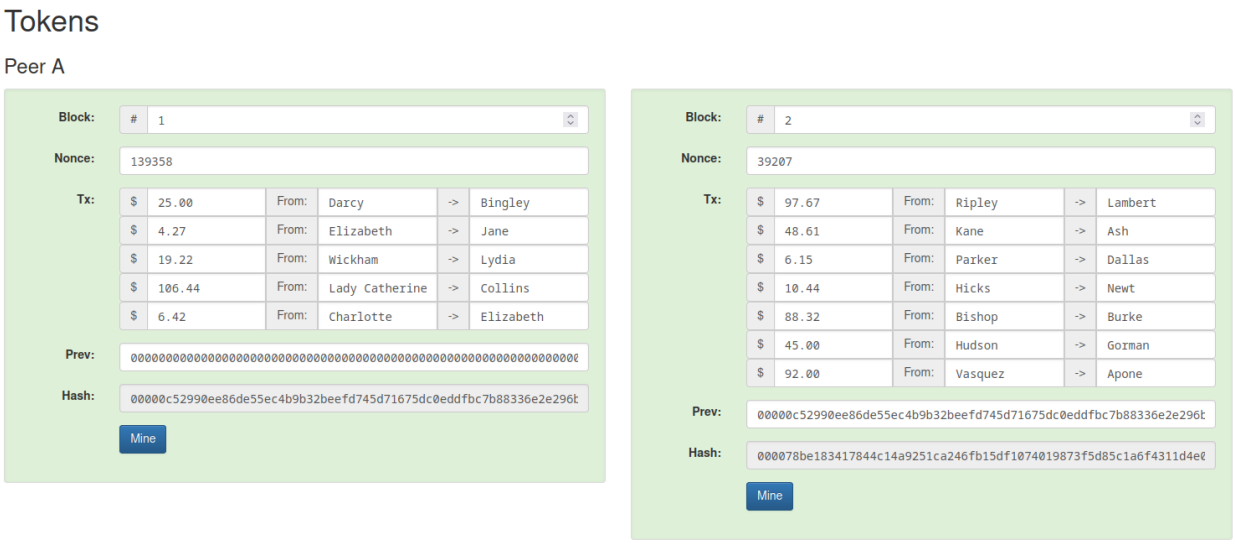
C'est la partie "Distributed" du site https://andersbrownworth.com/blockchain/distributed



Dans cet exemple, le nœud A et le nœud C sont cohérents, alors qu'une erreur a été introduite dans le second bloc du nœud B. La chaîne de bloc de B ne sera plus considérée comme valide et le nœud ne participera plus à la distribution de la chaîne de bloc, sauf si on arrive à corrompre plus de la moitié des nœuds.

B.5 Les tokens

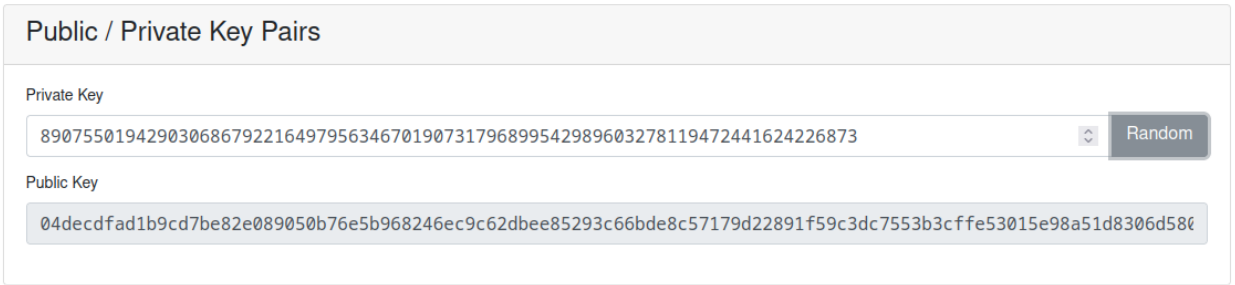
Dans les monnaies numériques, un bloc contient des opérations financières entre un émetteur et un bénéficiaire, c'est ce qu'illustre la partie du site https://andersbrownworth.com/blockchain/tokens :



Nous avons vu qu'il est possible de modifier une donnée et miner pour retrouver un nonce qui fonctionne : cela invalide toute la chaîne, mais on peut toujours imaginer isoler certains nœuds ou corrompre une partie du réseau.

