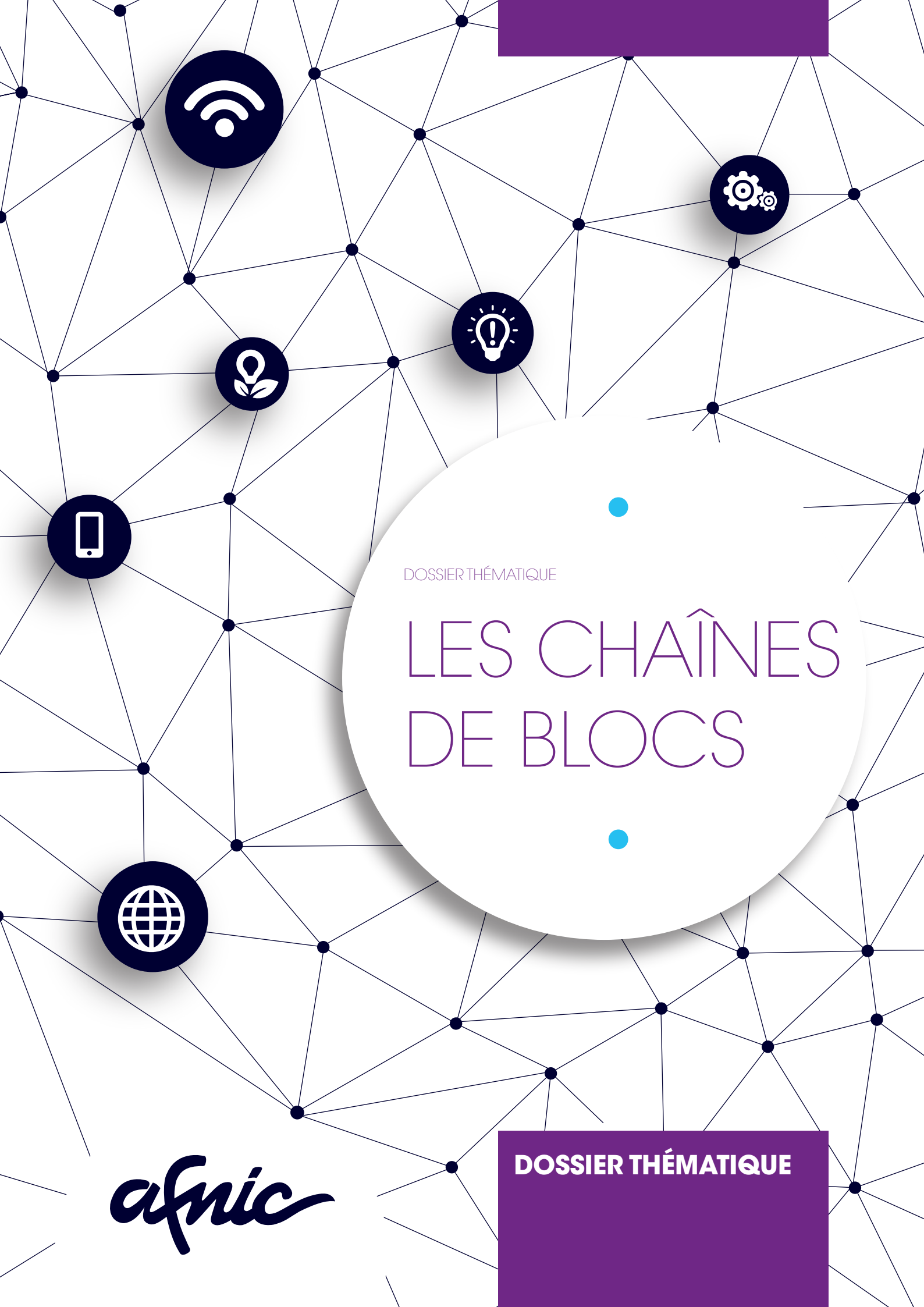


DOSSIER THÉMATIQUE

LES CHAÎNES DE BLOCS

afnic

DOSSIER THÉMATIQUE

QU'EST-CE QU'UNE CHAÎNE DE BLOCS ?

