HIRAM FINANCE

Les registres distribués dans l'industrie financière

Pierre-Jean Belin

Octobre 2015

La technologie des registres distribués, « blockchains » dans la terminologie anglo-saxonne, pourrait radicalement transformer les infrastructures traditionnelles de l'industrie financière en simplifiant les processus d'enregistrement, de conservation, de règlement, de rapprochements et de reporting. Les intervenants en retireraient de nombreux avantages : diminution notable du temps nécessaire aux confirmations, réduction des risques associés et des coûts de transaction.

Un blockchain, ou encore chaîne de blocs, peut être vu comme un registre contenant des informations horodatées, les blocs, qui s'empilent les unes sur les autres. Ce registre est indestructible, infalsifiable et partagé. Les informations qui y sont consignées sont par exemple des messages de transactions portant sur des devises, des titres, etc.[1]. Chaque message est signé numériquement, ce qui garantit que l'identité de son auteur ne peut pas être usurpée. Le système d'unité de compte et de paiement Bitcoin repose sur la technologie des blockchains.

Le registre est indestructible car distribué : un grand nombre de copies sont maintenues à jour via un réseau de pair à pair. La destruction de quelques-unes de ces copies n'a aucune importance tant que les pairs peuvent accéder à l'internet et communiquer entre eux. Distribuer le registre permet d'éviter qu'une entité en prenne le contrôle.

Le registre est infalsifiable grâce à l'utilisation combinée de condensats numériques et de preuves de travail. Présentons ces deux concepts :

- Le condensat d'un fichier est une courte chaîne de caractères qui caractérise ce fichier. C'est en quelque sorte l'équivalent d'une empreinte digitale pour un être humain. Il est impossible dans la pratique de modifier un fichier sans modifier son condensat.
- Une preuve de travail est un calcul qui nécessite du temps pour être mené à son terme mais qui peut être vérifié très rapidement. Un exemple est la factorisation en facteurs premiers d'un nombre entier. Il n'existe pas d'algorithme permettant de trouver les facteurs premiers d'un nombre entier rapidement ; en revanche, une fois ceux-ci trouvés, vérifier le résultat est très facile via de simples multiplications. L'intérêt de la preuve de travail est de contraindre un système informatique à attendre avant de mener une action même si ses capacités de calcul sont très importantes. La durée de la preuve ne doit pas être trop longue car il ne faut pas perdre de vue qu'à l'issue du calcul, le système doit effectuer une action. Cette durée est définie en fonction des besoins. Par exemple, dans le cas des Bitcoins, la durée des preuves de calcul est ajustée par le réseau de manière qu'en moyenne, un bloc soit ajouté à la chaîne toutes les dix minutes.

[1] La technologie des blockchains permet d'enregistrer « dans le marbre » et sécuriser tout type d'information : des contrats notariés, des brevets, etc. A titre d'illustration, le gouvernement du Honduras va lancer en 2016 un programme pilote de gestion du cadastre via une technologie basée sur les blockchains. L'objectif est de contrer la corruption qui mine les institutions de ce pays.

En plus des messages qu'il véhicule, chaque bloc contient le condensat des blocs précédents, ainsi que le résultat d'une preuve de travail qui dépend du condensat. A chaque nouvelle insertion, le condensat du bloc précédent est incorporé au bloc courant. Il n'est alors pas possible de falsifier une partie du blockchain car les condensats ne correspondraient plus. La stratégie de falsification préservant des condensats cohérents nécessite de reconstruire la partie du blockchain qui contient l'information falsifiée et au-delà. C'est ici que la preuve de travail intervient car l'attaquant est alors obligé de mobiliser une puissance de calcul prohibitive pour recalculer le résultat de la preuve à chaque fois qu'il doit réinsérer les blocs nécessaires à la reconstitution du blockchain.

Le registre est partagé : chacun peut écrire de l'information dans le blockchain sans être obligé de passer par une autorité centrale comme un dépositaire ou une chambre de compensation.

