La chaîne de blocs est économiquement pertinente

Les réseaux basés sur la technologie blockchain ont un avantage économique sur les monopoles comme Facebook : ils placent les utilisateurs au centre. *Mathias Bucher*

Abrégé La décentralisation et les interactions sécurisées par cryptographie sont les éléments clés de la chaîne de blocs. Ces caractéristiques permettent de nouvelles formes d'organisation des réseaux, dans lesquelles les utilisateurs sont aussi propriétaires et les avantages optimisés pour tous les participants. À long terme, cela est susceptible de mettre sous pression des réseaux comme Facebook. La gouvernance des réseaux basés sur la chaîne de blocs constitue un défi préalable à relever.

La chaîne de blocs (ou « blockchain ») a fait couler beaucoup d'encre ces derniers mois. D'abord pour l'effet pionnier et le potentiel disruptif de cette technologie, souvent commentée à grand renfort de superlatifs lors de la bulle du bitcoin, puis de manière banale et comme « sous-chapitre de l'histoire des technologies » après une correction réussie du prix. Le spectre d'opinions est donc large, car il est encore trop tôt pour estimer quantitativement le potentiel économique de la technologie de la chaîne de blocs.

Risquons toutefois un pronostic : la technologie blockchain révolutionnera les structures en réseau. Les réseaux constituent un important facteur économique. Selon une étude de société de capital-risque NFX, l'effet « de réseau » génère 70 % de la création de valeur des technologies. Intuitivement, cet effet est facile à comprendre : un réseau a d'autant plus de valeur qu'il compte de nombreux participants.

Lorsque des réseaux grandissent, des monopoles naturels se forment : plus un réseau compte de participants, plus il attire ceux qui n'en font pas encore partie. Les coûts de changement deviennent en même temps toujours plus élevés pour les anciens participants, car ils perdraient l'accès aux autres participants en cas de changement – les réseaux sociaux tels que Facebook ou Linkedin en sont l'illustration. Le monopole de réseau n'est pas mauvais en soi : du point de vue des membres, l'avantage augmente avec chaque nouveau participant. Un monopole compte par définition la majorité des utilisateurs. Un monopole de réseau peut ainsi, dans de bonnes conditions, maximiser l'avantage de chacun de ses membres.

Du point de vue des utilisateurs, les conditions ne sont toutefois jamais optimales dans les réseaux en mains privées, car les entreprises doivent en tirer le plus grand profit possible pour leurs actionnaires. Dès qu'un réseau est suffisamment fort sur le marché, les propriétaires l'exploitent pour obtenir le meilleur rendement possible – c'est le mécanisme de « l'impératif d'extraction ». Les possibilités sont nombreuses : vente des données d'utilisateurs, publicité imposée à l'utilisateur, exigence de frais d'accès, etc. Le propriétaire du réseau est en outre incité à internaliser certaines prestations.

Des jetons pour respecter les règles du jeu

La technologie blockchain permet de faire coïncider les incitations des utilisateurs et des propriétaires du réseau : la contrainte d'exploiter l'utilisateur au profit des actionnaires disparaît totalement lorsque l'utilisateur et le propriétaire sont identiques.

Comment cela fonctionne-t-il ? Une chaînes de blocs peut être considérée comme une base de données sécurisée par cryptographie et globalement décentralisée, à laquelle des données peuvent être ajoutées, mais jamais effacées. Ces données (qui résultent des transactions de tous les participants) sont infalsifiables et sauvegardées sous une forme inaltérable. Les chaînes de blocs modernes peuvent en plus exécuter des programmes informatiques (dits « contrats intelligents » ou « smart contracts ») qui sont également mémorisés sous une forme inaltérable.

1 Voir à ce propos l'article de Noël Bieri et Kaspar Ulmann (Finma) dans ce numéro (p. 9–11).

Des incitations économiques matérialisées par des jetons (ou « tokens ») garantissent que les règles du jeu soient respectées, tant au niveau de l'utilisation de la chaîne de blocs que des applications basées sur cette dernière. Un jeton est un droit numérique sur la chaîne de blocs. Il peut prendre la forme d'une cryptomonnaie, comme le bitcoin ou l'ether. L'Autorité fédérale de surveillance des marchés financiers (Finma) classe ce genre de jetons dans la catégorie des « jetons de paiement »[1]. Mais un jeton peut également représenter des droits d'utilisation pour des services ou des infrastructures fournis sur chaîne de blocs (« jetons d'utilité »), ou une valeur (« jetons d'investissement »). La plupart des jetons sont normés et transférables via la chaîne de blocs dont ils proviennent.

