Diploma Programme
Programme du diplôme
Programa del Diploma

Informatique
Étude de cas : Une economie locale dopée par blockchain

A utiliser en mai 2020, novembre 2020 et mai 2021

Instructions destinées aux candidats

- Ce livret d'étude de cas est indispensable pour l'épreuve 3 du niveau supérieur.

Introduction

Santa Monica est une ville qui ressemble à bien d'autres dans le monde. Depuis plusieurs décennies, la population est en déclin et de nombreuses entreprises locales ont fermé leurs portes. L'argent sort de la communauté lorsque les habitants de Santa Monica dépensent leurs pesos dans les magasins des multinationales.

Pablo, son maire, souhaite inverser le processus. Il a mené son enquête auprès de villes qui ont créé leur propre monnaie locale et pense que cette idée pourrait fonctionner à Santa Monica. Il a découvert que les monnaies locales étaient utilisées conjointement à la monnaie nationale. Un exemple de cela serait qu'une unité de monnaie locale équivaudrait à un peso. Par ailleurs, la monnaie locale ne détient aucune valeur en dehors de la municipalité. Elle ne peut donc pas être convertie en d'autres devises comme le dollar américain. Cependant, si la nouvelle monnaie locale était adoptée à Santa Monica, ses habitants seraient en mesure de la reconvertir en pesos à tout moment.

Les enquêtes de Pablo ont montré qu'une fois une monnaie locale bien implantée, celle-ci apportait des bienfaits considérables à une municipalité. Les commerces de proximité ont plus de clients et sont en mesure de donner des remises à ceux payant en monnaie locale. La main d'œuvre locale en comprend les avantages et accepte même de recevoir une partie de son salaire en monnaie locale. Toutefois, dans de nombreux cas, les monnaies locales ne fonctionnent pas en raison de frais d'administration trop élevés, par exemple le coût de l'impression des billets, la lutte contre la fraude et la prestation de services bancaires complémentaires.

Dolores, une habitante de Santa Monica diplômée en informatique, a proposé une solution qui pourrait surmonter ces problèmes. Elle suggère qu'« une *crypto-monnaie* (*cryptocurrency*) utilisant la technologie *blockchain* pourrait permettre à Santa Monica de les éviter car elle ne nécessite aucune gestion centralisée. Des personnes qui ne se connaissent pas peuvent effectuer des transactions sans avoir recours à une autorité centrale. Les coûts associés à cette dernière seraient donc éliminés. » Pablo et Dolores ont décidé que l'étape suivante serait de promouvoir une nouvelle crypto-monnaie appelée MONS pour Santa Monica.

Le projet MONS

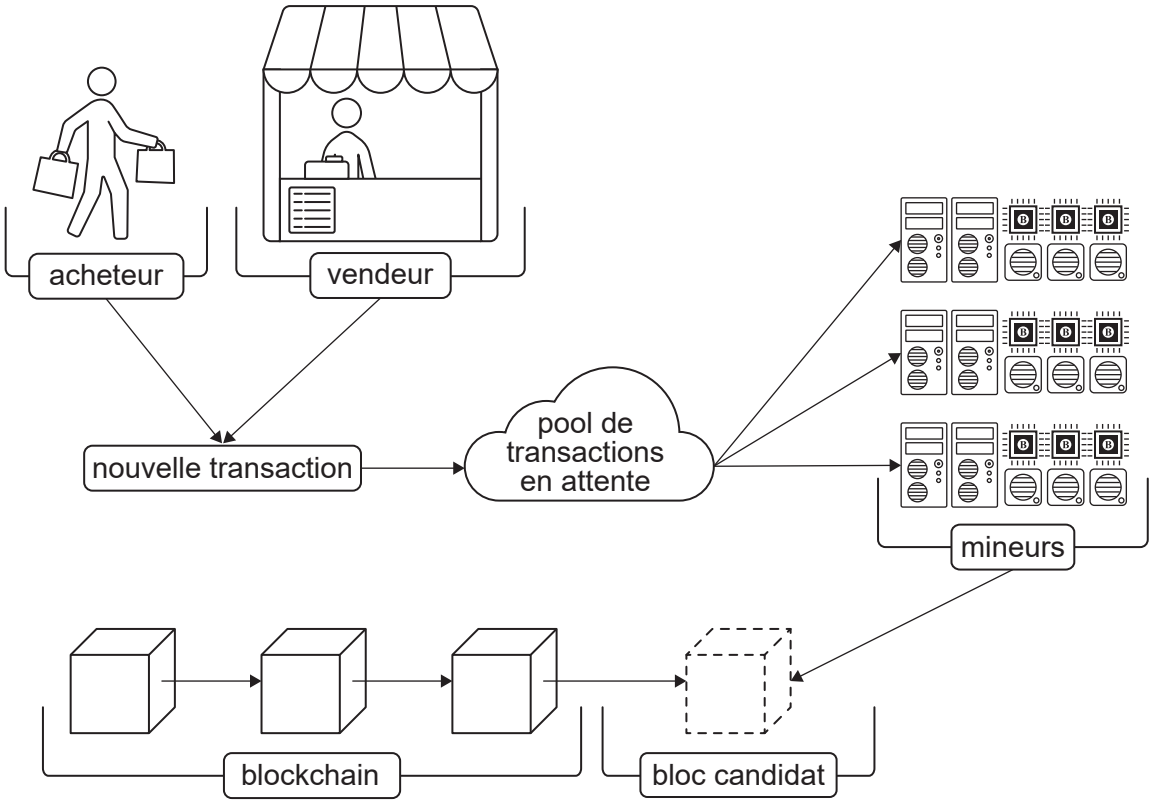
Dans le système bancaire traditionnel, un paiement est soumis à un processus de compensation qui peut prendre dix jours ouvrés. Pendant cette période, la banque du payeur et le bénéficiaire communiquent entre eux pour valider la transaction, transférer les fonds et vérifier la réussite du paiement. Le MONS ne disposerait pas d'une banque centrale pour ce processus ; il faudrait donc trouver une autre solution.

