LOGICIEL ET VIRTUEL

Décryptage de la blockchain

Chaque transaction d'une chaîne de blocs est unique et consignée dans un registre résistant aux pannes et à la falsification, configuration qui se prête à de multiples usages. Pour autant, cette technologie balbutiante n'est pas exempte de défauts.

01

Yvonne-Anne Pignolet
Thomas Locher
ABB Corporate Research
Baden-Dättwil (Suisse)

yvonne-anne.pignolet@ch.abb.com
thomas.locher@ch.abb.com

Une chaîne de blocs, ou « blockchain », est une base de données répliquée sur de multiples ordinateurs. Elle se compose d'une liste de transactions en croissance perpétuelle, regroupées en « blocs » horodatés contenant un lien vers le bloc précédent : une succession de blocs qui forme la chaîne. Si la blockchain suscite tant d'intérêt aujourd'hui, c'est à cause de ses propriétés uniques : chaque transaction ne peut être effectuée qu'une seule fois avant d'être stockée définitivement dans un registre tolérant aux pannes et infalsifiable. Ce registre étant de plus public, n'importe qui peut en vérifier l'exactitude →**1**.

Une chaîne de blocs est une base de données répliquée sur de nombreux ordinateurs et composée d'une liste de transactions en croissance perpétuelle.

Jusqu'à présent, lorsqu'une transaction exigeait un tel niveau d'intégrité, de disponibilité et de sécurité, il était nécessaire de passer par un tiers de confiance qui stockait l'information dans de multiples bases de données. Principal inconvénient : il faut avoir confiance dans la bonne foi et l'honnêteté de cet intermédiaire. Sans compter qu'il existe toujours un risque de voir un malfaiteur prendre la main sur le système du tiers et modifier ou supprimer des enregistrements, par exemple. La base de données d'une blockchain étant distribuée, elle est bien mieux immunisée contre les manipulations accidentelles ou intentionnelles.

—
01 Chaque transaction d'une chaîne de blocs est effectuée une seule fois avant d'être consignée dans un registre infalsifiable. Dans notre monde connecté, les applications de ce principe sont innombrables. La technologie blockchain est surtout connue pour être au fondement des cryptomonnaies, dont le bitcoin n'est qu'un exemple parmi d'autres.

Anamnèse

L'émergence de la blockchain remonte à la création du bitcoin, premier avatar pérenne d'une monnaie virtuelle ou « cryptomonnaie » [1], inventée en 2009 par un individu utilisant le pseudonyme de Satoshi Nakamoto. À défaut de révéler qui se cache derrière ce mystérieux créateur – il pourrait même s'agir de plusieurs personnes –, l'article fondateur publié par celui-ci constitue la première description de la chaîne de blocs qui sous-tend le bitcoin.

À la différence des devises classiques, les cryptomonnaies ne sont ni émises ni régulées par les banques centrales ou les États. Leur contrôle est décentralisé : n'importe qui peut participer et allouer des ressources (de calcul) pour garantir l'intégrité du système. Créer une monnaie virtuelle robuste et stable n'est pas une mince affaire.

En effet, en l'absence d'autorité régulatrice (banque centrale, par exemple), comment empêcher une âme mal intentionnée de dépenser la même somme virtuelle plusieurs fois ? Comment un vendeur peut-il être sûr que l'acheteur a de quoi payer l'article ? Comment garantir la non-répudiation des transactions ? Ces questions soulèvent quelques-uns des principaux obstacles à l'essor d'une monnaie virtuelle.

La blockchain →**3** y répond en assurant cohérence globale et sérialisation des transactions : l'ordre dans lequel ces dernières sont effectuées est mémorisé. Autre propriété centrale de la blockchain, les enregistrements sont immuables : impossible de modifier ou de supprimer une transaction effectuée.

02

Quoi qu'en disent certains, le concept de la chaîne de blocs n'est guère compliqué. C'est précisément sa simplicité, ainsi que ses multiples propriétés incontournables pour un grand nombre d'applications distribuées, qui en font tout l'intérêt. En deux mots, la blockchain est capable de simplifier et d'automatiser le traitement d'une multitude de cas d'usage.