Grâce à ces jetons, la technologie blockchain permet de nouvelles formes d'organisations : ces dernières ne sont pas structurées comme des entreprises, mais construites en soi de manière décentralisée. Cette décentralisation est souvent souhaitable lorsqu'il faut concilier les motivations de tous les acteurs d'un système (propriétaires, employés, clients). Il s'agit là d'avantages évidents dans les structures en réseau.

Structuration par étapes

La décentralisation complète d'un réseau n'est toutefois pas réalisable – du moins durant la phase de développement – sans une instance qui coordonne la construction du réseau. Si le

Le système bicaméral utilisé comme modèle pour les réseaux basés sur la chaîne de blocs ? La salle du Conseil des États.

KEYSTONE

but est d'échapper à l'« impératif d'extraction », des fondations à but non lucratif se profilent comme unités de coordination. Mais un réseau décentralisé coordonné par un organisme à but non lucratif n'implique pas que l'utilisation du réseau soit (ou doive être) gratuite : chaque ressource librement accessible court le risque d'une surexploitation – phénomène connu en économie sous le nom de « tragédie des biens communs ».

La pertinence économique de la technologie blockchain intervient précisément ici : elle permet de réguler efficacement l'utilisation d'un réseau au moyen de jetons sans centraliser le réseau. Prenons un réseau typique basé sur une chaîne de blocs, sans actionnaires ni entreprise. Il existe à la place des « jetons de réseau » spécifiques, que chaque participant au réseau doit posséder pour y accéder et l'utiliser. Ces jetons peuvent être configurés différemment : dans le cas le plus simple, le jeton autorise son propriétaire à participer au réseau. Les jetons peuvent également constituer un moyen de paiement pour les services proposés par le réseau. Ils peuvent aussi servir de « récompense » pour les prestataires externes du réseau ou à « faire fructifier » l'écosystème des développeurs de réseau. Le négoce des matières premières en donne un bon exemple : la fondation décentralisée ABC Platform permet de liquéfier un marché pour des matières premières difficiles à négocier grâce à la chaîne de blocs. L'accès au réseau est réservé aux négociants en matières premières qui disposent de jetons spécifiques à la plateforme et qui peuvent payer les prestations consommées sur le réseau au moyen de ces mêmes jetons.

Le casse-tête des modifications

La régulation de l'accès au réseau par les jetons constitue un élément clé dans la conception d'un réseau décentralisé viable à long terme. Le réseau doit en même temps pouvoir se développer afin de s'adapter à l'évolution des conditions réglementaires ou d'intégrer de nouvelles fonctions.

Les contrats intelligents jouent ici un rôle essentiel : ils permettent de définir la gouvernance du processus de développement de manière transparente pour tous les participants et de l'imposer directement sur la chaîne de blocs. Il existe plusieurs possibilités d'autoriser les détenteurs d'un jeton à modifier le réseau. La configuration optimale de cette gouvernance sur la chaîne fait actuellement l'objet de gros efforts en termes de recherche : les essais vont du mécanisme naïf « un jeton – un vote » par « vote quadratique » aux diverses formes du « jugement majoritaire ». Les deux procédures de vote vont au-delà du schéma « oui-non » et permettent un échelonnement.

Étudier les acquis des systèmes de consensus sociaux qui se sont développés au fil des siècles semble être une approche prometteuse. Exemple typique, le système bicaméral tel qu'on le connaît en Suisse ou aux États-Unis empêche l'hégémonie d'un groupe de pouvoir et peut, s'il est bien mis en œuvre dans un contexte de chaîne de blocs, bloquer les attaques dites « à 51 % ». L'exemple d'ABC Platform en est l'illustration : la fondation d'utilité publique qui fait office de coordinateur du réseau prend le rôle d'une chambre, tandis que les acteurs du réseau jouent le rôle de la seconde chambre. Les deux chambres doivent être d'accord pour que les règles du réseau soient modifiées. Dans une telle structure, aucun groupe d'acteurs ne peut se former au détriment des autres participants au réseau. En clair, la fondation fait contrepoids. D'un autre côté, les participants ne sont pas livrés à son bon vouloir – elle doit œuvrer pour le bien des participants.

Mathias Bucher
Chargé de cours en technologie blockchain, Institut des services financiers de Zoug (IFZ), Haute école de Lucerne ; fondateur d'ABC Platform