Une crypto-monnaie fait face à plusieurs défis, dont :

- la création d'une transaction ;
- la vérification de l'exactitude de la transaction ;
- l'enregistrement de la transaction de sorte qu'elle ne puisse pas être ultérieurement modifiée.

Dolores a expliqué à Pablo comment les transactions sont créées et validées par les nœuds du réseau, plutôt que par une autorité centrale. Ceux-ci sont ensuite ajoutés dans des groupes appelés *blocs* (*blocks*), similaires à des pages dans un *registre* (*ledger*) numérique. « Dès que la transaction est validée, un nouveau bloc peut être ajouté à la blockchain », précise-t-elle. « Il est accessible à tous mais ne peut pas être modifié. »

Figure 1 : le parcours d'une transaction



Dolores explique que « les crypto-monnaies contemporaines utilisent un réseau pair-à-pair (P2P) pour émettre et recevoir les paiements. L'appareil de chaque utilisateur MONS représente un nœud dudit réseau. Ce nœud détient une adresse de 26 caractères alphanumériques. Lorsqu'un utilisateur dépense de la monnaie, il transfère le montant de MONS de son adresse à l'adresse du compte de la personne qu'il paye. Les détails de la transaction sont ensuite émis sur le réseau. »

« Les autres nœuds du réseau valident la transaction indépendamment les uns des autres en effectuant une série de vérifications. L'une d'entre elles utilise la *signature numérique* (*digital signature*) de la transaction pour vérifier l'identité de l'expéditeur. Une autre s'assure que l'acheteur n'a pas déjà dépensé le MONS de la transaction (*problème de double dépense – double-spend problem*). » Si la transaction est valide, le nœud l'envoie à ses nœuds voisins qui la vérifient et l'envoient à leur tour. Ainsi, seules sont propagées sur le réseau les transactions valides et, importance cruciale, il n'existe aucune autorité unique déterminant la validité desdites transactions. Les transactions validées sont regroupées dans le *pool de transactions en attente* (*transaction pool*).

Même si les transactions se trouvant dans le pool de transactions en attente ont été validées, elles demeurent non confirmées. Certains nœuds spécialisés du réseau sont appelés *mineurs* (*miners*). Ils se chargent de regrouper les transactions du pool non confirmées dans des *blocs candidats* (*candidate blocks*) à ajouter à la blockchain. Celle-ci contient toutes les transactions confirmées qui aient jamais été effectuées.

