Les infrastructures et les services de l'Internet

Par Stéphane BORTZMEYER
Ingénieur à la direction des systèmes d'information et des opérations de l'Association française pour le nommage Internet en coopération (AFNIC)

De nombreuses applications ont été proposées pour la chaîne de blocs (*blockchain*). Mais on doit constater que, dans beaucoup de cas, la description de « comment » la chaîne de blocs pourrait être utilisée pour cette application est tellement approximative qu'il est impossible d'évaluer si l'utilisation de la chaîne de blocs est, dans ce cas, raisonnable. Or, cette chaîne n'est pas utile pour toutes les applications.
Nous explorerons ici deux applications liées à l'infrastructure de l'Internet : les journaux (au sens de journal de bord) et, surtout, les registres de noms, pour lesquels il y a déjà eu d'innombrables débats sur leur fonctionnement.
Comment un registre de noms peut-il être réalisé sur une chaîne de blocs ? Qu'y gagnerait-on ? Quels seraient les problèmes et les obstacles ?

Depuis que le concept de chaîne de blocs (*blockchain*) est à la mode, d'innombrables articles et présentations en ont exposé des applications possibles, souvent décrites en des termes très vagues (« il sera désormais impossible de mentir sur son diplôme, grâce à la *blockchain* », « les données de santé seront dans la *blockchain* »…). Ce flou fait qu'il est difficile de discuter de ces applications, ou même de voir si la chaîne de blocs est vraiment une solution adaptée à ce problème.

Notre but sera ici, au contraire, de détailler les applications de la chaîne de blocs pour les services de base de l'Internet, ainsi que pour son infrastructure.

Deux types de services « blockchainisables »

Le bon fonctionnement de l'Internet dépend d'un certain nombre de registres. Un registre est un service par lequel on va assurer l'unicité et la bonne gestion de certaines ressources, ainsi que la conservation de données sociales. Par exemple, un nom de domaine doit être unique. Les données rares (comme les adresses IPv4) doivent être sévèrement rationnées. Le nom et l'adresse de l'organisation qui a enregistré un numéro de système autonome – un nombre indispensable au fonctionnement du protocole de routage BGP (*Border Gateway Protocol*) – doivent être enregistrés.

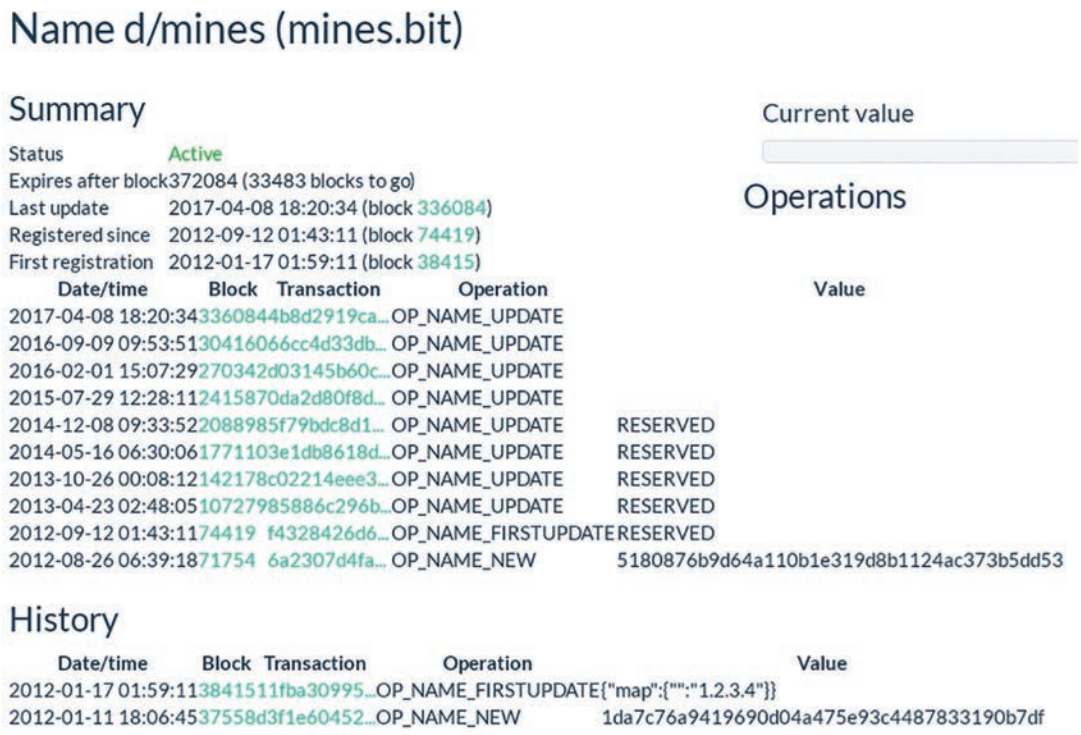
Le terme de « registre » désigne non seulement le service, mais aussi l'organisation qui assure ce service. Avant la chaîne de blocs, la sagesse conventionnelle était en effet que ce service devait être assuré par une organisation unique qui recevait les demandes, jugeait parfois de leur acceptabilité, mettait les enregistrements dans une base de données et, enfin, en assurait la publication.

