MIAGE NANCY

Bibliographie et application
Analyse bibliographique

La blockchain

Élèves :
Benoît Cante
Nicolas Lamblin

Enseignant :
Olivier Perrin

8 janvier 2019

Table des matières

1 Introduction

1.1 Qu'est-ce que la blockchain ?

La blockchain est un registre de transactions publiques créée en octobre 2008 suivi d'une publication des sources l'année suivante.
En effet, grâce à cette technologie les utilisateurs ont la possibilité de procéder à des échanges de diverses natures sans utiliser d'intermédiaire. L'ensemble des échanges réalisés depuis la création de la chaîne sont stockés dans un registre, ce qui permet d'identifier les auteurs des transactions. Enfin, le consensus distribué permet aux utilisateurs eux-mêmes de conserver le registre mais également de valider les transactions.

La blockchain a été rendue "populaire" avec l'essor des cryptomonnaies et notamment du Bitcoin. Elle est peut être utilisée pour répondre à diverses problématiques telles que les transactions financières ou encore les signatures de pétitions.

La blockchain, n'est comme son nom l'indique ni plus ni moins qu'une chaîne de blocs liés entre eux où chaque bloc stocke des transactions. La plus part des informations sur cette partie nous proviennent d'une conférence Devoxx sur la blockchain [1]

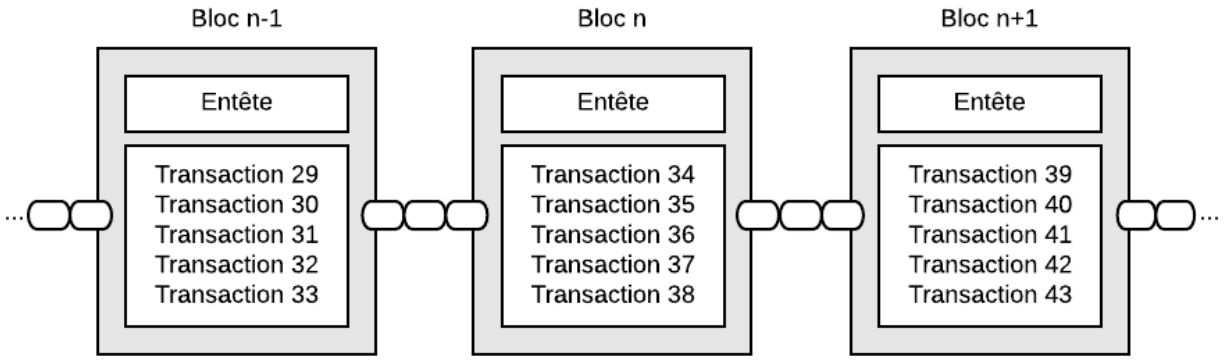

FIGURE 1 – Blockchain simplifiée

1.2 Objectifs de la blockchain

1.2.1 Indépendance vis-à-vis des intermédiaires

La possibilité de se passer d'intermédiaires, offerte par la décentralisation, est extrêmement attractive pour beaucoup. Que ce soit par éthique (souhait de garder le minimum de personnes possibles impliquées dans un contrat), ou pour l'aspect pratique (limiter les coûts et la lourdeur des transactions). Bien entendu, se passer des intermédiaires ne peut s'envisager qu'à long terme. Déplacer la confiance d'un tiers vers un réseau est très difficile, et n'aura pas lieu de sitôt.

1. https://www.youtube.com/watch?v=J0MgFQ-j6nE

1.2.2 Traçabilité

Un des points les plus importants est l'aspect "gravé dans le marbre" que prennent les transactions. Une fois celle-ci vérifiée par le réseau (et qu'un certain délai soit passé), on peut toujours faire référence à cette transaction, car tous les noeuds l'ont renseigné. Ainsi, cela permet d'avoir plus aisément confiance dans le réseau, car les utilisateurs savent ce qu'il s'y est passé. On imagine sans peine l'énorme gain qu'on peut trouver dans les professions d'audit, qui ont pour principale difficulté de démêler le vrai du faux et trouver des documents qui font foi.

1.2.3 Transparence

Nous avons vu que chaque transaction est consignée et connue des autres noeuds du réseau. De cette manière, on évite l'aspect "boîte noire" et chaque utilisateur à la garantie que toutes les transactions qui ont lieu peuvent être visibles.

2 Comment fonctionne la blockchain ?

2.1 La chaîne

La chaîne est composée de blocs qui sont liés entre eux.

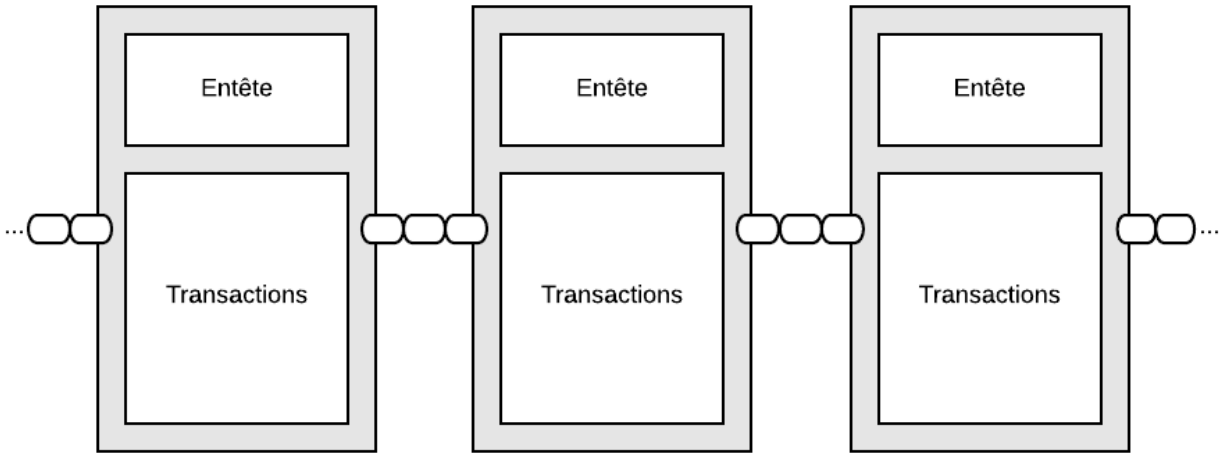

FIGURE 2 – Schéma simplifié de la chaîne

2.2 Les blocs

Les blocs sont composés de deux parties : l'entête et les données.