Les mineurs calculent une *preuve de travail* (*proof of work*), qui est nécessaire pour trouver un *nonce* (mot a usage unique) de résolution du bloc, puis pour ajouter le bloc candidat à la blockchain. Ce qui motive les mineurs à effectuer ce travail est le paiement par le réseau d'une petite somme de MONS ainsi que la perception de frais modiques provenant des participants à la transaction. Dolores ajoute que « le temps nécessaire à résoudre un bloc ne doit être ni trop court, ni trop long. Nous avons pour objectif une durée de 10 minutes environ. »

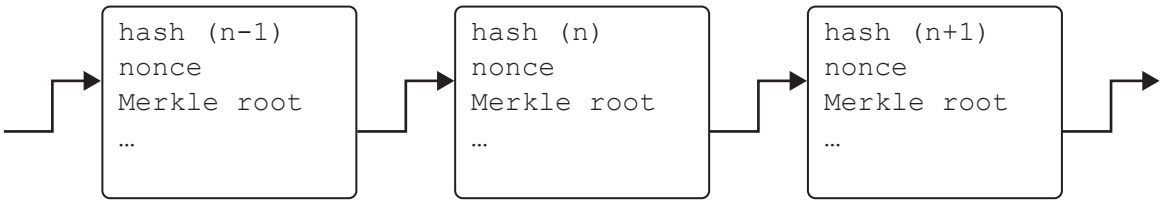
Tournez la page

Un mineur peut améliorer ses chances d'être le premier à résoudre un bloc en utilisant un grand nombre de processeurs graphiques (GPU – *graphics processing unit*). « Plus la monnaie est utilisée, plus le nombre de mineurs qui essaient de résoudre la preuve de travail augmente et bien sûr plus il y a de mineurs capables de résoudre les blocs rapidement. Cependant, l'un des grands avantages de la blockchain est d'assurer que le temps de résolution ne dépasse pas 10 minutes, ce qui est possible même si le nombre de mineurs de MONS augmente », affirme Dolores.

La structure de la blockchain

La blockchain est une *structure de données autoréférentielle* (*self-referential data structure*) dans laquelle chacun des blocs fait référence au bloc suivant.

Figure 2 : diagramme de représentation de la blockchain



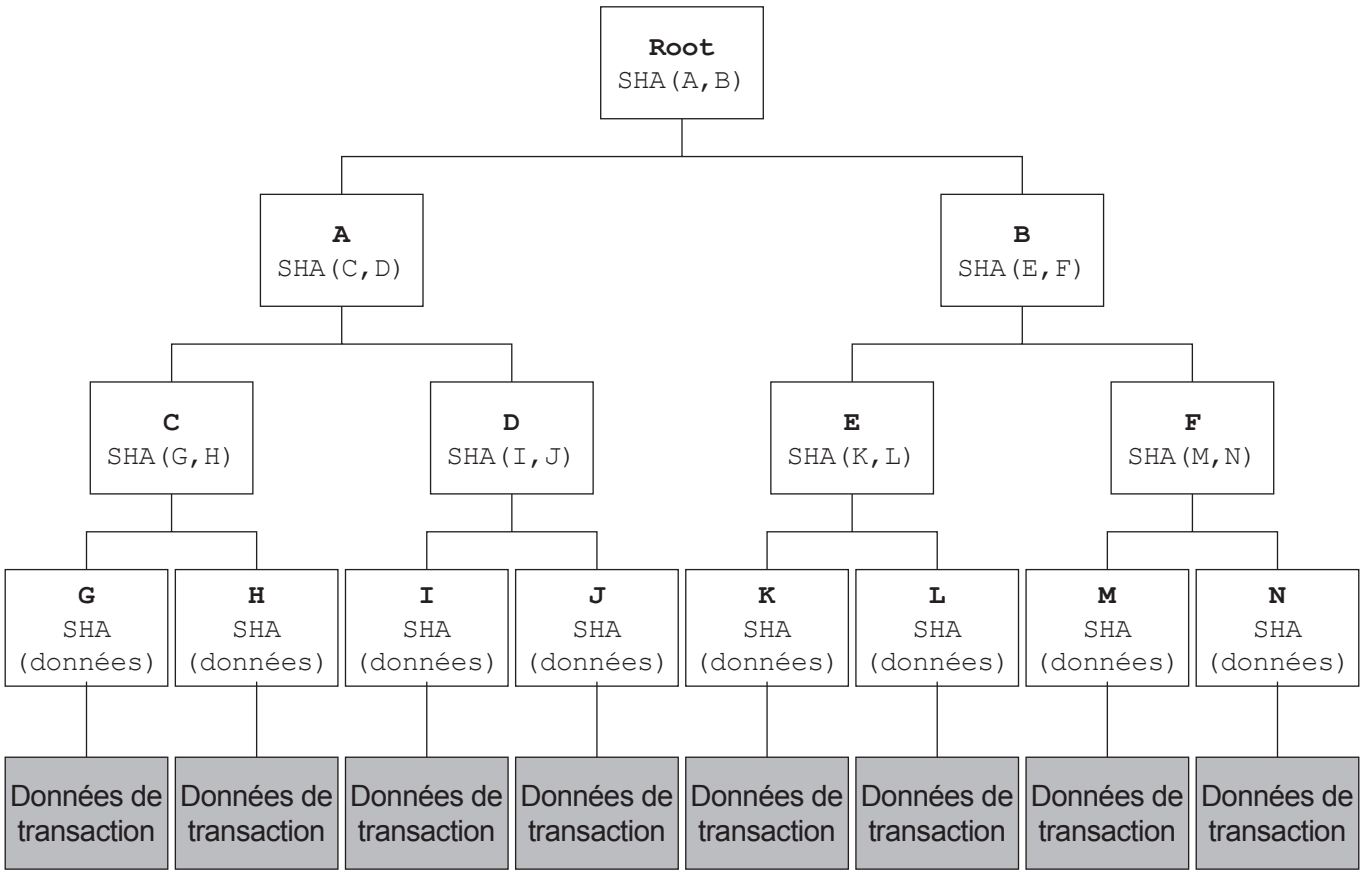
Un ensemble de métadonnées appelé *en-tête de bloc* (*block header*) contient les données détaillées relatives à chaque bloc.

