Accepter, adopter, utiliser : faire place à la chaîne de blocs

Par **Nicky Liu**
Services-conseils – Risques technologiques
KPMG au Canada

Voilà près d'une décennie qu'un programmeur utilisant le pseudonyme de Satoshi Nakamoto est entré au panthéon des innovateurs technologiques en concevant la première chaîne de blocs au monde. Au cours de cette décennie, ce programmeur (ou, peut-être, ces programmeurs) et sa technologie de registres distribués ont transformé la façon dont les gens et les entreprises négocient des fonds, des stratégies et des données sensibles.

La technologie de la chaîne de blocs et des registres distribués continue d'évoluer. Bien qu'il soit facile, en raison de son caractère perturbateur, de la concevoir comme une technologie risquée et à éviter, il y a un avantage à accepter, à adopter et à utiliser l'approche révolutionnaire de Nakamoto en matière de transactions humaines.

Une nouvelle façon de transiger

La chaîne de blocs est l'exemple par excellence des perturbations qui touchent différents secteurs d'activité. Par sa conception même, cette technologie permet aux participants de partager des enregistrements cryptés dans un réseau poste à poste ouvert et décentralisé.

Un livre blanc complet pourrait être consacré à l'explication de la mécanique (ou plutôt de l'informatique) de la chaîne de blocs. En fait, KPMG produit de plus en plus de documents portant expressément sur ce sujet. Cependant, pour nos besoins, la meilleure façon d'expliquer la chaîne de blocs est de suivre pas à pas une transaction typique. Dans le cas présent, il s'agit d'une transaction sur une monnaie numérique.

1. Le payeur soumet une transaction par l'entremise d'un nœud dans la chaîne, puis la technologie de la chaîne de blocs copie son registre pour vérifier son solde.
2. Si le solde du payeur est supérieur au montant de la transaction, la transaction est jugée légitime et est diffusée aux nœuds à proximité. La transaction doit obtenir la validation de plus de 12 nœuds avant de poursuivre.
3. La transaction est déplacée vers le bassin de transactions en attente composé des blocs « provisoires » du nœud. Par ailleurs, un « mineur » de chaînes de blocs, c'est-à-dire une personne qui utilise un ordinateur pour effectuer les calculs complexes nécessaires pour vérifier et décrypter des transactions, continuera de déchiffrer l'énigme à partir du dernier bloc (le bloc 1004) afin de relier son bloc provisoire à la chaîne.
4. Une fois que l'énigme a été résolue et que le bloc provisoire a été confirmé et ajouté à la chaîne (le bloc 1005), le nœud diffuse cette information aux autres nœuds du réseau. À ce moment, la transaction effectuée par les deux clients a été enregistrée dans le bloc et devient ainsi à l'épreuve des manipulations.
5. Les autres nœuds recevront la diffusion, déposeront cette transaction dans leur bassin de transactions en attente et réuniront d'autres transactions en attente dans leur bloc provisoire. Ils continuent ensuite à déchiffrer l'énigme générée à partir du nouveau bloc.

Une introduction à la chaîne de blocs

- **Chaîne de blocs :** type de base de données de registre distribué qui maintient une liste croissante d'enregistrements sur les transactions ordonnées en bloc et comportant diverses protections contre la manipulation et la modification.
- **Registre distribué :** enregistrement numérique de propriété qui diffère des technologies de base de données traditionnelles, puisqu'il n'y a pas d'administrateur central ni d'entreposage central des données; le registre est plutôt reproduit dans différents nœuds au sein d'un réseau poste à poste, et chaque transaction porte une signature unique faite au moyen d'une clé privée.
- **Mécanisme de consensus :** méthode permettant d'authentifier et de valider une valeur ou une transaction dans une chaîne de blocs ou un registre distribué sans qu'il soit nécessaire de se fier à une autorité centrale. Les mécanismes de consensus sont au cœur du fonctionnement d'une chaîne de blocs ou d'un registre distribué.
- **Nœud :** membre ou système d'un réseau de consensus ou d'un serveur qui détient une copie du registre et qui peut assumer divers rôles : émettre, vérifier, recevoir, informer, etc. À toutes fins utiles, un nœud peut être une forme de machine virtuelle.

Adoption de la chaîne de blocs pour les paiements internationaux

Les transactions réalisées par l'entremise de la chaîne de blocs comportent plusieurs avantages, en particulier lorsqu'elles sont appliquées à des paiements internationaux. Pensons par exemple à une transaction de la chaîne de blocs entre un client situé au Canada et une entreprise située en Chine. Une fois envoyé, le paiement est converti en une monnaie intermédiaire (p. ex., une « cryptomonnaie » acceptée par toutes les banques du réseau) et transmis aux nœuds avoisinants dans le réseau de la chaîne de blocs. Ensuite, les

© 2018 KPMG s.r.l./s.e.n.c.r.l., société canadienne à responsabilité limitée et cabinet membre du réseau KPMG de cabinets indépendants affiliés à KPMG International Cooperative (« KPMG International »), entité suisse. Tous droits réservés.

informations relatives au compte et au solde du client sont vérifiées presque immédiatement au moyen du registre distribué disponible sur les réseaux, et la diffusion de la transaction se poursuit, puis la transaction est confirmée lorsqu'un nouveau bloc est créé et relié à la chaîne. Le délai de traitement peut être sous le contrôle total des banques participantes, selon la manière dont elles ont conçu le protocole technique. La cryptomonnaie reçue à la banque bénéficiaire chinoise est ensuite convertie dans la monnaie désignée, conformément aux instructions du client, pour ensuite être transférée dans le compte du bénéficiaire.

