par P. Lafourcade et M. More

Bitcoin et la *blockchain*

En 2009, Satoshi Nakamoto a créé Bitcoin, la première crypto-monnaie décentralisée. Cette invention repose sur le principe cryptographique de la blockchain. Dans cette activité, les élèves travaillent sur une version simplifiée de cette dernière permettant de découvrir certains aspects de son fonctionnement.

Environ 1 h 30. Plusieurs groupes de trois ou quatre élèves. Niveau lycée.
Objectif : découvrir le fonctionnement de Bitcoin.
Compétences travaillées :
• utiliser une fonction de hachage ;
• appliquer les critères de divisibilité ;
• algorithmes distribués et travail coopératif.

Dans les années 1980, l'informaticien américain David Lee Chaum (né en 1955) propose la première crypto-monnaie électronique, DigiCash. Le défi principal est de concevoir des « pièces » numériques (autrement dit, des caractères écrits dans un fichier) ayant les mêmes propriétés que les pièces de monnaie physiques. En particulier, il paraît très simple de dupliquer une telle pièce, avec un simple copier-coller. Pour éviter cela, l'idée de David Chaum est que tout individu ayant reçu une pièce en paiement doit la faire valider auprès de la banque pour obtenir une nouvelle pièce de même valeur qu'il puisse dépenser ensuite. 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 (une banque) pour valider les transactions. L'objectif de cette activité est de découvrir le mécanisme de validation décentralisée des transactions dans Bitcoin, appelé la *blockchain* (en français, la *chaîne de blocs*).

Dans cet article, quelques concepts fondamentaux sont introduits à propos de la *blockchain* ; une version simplifiée destinée à être mise en œuvre par des élèves sera présentée.

Le code ASCII.

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

Lettres	ASCII	Lettres	ASCII	Lettres	ASCII	Lettres	ASCII
A	65	N	78	a	97	n	110
B	66	O	79	b	98	o	111
C	67	P	80	c	99	p	112
D	68	Q	81	d	100	q	113
E	69	R	82	e	101	r	114
F	70	S	83	f	102	s	115
G	71	T	84	g	103	t	116
H	72	U	85	h	104	u	117
I	73	V	86	i	105	v	118
J	74	W	87	j	106	w	119
K	75	X	88	k	107	x	120
L	76	Y	89	l	108	y	121
M	77	Z	90	m	109	z	122

Les fonctions de hachage

Le premier ingrédient de la *blockchain* s'appelle une *fonction de hachage* : elle transforme n'importe quelle donnée en une chaîne de bits de longueur limitée (par exemple, 256 bits) appelée un *haché*. Une telle fonction présente forcément des *collisions*, c'est-à-dire des données différentes ayant le même haché, et elle doit aussi posséder certaines propriétés. En particulier, il doit être « difficile » (en un sens technique) de trouver une donnée ayant un haché spécifique.
La fonction de hachage est utilisée lors de deux moments clés du processus de validation d'une transaction avec la *blockchain* : l'enchaînement des blocs et l'objectif de hachage.

Dans cette activité d'introduction, une fonction de hachage H très simplifiée est présentée et manipulée. Elle sera utilisée par la suite sur notre version jouet de la *blockchain*. La fonction H est basée sur le code ASCII des caractères donné dans la table ci-dessus.

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

H(Pi314)
= ASCII(P) + ASCII(i)+ ASCII(3)
+ ASCII(1) + ASCII(4)
= 80 + 105 + 51 + 49 + 52 = 337.

Les élèves calculent le haché de « Tangente2023 » (lequel vaut 1022), ou de toute autre expression mêlant des majuscules, des minuscules et des chiffres.

La condition « les dix derniers chiffres » n'est pas utile dans l'activité, où les nombres restent « petits ». Ce-

Le hachage dans la « vie réelle »

Les fonctions de hachage utilisées dans la « vie réelle » sont par exemple SHA-256 ou BCRYPT.
Ainsi, dans Bitcoin, valider une transaction représentée par une chaîne T, lorsque la valeur du dernier bloc de la chaîne est P, consiste à trouver un nombre N tel que SHA-256(SHA-256(P, T, N)) soit inférieur ou égal à une certaine valeur, automatiquement modifiée à chaque bloc pour que ce calcul prenne toujours environ dix minutes.

pendant, on l'explicite ici pour sensibiliser au fait que 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. Ce n'est pas gênant pour l'activité proposée plus loin, mais une telle fonction de hachage n'est pas cryptographiquement sûre (voir encadré).

