Cryptomonnaie : la seconde génération

Vous avez probablement suivi ma petite série sur le bitcoin. Si ce n'est pas le cas, prenez une bonne dose d'aspirine et lancez vous dans la lecture, sinon, vous serez paumés dans le présent billet.

Voici venir la seconde génération de cryptomonnaie, NXT en tête.

De quoi s'agit-il ? Non, pas d'une Nième version du Bitcoin avec quelques ajustements. Il s'agit principalement d'une refonte du principe de base. Le bitcoin est majoritairement basé sur le « Proof-of-Work » (PoW) qui, si on schématise, donne la masse monétaire créée à ceux qui mettent les plus grosses ressources techniques à disposition du réseau. Il utilise également un peu du « Proof-of-Stake » (PoS) qui consiste à rémunérer les créateurs de blocs avec les commissions de transaction.

NXT, lui, élimine quasi totalement le PoW, permettant de constituer un réseau qui ne demande pas une énergie phénoménale. Il est en ce sens un peu plus égalitariste et carrément plus écolo, un simple Raspberry Pi suffit à « miner » (dans le monde du NXT, on dit « forger »).

Petit bémol : la problématique connue sur le bitcoin (les premiers mineurs sont assis sur un tas d'or monstrueux) se retrouve également dans NXT puisque l'ensemble de la monnaie (1 milliard de NXT) a été émise par le premier bloc et partagée entre les 73 fondateurs. Ceci étant, ils semblent décidés à dilapider ce capital en le donnant aux nouveaux arrivants, rétablissant ainsi une sorte d'égalité. On reste tout de même dans un schéma pyramidal, puisque les premiers servis seront sans doute les plus riches de demain en ayant amassé un capital, au détriment des derniers qui devront trimer pour obtenir des NXT de la part des premiers.

Vivement la 3ème génération qui implémentera le « Proof-of-Unique-Life » (PoUL) permettant d'appliquer les concepts de revenu de base aux cryptomonnaies et, pourquoi pas, une notion de dévaluation de la valeur de l'argent stocké évitant l'effet capitalisation.

Pour se lancer dans le NXT, rien de plus simple, il suffit de télécharger le client pour son OS et de le lancer. Une fois passée l'inévitable étape de téléchargement de la blockchain, on peut commencer à jouer avec.

Passons maintenant aux petites choses croustillantes qui font la particularité des NXT :

L'ensemble des NXT existant est issu du premier bloc de la blockchain, lui-même forgé par le « genesis account ». Mais, contrairement aux bitcoins qui naissent du néant, les NXT sont nés de la séparation d'avec les AntiNXT qui sont tous propriété du genesis account.

Du coup, contrairement au bitcoin où la monnaie peut être perdue mais pas détruite, les NXT peuvent être détruits : il suffit de les renvoyer au genesis account pour qu'ils rencontrent leurs alterégos AntiNXT et disparaissent corps et âme, comme la matière disparaît (théoriquement) au contact de l'antimatière. L'histoire ne dit pas (encore) ce qui est fait de l'énergie de la rencontre d'un NXT avec un Anti-NXT.

On peut accéder au genesis account (NXT-MRCC-2YLS-8M54-3CMAJ) avec la passphrase « It was a bright cold day in April, and the clocks were striking thirteen. » (tirée de 1984, pour les connaisseurs) où on constatera qu'il y a déjà quelques 3022 NXT qui y ont été envoyés et qui ont donc été détruits puisque le solde est de -999996978.

Le protocole interdit l'émission de transaction depuis des comptes à soldes négatifs, ce qui est logique, puisqu'il serait possible de détruire la monnaie à distance en envoyant des AntiNXT.

Un petit mot sur la sécurité à présent. Dans l'immense majorité des cryptomonnaies, la clé privée qui protège la monnaie d'un utilisateur est générée par la machine. Dans le cas de NXT, vous êtes libres de la choisir. Du coup, évitez de choisir « 1234? … Il suffit, pour vous en convaincre, de regarder l'état du compte dont la clé est 1234 : une seule transaction de 4 NXT presque immédiatement redépensée.

Des cohortes de robots scrutent les transactions en live à la recherche de destinataires connus de ce genre pour aller piquer l'argent dans la foulée.