2.2.1 L'entête

Dans l'entête d'un bloc sont contenues l'ensemble des informations qui permettent d'obtenir son hash [2]. Le hash est obtenu en cryptant l'ensemble des informations contenues dans l'entête. Et c'est ce hash qui permettra de faire le lien entre les blocs.

2. Série de chiffre et de lettres générée par une fonction de hash. Cette fonction permet, à partir d'une donnée fournie en entrée d'obtenir une empreinte numérique.

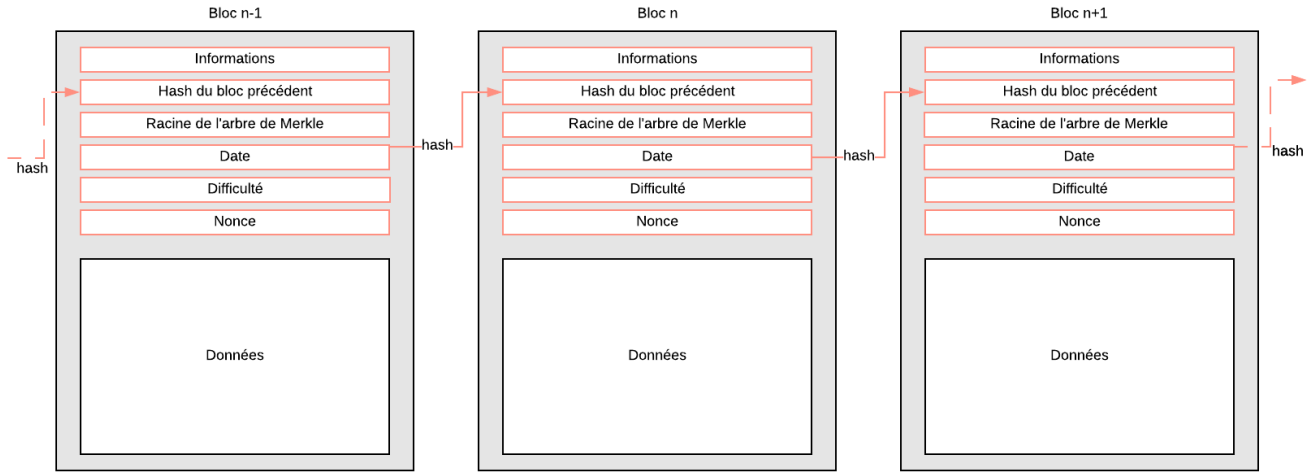

FIGURE 3 – Schéma détaillé de la blockchain

Des informations techniques

Dans cet attribut peuvent se stocker diverses informations telles que la version de la blockchain utilisée.

Le hash du bloc précédent

En effet, il est nécessaire d'établir un lien entre les blocs afin de créer une chaîne. Cela est rendu possible par cet attribut.

La racine de l'arbre de Merkle

Cet élément est essentiel puisque c'est lui permet de retrouver les transactions présentes dans le bloc.

La date

Stockée sous la forme d'un timestamp, cette valeur correspond à la date de création du bloc.

La difficulté ciblée

La difficulté est une mesure relative qui permet de calculer combien il est difficile d'attendre une valeur inférieure à la cible. La cible est la borne supérieure selon laquelle un mineur peut créer un bloc et l'ajouter à la chaîne. En effet, un bloc ne peut être considéré comme valide que si seulement et seulement si la valeur du hash du bloc courant est inférieure à la cible. Prenons comme exemple une cible de 000000000d45f8, un bloc ne pourra être ajouté que si la valeur de son hash est inférieure à 000000000d45f8.

Le nonce utilisé

Le nonce correspond à un nombre aléatoire utilisé par les mineurs afin de trouver un hash qui satisfait la difficulté. Le nonce est la seule valeur de l'entête du bloc qui va être modifiée lors de la recherche d'un hash.

2.2.2 Les données

Les données sont stockées à l'aide d'un arbre de Merkle (figure 5) dans la seconde partie du bloc. Les feuilles de l'arbre sont les valeurs de hash de chacune des données initiales. Puis, ces hash sont alors concaténés deux à deux pour pouvoir calculer un nouveau hash parent. Ainsi de suite jusqu'à la racine, racine qui se retrouve dans l'entête.

