EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Contribution au débat à propos du recours aux systèmes fondés sur des registres distribués (blockchain)

Point de vue du Contrôle fédéral des finances

novembre 2019

Contribution au débat à propos du recours aux systèmes fondés sur des registres distribués (blockchain)

Point de vue du Contrôle fédéral des finances

La blockchain (chaîne de blocs) – une des technologies dominantes des systèmes de registres distribués (*distributed ledgers*) – est sur toutes les lèvres. De nombreux spécialistes s'accordent à dire que les nouvelles technologies sur lesquelles s'appuient ces systèmes révolutionneront la manière dont nous effectuerons des transactions électroniques à l'avenir. Ce n'est qu'à propos de la vitesse à laquelle cette évolution s'imposera que les avis divergent[1]. Les pouvoirs publics envisagent eux aussi de recourir à ces systèmes, et de premiers projets pilotes utilisent déjà des technologies blockchain: depuis novembre 2017, la ville de Zoug propose ainsi à ses habitants une identité numérique qui s'appuie sur une technologie de ce type. Les détenteurs de l'e-ID zougoise ont pu s'en servir lors d'une consultation populaire en juin 2018, et 72 personnes ont saisi cette occasion[2]. Le canton de Genève délivre en guise de test des extraits électroniques du registre de commerce basés sur Ethereum, qui permettent au destinataire de vérifier s'ils ont effectivement été émis par ce canton[3]. Et dans le cadre d'un partenariat public-privé (PPP), le canton d'Argovie a participé à la mise en place de la plateforme cardossier, qui est fondée sur une blockchain[4]. Le cardossier devrait rassembler toutes les informations pertinentes sur le cycle de vie complet d'un véhicule, du fabricant jusqu'au ferrailleur (fabricant, importateur, concessionnaires, assureurs, autorisations, garages, sinistres, propriétaires, contrats de leasing etc.), et contribuer à la numérisation de l'écosystème des voitures. À l'heure actuelle, une douzaine d'autres acteurs font partie de ce PPP aux côtés du canton d'Argovie.

Tout comme l'ensemble des autorités, le CDF doit lui aussi analyser la question des conséquences qu'a l'utilisation des technologies des registres distribués (TRD) sur les unités administratives qu'il examine. Quand est-il approprié de recourir à ces technologies? Quels sont les risques spécifiques inhérents à ces dernières? Et quels sont par conséquent les aspects à examiner lorsqu'une unité administrative souhaite mettre en place ces nouvelles technologies?

Après avoir analysé l'état actuel de la technologie, le CDF a identifié en particulier les questions suivantes, auxquelles il y a lieu de répondre lorsqu'une entité envisage de recourir à des technologies de registres distribués:

1. *Les technologies de registres distribués permettent-elles de mieux satisfaire aux exigences métier que d'autres technologies?*

   Initialement, les technologies de registres distribués ont été mises au point pour pouvoir effectuer des transactions financières de manière fiable sans intermédiaire. Depuis lors, de nombreux autres champs d'application intéressants ont été identifiés, dont la traçabilité intégrale des marchandises (les diamants notamment) ou les contrats automatisés (contrats intelligents), pour ne citer que deux exemples. Cependant, il se peut, et c'est un risque à l'heure actuelle, que l'on mise sur cette nouvelle technologie parce qu'elle est à la

[1] Voir notamment https://hbr.org/2017/01/the-truth-about-blockchain (en anglais)
[2] https://www.luzernerzeitung.ch/zentralschweiz/zug/erfolgreiche-digitale-abstimmung-ld.1074829?reduced=true (en allemand)
[3] https://www.ge.ch/dossier/geneve-numerique/blockchain
[4] https://cardossier.ch/

mode, sans avoir vérifié de manière suffisamment approfondie si son utilisation se justifie sur le plan économique, si elle apporte une réelle valeur ajoutée, ou si, au contraire, elle complique la mise en place de solutions globales efficaces (l'interaction avec d'autres solutions de cyberadministration qui ne s'appuient pas sur une technologie de registres distribués notamment).

2. *Les exigences métier impliquent-elles que les données stockées dans le registre distribué sont destinées à ne jamais être modifiées ni supprimées?*

   Les systèmes actuels de registres distribués ont comme caractéristique de rendre impossible toute modification des données enregistrées après la réalisation d'une transaction, ce qui présente un avantage lorsque la traçabilité est déterminante. En revanche, cela signifie aussi que cette technologie ne se prête pas aux cas de figure où les données doivent être modifiées ultérieurement, même si ce besoin ne se présente que rarement. Et l'emploi de ces systèmes pose également un problème dans les contextes où les personnes concernées jouissent d'un droit à l'oubli (casier judiciaire entre autres).