La **chaîne de blocs** (blockchain en anglais) est une invention récente qui permet à un groupe d'acteurs qui ne se font pas mutuellement confiance (voire qui ne se connaissent pas) de parvenir quand même à un accord sur un **livre des opérations** commun. Ce livre contient la liste ordonnée des transactions entre ces acteurs.

La chaîne de blocs est surtout connue par son utilisation dans le système de paiement Bitcoin. Mais elle a bien d'autres applications que celles du monde de la finance. Avant elle, un accord sur une liste d'opérations nécessitait quasiment toujours un tiers auquel tous les acteurs devaient faire confiance. Depuis, cet accord peut se faire de manière complètement pair à pair, sans autorité centrale.

/// INTRODUCTION

Figure 1 : le premier article scientifique décrivant la chaîne de blocs, en 2008

Potentiellement, la chaîne de blocs peut donc remplacer tous les cas où une telle autorité centrale n'a d'autre usage que de servir d'intermédiaire. Ce phénomène qu'on nomme parfois « ubériser Uber » ou, plus amusant, la « blockchainisation », est souvent cité dans les débats sur les conséquences pratiques de la chaîne de blocs.

La chaîne est, techniquement, une invention remarquable et, socialement, met en cause bien des situations acquises. Résultat, des proclamations très exagérées ont parfois été faites, attribuant à la chaîne de blocs des pouvoirs qu'elle n'a pas. Ce dossier thématique de l'Afnic a pour but d'explorer les usages possibles de la chaîne de blocs, notamment dans les activités de registre.

À QUOI ÇA SERT ?

Les applications de la chaîne de blocs sont a priori nombreuses : toutes les fois où des acteurs différents faisaient appel à une autorité centrale, on pourrait mettre à la place une chaîne de blocs.

L'exemple évident est la monnaie. Depuis le Moyen Âge, elle est typiquement garantie par un État (autorité centrale). Avec la chaîne de blocs, on peut concevoir une monnaie sans autorité centrale, et c'est bien le cas de Bitcoin, la technologie qui a lancé et popularisé cette idée de chaîne de blocs. Les motivations pour ces monnaies « réparties » ou « pair à pair » sont nombreuses : éviter de devoir faire confiance à des autorités qu'on n'approuve pas, faciliter les micropaiements sur Internet, avoir des frais de transaction réduits.

Après la monnaie, un autre cas de service qui est souvent géré de manière centralisée est celui de la **gestion de noms** (création, suppression, etc) dans un espace de nommage. Par exemple, les noms d'utilisateur d'un réseau social sont aujourd'hui gérés de manière centralisée par l'entreprise qui possède l'infrastructure dudit réseau social, ce qui permet notamment d'assurer l'unicité de ces noms. Mais cette centralisation donne aussi un contrôle excessif à l'entreprise : elle a par exemple le pouvoir fermer des comptes sur la base d'un simple signalement, sans vérification sérieuse. La chaîne de blocs fournit une alternative : l'enregistrement des noms « premier arrivé, premier servi » peut se faire sur une chaîne de blocs. Ainsi, il n'y a plus d'autorité centrale qui peut supprimer des comptes, la censure devient bien plus difficile.

Un exemple très proche de celui-ci est celui des registres de **noms de domaine**. Ceux-ci enregistrent des noms de domaine, indispensables pour l'utilisation de l'Internet. Mais ils ont aussi le pouvoir de les supprimer (comme dans l'affaire Sci-Hub). On peut donc envisager de remplacer ces registres par une chaîne de blocs, où les transactions sont la création d'un nom de domaine.

