Janvier 2024

Bitcoin et la blockchain

En 2009, Satoshi Nakamoto a créé Bitcoin, la première crypto-monnaie décentralisée. Cette invention repose sur un principe cryptographique appelé la « blockchain ». L'objectif de cette activité est de faire travailler les élèves sur une version simplifiée permettant de découvrir certains aspect de son fonctionnement.

- Environ 1h30.
- Plusieurs groupes de 3 ou 4 élèves.
- Niveau lycée.
- Objectif : Découvrir le fonctionnement de Bitcoin.
- Compétences travaillées :
  - Critères de divisibilité ;
  - Algorithmes distribués et travail coopératif ;
  - Culture numérique : Bitcoin.

Introduction.

Dans les années 1980, le cryptographe David Chaum propose la première monnaie électronique reposant sur des concepts cryptographiques, « DigiCash ». C'est le début des crypto-monnaies. Le challenge le plus important est de concevoir des « pièces » numériques (autrement dit, ce ne sont rien d'autre que des caractères écrits dans un fichier) ayant au moins les mêmes propriétés que les pièces de monnaie physiques régissant l'économie depuis des siècles. En particulier, dans un monde dématérialisé, il paraît très simple de dupliquer une telle pièce, avec un simple copier-coller. Or il est essentiel de ne pas pouvoir dépenser deux fois la même pièce pour garantir la stabilité du système. Pour cela, l'idée de David Chaum est qu'une fois une pièce reçue en paiement par un individu, il doit la faire valider auprès de la banque pour obtenir une nouvelle pièce de même valeur qu'il puisse

dépenser à son tour. Ainsi, la banque assure qu'une même pièce n'est pas dépensée deux fois, selon un principe très similaire à celui des chèques bancaires. La révolution introduite par Bitcoin est qu'il n'est plus nécessaire d'avoir une autorité centrale pour valider les échanges de pièces. L'objectif de cette activité est de découvrir le mécanisme de validation décentralisée des transactions dans Bitcoin, appelé la blockchain.
Dans cette fiche, nous introduisons quelques concepts fondamentaux à propos de la blockchain et en présentons une version simplifiée destinée à être mise en œuvre par des élèves.

Partie 1 : Fonction de hachage.

Le premier ingrédient de la blockchain s'appelle une « fonction de hachage ». Il s'agit d'une fonction qui transforme n'importe quelle donnée (nombre, texte, image, son,...) en une chaîne de bits de longueur limitée (par exemple 256 bits) appelée un haché. Cette fonction présente forcément des collisions, c'est-à-dire des données différentes qui ont le même haché, et elle doit posséder plusieurs propriétés, en particulier, il doit être difficile (en un sens technique) de trouver une donnée ayant un haché spécifique. Par ailleurs, une fonction de hachage est déterministe, c'est-à-dire que la même donnée, hachée à deux moments différents, donne toujours un haché identique.
Ces propriétés sont nécessaires pour l'une des utilisations les plus courantes des fonctions de hachage : dans une base de données d'utilisateurs, il est préférable de ne pas stocker leurs mots de passe en clair, pour se prémunir contre un risque de piratage. À la place, la base contient seulement les hachés des mots de passe. Ainsi, lorsqu'un utilisateur tape un mot de passe, le haché correspondant est calculé, et comparé à celui stocké dans la base pour cet utilisateur avant d'autoriser ou pas la connexion. Dans le cas de la blockchain, la fonction de hachage est utilisée lors de deux moments clés du processus de validation d'une transaction, l'enchaînement des blocs et l'objectif de hachage, qui seront présentés par la suite.
Les fonctions de hachage utilisées dans la vie réelle sont par exemple SHA-256 ou BCRYPT. Dans l'activité 1 proposée ci-dessous, une fonction de hachage très simplifiée appelée H est présentée, et utilisée par la suite dans l'activité 2 sur la blockchain proprement dite. Cette fonction est basée sur le code ASCII des caractères donnés dans la table :

