LARGEUR.COM
MAGAZINE D'AVANT-GARDE DEPUIS 1999

Online lesen

Datum: 31.03.2016

echanges JEUDI 31 MARS 2016

Blockchain, comment le registre distribué va révolutionner la société

On commence à mesurer l'immense potentiel de la blockchain, une forme de registre des transactions numérique sûre et infalsifiable. L'onde de choc créée par cette technologie liée au bitcoin s'étend bien au-delà du domaine financier.

Par Guillaume Meyer

Des paiements par internet sont détournés vers des poches malveillantes. Un parti politique conteste le résultat d'une élection. Deux auteurs se disputent la paternité d'une idée. Quel est le point commun entre ces dysfonctionnements? Tous pourront être évités si une technologie révolutionnaire, la blockchain, s'impose dans les domaines en question.

Le commun des mortels devra sans doute attendre plus d'une décennie pour en réaliser les implications concrètes. Mais la blockchain n'est déjà plus de la science-fiction. Cette technologie forme la colonne vertébrale du bitcoin, la mystérieuse monnaie électronique apparue en 2009. Elle constitue le mécanisme qui permet au bitcoin d'exister sans banque centrale. En effet, ce n'est pas une institution centralisée qui décide d'émettre des bitcoins et gère les transactions dans cette monnaie: le réseau s'auto-administre par protocole informatique.

Concrètement, la blockchain prend la forme d'un registre numérique qui consigne tous les échanges effectués entre les utilisateurs depuis sa création. A tout moment, le système sait qui possède quoi et en fournit la preuve. Chaque ordinateur connecté au réseau héberge une copie de ce journal, certains usagers (volontaires) laissant tourner leur machine en permanence pour participer au processus d'authentification. Ces derniers sont incités à mettre à disposition leur matériel par une forme de loterie (appelée minage) où le premier utilisateur qui effectue la validation reçoit des bitcoins. Une fois qu'un bloc de transactions est approuvé par le réseau, il s'ajoute au registre, formant une chaîne de blocs: la blockchain.

La deuxième révolution internet?

«Ce mécanisme permet d'atteindre un consensus global sur un historique d'événements, explique Maxime Augier, doctorant en cryptographie à l'EPFL et connaisseur du projet. Cela signifie que tous les participants sont d'accord sur le contenu de ce journal. Et c'est parce qu'ils ont mis en place ce système de consensus que toute tentative de tricherie, en effaçant ou en modifiant des informations a posteriori, est vouée à l'échec.» Ces transactions virtuelles sont donc irréversibles: impossible de faire marche arrière à moins d'obtenir l'assentiment du réseau.

La blockchain est également réputée incorruptible, un individu malveillant isolé n'ayant aucun poids. «Pour mettre la main sur le réseau, l'adversaire doit contrôler plus de 50% de sa puissance de calcul totale, précise le spécialiste. On espère qu'il s'agit d'un scénario théorique, mais on ne peut pas en être certain: le cas échéant, l'individu en question prendra toutes ses précautions pour ne pas être détecté.» A cette limite s'en ajoute une autre: le gaspillage énergétique associé au travail des ordinateurs qui font tourner la blockchain.

Cela n'enlève rien aux avantages de cette technologie, selon Maxime Augier. «A l'heure actuelle, il n'existe pas d'autre mécanisme aussi simple et populaire permettant d'atteindre ce consensus global. Ce système a fait la preuve de sa viabilité. Et le principe d'un journal qui offre seulement la possibilité d'écrire, et pas celle

de modifier, peut trouver des applications intéressantes bien au-delà des transactions financières.» C'est bien pour cela que, outre la finance, des domaines aussi divers que le e-voting et la propriété intellectuelle s'intéressent de près à la blockchain (voir encadrés).

«On va au-devant d'une révolution avec la blockchain, estime Alexis Roussel, cocréateur de Bity , une plateforme d'achat et de vente de bitcoins. L'onde de choc sera similaire à celle de l'apparition d'internet, qui n'intéressait que les scientifiques à l'origine et dont on ne peut plus se passer aujourd'hui.»

———

ENCADRES

Banques: une baisse massive des coûts

La finance a été le premier secteur à s'intéresser de près à la blockchain pour des applications en dehors du bitcoin. La raison? «Ce mécanisme permet d'effectuer des transactions financières plus rapidement, plus sûrement et à moindre coût», résume Andreas Lenzhofer, associé de PwC Strategyand. Ce spécialiste de la blockchain précise que «le client ne percevra pas clairement le changement, qui touche avant tout les fournisseurs d'infrastructures».

Pour mémoire, la plupart des systèmes de paiement sont centralisés — les transactions sont validées par la banque centrale — tout en impliquant de nombreux intermédiaires. Quand les sociétés financières font des affaires entre elles, elles doivent synchroniser leurs registres internes: cette lourde tâche peut prendre plusieurs jours, ce qui mobilise du capital et augmente le risque. Au contraire, avec un système de validation décentralisé, les transactions pourraient être réglées en quelques minutes ou secondes. Les établissements pourraient ainsi économiser jusqu'à 20 milliards de dollars par an d'ici à 2022, selon la banque Santander.