Dernier exemple d'une application qui est bien adaptée à la chaîne de blocs, **l'enregistrement d'œuvres à des fins de prouver l'antériorité.** Imaginons un artiste qui produise une vidéo, ne peut pas ou ne veut pas la publier tout de suite, mais souhaite pouvoir prouver plus tard qu'on était bien l'auteur. Il existe des solutions centralisées traditionnelles, nécessitant d'avoir confiance dans un organisme. À la place, on pourrait utiliser la chaîne. Mais mettre directement leur œuvre dans la chaîne de blocs aurait deux inconvénients : cela pourrait leur coûter cher et cela révèlerait leur œuvre (puisque la chaîne est publique, et lisible par tous).

Une solution possible est le condensat. C'est une opération mathématique simple qui réduit (condense) un document de taille quelconque en un nombre relativement court. La condensation n'est pas inversible (à partir du condensat, on ne peut pas retrouver le contenu original). Les fonctions mathématiques utilisées ont pour propriété qu'on ne peut pas fabriquer un document ayant un condensat donné. Ainsi, si le condensat est stocké dans la chaîne de blocs, seul l'auteur original pourra, le jour venu, produire un document qui correspondra, prouvant ainsi qu'il était bien celui qui avait enregistré le condensat. Plusieurs projets existent déjà pour mettre en œuvre cette idée.

C'est cette possibilité de remplacer, en tout ou en partie, des traditionnelles fonctions d'intermédiaire, qui justifie le discours comme quoi la chaîne pourrait « ubériser Uber ». Derrière ce slogan, il y a l'idée qu'au moins en théorie, les acteurs économiques pourraient interagir sans avoir besoin d'un intermédiaire de confiance.

Toutefois, il n'est pas prouvé que cela soit possible dans tous les cas, ni même que cela soit souhaitable.

Ainsi, interagir directement via la chaîne de blocs fait qu'on n'a pas de recours en cas de litige, ou en cas d'erreur de manipulation (voir plus loin les exemples liés à une mauvaise gestion de la clé privée). Il est donc probable qu'il restera toujours un rôle, peut-être plus réduit et redéfini, pour des intermédiaires choisis librement.

/// UN EXEMPLE CONNU, LE BITCOIN

La première chaîne de blocs, et sans doute la plus importante aujourd'hui, est celle de Bitcoin. Bitcoin est un système de paiement. Les seules transactions possibles sont l'envoi et la réception d'argent (les bitcoins). La monnaie étant un secteur très sensible et très régulé, il n'est pas étonnant que Bitcoin ait été au centre de plusieurs polémiques, pas toujours fondées.
Ainsi, des personnes ont critiqué le fait que l'auteur de Bitcoin, Satoshi Nakamoto, n'était connu que par un pseudonyme, et qu'on ne pouvait donc pas faire confiance à Bitcoin pour cette raison. Outre que cela revient à ne pas faire confiance aux textes imprimés si on ne connaît pas Gutenberg, cet argument montre une méconnaissance du mécanisme de la chaîne de blocs : **la confiance ne repose justement pas dans le gestionnaire de la chaîne (il n'y en a pas) mais dans l'exposition à tous de son fonctionnement**.

D'autres reproches faits à Bitcoin ont porté sur son caractère « virtuel » comme si les monnaies étaient encore en or, gagées sur la production d'objets matériels.

Figure 2 : le portefeuille Bitcoin Electrum

Mais, de toute façon, quelle que soit l'appréciation qu'on porte sur Bitcoin, elle ne déteint pas forcément sur le concept de la chaîne de blocs. Celui-ci peut être utilisé pour bien des choses, parfois sans aucun rapport avec l'argent.

