The DAO, Ethereum, et l'attaque de juin 2016

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 juin 2016

http://www.bortzmeyer.org/the-dao-ethereum-et-une-attaque.html

---

Vendredi 17 juin 2016, une attaque spectaculaire contre l'organisation The DAO a eu lieu, menant à la soustraction d'environ un tiers de ses fonds. Quelles leçons à en tirer ?

Si vous connaissez au moins un peu The DAO et Ethereum, vous pouvez lire tout de suite mes réflexions sur cette crise. Si vous ne connaissez pas, vous pouvez lire en anglais la bonne explication de Robert Graham <http://blog.erratasec.com/2016/06/etheriumdao-hack-similfied.html> ou bien en français les articles de Wikipédia sur Ethereum et les contrats.

Comme d'habitude lorsqu'un gros problème de cybersécurité est publié, on trouve du grand n'importe quoi dans les médias ou sur les rézosocios. Il est donc important de commencer par être précis sur les faits :

— La bogue n'était pas dans la chaîne de blocs Ethereum, ni même dans un autre élément d'infrastructure comme le compilateur Solidity. Elle était uniquement dans un contrat (un programme stocké dans la chaîne Ethereum), le contrat The DAO. Dire qu'Ethereum est menacé, ou que le concept de chaîne de blocs est menacé, revient à affirmer que PHP, voire le Web entier, est menacé parce qu'on a trouvé une bogue dans WordPress.
— Le voleur n'a pas réussi à récupérer les fonds soustraits à The DAO et il n'est pas sûr qu'il y arrive jamais. On est loin du casse du siècle. La transparence de la chaîne de blocs <http://www.bortzmeyer.org/tousapoil.html>, qui crée bien des vulnérabilités, fournit également les moyens d'empêcher le voleur de jouir du fruit de son forfait.
— L'attaque n'a rien à voir avec les problèmes de Mt. Gox, souvent cités par des journalistes paresseux (« crypto-monnaie ? Citons MtGox ! »). Il ne s'agit pas du piratage (ou de la malhonnêteté) d'un site centralisé particulier, mais d'une faille d'un contrat, un concept spécifique à Ethereum et qui n'a donc pas de vrai équivalent jusqu'à présent.

Mais cela ne veut pas dire que cette bogue est juste un détail sans importance et qu'on peut passer. Il s'agit d'une crise grave, dont il faudra tirer les leçons. D'abord, sur l'aspect technique (mais je parle des questions financières, légales et de gouvernance par la suite). L'origine du problème est une bogue dans le code de The DAO (pour les cœurs bien accrochés, voici les explications techniques complètes <http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/>). C'est une banalité de noter qu'on ne sait pas écrire du logiciel sans bogues. Tout logiciel a des bogues et, avant de confier des fonds à un contrat, il faut garder ce point en tête. Un des rares cas dans cette affaire où les pessimistes systématiques (« ce n'est pas moi qui a inventé ce truc, donc ça va rater ») avaient raison est quand ils pointaient le fait qu'il y aura forcément des bogues dans les contrats et, qu'en l'absence de mécanisme de recours, on aura du mal à en gérer les conséquences.

Cela ne veut pas dire qu'il faut baisser les bras et renoncer à programmer. Mais il faut changer, et d'état d'esprit, et sans doute de techniques utilisées. Emin Gün Sirer fait remarquer à juste titre <http://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack/> que l'écriture d'un contrat devrait ressembler à celle du code d'un avion ou d'une centrale nucléaire, pas à celle d'un site Web avec images et CMS. Or, aujourd'hui, pas mal de programmeurs de contrat sont plutôt dans la mentalité « si le code semble faire vaguemement ce qu'on veut, c'est bon », qui a mené à pas mal de désastres de sécurité sur le Web. Du point de vue des techniques utilisées, le même Sirer a raison de dire qu'il faut se poser la question des langages de programmation. Un langage impératif comme Solidity est-il vraiment la meilleure solution pour faire des contrats sûrs, et ne faudrait-il pas plutôt utiliser des langages plus adaptés, par exemple plus fonctionnels, inspirés d'Haskell ? Ces langages ont un fossé plus réduit entre la spécification et l'exécution. Plus radicale, la vérification formelle des contrats devrait-elle être la norme ? A priori oui, mais soyons prudents : les mécanismes de vérification formelle des programmes sont lourds et compliqués et ont leurs propres bogues.

