La blockchain est-elle une technologie de confiance

Maryline Laurent

La Blockchain est-elle une technologie de confiance ?

Maryline Laurent, professeur à Télécom SudParis, SAMOVAR, CNRS, Télécom SudParis, CNRS, Université Paris-Saclay

Cette fiche présente le fonctionnement et les limites du trust by design sur l'exemple de la blockchain.

La Blockchain est une technologie inventée à la fin des années 2000. C'est le projet Bitcoin d'échange de crypto-monnaie (des Bitcoins) sur Internet qui en est à l'origine, qui l'a rendue populaire et qui a permis de démontrer sa grande fiabilité. En 2014, la fondation à but non lucratif Ethereum dirigée par Vitalik Buterin se lance dans le projet d'étendre le principe de la Blockchain à une Blockchain programmable, ouvrant ainsi le champ à tout type de transactions (smart contracts) et à pléthore de nouveaux services. Avec la première version du code source d'Ethereum mise à la disposition du grand public en 2015, de nombreux industriels et développeurs indépendants se lancent alors dans la course pour proposer de nouvelles innovations.

La Blockchain est souvent comparée à un gros livre de comptes publiquement accessibles et auditables. Ses membres peuvent y ajouter des écritures, mais cette opération nécessite une validation par plusieurs membres du groupe, voire la majorité du groupe. Les membres agissent sous pseudonymat, ce qui permet de tracer les écritures de chacun, sans connaitre pour autant leur identité réelle.

Après l'introduction de quelques techniques élémentaires utiles à la compréhension, cette fiche présente le fonctionnement technique de la Blockchain. Puis, elle identifie les propriétés clés qui permettent de lui conférer un certain degré de confiance. Enfin, elle dresse un état des lieux des risques et limites associés à la Blockchain et discute de la capacité de la Blockchain à garantir la protection des données personnelles.

La difficulté de l'exercice est de distinguer ce qui relève du concept propre à la Blockchain, des différentes instanciations qui en ont été faites par les projets Bitcoin, Ethereum, mais aussi Ripple, Litecoin... Notons que les explications fournies ont principalement trait au projet Bitcoin pour lequel existe une littérature beaucoup plus fournie et stable.

3.1. Eléments techniques utiles à la compréhension

La sécurité de la Blockchain repose sur des mécanismes cryptographiques standards relevant essentiellement de la cryptographie à clés publiques et des fonctions de hachage dont nous fournissons une description simplifiée ci-dessous.

Par définition, la cryptographie à clés publiques suppose que chaque entité du système dispose de deux clés, une **clé publique** connue de tous et une **clé privée** maintenue secrète par son entité propriétaire. C'est cette clé privée qui permet à une entité de signer une demande de transaction et donc de prouver qu'elle en est à l'origine. La clé publique permet à une autre entité du système de vérifier l'authenticité de la signature. Le niveau de sécurité d'un cryptosystème se mesure à la difficulté de craquer ses clés privées. Dans un cryptosystème, la taille des paramètres influe directement sur le niveau de sécurité obtenu, avec pour règle que plus leur taille est grande, plus il est difficile d'en craquer la clé privée. Avec du matériel informatique de moins en moins cher et offrant de plus en plus de puissance de calculs et de mémoire, il est nécessaire de réviser régulièrement à la hausse la taille des paramètres choisis, pour maintenir le niveau de difficulté. Notons qu'aujourd'hui, un niveau de sécurité 112 est jugé suffisant, ce qui correspond à un attaquant à qui on confère la capacité de réaliser 2^{112} opérations pour réaliser une attaque.

Dans le projet Bitcoin, c'est le cryptosystème ECC (Elliptic Curve Cryptography) qui a été retenu, avec l'algorithme de signatures ECDSA (Elliptic Curve Digital Signature Algorithm). Il s'appuie sur les courbes elliptiques qui ont l'avantage de garantir, pour un même niveau de sécurité, des tailles de clés raisonnables par rapport à d'autres cryptosystèmes à clés publiques plus classiques tels que le RSA. En effet, pour un niveau de sécurité 112, là où le RSA exige des clés de 3072 bits, ECC exige seulement 256 bits.

Les signatures électroniques permettent de garantir l'authenticité de chacune des transactions injectées dans une Blockchain. Techniquement, la génération d'une signature suppose, pour le signataire, de commencer par appliquer une fonction de hachage (cf. ci-dessous) sur les éléments de la transaction à authentifier, puis de chiffrer le résultat obtenu avec sa clé privée.

Les fonctions de hachage (Hash) sont très présentes dans les Blockchains, en particulier la fonction SHA256 (cf. encadré). Elles servent aussi bien à générer des signatures pour authentifier chaque transaction, à garantir un lien fort entre un membre de la Blockchain et sa clé publique, à identifier une transaction ou un bloc, et à lier les blocs (resp. transactions) de la Blockchain entre eux de manière à rigidifier l'enchaînement des blocs (resp. transactions) et à garantir au final l'intégrité de la Blockchain.