/// ENREGISTRER DES NOMS

Le premier exemple d'enregistrement de noms dans une chaîne de blocs avait été le système Namecoin, un autre exemple a été présenté à la Journée du conseil scientifique de l'Afnic de 2016. Attention, nous avons dit que le remplacement des registres de noms de domaine était possible techniquement, pas forcément qu'il était souhaitable, ni qu'il serait adopté (des tas de très bonnes idées n'ont connu aucun succès). En effet, la chaîne de blocs a aussi ses limites (voir plus loin).

L'activité de veille et de recherche de l'Afnic dans ce domaine est ancienne. Le premier exposé sur la chaîne de blocs avait été fait lors de la réunion du CENTR, association européenne des registres de noms de domaine, à Paris en 2014.
Cet exposé de l'Afnic portait sur le système Namecoin, une variante de Bitcoin.

Parmi les limites identifiées de Namecoin, il y avait le cas de réservations de noms en masse à des fins de spéculation (les noms Namecoin sont très bon marché, et presque tous les noms intéressants sont déjà réservés), et la difficulté de gestion des clés par les utilisateurs : s'ils perdent leur clé privée, tous leurs noms sont perdus, il n'y a aucun recours.

/// UNE CHAÎNE GÉNÉRALISTE ?

Si Bitcoin est certainement la chaîne de blocs la plus connue, il en existe d'autres, comme Ethereum. Cette dernière a la particularité que les transactions stockées dans la chaîne ne sont pas restreintes à un petit nombre d'opérations, mais sont des programmes écrits dans un langage généraliste. On peut donc utiliser Ethereum pour des applications très diverses. Ainsi, l'exemple étudié à la journée du Conseil Scientifique de l'Afnic était celui d'un registre de noms Internet, développé sur Ethereum.

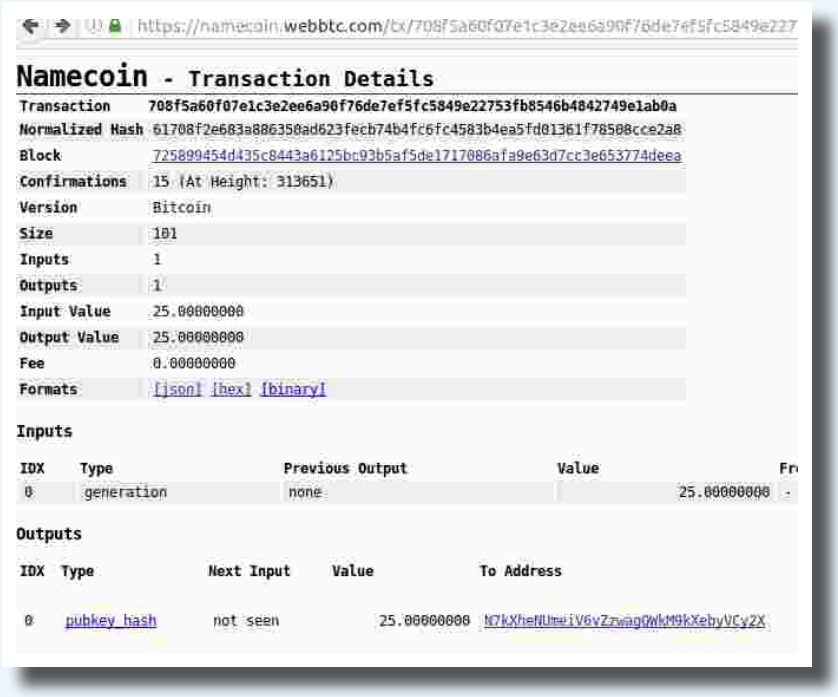


Figure 3 : la chaîne de blocs, ici, une transaction Namecoin, accessible à tous sur le Web.

/// À QUOI ÇA NE SERT PAS ?

LA CHAÎNE DE BLOCS N'EST PAS UNE SOLUTION MAGIQUE À TOUS LES PROBLÈMES

Ainsi, elle n'est pas adaptée au stockage de grandes quantités de données, puisque la chaîne doit être intégralement dupliquée sur toutes les machines du réseau pair-à-pair. En novembre 2016, la chaîne Bitcoin représentait à peu près 80 Go de données. Y stocker seulement une centaine de films en haute définition ferait plus que doubler sa taille !