3. *Tous les participants ont-ils le droit de consulter l'ensemble des informations stockées dans le système de registres distribués? Si tel n'est pas le cas, a-t-on pris des mesures adéquates pour garantir leur confidentialité?*

   Une blockchain, entre autres, est conçue comme un réseau «peer-to-peer». Chaque participant dispose d'une copie complète des données, l'avantage étant que les parties prenantes ne doivent dès lors pas faire appel à des tiers de confiance[5]. En conséquence, tous les participants ont en principe accès à l'ensemble des données, ce qui n'est pas acceptable dans tous les cas de figure. Il est certes possible d'empêcher la consultation de certaines données critiques en les chiffrant, mais il est difficile de mettre en œuvre des processus plus complexes de contrôle d'accès. Et en pratique, l'on a constaté que les mécanismes d'anonymisation et de pseudonymisation n'étaient pas fiables. Par conséquent, il faudrait éviter de stocker des données sensibles dans une blockchain.

4. *La technologie des registres distribués qui a été choisie est-elle appropriée?*

   Il est inexact de parler de «la blockchain». Le terme «blockchain» regroupe en fait plusieurs technologies[6] et composants différents (cryptographie, logique de contrôle, réseau «peer-to-peer», mécanisme de consensus, contrats intelligents, etc.), qui peuvent être combinés de diverses manières. Pour chacun de ces composants, il existe plusieurs formes de mise en œuvre qui ont chacune leurs forces et leurs faiblesses spécifiques. En outre, les systèmes fondés sur des registres distribués peuvent être publics ou privés, et être soumis ou non à autorisation[7]. Tous les modèles ne se prêtent pas à toutes les utilisations dans tous les environnements. La technologie doit être choisie en tenant compte du contexte global.

[5] Une nouvelle violation partielle du principe «peer-to-peer» a cependant été constatée dans des applications utilisées en situation réelle – l'application bitcoin par exemple. Étant donné que tout le monde n'est pas nécessairement en mesure de et disposé à fournir l'infrastructure technique requise, de nombreux utilisateurs de bitcoins font appel aux services de tiers.

[6] Blockchain, Ethereum, Hashgraph, etc.

[7] Dans une blockchain soumise à autorisation, seuls les participants dûment autorisés selon une procédure bien définie peuvent prendre part à la validation de transactions et à la création de nouveaux blocs.

5. *La sécurité requise des informations peut-elle être garantie?*

   Les systèmes de registres distribués favorisent clairement l'inviolabilité des données et la traçabilité des transactions, grâce à des procédés cryptographiques hautement perfectionnés. Combinées à la distribution des responsabilités, ces caractéristiques peuvent avoir un impact positif sur la sécurité mais elles ne suffisent pas. Il y a lieu d'accorder l'attention requise à la sécurité du système distribué dans son ensemble, et en particulier à celle du contrôle d'accès, de la protection du matériel et des logiciels utilisés pour *tous* les nœuds du réseau, ainsi que des processus et protocoles cryptographiques employés, et à la défense contre les attaques engendrant un déni de service. Les blockchains publiques doivent en outre garantir que des participants dotés de puissances de calcul extrêmement élevées ne puissent pas manipuler des données. D'après une estimation du BSI, l'Office fédéral allemand de la sécurité des technologies de l'information[8], l'on ne peut dès lors pas supposer d'emblée que le recours à une blockchain garantit la sécurité requise dans un cas de figure donné.

   Le fait de devoir stocker dans la blockchain des données qui ont une longue durée de vie représente un défi particulier: les solutions blockchain s'appuient sur des logiciels en source ouverte. Lorsque le code source continue à évoluer, ce qui est inévitable, des bifurcations («forks») peuvent se créer, et à ces occasions, diverses communautés de développeurs peuvent faire évoluer ce code de différentes manières. Et des fonctions que l'on avait choisi d'utiliser pourraient ne plus être disponibles dans de nouvelles versions logicielles. L'archivage des données représente également un défi. Enfin, à long terme, des procédés cryptographiques considérés comme sûrs actuellement pourraient se révéler insuffisants à l'avenir.

   De manière générale, l'on ne connaît pas assez les limites de ces technologies à présent. Et l'on ne sait pas non plus comment les coûts des transactions évolueront à long terme.

6. *La conformité du système est-elle garantie de manière pérenne?*

   À l'instar de tous les autres systèmes, ceux qui font usage de registres distribués doivent eux aussi être mis en œuvre correctement. De même, il faut veiller à ce que la logique métier soit représentée correctement dans le système (au moyen de contrats intelligents par exemple). Compte tenu de la complexité de cette technologie, il est laborieux de faire attester par un organisme neutre que le système a été mis en œuvre correctement. En outre, il faut garantir à long terme la possibilité de contrôler les modifications apportées au système, ce qui est également complexe avec les systèmes distribués qu'utilisent les blockchains publiques par exemple. À cet égard, les blockchains privées sont plus faciles à mettre en place et à entretenir.

7. *Dispose-t-on d'un savoir-faire suffisant à propos des registres distribués?*

   Les technologies utilisées sont extrêmement complexes, et l'on ne dispose pas encore d'un savoir-faire solide à leur égard. Les organisations responsables achèteront généralement la solution, avec le risque que ni ces dernières ni leurs fournisseurs n'aient la maîtrise nécessaire des technologies utilisées, surtout lorsqu'il faudra les faire évoluer ultérieurement et éventuellement les adapter en cas de comportement défectueux ou de problèmes de sécurité.

[8] Voir l'étude du BSI à ce sujet : https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf (en allemand)