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

Plus précisément, étant donnée une chaîne de caractères composée de lettres majuscules, de lettres minuscules sans accents et de chiffres, son haché est constitué des 10 derniers chiffres de la somme des codes ASCII des caractères. Par exemple :

$$\begin{aligned} H(Pi314) &= ASCII(P) + ASCII(i) + ASCII(3) + ASCII(1) + ASCII(4) \\ &= 80 + 105 + 51 + 49 + 52 \\ &= 337 \end{aligned}$$

Activité 1

Les élèves calculent le haché de « 2009Blockchain », ou de toute autre expression mêlant des lettres majuscules et minuscules et des chiffres.

$$\begin{aligned} H(2009Blockchain) &= ASCII(2) + ASCII(0) + ASCII(0) + ASCII(9) + ASCII(B) \\ &\quad + ASCII(l) + ASCII(o) + ASCII(c) + ASCII(k) + ASCII(c) \\ &\quad + ASCII(h) + ASCII(a) + ASCII(i) + ASCII(n) \\ &= 50 + 48 + 48 + 57 + 66 + 108 + 111 + 99 + 107 + 99 + 104 \\ &\quad + 97 + 105 + 110 \\ &= 1209 \end{aligned}$$

La condition « les 10 derniers chiffres » n'entre pas en jeu dans l'activité, où les nombres manipulés sont relativement petits. Cependant, nous avons choisi de l'expliciter car la taille limitée des hachés est une caractéristique essentielle d'une fonction de hachage.
Pour illustrer le fait que H n'est pas une bonne fonction de hachage dans la vie réelle, l'enseignant peut faire remarquer aux élèves que deux anagrammes ont le même haché : $H(ALICE) = H(CELIA)$ par exemple.
D'autre part, il est assez facile de trouver des chaînes de caractères qui ont le même haché : « cactus » et « adroit » ont pour haché 643 et « 42 » et « 51 » ont pour haché 102. Ce n'est pas gênant pour l'activité 2 proposée plus bas, mais il faut savoir que cette fonction de hachage n'est pas cryptographiquement sûre. En complément de l'activité 1, les élèves peuvent être invités à rechercher des paires de mots différents qui ont le même haché.

Partie 2 : Blockchain, mineurs et fermes de calcul.

La blockchain, « chaîne de blocs » en français, archive l'ensemble des transactions en bitcoins effectuées depuis la création de cette monnaie. En 2023, celle de Bitcoin mesure plus de 500 Go. La validation de chaque nouvelle transaction ajoute un « bloc » à la chaîne, et le contenu de ce bloc dépend de cette transaction (la date, le client, le vendeur, le montant, et d'autres informations), mais aussi de la valeur du bloc précédent de la chaîne elle-même. C'est en ce sens que les blocs sont « chaînés » les uns aux autres. Par conséquent, modifier à un instant donné une transaction effectuée dans le passé impliquerait de modifier aussi toutes les transactions qui ont eu lieu entre temps : c'est

pourquoi la blockchain est dite infalsifiable. La blockchain et la liste des transactions à valider sont stockées sur des serveurs publics et mises à jour en temps réel.
Ceux qui effectuent les calculs nécessaires pour ajouter des blocs à la chaîne, autrement dit pour valider des transactions, sont appelés des « mineurs », en référence aux véritables mineurs qui extraient de l'or d'une mine, car ce travail produit des bitcoins.
Leur tâche consiste en partie à faire un calcul cryptographique nécessitant de longs calculs. Lorsqu'un mineur réalise en premier ce calcul pour une certaine transaction, celle-ci est alors validée, un nouveau bloc est ajouté à la chaîne, et le mineur reçoit un paiement en bitcoins. Il y a concurrence entre les différents mineurs pour valider les transactions le plus vite possible, puisque seul le plus rapide gagne des bitcoins, tandis que les autres ont travaillé pour rien. À l'origine, les mineurs étaient des particuliers qui utilisaient leurs ordinateurs personnels pour effectuer les calculs. En 2023, ce sont plutôt des sociétés qui possèdent des « fermes de calcul » regroupant des milliers de machines. Dans l'activité 2 proposée ci-dessous, les élèves jouent le rôle de mineurs regroupés dans des fermes de calcul, elles-mêmes en concurrence pour miner des bitcoins.