La chaîne n'est pas non plus adaptée aux gros calculs (pour le cas des chaînes acceptant des programmes arbitraires, comme Ethereum), pour une raison analogue : il faut effectuer ces calculs sur toutes les machines, pour que chacune puisse vérifier le résultat indépendamment.

Enfin, du fait du caractère public de la chaîne, il n'est pas recommandé d'y stocker des données privées. Stocker un condensat de ces données, comme dans l'exemple de l'enregistrement d'œuvres de l'esprit, est raisonnable, mais il ne faut pas écrire de données en clair.

/// UN (TOUT PETIT) PEU D'EXPLICATIONS

Ce dossier thématique n'a pas vocation à être un cours complet sur la chaîne de blocs. Néanmoins, cette section vise à expliquer quelques concepts de base nécessaires. Ce sera la seule partie technique du dossier.

Une chaîne de blocs devrait en fait être appelée *chaîne de transactions*. C'est une suite ordonnée de transactions et d'opérations. Elle est publique : n'importe qui peut accéder aux données de la chaîne, ce qui a notamment des conséquences en matière de vie privée.

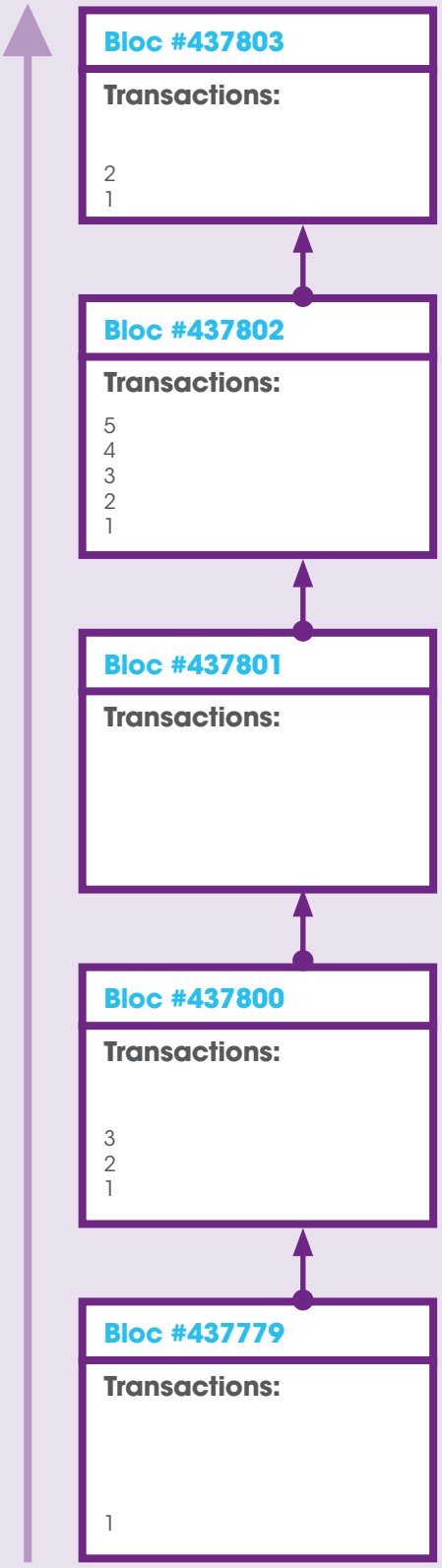
Pour diverses raisons techniques, les transactions sont regroupées en blocs, et ce sont ces blocs qui sont chainés. Voici une représentation simplifiée de la chaîne Bitcoin, le dernier bloc étant le #437803. Cinq blocs sont montrés ici, le plus récent étant en haut. Certaines comprennent plusieurs transactions, le bloc #437801 n'en comportant aucune.