Si la blockchain suscite tant d'intérêt aujourd'hui, c'est à cause de ses propriétés uniques.

Un fort potentiel
Le principal apport de la blockchain tient en ce qu'elle rend caduque la question du tiers de confiance. Autrement dit, l'utilisateur n'a plus besoin de se fier à un tiers donné mais seulement à un système distribué et aux protocoles informatiques sous-jacents. Il suffit pour cela d'avoir foi en la capacité de la majorité des acteurs gérant le registre à assurer un déroulement des opérations conforme aux protocoles et à empêcher les autres entités (malveillantes) de corrompre le système.

Une nouvelle transaction est soumise à la chaîne de blocs.

—
02 Par sa nature distribuée, la blockchain se prête parfaitement au suivi et à la vérification de toutes sortes de transactions, comme par exemple l'exécution d'un contrat « intelligent ».

—
03 Principe de la blockchain

La confiance étant précieuse et fondamentale à n'importe quel système distribué, il n'est pas étonnant que la technologie blockchain suscite de l'intérêt bien au-delà des monnaies virtuelles. La plupart des applications envisagées par ABB et bien d'autres entreprises relève d'une des trois catégories suivantes, par ordre de complexité croissante :

—

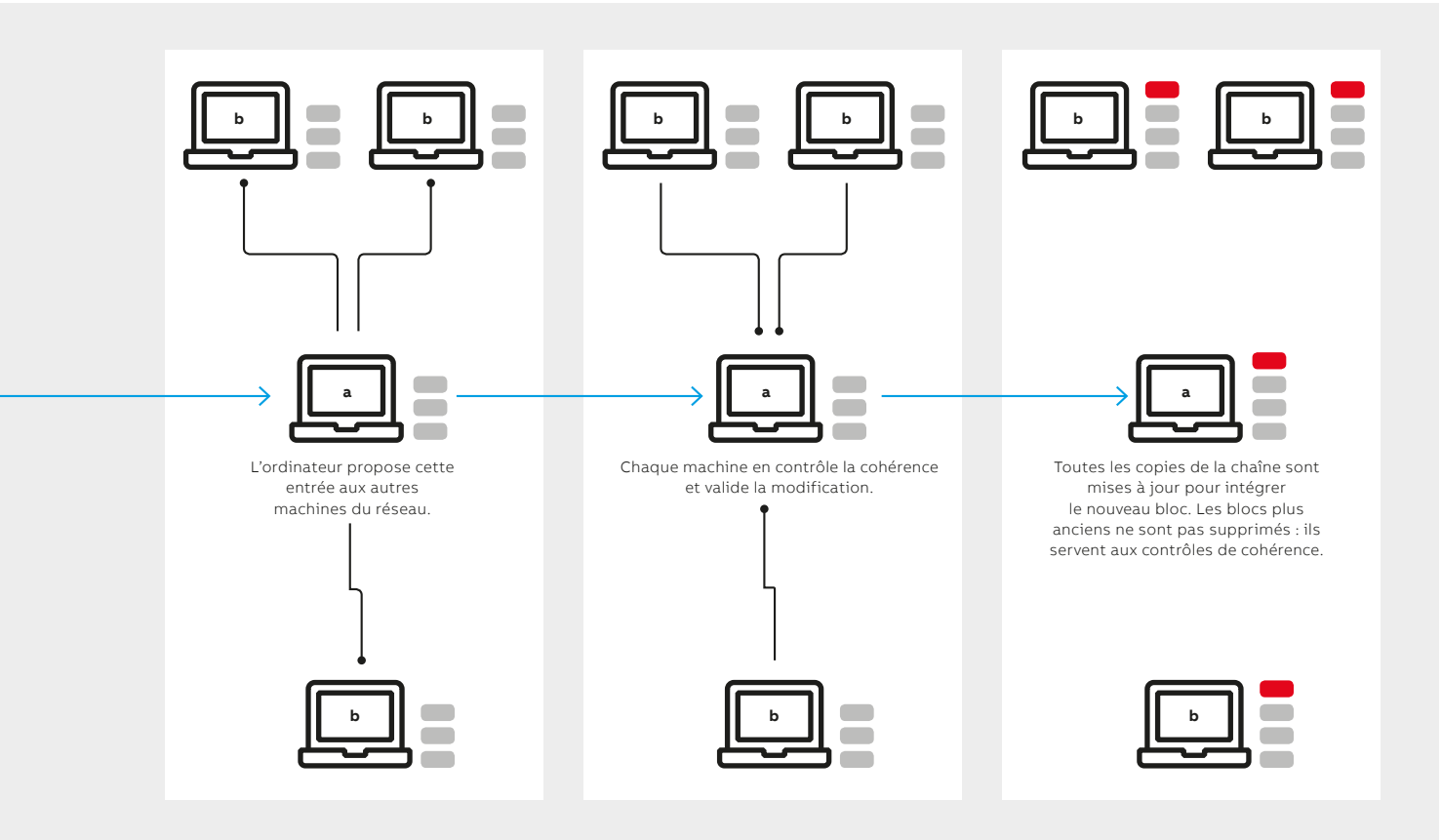
La blockchain assure la cohérence globale et la sérialisation des transactions, ainsi que leur immuabilité.

