Bitmessage, le bitcoin de l'email

A la faveur d'un article de l'ami Korben, Bitmessage a débarqué sur le devant de la scène people en France la semaine dernière.

De quoi s'agit-il exactement ? D'un réseau peer to peer de messagerie chiffré. Les principes de base sont les mêmes que le bitcoin (voir ma série sur le sujet) :

- Aucune autorité centrale d'aucune sorte (pas même l'infrastructure DNS)
- Chiffrement de bout en bout
- Diffusion par inondation totale de l'ensemble du réseau (ou presque)

Les mécanismes mis en jeu sont toutefois plus simple que le bitcoin, l'historique n'ayant pas besoin d'être conservé à long terme pour assurer la traçabilité d'une monnaie.

Lorsque vous lancez le client bitmessage pour la première fois, vous allez créer une adresse, par exemple BM-2DACG68CuqSrLHxyXdWug3nZZxhBn6cQTt. Celle-ci contient un hash (si vous avez décroché, allez lire la série sur le bitcoin) de votre clé publique. Lorsque vous allez envoyer un message, à une autre adresse de la même forme, donc, votre client bitmessage va générer une demande pour obtenir la clé publique correspondant au hash de l'adresse de votre destinataire pour pouvoir chiffrer le message.

Cette demande va parcourir l'ensemble du réseau jusqu'à tomber sur le destinataire en question qui va répondre avec sa clé publique. Puisque vous disposez du hash de cette clé, le logiciel pourra vérifier rapidement que la clé qu'on vous a fournie est la bonne, puis chiffrer votre message avec, le signer avec votre propre clé, et renvoyer le tout sur le réseau. Pour être valable, ce paquet doit, comme dans le cas du bitcoin, faire l'objet d'un travail sur son hash en SHA256 pour tomber sur un certain nombre de zéros dans le hash. Le protocole est prévu pour qu'un ordinateur lambda mette 4 minutes à accomplir ce travail.

Une fois envoyé, chaque membre du réseau tente de déchiffrer chaque message. S'ils n'ont pas la bonne clé privée, c'est peine perdue, sinon, le message est déchiffré, et la signature vérifiée à partir de votre clé publique contenue dans le message, elle même vérifiable par le hash qui est inclus dans votre adresse bitmessage.

C'est, comme bitcoin, brillant de simplicité et d'efficacité. Car non content de permettre le chiffrement de bout en bout sans recourir à aucun artifice de type échange et vérification préalable de clé ou autorité centrale, bitmessage permet efficacement de lutter contre le spam, puisqu'il faut, quoi qu'il arrive, 4 minutes pour fabriquer un seul et unique message, rendant le spam trop cher pour être efficace. Il est même possible pour chacun de définir un facteur de

difficulté plus élevé pour obliger les correspondants à travailler plus pour vous envoyer un message.

Les performances du système, en cas d'utilisation massive, ont même été pensées : le réseau pourra se hiérarchiser de lui même pour éviter que chaque participant doive tester l'ensemble des messages transmis. Ce petit artifice est réalisé par la constitution d'un arbre de flux de messages. Pour faire simple, on peut comparer ce fonctionnement à celui du courrier classique : lorsque vous envoyez une lettre dont la destination est dans la même ville que vous, elle ne va pas sortir de la ville. Par contre, quand vous écrivez à quelqu'un à l'autre bout du monde, votre courrier va parcourir un certain nombre de points de collecte.

Même si la version actuelle de bitmessage est un peu rébarbative, je vous invite à jouer avec et à suivre ses évolutions ! Vous pouvez me causer à la maison
sur BM-2D7AjVjnrV2fFbZ9SYHfxfkjfbPntpEEJQ et au bureau
sur BM-2DACG68CuqSrLHxyXdWug3nZZxhBn6cQTt :)

(Et puis si vous ne faites rien jeudi vers 14h, je parlerai bitcoin & bitmessage avec qui voudra venir dans le cadre de Pas Sage en Seine. Rendez-vous aussi vendredi à 17h au même endroit pour une conf sur @maisonquitweet !)