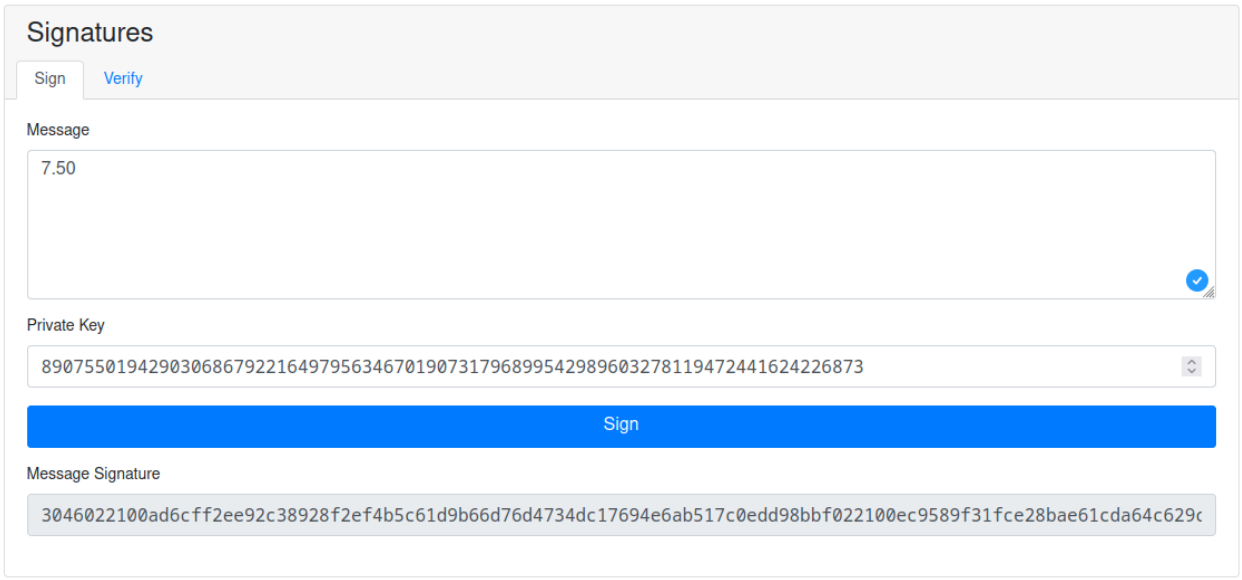
C'est ici que nous allons faire intervenir une autre notion importante dans le chiffrement : le chiffrement asymétrique et les clés privées et publiques.

Encore une fois, Anders nous permet de tester la génération de tels éléments que nous faisons généralement à l'aide d'OpenSSL, https://andersbrownworth.com/blockchain/public-private-keys/keys :



Pour chaque clé publique, il existe une clé privée unique. Ce système va servir à signer les opérations financières : ce ne seront donc pas des noms qui seront enregistrés dans le bloc de données, mais des signatures de données (c'est à dire, une données chiffrées à l'aide de la clé privée).

