

Qu'est-ce qu'une « chaîne de blocs » et quels sont ses enjeux en PI?

Yuhon Tom Zhang
ROBIC, S.E.N.C.R.L.

Avocat et agent de brevets au Canada et aux États-Unis

Lorsqu'on pense aux systèmes informatiques qui traitent de grandes quantités de données, ce sont habituellement les grappes de serveurs composées de plusieurs ordinateurs centraux et fonctionnant dans une installation climatisée qui nous viennent à l'esprit. L'informatique répartie se trouve à l'extrémité opposée du spectre; dans ce type de système, les données sont stockées de manière disparate dans un réseau de serveurs faiblement connectés. La « chaîne de blocs » (blockchain en anglais) est un concept particulièrement intéressant qui applique l'informatique répartie.

Une chaîne de blocs est un type de données réparties qui sont stockées dans plusieurs ordinateurs d'un réseau pair à pair et qui préserve l'intégrité des données, en dépit de leur caractère décentralisé. Dans une chaîne de blocs, les transactions sont enregistrées dans des « blocs » qui sont stockés dans chacun des ordinateurs du réseau. Les transactions validées stockées dans un bloc sont liées à toutes les transactions précédentes, formant ainsi une chaîne de blocs. Une nouvelle transaction est validée par la vérification de celle-ci par rapport aux transactions précédentes dans la chaîne de blocs stockée dans l'ordinateur. Étant donné que la chaîne de blocs est stockée dans plusieurs ordinateurs, les données stockées peuvent être plus difficiles à pirater que les méthodes classiques, qui stockent toutes les données dans un endroit central.

Les chaînes de blocs et la cryptomonnaie

La technologie des chaînes de blocs est la technologie qui soutient le bitcoin et d'autres types de cryptomonnaie semblables. Les transactions de bitcoins sont stockées dans des registres de transactions de chaînes de blocs. Le propriétaire d'un bitcoin donné stocke les authentifiants numériques de ses avoirs en bitcoins dans un portefeuille numérique. Ces authentifiants sont utilisés pour valider la propriété au moyen de la vérification du registre de la chaîne de blocs. Par exemple, si la partie A transfère un bitcoin à la partie B, la partie A fournit ses authentifiants, et le registre de la chaîne de blocs est vérifié pour déterminer si la partie A est bien le véritable propriétaire du bitcoin. La chaîne de blocs est ensuite mise à jour afin d'indiquer que la partie B est maintenant le nouveau

propriétaire du bitcoin transféré. Il est actuellement possible d'acheter différents biens ou services en ligne avec des bitcoins.

Les entrées dans le registre de la chaîne de blocs sont protégées à l'aide de la cryptographie, donnant ainsi le nom cryptomonnaie. Les pairs du réseau vérifient la chaîne en décodant les entrées encryptées. Des nouvelles d'unités d'une cryptomonnaie sont accordées comme récompense pour ceux qui connectent leurs ordinateurs au réseau pour participer à la vérification des transactions.

Actuellement, il est possible d'acheter des biens et des services en ligne en utilisant divers types de cryptomonnaie. Il est aussi possible d'échanger un type de cryptomonnaie contre d'autres types de cryptomonnaie, ou même des devises réelles.

Au-delà de la cryptomonnaie

Étant donné le potentiel que représente l'utilisation des chaînes de blocs à titre de registre public, on a déjà commencé à imaginer comment on pourrait utiliser les chaînes de blocs dans des applications autres que la cryptomonnaie. Ces applications sont appelées « Blockchain 2.0 ». À cet égard, les contrats intelligents sont particulièrement intéressants. Les modalités d'un tel contrat peuvent être établies dans un code informatique. Lorsque deux parties à un contrat exécutent leurs obligations contractuelles respectives, un programme informatique intelligent peut vérifier et faire respecter les conditions du contrat. Le contrat intelligent comme tel, l'exécution du contrat et la vérification peuvent être stockés dans la chaîne de blocs.

Les contrats intelligents sont particulièrement bien adaptés au monde en ligne. Un contrat peut définir les actions des parties en ligne ainsi que l'échange d'une somme monétaire qui aura lieu (ex : l'écoute d'une chanson via un service de diffusion et le paiement d'une royauté à l'auteur du chanson).

Cela ouvre la possibilité aux micropaiements décentralisés, comme le paiement de frais très peu élevés (par ex. quelques cents) en contrepartie de l'accès à de petites parties de contenu numérique (par ex. payer pour lire un article de journal ou écouter une chanson). Il est possible de penser qu'à l'avenir, les contrats intelligents puissent jouer un rôle important dans un monde de plus en plus automatisé.

