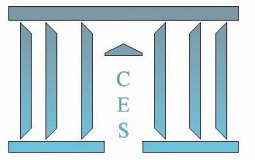
Blockchain Publique versus Blockchain Privée : Enjeux et Limites

Dominique Guegan

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

Documents de Travail du
Centre d'Economie de la Sorbonne

CES Working Papers



Blockchain Publique versus Blockchain Privée : Enjeux et Limites

Dominique GUEGAN

2017.53

Maison des Sciences Économiques, 106-112 boulevard de L'Hôpital, 75647 Paris Cedex 13
http://centredeconomiesorbonne.univ-paris1.fr/
ISSN : 1955-611X

Blockchain Publique versus Blockchain Privée : Enjeux et Limites

Dominique GUEGAN

Université Paris 1 Panthéon –Sorbonne - LabEx ReFi

La blockchain est un sujet très prisé dans le milieu bancaire et de l'assurance, de quoi s'agit-il ? La notion de blockchain émane de la cryptographie et il s'agit d'un protocole permettant de transmettre des informations de manière sécurisée. Nous distinguerons deux approches, l'approche publique décentralisée et l'approche privée centralisée. Le concept de blockchain est apparu grâce à l'émergence de crypto-monnaie et en particulier du Bitcoin. Si la blockchain doit devenir un outil important au sein des banques alors il est nécessaire d'avoir une connaissance assez juste des outils sous-jacents et des enjeux associés à cette nouvelle technologie. En effet, il apparait nécessaire d'identifier les risques qui y sont associés et de proposer des stratégies en vue de les contrôler.

La cryptographie est une discipline consacrée à la protection des messages (confidentialité, authenticité, intégrité) grâce à l'usage de clefs. Cette technique date de l'antiquité et fut longtemps considérée comme un art et ce n'est qu'au 20ème siècle qu'elle est devenue une science. C'est l'utilisation massive des ordinateurs qui a démocratisé son utilisation. On peut distinguer plusieurs algorithmes en cryptographie : la cryptographie classique, la cryptographie symétrique, la cryptographie asymétrique (avec une clef publique et un clef privée). Dans ce dernier cas, la clef publique permet le chiffrage et la clef privée le décryptage. La cryptographie asymétrique est utilisée pour assurer l'authenticité d'un message. La signature du message est cryptée grâce à la clef privée attachée au message et les destinataires décryptent le message en utilisant la clef publique qui leur permet de récupérer la signature. Ce processus assure que l'expéditeur est l'auteur du message. C'est cette approche qui fut utilisée à l'origine pour définir le protocole blockchain du Bitcoin.

Le bitcoin est une monnaie électronique basée sur un système pair-à-pair ou décentralisé utilisant la cryptographie pour valider les transactions et aussi pour créer de la monnaie. Le protocole est un mécanisme fiduciaire décentralisé pour éviter l'utilisation d'un tiers de confiance. Le principe de décentralisation implique que tout le monde peut participer à la rédaction du code (il faut néanmoins obtenir un droit d'entrée). La blockchain du Bitcoin est l'ensemble des fichiers de toutes les transactions, qu'elles aient été acceptées ou non. L'utilisation de la cryptographie assure la sécurité des transactions et leur acheminement dans le monde entier. A l'heure actuelle, le Bitcoin est le système de blockchain public le plus abouti. Les bitcoins sont créés en échange du traitement de chaque transaction, selon le code source du logiciel. Des utilisateurs (les mineurs) utilisent leur puissance de calcul pour vérifier, sauver et garantir les transactions et les graver dans la blockchain. Ce travail effectué par les mineurs s'appelle la Preuve de Travail et consiste en la résolution de problèmes algorithmiques qui font partie du protocole Bitcoin. Une fois le transaction validée, elle est horodatée, ajoutée à la blockchain et est alors visible par le destinataire ainsi que par tous les membres du réseau.

La blockchain décrite précédemment et utilisée pour générer des bitcoins est une blockchain publique. C'est une technologie sécurisée, transparente pour le stockage et la transmission de données sans dispositif de contrôle centralisé. Chaque participant peut l'utiliser pour faire des transactions et tout le monde peut participer au processus de contrôle. Il n'y a aucun registre central ni tiers de confiance. C'est une base de données contenant la suite des transactions validées et

automatiquement protégées contre la falsification ou la modification grâce au stockage dans les nœuds du réseau avec une chronologie décentralisée. Une blockchain contient donc tout l'historique des échanges entre les utilisateurs, depuis sa création. L'information est partagée par tous les utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne d'informations. Le principe du partage est basé sur un consensus qui historiquement utilise ce que l'on appelle La Preuve de Travail. Le mineur qui fait le travail en question utilise l'énergie comme moyen de vérification. Pour être sûr que le système ne soit pas corrompu, il est indispensable qu'aucun opérateur (mineur) ne détienne plus de la moitié de la puissance de calcul. Le principe de la Preuve de Travail est celui de la crypto-économie qui allie à la fois des incitations économiques et la vérification des transactions en utilisant la cryptographie. Le principe repose sur une communauté qui est une alternative au système économique classique, et qui a montré sa force et sa résilience tant que le consensus est respecté.

A l'opposé de la blockchain publique, une blockchain est dite privée si le principe de consensus est vérifié par un nombre limité et prédéfini de participants. La possibilité de participer aux transactions est définie par une organisation, il en est de même pour le travail de vérification. La *blockchain of place* évoquée dans la littérature est un exemple de réseaux privés ou le processus de contrôle est organisé autour d'un nombre prédéfini de nœuds. La blochchain privée n'utilise pas forcément des mécanismes basés sur la cryptographie.