Si vous avez bien lu l'identifiant du genesis account, vous avez remarqué comme il semble court et simple comparé à une adresse bitcoin. Tous les identifiants sont sur le même format. Une discussion a eu lieu à ce sujet fin 2013 en amont du lancement du projet. Concrètement, il existe effectivement une multitude de phrases secrètes qui mènent à la création d'un même identifiant de compte, c'est pour cela que la sécurité d'un compte n'est garantie qu'après avoir dépensé au moins une fois un bout de NXT, ce qui permet la publication de la clé publique complète auprès de tous les membres du réseau qui n'accepteront ensuite plus aucune transaction vers un identifiant partiel commun mais à une clé publique différente.

Namecoin avait, il y a quelques temps, posé les base des alias utilisés dans NXT. L'idée est d'enregistrer, dans la blockchain, des correspondances. Par exemple « Spyou » => « http://blog.spyou.org » et « Spyou-code-CB » => « 1234?. Chaque création d'alias coute 1NXT (qui va dans la poche de celui qui forge le bloc qui contient l'alias). On peut ainsi

constituer un système ressemblant au DNS.

Le créateur d'un alias peut bien entendu le modifier en le recréant.

Pour finir cette introduction aux cryptomonnaies nextgen, comme pour bitcoin, la blockchain ne sert pas nécessairement qu'à transférer des fonds. On peut s'en servir pour papoter (comme l'implémentation twister de la blockchain bitcoin ou bitmessage dans le même genre), pour voter (j'ai pas encore tout exploré de ce côté) ou bien pour échanger des biens, services ou même concepts.

Peu après la naissance du bitcoin est apparue la notion de « colored coin ». Il s'agit d'une transaction particulière qui transmet également d'autres informations.

Jusqu'à présent, ces biens ne pouvaient pas être échangés directement dans le protocole. Il fallait acheter les unités de monnaie les représentant, souvent via une place de marché externe et centralisée qui supervisait la transaction, cassant l'intérêt de la décentralisation des cryptomonnaies.

NXT solutionne le problème avec les assets. On peut émettre un asset contre des NXT (1000 au minimum). Ces 1000 NXT vont au créateur du bloc qui validera la création de l'asset (comme une transaction). L'idée est d'éviter que des assets fantaisie soient créés.

Un asset peut être à peu près ce qu'on veut : une réduction dans un magasin, une part de capital dans une entreprise, un kilo de fromage…

Là où ça devient intéressant, c'est qu'on peut vendre tout ou partie de ses assets pour le prix qu'on veut, en peer2peer, sans aucune autorité centrale.

Exemple typique, je veux monter une petite affaire de vente de bracelets loom-bands. J'ai trouvé quelqu'un pour me vendre des élastiques pour 10000NXT et je peux faire 100 bracelets avec cette matière première. Je vais donc créer un asset « loom-bands » avec 100 parts que je vais vendre 120 NXT chacune. La contrepartie promise est d'obtenir un bracelet quand je les aurai faist.

Je vais donc réunir théoriquement 12000 NXT (si je me débrouille bien), dépenser 10000NXT pour acheter mes élastiques et garder 2000NXT pour ma pomme. Quelqu'un peut donc vulgairement acheter un bracelet pour 120 NXT.

Sauf qu'entre le moment où j'ai créé cet asset et le moment où je vais finaliser les bracelets et les envoyer, je suis devenu une célébrité incontournable du loomband et mes créations s'arrachent 12000 NXT pièce : n'importe qui ayant acheté un asset peut le revendre à qui voudra bien l'acheter pour le prix qu'il veut.

Une variante peut être aussi de promettre aux gens ayant acheté mon asset un revenu mensuel de 3 NXT. Si ma petite affaire de bracelets marche bien, je vais donc les rémunérer chaque mois et ils pourront revendre leurs parts dans mon entreprise à qui ils voudront. On obtient donc

un marché du même type que ce qu'on connaît en économie classique sauf qu'il n'est pas tenu et réglementé par une institution : c'est l'ensemble des participants au réseau NXT qui le régule.

On peut même créer une cryptomonnaie par dessus NXT sur ce principe. Principe qui a d'ailleurs été appliqué à la création des NXT : le milliard d'unité de monnaie sorti du genesis bloc provient de la coloration de 21… bitcoins.

Accrochez-vous bien au pinceau, ce monde d'innovation décoiffe dur… Et si vous cherchez un compte à qui envoyer des NXT, pensez à NXT-NJEU-EL29-EHVX-6A6MH :)