Désassemblons le numérique #Episode6 – Enfiler des blocs à la chaîne

Bonjour à toutes et à tous, et bienvenue dans ce nouvel épisode de *Désassemblons le numérique* ! Aujourd'hui, nous accueillons Damien Robert, chercheur au sein de l'équipe-projet LFANT du Centre Inria de l'université de Bordeaux pour nous parler de la *blockchain*, la technologie derrière la cryptomonnaie *Bitcoin*. Bonjour Damien !

Damien Robert : Bonjour.

Merci de nous accompagner dans cet épisode ! Pour commencer, est-ce que tu pourrais nous rappeler comment le système bancaire fonctionne aujourd'hui ?

DR : Actuellement, le système bancaire est centralisé, c'est-à-dire que ce sont les banques qui stockent le registre contenant l'historique de toutes les transactions. C'est grâce à ce registre que l'on peut déduire le solde de tous les comptes. Les banques s'occupent aussi de vérifier l'identité de la personne qui réalise une transaction avant de l'ajouter au registre, par exemple par son code de carte bleue. Mais un tel système exige de faire confiance aux personnes qui sont responsables du registre. Il faut aussi anticiper les pannes qui pourraient altérer les fichiers et les protéger des attaques.

Quelles différences y-a-t-il avec un système de transaction comme *Bitcoin* alors ?

DR : L'objectif de *Bitcoin* et de toutes les cryptomonnaies, c'est de proposer un système de transaction décentralisé. Plutôt que d'avoir un seul registre centralisé, *Bitcoin* est organisé en un réseau où chaque personne peut devenir validateur et disposer d'une copie du registre. Donc tout le monde peut posséder un historique complet de tous les échanges. Ensuite, quand quelqu'un souhaite faire une transaction, il va informer l'ensemble du réseau pour que toutes les personnes qui possèdent une copie du registre soient au courant. Chaque personne doit alors vérifier le solde et l'identité de celui qui fait la transaction. Pour vérifier le solde, c'est facile, il suffit de reprendre l'historique des transactions inscrites dans sa copie du registre. Pour vérifier l'identité, il faut que celui qui fait la transaction y appose une signature. C'est un outil cryptographique qui a trois propriétés. Premièrement, elle permet de garantir l'identité de celui qui fait la transaction. Deuxièmement, elle empêche les modifications de la transaction après qu'elle ait été validée. Et enfin elle empêche celui qui fait la transaction de se rétracter. Après ces vérifications, chaque propriétaire d'une copie du registre décide librement d'ajouter ou non la transaction à leur copie.

Mais alors, il peut y avoir des désaccords sur les transactions à inclure ou non et donc un risque que les copies du registre divergent. Qu'est-ce qu'il faut faire pour maintenir la cohérence entre les copies ?

DR : C'est justement le problème de la synchronisation des registres qui est difficile. En théorie, il ne faudrait prendre en compte que les transactions considérées comme valides par la majorité des personnes disposant d'une copie du registre. Pour ça, il faudrait vérifier toutes les copies du registre à chaque transaction pour connaitre la version majoritaire. En pratique, ça semble insoutenable. Pour *Bitcoin*, il y a 50 000 validateurs et donc autant de copies à vérifier, chacune faisant une taille considérable à cause du très grand nombre de transactions déjà réalisées, de l'ordre de plusieurs centaines de giga-octets par copie. Il faut alors utiliser des fonctions de hachage. C'est un outil mathématique qui va transformer n'importe quel paquet de données en une chaîne de caractères de courte longueur fixe, appelée haché. L'intérêt, c'est qu'une toute petite modification dans le paquet de données entrainera un haché complètement différent. Chaque copie du registre peut alors être hachée en une courte chaîne de caractères garantissant son intégrité, ce qui est beaucoup plus rapide à vérifier que l'intégralité de la copie. Au final, pour trouver la version majoritaire du registre parmi toutes les copies, il suffit de trouver le haché le plus fréquent. C'est cette version majoritaire qui est considérée comme la bonne et sur laquelle toutes les copies doivent s'aligner.

Bitcoin repose aussi sur la technologie de la *blockchain.* Qu'est-ce que c'est exactement ?

DR : C'est là que la solution devient astucieuse ! La *blockchain* organise les transactions différemment. Plutôt que d'avoir un seul gros registre qui liste toutes les transactions dans l'ordre chronologique, il est découpé en plusieurs morceaux, qui sont appelés des blocs et qui contiennent chacun à peu près le même nombre de transactions. Ensuite, ces blocs sont reliés les uns aux autres chronologiquement grâce à une fonction de hachage. En fait, chaque bloc contient le haché du bloc précédent. Donc quand un bloc est synthétisé par une fonction de hachage, cette dernière prend en compte tout son contenu y compris le haché du bloc précédent. Autrement dit, le haché d'un bloc dépend des transactions qu'il contient mais aussi du haché des blocs précédents. Donc si un bloc est modifié, son haché change, ce qui change aussi le contenu du bloc suivant et donc son haché à lui et ainsi de suite. C'est ça la *blockchain*. Grâce à ça, plutôt que d'ajouter les transactions une à une, ce sont des blocs de transactions qui sont rajoutés aux copies de la *blockchain*. L'avantage c'est qu'il n'y a plus besoin de hacher l'intégralité des copies du registre à chaque nouvelle transaction, mais seulement le nouveau bloc.

