Des leçons à tirer du problème du .coin

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 octobre 2022

https://www.bortzmeyer.org/blockchain-domaines-collisions.html

---

Le 18 octobre 2022, la société Unstoppable Domains a annoncé <https://unstoppabledomains.com/blog/coin> qu'elle arrêtait de vendre des noms sous .coin. Il y a des leçons intéressantes à en tirer.

Ces noms ont la syntaxe de noms de domaine mais ne « fonctionnent » pas, au sens où un nom de domaine habituel fonctionne, via une résolution par le DNS. Ils sont enregistrés, oui, dans une chaine de blocs, mais ne fonctionnent pas avec vos logiciels classiques. En pratique, ils sont très peu utilisés, ceux qui les achètent sont plutôt dans une démarche d'investissement, espérant qu'ils prendront de la valeur plus tard, plutôt que dans une démarche de présence en ligne, comme lorsqu'on achète un nom de domaine plus classique pour recevoir du courrier électronique ou afficher un site Web.

Plusieurs services analogues existent, certains commerciaux (on peut vendre des noms, des identificateurs), d'autres pas. C'est aussi un monde où on rencontre de tout, du marketing boursouflé (Web3 !), à certains vendeurs qui induisent en erreur leurs clients, par exemple en leur faisant croire que ces noms auront le même usage qu'un nom classique, utilisable via le DNS. Et il y a aussi de purs escrocs. L'intérêt, en théorie, d'enregistrer des noms dans une chaine de blocs, plutôt que via un registre traditionnel, est que la chaine fonctionne automatiquement, sans intervention humaine une fois lancée, et qu'on peut donc rester titulaire de son nom de domaine, sans risque de le voir saisi ou censuré (d'où le nom de la société Unstoppable Domains). L'idée est très ancienne (elle avait commencé avec Namecoin en 2010) mais a pris de l'ampleur ces dernières années, avec l'apparition d'intermédiaires comme Unstoppable Domains, ENS, Emercoin, etc. La vogue récente des NFT <https://www.bortzmeyer.org/nft.html> a mené certains à renommer leurs produits « NFT » mais il n'y a pas de changement de fond.

Un point important de toute cette offre est qu'il n'y a pas de coordination. Tout le monde (et son chat) peut créer une chaine de blocs ou, si on est moins ambitieux, un service de création de noms sur une chaine de blocs existante (la façon de réaliser un tel service avait été détaillée lors de la JCSA 2016 <https://www.afnic.fr/observatoire-ressources/actualites/jcsa16-retour-sur-la-journee-du->). L'Internet est « sans permission » ce qui veut dire, et heureusement, qu'une innovation peut être créée et déployée sur l'Internet, sans l'autorisation de personne. Cela a permis Bitcoin (qui a créé le

concept de chaine de blocs), BitTorrent mais aussi le Web (si Tim Berners-Lee avait dû patienter jusqu'à l'autorisation d'un comité, on attendrait toujours le Web). La contrepartie de cette liberté est qu'il y a aussi de mauvaises idées et des concurrences dommageables. Comme chacun (et son hamster) peut lancer un service de création et de vente de noms sur une chaine de blocs, si ces noms ont une syntaxe compatible, il y a des risques de **collision**. Une collision, c'est quand deux noms identiques sont enregistrés via des services différents. C'est inévitable si deux services vendent des noms avec le même suffixe.

Et c'est justement ce qui s'est produit ici : Unstoppable Domains vendait du `.coin` mais Emercoin le faisait également. Les collisions étaient donc inévitables. Finalement, Unstoppable Domains a décidé d'arrêter, notant qu'Emercoin était présent avant (mais qu'ils ne le savaient pas <https://twitter.com/unstoppableweb/status/1582401601691877377>). Notons l'ironie du nom Unstoppable Domains puisque cette entreprise peut supprimer un nom à sa guise…

Ces problèmes de collision sont inévitables dès que plusieurs organisations créent des noms sans aucune coordination. C'est une des raisons pour lesquelles les racines DNS alternatives <https://www.bortzmeyer.org/racines-alternatives.html> n'ont jamais décollé. Leurs promoteurs évacuent souvent le problème des collisions avec de vagues promesses « on s'arrangera ». Ici, un des deux acteurs impliqués dans la collision a décidé d'arrêter mais il n'y a aucune garantie que cela se passera toujours bien. C'est pour cela que le RFC 2826 [1] insiste sur l'importance d'une coordination formelle. Dit autrement, il ne faut qu'un seul registre pour `.coin` (ou `.nimporte-quoi`).

J'ai dit plus haut qu'Unstoppable Domains avait supprimé les noms en `.coin`. En fait, c'est plus compliqué que cela. Les noms sont toujours dans la chaine de blocs (dont l'un des buts est justement d'empêcher l'effacement du passé) et Unstoppable Domains peut donc expliquer qu'en fait, ils n'ont pas supprimé les noms. Mais, comme indiqué précédemment, presque aucune application ne va regarder directement dans la chaine de blocs. Elles passent quasiment toutes par des passerelles diverses, utilisant des protocoles normalisés comme HTTP ou DNS. Ce qu'Unstoppable Domains a coupé, comme ils l'indiquent <https://twitter.com/unstoppableweb/status/1582401612290568192>, ce sont ces passerelles. C'est en effet une malhonnêteté intellectuelle fréquente chez certains services se présentant comme pair-à-pair : le support (ici, la chaine de blocs) est bien pair-à-pair, mais en pratique presque tout le monde y accède via une passerelle qui, elle, est centralisée. Lorsque cette passerelle est fermée, vous perdez tout. (Le problème est loin d'être spécifique à Unstoppable Domains ; regardez comme les ressources IPFS, service censément pair-à-pair sont toujours annoncées sous forme d'un URL passant par une passerelle centralisée. C'est en partie dû au fait que le logiciel est très complexe à compiler et installer.)

Cette dépendance de nombreux services pair-à-pair vis-à-vis de passerelles centralisées, donc vulnérables à la censure ou à des décisions "*business*", est un des gros problèmes, à l'heure actuelle, de beaucoup de solutions pair-à-pair.

Quelques bonnes lectures pour finir :

— Unstoppable Domains a fait une FAQ sur l'affaire du .coin <https://unstoppabledomains.freshdesk.com/support/solutions/articles/48001223398-faq-on-coin-tld>.
— Un article de Domain Name Wire <https://domainnamewire.com/2022/10/18/unstoppable-domain> estime qu'Unstoppable Domains n'a pas agi par gentillesse mais parce qu'eux-mêmes étaient dans un litige au sujet du `.wallet`.
— Un article plutôt polémique, sur "Web 3 is going great" <https://web3isgoinggreat.com/?id=unstoppable-domains-disables-coin-extensions>.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc2826.txt`