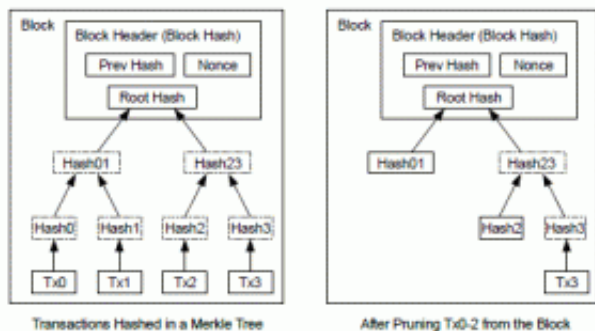




Comment ça marche les bitcoins (5)



Précédemment, sur ce blog, nous avons vu comment les [blocs de bitcoins sont découpés en transactions](#). Ce qui ne vous a, finalement, avancé que sur le mystère de comment un simple petit bloc de quelques octets peut contenir des milliards de satoshis.

Vous n'en savez par contre toujours pas plus sur comment ces transactions sont incluses dans la chaîne de blocs ni comment on va bien pouvoir se débrouiller pour que cette chaîne ne devienne pas énorme au fur et à mesure qu'elle enregistre des transactions.

J'ai un peu menti par omission dans les articles précédent. Lors de la fabrication d'un bloc, il n'y a pas que le hash du bloc précédent et un nombre à trouver qui entrent en ligne de compte. L'ensemble des transactions déjà validées et pas encore incluses dans la chaîne sont à prendre en compte lors du calcul.

La chaîne qui doit être hachée deux fois pour trouver une chaîne contenant le nombre de zéros requis au début est donc composée du double hash du bloc précédent, du hash des transactions en attente d'inclusion et de quelques autres données (chaîne aléatoire, version du logiciel utilisé, timestamp, première transaction affectant le bloc à son mineur...).

L'avantage de cette méthode, c'est qu'un bloc peut contenir autant de transactions qu'on le souhaite et qu'il n'y a absolument pas besoin d'aller toucher aux blocs précédents lorsqu'une transaction a lieu. On est, en prime, certain de pouvoir, à un instant T, retrouver l'ensemble des transactions ayant été effectuées puisqu'elles sont toutes inscrites dans un bloc ou dans un autre. La traçabilité est donc garantie. Là où c'est un peu déroutant, c'est qu'une transaction n'est pas nécessairement inscrite dans le bloc contenant les bitcoins dont elle fait l'objet.

Abordons à présent le petit bout de théorie de Merkle qui va nous permettre (ça n'a, à priori, pas encore été mis en route dans les logiciels utilisés actuellement sur le réseau bitcoin) de gagner de l'espace disque et d'éviter que, dans 20 ans, la chaîne de bitcoins pèse plusieurs Go.

Il y a deux schémas de données imbriqués :

- D'une part, chaque transaction est enregistrée chronologiquement dans les blocs en fonction du moment où elles interviennent, chaque bloc contenant un hash de



l'ensemble des transactions qu'il contient.

- D'autre part, chaque transaction fait référence à une transaction (très probablement enregistrée dans un autre bloc) précédente pour assurer la traçabilité de qui a combien de bitcoins.

En regardant le second schéma, on se rend donc compte que les transactions forment un arbre qui commence par la fausse transaction attribuant tous les bitcoins du bloc à son mineur et se terminant par l'ensemble des transactions n'ayant pas de transactions suivantes et qui composent donc la répartition actuelle de l'ensemble des bitcoins.

L'idée étant qu'une transaction totalement dépensée (c'est à dire qu'il existe une ou plusieurs autres transactions ultérieures qui répartissent la totalité des bitcoins de la transaction d'origine) n'a pas besoin d'être conservée outre mesure si l'ensemble des sous-transactions qui vont après ont été déjà validées par le réseau, les nouvelles transactions se basant uniquement sur des transactions non totalement dépensées.

Le premier schéma est celui de l'enregistrement réel des transactions dans la chaîne. Il s'agit d'un arbre binaire comprenant autant de branches finales que de transactions à valider. Chaque niveau de l'arbre hash deux entrées du niveau inférieur (voir le schéma en tête d'article ou dans le [doc d'origine](#), page 4). Pour permettre de vérifier que le hash racine (Merkle Root) inclus dans le bloc est toujours bon, on conserve toujours au moins un niveau de hash ainsi que tous les sous-hash permettant d'aller vérifier les transactions qui n'ont pas encore été dépensées et qui ne peuvent donc être supprimées.

La beauté de la chose est que chacun est libre ou pas d'effectuer cette compression : le but du jeu est d'alléger la charge pour la quasi totalité des gens, sauf quelques malades qui prendront plaisir à conserver l'ensemble de la chaîne... pour pas grand chose si ce n'est la gloire de conserver tout l'historique monétaire.

Si vous avez tenu jusqu'ici sans lâcher, je vous tire mon chapeau, et je vous avoue humblement que j'ai découvert tout ceci au fur et à mesure que j'écrivais les articles, ce qui explique en partie les approximations de certains articles corrigées dans le suivant.

Si vous avez des questions, faites vous plaisir, j'ai pas d'autres idées sous la main pour la suite mais je peux continuer la série « on demand » :)