Propriétés d'une fonction de hachage (Hash) cryptographique :

- Production d'un résultat (ou haché) de taille fixe : Quel que soit le message fourni en entrée, la fonction retourne toujours un résultat de même taille. L'algorithme SHA256 retourne un haché sur 256 bits.
- Irréversibilité : Connaissant le résultat de la fonction, il est très difficile de trouver le message fourni en entrée.
- Résistance aux collisions : Il est très difficile de trouver deux messages qui aboutissent au même haché.
- Effet avalanche : La modification d'un bit du message en entrée aboutit à au moins la moitié des bits modifiés en sortie. Cette propriété est intéressante pour garantir la propriété d'intégrité.

Pour les propriétés d'irréversibilité et de résistance aux collisions, « très difficile » signifie que les outils algorithmiques et informatiques actuels ne le permettent pas en un temps raisonnable.

3.2. Fonctionnement de la Blockchain

D'un point de vue technique, les membres de la Blockchain sont des ressources informatiques (par ex. des ordinateurs) qui sont préalablement connectées à la Blockchain, suite à une phase d'enrôlement. Ces ressources sont couramment appelées des **nœuds** du fait qu'elles sont mises en réseau au travers d'Internet.

Deux types de nœuds coexistent :

- les **nœuds réguliers**, la plupart dotés de capacités informatiques ordinaires, à partir desquels des personnes physiques peuvent émettre des demandes de transactions ;
- les **nœuds « miners » ou mineurs**, dotés de grosses capacités de traitement, directement utiles au fonctionnement de la Blockchain et capables d'émettre des transactions au même titre qu'un nœud régulier.

Les nœuds, qu'ils soient réguliers ou mineurs, pour peu qu'ils disposent de grosses capacités de stockage, peuvent stocker toute la Blockchain. Ils sont appelés « full node ». Notons que la Blockchain Bitcoin lancée en 2009 atteint en 2016 plus de 80GB.
Dans la suite, quand il sera fait mention d'un nœud sans plus de précision, il s'agira d'un nœud régulier ou d'un mineur.

3.2.1. La phase d'enrôlement dans la Blockchain

Pour participer aux activités d'une Blockchain, une personne doit enrôler un de ses équipements informatiques comme nœud de la Blockchain. Au cours de cette opération, le nœud, qu'il soit régulier ou mineur, télécharge un logiciel qui lui permet de s'interfacer avec la Blockchain. Ce logiciel est personnalisé avec un numéro de

compte Blockchain (ex : adresse Bitcoin de 160 bits) et un jeu de clés publique et privée. Il est impératif que le propriétaire du nœud conserve précieusement le logiciel téléchargé et le mot de passe lui permettant de déverrouiller la clé privée, sinon il perdra l'accès à son compte Blockchain et ne pourra plus passer aucune transaction sur ce compte.

Il doit exister un lien évident et facilement vérifiable entre le numéro de compte et la clé publique. Classiquement comme c'est le cas pour Bitcoin, l'adresse Bitcoin correspond au résultat du hachage de la clé publique associée. Cela permet à tout nœud de vérifier la cohérence entre la propriété d'un compte et la signature d'une transaction qu'il est supposé avoir émise. Cette astuce permet d'éviter de recourir à une infrastructure de gestion de clés où la gestion des certificats électroniques est particulièrement lourde et coûteuse.

3.2.2. La phase de transaction

Une Blockchain est un ensemble de transactions individuelles qui sont regroupées en blocs, chaque bloc contenant les transactions émises depuis le dernier bloc (environ toutes les 10 minutes pour Bitcoin). Chaque transaction est émise par un nœud qui la diffuse à tous les membres de la Blockchain. Les nœuds qui stockent la Blockchain vérifient l'authenticité et la légitimité de chaque transaction en se référant à l'historique des transactions enregistrées depuis l'origine dans la Blockchain, puis ce sont les mineurs qui agglomèrent sous forme d'un bloc les transactions valides et tentent de valider le bloc par la résolution d'un problème mathématique complexe appelé Proof of Work (PoW) décrit à la section 3.2.5[1]. Ce travail de résolution de problème s'appelle « minage ». Le mineur qui a terminé le minage en premier diffuse sa solution à tous les nœuds qui vérifient la preuve PoW associée. En cas de validité avérée, chaque nœud ajoute le bloc dans la Blockchain et les mineurs commencent à miner le bloc suivant. Le fait d'inscrire massivement un bloc dans la Blockchain signifie qu'un consensus a été atteint parmi les nœuds.