Non seulement la chaîne est publique, mais elle est maintenue en pair à pair c'est-à-dire qu'aucune machine n'a de privilège particulier. Tout le monde peut contribuer à l'ajout de blocs à la chaîne (mais ne peut pas modifier les anciens blocs, ou les retirer). Pour empêcher les modifications non autorisées, la chaîne est sécurisée par la cryptographie. Notamment, toutes les transactions sont signées.

D'où peut venir la confiance dans une base de données répartie, que tout le monde peut modifier ? Elle repose sur le caractère public des logiciels (tous des logiciels libres), des algorithmes, et de la chaîne elle-même. Chacun peut vérifier que tout s'est bien déroulé selon l'algorithme officiel, en faisant tourner le logiciel sur sa propre machine.

La chaîne de blocs est un concept, pas une entité unique. La chaîne la plus connue est celle de la monnaie Bitcoin mais il en existe de nombreuses autres.

Figure 4 : la chaîne de blocs (le temps s'écoule de bas en haut)



/// QUI FAIT QUOI ?

Une question souvent posée sur le fonctionnement de l'Internet est celui de sa gouvernance. **Qui prend les décisions et comment ?** La même question se pose pour la chaîne de blocs. Certains disent qu'elle marche seule, sans intervention humaine. Mais, comme elle tourne sur des ordinateurs physiques, gérés par des humains réels, et est programmée par ces mêmes humains, elle ne peut pas être entièrement déconnectée de la politique. Des décisions sont prises, des choix faits, et tout le monde n'est pas toujours d'accord, d'autant plus que les acteurs n'ont pas tous les même intérêts.

Deux exemples sont souvent cités, le débat au sein du monde Bitcoin sur un point qui semble un détail technique (l'augmentation de la taille des blocs) mais qui soulève en fait des questions d'orientation de Bitcoin. Et le second est le débat qui a déchiré le monde Ethereum en 2016 pour savoir ce qu'il fallait faire suite au vol de nombreux ethers. Dans les deux cas, des mécanismes de prise de décision devront être développés.

/// LES FREINS

SÉCURITÉ DES CLÉS

La sécurité du portefeuille de l'utilisateur repose sur la cryptographie asymétrique, où l'utilisateur a à la fois une clé publique et une clé privée. Cette dernière sert à authentifier les transactions.

Il faut à la fois empêcher des tiers de lire les clés privées et s'assurer que ces clefs privées sont bien sauvegardées, pour faire face, par exemple, à une panne du disque dur. Cela complique sérieusement l'utilisation de la chaîne de blocs pour l'utilisateur ! Il existe bien sûr des solutions techniques (signatures multiples) et organisationnelles (des « notaires » à qui on sous-traiterait ce travail) à ce problème mais elles sont encore rares.

Le premier risque est celui de la sécurité de la machine qui stocke les clés. Pas facile de garder ses clés confidentielles sur une machine utilisant un système grand public infesté de logiciels malveillants. Les bonnes pratiques sont celles de l'hygiène numérique, et peut-être de mécanismes plus high-tech comme des dispositifs matériels de stockage des clés.

Un exemple fameux du deuxième risque avait été celui d'un infortuné britannique qui avait jeté le disque dur contenant sa clé privée perdant ainsi 7 500 bitcoins. Il existe plusieurs solutions techniques à ce problème, la principale étant évidemment les sauvegardes des fichiers.