Voici un exemple de données ayant une telle signature :

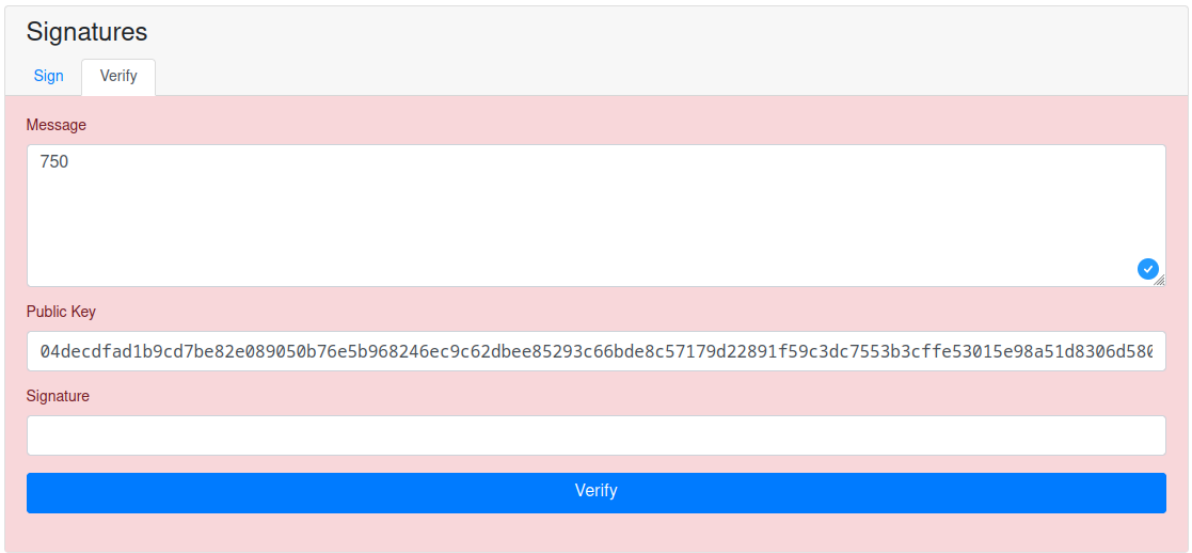


Ainsi, la signature ne peut être décodée que par la clé publique correspondant à la clé privée. Ce mode de fonctionnement permet à tout le monde de connaître le contenu du message (ce n'est pas le secret), mais surtout, il n'y a aucun doute sur l'origine du message (il s'agit du possesseur de la clé privée, correspondant la clé publique).

Rappel : il est absolument impossible de déduire la clé privée à partir de la clé publique, c'est ce qui rend le chiffrement asymétrique aussi efficace.

Vous pouvez effectuer des tests sur le site dédié au fonctionnement des clés publiques et privées https://andersbrownworth.com/blockchain/public-private-keys/signatures.

Si dans l'onglet [Sign] vous mettez une somme de 7.50 euros, signez le message puis allez dans l'onglet [Verify] et enlevez le point pour faire 750 euros, la vérification ne fonctionnera donc pas.