C'est ainsi que l'AFNIC est le registre du domaine « .fr ». C'est son intervention qui assure qu'il n'y aura qu'un seul paris.fr ou qu'un seul wikipedia.fr, que l'on pourra retrouver le nom et l'adresse du titulaire de ces domaines, et que ces noms « marcheront », c'est-à-dire qu'ils seront proprement publiés dans le DNS (*Domain Name System*, le protocole par lequel les noms de domaines sont utilisés).

Cette intervention d'une organisation unique fait peser une lourde pression politique sur le registre. Sa légitimité doit être établie (par exemple, par la loi), ses décisions vont être contestées et il y aura même des interrogations sur son éventuel remplacement (que l'on songe aux nombreux débats sur la gouvernance de la racine du DNS).

Un second type de service potentiellement « blockchainisable » est le « journal ». Un journal (« log », pensez au journal de bord d'un navire) est une suite d'informations dont l'ordre est important et qui ne doit pas être modifié, une fois écrit. Là encore, la sagesse conventionnelle était qu'il devait être tenu par une organisation unique en garantissant l'intégrité.

Il existe bien sûr beaucoup d'autres services qui sont tout aussi « blockchainisables » (comme Twister, concurrent de Twitter, mais entièrement pair-à-pair), mais qui ne font pas partie de ce que l'on peut appeler l'infrastructure de l'Internet.



Name d/mines (mines.bit)

Summary

Current value

Status Active
Expires after block 372084 (33483 blocks to go)
Last update 2017-04-08 18:20:34 (block 336084)
Registered since 2012-09-12 01:43:11 (block 74419)
First registration 2012-01-17 01:59:11 (block 38415)

Operations

Date/time	Block	Transaction	Operation	Value
2017-04-08 18:20:34	3360844	b8d2919ca...	OP_NAME_UPDATE	
2016-09-09 09:53:51	30416066	cc4d33db...	OP_NAME_UPDATE	
2016-02-01 15:07:29	270342	d03145b60c...	OP_NAME_UPDATE	
2015-07-29 12:28:11	2415870	da2d80f8d...	OP_NAME_UPDATE	
2014-12-08 09:33:52	2088985	f79bdc8d1...	OP_NAME_UPDATE	RESERVED
2014-05-16 06:30:06	1771103	e1db8618d...	OP_NAME_UPDATE	RESERVED
2013-10-26 00:08:12	142178	c02214eee3...	OP_NAME_UPDATE	RESERVED
2013-04-23 02:48:05	10727985	886c296b...	OP_NAME_UPDATE	RESERVED
2012-09-12 01:43:11	74419	f4328426d6...	OP_NAME_FIRSTUPDATE	RESERVED
2012-08-26 06:39:18	71754	6a2307d4fa...	OP_NAME_NEW	5180876b9d64a110b1e319d8b1124ac373b5dd53

History

Date/time	Block	Transaction	Operation	Value
2012-01-17 01:59:11	38415	11fba30995...	OP_NAME_FIRSTUPDATE	{"map":{"":"1.2.3.4"}}
2012-01-11 18:06:45	37558	d3f1e60452...	OP_NAME_NEW	1da7c76a9419690d04a475e93c4487833190b7df

« Blockchainiser » les registres

La chaîne de blocs permet d'obtenir un consensus entre des acteurs qui ne se font pas confiance, un consensus sur un état (par exemple, sur le contenu d'un registre). Le point important, dans cette définition, est : « entre des acteurs qui ne se font pas confiance ».

Si tous font confiance à un tiers, les traditionnelles bases de données conviennent mieux (et c'est pour cela que des chaînes de blocs privées n'ont guère de sens).

Potentiellement, la chaîne de blocs permet de remplacer complètement un registre. Cela aurait l'avantage de mettre fin aux polémiques sur la politique du registre, voire sur sa légitimité. Avant d'étudier la différence entre théorie et pratique, voyons les moyens concrets de réaliser cet objectif.