VIE PRIVÉE

On lit parfois que Bitcoin est « anonyme ». En fait, le terme correct serait « pseudonyme ». Si une adresse Bitcoin n'identifie pas directement un être humain, en revanche, elle permet la traçabilité de toutes les opérations liées à cette adresse. Si une fuite, une seule fuite, permet de faire le lien entre une adresse et une personne physique, toute son activité Bitcoin est exposée. Il n'est donc pas exagéré de dire que l'adresse Bitcoin est proche d'une donnée personnelle.
Plusieurs approches techniques sont testées pour préserver la vie privée des utilisateurs de la chaîne de blocs. Elles vont de l'utilisation de mélangeurs (des services qui reçoivent plusieurs paiements et les mélangent) aux adresses à usage unique (pour diminuer la traçabilité), jusqu'à des solutions radicalement nouvelles, et conçues pour un vrai anonymat, comme les chaînes Monero ou Zcash.

Dans certains cas, la chaîne de blocs peut protéger la vie privée. Par exemple, dans les systèmes d'enregistrement de noms Internet, comme Namecoin, une requête pour un nom (l'équivalent d'une requête whois ou DNS) est purement locale, faite sur une copie locale de la chaîne, et n'est donc pas connue des autres acteurs.

DOUTES SUR L'IMMUABILITÉ

En théorie, la chaîne de blocs est immuable. Une fois qu'une transaction est écrite, elle l'est pour l'éternité. Cela peut être une bonne ou une mauvaise chose. La bonne est que cela protège contre l'arbitraire de modifications faites par un intermédiaire. C'est essentiel pour la confiance. La mauvaise est que cela peut entrer en conflit avec le droit à l'oubli. Et que cela peut rendre difficile la correction de bogues, comme expliqué dans la section suivante.

En fait, rien n'est réellement immuable. La chaîne n'est après tout qu'un fichier informatique et peut toujours être changée. Mais cela nécessite un consensus d'un grand nombre d'acteurs, puisque le réseau n'a pas de direction centrale. C'est ce consensus qui protège contre les modifications arbitraires, tout en permettant de changer les règles du jeu de temps en temps, s'il y a une très bonne raison.

BOGUE

Un bon exemple d'une telle raison avait été le vol commis au détriment du fonds d'investissement « The DAO » en juin 2016, sur la chaîne Ethereum. Les règles suivies par la chaîne avaient été modifiées, pour récupérer l'argent volé.

Dans ce cas, le vol avait été possible suite à une bogue dans un programme (un contrat) s'exécutant sur la chaîne Ethereum. Une telle bogue, survenant dans un programme ou bien dans le logiciel de la chaîne lui-même, est plus difficile à corriger qu'une bogue classique, car il n'y a pas d'autorité centrale pour décider des mises à jour du code ou bien des données. C'est actuellement un des facteurs d'incertitude pour certaines chaînes notamment celles qui permettent l'exécution de programmes quelconques.

/// CONCLUSION

La chaîne de blocs est une technologie encore récente, et il est donc logique qu'il y ait beaucoup de questions non résolues, et de problèmes agaçants. Il ne faut pas la comparer à des technologies mûres mais plutôt à ce que pouvait être, mettons, l'automobile en 1900 : pleine de promesses mais encore difficile (et parfois dangereuse) à utiliser.

RENSEIGNEMENTS UTILES

Contact Afnic

Afnic
Immeuble Le Stephenson
1, rue Stephenson
78180 Montigny-Le-Bretonneux
France
www.afnic.fr

Tél. : +33(0)1 39 30 83 00

@AFNIC

support@afnic.fr

Fax : +33(0)1 39 30 83 01

afnic.fr

À propos de l'Afnic :

L'**Afnic** est le registre des noms de domaine .fr (France), .re (Île de la Réunion), .yt (Mayotte), .wf (Wallis et Futuna), .tf (Terres Australes et Antarctiques), .pm (Saint-Pierre et Miquelon).

L'**Afnic** se positionne également comme fournisseurs de solutions techniques et de services de registre. L'**Afnic** - Association Française pour le Nommage Internet en Coopération - est composée d'acteurs publics et privés : représentants des pouvoirs publics, utilisateurs et prestataires de services Internet (bureaux d'enregistrement). Elle est à but non lucratif.