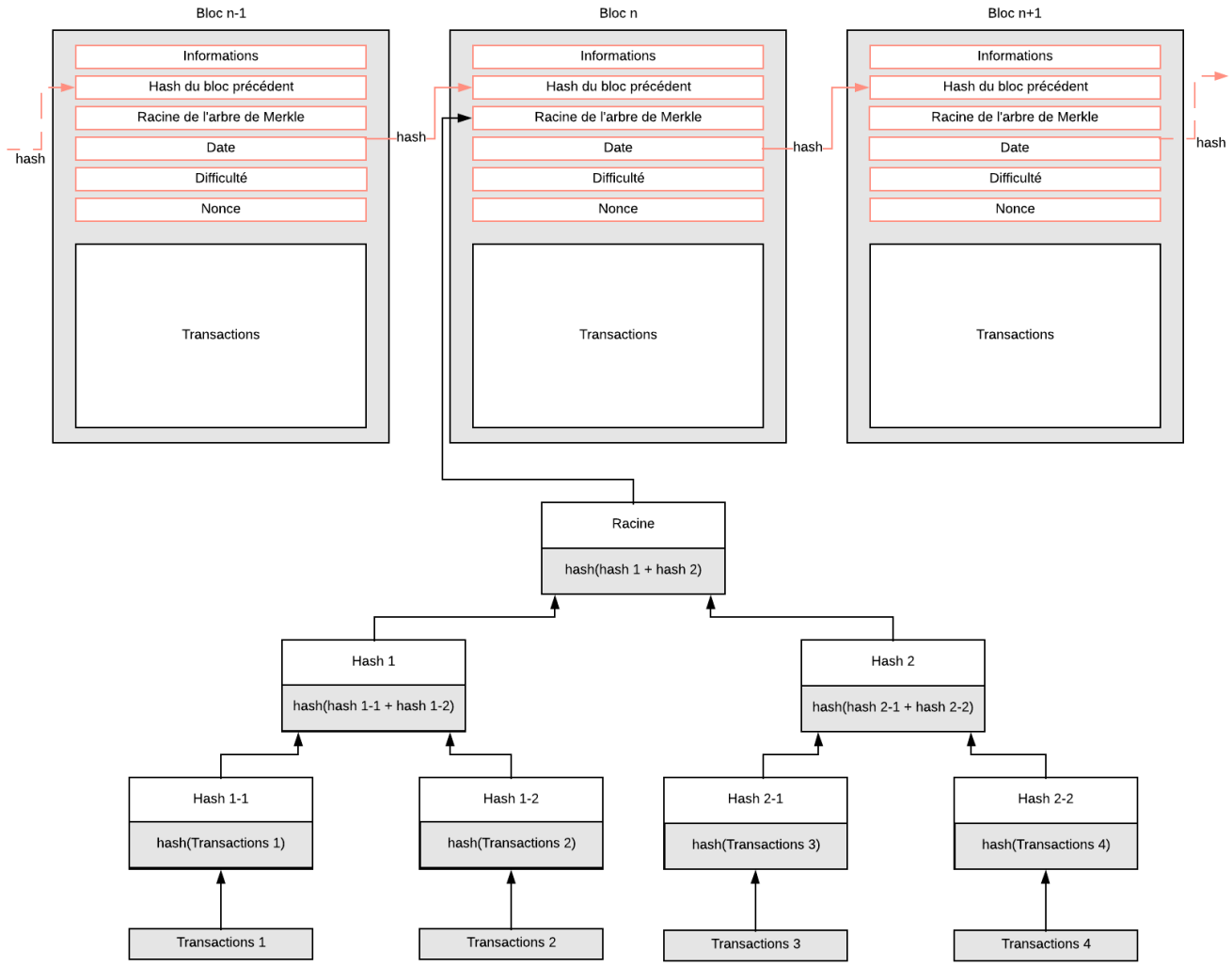

FIGURE 4 – Arbre de Merkle

2.3 Clé publique et clé privée

Dans la blockchain, chaque compte est représenté par deux clés. La première est l'adresse publique et peut être communiquée, la seconde est privée et doit être proté-

gée et inaccessible. La clé publique est générée à partir de la clé privée. Ce procédé de signature électronique est basé sur la cryptographie asymétrique. La clé privée permet alors de chiffrer un message déposé sur la blockchain et la clé publique de déchiffrer ce message. Ce procédé permet alors de s'authentifier de manière sûre. Le détail de l'article utilisé pour comprendre comment fonctionnent les clés publiques et privées peut être trouvée ici : `https://bit.ly/2scccSI`

Cependant, si la clé privée venait à être dérobée par un tiers, ce dernier pourrait alors procéder à des échanges frauduleux en signant des opérations dans le but de vider un compte par exemple.

2.4 Proof Of Work

"Proof Of Work" (preuve de travail) est un système de validation permettant l'ajout d'un bloc à la chaîne. Il permet notamment d'éviter le problème de double dépense.On parle de ce problème quand un utilisateur frauduleux veut envoyer le même argent à un utilisateur A et B (dans la vraie vie, on parlerait d'un chèque en bois). Pour éviter ce problème dans la vie courante, on utilise un intermédiaire de confiance : les banques ou des sites de paiement tels que Paypal. Si on veut se passer de ces derniers, il faut alors échanger en espèces, ce qui est bien moins pratique. La blockchain évite le recours à cet intermédiaire de confiance, en faisant vérifier les transactions par l'ensemble du réseau. Le Proof of Work est un exemple de solution à ce problème.

Le principe du Proof of Work est simple : pour garder une cohérence dans le réseau et éviter que des blocs soient ajoutés de manière anarchique, les noeuds qui veulent ajouter un bloc doivent prouver leur implication en mettant à la disposition des membres du réseau les capacités de calcul de son (ou plutôt ses) ordinateur(s). Le mineur doit trouver un argument, dont le hash est inférieur à une certaine valeur. Pour cela il fait varier le nonce défini plus haut. La seule possibilité de trouver la bonne valeur est de faire l'équivalent d'une attaque en brute force, à savoir tester toutes les valeurs possibles jusque à ce que l'équation soit résolue. Ainsi, tous les noeuds vérifient en permanence les transactions qui sont émises. Si celles-ci sont impossibles (dans le cas où une même somme est envoyée deux fois), seulement une des chaînes sera considérée comme valide. En théorie donc, si un utilisateur veut écrire plus vite que les autres, il doit rassembler 51% de la puissance de calcul du réseau.

Évidemment, plus il y a d'acteurs intéressés, plus vite ces équations seront résolues, car les machines utilisées seront de plus puissantes. Si on laisse les choses en l'état, les équations seront résolues dans des temps de plus en plus courts. C'est pour cela qu'on va utiliser la notion de difficulté pour que le temps pris soit plus ou moins constant. L'algorithme va augmenter la difficulté en obligeant les mineurs à trouver un hash avec des valeurs de plus en plus basses. Pour le bitcoin, l'idée est de maintenir une difficulté telle que l'on mine un bloc toutes les 10 minutes. Pour inciter des acteurs à miner ces blocs, processus énergivore et coûteux, on leur accorde une rétribution chaque fois qu'ils ont miné un bloc. Ainsi, pour le bitcoin, la récompense est de 12.5 BTC par bloc miné [3], soit environ 50 000$ aujourd'hui. Actuellement, le nombre très élevé d'acteurs sur le réseau, cumulés avec la puissance de calcul nécessaire pour espérer résoudre les hash,

3. `https://bitcoin.fr/minage/`

oblige les acteurs à se regrouper en s [4] pour répondre aux exigences du Proof Of Work. Par exemple, un utilisateur avec un EBIT E11++ [5] peut espérer miner 0.06 BTC par mois en moyenne(calculs réalisés avec le Bitcoin Mining Calcultator [6]). Rappelons que cet équipement coûte 1465 euros, et on imagine donc qu'avoir une probabilité de l'ordre de 6% d'obtenir un bitcoin par mois est un peu légère pour cet investissement.