Dans le cas où deux mineurs résolvent simultanément le PoW, les autres nœuds reçoivent alors deux blocs différents valides, correspondant au même maillon de la chaîne. Les deux blocs sont ajoutés à la chaîne au même niveau, ce qui crée un effet de fourche démarrant deux chaînes distinctes. Ce problème de dédoublement de la Blockchain s'autorégule, tout simplement par le fait que la Blockchain de plus longue taille est considérée valide. Pour Bitcoin, il est admis qu'au bout de 100 blocs ajoutés à la Blockchain, le problème de dédoublement est résolu. Bien entendu, cela suppose que l'ensemble des transactions de la Blockchain invalidées soient incorporées dans la Blockchain valide. De ce fait, une transaction de type Bitcoin est considérée effectivement passée à la condition qu'elle soit « enterrée » sous 6 blocs, ce qui

[1] Le procédé de validation par Proof of Stake radicalement différent du PoW, est expliqué à la section 3.2.6.

nécessite d'attendre 1h avant que le bénéficiaire ne puisse disposer de ses Bitcoins et réaliser lui-même une transaction. Cette condition est un frein très fort à l'utilisation des Blockchains dans un environnement dynamique, ce qui amène les chercheurs à s'intéresser à des alternatives comme le Proof of Stake (cf. section 3.2.6).

3.2.3. Qu'est ce qu'une transaction ?

Une transaction est toujours émise à la demande d'un nœud avec pour objectif d'être ajoutée à la Blockchain. Chaque Blockchain impose d'une part un cadre strict et donne d'autre part une certaine latitude au nœud émetteur pour préciser les conditions à satisfaire pour que la transaction soit effective. Pour le projet Bitcoin qui vise à dépenser des Bitcoins, la règle implicite consiste à vérifier qu'un nœud dispose de Bitcoins en suffisance pour émettre la transaction, et le nœud émetteur quant à lui peut imposer, sous forme d'un programme écrit en script, ses propres conditions comme la condition que le bénéficiaire prouve son identité en émettant une signature valide ou que plusieurs signataires soient nécessaires pour émettre une nouvelle transaction. Pour Ethereum, c'est aux développeurs de Smart contracts de fixer l'ensemble des règles. Un exemple de transaction ou smart contract pour Ethereum serait de déclencher un virement (en crypto-monnaies) à la réception d'un colis, ou bien l'ouverture d'une porte (véhicule, location de maison…) après prépaiement du service…

Une transaction doit nécessairement contenir :

- un identifiant de transaction, ce qui permet plus tard de pointer vers cette transaction ;
- toute information utile permettant de valider la légitimité de la transaction ou plus largement de situer le contexte de la transaction. Le projet Bitcoin fait référence à des inputs (cf. Figure 1) qui permettent à l'émetteur Bertrand d'identifier plusieurs transactions antérieures (celles d'Anne et Alice) pour justifier d'un solde suffisant, et de prouver qu'il satisfait bien les conditions d'Anne et Alice pour en être bénéficiaire (clé publique et signature) ;
- toute information utile permettant de formaliser le résultat de la transaction. Le projet Bitcoin (cf. Figure 1) définit des outputs qui précisent les bénéficiaires du virement (Charles et Zoé), le montant associé, et les conditions que les bénéficiaires doivent satisfaire pour prétendre récupérer le montant. A la manière d'un livre de compte, l'équilibre peut être atteint entre inputs et outputs, mais si le montant en output est moins élevé qu'en input, cela signifie que le mineur peut bénéficier de la différence pour son travail de minage. Notons que les frais de transaction sont parfois obligatoires et que le montant alloué permet d'inciter les mineurs à intégrer la transaction dans leur opération de minage.