Partie 3 : Objectif de hachage et preuve de travail.

Le nom technique du calcul cryptographique que les mineurs s'efforcent de résoudre est « objectif de hachage », il est basé sur l'utilisation d'une fonction de hachage. Lorsqu'un mineur remplit l'objectif de hachage pour une transaction, il en fournit la justification, sous la forme d'un nombre appelé « preuve de travail ». Le calcul est long à effectuer, mais ensuite, n'importe qui peut vérifier facilement que le nombre remplit bien l'objectif.
Dans l'activité 2 proposée aux élèves ci-dessous, pour valider par exemple la transaction « Alice donne 5 unités monétaires à Bob », modélisée par la chaîne de caractères « A5B », lorsque la valeur du dernier bloc de la chaîne est par exemple 45, **l'objectif de hachage est de trouver une chaîne de caractères N de telle sorte que $H(H(45A5BN))$ soit divisible par 5 et 3** (ou tout autre objectif mathématique simple qui convienne à l'enseignant), en utilisant la fonction de hachage H présentée plus haut. La preuve de travail est simplement N.

Par exemple, avec $N = 8$, le calcul est :

$$\begin{aligned} H(45A5B8) &= ASCII(4) + ASCII(5) + ASCII(A) + ASCII(5) + ASCII(B) + ASCII(8) \\ &= 52 + 53 + 65 + 53 + 66 + 56 \\ &= 345 \end{aligned}$$

Puis :

$$\begin{aligned} H(345) &= H(3) + H(4) + H(5) \\ &= 156 \end{aligned}$$

.

Ce dernier nombre est divisible par 3, mais pas par 5, donc $N = 8$ ne convient pas.

Le choix de l'objectif de hachage est en grande partie arbitraire. Celui que nous proposons ici ressemble dans la forme à celui utilisé dans la vie réelle pour Bitcoin, tout en donnant lieu à des calculs réalisables par des élèves. En effet, dans Bitcoin, l'objectif de hachage utilise la fonction de hachage appelée $SHA-256$: pour valider une transaction représentée par une chaîne T, lorsque la valeur du dernier

bloc de la chaîne est P, il consiste à trouver un nombre N tel que $SHA-256(SHA-256(P,T,N))$ soit plus petit qu'une certaine valeur, automatiquement modifiée à chaque bloc pour que ce calcul prenne toujours environ 10 minutes. Pour rappel, la chaîne T contient l'ensemble des informations concernant la transaction, comme la date, le client, le vendeur, le montant, et encore d'autres.

Activité 2.

Le seul matériel nécessaire est la calculatrice, du papier et un stylo. Une liste de transactions choisies par l'enseignant (voir Appendice) est affichée au tableau, ainsi que la valeur du dernier bloc en date de la chaîne, lui aussi choisi par l'enseignant. Pour commencer, chaque groupe d'élèves sélectionne une transaction, puis s'efforce de remplir l'objectif de hachage correspondant.

En suivant notre exemple précédent, avec 45 comme état initial de la blockchain, et $A5B$ comme transaction, la valeur $N = 59$ convient puisque :

$$\begin{aligned} H(45A5B59) &= ASCII(4) + ASCII(5) + ASCII(A) + ASCII(5) + ASCII(B) \\ &\quad + ASCII(5) + ASCII(9) \\ &= 52 + 53 + 65 + 53 + 66 + 53 + 57 \\ &= 399 \end{aligned}$$

Et :

$$\begin{aligned} H(399) &= ASCII(3) + ASCII(9) + ASCII(9) \\ &= 51 + 57 + 57 \\ &= 165 \end{aligned}$$

,

et ce dernier est bien divisible par 3 et par 5.