4. Rassemblement de mineurs mettant en commun leur puissance de calcul afin de se partager les récompenses

5. `https://www.ebitminer.org/ebitminer-e9/EBIT-E11-44TH-S-with-PSU-shipping-on-March-31-2019-p1276`

6. `https://alloscomp.com/bitcoin/calculator`

3 Discussions autour de la blockchain

3.1 Technologie très lourde

Nous avons vu que pour être définie comme valable, une transaction doit pouvoir être vérifiée par tous les membres du réseau, et qu'il est prudent de laisser un peu de temps s'écouler pour s'assurer qu'elle soit considérée valide. Ce temps de vérification varie d'une implémentation à l'autre, mais dans tous les cas il est impossible de faire une transaction instantanée, ce qui rend ce système peu adapté aux achats du quotidien qui nécessitent d'être rapides. Ce problème pourra également être rencontré si on fait en sorte que les objets connectés communiquent entre eux : certes, ils n'auront plus besoin de passer par un tiers, mais ils ne pourront plus être aussi réactifs sans que des risques soient pris.

3.2 Impact des données émises malicieusement

Comme expliqué précédemment, une fois qu'une donnée est vérifiée par le réseau, celle-ci devient virtuellement gravée. Qu'en est-il si cette transaction a été réalisée de manière malicieuse, et à l'insu de la personne émettant la transaction ? Si un utilisateur mal intentionné arrive à faire valider des transactions, il est quasiment impossible de faire marche arrière sans un "hard-fork" qui vise à invalider les transactions faites à partir d'un moment donné.

3.3 Impact environnemental

L'impact en lui même de toute la blockchain est difficile à évaluer, car cela dépend du consensus utilisé. Le bitcoin, qui utilise le Proof Of Work, est régulièrement pointé du doigt. En effet, les noeuds du réseau sont en concurrence pour trouver le hash du précédent bloc, et seul un d'entre eux sera gagnant, ce qui implique que tous les autres ont miné pour rien. De plus, tous les noeuds vont ensuite faire des vérifications de leur côté pour voir si les transactions rajoutées sont légitimes. D'après cette publication de 2014, `http://karlodwyer.com/publications/pdf/bitcoin_KJOD_2014.pdf` la consommation d'énergie uniquement pour le Bitcoin était équivalente à celle d'Irlande. Aujourd'hui elle avoisine celle de l'Autriche, d'après `https://digiconomist.net/bitcoin-energy-consumption`

Il faut également prendre en compte les avantages que pourrait procurer la blockchain en général avec un algorithme plus adapté, comme le Proof of Stake qui nécessite beaucoup moins de calculs. De plus, la mise en place d'un système décentralisé pour l'IoT permettrait aux équipements d'échanger directement entre eux, et plus par l'intermédiaire d'un serveur centralisé, ce qui limiterait les échanges.

3.4 Une décentralisation discutable

Nous avons vu que l'un des principes de base de la blockchain est de s'assurer que le réseau ne soit pas dominé par un acteur en particulier. Cependant nous avons vu que les mineurs se retrouvent en pour mettre en commun leur puissance de calculs et ensuite se partager les gains. Pour le bitcoin, cette logique est poussée à un point qu'aucun acteur ne mine réellement seul, car les gains sont trop faibles. Le regroupement en fait que ces derniers se partagent l'essentiel de la cryptomonnaie en circulation, et on peut craindre

qu'ils agissent de manière concertée pour écrire des transactions frauduleuses et les faire valider.

Ainsi théoriquement, un qui détient 51% de la puissance de calcul peut écrire l'histoire plus vite qu'aucun de ses concurrents. Il faut nuancer cette affirmation de deux manières. Premièrement, un qui arrive à sécuriser 51% ou plus de la puissance de calcul n'a pas d'intérêt à saborder le réseau, sous peine de couler la valeur de la cryptomonnaie. Les autres acteurs constatant que des transactions frauduleuses sont publiées, ils n'utiliseront plus la cryptomonnaie et celle-ci perdra en valeur. Deuxièmement, le seuil des 51% est à relativiser. Cette affirmation implique que les deux groupes sur le réseau sont clairement définis et qu'ils travaillent ensemble. En réalité, si un groupe réunit un quart de la puissance, il est tout à fait envisageable que cela suffise à prendre le contrôle. Les 3 quarts restants peuvent ne pas être au courant, et travailler de manière non coordonnée. Le quart coordonné peut valider des transactions frauduleuses, qui ne peuvent être "contrées" par le reste du réseau à moins de se coordonner également.

4 Le protocole Ethereum

4.1 Objectifs

Ethereum est un protocole d'échanges décentralisés permettant la création par les utilisateurs des smart contracts grâce à un langage Turing-complet [7], Solidity . Ethereum utilise une unité de compte dénommée Ether comme moyen de paiement. Son sigle correspondant, utilisé par les plateformes d'échanges, est « ETH ». Cette plateforme offre la possibilité de créer un nouveau bloc toutes les 12 secondes [8] afin de l'ajouter à la chaîne existante.

4.2 Proof Of Stake

"Proof Of Stake" [9] (preuve d'enjeu) est un algorithme qui vise à servir d'alternative à "Proof Of Work". En effet, la preuve d'enjeu demande à l'utilisateur de prouver la possession d'une certaine quantité de cryptomonnaie afin de prétendre à pouvoir valider des blocs supplémentaires dans la chaîne. Une fois validé, il peut toucher la récompense. Cependant, afin d'éviter que la personne la plus riche ait en permanence un avantage, les algorithmes ont été affinés.

Le principe est le suivant : un noeud sera désigné par l'algorithme. Plus le noeud dispose de cryptomonnaie, plus il a de chance d'être élu. La "stake" désigne l'argent détenu. Pour avoir le droit de vérifier la transaction, le noeud doit être prêt à "geler" ses fonds. Le noeud n'est pas récompensé à la création du bloc, mais quand il vérifie la transaction. Il est donc rémunéré sur les frais de transactions. Ainsi, plus un noeud dispose de cryptomonnaie, plus il est puissant. Corollairement, il a de plus en plus d'intérêt à s'assurer que le réseau fonctionne, sous peine de quoi il perdra beaucoup.

4.2.1 Avantages

L'avantage le plus évident est lié à la consommation d'énergie. Quand les noeuds s'affrontent pour valider un bloc, et au final rendre inutile le travail de tous les autres noeuds, nous avons ici seulement un noeud qui va travailler à la vérification. Cela permet de limiter la course à la puissance, car ce n'est pas toujours le plus fort/riche qui gagne.

4.2.2 Inconvénients

Là où c'était le noeud le plus fort qui détenait le pouvoir, c'est désormais le noeud le plus riche qui en hérite. En effet, on retrouve le même risque de centralisation. Si un individu dispose de la majorité des fonds disponibles, alors c'est lui qui vérifiera la majeure partie des blocs.

