Publié le : 20/05/2022

Par : Pascal Lafourcade & Malika More

Niveau ○○○

Niveau 2 : Intermédiaire

Comment fonctionnent les bitcoins ?

CULTURE & SOCIÉTÉ

RÉSEAUX & COMMUNICATION

 # Finance *# Cryptographie* *# Blockchain* *# Bitcoin* *# NSI*

En 2009, un bitcoin ne valait que quelques euros et son cours a atteint jusqu'à 59 717 euros en 2021. Si cette cryptomonnaie est désormais connue de tous, son fonctionnement n'est pas toujours évident à comprendre… Revenons sur les mécanismes sous-jacents à la création de ces fameux bitcoins.

En 2009, le toujours mystérieux **Satoshi Nakamoto** créa *Bitcoin*, le protocole permettant la mise en œuvre de la première cryptomonnaie décentralisée, le *bitcoin* (de l'anglais *bit,* unité d'information binaire, et *coin* « pièce de monnaie », souvent noté ₿, *BTC* ou encore *XBT*). Il s'agit d'une monnaie numérique qui se passe d'une autorité centrale. Ainsi les « pièces » sont créées et échangées directement entre les participants à l'aide de la ***technologie blockchain***, ceci sans l'intermédiaire d'une institution pour garantir la sécurité du système, comme c'est le cas avec les banques traditionnelles et les monnaies nationales, comme le dollar, ou supranationales, comme l'euro. Dans *Bitcoin* et les nombreux protocoles qui en sont les héritiers (*Ethereum*, *Ripple*, *Bitcoin Cash*, *Cardano*, etc.), la sécurité repose sur l'utilisation de divers concepts cryptographiques, d'où leur nom générique de cryptomonnaies. La sécurité de ces cryptomonnaies repose en partie sur la validation des transactions faites. Effectuer ces validations nécessite une grande quantité de calculs afin d'assurer la sécurité, cela consomme donc beaucoup d'énergie et génère par

conséquent une empreinte écologique élevée. Il s'agit d'un désavantage considérable pour l'avenir des cryptomonnaies décentralisées. Un axe de recherche qui occupe de nombreux scientifiques dans le monde consiste à essayer de diminuer la consommation d'énergie tout en continuant d'assurer la sécurité des transactions. Par exemple, le prix Turing de 2012, **Silvio Micali**, a fondé en 2017 la plate-forme *Algorand* qui est une *blockchain* lancée en 2019 consommant moins d'énergie que *Bitcoin*.

La technologie *blockchain*, sur laquelle repose *Bitcoin*, n'est pas seulement une innovation mais clairement une révolution qui a été introduite par *Bitcoin*. Pour comprendre le fonctionnement de la *Blockchain*, il est nécessaire de comprendre celui du protocole *Bitcoin*. Cette nouvelle technologie repose sur l'utilisation de nombreux concepts cryptographiques. Un des plus importants est la notion de fonction de **hachage**.

Fonction de hachage

Une fonction de hachage H est une **fonction déterministe** qui prend en entrée n'importe quel message, par exemple une phrase, un poème de Victor Hugo ou un DVD d'un film de Steven Spielberg et produit un message de taille fixe, appelé une empreinte ou haché. Cette taille vaut par exemple 256 bits dans le standard SHA-256. Pour hacher un message, il faut donc réduire le message jusqu'à atteindre la taille souhaitée.

Une fonction de hachage beaucoup trop naïve consiste à prendre les 256 derniers bits d'un message : elle présente l'inconvénient qu'il est facile de trouver plusieurs messages ayant le même haché.

En effet, la propriété de sécurité qu'une fonction de hachage doit avoir est qu'il soit difficile de trouver une *collision* : c'est-à-dire trouver deux messages différents m et m' qui ont les mêmes empreintes $H(m) = H(m')$.

