De lâ€™inviolabilitÃ©Â dâ€™une blockchain

Description

Ã€ la suite dâ€™une faille de sÃ©curitÃ© dans une application construite sur Ethereum, ayant provoquÃ© le dÃ©tournement de 50 millions de dollars, laÂ *blockchain*Â a Ã©tÃ© rÃ©Ã©crite pour annuler la transaction, revenant sur le principe mÃªme de son immuabilitÃ©.

Les *blockchains* nâ€™ont pas fini de faire parler dâ€™elles. Selon le mathÃ©maticien Jean-Paul Delahaye une *blockchain* sâ€™apparente Ã Â« *un trÃ¨s grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut Ã©crire, mais qui est impossible Ã effacer et indestructible* Â». Autrement dit, une *blockchain* est une base de donnÃ©es qui contient lâ€™historique de tous les Ã©changes effectuÃ©s entre ses utilisateurs depuis sa crÃ©ation. Tous les Ã©changes sontÂ Â« minÃ©s Â»Â (validÃ©s par des intermÃ©diaires baptisÃ©sÂ Â« mineurs Â»Â) dans des blocs enchaÃ®nÃ©s de maniÃ¨re chronologique,Â impossibles Ã effacer ou Ã falsifier. Parce quâ€™elle est sans intermÃ©diaire et partagÃ©e par ses diffÃ©rents utilisateurs, quiconque peut vÃ©rifier la validitÃ© de la chaÃ®ne.

Â« The DAO Â»

Parmi les nombreusesÂ *blockchains*Â crÃ©Ã©es depuis 2008, Ethereum est une chaÃ®ne de blocs publique permettant Ã ses utilisateurs de crÃ©er et dâ€™exÃ©cuter des contrats ditsÂ Â« intelligents Â», câ€™est-Ã -direÂ *Â« des applications quiÂ s'exÃ©cutent exactement telles que programmÃ©es, sans possibilitÃ© de les arrÃªter, non censurables, sans fraude possible et sans interfÃ©rence de tierce partie Â»* , comme le rapporte le site Ethereum.org. Les contrats sont dits intelligents parce quâ€™ils sont basÃ©s sur un protocole informatique inviolable permettant de vÃ©rifier et de mettre en application ledit contratÂ : par exemple, la possibilitÃ© pour un locataire dâ€™ouvrir la porte Ã©lectronique dâ€™un appartement Ã la suite dâ€™un contrat de location inscrit et validÃ© dans laÂ *blockchain*. Comme moyen de paiement, Ethereum utilise uneÂ crypto-monnaieÂ appelÃ©eÂ Â« etherÂ *Â»*(ETH), deuxiÃ¨me capitalisation boursiÃ¨re aprÃ¨s le bitcoin.

En mai 2016, une campagne de financement participatif, nommÃ©eÂ Â« The DAO Â»Â (Decentralized Autonomous Organization), a Ã©tÃ© lancÃ©e sur cetteÂ *blockchain*Â : elle a rassemblÃ©Â 11 000Â utilisateurs qui ont chacun achetÃ© des parts de lâ€™entitÃ© et ont rÃ©uni 12 millions dâ€™ethers, soit 150 millions de dollars, reprÃ©sentant quelque 15 %Â de la totalitÃ© des ethers en circulation.Â Une DAO est un concept dâ€™entreprise autonome et dÃ©centralisÃ©eÂ fonctionnant sur laÂ *blockchain* Â Ethereum. Selon Ethereum-France,Â *Â« il sâ€™agit dâ€™une sorte de conseil dâ€™administration dotÃ© dâ€™un pouvoir de dÃ©cision et dâ€™un pouvoir financier. La DAO dÃ©cide Ã la majoritÃ© de la faÃ§on dâ€™allouer ses fonds et des prestataires quâ€™elle recrute. Elle peut dÃ©cider dâ€™arrÃªter de travailler avec un prestataire et dâ€™en recruter un autre. Elle garde toujours le contrÃ´le des fonds quâ€™elle possÃ¨de en ethers et qui sont dans laÂ*

blockchainÂ Â».

Autrement dit, laÂ DAOÂ nâ€™a aucune existence juridique Ã proprement parler et ne possÃ¨de ni actif ni salariÃ©. Son rÃ´le est seulement de crÃ©er et de signer des contrats avec des prestataires extÃ©rieurs qui vont agir dans le monde physique. Les contrats sont inscrits dans laÂ *blockchain*Â Ethereum et lâ€™intÃ©gralitÃ© des comptes et des Ã©changes entre les participants sont ainsi transparents. Deux projets ont Ã©mergÃ© parmi les propositions et les discussions entre utilisateurs deÂ Â« The DAO Â»Â : le premier consistant Ã crÃ©er un rÃ©seau dÃ©diÃ© Ã lâ€™internet des objets basÃ© sur laÂ *blockchain*Â EthereumÂ ; le second, au dÃ©veloppement de vÃ©hicules Ã©lectriques modulaires.