Dans la version de base du PoS, on trouve le problème du Nothing At Stake. Si un agent est élu responsable de la validation d'un noeud alors qu'il n'a rien en jeu, il a tout intérêt à valider plusieurs versions possibles, car cela augmente ses chances de gagner et il n'a rien à perdre. Cela favorise le problème de la double dépense, où deux transactions qui ne peuvent avoir lieu en même temps sont validées.

7. Système formel ayant une puissance de calcul au moins équivalente à celle des machines de Turing
8. `https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/`
9. `https://www.ethereum-france.com/quest-ce-que-la-preuve-denjeu-proof-of-stake-faq-par-v-buterin-`

Ces problèmes sont adressés de manière différente par les cryptomonnaies qui les implémentent. Cela peut passer par la création de points de contrôle (qui empêchent la réorganisation passé un certain point). On peut aussi tempérer le PoS avec une fonction qui met en avant les utilisateurs n'ayant pas été choisis depuis un moment pour valider un bloc. On peut retrouver un panel plus exhaustif des algorithmes ici : `https://fr.wikipedia.org/wiki/Preuve_d%27enjeu#Options`

4.3 Smart contracts

4.3.1 Présentation

Les smart contracts, ou contrats intelligents, sont des programmes informatiques conçus pour exécuter les termes d'un contrat de façon automatique. Il est donc possible d'automatiser un échange sans que les parties n'aient besoin de se faire confiance et sans intervention d'un pouvoir central. Ainsi il est correct de dire qu'ils peuvent "modifier" l'état de la blockchain. A noter que ces contrats sont tout de même associés à un identifiant unique et qu'ils ne peuvent pas communiquer directement entre eux, ils doivent passer par les données stockées dans la blockchain.

4.3.2 Propriétés et contraintes

4.3.3 Propriétés

Les smart contracts sont atomiques, séquentiels et durables vis-à-vis des transactions. Concernant le code avec lequel ils sont écrits, il est durable et immuable. En effet, il est impossible de modifier un smart contract qui a été publié sur la blockchain. C'est pourquoi il est important que ce dernier soit suffisamment solide afin d'éviter tout problème qui pourrait être préjudiciable à la blockchain sur laquelle il a été déposé.

4.3.4 Contraintes

Cependant, comme toute technologie, il existe des contraintes à prendre en compte lors de l'écriture et la publication d'un smart contract. La première est que son exécution doit être déclenchée par quelqu'un de l'extérieur, il ne peut pas être déclenché automatiquement. La deuxième est l'impossibilité d'accéder à des données externes car, par exemple, il n'y a pas de web service. Ensuite, le temps d'exécution d'un smart contract est limité, ce qui peut poser problème en cas de traitement lourd à effectuer. Enfin, la dernière contrainte est le prix. En effet, "tout se paie" dans la blockchain. Il existe alors le principe de "l'exécuteur-payeur". En d'autres mots, la personne qui souhaite exécuter un smart contract va devoir payer son exécution.

4.4 Les oracles

Les oracles sont des smart contracts spécifiques qui ont pour objectif de fournir des informations du monde extérieur à la blockchain. En effet, comme mentionné précédemment le smart contract "classique" ne peut pas récupérer de données venant de l'extérieur.

Les oracles ont donc un rôle de "passerelle" entre la donnée externe et le smart contract stocké à l'intérieur de la blockchain.

4.5 Améliorations possibles d'Ethereum

Les évolutions majeures que pourrait connaître Ethereum seraient l'amélioration de la scalabilité, l'ajout d'un support de transactions privées, une sécurité accrue des smart contracts et de la confidentialité en général. A noter que certaines de ces évolutions ont déjà été annoncées par M. Buterin, co-fondateur de Ethereum pour fin de l'année 2018. De plus, selon ses dires, résoudre le problème de la scalabilité prendra encore minimum 2 ans :

> « I would say two to five, with early prototypes in one year. The various scaling solutions, including sharding, plasma and various state channel systems such as Raiden and Perun, are already quite well thought out, and development has already started. Raiden is the earliest, and its developer preview release is out already.» *Vitalik Buterin, (cofondateur de Ethereum) Septembre 2017*

4.6 The DAO et le problème de la persistance des blocs

L'exemple d'Etherum à ce niveau est particulièrement important : une fois qu'un smart contract est déployé, il ne peut être modifié. Il faut alors déployer un nouveau contrat. Il existe des possibilités pour "modifier" le contrat, mais cela nécessite de les avoir définis correctement, et en se préparant pour une éventuelle modification. (cf : `https://ethereum.stackexchange.com/questions/2404/upgradeable-smart-contracts`)

L'exemple le plus connu lié à cet inconvénient est l'incident de "The DAO". L'origine de cet incident réside dans un défaut de programmation, qui a permis à un utilisateur malicieux de "voler" 50 millions de dollars, mais peut-on parler de vol si le programme d'origine est mal défini ?). La communauté Etherum s'est ensuite concertée pour savoir comment répondre à ce dilemme : faut-il laisser les choses se faire, et assumer le statut de far-west d'Etherum, ou au contraire faire un "hard-fork" qui va à l'encontre des principes d'Etherum pour essayer de limiter les dégâts ? Après délibération la communauté à décider de faire un hard-fork : l'idée était de permettre de retourner à un état antérieur à l'incident pour que les personnes concernées retrouvent leurs Ethers investis, dérobés par l'attaquant. Les utilisateurs devaient choisir entre suivre la chaîne non altérée, où les Etherum étaient volés, ou alors rejoindre la chaîne nouvellement créée. Théoriquement, ils avaient le choix, mais rester sur la chaîne impactée par "The Incident" était lourd de conséquences. Les plateformes d'échanges majoritaires, comme Kraken, annoncent qu'elles ne suivraient pas les Etherum Classic, ce qui rend impossible la vente de cette monnaie sur ces plateformes. La fondation elle-même ne suit plus les Etherum Classic. Ainsi, seule une minorité a décidé de suivre la branche Etherum Classic. Ce sont les personnes pour qui le principe d'immutabilité compte le plus, et qui acceptent donc l'existence de ce vol tel quel.