D'autres valeurs possibles pour N sont 68, D, ou encore 89, puisque $H(45A5B68) = H(45A5BD) = 399$ et $H(45A5B89) = 402$ avec $H(402) = 52 + 48 + 50 = 150$, lui aussi divisible par 3 et par 5.

Le premier groupe d'élèves qui trouve un N correct pour la transaction choisie l'annonce publiquement, ainsi que la valeur du nouveau bloc (ici 165 est ajouté au tableau), valide la transaction correspondante (ici Alice paye 5 unités à Bob) en la barrant sur la liste affichée et remporte une récompense à se partager entre les membres du groupe. Pour concrétiser ce dernier point, l'enseignant peut utilement envisager de se munir d'un paquet de bonbons, ou attribuer un score en bitcoins à l'équipe qui parvient à valider une transaction.

Par la suite, pour valider une autre transaction, la nouvelle valeur du dernier bloc de la chaîne est maintenant 165 à la place de 45, et il faut recommencer tous les calculs.

Comme dans une véritable ferme de calcul, il est essentiel que les élèves de chaque groupe s'organisent pour travailler efficacement, puisque les calculs peuvent être exécutés en parallèle. Par exemple, ils peuvent se partager les nombres par paquets de dix : 0 à 9 pour l'un, 10 à 19 pour le deuxième et 20 à 29 pour le troisième, puis on recommence 30 à 39, etc. au cas où le premier paquet de nombres ne suffise pas à trouver un N qui marche. Dans notre exemple, $N = 59$ est le plus petit entier qui convient.

Partie 4 : Quelques aspects du protocole Bitcoin non traités dans l'activité.

Comme toute métaphore, l'activité proposée dans cet article ne reflète que partiellement la réalité. Nous listons ci-dessous quelques point importants laissés de côté, par souci de simplicité.
Tout d'abord, avant de commencer à miner pour valider une transaction, les mineurs doivent vérifier qu'elle est possible : les comptes concernés doivent exister, celui du client doit être suffisamment approvisionné, etc. Pour cela, ils examinent un index où sont référencées l'ensemble des transactions validées depuis le début de la blockchain. Ces index peuvent être maintenus à jour par les mineurs eux-mêmes ou bien fournis par des personnes tierces. Sans cela, chaque vérification demanderait de recalculer l'ensemble de la blockchain depuis le tout début pour trouver les informations utiles. Comme la taille de la blockchain dépasse les 500 Go, ceux qui s'y essayeraient n'auraient aucune chance de gagner la course à la preuve de travail. Ensuite, les bitcoins avec lesquels les mineurs sont rétribués pour le moment sont de nouvelles pièces créées à cet effet. La quantité de bitcoins en circulation augmente ainsi avec le temps, mais elle est limitée, par choix de son concepteur. En effet, la récompense est divisée par 2 toutes tous les 210 000 blocs (environ tous les 4 ans). Un jour, il n'y aura plus de création de nouveaux bitcoins, et les mineurs se rémunéreront par des frais prélevés sur les transactions.
Enfin et surtout, il faut expliquer comment la double dépense est évitée grâce à la blockchain. Dans la vraie vie, il s'agit évidemment d'une caractéristique indispensable pour une cryptomonnaie, bien que cela ne risque pas de se produire dans l'activité proposée aux élèves. Par exemple, si Alice décide de payer 5 bitcoins à la fois à Bob et à Charlie, alors qu'elle ne possède que 8 bitcoins au total, la liste des transactions à valider en contient deux concernant la même pièce. Si chacune est validée simultanément par un mineur différent, un embranchement se produit dans la blockchain. Les deux branches se poursuivent indépendamment pendant quelques transactions, puis la plus longue est finalement choisie, par consensus entre tous les mineurs. Dans ce cas, toutes les transactions sur l'autre branche sont annulées (et remises dans la liste des transactions à valider), ainsi que les paiements des mineurs. La validation d'une transaction est considérée comme définitive au bout d'une heure environ (après validation de 6 blocs). Les mineurs ont intérêt à parvenir le plus vite possible à un consensus, pour risquer le moins possible de travailler sans rien gagner au final.