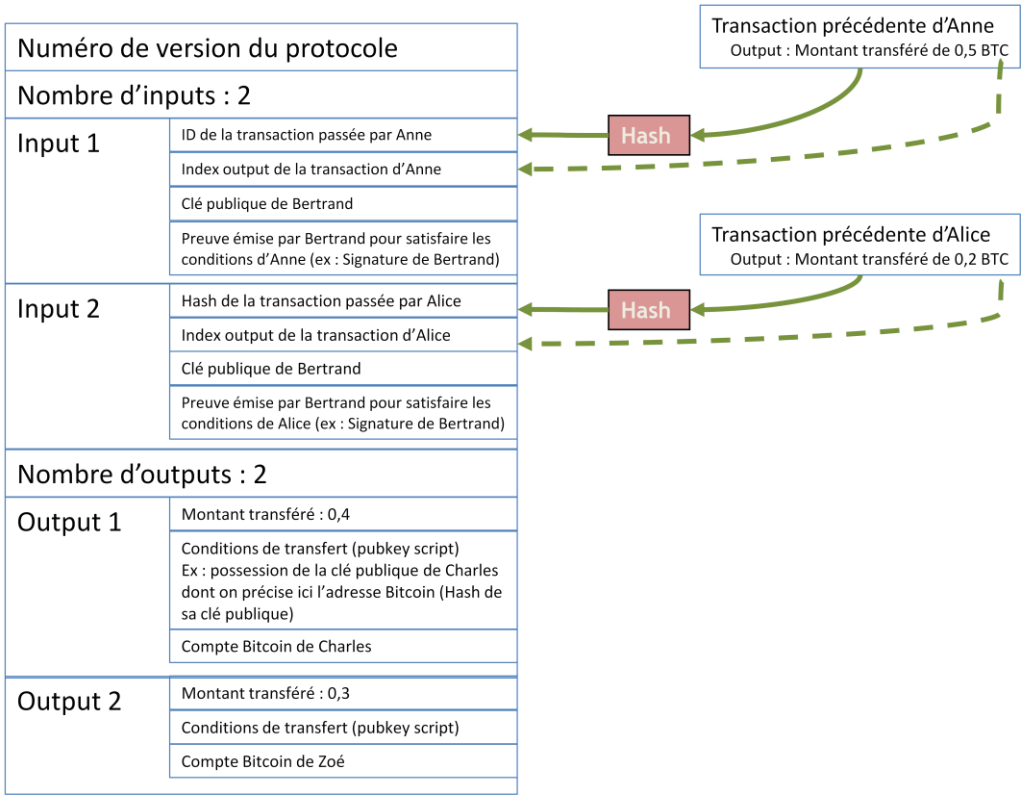

Figure 1 : Format simplifié d'une transaction Bitcoin

3.2.4. Qu'est ce qu'un bloc ?

Un bloc regroupe un ensemble de transactions et vise à cristalliser le contenu des transactions et du bloc, et la position du bloc dans la Blockchain de manière à rendre impossible toute modification accidentelle ou malveillante du contenu de la Blockchain. Cette cristallisation repose sur deux procédés essentiels complémentaires. Tout d'abord, les fonctions de hachage utilisées intensivement et parfois organisées pour produire un arbre de Merkle permettent de rigidifier la structure de transactions et de blocs en venant souder tous ces éléments entre eux. Les fonctions de hachage empêchent de modifier partiellement un bloc de la chaîne, mais n'éliminent pas les actes d'écrasement éventuel des derniers blocs. Ce sont les mécanismes de minage couplés à l'architecture décentralisée de stockage et de calculs qui garantissent un certain niveau de confiance. Tous les éléments apportant structurellement et fonctionnellement de la confiance sont présentés à la section 4.

Comme le présente la figure 2 pour le projet Bitcoin, un bloc est composé d'un entête incluant une signalétique utile au fonctionnement de la Blockchain et un contenu dans lequel les transactions sont regroupées. L'entête comprend un nonce, c'est-à-dire un nombre aléatoire utile à l'opération de minage (cf. section 3.2.5) et d'autres éléments explicités ci-dessous.

Pour chaque transaction se trouve calculé un identifiant (TxID) qui est le haché du contenu de la transaction. L'arbre de Merkle permet ensuite de solidifier l'ensemble des transactions par calcul de hashs successifs, et ce jusqu'à trouver la racine de l'arbre. Le résultat est alors renseigné dans l'entête du bloc (bloc 2 de la figure 2), ce qui a l'avantage de lier fortement le contenu de l'entête au contenu du bloc et de servir à prouver ultérieurement l'intégrité du contenu du bloc.
Reste ensuite à s'assurer de l'intégrité de la place du bloc dans la Blockchain. Cette propriété est assurée essentiellement par un chainage des blocs entre eux, et ce depuis le premier bloc de la chaîne appelé « Genesis Block ». A la figure 2, le bloc 2 est bien situé entre les blocs 1 et 3, ce qui peut être vérifié en s'assurant que le haché du bloc 1 est correctement renseigné dans l'entête du bloc 2 et de même pour le haché du bloc 2 dans l'entête du bloc 3.