C'est un problème extrêmement intéressant, qui permet de voir jusqu'où un système annoncé comme immuable et décentralisé l'est vraiment. Nous avons vu à travers cet exemple que rien n'est vraiment gravé dans le marbre. Mais alors comment définir clairement ce qui mérite un hardfork et ce qui ne le mérite pas ? The DAO a été hardfork principalement car il y avait énormément d'argent investi dedans. Mais cela implique que

le réseau n'est pas impartial, et que seules les erreurs des plus grandes structures peuvent être récupérées. Une fois que les institutions les plus puissantes ont choisi leurs camps, les autres acteurs du réseau n'avaient guère le choix que de suivre, sous peine de se retrouver sur une branche délaissée. C'est donc les acteurs les plus puissants qui centralisent le pouvoir. Ces réflexions nous amènent à nuancer les principes annoncés par la blockchain. Nous voyons qu'en réalité, ces principes ne peuvent être appliqués à la lettre.

5 Avenir et autres utilisations ?

Au travers des exemples du Bitcoin et d'Etherum, nous avons pu voir que la blockchain est, malgré ses défauts, particulièrement adaptée au concept des cryptomonnaies. Mais qu'en est-il des autres domaines d'application ?

5.1 La traçabilité alimentaire

De multiples scandales liés à la traçabilité alimentaire font régulièrement surface. Ce fut le cas de la fraude à la viande de cheval en 2013, où de la viande de cheval fut affichée comme de la viande de boeuf. Cela révéla notamment que toute la chaîne du commerce alimentaire européen était compromise, des abattoirs jusqu'aux négociants. Le détail de cette affaire est accessible sur `https://fr.wikipedia.org/wiki/Fraude_%C3%A0_la_viande_de_cheval_de_2013`

L'Europe n'est pas le seul territoire concerné : on peut citer aussi la Chine, où l'on faisait passer de la viande de rat pour de la viande de boeuf [10]. Se pose ainsi la problématique suivante : comment regagner la confiance du consommateur quand la chaîne du commerce est aussi opaque ? Toutes les certifications que l'on appose sur les produits (Bio par exemple) ne peuvent être vérifiées directement par les consommateurs. D'où l'initiative d'utiliser la blockchain pour l'industrie alimentaire. Cela permettrait de certifier toutes les étapes de la transformation alimentaires. Si la grande surface déclare avoir reçu la nourriture un tel jour, alors cette information sera confirmée par les autres membres du réseau. Appliquée à tous les échanges entre les parties impliquées, on aura un historique complet de tous les mouvements de la nourriture, et s'il y a manquement aux règles, le coupable ne pourra pas se défausser de ses responsabilités.

Dans la pratique, on aurait à chaque étape de la chaîne une saisie d'informations qui dépend du type d'aliments. Cela peut aller de la date de l'abattage, à celle d'ensachage. Une fois que le produit est passé par ces nombreuses étapes, et qu'il est en rayon, le consommateur pourra scanner un QR code sur le produit qui lui donnera accès aux différentes informations qui ont été saisies dans le processus.

Les principes de la blockchain, notamment traçabilité, immutabilité des informations, et décentralisation sont particulièrement attrayants. Actuellement, les traces des opérations sont maintenues par chacun des acteurs et ne sont pas mises en commun. Les parties prenantes ne se font pas confiance, et la recherche de la vérité devient particulièrement laborieuse quand il y a un cas d'intoxication alimentaire.

Avec une chaîne dont les acteurs se retrouvent sur la blockchain, on y gagnerait énormément. La recherche d'information serait plus rapide, car nous n'aurions pas à devoir parcourir les SI de chaque participant. Les différents acteurs seront incités à être honnêtes, car leurs actions seront beaucoup plus traçables. Les labels auraient plus de valeurs, car toute personne accédant à la blockchain pourra vérifier la véracité de ces propos.

5.2 L'industrie de la musique

L'industrie de la musique a plusieurs grands challenges à relever. D'une part, la rétribution extrêmement faible des auteurs. On parle en effet de 2% des revenus générés par

10. `https://www.lemonde.fr/asie-pacifique/article/2013/05/03/scandale-alimentaire-en-chine-des-plats-a-base-de-rat-ou-de-renard_3170501_3216.html`

un titre qui reviennent à l'auteur. Ceci est le résultat d'un modèle centralisé, où les plateformes de streaming ont beaucoup plus de pouvoirs que les artistes qui les alimentent. La gestion des droits est également difficile : une fois que l'on a un titre, il peut être difficile de retrouver les méta-données le concernant : quels sont les auteurs d'origines ? Avec quelle maison de disques étaient-ils liés ?

De par sa nature décentralisée, la blockchain adresse le problème de l'intermédiaire. Les fans pourront rétribuer directement les auteurs, sans avoir à passer par une plateforme tierce. Grâce à l'utilisation des smart contracts, les fans pourront accéder aux titres en streaming après avoir payé. La gestion des copyright se fera plus aisément : l'accès à tout l'historique de la création du titre jusqu'à sa diffusion restera gravé dans la blockchain.

On peut pousser le raisonnement des smart contracts encore plus loin. Les artistes pourraient mettre en place des smart contracts incitant les fans à partager leurs titres. Les 500 premières personnes qui partagent un lien sur Twitter pourraient avoir une réduction de 10% sur le prix du streaming pendant un mois.

On peut par exemple citer Musicoin ([11]) ou encore Mycelia ([12]). De multiples plateformes existent déjà, et leurs différences se retrouvent dans l'application qu'elles veulent faire de la blockchain. Certaines s'en servent pour payer immédiatement les artistes, d'autres pour retrouver les droits associés avec chaque titre. Il est possible de retrouver les grandes lignes des utilisations de la blockchain par plateforme sur `https://www.builtin.com/blockchain/blockchain-music-Innovation-examples`

5.3 Internet of Things

5.3.1 L'IoT en général

Certains pensent qu'utiliser la blockchain avec les objets connectés permettrait de conséquentes améliorations. On peut se représenter la blockchain comme la possibilité de garder trace de tous les échanges entre les différents objets. Ceci permettrait de couper l'intermédiaire nécessaire à la communication entre les objets connectés. Actuellement, si deux objets veulent communiquer ensemble, ils doivent d'abord passer par un serveur pour ensuite s'envoyer les messages. Avec une incorporation de la technologie blockchain, on peut imaginer que les appareils qui s'envoient des messages seront ensuite vérifiés par d'autres appareils. Cette hypothèse reste très optimiste. Nous avons vu préalablement que la consommation énergétique était très élevée, notamment pour l'algorithme "Proof Of Work". Comparé avec la puissance de la majorité des objets connectés, cela semble trop consommateur : en effet, on voit souvent que ce sont des capteurs, par conséquent très légers. On les imagine difficilement capables de calculer des hash complexes.

