FONCTIONS DE HACHAGE

Une fonction de hachage est une fonction mathématique, très souvent utilisée dans le domaine de la cryptographie, qui permet de calculer ce que l’on appelle une empreinte numérique (un hash) qui est une chaine de bits permettant de caractériser un fichier, au même titre qu'une empreinte permet d’identifier une personne.

Il existe différents types de fonction de hachage, les plus connues étant les algorithmes MD5 et SHA-2 ([SHA-256](https://fr.wikipedia.org/wiki/SHA-256), [SHA-384](https://fr.wikipedia.org/wiki/SHA-384) ou [SHA-512](https://fr.wikipedia.org/wiki/SHA-512) selon le nombre de bits)

Par exemple, la fonction [SHA-256](https://fr.wikipedia.org/wiki/SHA-256) est celle utilisée pour la blockchain du bitcoin.

Un hash est une suite d’un certain nombre de bits. Pour faciliter la lecture d’un hash, on traduit la chaine de bits en hexadécimal.

Un hash est une solution au problème de la signature d’un fichier. En effet, généralement une signature électronique a la même taille de stockage que son fichier. Donc si l’on souhaite réaliser une signature électronique pour un fichier de 10Go, alors la signature fera également 10Go.

Or, si l’on ne choisi de prendre que le hash de la signature électronique on gagne énormément de place de stockage car un hash ne prend que très peu d’espace de stockage. En ce qui concerne la sécurisation des mots de passe, il faut savoir qu’un disque dur ne stocke pas les mots de passe eux même, mais plutôt leur hash. Donc lors d’une authentification on compare le hash du mot de passe avec le hash de la chaine de caractères saisie.

Cela sert également à vérifier l’intégrité d’un fichier (savoir si le fichier n’a pas été modifié) car si un fichier est modifié alors son hash change automatiquement.

Enfin, cela permet également de sécuriser des BlockChain.

Afin d’obtenir une chaine de bits pour un fichier, la fonction de hachage va procéder à de nombreuses applications que l’on appelle « portes logiques ».

Les portes logiques sont des circuits combinatoires simples. Elles sont la base de la logique mathématique qui effectue les opérations à l'intérieur du processeur, c’est la base de tous les calculs internes du processeur. Les portes logiques sont à l'origine de tous les calculs effectués dans les transistors. Leur fonctionnement étant basé sur le passage éventuel du courant, elles ne peuvent que traiter des informations en langage binaire. Enfin l'association de portes logiques permet de traiter une instruction du microprocesseur.

C’est donc grâce à ces applications que l’on obtient des chaines de bits.

Les applications le plus connues sont le NOT, le AND, le OR ou encore le XOR.

De façon générale, une fonction de hachage va « découper » un fichier en différents morceaux d’un certain nombre de bits puis elle va lui appliquer différentes applications selon l’algorithme utilisé.

La fonction de hachage est effectuée dans le but de pouvoir résister aux collisions, c’est-à-dire deux fichiers qui donnent le même hash.

Il y a tout de même un problème, nous n’avons actuellement aucune preuve mathématique qui permet de prouver qu’il existe une fonction de hachage pour laquelle il serait difficile, voire impossible de calculer des collisions.

Cependant, il existe plusieurs algorithmes de hachage, donc si ce problème survient sur un algorithme, il suffit de le remplacer cet algorithme par un autre.

Par exemple, en 2004, une équipe de recherche chinois a trouvé un moyen afin de calculer des collisions pour l’algorithme MD5 en une heure. Il est donc à présent déconseillé d’utiliser cet algorithme.