Et d'un point de vue sécurité, est-ce qu'il serait possible de faire inscrire des transactions frauduleuses ?

DR : Jusqu'ici, nous avons supposé que seules les transactions ajoutées à une majorité des copies étaient réellement prises en compte. Pour la *blockchain*, nous pourrions faire la même chose avec les blocs, c'est-à-dire de ne rajouter que ceux proposés par la majorité des copies. Mais, comme le système est décentralisé, si une seule personne crée suffisamment de copies pour que cela représente plus de la moitié de toutes les autres copies du réseau, alors elle peut ajouter les blocs qu'elle veut car elle détient la majorité des copies. C'est le problème Sybil. Pour contrer ça, il faudrait

par exemple authentifier chaque validateur mais le système ne serait alors plus complètement décentralisé. Le créateur du *Bitcoin* a eu une autre idée. Il a inventé la preuve de travail. Dans ce cas, il faut réaliser un calcul très lourd pour créer et proposer un bloc valide. La première personne qui y arrive peut alors proposer son bloc qui est ajouté à toutes les copies du réseau. Le système marche car tout le monde peut vérifier efficacement que le travail a bien été effectué. Pour inciter les gens à faire ce travail, ils sont rémunérés à chaque bloc créé, avec des *bitcoins* générés *ex nihilo*. C'est pour ça que ces personnes sont souvent appelées des mineurs, par analogie avec les mineurs de diamants. Maintenant, si quelqu'un souhaite prendre le contrôle de toute la chaîne, il faudrait qu'il réussisse le calcul difficile avant tout le monde à chaque nouveau bloc. Il faudrait donc que cette personne dispose de moyens de calcul plus puissants que l'ensemble des ordinateurs de toutes les personnes du réseau pour être sûr de gagner à chaque fois. C'est une situation qui semble très improbable.

Quels inconvénients y-a-t-il avec la preuve de travail ?

DR : Le premier inconvénient est son inefficacité. Pour *Bitcoin*, la difficulté du calcul est réajustée en permanence pour qu'un bloc soit ajouté toutes les 10 minutes environ. Comme chaque bloc contient environ 2048 transactions, ça ne fait que 3,4 transactions par seconde. Pour comparer, en France, le système derrière les cartes bleues permet de réaliser 400 transactions par seconde. *Bitcoin* est donc beaucoup plus lent. Et pour des raisons plus techniques, il faut en général attendre la création de 6 blocs après l'émission d'une transaction pour être sûr de sa réalisation, ce qui fait une heure d'attente. C'est énorme !

On entend aussi beaucoup parler du problème énergétique de *Bitcoin*. Qu'en est-il ?

DR : C'est le principal problème à mon sens. Tous les mineurs sont en compétition et augmentent constamment leur vitesse de calcul, qui est proportionnelle à la consommation d'énergie. Aujourd'hui, la consommation électrique du réseau *Bitcoin* est équivalente à celle d'un pays comme la Finlande qui aurait besoin d'une puissance de 5 000 à 15 000 MW. Et du point de vue de la quantité de données générées, pour ajouter un seul octet dans la *blockchain*, il faut dépenser la même énergie que pour faire bouillir entre 10 à 30 litres d'eau à 90°C. Il s'agit donc d'un gâchis énergétique qui est inéluctable face au succès de *Bitcoin*. Un système de preuve de travail à l'échelle mondiale doit consommer une énergie importante pour résister aux attaques.

Malgré ces problèmes, est-ce que la technologie de la *blockchain* peut avoir d'autres applications que la gestion des transactions ?

DR : Tout à fait ! En réalité, la *blockchain* est une base de données distribuée dont le contenu est infalsifiable. C'est donc possible de mettre autre chose que des transactions. Par exemple, des plates-formes de vente en ligne peuvent utiliser une *blockchain* pour suivre le trajet des colis. S'il y a un problème avec une livraison, c'est facile de retrouver rapidement d'où vient le problème puisque la *blockchain* conserve toutes les informations. Il est aussi possible d'imaginer un système universitaire où les diplômes sont enregistrés dans une *blockchain*. Les étudiants pourraient alors certifier l'authenticité de leurs diplômes auprès des recruteurs.

Comment toi et l'équipe-projet LFANT êtes-vous impliqués dans le développement de cette technologie ?

DR : La preuve de travail est une solution intéressante mais qui a beaucoup de défauts. Aujourd'hui, les objectifs sont d'améliorer le coût énergétique et la vitesse de transaction des *blockchains*, par exemple avec la preuve d'enjeu. Avec LFANT, nous sommes en train de travailler sur de nouveaux outils mathématiques pour développer ces nouveaux outils cryptographiques qui y répondent. Nous cherchons également à contrer de potentielles futures menaces comme l'apparition d'ordinateurs quantiques.

De beaux défis en perspective ! Merci beaucoup Damien pour toutes ces explications sur la *blockchain*. Et merci à vous de nous avoir écoutés. À très bientôt pour le prochain épisode de *Désassemblons le numérique* !