Une fois la transaction conclue, le registre numérique est synchronisé avec toutes les banques participantes du réseau. Ainsi, il n'est plus nécessaire d'effectuer un rapprochement entre la banque d'origine et la banque bénéficiaire, puisque les transactions sont conservées dans chacun des registres de toutes les banques du réseau et qu'il est presque impossible de les manipuler.

Bien qu'il s'agisse seulement d'un exemple hypothétique, ce scénario illustre les avantages de la chaîne de blocs comparativement au processus traditionnel fastidieux et lourd en paperasse. Voici des avantages généraux de cette technologie.

- **Vérification avant la transaction :** la vérification des informations relatives au compte et au solde est pleinement automatisée et confirmée instantanément.
- **Authentification :** le système de cryptographie intégré dans la chaîne de blocs accroît la sécurité et la transparence de la transaction.
- **Coûts de transaction :** les banques correspondantes ne sont plus nécessaires, puisque le paiement s'effectue par un réseau poste à poste. Le risque de profit et de perte de change est aussi réduit puisque la transaction est confirmée presque instantanément.
- **Délai de traitement :** la technologie de vérification de la chaîne de blocs et l'élimination d'un intermédiaire (p. ex., une banque ou un médiateur financier) accélèrent le délai de validation et de règlement des paiements.
- **Rapprochement interbancaire :** le processus automatisé de la chaîne de blocs réduit le travail de rapprochement par les banques; il pourrait éventuellement l'éliminer complètement.
- **Efficience de la transaction :** la réduction du délai de traitement et du coût de transaction a pour effet d'accroître l'efficience de la transaction et d'augmenter considérablement l'utilisation de l'actif pour les clients.
- **Gestion de la trésorerie :** le délai de traitement totalement contrôlable et l'efficience accrue de la transaction permettent une meilleure surveillance de la gestion de la trésorerie des banques, ce qui réduit le risque de liquidité et le risque de crédit pour les banques.

Utilisation de la chaîne de blocs au sein de votre entreprise

De nombreuses institutions financières cherchent à tirer avantage de la technologie de la chaîne de blocs. Comme nous l'avons décrit dans les sections précédentes, les paiements internationaux ne sont qu'un exemple des capacités offertes par la chaîne de blocs dans le contexte traditionnel de la finance. L'adoption de cette technologie peut aussi être adaptée pour inclure des transactions plus complexes, comme les dérivés, la vente de titres en espèces et la négociation. Toutefois, puisque la réglementation s'alourdit et que le secteur financier se transforme lui-même à un rythme sans précédent, le coût de l'adoption peut représenter un défi.

Pour bénéficier des avantages de la chaîne de blocs, les institutions doivent se poser des questions clés.

- Pour quelle activité ou quel processus cette nouvelle technologie peut-elle être utile? En quoi est-ce une priorité pour mon investissement? **(Étendue)**
- En quoi le processus actuel se distingue-t-il d'une application de chaînes de blocs? Comment arrive-t-on à des ententes au niveau des données, de l'entreprise et du secteur? **(Processus)**
- Quelles données faut-il partager? Avec qui faut-il les partager et à quel moment? De plus, quelle catégorie d'actifs sera transférée, et où les données doivent-elles être stockées? Doivent-elles être authentifiées et notariées? **(Données)**
- Comment le contexte technologique sous-jacent se présente-t-il actuellement, et en quoi serait-il touché? Quels sont les coûts technologiques sous-jacents? Qui peut nous assurer que cette technologie est sécuritaire? **(Technologie)**
- Quelles compétences, formations et modifications de la main-d'œuvre sont nécessaires pour maximiser l'utilisation de la chaîne de blocs? **(Main-d'œuvre)**
- Cette solution nous aide-t-elle à répondre aux exigences réglementaires de manière plus efficiente? **(Réglementation)**
- Y a-t-il un événement sectoriel qui nous pousse à nous recentrer sur les activités courantes, de même qu'à faire les choses plus rapidement et avec un niveau de confiance accru? **(Secteur)**
- Quelle est l'analyse de rentabilité globale, y compris la prise en compte des coûts de mise en place? Quelle est la taille du marché et quel est le taux de croissance annuel composé? Quel est le rendement du capital investi? **(Analyse de rentabilité)**
- La solution est-elle adaptable et transférable? **(Exécution)**

Les auditeurs prennent des notes

Le monde change, et les auditeurs aussi. Tout comme les sociétés se préparent à bénéficier du potentiel de la technologie de la chaîne de blocs, les auditeurs adoptent des outils et des méthodologies perfectionnées qui leur permettront d'examiner les enregistrements de la chaîne de blocs pour le compte d'investisseurs, afin de leur fournir une assurance raisonnable quant à l'exactitude et à l'intégrité de ces enregistrements.

L'évolution de l'audit est loin d'être terminée. Au fur et à mesure que la chaîne de blocs évolue et que les procédures d'audit automatisées se concrétisent, nous devons aussi accepter, adapter et utiliser les nouveaux outils numériques de notre profession.

Communiquez avec nous :
Nicky Liu
Services-conseils – Risques technologiques
KPMG au Canada
nickyliu1@kpmg.ca

kpmg.ca/repenserlerisque
#repenserlerisque

© 2018 KPMG s.r.l./s.e.n.c.r.l., société canadienne à responsabilité limitée et cabinet membre du réseau KPMG de cabinets indépendants affiliés à KPMG International Cooperative (« KPMG International »), entité suisse. Tous droits réservés. 19844
KPMG et le logo de KPMG sont des marques déposées ou des marques de commerce de KPMG International.

kpmg.ca/fr