Les grandes banques ne veulent pas rater le train. UBS, Goldman Sachs, JP Morgan et 22 autres établissements ont investi à cette fin dans la startup R3 CEV , chargée de développer une architecture commune pour des registres privés. Autre exemple: le Nasdaq, le marché américain des valeurs technologiques, a lancé un système basé sur la blockchain pour enregistrer les échanges dans les sociétés non cotées. La première transaction utilisant ce canal a été réalisée fin 2015.

———

Vote électronique: une évolution nécessaire

Et si la blockchain représentait l'avenir du vote électronique? La sécurité reste l'obstacle principal à la généralisation du e-voting — notamment par internet — dans le monde. Le caractère sûr et infalsifiable d'un registre décentralisé constitue un atout de taille dans ce contexte. «C'est une évolution nécessaire, estime Eric Dubuis, professeur à la Haute école spécialisée bernoise (BFH) et spécialiste du e-voting. Mais on ne pourra pas simplement répliquer le mécanisme du bitcoin: ona besoin d'un modèle sui generis.»

L'idée consiste à distribuer le «tableau d'affichage» virtuel des résultats du vote sur un certain nombre d'ordinateurs, couplés mais indépendants. La synchronisation de tous les registres permet d'éliminer d'éventuels écarts dans l'une ou l'autre des bases de données. «Mais vu la masse d'informations, il ne serait pas efficace de synchroniser les registres en continu, comme dans le cas du bitcoin, souligne Eric Dubuis. L'harmonisation des bases de données devrait plutôt se faire à intervalles réguliers.»

Qui seraient les participants au processus de validation? «Pour aboutir au registre électoral décentralisé sur

blockchain, il faut d'abord que des oracles se développent, c'est-à-dire des arbitres qui se prévaudront de leur réputation pour pouvoir valider le réel dans le numérique, explique Alexis Roussel, cocréateur de Bity. Une fois qu'ils se seront imposés aux quatre coins du monde, il y aura un mécanisme de confiance tellement fort que les Etats pourront se déposséder de certains pouvoirs pour la construction du monde numérique.»

———

Propriété intellectuelle: un système de preuves

L'artiste qui crée un morceau de musique et le scientifique qui produit un papier de recherche ont une préoccupation commune: protéger leur bébé contre le pillage. La blockchain devrait leur permettre de le faire plus efficacement, en fournissant une preuve qu'ils sont les auteurs de leur travail. «La copie sera toujours possible, mais la première référence du document sera gravée dans le marbre de la blockchain, expose Alexis Roussel. Si vous produisez quelque chose, que vous l'enregistrez dans la base de données décentralisée et que vous êtes le premier à le faire, vous pourrez toujours prouver que vous en êtes l'auteur.»

Où enregistrer son bien? Par exemple sur le site alexandria.media , une plateforme d'auto-archivage et de diffusion. L'intérêt de cette plateforme, utilisée notamment par la diva électro Imogen Heap, est qu'elle fournit des mécanismes de paiement (en bitcoins) pour rémunérer les auteurs. «Quand vous archivez un fichier musical sur le réseau, reprend Alexis Roussel, vous définissez un mode de partage: pay-per-view, pourboire… Et si vous partagez votre musique, vous ne payez plus pour l'écouter. Comme dans le cas du bitcoin, la participation au réseau est récompensée.»

Cette initiative montre comment la blockchain peut révolutionner la gestion des droits numériques, selon le spécialiste: «L'information nécessaire au référencement et au paiement de l'auteur est fournie automatiquement à travers le registre commun. Cette automatisation permet de se passer des sociétés complexes comme celles qui gèrent les droits.»

———

Le mystérieux M. Nakamoto

Apparu en 2009, le bitcoin n'a pas encore livré tous ses secrets. Il faut dire que le père de la monnaie virtuelle — et de la technologie blockchain — n'a jamais révélé son identité, préférant se dissimuler derrière le pseudonyme de Satoshi Nakamoto. Des journalistes se sont juré de retrouver le géniteur. En décembre dernier, le magazine américain Wired a cru le démasquer en la personne de Craig Steven Wright, un Australien anonyme de 44 ans, informaticien archi-diplômé de son état. Mais d'autres sources affirment qu'il s'agit d'un canular. A ce jour, le mystère reste entier.

———

Une version de cet article est parue dans le magazine Technologist (no 8).

Pour souscrire un abonnement à Technologist au prix de CHF 45.- (42 euros) pour 8 numéros, rendez-vous sur technologist.eu

LARGEUR.COM
MAGAZINE D'AVANT-GARDE DEPUIS 1999

Datum: 31.03.2016