Des mécanismes reposant sur des évaluations de consensus sont mis en place afin de propager la mise à jour du blockchain au sein des différents nœuds du réseau pair à pair.

Pour minimiser les risques de mauvaise conception et de bogues, la spécification du blockchain et le code source de son implémentation sont ouverts à tous : développeurs, utilisateurs, spécialistes en sécurité informatique, universitaires, etc.

Les applications dans le domaine de la finance sont multiples. Il y a tout d'abord les activités classiques de post-marché comme la gestion des titres au sens large - conservation, transferts, opérations sur titres – ou encore le transfert des devises réelles où le registre distribué remplace les systèmes de comptabilisation des conservateurs ou des compensateurs. Il est aussi possible de confier au blockchain la gestion de contrats en intégrant le principe des contrats astucieux – « smart contracts » dans la technologie anglo-saxonne. Il s'agit par exemple de programmer les conditions d'exécution de contrats dérivés dans le blockchain via un langage formalisé qui exécute des actions comme des valorisations, des appels de collatéral et des règlements. Les insertions et les validations dans les blocs peuvent se faire très rapidement avec par exemple pour application des règlements ou des appels de marge en temps quasi réel. Notons aussi qu'une transaction validée est irrévocable et ne peut pas être annulée.

Les cadres juridique et réglementaire doivent être adaptés afin de répondre aux défis posés par ces nouveaux types d'architecture distribuée. Le Berkman Center For Internet & Society, un centre de recherche lié à l'université de Harvard mène de nombreux travaux sur les aspects juridiques des devises numériques et des blockchains. https://cyber.law.harvard.edu/node/99093

L'ESMA – European Securities and Markets Authority – a lancé une consultation en avril 2015 portant sur les « investissements utilisant des devises virtuelles ou la technologie des registres distribués » https://www.esma.europa.eu/news/ESMA-seeking-information-new-developments-virtual-currency-investment. L'objectif est de comprendre l'apport de ces nouvelles technologies et les risques qu'elles peuvent faire courir. Les banques et autres prestataires de services d'investissement déclarent suivre avec la plus grande attention les développements portant sur les registres distribués. Certains mènent des tests en interne afin de se familiariser avec le concept. Tous considèrent que le potentiel des registres distribués est très important, même si la technologie est encore balbutiante et que de nombreux écueils législatifs et réglementaires doivent être surmontés.

Des acteurs non financiers, startups et communautés, commencent à occuper le terrain en lançant des projets qui restent pour l'instant majoritairement expérimentaux.

- R3, une entreprise basée à New York, a fédéré neuf très grandes banques - Goldman Sachs, JP Morgan et UBS notamment – autour d'un projet visant à créer un registre distribué. http://r3cev.com
- Ethereum est un projet ambitieux qui va au-delà du simple registre distribué. Il propose la gestion de contrats astucieux dont les clauses s'exécutent dans le blockchain. https://www.ethereum.org/
- Le projet Bitcoin, qui est à l'origine du concept de blockchain, propose un service qui peut être considéré comme opérationnel. Son registre distribué a prouvé sa robustesse en résistant à toutes les tentatives d'attaques. En revanche, son environnement a fait l'objet de nombreux scandales. https://bitcoin.org/fr/
- Notons pour mémoire que la société Ripple Lab Inc, basée à San Francisco, propose un système distribué de compensation et de règlement de transactions destiné aux banques. Cependant, la technologie sous-jacente ne repose pas strictement sur un blockchain https://ripple.com/integrate/executive-summary-for-financial-institutions/.

L'augmentation de la puissance de calcul et des capacités de stockage distribué permet de transformer ces concepts en toutes sortes d'applications innovantes qui pourraient révolutionner la chaîne de valeur des infrastructures financières.

Autres références :

- Pour la science – N°449 – Mars 2015 – Les blockchains, clefs d'un nouveau monde – Jean-Paul Delahaye
- Pour la science – N°438 – Avril 2014 – Les preuves de travail – Jean-Paul Delahaye