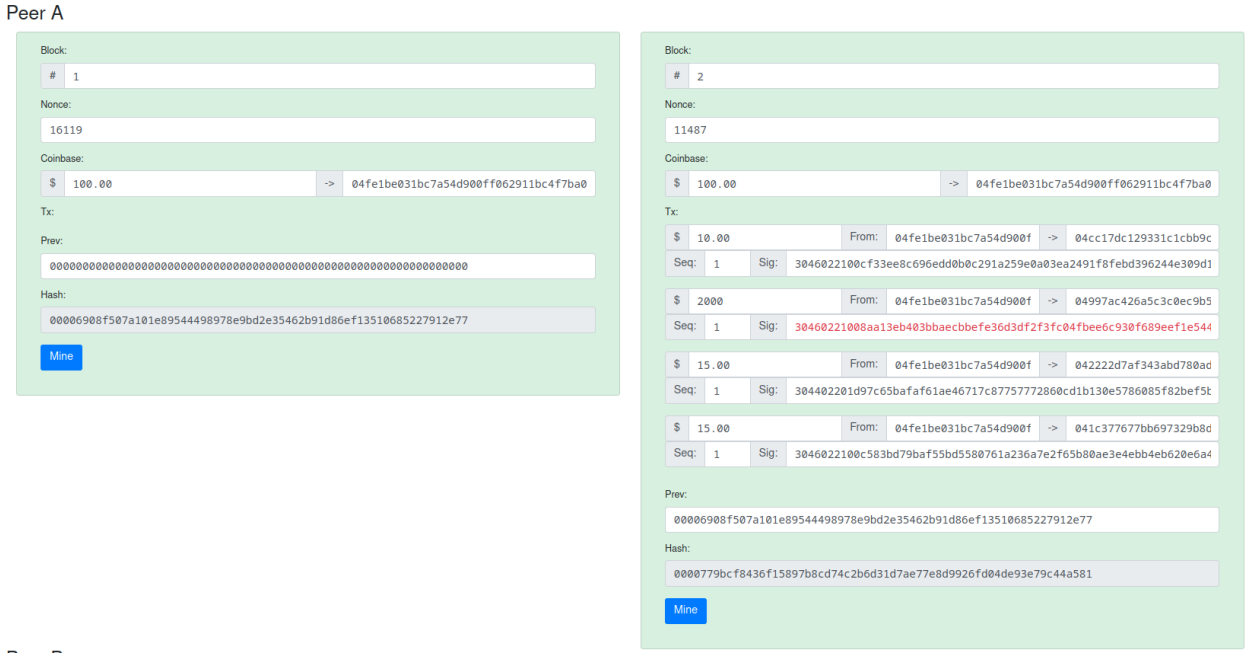
B.6 Transactions

Grâce au mécanisme précédent, nous allons pouvoir renforcer la sécurité des données et des tokens : les clés publiques de l'émetteur et du destinataire remplacent désormais leurs noms dans les données.

La signature permet d'éviter toute altération dans la transaction, que ce soit le montant ou l'une des clés publiques.

Vous pouvez le tester sur le lien https://andersbrownworth.com/blockchain/public-private-keys/transaction

Ainsi, même si le bloc est miné à nouveau (pour obtenir un nonce valide), l'opération en erreur est rapidement décelable (https://andersbrownworth.com/blockchain/public-private-keys/blockchain).



Tenter de modifier la signature ne fera qu'empirer les choses, ce qui rend le fonctionnement de la blockchain aussi fiable.

C Usages de la chaîne de blocs

La chaîne de blocs est un système extrêmement robuste et fiable, ce qui en fait l'élément essentiel pour traiter des flux financiers, comme pour les monnaies numériques (Bitcoins, Ethereum, etc.) et garantir un fonctionnement décentralisé. Chaque nœud participe à la sécurité du système et le nombre de nœuds est tellement élevé, que la corruption en devient presque impossible (du moins pour le moment).

C.1 Autres usages

On retrouve toutefois la chaîne de blocs dans d'autres applications, qui nécessitent de fournir des informations de traçabilité des informations :

- Le transport maritime et le commerce international, afin de réduire les erreurs de fraude et de livraison.
- La santé, pour assurer le stockage complètement décentralisé des dossiers médicaux et donner aux patients un contrôle sur leurs propres données médicales.
- L'industrie pharmaceutique, pour lutter contre la prolifération des médicaments dangereux, contrefaits.
- La transformation des aliments pour assurer un meilleur suivi de la provenance des aliments, le stockage et les conditions de transport.
- La certification des documents (identité, certificats de naissance, diplômes, voix ...), pour améliorer la lutte contre le vol d'identité.
- Les produits de luxe (bijoux, vin) pour lutter contre le risque croissant de la contrefaçon.

(source : https://academy.swissborg.com/fr/learn/blockchain-use-cases)

C.2 NFT

On retrouve également ce genre de besoins dans les NFT (Non Fongible Token) : une monnaie est généralement fongible, car on peut remplacer un billet d'une valeur particulière par un autre billet de même valeur.

À l'inverse, les tokens non fongibles (NFT) sont uniques et identifiables. Pour garantir la conformité des copies des NFT et assurer l'absence d'altération, la blockchain est alors le moyen idéal de gérer ces tokens. Le NFT ne garantit pas que le token ne sera pas copié, mais il garantit que celui qui possède le token en est le propriétaire (et peut donc le céder).