5.3.2 L'IoT au service d'une industrie

Nous allons prendre ici l'exemple de l'assurance. Nous allons étudier un cas concret, où la flexibilité des appareils de l'IoT est couplée avec la transparence et la sécurité de l'IoT, pour servir un secteur en particulier. L'idée est d'obtenir une politique d'assurance qui soit la plus proche possible des besoins de l'assuré, et donc éviter une politique d'assurance trop restrictive ou au contraire englobant des prestations non nécessaires. De plus, l'utilisation de la blockchain permet de garder trace de toutes les plaintes et autres documents déposés.

11. `https://musicoin.org/`
12. `http://myceliaformusic.org/`

L'IoT permet également de collecter des données (par exemple la vitesse du véhicule de l'assuré) qui serviront à appliquer des tarifs différents et plus adaptés pour l'assuré. Les données recueillies pourront servir à alimenter les smart contracts mis en places entre les différents partis. Par exemple, un agriculteur qui a souscrit une assurance (traduite par un smart contract) stipulant qu'il touchera 10 000$ si il y a 100 jours de sécheresse de suite touchera automatiquement sa prime, sans devoir manuellement remplir un dossier.

Dans cet exemple, la température est une donnée librement accessible, et ne nécessite par conséquent pas l'utilisation d'objets connectés. Mais si on prenait par exemple comme condition la vitesse moyenne d'une voiture, alors une sonde dans le véhicule pourrait communiquer avec le smart contract pour décider ou non si la prime doit être versée.

Il nous paraît important de nuancer cet exemple, notamment en précisant que le plus grand bénéficiaire de cette association est l'assureur lui même. En effet, c'est lui qui va disposer de toutes les données émises par ces assurés, et il sera donc en mesure de déterminer les différents profils qui coûtent le plus cher. Bien évidemment, l'assureur mettra en avant les bénéfices pour l'assuré, en montrant que disposer de plus d'informations sur lui permet de définir un profil plus "adapté".

5.4 Quels enseignements en tirer ?

A travers ces exemples, nous pouvons voir quelles tendances poussent les industries vers la blockchain.

5.4.1 La traçabilité

L'idée d'avoir un historique fiable et particulièrement important, notamment dans le cas où le produit fini passe par une succession d'acteurs avant d'être délivré. Si chacun des acteurs est impliqué dans la blockchain on peut avoir un historique facilement accessible et non modifiable. C'est particulièrement attrayant dans les domaines où il y a de lourdes formalités administratives, et où des acteurs peuvent avoir intérêt à être malhonnêtes.

5.4.2 Décentralisation

Dans le même état d'esprit que pour le point précédent, le fait d'avoir un réseau décentralisé permet à des acteurs de se faire confiance sans avoir à se baser sur un organisme central, qui concentre alors beaucoup de pouvoir. Le fait que le réseau est alimenté par tout le monde oblige les acteurs à se faire confiance et est censé empêcher quelqu'un de fausser les informations. La décentralisation permet aussi de limiter les coûts : les échanges pourront se faire directement entre acteurs concernés, et pas en faisant des aller-retour avec le service censé centraliser le tout.

5.4.3 Automatisation de tâches répétitives

Nous avons pu voir à quel point les smart contracts, particulièrement ceux proposés par Etherum peuvent permettre d'automatiser des tâches. Grâce à des objets connectés notamment, il est possible de déclencher des opérations grâce aux smart contracts sans avoir besoin d'un humain. Toute activité nécessitant la vérification par un être humain peut maintenant être automatisée par des smart contracts qui se baseront sur des sources de confiance.

5.4.4 Légèreté des données et vitesse des transactions

Pour garantir l'intégrité des données mise sur la blockchain, il faut que les noeuds aient le temps de vérifier les transactions publiées. Cela ne pose pas de problème pour les activités que l'on a cité, car la réactivité n'est pas demandée à la seconde près. De plus, les données mises en ligne doivent rester légères, car nous avons vu que le coût pour mettre des données en ligne est très coûteux. On imagine ainsi que mettre en ligne des documents ou des mp3 est réalisable, mais un système de streaming de jeux semble bien trop volumineux.

6 Analyse technique

La seconde partie de ce projet, la partie applicative aura pour objectif de concevoir et implémenter une blockchain.

L'utilisation d'un langage objet semble être adéquat à cette problématique. En effet nous pouvons ainsi représenter chaque grande entité comme une classe.