Mineurs et fermes de calcul

La *blockchain* archive toutes les transactions en *bitcoins* effectuées depuis la création de cette monnaie. La validation de chaque nouvelle transaction ajoute un « bloc » à la chaîne, dont le contenu dépend de cette transaction (la date, le client, le vendeur, le montant…), et de la valeur du bloc précédent de la chaîne. 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 : la chaîne de blocs 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 pour valider des transactions sont appelés des *mineurs*, en référence aux véritables mineurs qui extraient de l'or, car ce travail produit des *bitcoins*. Leur tâche consiste en partie à effectuer un long calcul cryptographique. Lorsqu'un mineur réalise en premier ce calcul pour une transaction, celle-ci est 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* ! En 2023, les mineurs sont des sociétés qui possèdent des *fermes de calcul* regroupant des milliers de machines.
Dans l'activité proposée ici, les élèves jouent le rôle de mineurs réunis dans des fermes de calcul en concurrence pour miner des *bitcoins*.

Objectif de hachage et preuve de travail

Le nom technique du calcul cryptographique que les mineurs s'efforcent de réaliser 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 fournit comme justification un nombre appelé *preuve de travail*. Le calcul est long, mais ensuite, n'importe qui peut vérifier facilement que le nombre remplit bien l'objectif.
Dans notre activité, pour valider par exemple la transaction « Alice donne cinq 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 un nombre N de telle sorte que H(H(45A5BN)) soit divisible par 5 et 3, 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 :

H(45A5B8)
= ASCII(4) + ASCII(5) + ASCII(A)
+ ASCII(5) + ASCII(B) + ASCII(8)
= 52 + 53 + 65 + 53 + 66 + 56
= 345.

Puis H(345) = H(3) + H(4) + H(5) = 156.
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 proposé ici ressemble dans la forme à celui utilisé dans Bitcoin, tout en donnant lieu à des calculs réalisables par des élèves.

Des mineurs en activité

L'enseignant choisit et affiche au tableau une liste de transactions à valider (du type A5B, en faisant varier les initiales et les montants) ainsi que la valeur du dernier bloc en date de la chaîne.
Pour commencer, chaque groupe d'élèves sélectionne une transaction, puis s'efforce de remplir l'objectif de hachage correspondant. En reprenant notre exemple, avec 45 comme état initial de la *blockchain*, et A5B comme transaction, la valeur N = 59 convient puisque :

H(45A5B59)
= ASCII(4) + ASCII(5) + ASCII(A)
+ ASCII(5) + ASCII(B) + ASCII(5)
+ ASCII(9)
= 52 + 53 + 65 + 53+ 66 + 53 + 57
= 399.
Or H(399)
= ASCII(3) + ASCII(9) + ASCII(9)
= 51 + 57 + 57 = 165,
qui est bien divisible par 3 et par 5. D'autres valeurs sont possibles pour N, comme 68 ou 89.

Le premier groupe d'élèves qui trouve une valeur de N correcte pour la transaction qu'ils ont choisie l'annonce publiquement, ainsi que la valeur du nouveau bloc (ici, 165 est ajouté au tableau, à la suite de 45), puis valide la transaction correspondante (ici, Alice paye cinq unités à Bob) en la barrant sur la liste affichée et remporte une récompense (des sucreries ou un score) à se partager.
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 ferme de calcul, il est essentiel que les élèves de chaque groupe s'organisent pour exécuter les tâches en parallèle. Par exemple, ils peuvent se partager les nombres par paquets de dix.
Par la suite, cette activité peut motiver le codage de l'algorithme de recherche exhaustive de N.

L'activité vise à présenter quelques aspects du fonctionnement de la *blockchain* en utilisant des calculs simples. Elle met l'accent sur les notions d'objectif de hachage et de preuve de travail, et sur l'aspect distribué du minage. Elle permet d'initier les élèves à certains principes de la cryptomonnaie décentralisée Bitcoin. Comme toute métaphore, elle ne reflète que partiellement la réalité. En particulier, la vérification de l'existence et de l'approvisionnement des comptes, la création de nouveaux *bitcoins* par le minage, l'évitement de la double dépense et le coût énergétique du minage ne sont pas abordés. Pour en savoir plus sur ces aspects, vous pouvez consulter les références proposées.

P. L. & M. M.

Références

- *Les blockchains en 50 questions*. Jean-Guillaume Dumas, Pascal Lafourcade, Ariane Tichit et Sébastien Varrette, Dunod, 2022.
- *Le Bitcoin, première cryptomonnaie*. Jean-Paul Delahaye, *1024* 4 (Bulletin de la Société informatique de France), 2014.
- La page « Autour du *bitcoin*, des monnaies cryptographiques et des *blockchains* » administrée par Jean-Paul Delahaye (**cristal.univ-lille.fr/~jdelahay/LeBitcoin**).