À QUOI TIENNENT LA SÉCURITÉ ET LA FIABILITÉ DES CRYPTOMONNAIES ?

Les cryptomonnaies n'étant *in fine* que des logiciels, leur fiabilité provient de leur code source. N'importe qui peut créer une cryptomonnaie et lever des fonds en la vendant par l'intermédiaire d'une offre initiale d'unités de monnaie ; mais ce n'est pas un hasard si les deux cryptomonnaies les plus populaires, le bitcoin et l'ether, ont été développées par des spécialistes en informatique. Cela dit, même des monnaies reposant sur des systèmes techniques impressionnants peuvent être exposées au risque. L'« organisation autonome décentralisée » nommée The DAO, un fonds d'investissement en ethers utilisant le système Ethereum, et qui a levé plus de 100 millions de dollars en 2016, souffrait d'un bug grâce auquel des pirates ont subtilisé des ethers pour une valeur de 50 millions de dollars.

33 %

des conversions entre bitcoins et monnaies usuelles ont été piratées entre 2009 et 2015, selon un rapport de 2017 du département de la Sécurité intérieure des États-Unis.

COMMENT RÉGULER UN SYSTÈME DÉCENTRALISÉ ?

Étant donné la réputation sulfureuse des monnaies virtuelles décentralisées, on pourrait supposer qu'elles ont été créées pour supprimer la réglementation financière, ou au moins lui échapper. Mais ce n'est pas tout à fait exact. Le système du bitcoin est lui-même doté de nombreuses règles, après tout ; simplement, elles sont définies et implémentées par le code source (et l'activité collective de son réseau pair à pair) plutôt que par des États ou des institutions financières. « Toute l'innovation du système Bitcoin réside dans le fait qu'il évite une gestion humaine de la tenue de dossiers », dit Patrick Murck, juriste qui travaille sur la politique et la réglementation des blockchains à l'université Harvard. L'objectif déclaré d'Ethereum, soutenir le déploiement de contrats intelligents autonomes, est essentiellement un objectif de contrôle. Et une blockchain n'est rien d'autre qu'un système de règles dictant mathématiquement ce qui peut être fait ou non avec l'enregistrement des données dans une base.

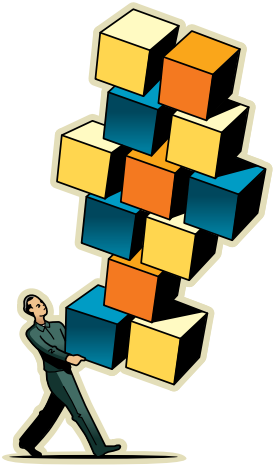
Ce qui est toujours important avec la régulation financière, qu'elle soit décentralisée ou non, c'est qui a le privilège de réguler, et comment. D'ailleurs, les États interviennent parfois pour réguler de l'extérieur l'usage des cryptomonnaies. Ainsi, en 2013, la Chine a interdit les cryptomonnaies dans son système bancaire, et en septembre dernier elle a bloqué l'accès aux bourses d'échange de cryptomonnaies (permettant par exemple d'acheter ou vendre des bitcoins contre des monnaies nationales). Les États-Unis et le Japon sont en train d'intervenir pour réguler ce type de plateformes et les « offres initiales d'unités de compte » avec la même vigilance que celle qu'ils exercent dans le cadre des ventes d'actions et des activités de placements bancaires.

Une application future de la technologie des blockchains concerne la sécurisation des identités numériques. D'après l'investisseur en capital-risque Charlie Morris, il pourrait émerger de nouvelles cryptomonnaies qui réunissent identité numérique et information financière. Elles n'auraient pas l'anonymat du système Bitcoin (Charlie Morris estime que seuls quelques centaines de détenteurs de bitcoins paient honnêtement leurs impôts sur ces avoirs). Mais quand la monnaie numérique se généralisera, le compromis entre sécurité perçue et stabilité rendra peut-être la surveillance tolérable, voire souhaitable. Comme l'exprime Patrick Murck : « Si je vous confie un bien à garder en mon nom et avec lequel vous pouvez effectuer des transactions, qu'il s'agisse de bitcoins ou d'ours en peluche, alors vous êtes soit régulé, soit sur le point de l'être. »

LES BLOCKCHAINS SONT-ELLES VULNÉRABLES ?

Jusqu'à présent, la blockchain du bitcoin, qui est la première, et à ce jour la plus vaste et la plus utilisée, n'a jamais été défaillante ou piratée. Mais cela ne signifie pas que toute blockchain est invulnérable par définition. « Il n'existe pas de technologie parfaite », prévient Emin Gün Sirer, de l'université Cornell, codirecteur de l'Initiative pour les cryptomonnaies et contrats. Voici trois points faibles que peut présenter une blockchain :

L'attaque des 51 %. La sécurité des réseaux de cryptomonnaie à base de blockchain repose sur deux ressources sans fond : la rapidité et l'appât du gain de leurs mineurs. Mais il est en théorie possible de vaincre ces deux obstacles. Pour subvertir le mécanisme de consensus de la blockchain, les pirates devraient prendre le contrôle d'une majorité (51 %) de la puissance du réseau. Ils pourraient alors, par exemple, bloquer la validation des transactions d'autres utilisateurs. Le réseau Bitcoin, avec ses milliers de nœuds, semble assez bien protégé contre une telle attaque. Mais des cryptomonnaies plus modestes sont exposées : l'une d'elles, Krypton, a ainsi été attaquée en 2016 par un groupe nommé 51crew. Même les blockchains ne faisant pas appel au procédé du minage sont vulnérables parce qu'elles reposent encore sur « l'hypothèse qu'une majorité de nœuds de leur réseau sont bienveillants », prévient Emin Gün Sirer.



La bonne vieille erreur humaine. Pour affecter la blockchain elle-même, il faudrait certes déplacer des montagnes (ou l'équivalent informatique). Mais le reste est vulnérable. En 2014, Mt. Gox, une plateforme d'échange entre devises classiques et bitcoins, a été victime d'une mauvaise gestion et d'un code défectueux ; elle a ainsi perdu 850 000 bitcoins (valant 620 millions de dollars à l'époque). Par ailleurs, si votre portefeuille numérique est rempli de cryptomonnaie et que vous perdez votre mot de passe, cet argent est presque certainement perdu. Comble de l'ironie, certains utilisateurs de cryptomonnaies gardent une copie de leurs codes confidentiels dans un coffre bancaire...

L'engorgement. Comme chaque nouveau bloc ajouté à une blockchain revalide tous les blocs précédents, chaque nœud effectuant la validation a besoin d'une copie de la dernière version en date de la chaîne entière. Avec déjà plus de 150 gigaoctets, la blockchain du bitcoin devient difficile à manipuler. Le registre d'Ethereum, conçu pour être plus flexible (afin de gérer des transactions plus complexes, telles que des contrats intelligents), est déjà plus gros que celui du bitcoin. Si tout le monde se mettait à l'utiliser, les superordinateurs à haute performance seraient-ils les seuls à pouvoir gérer la charge de données ? Il en résulterait une recentralisation du réseau, contraire à l'objectif des registres distribués !