Comment fonctionne la chaîne de blocs ?

La chaîne de blocs est une technologie réputée infalsifiable. Le bitcoin en constitue l'application la plus connue. *Jan Thomas Frecè, Sebastian Höhn*

L'idée fondamentale de la chaîne de blocs (ou « blockchain ») est simple : plusieurs parties gèrent ensemble une base de données dont ils sont coresponsables. Il n'y a pas d'autorité centrale de contrôle. Tous les participants détiennent des copies identiques de la chaîne de blocs et de nouvelles entrées n'y sont inscrites qu'en cas de consensus sur son état actuel. Les données sont réparties et le consensus établi selon différents protocoles propres au type de blockchain. La cryptomonnaie bitcoin, plus exactement sa base de données des transactions, est l'exemple le plus connu de cette technologie.

Pour pouvoir être stockées dans la blockchain, les transactions sont regroupées dans des blocs permettant d'inscrire des données de tous genres. Il est en revanche impossible de les supprimer. Les blocs sont ensuite interconnectés par des techniques cryptographiques qui permettent de déceler toute absence ou modification de l'un d'eux. Telle la numérotation continue de factures, il est ainsi possible de prouver l'exhaustivité des données stockées dans la chaîne de blocs. Pour ajouter un nouveau bloc de données, un nombre prédéfini de participants doit confirmer électroniquement son authenticité. Chaque nouveau bloc valide tous les blocs de transactions précédents, ce qui permet d'identifier toute tentative de manipulation.

Tout changement est remarqué

L'exploitation d'une chaîne de blocs publique nécessite une grande capacité de calcul pour inscrire un nouveau bloc. Le côté énergivore du bitcoin est ainsi souvent critiqué. En cause : la « preuve de travail » (« proof of work »), une opération qui protège la blockchain des pirates informatiques et d'un ajout en masse de blocs manipulés. En revanche, lorsque le cercle de participants est connu, des procédés plus efficaces s'appliquent pour le consensus et l'utilisation de ressources peut être sensiblement réduite. Dans une chaîne de blocs, les données sont réputées « inaltérables ». En clair, il peut certes y avoir des modifications comme pour chaque document enregistré sous forme numérique, mais elles sont révélées par l'usage de la signature numérique, du chiffrement et de la redondance. En outre, chaque participant qui présente les données correctes peut également prouver qu'elles sont correctes.

Comment fonctionne le mécanisme de consensus ? À l'inverse d'une base de données centrale, qui exige que l'on fasse confiance à l'organisme qui la gère, la chaîne de blocs n'inscrit de nouvelles données que si un nombre prédéfini d'acteurs les a vérifiées et validées par des techniques cryptographiques (traitement de bout en bout). Dès lors, peu importe la confiance que l'on peut avoir dans chaque participant pris isolément : quelques fraudeurs ne peuvent pas menacer l'exactitude des données.

Les « contrats intelligents » (« smart contracts ») offrent un champ d'étude passionnant : il s'agit de protocoles informatiques pouvant s'exécuter dans une blockchain et qui représentent des contrats dynamiques. Les mécanismes de la chaîne de blocs garantissent l'inaltérabilité du protocole informatique ainsi que des conditions menant à son exécution. Cela permet par exemple d'élaborer des solutions sûres et entièrement automatiques pour le trafic des paiements ou la traçabilité de produits qui peuvent être taillées sur mesure pour un grand nombre de clients et fournisseurs différents.

Jan Thomas Frecè
Collaborateur scientifique, Institut de cyberadministration, Haute école spécialisée bernoise (BFH), Berne

Sebastian Höhn
Chargé de cours, Institut de cyberadministration, Haute école spécialisée bernoise (BFH), Berne

SHUTTERSTOCK