1. Registre : inscription de transactions numériques dans un registre distribué public et immuable ;
2. Échange d'actifs : création et transfert de propriété ;
3. Contrats intelligents →**2** : automatisation de procédures administratives via l'exécution de code.

L'information stockée dans la blockchain est protéiforme : actifs physiques ou virtuels, identités, transactions ou encore contrats. La création, la validation, l'enregistrement et la répartition des entrées sont régis par protocole.

Dans la première catégorie, la chaîne fait office de registre pour l'enregistrement d'événements et de documents importants : naissance, mariage, décès, titre de propriété physique ou intellectuelle, résultat de scrutin, décision de justice, investissement financier, police d'assurance, dossier médical, etc. →**4**. Le principal intérêt de la blockchain est l'immuabilité des données, ainsi que leur disponibilité même en dehors de l'entreprise ou du pays (sous réserve d'avoir installé des mécanismes de protection et de confidentialité). Cette faculté de partage transfrontalier est une condition sine qua non à la numérisation de secteurs comme la médecine, la finance et l'administration. ABB s'y intéresse de très près.

La deuxième catégorie, qui concerne plus particulièrement les banques, recouvre l'échange d'actifs (numériques), la facilitation des paiements transfrontaliers et le négoce d'actions, d'options et de produits dérivés. Pour les industriels, la blockchain peut servir de support aux transactions de transfert de propriété ou de mise à disposition de biens matériels. Sont envisagés, entre autres, le suivi logistique et la décentralisation du contrôle d'accès.



L'étape suivante consiste à mettre en place des contrats dits « intelligents » dans lesquels un protocole distribué exécute en autonomie les clauses du contrat, réduisant par là même le risque d'erreur et de fraude. Il peut s'agir d'une couche supplémentaire coiffant la chaîne : le contrat y est enregistré sous la forme d'un code exécutable, les membres du réseau exécutant ce code selon les modalités du contrat. Chaque exécution partant du même état initial, ce déroulement automatique et distribué garantit un consensus entre tous les membres qui exécutent correctement le contrat. Ces contrats intelligents ouvrent la porte à de nouveaux instruments financiers, à des contrats d'assurance indiciels ou à tout autre service reposant sur une base de données partagée couplée à des calculs vérifiables ou à des procédures d'approbation automatique sans passage par un tiers de confiance. Ce type de contrats pourrait notamment faciliter l'échange et le négoce d'énergie, deux domaines pour lesquels ABB a des solutions →5.

04

Si nul n'hésite à vanter les avantages de la blockchain sur les solutions actuelles (potentiel d'économie par exemple), on se demande rarement à quel point elle est adaptée au cas d'emploi envisagé : est-elle vraiment pertinente pour déplacer l'objet de la confiance, d'un interlocuteur central à un système distribué ? Pour répondre à cette question, il faut étudier soigneusement l'aptitude de la blockchain à résoudre ces questions de confiance et voir si d'autres méthodes plus classiques, telles les bases de données distribuées, n'ont pas les mêmes atouts.

