

## La technologie blockchain s'apprête à révolutionner l'électronique et l'Internet des objets

*Aude Skorodensky, Community Manager DesignSpark, RS Components*

Ces dix dernières années, le bitcoin a montré comment un réseau distribué d'ordinateurs sans contrôleur central pouvait traiter les transactions financières en toute sécurité. Fondamentalement, le bitcoin est juste un instrument financier ; le vrai héros de l'histoire est le protocole de blockchain car c'est lui qui permet l'existence des cryptodevises. Pour faire simple, une blockchain est un grand registre distribué conçu pour enregistrer le transfert des actifs numériques. Elle le fait indépendamment de tout "fournisseur", c'est-à-dire, dans le cas de l'argent, une banque. La puissance de calcul combinée des nombreux nœuds indépendants est telle que chacun d'eux s'assure que chaque transfert effectué est enregistré et valide. Loin d'être applicable uniquement aux devises numériques, la technologie blockchain est considérée par ses partisans comme un changement majeur dans la gestion des informations.



Les applications basées sur des blockchains commencent à apparaître dans un éventail de secteurs commerciaux. Une application potentielle est l'amélioration par l'utilisation d'un grand registre distribué pour l'enregistrement des transactions valides en permanence. Les premiers exemples d'utilisation sont apparus dans les services financiers, mais les applications ont commencé à apparaître dans les chaînes d'approvisionnement, où la traçabilité est particulièrement importante. La force clé d'une blockchain est que rien n'est jamais supprimé dans l'un des nœuds de la chaîne. En rendant les transactions publiques (mais pas les détails des transactions), aucune personne ou agent ne peut les falsifier ou modifier. À l'ère où la numérisation ne cesse de progresser, cela aura des répercussions énormes sur la façon dont nous vérifions presque tout.

Par exemple, la société de café du commerce équitable Cambio a décidé d'employer un système à base de blockchain pour démontrer aux consommateurs la provenance de leurs grains sans avoir à gérer le processus directement. Chaque étape du voyage de la plantation à la tasse est enregistrée sur une blockchain pour prouver que les ingrédients n'ont pas été substitués. La blockchain peut même permettre aux consommateurs de donner un pourboire aux producteurs et aux torréfacteurs pour le café qu'ils apprécient, confiants que l'argent va bien à la bonne destination.

La traçabilité démontrable est déjà importante dans l'électronique, mais le besoin de rendre ce processus plus simple et plus robuste peut conduire les applications futures vers l'utilisation de blockchains. L'introduction de composants contrefaits dans les chaînes d'approvisionnement est devenue un grave problème qui menace la qualité et la sécurité des infrastructures vitales telles que les centrales électriques. Des méthodes basées sur la technologie blockchain permettraient que chaque composant enregistre ses mouvements pour prouver aux acheteurs qu'il n'a pas été remplacé par un faux.

Des blockchains plus sophistiquées peuvent aider à introduire de puissants mécanismes dans l'Internet des objets (IoT) pour améliorer la fonctionnalité et la sécurité. Par exemple, les blockchains avec gestion des autorisations contrôlent les informations que les utilisateurs individuels sont autorisés à voir. Seuls les utilisateurs autorisés peuvent voir les données du grand registre, tandis que les couches supplémentaires contrôlent les informations qu'un utilisateur particulier peut voir. Ces fonctionnalités peuvent être utiles notamment dans le domaine de la santé. La blockchain permet au médecin de s'occuper de la santé de son patient, mais l'assureur obtient seulement des informations globales, suffisantes pour prendre des décisions. La mise en œuvre sans blockchain impliquerait de nombreux niveaux administratifs supplémentaires, ce qui compliquerait les démarches.

Des blockchains peuvent également être utilisées pour identifier et authentifier les appareils IoT eux-mêmes ; c'est un des défis majeurs auxquels l'industrie est confrontée. Après avoir été expédié par un fabricant, chaque appareil peut recevoir une entrée dans une blockchain. Une fois installé, l'appareil est vérifié via l'entrée et des mises à jour supplémentaires sont effectuées pour prouver qu'il est maintenant membre autorisé d'un réseau. Si, pour une raison quelconque, l'appareil doit être mis hors service ou est détecté comme non fiable, une autre mise à jour montre l'état révisé de l'appareil. Les systèmes savent alors qu'ils doivent ignorer les données envoyées par cet appareil. Les périphériques peuvent aussi passer d'un réseau à un autre sans avoir à passer par un seul opérateur si les besoins de l'application évoluent. Au lieu de cela, les transactions autorisées qui peuvent être inspectées par toute personne avec un accès valide seraient enregistrées à chaque changement d'état de l'appareil.

Couplée avec des capteurs embarqués et l'Internet des objets, la blockchain peut modifier des modèles économiques. Aujourd'hui, les procédures des compagnies d'assurance automobiles exigent de nombreux documents papier et sont administrativement compliquées. À l'aide de groupes de capteurs, les véhicules peuvent détecter automatiquement les incidents de conduite tels que les collisions, puis enregistrer les incidents de manière sécurisée sur une blockchain. Les compagnies d'assurance et les courtiers pourraient utiliser ces informations pour améliorer leur service en réagissant aux événements de manière automatisée, ce qui éviterait de remplir de nombreux formulaires et aiderait à calculer les taux de bonus et les primes étant donné que tous les événements sont enregistrés. Pour lutter contre la fraude, les courtiers en assurance seraient également en mesure de faire correspondre les conducteurs et leurs véhicules aux fournisseurs avec beaucoup plus de précision.