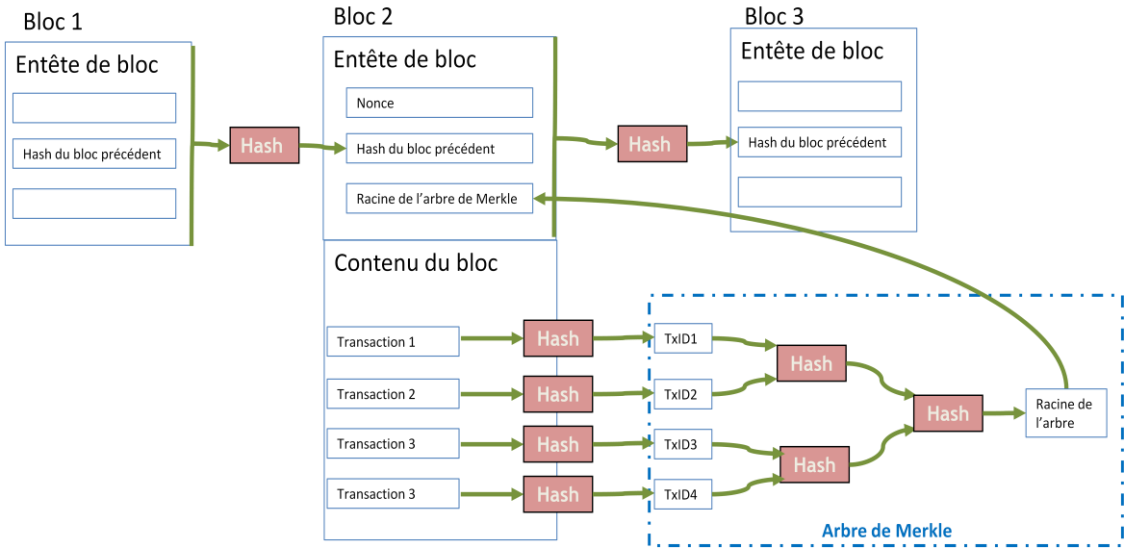

Figure 2 : Format simplifié d'un bloc Bitcoin

3.2.5. L'opération de minage pour l'obtention d'une preuve PoW (Proof of Work)

Le minage est l'opération qui permet au mineur de trouver un bloc valide par la résolution d'un problème mathématique complexe et de s'octroyer un gain. Plus exactement, avant de démarrer la résolution du problème, le mineur ajoute une transaction supplémentaire dans le bloc à traiter. Cette transaction appelée transaction « coinbase » ne satisfait pas les règles des transactions standards décrites à la section 3.2.3 (montant en output inférieur au montant en input), du fait que le mineur peut créer de la monnaie dans la limite fixée par la politique de la Blockchain. Cette transaction « coinbase » précise le bénéficiaire qui est le mineur et le montant du gain. De la sorte, après résolution du problème, si le bloc est accepté par les mineurs de la Blockchain, le gain sera acquis au mineur, ainsi que l'ensemble des frais

de transaction. Notons que la récompense du bloc diminue avec le temps, et que les mineurs compterons de plus en plus sur les frais de transaction pour leur rémunération.
Le problème à résoudre, encore appelé PoW pour Proof of Work, pour valider un bloc nécessite beaucoup de calculs de la part du mineur et consiste à trouver la valeur du champ Nonce de 32 bits à renseigner dans l'entête du bloc pour que le hachage de l'entête du bloc aboutisse à un résultat inférieur à une certaine valeur. Plus cette valeur est petite, plus le problème est difficile à résoudre. Pour conserver une même complexité calculatoire au fil du temps, il est intéressant que la Blockchain ajuste le niveau de difficulté. C'est le cas pour le projet Bitcoin qui s'appuie sur une moyenne de minage d'un bloc de 10 minutes. Ainsi, tous les 2016 blocs qui correspondent à une période théorique de deux semaines, une moyenne est calculée ; si le temps moyen est trop court, la difficulté est alors revue à la hausse ; s'il est trop long, la difficulté est revue à la baisse.

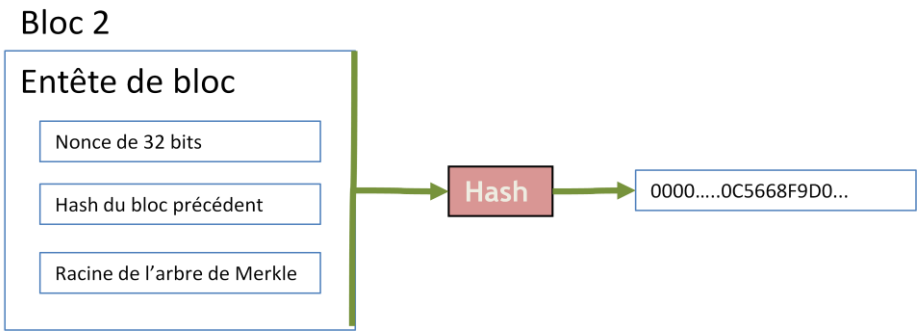

Figure 3 : Travail de minage de type PoW sur l'entête du bloc Bitcoin

3.2.6. L'opération de validation simple par PoS (Proof of Stake)

L'objectif de la validation par PoS est d'alléger la procédure de minage par PoW. Les enjeux sont à la fois écologiques avec des coûts énergétiques réduits par rapport à PoW et économiques avec une meilleure réactivité de la Blockchain qui peut inscrire plus rapidement des transactions, et de plus gros volumes de transactions traités. Le projet Ethereum travaille sur l'algorithme PoS appelé Casper vers lequel il prévoit de migrer d'ici un à deux ans. Casper devrait atteindre des performances de validation de bloc de quelques secondes, voire moins de 1 seconde, et devrait permettre ainsi le traitement de 20.000 transactions par seconde.

D'un point de vue fonctionnel, la validation par PoS est encore plus décentralisée que celle par PoW. En effet avec PoW, les nœuds effectuent exactement les mêmes opérations de minage depuis la validation des transactions jusqu'à la résolution du problème, ce qui a pour travers que c'est finalement la Chine avec de gros moyens mis en jeu qui centralise aujourd'hui le minage des Bitcoins. Avec l'approche PoS Casper, les nœuds sont organisés en plusieurs sous-groupes de sorte que le volume de transactions à valider est réparti sur plusieurs de ces sous-groupes, et qu'il en

résulte de meilleures performances. Le système privilégie les nœuds qui ont le plus fort engagement, c'est-à-dire ceux qui ont un portefeuille le plus fourni et qui ont donc le plus à perdre en cas de malveillance du fait qu'un système d'amendes est prévu pour dissuader les mauvais comportements.