Les contrats intelligents peuvent prendre la forme d'une couche supplémentaire ajoutée à la blockchain, facilitant par exemple le négoce d'énergie.

Des limites

En dépit des avantages et des remarquables potentialités de la blockchain, son adoption risque de se heurter à quelques obstacles, au premier rang desquels le manque de flexibilité. En effet, faute de consensus, toute modification des protocoles ou de leur exécution est pour ainsi dire impossible ; si seulement quelques acteurs de la blockchain, ou « mineurs », adoptent le nouveau protocole tandis que les autres conservent l'ancien, la chaîne se scinde en deux réalités incompatibles, ou « fourches ». Qui dit modification implique donc coordination étroite de tous les maillons de la chaîne. Le code peut aussi pâtir de cette lacune : certains bugs touchant le bitcoin sont connus de longue date sans être pour autant corrigés à ce jour. Outre cette rigidité, la blockchain est limitée en taille ; le nombre d'utilisateurs et de nouveaux blocs par unité de temps est figé. Ainsi, la chaîne du bitcoin s'enrichit d'un nouveau bloc toutes les 10 minutes, soit un rythme de croissance d'environ 8 gigaoctets par an. Si ce chiffre reste modique au regard de la puissance de calcul disponible, il implique néanmoins que le nombre de transactions par seconde ne peut pas être supérieur à 7, un plafond bien trop faible à l'échelle mondiale.

—
04 Une chaîne de blocs peut enregistrer de manière fiable quantité de données financières, juridiques ou personnelles (dossier médical, par exemple).

—
05 Les contrats intelligents reposant sur la blockchain pourraient révolutionner l'échange et le négoce d'énergie.

—
Bibliographie
[1] www.bitcoin.org

05

Nous l'avons vu, toute proposition de modification devant être avalisée par la majorité, ce problème ne sera pas réglé du jour au lendemain. Autre désagrément, la chaîne de blocs souffre d'un appétit d'énergie insatiable tant son principe de validation par « preuve de travail », chronophage, fait s'envoler le temps-machine et donc la puissance de calcul à chaque nouveau bloc. Actuellement, on estime que le bitcoin engloutit l'équivalent de la production de deux centrales nucléaires !

—

D'autres méthodes plus usuelles permettent-elle d'obtenir le même résultat que la blockchain en termes de confiance ?

Enfin, même si l'idée-force d'une immuabilité des transactions est sécurisante, les exécutions et mises en œuvre de la chaîne de blocs sont vulnérables aux cyberattaques : vol de portefeuille en bitcoins, interception de paquets de données, attaques par déni de service, etc. Pire, le pirate qui contrôle plus de 50 % de la puissance de calcul totale a de fait la maîtrise de toute la chaîne, voire la capacité d'effacer des transactions passées.

Les chercheurs ne ménagent pas leurs efforts pour tenter de pallier ces failles. Concernant le manque de flexibilité, on pourrait envisager de confier la gestion des protocoles à un consortium, qui deviendrait ainsi le tiers de confiance. De même, le coûteux mécanisme de la preuve de travail pourrait être avantageusement remplacé par des algorithmes distribués de consensus, comme dans le projet Hyperledger. Reste à savoir s'il existe un système capable de lever les verrous de la blockchain tout en conservant ses atouts. L'avenir nous le dira....

Promesses industrielles ?
La médiatisation de la blockchain a fait naître des attentes démesurées. Bon nombre des cas d'utilisation envisagés fondent leur réussite sur la confiance, alors que cette technologie n'est pas toujours à la hauteur des exigences. Ce n'est donc pas la panacée. Chaque cas de figure exige une mise en œuvre réfléchie pour pouvoir tirer profit des principes du bitcoin ou des chaînes de blocs. Balbutiante, la technologie suscite un engouement qui ne doit pas masquer ses indéniables défauts. ABB observe de près les développements en cours ; à force d'innovations, la blockchain atteindra probablement un niveau de maturité qui libérera tout son potentiel au service de l'automatisation et de la simplification des process industriels. ●