Dans le cas d'une blockchain privée, il n'y a ni mineurs, ni preuve de travail, ni rémunération. Ce sont ces points qui différentient les deux systèmes (publics et privés) principalement pour le stockage et la transmission des données.

Ainsi une blockchain quelle qu'elle soit est une technologie de stockage et de transmission numérique à coût minimal, décentralisé et totalement sécurisé. Concrètement, c'est un livre de compte - un registre - contenant une liste de tous les échanges effectués entre les utilisateurs de la blockchain depuis sa création. . Ce registre est décentralisé, stocké sur les serveurs de ses utilisateurs, fonctionnant sans intermédiaire, éliminant ainsi les coûts d'infrastructure. C'est un historique infaillible d'échanges, conservés et mis à jour en temps réel de manière indépendante par tous les utilisateurs. Pour manipuler ce registre, on doit accéder et modifier en même temps des dizaines de milliers de bases de données indépendantes. C'est un challenge pour les banques si elles veulent s'en emparer et qui doit inciter aussi celles-ci à s'orienter sur la maîtrise de la technologie Big Data. Ainsi les utilisateurs de la blockchain valident chaque transaction par un processus transparent qui empêche toute manipulation. Ils vérifient, par exemple, par le biais du registre, que l'expéditeur est le propriétaire de ce qui est envoyé et que le destinataire des données est le correspondant approprié. Les groupes de transactions validées sont finalement inscrits dans le registre, sous la forme d'une chaîne de blocs inaltérable : la blockchain.

Les banques sont intéressées par ces protocoles basés sur la blockchain pour effectuer des transferts encore plus sécurisés et plus rapides. Pour ce faire, elles doivent créer leur propre blockchain. Donc, pour entrer dans l'ère de la blockchain, les banques ont besoin d'un registre entièrement distribué. Plusieurs initiatives ont émergé pour mettre en place des blockchain dites privées ou hybrides: il s'agit de blockchain réglementées, qui n'autorisent qu'un nombre limité d'acteurs habilités à enregistrer leurs transactions et à avoir un registre. Un exemple est R3 CEV, une blockchain FinTech autour de laquelle gravitent 25 banques internationales, dont Goldman Sachs et JP Morgan.

Que peuvent espérer les banques de ces technologies ? (i) Réduire les coûts d'infrastructure liés aux paiements, aux échanges internationaux. En d'autres termes, grâce à la blockchain, les banques pourront réduire leurs coûts d'exploitation et augmenter leur rentabilité. (ii) Mettre en place de nouveaux services en simplifiant de nombreux processus: micro-paiements, transactions à faible coût, micro-crédits pour consommation, etc.

Alors que la blockchain publique peut être assimilée à un registre public, anonyme et infaillible , comment s'assurer qu'une blockchain privée centralisée sera aussi infaillible et quels autres intérêts peut-elle apporter aux banques ?

À l'heure actuelle, les applications potentielles de la blockchain privée peuvent être classées en trois catégories: (i) Applications pour le transfert d'actifs (utilisation monétaire, mais pas seulement: titres, votes, brevets industriels, objets connectés, sécurité des diplômes, stocks, obligations , etc.); (Ii) Applications de la blockchain en tant que registre: ceci assure une meilleure traçabilité des produits et des actifs; (Iii) Contrats intelligents: ce sont des programmes autonomes qui exécutent automatiquement les termes et conditions d'un contrat sans nécessiter une intervention humaine.

Quels sont les risques et les limitations associés à ces applications? Les blockchains remplacent les tiers de confiance centralisés (métiers bancaires, notaires, cadastres, etc.) par des systèmes informatiques distribués. Il est nécessaire d'analyser et de contrôler les risques, la sécurité, le coût. Quelles sont les limites économiques, juridiques, de gouvernance ou écologiques, ainsi que toutes les questions concernant la fiscalité, la territorialité, la propriété. Ces questions nécessitent de comprendre la technologie utilisée, son cadre, ses limites et ses contraintes. Ainsi La formation des *data scientists* au sein des banques est indispensable et ne doit pas se limiter à utiliser des systèmes « presse-bouton ». Tous les points précédents doivent être analysés en détail avant d'être utilisés.

D'autres éléments sont à prendre aussi en compte si on veut utiliser la technologie blockchain. Les données individuelles sont actuellement concentrées entre les mains de sociétés américaines telles que Google et Microsoft : serveurs par nature vulnérables aux attaques informatiques et aux exigences du gouvernement américain. La blockchain peut constituer un enjeu de souveraineté. Les normes des blockchain ne sont pas encore écrites: de nouveaux droits et devoirs doivent être définis, en particulier la propriété des données. Dans quelle mesure les entreprises ou les citoyens accepteront ils de remplacer les autorités de confiance historiques (banques, gouvernements, etc.) par des programmes informatiques? Comment gérer la diversité culturelle et sociale grâce aux lois mathématiques? Les réponses à ces questions jetteront les bases de l'utilisation future de la blockchain. Il est facile de tracer un parallèle entre la situation actuelle de la blockchain et celle d'Internet dans les années 1990: nous sommes au début d'une révolution dont la portée est encore difficile à mesurer, mais aux champs d'applications infinies. Il est donc indispensable de maîtriser l'ensemble des concepts.