Si le principe PoS est prometteur à première vue, la prudence est de mise car pour l'instant, même s'il est en test sur Ethereum, il n'a pas réellement fait ses preuves, contrairement au procédé PoW déjà testé dans les projets large échelle Bitcoin et Ethereum.

3.2.7. Les mécanismes d'incitation à miner

Sans le minage réalisé par les mineurs, la Blockchain ne pourrait pas fonctionner. Il est donc primordial d'identifier un gain (ou crypto-carburant) suffisamment attractif pour inciter un nombre suffisant de mineurs à assurer le minage et le stockage de la Blockchain. Notons que le mineur doit disposer de puissances de calculs importantes, voire très importantes pour le mécanisme PoW. Le gain doit donc venir compenser l'achat du matériel, mais aussi l'effort à maintenir le matériel en usage et la facture d'électricité. Le gain est versé au bénéfice du mineur pour chaque minage réussi et accepté par ses pairs, et ce sous forme d'une transaction qu'il ajoute dans le bloc (cf. section 3.2.5).

Les concepteurs sont libres de définir la nature du crypto-carburant pour les mineurs. Le crypto-carburant est généralement lié à l'activité portée par la Blockchain. Il peut s'agir de gagner de la crypto-monnaie, comme c'est le cas pour le projet Bitcoin, ou bien à la manière des techniques de fidélisation classiques : de l'espace de stockage, des ressources de calculs, quelques heures de location de voiture, un séjour dans un hôtel, un voyage, ou bien une capacité à voter plus importante dans un processus de vote…
Dans tous les cas, ce procédé d'incitation nécessite de définir une unité virtuelle qui permet d'accumuler des gains en fonction des efforts fournis, au même titre qu'une carte de fidélité. Cette unité qui est aussi une crypto-monnaie, est appelée ether dans le projet Ethereum. Ainsi, chaque nœud dispose d'un volume d'ethers gagnés et associés à son compte et son propriétaire décide du bon moment pour consommer ses ethers.

4. Sur quoi repose la confiance ?

Une Blockchain dispose des atouts suivants pour susciter la confiance :

- Architecture décentralisée reposant sur un grand nombre de nœuds dépendant d'organisations variées. Cela signifie, contrairement à une architecture centralisée où les décisions peuvent être prises unilatéralement,

qu'il faut atteindre un consensus ou bien réussir à contrôler plus de 50% des nœuds (ou de la puissance de calculs) pour avoir un effet sur le système. Le fait que l'architecture repose sur une multitude de nœuds qui assurent la validation et le stockage de la Blockchain, garantit par ailleurs une meilleure disponibilité du service.

- Des mécanismes d'incitation attractifs : Les nœuds doivent être en nombre suffisant et issus d'organisations différentes pour garantir l'indépendance et la disponibilité de la Blockchain.

- Traçabilité et auditabilité de toute la chaîne de transactions : La publication dans l'espace public de toutes les transactions réalisées depuis l'origine de la Blockchain (Bloc 0 ou « Genesis Block ») permet à chacun de vérifier l'intégrité de la chaîne, et de retracer tous les mouvements associés à un compte. Ainsi, il n'y a plus de triche possible ; tout se voit, tout se sait, dans la limite des garanties offertes par le pseudonymat.

- Transparence des algorithmes : Le code utilisé pour miner, pour s'interfacer avec la Blockchain, ou pour mettre en œuvre un smartcontract est lisible par tous. L'avantage est de permettre aux experts de la communauté d'utilisateurs de scruter le code et d'alerter en cas de suspicion. La confiance repose donc sur les lanceurs d'alertes.

- Authenticité des transactions protégées par pseudonyme : Les transactions doivent être approuvées par le(s) propriétaire(s) des comptes grâce à du matériel cryptographique de sécurité suffisante, et ce pour éviter que des ordres ne soient passés à leur insu. Pour s'adapter aux avancées technologiques, il est important de prévoir des mécanismes dont le niveau de sécurité soit adaptatif.

- Une blockchain rigidifiée avec des garanties importantes de sécurité : Il faut rigidifier les blocs contenus dans la Blockchain ainsi que l'enchaînement de ces blocs pour éviter toute altération postérieure de la Blockchain. Pour cela, il faut s'appuyer sur le caractère distribué de l'architecture, et sur un mécanisme de consensus fort. A cela, on peut éventuellement ajouter un mécanisme d'incitation au bon comportement, un mécanisme de dissuasion des mauvais comportements, et du matériel cryptographique pour apporter des garanties techniques fortes. PoW s'appuie sur un consensus et une preuve cryptographique coûteuse en calculs tandis que PoS s'appuie sur un consensus et des mécanismes d'incitation et de dissuasion qui n'ont pas encore fait leurs preuves sur un système réel.