Pour le cas d'un registre de noms de domaine, il existe depuis de nombreuses années une solution opérationnelle nommée Namecoin. Namecoin est un logiciel dérivé du code du célèbre Bitcoin, mais qui a sa propre chaîne de blocs (et donc ses propres mineurs et ses propres explorateurs). Les auteurs ont ajouté au code la possibilité d'effectuer un nouveau type de transaction : l'enregistrement de noms et l'association de données à ces noms (de même que le DNS permet d'associer des données, comme les adresses IP, à des noms de domaine). Namecoin est parfois présenté avec des formules raccourcies du genre « un DNS pair-à-pair », mais ces formules sont trompeuses : Namecoin n'a rien à voir avec le DNS, l'unique point commun étant que dans les deux cas, il s'agit de systèmes permettant de récupérer des données associées à un nom.

Namecoin a toutefois une passerelle permettant à des clients DNS traditionnels de résoudre les noms Namecoin en données *via* le TLD (non officiellement enregistré) « .bit ». Si votre résolveur DNS a été configuré pour résoudre le « .bit », vous pouvez accéder aux noms Namecoin depuis un logiciel ordinaire, comme votre navigateur *Web*.

Il existe d'autres logiciels de gestion de chaînes de blocs qui sont sans doute meilleurs, techniquement, que Namecoin. C'est le cas d'Ethereum qui, au lieu d'imposer de modifier le logiciel de la chaîne pour chaque application différente, permet de faire exécuter des programmes quelconques par la chaîne de blocs. On peut ainsi écrire un logiciel de registre et le déployer sur la chaîne Ethereum commune. Un tel logiciel avait d'ailleurs été présenté en détail par l'auteur de ces lignes à la Journée du conseil scientifique de l'AFNIC, en juillet 2016. En voici une version simplifiée, écrite dans le langage Solidity :

Et c'est quasiment tout ! C'est la chaîne de blocs qui assure les fonctions essentielles, comme celle d'ordonner les demandes pour réaliser le « premier arrivé, premier servi ». Donc, un registre de noms sur la chaîne de blocs est parfaitement réaliste et, d'ailleurs, plusieurs existent déjà (comme EtherID ou Ethereum Name Service). Mais voyons les limites. D'abord, il faut noter que la chaîne de blocs ne permet pas de changer facilement la politique d'enregistrement en cours (à moins qu'il n'existe un mé-

canisme permettant qu'un acteur de confiance le fasse, mais, dans ce cas, on est presque revenu au registre traditionnel, justement ce que beaucoup de promoteurs de la chaîne de blocs voulaient éviter). Si cette politique d'enregistrement est « premier arrivé, premier servi », il ne sera donc pas possible de mettre en œuvre une politique d'enregistrement plus restrictive. La plupart des promoteurs de registres fondés sur la chaîne de blocs voient d'ailleurs cela comme un avantage : la chaîne est à l'abri de l'arbitraire et des passions (notons qu'elle a bien une politique, mais c'est celle définie au lancement, et généralement on ne peut pas la modifier). Il faut juste être bien conscient de cette caractéristique.

Ainsi, la chaîne de blocs ne conviendrait sans doute pas pour l'allocation d'adresses IPv4, une activité dans laquelle, en raison de l'ancienne pénurie, on ne peut allouer de nouvelles adresses qu'après un strict examen. Or, la chaîne de blocs ne sait pas gérer des ressources rares.

De même, pour le cas de la racine du DNS (citée plus haut), la chaîne ne pourrait pas facilement limiter le nombre de nouveaux TLD (domaines de premier niveau, comme « .re », .com ou « .pizza »). Si l'on voulait résoudre les actuels problèmes de gouvernance de la racine en passant celle-ci sur une chaîne de blocs, on aurait une dynamique de création de TLD très différente de l'actuelle.