6.1 Diagramme de classe

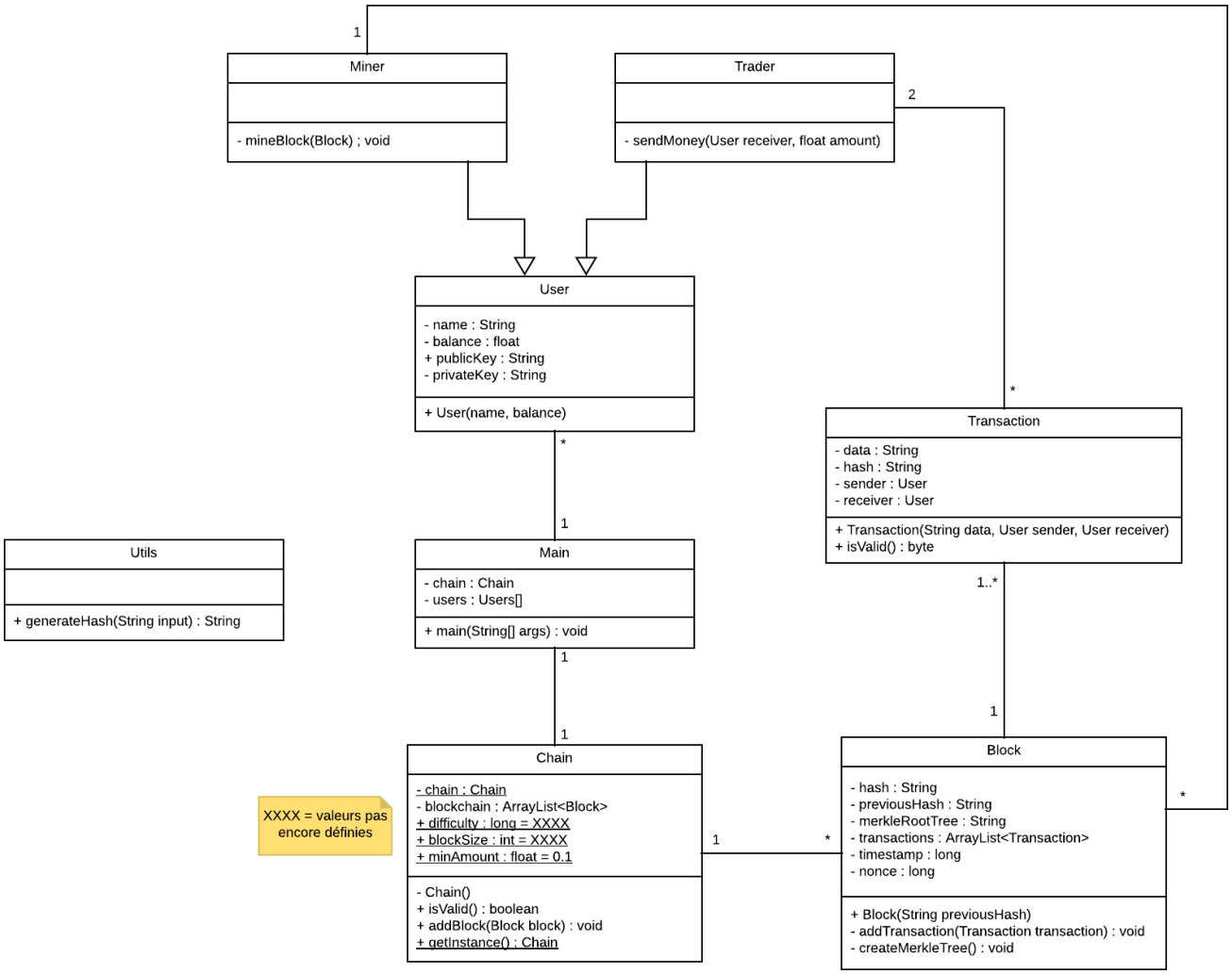

FIGURE 5 – Diagramme de classe (version 1)

A noter que la classe "Chain" est construite sur le modèle du Singleton afin de s'assurer qu'une seule instance de blockchain n'est utilisée.

6.2 Utilisation des threads et rôles des utilisateurs

Afin de simuler chacun des acteurs sur notre blockchain, nous souhaitons modéliser tous les acteurs par des threads. Ceci permet de simuler le comportement non coordonné des différents acteurs. Nous avons vu que même si les différents acteurs avaient la possibilité de miner et faire des transactions, des profils d'utilisateurs se dégagent. Les premiers sont ceux qui se servent du blockchain comme d'un moyen de transaction, et ils vont donc uniquement essayer de s'échanger de la cryptomonnaie. Nous souhaitons enlever à ces derniers la possibilité de miner ces blocs, et de laisser ce travail aux mineurs, censés avoir des machines plus puissantes. Les seconds sont donc les mineurs. Ce sont eux qui vont vérifier les transactions émises par les premiers, afin de créer des blocs qui seront gravés dans la chaîne. Ces profils ne sont dans notre exemple pas intéressés par la création de transactions et ne vont donc pas essayer d'en créer. Ainsi, on peut imaginer par exemple une micro blockchain de 5 utilisateurs : 2 individus qui font des transactions entre eux, et les 3 derniers sont des mineurs qui vont être en concurrence pour vérifier les transactions entre eux. On imagine très bien qu'il peut y avoir des profils plus complexes d'utilisateurs, et notamment des utilisateurs malicieux. Pour le début, nous allons cependant nous centrer sur ces différents acteurs, avant d'éventuellement incorporer des rôles plus complexes. Selon l'avancement de notre projet, nous pouvons réfléchir à une blockchain hybride, qui permet à des utilisateurs de consulter la blockchain sans écrire dedans. Nous préférons pour le moment nous concentrer sur une base solide avant d'inclure d'autres fonctionnalités.

7 Conclusion

Cela fait quelques années que les cryptomonnaies ont le vent en poupe. A tel point que des géants du numérique comme Opéra, ont décidé d'intégrer un porte-monnaie virtuel à leur navigateur afin de permettre au développeur de créer des applications sur Ethereum sans avoir besoin de s'appuyer sur un portefeuille extérieur. C'est en partie grâce à cette popularité des monnaies virtuelles que la blockchain s'est fait connaître du grand public.

Même si dernièrement les cryptomonnaies connaissent une période assez difficile, ce n'est pas le cas de la technologique blockchain. En effet, de plus en plus d'entreprises l'utilisent et expérimentent des nombreux développements dessus. Par exemple, Deloitte Luxembourg a ouvert un pôle d'expertise Blockchain. Le géant français de la télécommunication, Orange, se lance dans la blockchain avec un système de vote en ligne afin d'y stocker la preuve de vote. Facebook souhaite de son côté élargir son équipe "Blockchain". De plus, d'autres éléments prouvent que la blockchain est en plein essor, comme le fait que l'emploi "Développeur Blockchain" est celui qui connaît la croissance la plus rapide sur ces 4 dernières années [13], presque trois fois plus que l'ingénieur en machine learning.

De nouveaux types de blockchain voit notamment le jour comme les blockchain privées ou hybrides. Les blockchain privées ne seraient accessibles qu'aux personnes disposant des droits d'accès. Tandis que sur les blockchain hybrides tout le monde aurait un droit de consultation, mais pas un droit d'écriture. On peut également parler de blockchain de "consortium". En effet, le processus de validation d'un bloc est contrôlé par un nombre restreint et choisi à l'avance de noeud. Il s'agit alors d'un changement significatif par rapport au modèle originel car les intervenants seraient sélectionnés et limités. On peut par exemple imaginer une blockchain hybride mise en place par des organismes financiers, où seulement un nombre prédéfini d'organismes seraient chargés d'approuver ou non les blocs.

Tout cela peut laisser penser que cette nouvelle technologie risque de bouleverser le monde numérique actuel.

13. https://www.developpez.com/actu/237551/Le-developpeur-Blockchain-est-l-emploi-qui-connait-la-cr