5. Risques et limites

Neutralité de la gouvernance : Avant d'investir de son temps et son argent dans une Blockchain, il est nécessaire de se poser les questions suivantes : La neutralité de la gouvernance est-elle garantie ? Les acteurs impliqués, c'est-à-dire le petit groupe de personnes impliquées à faire évoluer le code et le protocole, sont-ils réellement indépendants dans leurs prises de décision et capables de résister à des pressions politiques, industrielles… ? Si ce n'est pas le cas, le principe fondamental du « décentralisé » n'est plus respecté. Si de plus, l'ensemble de ces acteurs ont la main mise sur plus de la moitié de la puissance de calcul de la Blockchain (voir le point ci-dessous sur la neutralité des infrastructures), alors le principe de consensus n'est lui non plus pas respecté pour les raisons suivantes. Quand une mise à jour du code de la Blockchain avec de nouvelles règles de fonctionnement est diffusée dans la Blockchain, l'administrateur d'un mineur a le choix d'accepter ou de refuser la mise à jour. Il peut s'agir d'une transformation des règles mineure et rétrocompatible - on parle alors de « soft fork » - ou bien d'une transformation importante et sans compatibilité ascendante - on parle de « hard fork ». Pour devenir fonctionnel, un « soft fork » nécessite le soutien d'une majorité de mineurs, tandis que le « hard fork » nécessite le soutien d'un consensus beaucoup plus large. Dans le cas de non consensus avec deux populations conséquentes de mineurs qui se détachent, la Blockchain initiale se scinde en deux, avec deux Blockchains qui suivent leur propre chemin. En conclusion, il est facile de comprendre qu'un regroupement d'acteurs qui détiendraient la majorité de la capacité de minage, peuvent, par collusion, modifier les règles de gouvernance, créer des « forks » qui apportent de la confusion, de la double dépense (cf. point plus bas) et un risque de dévaluation de la crypto-monnaie.

Neutralité des infrastructures informatiques sous-jacentes : La répartition des ressources informatiques utiles aux calculs et au stockage dans une blockchain doit être équilibrée entre organisations. La tendance dans Bitcoin a été la création de fermes de minage (mining pool), qui, à plusieurs reprises, a conduit les trois plus grosses fermes à réunir à elles seules plus de 50% de la puissance du réseau. Il faut comprendre que cette barre des 50% est critique car elle permet à une organisation ou un regroupement d'organisations de réaliser l'attaque des 51%, cette attaque leur permettant de censurer des transactions (avant le processus de minage), de favoriser le travail de minage de ses mineurs pour empocher les gains à la place de mineurs plus rapides, de réussir en cas de dédoublement de la chaîne à imposer une chaîne plus longue avec une probabilité raisonnable de succès, et donc de maitriser l'historique de la chaîne. Notons cependant que l'attaque des 51% ne permet ni de voler des gains, ni d'émettre des transactions frauduleuses.

Erreurs de programmation : Pour les Blockchains programmables (ou non), un risque fort est lié à des erreurs humaines de programmation, comme ce fut le cas en 2016 pour l'attaque de détournement de fond réalisé sur Ethereum « The DAO » (DAO pour Decentralized Autonomous Organization). En quatre semaines, « The DAO » a

réussi une levée de fond spectaculaire de 120 millions de dollars par crowdfunding, mais elle en a ensuite perdu un tiers suite à une attaque qui a mis en évidence une erreur de programmation. Cette erreur permettait à l'escroc de boucler indéfiniment sur la fonction provoquant une sortie de fonds. En 2017, une autre attaque a mis en cause une erreur dans le logiciel de porte-monnaie Parity Wallet, et a conduit au vol de 30 millions de dollars en ethers. Attention, soyons bien clair, ce n'est pas la technologie Blockchain qui est remise en cause ici, mais bien des erreurs de programmation.

Double dépense : La double dépense consiste à émettre deux transactions portant sur le même objet et qui devraient normalement s'exclure l'une l'autre. Il s'agit d'un acte volontaire malveillant d'un participant qui est normalement arbitré lors du minage. Cependant, il peut arriver que dans un processus de dédoublement de chaîne, chaque transaction soit validée indépendamment par chaque chaîne. A ce moment là, le bénéficiaire sait s'il dispose ou non des gains qu'une fois la chaîne la plus courte abandonnée. Pour Bitcoin, le délai raisonnable considéré est d'environ 1h, soit l'équivalent de 6 blocs.

Rétention de transactions : Un mineur peut avoir intérêt à ne pas partager une transaction dont les frais de transaction sont élevés. En gardant cette transaction pour lui jusqu'au succès du minage d'un bloc, il s'assure qu'elle sera incluse dans un de ses blocs et qu'il touchera la récompense. Cette transaction peut donc mettre longtemps avant d'être inclue dans la Blockchain. Cette attaque de rétention sera de plus en plus crédible à l'avenir du fait que le modèle de paiement reposera de plus en plus sur les frais de transaction à mesure que les récompenses de bloc diminuent. De la même façon, un mineur bien connecté peut retenir un bloc avant de le diffuser pour bénéficier d'un délai supplémentaire dans l'opération de minage. Ce n'est que lorsqu'il recevra un bloc concurrent qu'il pourra alors diffuser massivement son propre bloc. Ces attaques forcent à réfléchir à l'amélioration des mécanismes d'incitation.