Étant donné ce vaste potentiel, il n'est pas surprenant de voir se multiplier les jeunes entreprises technologiques afin de fournir des approches novatrices dans l'offre de services fondés sur les chaînes de blocs. Parallèlement, de grandes sociétés financières ont aussi commencé à mener des activités de recherche et de développement dans ce marché. Sans surprise, afin de pouvoir revendiquer une partie de cet espace et ne pas rester derrière, les entreprises ont également commencé à déposer des demandes de brevet pour les nouvelles technologies axées sur les chaînes de blocs qu'elles ont développées.

La technologie des chaînes de blocs est-elle brevetable?

La question de l'admissibilité des inventions mises en œuvre par ordinateur à la protection par brevet fait l'objet de débats continus dans de nombreux pays. Aux États-Unis, les tribunaux ont rejeté l'interdiction totale des brevets sur les inventions liées à un logiciel, mais ont statué que les inventions visant des idées abstraites, comme les pratiques et les méthodes économiques fondamentales pour organiser le comportement humain, n'étaient pas brevetables.

Au Canada, la Cour d'appel fédérale a statué en 2011, dans la cause portant sur la commande en un clic d'Amazon, qu'une invention ne doit pas être une idée désincarnée, et qu'elle doit avoir une méthode d'application pratique et qu'elle doit produire des résultats ou des effets utiles de façon commerciale. Ici encore, on n'interdit pas totalement les brevets sur les inventions logicielles en vertu de la loi canadienne.

En Europe, bien que les logiciels ne soient pas brevetables en soi, l'interdiction ne s'applique pas aux inventions de systèmes informatiques complets.

Le fait qu'une invention liée à une chaîne de blocs soit admissible à un brevet dépend de la nature particulière de l'invention. Étant donné que le cœur de la chaîne de blocs est de nature technologique (on définit des structures de données, des algorithmes et des configurations de réseau), il est probable que ces innovations soient admissibles à la protection par brevet dans de nombreux pays. Les innovations qui s'appliquent à la technologie de la chaîne de blocs de manière novatrice afin de modifier les pratiques financières actuelles seront également probablement admissibles à un brevet. Cependant, l'application d'une technologie générique de la chaîne de blocs à des pratiques financières reconnues sera vraisemblablement plus difficile à protéger.

Protection par brevet et innovation future

Selon une vision pessimiste, les brevets sont considérés comme des obstacles à l'innovation future. Alors que certaines entreprises font leur place sur le marché des chaînes de blocs, d'autres pourraient être empêchées de mener des activités et d'innover dans cet espace.

Il serait également possible que les technologies des chaînes de blocs convergent vers un ensemble commun de pratiques standard et de normes technologiques, à mesure que la technologie évolue. La normalisation semble probable, si l'on considère le fait que des régimes juridiques et réglementaires seront certainement mis en place. Par conséquent, un ensemble de brevets essentiels pourrait également émerger, et les entreprises souhaitant mener leurs activités sur ce terrain devront obtenir des licences pour de tels brevets. Ce scénario ressemble à celui qui prévaut dans l'industrie des télécommunications.

Une augmentation des activités de « troll aux brevets » est également à prévoir. Les entreprises qui détiennent des brevets pour la technologie de la chaîne de blocs mais qui ne mènent pas d'activités à cet égard tenteront de tirer profit de leurs brevets en entamant des poursuites ou en cherchant à obtenir des droits de licence des autres entreprises qui sont actives sur ce terrain. Cependant, si les bureaux des brevets continuent d'examiner

les demandes de brevet de manière stricte et n'accordent pas de brevets trop larges, les activités de troll aux brevets pourraient être inférieures à celles qui ont cours actuellement.

Chaînes de blocs, brevets et code source libre

Il y a une contradiction fondamentale philosophique entre les logiciels à code source libre et le processus de brevetage. Alors que les logiciels à code source libre sont fondés sur le concept que toutes les innovations devraient être utilisées gratuitement par tous, l'obtention d'un brevet vise à empêcher les autres d'utiliser les innovations brevetées. De nombreux logiciels à code source libre détiennent une licence aux termes de conditions qui obligent le titulaire de licence à rendre le logiciel accessible à autrui. Les tribunaux doivent maintenant apporter une réponse à la question des répercussions des licences de logiciels à code source libre sur les brevets qui couvrent les innovations élaborées au moyen de tels logiciels.

Une grande partie des technologies des chaînes de blocs sont développées au moyen de logiciels à code source libre. Par exemple, le logiciel permettant l'utilisation du bitcoin est un logiciel à code source libre. Il sera intéressant de voir si la dichotomie entre le processus de brevetage et le code source libre deviendra un problème important à mesure que l'industrie prend de la maturité.

Conclusion

Il ne serait pas surprenant que les technologies des chaînes de blocs changent rapidement la façon dont les transactions financières sont effectuées sur Internet. Il sera intéressant de voir si les cadres juridiques, telles les questions liées à la propriété intellectuelle, parviendront à suivre ces changements.