Lâ€™histoire de cette auto-organisation aurait pu continuer, mais câ€™Ã©tait sans compter quâ€™un tel butin attire aussi des gens mal intentionnÃ©s, Ã lâ€™esprit parfois des plus brillants. Le 17 juin 2016, un pirate informatique a crÃ©Ã© un contrat intelligent avecÂ The DAOÂ pour la fourniture dâ€™un service quelconque. Or, selon Andrew Miller, doctorant de l’universitÃ© du Maryland,Â ce contrat exploitait une faille de sÃ©curitÃ© dans le code informatique, qui permettait dâ€™effectuer de faÃ§on rÃ©cursive un retrait de fonds sans que le solde soit prÃ©alablement vÃ©rifiÃ©. En quelques heures, plus de 3,6 millions dâ€™ethers ont ainsi Ã©tÃ©Â Â« siphonnÃ©s Â»Â et placÃ©s dans une copie de la plate-forme, appelÃ©eÂ Â« DAO Child Â», provoquant par la suite des dÃ©bats passionnÃ©s au sein de la communautÃ© dâ€™utilisateurs sur les choix Ã opÃ©rer. En effet, le code informatique prÃ©voyait que les Ethers contenus dans uneÂ DAO ChildÂ ne pouvaient Ãªtre dÃ©placÃ©s avant un dÃ©lai de 27 jours, empÃªchant lâ€™attaquant dâ€™y avoir accÃ¨s pendant ce laps de temps.

RÃ©cupÃ©rer les fonds

Pour rÃ©cupÃ©rer les fonds dÃ©robÃ©s, plusieurs solutions ont Ã©tÃ© proposÃ©es par la communautÃ© des utilisateurs deÂ The DAOÂ et par les fondateurs dâ€™Ethereum. EffectuerÂ unÂ *soft fork*Â puisÂ unÂ *hard fork*Â – en langage informatique, unÂ *fork*Â ou une scission en franÃ§ais, consiste Ã crÃ©er un nouveau logiciel Ã partir du code source d’un logiciel existant. LeÂ *soft fork*Â apporte des modifications Ã laÂ *blockchain*Â qui vont sâ€™appliquer uniquement dans le futur, alors que les modifications introduites par unÂ *hard fork*Â valent Ã©galement pour le passÃ©. Il sâ€™agissait donc de rÃ©Ã©crire laÂ *blockchain*Â aprÃ¨s son lancement. La communautÃ© dâ€™utilisateurs a votÃ© de procÃ©der finalement Ã unÂ *soft fork*, avec pour objectif de geler toutes les transactions sur The DAO et de gagner ainsi du temps face Ã lâ€™attaquant. Les dÃ©bats furent houleux et passionnÃ©s entre les partisans ne souhaitant rien faire et ceux qui proposaient unÂ *hard fork*, câ€™est-Ã -dire une rÃ©Ã©criture valant Ã la fois pour le passÃ© et pour le futur.

Ã€ la suite dâ€™un second vote des utilisateurs dâ€™Ethereum, il fut dÃ©cidÃ©, le 20 juillet 2016, de procÃ©der Ã unÂ *hard fork*, câ€™est-Ã -dire de liquiderÂ The DAOÂ et de reprogrammer laÂ *blockchain*, afin dâ€™inverser les effets du piratage, en crÃ©ditant Ã nouveauÂ The DAOÂ des sommes dÃ©tournÃ©es pour rembourser, Ã terme, les investisseurs. MaisÂ ceÂ *hard fork*Â nâ€™a pas Ã©tÃ© validÃ© par lâ€™ensemble des acteurs, ce qui a eu pour effet de scinder en deux laÂ *blockchain*

Â Ethereum : dâ€™un cÃ´tÃ©, les utilisateurs ayant refusÃ© la modification et continuant par consÃ©quent Ã utiliser laÂ *blockchain*Â originale â€“ dorÃ©navant appelÃ©e Ethereum Classic et sa monnaie ETC et, de lâ€™autre, les utilisateurs de laÂ *blockchain*Â Ethereum rÃ©Ã©crite oÃ¹Â The DAOÂ nâ€™est plus quâ€™une coquille vide, avec un contrat intelligent permettant de se faire rembourser, les transactions originales Ã©tant restÃ©es inscrites dans laÂ *blockchain*.

RÃ©Ã©crire laÂ *blockchain*

Pour les puristes desÂ *blockchains*, procÃ©der Ã unÂ *hard fork*Â consiste Ã revenir sur lâ€™intÃ©rÃªt principal dâ€™uneÂ *blockchain*, par essence immuable et inviolable. LeÂ *hard fork*Â fait en effet exception au principe dâ€™immuabilitÃ© de laÂ *blockchain*, puisquâ€™il sâ€™agit de la rÃ©Ã©crire en modifiant ou en Ã©cartant une transaction passÃ©e. PuisqueÂ *Â«Â le code, câ€™est la loi Â»*,Â il ne doit absolument pas Ãªtre modifiÃ©, au risque Ã lâ€™avenir de permettre de nouveaux changements. Pour certains,Â *Â« cette manipulation crÃ©erait un prÃ©cÃ©dent sur lequel un tribunal pourrait sâ€™appuyer pour rÃ©clamer le mÃªme genre de manÅ“uvre Ã lâ€™avenir Â»*.