Chiffres	ASCII
0	48
1	49
2	50
3	51
4	52
5	53
6	54
7	55
8	56
9	57

Lettres	ASCII
A	65
B	66
C	67
D	68
E	69
F	70
G	71
H	72
I	73
J	74
K	75
L	76
M	77

Lettres	ASCII
N	78
O	79
P	80
Q	81
R	82
S	83
T	84
U	85
V	86
W	87
X	88
Y	89
Z	90

Lettres	ASCII
a	97
b	98
c	99
d	100
e	101
f	102
g	103
h	104
i	105
j	106
k	107
l	108
m	109

Lettres	ASCII
n	110
o	111
p	112
q	113
r	114
s	115
t	116
u	117
v	118
w	119
x	120
y	121
z	122

Afin d'illustrer le principe d'une fonction de hachage, considérons la fonction de hachage un peu moins naïve H définie par la somme des valeurs **ASCII** des caractères d'un message *modulo* une valeur fixée très grande qui ne sera pas atteinte dans les exemples traités dans cet article. Dans la figure 1 ci-dessus, les codes ASCII des chiffres et des lettres de l'alphabet sont donnés. Ainsi le haché du message $Bonjour$ vaut $H(«Bonjour») = 66 + 111 + 110 + 106 + 111 + 117 + 114 = 735$. Cette fonction de hachage n'est évidemment pas sûre car par exemple $H(«Bonjour») = H(«bascule») = H(«anglais») = H(«indices»)$.

Le résultat de la fonction de hachage SHA-256 publiée par le *National Institute of Standards and Technology* (NIST), l'institut qui standardise les algorithmes cryptographiques, donne le résultat suivant :

$$H(«Bonjour») = 8dc2a6966f1be1644ec6b1f7223f47e53de5ad05e1c976736d948e7977a13dd3$$

$$H(«bonjour») = 9cec0af545144159bac85c7b908d5e0b9b0ef961497401c5ad8da26f065ad926$$

Ce résultat est obtenu par la commande `openss1 dgst sha 256 bonjour.txt` où le fichier contient la chaîne de caractères «$Bonjour$» ou «$bonjour$».

Le changement d'un seul caractère change totalement le résultat, dans l'exemple ci-dessus 'B' est remplacé par 'b' et les valeurs des hachés sont totalement différentes.

Chaîne de blocs

Une *blockchain* est un registre distribué sécurisé et décentralisé qui est construit en écrivant les données les unes après les autres. Par exemple, si les messages suivants : «$Bonjour$», «$Chere$», «$Alice$», «du», «$site$», «$Interstices$», doivent être stockés dans cet ordre dans la *blockchain*, alors il va falloir créer six blocs B_1 à B_6 de la manière suivante, où $||$ est la concaténation de messages :

$$B_1 = H(\text{«}Bonjour\text{»})$$
$$B_2 = H(B_1||\text{«}Chere\text{»})$$
$$B_3 = H(B_2||\text{«}Alice\text{»})$$
$$B_4 = H(B_3||\text{«}du\text{»})$$
$$B_5 = H(B_4||\text{«}site\text{»})$$
$$B_6 = H(B_5||\text{«}Interstices\text{»})$$

En reprenant la fonction de hachage naïve H introduite précédemment, il en découle que B_1 vaut 735. Ensuite il faut calculer B_2 comme suit :

$$B_2 = H(B_1||\text{«}Chere\text{»})$$

$$= H(\text{«}735Chere\text{»})$$

$$= 55 + 51 + 53 + 97 + 108 + 105 + 99 + 101$$

$$= 646$$

En utilisant la même méthode, il est possible de calculer les autres blocs. Si un des messages inscrits dans la *blockchain* est modifié, alors les autres messages stockés seront eux aussi changés. Ainsi, si par exemple une personne prétend que le second message est «$Madame$» au lieu de «$Chere$» alors tout le monde pourra vérifier qu'elle a tort car en refaisant les calculs les valeurs de B_4, B_5 et B_6 seront différentes de celles inscrites sur la blockchain. De même, prendre les messages dans l'ordre suivant «$Chere$», «$Alice$», «$Bonjour$» ne fonctionne pas non plus car $H(\text{«}Bonjour\text{»})$ est différent de $H(\text{«}Chere\text{»})$. Par contre, il est important qu'il soit difficile de trouver des collisions sur les fonctions de hachage utilisées. Par exemple, avec la fonction naïve utilisée ici, il est possible de transformer les transactions pour «$alice$» en des transactions pour «$celia$», car ce sont des anagrammes.

Afin d'assurer l'intégrité des données stockées sur la *blockchain*, la solution utilisée par *Bitcoin* est donc de chaîner les blocs les uns aux autres en utilisant une fonction de hachage. Ceci correspond à écrire dans un registre les transactions avec un stylo indélébile et de plastifier le document à chaque fois pour lier les écritures passées avec la dernière effectuée.