En parlant de spécification, Vitalik Buterin a fait un très bon article <https://blog.ethereum.org/2016/06/19/thinking-smart-contract-security/> pour expliquer qu'une bogue, c'est par définition une déviation par rapport à la spécification, et que réduire le nombre de bogues implique d'être clair dans la spécification, ce qui est déjà un défi considérable. Dans un message non authentifié <http://pastebin.com/CcGUBgDG>, un individu se présentant comme l'attaquant prétend ainsi que, le code du contrat étant sa loi, par définition, toute opération faite avec le contrat The DAO est légale, y compris son vol. Il est bien sûr de mauvaise foi, mais on peut noter qu'il n'est pas possible de lui opposer une spécification précise de ce que le contrat était censé faire.

Autre leçon technique, un rappel que la complexité est l'ennemie de la sécurité. Le code de The DAO comprenait de nombreuses fonctions (comme celle permettant de retirer ses fonds, à l'origine de la bogue), ce qui augmentait la probabilité d'avoir une bogue. J'ai toujours expliqué que le terme de "*smart contract*" était dangereux car il encourageait les programmeurs à faire du code compliqué, alors qu'un bon contrat est au contraire trivial à lire et à analyser. Un programmeur de contrat ne devrait pas être admiré pour ses hacks astucieux mais au contraire pour sa capacité à faire du code ennuyeux et évident. (Je pensais à la validation d'un contrat <http://www.bortzmeyer.org/valider-contrats-ethereum.html> par ses utilisateurs, mais ce raisonnement s'applique également à la sécurité.)

A posteriori, il est clair qu'on est passé trop rapidement du petit contrat « "*Hello, World*" », à un gros truc complexe, avec plein de fric, comme The DAO. C'est un peu comme si, immédiatement après la traversée de la Manche par Blériot, on avait lancé sur l'Atlantique un avion de 500 passagers payants...

Il y a aussi des leçons à tirer de l'excessive focalisation sur l'argent, commune à une bonne partie de la communauté Ethereum, et aux médias. Les médias ont surtout présenté cette crise sous son angle financier (The DAO a perdu 50 millions, l'ether a baissé de 50 %, etc) alors que la chaîne de blocs Ethereum, contrairement à celle de Bitcoin, ne sert pas qu'à des transactions financières. Des tas de contrats ne consomment des ethers que pour acheter l'essence (le mécanisme par lequel on paie pour l'exécution

des contrats). Se focaliser sur les contrats à caractère financier, comme The DAO, empêche de voir toutes les potentialités de la chaîne de blocs (plusieurs articles ont ainsi présenté, de manière erronée, Ethereum comme étant juste « une crypto-monnaie concurrente de Bitcoin »). Et, évidemment, stocker autant d'argent allait attirer les voleurs. Bref, tant que les articles sur Ethereum continueront à mettre en avant le cours de l'ether en comparant avec la monnaie étatique traditionnelle, on n'arrivera pas à comprendre toutes les potentialités (disruptives, forcément disruptives) de la chaîne de blocs.

