

De l'inviolabilité d'une blockchain

Description

À la suite d'une faille de sécurité dans une application construite sur Ethereum, ayant provoqué le détournement de 50 millions de dollars, la *blockchain* a été réécrite pour annuler la transaction, revenant sur le principe même de son immuabilité.

Les *blockchains* n'ont pas fini de faire parler d'elles. Selon le mathématicien Jean-Paul Delahaye une *blockchain* s'apparente à « *un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible* ». Autrement dit, une *blockchain* est une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Tous les échanges sont « minés » (validés par des intermédiaires baptisés « mineurs ») dans des blocs enchaînés de manière chronologique, impossibles à effacer ou à falsifier. Parce qu'elle est sans intermédiaire et partagée par ses différents utilisateurs, quiconque peut vérifier la validité de la chaîne.

« The DAO »

Parmi les nombreuses *blockchains* créées depuis 2008, Ethereum est une chaîne de blocs publique permettant à ses utilisateurs de créer et d'exécuter des contrats dits « intelligents », c'est-à-dire « *des applications qui s'exécutent exactement telles que programmées, sans possibilité de les arrêter, non censurables, sans fraude possible et sans interférence de tierce partie* », comme le rapporte le site Ethereum.org. Les contrats sont dits intelligents parce qu'ils sont basés sur un protocole informatique inviolable permettant de vérifier et de mettre en application ledit contrat : par exemple, la possibilité pour un locataire d'ouvrir la porte électronique d'un appartement à la suite d'un contrat de location inscrit et validé dans la *blockchain*. Comme moyen de paiement, Ethereum utilise une crypto-monnaie appelée « ether » (ETH), deuxième capitalisation boursière après le bitcoin.

En mai 2016, une campagne de financement participatif, nommée « The DAO » (Decentralized Autonomous Organization), a été lancée sur cette *blockchain* : elle a rassemblé 11 000 utilisateurs qui ont chacun acheté des parts de l'entité et ont réuni 12 millions d'ethers, soit 150 millions de dollars, représentant quelque 15 % de la totalité des ethers en circulation. Une DAO est un concept d'entreprise autonome et décentralisée fonctionnant sur la *blockchain* Ethereum. Selon Ethereum-France, « *il s'agit d'une sorte de conseil d'administration doté d'un pouvoir de décision et d'un pouvoir financier. La DAO décide à la majorité de la façon d'allouer ses fonds et des prestataires qu'elle recrute. Elle peut décider d'arrêter de travailler avec un prestataire et d'en recruter un autre. Elle garde toujours le contrôle des fonds qu'elle possède en ethers et qui sont dans la blockchain* ».

Autrement dit, la DAO n'a aucune existence juridique à proprement parler et ne possède ni actif ni salarié. Son rôle est seulement de créer et de signer des contrats avec des prestataires extérieurs qui vont agir dans le monde physique. Les contrats sont inscrits dans la *blockchain* Ethereum et l'intégralité des comptes et des échanges entre les participants sont ainsi transparents. Deux projets ont émergé parmi les propositions et les discussions entre utilisateurs de « The DAO » : le premier consistant à créer un réseau dédié à l'internet des objets basé sur la *blockchain* Ethereum ; le second, au développement de véhicules électriques modulaires.

L'histoire de cette auto-organisation aurait pu continuer, mais c'était sans compter qu'un tel butin attire aussi des gens mal intentionnés, à l'esprit parfois des plus brillants. Le 17 juin 2016, un pirate informatique a créé un contrat intelligent avec The DAO pour la fourniture d'un service quelconque. Or, selon Andrew Miller, doctorant de l'université du Maryland, ce contrat exploitait une faille de sécurité dans le code informatique, qui permettait d'effectuer de façon réursive un retrait de fonds sans que le solde soit préalablement vérifié. En quelques heures, plus de 3,6 millions d'ethers ont ainsi été « siphonnés » et placés dans une copie de la plate-forme, appelée « DAO Child », provoquant par la suite des débats passionnés au sein de la communauté d'utilisateurs sur les choix à opérer. En effet, le code informatique prévoyait que les Ethers contenus dans une DAO Child ne pouvaient être déplacés avant un délai de 27 jours, empêchant l'attaquant d'y avoir accès pendant ce laps de temps.

Récupérer les fonds

Pour récupérer les fonds dérobés, plusieurs solutions ont été proposées par la communauté des utilisateurs de The DAO et par les fondateurs d'Ethereum. Effectuer un *soft fork* puis un *hard fork* – en langage informatique, un *fork* ou une scission en français, consiste à créer un nouveau logiciel à partir du codesource d'un logiciel existant. Le *soft fork* apporte des modifications à la *blockchain* qui vont s'appliquer uniquement dans le futur, alors que les modifications introduites par un *hard fork* valent également pour le passé. Il s'agissait donc de réécrire la *blockchain* après son lancement. La communauté d'utilisateurs a voté de procéder finalement à un *soft fork*, avec pour objectif de geler toutes les transactions sur The DAO et de gagner ainsi du temps face à l'attaquant. Les débats furent houleux et passionnés entre les partisans ne souhaitant rien faire et ceux qui proposaient un *hard fork*, c'est-à-dire une réécriture valant à la fois pour le passé et pour le futur.

