Exposé - Histoire de l'informatique

Bitcoin : Consensus de Nakamoto, preuve de travail et immutabilité

yogg

bitcointalk.org

4 octobre 2018

SHA-256

Le SHA-256 est une fonction cryptographique qui sert à calculer l'empreinte (hash) d'un ensemble de données de taille quelconque.
C'est une fonction déterministe qui produira partout et toujours le même hash avec la même entrée. Un hash de SHA-256 a une longueur de 64 digits hexadécimaux (256 bits).
Cette fonction est utilisée pour prouver un ensemble de données.

Preuve de travail

Hashcash (2002), Adam Back :
Un des premiers systèmes de preuve de travail (SHA-1). Il a été crée pour lutter contre le spam.
Le serveur demande à l'utilisateur de calculer différents hash plusieurs milliers de fois pour trouver un hash SHA-1 spécifique avant d'envoyer son message.
En conséquence, si cette validation nécessite 0,5s de calcul pour un utilisateur légitime, elle prendra un million de fois 0,5s à un spammeur pour envoyer un million de messages.

SHA-256 & preuve de travail

`sha256("coucou")` produit :

- hash en hexadécimal :
  110812f67fa1e1f0117f6f3d70241c1a42a7b07711a93c2477cc516d9042f9db
- hash en binaire :
  0001 0001 0000 1000 0001 0010 1111 0110 0111 1111 1010 0001 1110 0001 1111 0000 0001 0001 0111 1111 0110 1111 0011 1101 0111 0000 0010 0100 0001 1100 0001 1010 0100 0010 1010 0111 1011 0000 0111 0111 0001 0001 1010 1001 0011 1100 0010 0100 0111 0111 1100 1100 0101 0001 0110 1101 1001 0000 0100 0010 1111 1001 1101 1011

Quelle est la probabilité d'obtenir un hash :

- avec le premier bit à 0 ? $\rightarrow$ 50%
- avec les 2 premiers bit à 0 ? $\rightarrow$ 25%
- avec les 8 premiers bit à 0 ? $\rightarrow$ 0,390625%

Cela devient exponentiellement plus difficile de trouver un hash lorsqu'on augmente le nombre de bits à 0 requis au début.

La preuve de travail dans bitcoin

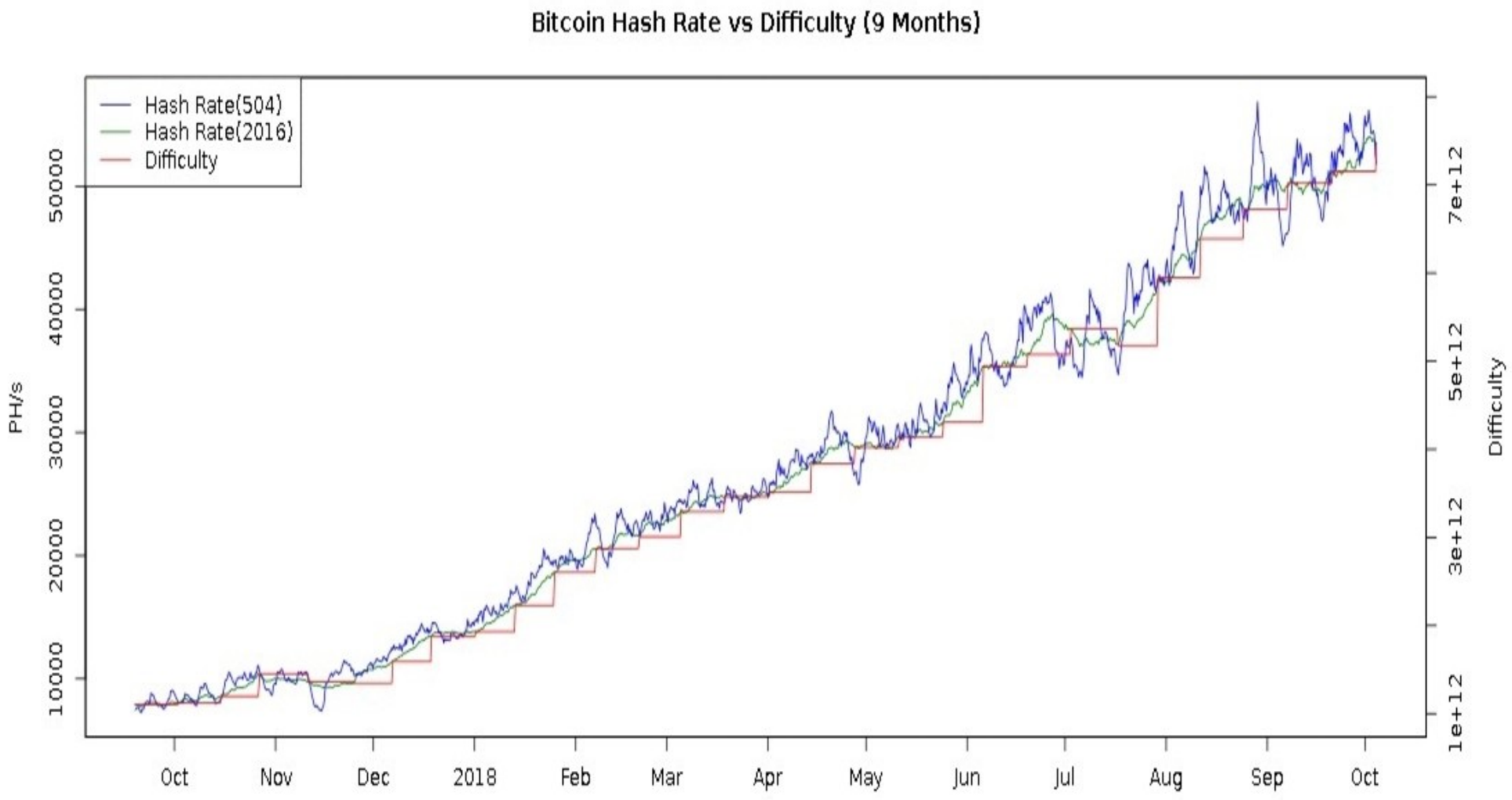
Un hash peut être vu comme un nombre.
Avec bitcoin, la preuve de travail utilise des valeurs numériques et considère un hash comme un grand nombre.