Il y a également bien des leçons à tirer de la crise de The DAO en terme de gouvernance de la chaîne de blocs. Normalement, les contrats « intelligents » étaient censés se gouverner tout seuls. Le code est la loi, il est exécuté fidèlement par la la machinerie Ethereum, et il n'y a donc pas de place pour l'interprétation ou l'action humaine. Face à la crise et au vol d'ethers, que fallait-il faire ? En schématisant, il y avait deux positions : les principiels voulaient qu'on laisse les choses se produire. The DAO avait une bogue, ils perdent leur argent. Selon eux, toute autre solution aurait mis en cause ce qui était justement l'un des principaux arguments en faveur des contrats, leur côté automatique, insensibles aux passions et aux manipulations humaines. Les réalistes, de l'autre côté, considéraient qu'on ne pouvait pas rester sans rien faire et voir le voleur emporter l'argent. Ils prônent un "*fork*", c'est-à-dire une scission délibérée de la chaîne : une nouvelle version des logiciels est produite, appliquant des règles différentes (par exemple empêchant les transferts depuis le compte du voleur). Certains nœuds du réseau adoptent le "*fork*", d'autres pas. Si les premiers sont plus nombreux, leur chaîne est considérée comme la bonne, les autres n'ont plus qu'à se soumettre, ou à partir et faire leur chaîne de leur côté (ce qui serait évidemment une grosse tuile pour Ethereum). Vu superficiellement, cela serait une décision centrale dans un système, la chaîne de blocs, conçu justement pour éviter cela. Mais si une telle décision peut en effet être prise par un petit groupe de gens (en gros, les développeurs des logiciels qui font marcher la chaîne ; notez que, contrairement à Bitcoin, il n'existe pas qu'un seul logiciel), sa mise en œuvre, elle, dépend de tous les gens qui gèrent des nœuds (enfin, surtout des mineurs), et qu'il faut convaincre. C'est pour cela que les articles de Buterin, par exemple, insistent sur le fait que les développeurs comme lui n'imposent pas, ils proposent. Une attitude tout à fait opposée était celle de de Stephan Tual qui, dans ce tweet <https://twitter.com/slockitproject/status/743790742146023424> et celui-ci <https://twitter.com/slockitproject/status/743790901877706752> accusait tout opposant (ceux qui refusent le "*fork*", les principiels), d'être forcément en cheville avec le voleur, et appelait même à les dénoncer ! Ce délire robespierro-stalinien a certainement fait bien plus de mal à Ethereum que la bogue elle-même.

Un des éléments du débat était aussi le statut particulier de The DAO. Pourquoi "*forker*" juste pour eux, disent les principiels ? Fera-t-on pareil à chaque fois qu'un contrat a une bogue ? Le seul argument des réalistes est la taille : The DAO est « "*too big to fail*" ». Après que tant de gens, aussi bien à l'intérieur de la communauté Ethereum qu'à l'extérieur, aient entretenu une certaine confusion entre Ethereum et The DAO, il est difficile de laisser tomber le canard boiteux. Même si cela a mené à des injustices flagrantes, comme l'appel lancé par Slock.it <https://blog.slock.it/dao-security-advisory-live-updates-2a
à faire une attaque par déni de service contre toute la chaîne Ethereum, pour ralentir l'attaquant (cette boîte a fait une bogue, et la fait payer à tout le monde).

Cette crise pose donc évidemment la question de ce mode de gouvernance « le code [des contrats] est la seule règle ». Thibault Verbiest a ainsi estimé que ce n'était pas souhaitable <https://www.linkedin.com/pulse/ethereum-attaqu%C3%A9-le-code-ne-peut-%C3%AAtre-la-seule-loi-thibault-
et qu'il fallait une régulation étatique des chaînes de blocs.

Les habituels ricaneurs ont évidemment proclamé qu'ils avaient bien raison, et que la chaîne de blocs était fichue, et que cela les faisait bien rigoler (manger le popcorn en regardant le film est évidemment plus facile que de travailler). Mais on est loin d'une telle conclusion. Si The DAO ne survivra probablement pas à cette crise, l'idée de contrat, les autres contrats et Ethereum lui-même sont bien vivants et continueront, une fois la crise actuelle digérée. Les contrats sont une innovation et, comme toute innovation, les débuts sont un peu cahotiques. Lors des débuts de l'aviation, le projet le plus

---

http://www.bortzmeyer.org/the-dao-ethereum-et-une-attaque.html

sérieux, celui qui avait de très loin le plus gros budget et la plus grande attention des médias était celui de Langley. Le 8 décembre 1903, son projet se termine après un nouveau crash, qui mène beaucoup de gens à affirmer que l'aviation est morte. Une semaine après, le premier avion des frères Wright décolle avec succès... Matthew Spoke estime même que cette attaque est une bonne chose <http://www.coindesk.com/dao-attack-good-thing-ethereum/>, elle va forcer à être plus sérieux.

PS : j'ai oublié d'en parler initialement, mais voici la déclaration de conflit d'intérêt. Je ne possède pas (et n'ai jamais possédé) de "*tokens*" (de parts) de The DAO.

---

http://www.bortzmeyer.org/the-dao-ethereum-et-une-attaque.html