À la suite d'un second vote des utilisateurs d'Ethereum, il fut décidé, le 20 juillet 2016, de procéder à un *hard fork*, c'est-à-dire de liquider The DAO et de reprogrammer la *blockchain*, afin d'inverser les effets du piratage, en créditant à nouveau The DAO des sommes détournées pour rembourser, à terme, les investisseurs. Mais ce *hard fork* n'a pas été validé par l'ensemble des acteurs, ce qui a eu pour effet de scinder en deux la *blockchain* Ethereum : d'un côté, les utilisateurs ayant refusé la modification et continuant par conséquent à utiliser la *blockchain* originale – dorénavant appelée Ethereum Classic et sa monnaie ETC et, de l'autre, les utilisateurs de la *blockchain* Ethereum réécrite où The DAO n'est plus qu'une coquille vide, avec un contrat intelligent permettant de se faire rembourser, les transactions originales étant restées inscrites dans la *blockchain*.

Réécrire la *blockchain*

Pour les puristes des *blockchains*, procéder à un *hard fork* consiste à revenir sur l'intérêt principal d'une *blockchain*, par essence immuable et inviolable. Le *hard fork* fait en effet exception au principe d'immuabilité de la *blockchain*, puisqu'il s'agit de la réécrire en modifiant ou en écartant une transaction passée. Puisque « *le code, c'est la loi* », il ne doit absolument pas être modifié, au risque à l'avenir de permettre de nouveaux changements. Pour certains, « *cette manipulation créerait un précédent sur lequel un tribunal pourrait s'appuyer pour réclamer le même genre de manœuvre à l'avenir* ».

Les tenants de l'Ethereum Classic qui ne souhaitent pas modifier la *blockchain*, justifient leur choix en ces termes : « *Nous croyons en une blockchain décentralisée, publique et ouverte qui ne permet pas la censure. Nous souscrivons au projet initial d'Ethereum en tant qu'ordinateur global sur lequel s'exécutent en continu des contrats intelligents de manière irréversible. Nous n'acceptons les « forks » que s'il s'agit de corriger des bugs concernant le fonctionnement de la plateforme elle-même et non pas dans l'intérêt de quelques-uns.* » Cette interprétation à la lettre du contrat initial d'Ethereum n'aura pas résisté à la volonté des milliers d'utilisateurs de The DAO de récupérer leur gain. C'est donc l'esprit de la *blockchain* qui est remis en cause. En décidant sa réécriture, les utilisateurs de la *blockchain* Ethereum semblent avoir écorné son fondement.

A contrario, le caractère immuable des blocs de transaction, empêchant de revenir sur ce qui est écrit dans une *blockchain* embarrasse bon nombre de banquiers et d'assureurs qui testent cette technologie. Le cabinet Accenture a ainsi récemment breveté un concept de *blockchain* privée permettant aux participants d'effacer des opérations *a posteriori*. Comme l'explique Richard Lumb, responsable mondial des services financiers chez Accenture, « *pour les systèmes de crypto-monnaie, cette comptabilité permanente a été cruciale pour gagner la confiance des participants. Mais pour les institutions de services financiers qui font face à une multitude de risques et d'éléments de régulation, l'immuabilité absolue est un obstacle* ».

Quoi qu'il en soit, il faut retenir que ce n'est pas la *blockchain* qui a été piratée, mais une application construite à partir de celle-ci. Et Vitalik Buterin, le cofondateur d'Ethereum, de rappeler : « *Le problème affecte seulement The DAO, la blockchain Ethereum reste parfaitement sûre.* »

Sources :

- « Ethereum : deux forks à venir à la suite d'un hack ? », Arthur Bouquet, Bitcoin.fr, 17 juin 2016.
- « A \$50 Million Hack Just Showed That the DAO Was All Too Human, Klint Finley », Wired.com, 18 juin 2016.
- « To fork or not to fork, telle est la question ! » Simon Polrot, Ethereum-france.com, 27 juin 2016.
- « La Blockchain pose de sérieux problèmes de confiance, de droit... et de sécurité », Eric A. Caprioli, Usine-digitale.fr, 8 juillet 2016.
- « Le Hard Fork « The DAO » aura bien lieu, mode d'emploi », Simon Polrot, Ethereum-france.com, 19 juillet 2016.
- « Ethereum : un « hard-fork » controversé pour oublier The DAO », Kevin Hottot, Nextinpact.com, 20 juillet 2016.
- « Le hard fork est un succès », Gautier Marin-Dagannaud, Ethereum-france.com, 21 juillet 2016.
- « The Great Digital-Currency Debate: « New » Ethereum Vs. Ethereum « Classic » », Paul Vigna, Blog The Wall Street Journal, 1^{er} août 2016.
- « Après un « cyber-casse », la technologie blockchain se cherche un avenir », Eric Albert, LeMonde.fr, 26 septembre 2016.
- « Accenture imagine une blockchain modifiable pour les entreprises », Ninon Renaud, *Les Echos*, 5 octobre 2016.
- « Ethereum », Wikipedia.org, consulté le 10 octobre 2016.

Categorie

1. Techniques

date créée

1 février 2017

Auteur

jacquesandrefines