Figure 3 : exemple d'en-tête de bloc

```
"number_of_transactions":188
"height":5432
"block_reward":2
"timestamp":1391270636
"merkle_root":0e83db9efb10076982a……94574318e7e
"previous_block":5341
"difficulty":2548.2
"bits":172758700
"size":317202
"version":912
"nonce":196898444
"next_block":5433
```

La liste des transactions de chaque bloc est stockée dans un *arbre de Merkle* (*Merkle tree*), dont la racine est référencée par l'en-tête de bloc. Un arbre de Merkle est un arbre binaire dans lequel chaque nœud parent contient le *hachage cryptographique* (*cryptographic hash*) de ses nœuds enfants, et chaque nœud terminal contient le hachage cryptographique de ses propres données. Dans la blockchain MONS, chacun des nœuds de données stocke les informations relatives à une transaction.

Figure 4 : exemple d'un arbre de Merkle



L'utilisation de la cryptographie dans le projet MONS

Dolores a bien fait ressortir l'importance du rôle des algorithmes de chiffrement dans le projet MONS envisagé. « La cryptographie sera utilisée dans tout le système, en particulier les algorithmes de hachage comme le *SHA256*, » explique-t-elle. « Les caractéristiques essentielles d'un bon algorithme de hachage sont le *déterminisme* (*determinism*), l'*irréversibilité* (*non-invertibility*) et la *résistance aux collisions* (*collision resistance*). »

Tableau 1 : exemples d'entrées et de sorties SHA256

Entrée	Sortie
`"a"`	`87428fc522803d31065e7bce3cf03fe4750 96631e5e07bbd7a0fde60c4cf25c7`
`"Voix ambiguë d'un cœur qui au zéphyr préfère les jattes de kiwis"`	`c03905fcdab297513a620ec81ed46ca44dd b62d41cbbd83eb4a5a3592be26a68`
`"Voix ambiguë d'un cœur qui au zéphyr préfère les jattes de kiwis."`	`b47cc0f104b62d4c7c30bcd68fd8e67613e 287dc4ad8c310ef10cbadea9c4381`
`[PDF du Guide de l'IB pour l'Informatique]`	`370e5655ff2e4e63e307e09e560639c72abb b8b5066616a72a130e2eb0240b8f`

Dolores a ensuite énuméré les quatre domaines clés du projet, dans lesquels les algorithmes de chiffrement joueront un rôle essentiel.

La signature numérique

La signature numérique se repose sur le hachage et la cryptographie à clé asymétrique pour garantir les trois critères essentiels suivants :

- l'authentification ;
- la *non-répudiation* (*non-repudiation*) ;
- l'intégrité.

Les signatures numériques servent à valider les transactions MONS avant leur ajout au pool de transactions en attente. Le processus de validation comporte trois étapes :

- la génération de clés ;
- la création de la signature ;
- la vérification de la signature.

« Les logiciels de génération de clés comme *PuTTYgen* utilisent souvent une source physique d'entropie pour générer les biclés », ajoute-t-elle.

La preuve de travail

Outre la signature numérique, la preuve de travail exige des mineurs qu'ils trouvent un hachage possédant une caractéristique particulière, qui est à déterminer. Par exemple, certaines crypto-monnaies spécifient que le hachage doit commencer par un nombre de zéros déterminé.