Conclusion

Cette activité vise à présenter quelques aspects du fonctionnement de la blockchain en utilisant des calculs simples à partir de la table ASCII et de critères de divisibilité élémentaires. En particulier, elle met l'accent sur la notion d'objectif de hachage et de preuve de travail, et sur l'aspect distribué du minage. Elle permet ainsi d'initier les élèves à certains principes de la cryptomonnaie décentralisée Bitcoin. Pour en savoir plus sur Bitcoin, vous pouvez consulter l'ouvrage [1].
Bitcoin et les autres cryptomonnaies représentent les utilisations les plus célèbres de la technologie blockchain, mais elle peut aussi servir dans des domaines non monétaires, dès lors qu'il s'agit de stocker des informations de façon infalsifiable et vérifiable. Par exemple, le MIT enregistre depuis 2018 sur

une blockchain les diplômes qu'il délivre à ses étudiants. Cela permet aux recruteurs de s'assurer de la sincérité des CV qui leur sont présentés. Dans un tout autre domaine, le Food Trust d'IBM est une blockchain dédiée à la traçabilité dans le secteur alimentaire. Elle permet à des producteurs, transformateurs et distributeurs de tenir un registre relatif à la provenance des aliments, aux données de transaction, aux détails de traitement, etc.

Adaptations

- Pour des lycéens à l'aise en Python, il est envisageable de coder l'algorithme de recherche exhaustive. Cela permet d'aborder des aspects plus avancés, comme la question de la double dépense.
- Pour des élèves plus jeunes, les calculs peuvent s'avérer fastidieux, même en les répartissant dans le groupe. Nous suggérons dans ce cas l'usage d'une table d'encodage numérique des caractères ad hoc, plus simple que la table ASCII.

RÉFÉRENCES

[1] Les blockchains en 50 questions - 2e édition, Comprendre le fonctionnement de cette technologie. Jean-Guillaume Dumas, Pascal Lafourcade, Ariane Tichit, Sébastien Varrette, Dunod 2022

Appendice

Pour générer la liste des transactions à valider à afficher au tableau dans l'activité 2, voici un programme Python qui recherche une valeur de N (dans une plage choisie) qui convient pour toutes les transactions de $A1B$ à $D9C$ (acheteur, montant et vendeur paramétrables), à partir d'une valeur fixée (paramétrable) bu bloc précédent. Il suffit ensuite de choisir quelques transactions dans la liste pour les afficher (sans le N, évidemment).

```
L=[]
init=45 #valeur initiale de la blockchain 45
for a in ["A","B","C","D"]: #nom de l'acheteur A
    for b in range(1,10): #montant de la transaction 5
        for c in ["A","B","C","D"]: #nom du vendeur B
            if a!=c:
                ordinit=sum(ord(i) for i in str(init))
                ordb=sum(ord(i) for i in str(b))
                deb=ordinit+ord(a)+ordb+ord(str(c))
                for N in range(1000): #recherche exhaustive de preuves de travail N entr
                    ordN=sum(ord(i) for i in str(N))
                    res=deb+ordN #H(45A5BN)
                    calc=sum(ord(i) for i in str(res)) #H(H(45A5BN))
```

```
                    if calc%3==0 and calc%5==0: #objectif de hachage:H(H(45A5BN)) divisi
                        L.append(str(init)+a+str(b)+c+str(N))
                        break #on arrête au plus petit N qui convient
print(L) #liste des transactions avec leurs preuves de travail
```