Il est aussi important de remarquer que l'ensemble des calculs peut être refait par tous à partir des messages. Ainsi, la vérifiabilité des calculs est une des propriétés importantes de la *blockchain*, offrant plus de confiance et de transparence dans son fonctionnement.

Dans *Bitcoin*, un bloc est constitué du haché du bloc précédent et d'un ensemble de transactions valides, par exemple Alice donne 15 *Bitcoins* à Bob et Charlie 3 *Bitcoins* à David, en ayant vérifié que les comptes respectifs d'Alice et de Charlie contiennent au moins la somme requise pour ces transactions.

Le dernier bloc dépend donc des valeurs stockées dans les blocs précédents mais aussi de leur ordre, car si le moindre changement dans un seul des messages précédents ou même dans l'ordre des messages se produit, alors la valeur du dernier bloc sera modifiée. Cette technique est appelée *chaîne de blocs* et est au cœur du fonctionnement de la *blockchain*. Elle consiste à hacher le premier message, puis ajouter le second message à ce haché et hacher le résultat. Il faut ensuite ajouter le troisième message au haché et hacher le résultat et ainsi de suite. Le haché du bloc précédent est contenu dans le bloc courant et le tout forme une chaîne de blocs d'où le nom de *blockchain*. La question qui reste à résoudre à ce stade est de savoir qui peut écrire les blocs dans la *blockchain* pour éviter la double dépense, propriété qui est assurée par la banque dans un système centralisé. En effet, avec une monnaie électronique, il est très facile de dupliquer une pièce car il s'agit d'un fichier qu'il suffit de copier. Pour éviter cela dans un système centralisé, la banque tient un registre des transactions pour savoir quand une pièce a été dépensée et ainsi éviter qu'un utilisateur ne dépense deux fois la même pièce. Dans *Bitcoin*, le registre des comptes (la *blockchain*) n'est pas géré par une seule entité mais par l'ensemble des personnes qui ont envie de devenir des mineurs. Les mineurs sont les personnes qui vérifient la solvabilité des transactions puis qui les valident et écrivent dans la *blockchain*.

Miner des *Bitcoins*

Dans *Bitcoin*, lorsqu'un participant qui a vérifié un ensemble de transactions, résout un challenge cryptographique appelé « objectif de hachage » alors il va pouvoir écrire dans la *blockchain* des transactions qui sont des transferts de *Bitcoins* entre différents participants. Pour ce travail, il est récompensé par la création de nouveaux *Bitcoins*. Au début, chaque mineur recevait 50 *Bitcoins* pour avoir vérifié la validité d'un ensemble de transactions non vide et bornée par une limite de taille 1 Mo et résolu l'objectif de hachage associé. De plus, dans *Bitcoin*, par construction du protocole et de manière arbitraire, toutes les 210 000 validations, la récompense est divisée par 2. Ainsi il n'y aura qu'un nombre fini de *Bitcoins* qui seront créés, ce nombre s'élève à 21 millions. Comme la validation d'un bloc prend par construction 10 minutes en moyenne, la récompense est divisée par deux environ tous les 4 ans.

Une fois que tous les *Bitcoins* seront créés, les transactions incluront des frais pour récompenser les mineurs de leur travail — ce qui est déjà le cas aujourd'hui — et une transaction sans récompense pour les mineurs ne sera pas écrite sur la *blockchain*.

Pour expliquer comment un mineur valide les transactions, nous allons reprendre la fonction de hachage naïve introduite précédemment. Considérons que Alice veuille transférer 5 *Bitcoins* à Bob. Cette transaction sera notée $T = (A, B, 5)$. La règle pour résoudre un objectif de hachage arbitrairement choisie ici est la suivante : un mineur, après avoir vérifié la validité des transactions, doit prendre la valeur du haché du dernier bloc B_{last} et la transaction T afin de trouver un nombre n tel que $H(H(T||B_{\text{last}}||n))$ soit divisible par 5 et par 3. Le premier qui trouve un tel nombre valide la transaction et par la même occasion sera récompensé par de nouvelles pièces. Par exemple, si $T = (A, B, 5)$ et $B_{\text{last}} = 42$ alors par exemple $n = 89$ permet de trouver $H(H(«A||B||5||42||89»)) = H(«399») = 165$ qui est divisible par 5 et par 3. Dans le véritable protocole *Bitcoin*, il faut que la valeur de ce calcul avec de vraies fonctions de hachage soit plus petite qu'un nombre fixé.