Le marché de l'énergie est un autre domaine où l'utilisation d'une blockchain pourrait apporter de nombreux changements. La croissance des énergies renouvelables, dont beaucoup sont déployées à domicile ou sur des campus, conduit à un réseau électrique beaucoup plus complexe que la structure traditionnelle. Les utilisateurs sont maintenant non seulement des consommateurs d'énergie approvisionnés par des générateurs à grande échelle, mais ils peuvent aussi être contributeurs en fournissant l'énergie non utilisée de leur système au réseau. Le réseau lui-même tend à se transformer en structure microréseau dans laquelle les voisins se fournissent de l'énergie les uns aux autres. La blockchain est plus adaptée à ces réseaux distribués que la facturation centralisée réalisée par les fournisseurs. Comme chaque kilowatt est transféré d'un utilisateur à un autre, la blockchain peut enregistrer l'activité. En se basant sur les informations de la blockchain, les services publics peuvent payer les utilisateurs pour l'électricité qu'ils fournissent, le gouvernement peut faire des crédits d'impôt pour encourager l'utilisation des énergies renouvelables, et les analystes peuvent examiner le flux d'énergie pour mettre en place des structures plus efficaces et mieux adaptées.

Il ne fait aucun doute que la blockchain est une technologie innovante qui a le potentiel de changer

en profondeur le positionnement de pays entiers sur le marché mondial : Malte s'est activement positionné en tant qu'utilisateur de la technologie blockchain. Le 4 juillet 2018, trois projets de loi ont été adoptés par le parlement maltais pour former la base d'un cadre réglementaire pour la technologie blockchain et les produits et services des registres distribués. Il faut espérer que ce renouveau apportera à l'île du blockchain de nouveaux investissements. En novembre de cette année, un plan de mise en œuvre d'une politique sur l'IA a été annoncé, pour vraisemblablement les mêmes lignes directrices et objectifs.

Avec des applications si variées pour les blockchains, le choix des technologies est important. Bien que le bitcoin ait été un succès pour les cryptodevises, le type de blockchain employé n'est pas nécessairement bien adapté aux applications dans l'IoT et d'autres secteurs commerciaux. Il est important de choisir une blockchain avec les bonnes propriétés pour l'application. Comme aucune partie d'une blockchain n'est approuvée par défaut, une des exigences fondamentales du protocole est d'établir la confiance entre les participants. Ceci est rendu possible par un mécanisme permettant aux utilisateurs de prouver leur statut aux autres sur le réseau. Sur bitcoin, c'est à travers la preuve de travail : les participants qui ajoutent des transactions à la blockchain résolvent des problèmes arithmétiques à l'aide de puissants ordinateurs.

Il existe de nombreux autres mécanismes de consensus blockchain qui peuvent être utilisés sur des chaînes d'approvisionnement et sur l'Internet des objets, par exemple les systèmes "preuve de la participation" ou "preuve d'autorité". Ces systèmes de calcul sont bien plus efficaces et sont donc adaptés aux petits points de terminaison IoT, même s'ils peuvent supporter l'infrastructure dédiée pour apporter de la fiabilité à la blockchain. Ils peuvent aussi mener à l'introduction de pannes localisées.

La preuve de l'autorité, par exemple, est semblable aux systèmes de confiance traditionnels car elle se base sur l'identité. Dans ce type de réseau, un "validateur" est un utilisateur qui dispose d'un compte approuvé pour des mises à jour de la chaîne. Pour devenir validateur, il doit prouver son identité au nœud de l'autorité racine, c'est ce qui différencie le système des certificats de sécurité X.509. Un tel système est efficace pour soutenir les applications IoT mais a l'inconvénient d'introduire un point d'attaque évident pour les pirates dans le nœud de l'autorité.

La preuve de l'intérêt permet d'éviter l'attaque d'un point unique en sélectionnant au hasard les participants au réseau qui ont déjà enregistré des transactions pour faire des mises à jour de la blockchain. Tant qu'il y a assez d'utilisateurs avec une preuve d'intérêt dans le réseau (ceci parce qu'ils ne souhaitent pas que leurs propres transactions soient invalidées), le système peut assurer un haut niveau de fiabilité sans le coût élevé de la preuve de travail.

Le concept blockchain évolue rapidement car les chercheurs tentent de trouver des moyens d'assurer la fiabilité et l'efficacité dans la mise en place et de résoudre les problématiques d'attaques potentielles que l'un de ces systèmes pourrait attirer. Si l'on se base aujourd'hui sur l'expérience des premiers utilisateurs, une application doit être capable d'évoluer et il apparaît difficile pour les bases de données centrales et les serveurs de gérer les transactions. La blockchain semble donc être une solution adaptée à ces problématiques. Il faut s'attendre à l'émergence de nouveaux mécanismes qui prendront en charge de nouvelles applications qui pourront être utilisées pour donner une valeur ajoutée à l'IoT.