Au secours, j'ai perdu mon nom Namecoin

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 mars 2016. Dernière mise à jour le 3 novembre 2017

https://www.bortzmeyer.org/maman-j-ai-perdu-mon-namecoin.html

---

J'ai déjà raconté ici comment j'avais enregistré dans la "*blockchain*" Namecoin le nom d/bortzmeyer, mon premier nom Namecoin <https://www.bortzmeyer.org/namecoin.html>. Eh bien, je l'ai perdu accidentellement et stupidement (puis récupéré après), et cette perte est l'occasion de regarder quelques faiblesses de Namecoin.

Pourquoi Namecoin ? Parce que, disent ses promoteurs, il permet l'enregistrement de noms de manière complètement pair à pair. En prime, depuis quelques mois, « "*blockchain*" » est devenu un "*buzzword*" et, justement, Namecoin utilise une "*blockchain*", un livre des opérations public, permettant une vérification par tous <https://www.bortzmeyer.org/tousapoil.html>. Mais les fans de Namecoin oublient de signaler que le prix à payer, pour cette indépendance vis-à-vis de tout organisme, est qu'il faut s'occuper de tout soi-même (par exemple faire sa gestion de clés cryptographiques) et que les erreurs ne pardonnent pas.

C'est une telle erreur que j'ai bêtement fait. Je n'ai pas renouvelé le nom. Il a donc été retiré, puis ré-enregistré mais par quelqu'un d'autre. Voyons les étapes, en utilisant un explorateur public <https://namecha.in/>. (Comme je l'ai récupéré par la suite, vous pouvez également chercher cette récupération.)

Le nom a été enregistré le 16 janvier 2014 <https://namecha.in/tx/29980b83702469fb954fd1f06f03b941ech
Il a ensuite été modifié, chaque modification remettant à zéro le compteur. Le dernier renouvellement (qui était juste un renouvellement, sans changement du contenu) a été fait le 22 janvier 2015 <https://namecha.in/tx/3393a1f8b428053c2b343deec3f3ff5ec10f360e9a7a82ae91606052c5edab76>. Non renouvelé, le nom d/bortzmeyer a expiré et a été ré-enregistré le 29 septembre 2015 <https://namecha.in/tx/1af7ef5e13c212eb00083e362838256fee3b8b9024dc34cf3f20e868772c038e>. Une seule donnée dans ce nom a été mise par le nouveau titulaire, le même jour <https://namecha.in/tx/b84d413feb0b08ae8b24e679d583c13df90ec2fec24bebc90891b927b09b0a91>. Cette donnée était une adresse BitMessage <https://www.bortzmeyer.org/bitmessage.html>. (Toute l'histoire peut se voir d'un coup en <https://namecha.in/name/d/bortzmeyer>. À noter qu'un autre explorateur de la "*blockchain*", plus connu mais plus bogué, ne voit pas le ré-enregistrement <http://explorer.namecoin.info/n/141015>.)

Pourquoi le nouveau titulaire a-t-il indiqué une adresse BitMessage <https://www.bortzmeyer.org/bitmessage.html> ? Probablement pour qu'on le contacte afin de payer une rançon pour récupérer le nom maladroitement perdu. Cette pratique semble assez courante dans le monde Namecoin en ce moment. Elle illustre l'absence de toute sécurité autre que technique : si on fait une erreur, ou qu'on est négligent, on est fichu. (J'ai écrit à l'adresse BitMessage en question, sans réponse, ce compte semble hors-ligne, mon client BitMessage ne reçoit pas sa clé publique, ou alors c'est que le réseau BitMessage ne marche plus.) Cette pratique d'enregistrer un nom abandonné est très répandu dans le monde des noms de domaine traditionnels.

Comme Namecoin est très peu utilisé en pratique, je ne m'étais même pas aperçu de la perte. J'étais abonné au système d'alarme Name Alert <http://namealert.mvps.eu/> mais celui-ci semble très bogué. Je n'ai pas reçu les messages prévenant que l'expiration approchait, et je n'ai reçu le message m'avertissant du nouveau contenu du nom que le 2 mars, plusieurs mois plus tard ! Cela donne une idée de l'état de l'écosystème Namecoin.

Par la suite, le détourneur a dû se lasser de ne pas avoir de proposition de rachat, et a laissé tomber le nom, que j'ai alors repris. (Cherchez avec les explorateurs, cela vous fera un bon exercice.) Si vous avez un résolveur DNS qui gère le `.bit`, vous pouvez à nouveau voir le nom :

```
% dig AAAA bortzmeyer.bit
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3037
...
;; ANSWER SECTION:
bortzmeyer.bit. 86257 IN AAAA 2605:4500:2:245b::42

;; AUTHORITY SECTION:
bit. 70716 IN NS ns5.opennic.glue.
bit. 70716 IN NS ns6.opennic.glue.
...
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Nov 03 09:39:55 CET 2017
;; MSG SIZE  rcvd: 264
```

Le problème de perte de noms est-il soluble ? Oui, bien sûr, on pourrait imaginer la mise en place d'un système de **notariat** où des notaires stockent les clés et renouvellent les noms pour le compte de leurs clients. Cela permettrait à des non-experts d'avoir des noms Namecoin, tout en préservant la liberté du choix : chacun serait libre d'utiliser le notaire qu'il veut. En l'absence d'un tel système, il y a peu de chance que Namecoin soit un jour adopté massivement.