Blanchiment d'argent : Le problème de blanchiment d'argent se pose dès qu'un nouveau moyen d'échanger de l'argent est à disposition. Contrairement à ce qu'on pourrait croire, la transparence des transactions passées dans la Blockchain n'empêche pas le blanchiment d'argent, elle le rend juste plus complexe. En effet, des techniques existent pour brouiller les pistes et la traçabilité. La première très simple consiste à détenir une multitude de comptes (certains pouvant même n'être utilisés qu'une fois) et à réaliser des transactions entre plusieurs de ces comptes. Une autre approche pour brouiller la traçabilité, appelée Coinjoin dans Bitcoin, consiste à fusionner plusieurs transactions en une. Plus le nombre de transactions fusionnées (entrantes et sortantes) est important, meilleure est la protection car plus il est difficile de relier un débiteur à un créditeur. Notons toutefois que l'approche Zerocash décrite dans la section 6 garantit la non traçabilité des transactions et

rend donc impossible la détection de blanchiment d'argent sur la seule base des éléments fournis dans la Blockchain.

6. La transparence de la chaîne est-elle un frein à la vie privée ?

Une Blockchain repose sur le pseudonymat des membres participants. Il suffit donc que soit dévoilée l'identité réelle de la personne associé à un compte pour que toutes les transactions effectuées par la personne depuis ce compte soient révélées, et ce, depuis son origine. Comme expliqué à la section 5, il existe plusieurs techniques pour améliorer la vie privée des usagers, à savoir posséder des comptes multiples, certains à usage unique, et effectuer plusieurs transactions simultanément sur le principe du Coinjoin de Bitcoin.

Le principe de transparence de la Blockchain ne permet pas d'héberger dans la Blockchain des éléments de nature privée, qu'ils soient algorithmiques ou informationnelles (données personnelles, cryptographiques…). Par contre, la Blockchain qui ne peut pas héberger de gros volumes d'informations, peut faire appel à une mémoire distribuée, externalisée et illimitée sous la forme d'un réseau pair à pair fonctionnant à la manière d'un réseau BitTorrent, Gnutella, Napster ou Kademlia. Il s'agit véritablement d'une mémoire externalisée dans la mesure où cette mémoire est indexée grâce à des clés DHT (Distributed Hash Table) qui peuvent être référencées dans la Blockchain. Cette mémoire peut héberger des données en clair ou chiffrées, mais dans ce dernier cas, reste à assurer la gestion des clés cryptographiques.

L'initiative Zerocash a proposé en 2014 une solution très intéressante de paiement anonymisé et décentralisé permettant le transfert de Bitcoins sur une Blockchain en toute transparence et sans traçabilité possible des flux monnétaires. L'approche permet en effet à un utilisateur de prouver la possession d'un certain montant de crypto-monnaie avant d'autoriser une transaction, mais sans qu'il ne soit possible de retracer sa provenance. C'est comme si, tous les utilisateurs accrochaient leurs billets sur un mur et qu'ils décrochaient, au moment d'une dépense, la somme correspondante du mur. La solution repose sur le principe du zero-knowledge (schémas dits « à apport nulle de connaissance ») qui permet de prouver la connaissance d'un secret à un tiers sans avoir à en révéler sa valeur. Pour cela, elle s'appuie sur le schéma zk-SNARKs (zero-knowledge Succinct Non-interactive ARguments of Knowledge), qui est particulièrement performant avec une preuve établie en quelques milli secondes pour prouver qu'un utilisateur dispose du montant en Bitcoin requis pour émettre une transaction sans avoir à révéler ni la source, la destination et le montant transféré.

Enfin, l'initiative Enigma du MIT développée en 2015 propose une plateforme cloud décentralisée garantissant la confidentialité des traitements opérés et des informations traitées. Elle s'appuie sur la Blockchain pour permettre la traçabilité des

opérations effectuées et sur le réseau pair-à-pair Enigma pour effectuer les traitements et le stockage des informations sensibles. L'idée est que chaque nœud du réseau Enigma n'ait qu'une vue partielle et sans valeur de l'information sensible et qu'il effectue un traitement partiel sur cette information. Ainsi, les nœuds n'ont accès individuellement à aucune information sensible et grâce à des techniques de type SMC (Secure Multi-party Computing), il leur est possible de produire de façon collaborative un résultat qui a du sens pour l'application.

Références

https://bitcoin.org/

https://blockchain.info/fr/charts

https://www.ethereum-france.com/

https://www.ethereum-france.com/interview-de-vitalik-buterin-createur-dethereum-et-president-de-la-fondation-partie-1-sur-2/

https://github.com/ethereum/wiki/wiki/White-Paper

« Comprendre la Blockchain, anticiper le potentiel de disruption de la Blockchain sur les organisations », Livre blanc, Editeur U, janvier 2016.

E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, M. Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin", 2014 IEEE Symposium on Security and Privacy.

G. Zyskind, O. Nathan, A. Pentland, "Enigma: Enigma: Decentralized Computation Platform with Guaranteed Privacy", 2015, http://enigma.media.mit.edu/enigma_full.pdf