La blockchain

La blockchain utilise le hachage pour s'assurer que les transactions présentes dans le registre, bien qu'accessibles à tous les utilisateurs du réseau, ne peuvent pas être modifiées.

L'arbre de Merkle

L'arbre de Merkle est aussi connu sous le nom d'arbre de hachage. Il permet de déterminer l'existence d'une transaction dans un bloc bien plus efficacement que si la transaction figurait simplement dans une liste.

La promotion du MONS aux habitants de Santa Monica

Dolores a convaincu Pablo des avantages de l'adoption du MONS comme crypto-monnaie locale, mais il craint que les habitants de Santa Monica soient réticents à passer du peso au MONS.

Il souligne qu'une différence particulière entre une monnaie traditionnelle et le MONS devra être expliquée avec soin : « Dans un système bancaire traditionnel, les usagers ont confiance dans la capacité des banques à protéger l'argent de tous. Avec le MONS, la blockchain entière, depuis la toute première transaction, sera visible par tous les usagers du MONS. Il est donc important de pouvoir expliquer aux citoyens que leur argent est garanti d'être protégé. »

Dolores ajoute à cela que « le solde en MONS d'un utilisateur n'est pas stocké : il est calculé en temps réel en vérifiant toutes les transactions précédentes. Donc, tant que toutes les transactions précédentes continuent d'être exactes, leur solde le sera également. La blockchain se repose sur un *consensus distribué* (*distributed consensus*) sur tous les nœuds du réseau. Par conséquent, dans un réseau de taille suffisante, il est difficile de monter une *attaque 51%* (*51% attack*). »

Pablo s'interroge également sur les possibles conséquences sur les habitants de l'absence d'une autorité centrale gérant le MONS, ainsi que sur les autres inconvénients potentiels d'une crypto-monnaie.

Défis rencontrés

De nombreux défis à relever sont associés à l'introduction du MONS. Ceux-ci incluent :

- comprendre comment les nouveaux blocs sont ajoutés au registre et comment la preuve de travail empêche les nœuds frauduleux de prendre le contrôle du réseau MONS ;
- comprendre comment l'architecture du MONS est évolutive et demeure efficace alors que le nombre d'utilisateurs augmente ;
- comprendre l'utilisation des techniques de cryptographie dans le projet MONS ;
- expliquer aux habitants de Santa Monica comment leurs soldes en MONS est calculé à partir des données de transaction stockées de manière sécurisée dans le registre blockchain, qui est accessible par tous ;
- étudier comment la nature distribuée d'une crypto-monnaie fondée sur la technologie blockchain et le processus de confirmation peuvent être désavantageux pour les habitants de Santa Monica.

Les candidats n'ont pas besoin de savoir en détail la manière dont un algorithme de hachage particulier est mis en œuvre.

L'analyse des arguments économiques pour ou contre les monnaies locales et les crypto-monnaies ne rentre pas dans le cadre de cette étude de cas.

Terminologie ne figurant pas dans le guide

Arbre de Merkle (*Merkle tree*)
Attaque 51 % (*51% attack*)
Attaque avec prise de contrôle (*takeover attack*)
Bloc (*block*)
Bloc candidat (*candidate block*)
Bloc de genèse (*genesis block*)
Blockchain
Consensus distribué (*distributed consensus*)
Crypto-monnaie (*cryptocurrency*)
Déterminisme (*determinism*)
En-tête de bloc (*block header*)
Entropie (*entropy*)
Fonction unidirectionnelle (*one-way function*)
Génération de biclé (*key pair generation*)
Hachage cryptographique (*cryptographic hash*)
Irréversibilité (*non-invertibility*)
Minage (*mining*)
Mineur (*miner*)
Nonce (mot a usage unique)
Non-répudiation (*non-repudiation*)
Pool de transactions en attente (*transaction pool*)
Preuve de Merkle (*Merkle proof*)
Preuve de travail (*proof of work*)
Problème de double dépense (*double-spend problem*)
PuTTYgen
Racine de Merkle (*Merkle root*)
Registre (*ledger*)
Résistance aux collisions (*collision resistance*)
SHA256
Signature numérique (*digital signature*)
Structure de données autoréférentielle (*self-referential data structure*)
Transactions inaltérables (*immutable transactions*)

Certains produits, sociétés et individus mentionnés dans cette étude de cas sont fictifs. Toute ressemblance avec des entités réelles ne saurait être que fortuite.