Pour trouver un n qui respecte cette contrainte, la technique de la recherche exhaustive sur toutes les valeurs de n fonctionne très bien (car le résultat d'une fonction de hachage est considéré comme étant aléatoire et non prévisible, il n'existe donc pas de stratégie pour déterminer les valeurs de n gagnantes), mais de nombreux calculs sont effectués dont le résultat est immédiatement rejeté. C'est ainsi que de nombreux calculs sont faits inutilement,

induisant le fait qu'il faille une grande quantité d'énergie pour assurer le fonctionnement de *Bitcoin*. Par exemple pour *Bitcoin*, nous avons vu qu'il faut 10 minutes pour valider un nouveau bloc, ce qui revient à effectuer 127.25 EH/s sachant que 1 EH correspond au calcul de 1 000 000 000 000 000 000 hachés. Cette puissance de calcul n'est possible que par les progrès du matériel consacré à ces calculs et au fait que les mineurs se regroupent en fermes de minage, sortes de coopératives pour miner ensemble. Afin d'assurer qu'il faille en moyenne 10 minutes pour miner un bloc, dans Bitcoin la difficulté (c'est-à-dire la valeur de l'objectif de hachage) est actualisée dynamiquement tous les 10 000 blocs en fonction de la puissance de calcul utilisée pour miner ces blocs et du temps mis. Ainsi la difficulté augmente si la puissance de calcul mondiale moyenne des mineurs augmente, mais elle diminuera si la puissance de calcul mondiale moyenne des mineurs diminue.

Consensus

Après avoir expliqué le principe de « chaîne de blocs », il faut maintenant comprendre qui va écrire dans la *blockchain*. Ces personnes sont appelées des *mineurs* et maintiennent le registre distribué d'informations qu'est la *blockchain*. Dans le cadre de *Bitcoin*, ce registre contient l'ensemble des transactions effectuées entre les participants. Dans le système bancaire classique, c'est la banque qui détermine si une transaction est valide ou non. Pour cela, la banque vérifie le solde des comptes des débiteurs avant de procéder au transfert de fonds mais assure aussi qu'une pièce n'est pas utilisée deux fois, évitant ainsi une double dépense. Dans *Bitcoin*, cette opération de vérification est faite par un mineur qui va jouer le rôle de la banque en vérifiant la solvabilité du compte (c'est-à-dire en regardant dans les blocs passés que les soldes des comptes contiennent assez de *bitcoins*), en assurant l'absence de double dépense (dans l'ensemble des transactions à valider, il ne faut pas que les mêmes pièces soient utilisées deux fois) et ensuite en écrivant la transaction dans la *blockchain*.

Pour écrire, un mineur doit faire des calculs le plus rapidement possible. Il se peut que deux mineurs qui valident deux transactions différentes utilisant la même pièce fassent ces calculs rapidement. Dans ce cas, le protocole *Bitcoin* doit faire un choix et n'inscrire qu'une seule des deux validations. Dans *Bitcoin*, c'est la chaîne la plus longue qui sera considérée comme valide. Ainsi, ce sont les choix de chacun des mineurs qui vont décider quelle est la chaîne principale. Il est admis qu'il faut attendre que six autres blocs soient ajoutés à un bloc pour considérer que les transactions contenues dans ce bloc soient bien inscrites dans la *blockchain*. Les transactions qui ne sont pas sur la chaîne la plus longue ne sont pas validées bien que les mineurs aient fait leur travail correctement. Ces blocs sont appelés des orphelins. Les mineurs ont intérêt à ne pas prolonger des orphelins (qui ne sont pas sur la chaîne la plus longue) car ils ont peu de chance de voir cette branche redevenir la plus longue, donc tout le monde abandonne les orphelins et le consensus se fait naturellement sur la blockchain la plus longue ! Cela marche bien, sauf si un mineur a plus de 50 % de la puissance de calcul car dans ce cas, il peut prendre en main une chaine d'orphelins pour la faire grandir et dépasser la chaine la plus longue.

En 2018, plus de la moitié de la puissance de calcul est possédée par des fermes de minage chinoises. En 2021, suite à l'interdiction de *Bitcoin* par le gouvernement chinois, la répartition mondiale de la puissance de calcul a changé et s'est rééquilibrée. De plus, l'ensemble du contenu de la *blockchain* est public et ainsi, tout le monde peut vérifier la validité des transactions.