Si le critère pour résoudre la preuve de travail est :
- Le hash produit doit commencer par $0000_{(16)}$

Cela signifie qu'il faut produire un hash *plus petit* que 16^{64-4}, soit 2^{256-16}. Ce nombre est la *cible*.
Plus la cible est petite, plus la difficulté augmente pour résoudre la preuve de travail.

La cible est recalculée tout les 2016 blocks. (2 semaines)
Cet ajustement prends en compte la vitesse du réseau au moment du recalcul.
Le but est de continuer à avoir des blocks toutes les 10 minutes en moyenne.

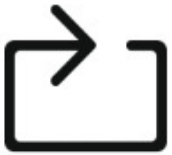
Puissance de calcul et difficulté



Comment résoudre la preuve de travail ?

Cherchons à valider la chaine "coucou" :
Pour cela, on utilise un nombre qu'on incrèmente, la nonce, et il n'existe qu'une seule façon : faire le travail !

```
sha256(coucou0) => bd175492f3a2f7515e1e7597d16979d8d85a3f307e6e392cc4dcecb27035a950
sha256(coucou1) => fae8b039d63e3ce5b178d685352f13387c684146eecb667dea1c3924522fd388
sha256(coucou2) => a37f701e4ca52e94e0ef7674108baf53dc15315201cf88681cad6889d3f3583c
sha256(coucou3) => 376b541264590bd74efed9e94d5e6fecc1a9cea20713c52c6dc85190d9199f72
sha256(coucou4) => a46ff2fd68eaa3a162c9233e8acbf7598e4b7209f86497c7331cfd18b70e5f60
sha256(coucou5) => f22187b27955e37c49184143980d341666a281eeb917d26f90fbe56645e8d252
sha256(coucou6) => b040b014ed64509d93f0c6d02e2972344fff1a836c83b895ed6c1f3387b94783
```



Tant qu'on a pas trouvé un hash qui satisfait les critères
on incrémente la nonce et on calcule le hash.

```
sha256(coucou103547) => 990734ee49009a14a7ebea4cb02bdc4361abfd73dc945bbc25c02958abfb697e
sha256(coucou103548) => f07f35314ad71bc85b55d6fec5ba24dfcf1a0d1788e54988fb2856e990b47e5d
sha256(coucou103549) => 277cd5e3c2b06bfb8c3f1a0a0f8a80384f496de751afe5c8ac1a2c1d18c46736
sha256(coucou103550) => 9741b8edf942b05648b40c7d4b0b718175edf3acdce4b10afe31cc76f1e69186
sha256(coucou103551) => 0000d138e73ad6dd3ab2c1a2b4ef02ae586e9f5aa6d71015af7760295c499d16
```