Notez également l'absence de recours, la chaîne de blocs étant conçue pour fonctionner automatiquement, sans intervention humaine. Si vous perdez un nom de domaine traditionnel (par exemple, parce que vous avez oublié de le payer et que, redevenu libre, il a été pris par un tiers), vous avez des mécanismes de recours auprès du registre (ou de la justice). Ces mécanismes peuvent être lents, compliqués et chers, mais ils existent. Si vous perdez un nom enregistré *via* le programme qui tourne sur la chaîne de blocs, il n'y a pas de recours : vous ne pouvez pas argumenter avec… un algorithme ! (Une telle mésaventure était survenue à l'auteur de cet article en septembre 2015, et elle explique pourquoi le nom bortzmeyer.bit ne marche plus…). La sécurité de vos noms, sur la chaîne de blocs, repose sur une bi-clé (dont une partie est privée et l'autre publique) cryptographique. Comme son nom l'indique, la partie privée doit être gardée rigoureusement secrète. Si elle est copiée par un tiers, celui-ci pourra faire ce qu'il veut avec vos noms (vu le nombre de logiciels malveillants qui tournent sur n'importe quelle machine Microsoft Windows, le risque n'est pas purement théorique). Si la partie privée de la clé est perdue (pas de sauvegarde, et le disque dur qui tombe en panne…), vous ne pouvez plus modifier vos noms, voire vous ne pouvez plus les renouveler.

Là encore, pas de recours auprès d'une institution (comme il peut y en avoir si vous oubliez le mot de passe d'accès à votre Bureau d'Enregistrement). Or, l'expérience de la cryptographie acquise jusqu'à présent nous enseigne que les utilisateurs ne sont pas de bons gestionnaires de clés cryptographiques. Dans le futur, des solutions technologiques (comme des dispositifs matériels durcis stockant la clé privée) limiteront (peut-être) les risques, mais ne les supprimeront pas totalement.

« Blockchainiser » les journaux

Et les journaux, est-il intéressant et possible de les faire passer sur la chaîne de blocs ? Il existe déjà des journaux publics, comme les journaux de certificats X.509 utilisés dans le cadre du projet *Certificate Transparency*. L'idée, normalisée dans le RFC 6962, est que les Autorités de Certification (AC) publient dans un journal les certificats qu'elles signent. Ce journal ne permet que les ajouts, jamais de modifications ou de retraits. Le navigateur *Web* peut alors vérifier, lorsque le certificat lui est présenté par le serveur, que le certificat a bien été publié dans le journal. Et les titulaires de noms de domaine peuvent examiner en permanence le journal afin de s'assurer qu'il n'y a pas eu signature de faux certificats (le projet *Certificate Transparency* est promu par Google, ce qui est logique puisque cette entreprise a souvent été victime de l'émission de faux certificats ; on a vu, par exemple, des gouvernements faire faire par une AC nationale de faux certificats gmail.com, pour pouvoir intercepter le trafic avec ce serveur).

Les journaux actuels sont gérés par des entreprises qui limitent l'écriture aux AC « reconnues ». Pourrait-on les « blockchainiser » ? Certainement, et cela supprimerait la dépendance vis-à-vis d'un acteur privé. Mais, aujourd'hui, il semble qu'il n'existe pas de projet concret allant dans ce sens.

Conclusion

Alors, verra-t-on le remplacement des actuels registres, qui jouent un rôle si important dans l'infrastructure de l'Internet, par des chaînes de blocs ? D'abord, rappelons-nous que le choix n'est pas binaire. Il n'y a pas forcément le seul registre traditionnel, d'un côté, et le système complètement pair-à-pair, de l'autre.

On pourrait ainsi imaginer des solutions organisationnellement innovantes, comme une chaîne de blocs, mais avec l'existence de « notaires » qui assureraient pour leurs clients des fonctions difficiles, comme la supervision de la chaîne de blocs ou la gestion des clés cryptographiques. Un tel système aurait pour avantage que le titulaire de nom aurait une liberté complète quant au choix de son notaire (il aurait aussi celle de s'en passer).

Découpler les différentes fonctions d'un registre a en outre l'avantage intellectuel de faire réfléchir sur le travail des registres. J'ai donné une version très simplifiée de ce travail plus haut. Par exemple, je n'avais pas parlé de la sauvegarde des données, une fonction essentielle (dans la chaîne de blocs, les données sont automatiquement dupliquées, mais si tous les nœuds de la chaîne disparaissent, les données sont perdues. Or, Namecoin est une petite chaîne que maintiennent quelques enthousiastes).

Mais évidemment, le plus gros défi pour la chaîne de blocs sera celui de son adoption. Namecoin existe depuis des années. Or, il n'a jamais eu de succès. Plusieurs de ses services associés (comme les résolveurs DNS publics pour « .bit ») n'existent plus. Aujourd'hui, tout le monde peut, techniquement parlant, créer sur Ethereum un registre de noms en très peu de temps et avec peu de compétences (c'est le côté, très important, « sans permission » de l'Internet).

Mais ce registre sera-t-il reconnu par les utilisateurs ?