Si une personne possède plus de 50 % de la capacité de calcul pour miner des blocs, alors elle contrôle la chaîne et peut donc décider quelles informations sont stockées sur la *blockchain*. Il est donc important que la sélection de la personne qui peut écrire sur la *blockchain* soit publique, équitable et acceptée par tous les participants. Savoir qui peut écrire le prochain bloc dans la chaîne de blocs est un des points importants. Cela est résolu par un algorithme de consensus. L'objectif d'un tel algorithme est de décider qui, parmi l'ensemble des participants, peut écrire le prochain bloc.

Il existe de nombreux algorithmes de consensus et tout est envisageable, par exemple tirer au hasard parmi les participants comme dans la *blockchain Algorand*, ou bien choisir une personne via un vote parmi les mineurs comme dans des *blockchains* de consortium. Dans *Bitcoin*, c'est la personne qui va résoudre un challenge cryptographique le plus rapidement possible qui écrit dans la *blockchain*. C'est ce côté décentralisé de la technologie *blockchain* qui permet d'assurer la confiance dans le système, ceci par opposition à un système centralisé comme le système bancaire actuel où il faut faire totalement confiance à la banque. Elle pourrait falsifier vos comptes en vous ôtant de l'argent ou en vous en ajoutant à sa guise. La *blockchain* permet d'avoir une confiance accrue et d'assurer que les données inscrites ne sont pas altérées.

Applications

Au-delà de la monnaie, la *blockchain* permet de nouvelles applications dans de nombreux domaines grâce à la création des *smart contracts,* ou contrats intelligents, par la *blockchain Ethereum*. Un *smart contract* est un programme qui est écrit sur la *blockchain* et est donc non modifiable et qui va s'exécuter par les acteurs intéressés. Par exemple, si mon compte A dépasse une certaine somme alors le reste est transféré sur le compte B. Ces nouveautés ont clairement ouvert de nouvelles possibilités comme par exemple dans l'art — où il y a eu en 2020 un réel engouement, menant peut-être à une bulle spéculative–, en dématérialisant les titres de propriété des œuvres d'art *via* les **jetons non fongibles** (NFT), une des applications phare de la *blockchain* qui permet de créer, échanger et stocker des objets numériques uniques sur la *blockchain*. Le marché de l'art numérique a connu un essor considérable, permettant à la fois sa démocratisation et favorisant l'exposition d'artistes contemporains. La *blockchain* apporte une traçabilité dans ce milieu où il n'est toujours pas facile de savoir qui est le propriétaire d'une œuvre. La *blockchain* permet aussi de rendre infalsifiable les transactions et de permettre à tout le monde de consulter les différents échanges, achats et ventes entres les acteurs de ce marché.

Les *cryptokitties* sont un exemple significatif d'application de NFT. Il s'agit d'œuvres numériques qui représentent des chats comme celui de la figure 2. Il y a des chats mâles et des chats femelles. Les chats peuvent se reproduire pour donner naissance à de nouvelles œuvres qui mélangent les caractéristiques des parents. Dans ce système, les enfants sont la propriété de la personne qui possède la mère. Les *Cryptokitties* sont entièrement régis par des *smart*

contracts sur la *blockchain Ethereum* et il est possible d'acheter des *Cryptokitties* avec la cryptomonnaie *Ethereum*. La *blockchain Ethereum* gère les titres de propriété de ces œuvres d'art. Il est donc aussi difficile de voler un *Bitcoin* à une personne que de lui voler son **CryptoKitty**.

Conclusion

Bitcoin a introduit la technologie *Blockchain* qui est une révolution au même titre que l'imprimerie ou Internet. En effet, cela remet en cause la conception de nombreux services de notre société et ces systèmes permettent de ne plus faire confiance à une autorité centrale comme une banque, un serveur ou encore un État. Cela ouvre de nombreuses applications possibles pour un monde plus sécurisé. Par exemple, durant l'été 2021, le monde de la mode s'est emparé de cette technologie avec les premières réalisations virtuelles et les premières ventes à l'aide de cryptomonnaies. De nombreuses autres initiatives dans ce domaine sont en cours. D'un autre côté, il reste encore de nombreuses améliorations à apporter à cette nouvelle technologie pour la rendre moins énergivore tout en assurant la sécurité.

Pour en savoir plus