Aujourd'hui dans bitcoin

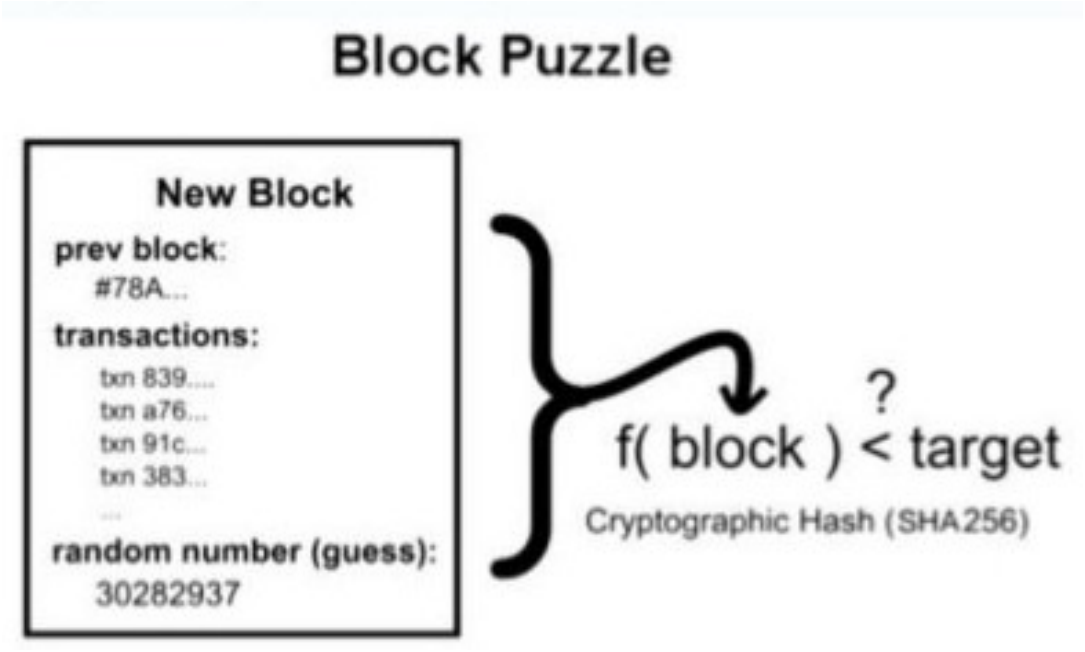
Height	543342 (Main chain)
Hash	0000000000000000000015185737f8ccdc882f28305b3507e1a4f014f550d3f77a
Previous Block	0000000000000000000019892d00b8e6554edbf03932f3b7f706b2885c7137bacc
Next Blocks	
Time	2018-09-27 20:08:55

Pour trouver ce hash, un mineur a utilisé le header du block, une structure de données connue qui contient des transactions, la date et l'heure, et quelques autres données. Ce header est comme le coucou de l'exemple.
Ce hash nous dit plusieurs choses sur le mineur :

- Il a fait des milliards de milliard de SHA-256 en quelques minutes.
- Il doit avoir un matériel très sérieux à disposition.
- Il a alloué une certaine quantité d'electricité pour trouver la peuve de travail.

Ce dernier point est crucial.

Les principes du consensus



Les mineurs construisent chacun un bloc, et ils s'assurent qu'il soit valide d'après les règles du consensus. Il y'a environ 30-40 règles pour qu'un block soit valide, et aussi 30-40 règles pour définir si une transaction est valide.
C'est la fonction première des mineurs : faire le travail de validation des transactions.
Les noeuds du réseau valident indépendament chaque block.
Si le block est valide, il est rajouté à la copie de la blockchain qui est locale au noeud, et puis retransmis sur le réseau.
Si il n'est pas valide, le block est rejeté par les noeuds.

Scénarios

Mineur malhonnête

Que se passe t'il lorsqu'un mineur essaie de tricher ?

Fork

Un mineur argentin trouve un block, 0.2s après un mineur chinois.
Que se passe t'il ?

Concept d'immutabilité

Qu'est-ce que l'immutabilité ?

L'immutabilité n'existe pas.

L'échelle de l'immutabilité

Ce qui sécurise bitcoin

Bitcoin est il *tamper-evident* ou *tamper-proof* ?
Qu'est-ce qui lui confère ces propriétés ?

La preuve de travail dans notre civilisation

La robustesse du consensus de Nakamoto

Aujourd'hui, bitcoin consomme au moins 50TWh d'electricité par an.
Cela fait 137GWh par jour, soit 5,7GWh en une heure.
A titre de comparaison, la consommation totale d'électricité en France en 2014 a été de 478 TWh.

Scénario

Un gouvernement investit massivement dans du matériel de minage, et acquiert 51% de la puissance de calcul.
Que se passe t'il ?

Références

- *Bitcoin: A Peer-to-Peer Electronic Cash System*, Satoshi Nakamoto
- *The Internet of Money* (vol 1 & 2), Andreas Antonopoulos