**Blolckchain : Le fonctionnement de la preuve de travail de Bitcoin**

**Pascal Lafourcade**

**En 2009 Satoshi Nakamoto a créé Bitcoin, la première crypto-monnaie décentralisée. Cette découverte repose sur des primitives cryptographiques et sur la technologie blockchain. L’objectif de cette activité est de faire découvrir le fonctionnement de Bitcoin, plus précisément du fonctionnement de la preuve de travail qui est au centre de cette crypto-monnaie.**

Une séance. Groupes d’élèves.

**Objectif :**Découvrir le fonctionnement de Bitcoin.

**Compétences travaillées :**

• calculs en arithmétique modulaires.

• critère de divisibilité ;

• algorithmes distribués.

Dans les années 1980, le cryptographe David Chaum a proposé la première monnaie électronique reposant sur de la cryptographie « DigiCash ». C’est le début des crypto-monnaies. Le challenge est de concevoir des pièces numériques qui ont au moins es mêmes propriétés que les pièces de monnaie physiques qui régissent l’économie et existent depuis des siècles. Dans un monde dématérialisé il est très simple de dupliquer une pièce en faisant un copier-coller. Or il est important de ne pas pouvoir dépenser deux fois la même pièce afin de garantir la stabilité du système. Pour cela l’idée de David Chaum est qu’une fois une pièce reçue par un individu il doit la refaire valider auprès de la banque pour avoir une nouvelle pièce valide. Ainsi la banque assure qu’une pièce n’est pas dépensée deux fois. Le principe des chèques bancaires est très similaire au principe du système proposé par David Chaum. 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 comprendre le principe de création des pièces dans Bitcoin et donc de comprendre le fonctionnement de la preuve de travail.

**Première Partie : Fonction de hachage naïve.**

Un exemple de fonctionnement de la fonction de hachage naïve utilisée dans cette activité est présenté et la table ASCII est donnée.

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

Les élèves doivent calculer le haché du mot « Tangente2023 » pour vérifier qu’ils ont compris le fonctionnement.

H(Tangente) = ASCII(T) + ASCII(a) + ASCII(n) + ASCII(g) + ASCII(e) + ASCII(n) + ASCII(t) + ASCII(e) + ASCII(2) + ASCII(0) + ASCII(2) + ASCII(3) = 84 + 97 + 110 + 103 + 101 + 110 + 116 + 101 + 50 + 49 + 50 + 51 = 1022.

**Deuxième Partie : Fonctionnement de l’algorithme de preuve de travail**

L’objectif de la preuve de travail dans Bitcoin est double. Le premier est de vérifier que les transactions sont valides et de les écrire dans la blockchain. Le second est de créer des nouvelles pièces pour récompenser les mineurs qui sont les personnes qui vont écrire dans la blockchain. Pour cela les mineurs sélectionnent des transactions de la formes suivantes : Alice donne 5 BTC à Bob. Dans cette activité cette transaction est modélisée par la chaîne de caractères A5B. Le mineur vérifier que le solde d’Alice contient bien 5BTC en parcourant la blockchain. Ensuite, il va effectuer une preuve de travail pour inscrire la transaction choisie sur la blockchain. Pour cette activité, il va prendre la valeur du block précédent, dénoté P, et il va chercher une chaîne de caractère N telle que : H(H(P,A,5,B,N)) soit divisible par 5 et 3.

Dans Bitcoin il doit chercher un nombre n tel que SHA-256(SHA-256(P,A,5,B,N)) soit plus petit qu’un objectif de hachage calculé à chaque block pour que ce calcul prenne environ 10 minutes.

Dans l’activité la valeur de P est fixée à 42 et les élèves doivent trouver une valeur de N qui satisfait l’algorithme de la preuve de travail.

Une solution possible est N=89 car H(H(42,A,5,B,89)) = H(399) = 165 qui est bien divisible par 3 et 5.

Le premier élève qui a trouvé remporte 50 BTC et annonce la valeur trouver comme la valeur du block courant. Ici pour valider la prochaine transaction il faudra prendre 165 comme valeur de P.

**Comment être sûr qu’il ny a pas de double dépense** ?

En effet il est possible de que deux mineurs valident en même temps d’une part la transaction A5B et d’autre part la transaction A5C, avec le solde du compte d’Alice qui n’est qu’à 5 BTC. Dans cette situation Alice a bien dépenser deux fois ses pièces. Chaque mineur a bien respecté le protocole et a fait une preuve de travail correcte. Les mineurs vont donc continuer la blockchain sur deux chaînes différentes et accepter pendant un temps que cette double dépense. Mais in fine c’est la chaîne la plus longue qui sera la seule chaîne valide, annulant ainsi une des deux transactions. Si cette transaction annulée est toujours valide (c’est-à-dire le solde du compte d’Alice contient suffisament de BTC) alors elle sera validée plus tard par un autre block. Pour en savoir plus sur le fonctionnement de Bitcoin veuillez consulter l’ouvrage [1]

**Conclusion**

Cette activité vise à expliquer le fonctionnement de la preuve de travail de Bitcoin en utilisant des calculs simples qui utilisent la table ASCII et un critère de divisibilité simple. Cela montre comment le système décentralisé Bitcoin fonctionne.

**Adaptation**

* Pour des lycéens, il est envisageable de coder ces algorithmes en Python.

**RÉFÉRENCES**

[1] 50 questions sur la Blockchain.