Les tenants de lâ€™Ethereum Classic qui ne souhaitaient pas modifier laÂ *blockchain*, justifient leur choix en ces termesÂ :Â *Â« Nous croyons en uneÂ* blockchain*Â dÃ©centralisÃ©e, publique et ouverte qui ne permet pas la censure. Nous souscrivons au projet initial dâ€™Ethereum en tant quâ€™ordinateur global sur lequel sâ€™exÃ©cutent en continu des contrats intelligents de maniÃ¨re irrÃ©versible.Â Nous nâ€™acceptons les Â«Â forksÂ Â»Â que sâ€™il sâ€™agit de corriger des bugs concernant le fonctionnement de la plateforme elle-mÃªme et non pas dans lâ€™intÃ©rÃªt de quelques-uns. Â»*Â Cette interprÃ©tation Ã la lettre du contrat initial dâ€™Ethereum nâ€™aura pas rÃ©sistÃ© Ã la volontÃ© des milliers dâ€™utilisateurs de The DAO de rÃ©cupÃ©rer leur gain. Câ€™est donc lâ€™esprit de laÂ *blockchain*Â qui est remis en cause. En dÃ©cidant sa rÃ©Ã©criture, les utilisateurs de laÂ *blockchain*Â Ethereum semblent avoir Ã©cornÃ© son fondement.

A contrario, le caractÃ¨re immuable des blocs de transaction, empÃªchant de revenir sur ce qui est Ã©crit dans uneÂ *blockchain*Â embarrasse bon nombre de banquiers et dâ€™assureurs qui testent cette technologie. Le cabinet Accenture a ainsi rÃ©cemment brevetÃ© un concept deÂ *blockchain*Â privÃ©e permettant aux participants d'effacer des opÃ©rationsÂ *a posteriori*. Comme lâ€™explique Richard Lumb, responsable mondial des services financiers chez Accenture,Â *Â« pour les systÃ¨mes de crypto-monnaie, cette comptabilitÃ© permanente a Ã©tÃ© cruciale pour gagner la confiance des participants. Mais pour les institutions de services financiers qui font face Ã une multitude de risques et d'Ã©lÃ©ments de rÃ©gulation, l'immuabilitÃ© absolue est un obstacle Â»*.

Quoi quâ€™il en soit, il faut retenir queÂ ce nâ€™est pas laÂ *blockchain*Â qui a Ã©tÃ© piratÃ©e, mais une application construite Ã partir de celle-ci. Et Vitalik Buterin, le cofondateur dâ€™Ethereum, de rappelerÂ :Â *Â« Le problÃ¨me affecte seulement The DAO, laÂ blockchainÂ Ethereum reste parfaitement sÃ»re. Â»*

SourcesÂ :

- Â« EthereumÂ : deux forks Ã venir Ã la suite dâ€™un hackÂ ? Â», Arthur Bouquet, Bitcoin.fr, 17 juin 2016.
- Â« A $50 Million Hack Just Showed That the DAO Was All Too Human, Klint Finley Â», Wired.com, 18 juin 2016.
- Â« To fork or not to fork, telle est la questionÂ ! Â» Simon Polrot, Ethereum-france.com, 27 juin 2016.
- Â« La Blockchain pose de sÃ©rieux problÃ¨mes de confiance, de droit… et de sÃ©curitÃ© Â», Eric A. Caprioli, Usine-digitale.fr, 8 juillet 2016.
- Â« Le Hard Fork Â«Â The DAOÂ Â» aura bien lieu, mode dâ€™emploi Â», Simon Polrot, Ethereum-france.com, 19 juillet 2016.
- Â« EthereumÂ : un Â«Â hard-forkÂ Â» controversÃ© pour oublier The DAO Â», Kevin Hottot, Nextinpact.com, 20 juillet 2016.
- Â« Le hard fork est un succÃ¨s Â», Gautier Marin-Dagannaud, Ethereum-france.com, 21 juillet 2016.
- Â« The Great Digital-Currency Debate: Â«Â NewÂ Â» Ethereum Vs. Ethereum Â«Â ClassicÂ Â» Â», Paul Vigna, Blog The Wall Street Journal, 1erÂ aoÃ»t 2016.
- Â« AprÃ¨s un Â« cyber-casse Â», la technologie blockchain se cherche un avenir Â», Eric Albert, LeMonde.fr, 26 septembre 2016.
- Â« Accenture imagine une blockchain modifiable pour les entreprises Â», Ninon Renaud,Â *Les Echos* , 5 octobre 2016.
- Â« Ethereum Â», Wikipedia.org, consultÃ© le 10 octobre 2016.

Categorie

1. Techniques

date crÃ©Ã©e
1 fÃ©vrier 2017
Auteur
jacquesandrefines