Projet Jasper : les systèmes de paiement de gros décentralisés sont-ils aujourd'hui chose faisable?

James Chapman, Rodney Garratt[1], Scott Hendry, Andrew McCormack[2] et Wade McMahon

- Le grand livre partagé — mieux connu comme la technologie à la base du réseau Bitcoin — offre un moyen fondamentalement différent d'exécuter et de suivre les transactions financières. Les chercheurs étudient son utilité dans tous les pans du système financier.
- Le projet Jasper propose un prototype de système de paiement de gros fondé sur la technologie du grand livre partagé. Il nous a éclairés sur les forces et les faiblesses relatives associées à l'utilisation de cette technologie dans les infrastructures de marchés financiers.
- Pour les infrastructures de marchés financiers essentielles, par exemple les systèmes de paiement de gros, les versions actuelles de la technologie du grand livre partagé pourraient ne pas procurer, dans l'ensemble, un avantage net par rapport aux systèmes centralisés en place. Cela dit, les versions récentes sont plus évoluées que les premières applications de cryptomonnaie utilisant cette technologie.
- Pour le système financier, les avantages d'un système de paiement de gros fondé sur un grand livre partagé pourraient découler de l'interaction de ce système avec un plus grand écosystème d'infrastructures de marchés financiers reposant sur ce type de registre décentralisé, et toucher peut-être les transactions transfrontières.

Introduction

Les technologies financières désignent des innovations financières qui résultent des avancées technologiques et peuvent se traduire par de nouveaux types de modèles opérationnels, d'applications, de processus ou de produits. Les technologies financières ont une incidence importante sur les marchés financiers, les institutions financières et la prestation de services financiers[3].

1 Université de Californie à Santa Barbara et R3

2 Paiements Canada

3 Pour connaître les déterminants de l'évolution des technologies financières, voir Schindler (à paraître).

Encadré 1

Le grand livre partagé, de quoi s'agit-il?

La technologie du grand livre partagé a été popularisée après l'avènement de la cryptomonnaie bitcoin en 2009. Un bitcoin (avec un « b » minuscule) est un jeton numérique qui représente une monnaie numérique. Le Bitcoin (avec un « B » majuscule) désigne le système dont se servent les utilisateurs pour transférer des bitcoins. Ce transfert s'opère à travers un grand livre de transactions pouvant être vu de tous et qui est tenu à jour par un réseau décentralisé de « mineurs », les validateurs exploitant les ordinateurs qui forment les nœuds du système Bitcoin. Ces nœuds mettent à jour le grand livre en assurant la consignation des nouvelles transactions réalisées. Le grand livre est constitué d'une série de blocs de transactions liés les uns aux autres par un procédé cryptographique. Ce grand livre est ce qu'on appelle une chaîne de blocs.

Ce système a marqué une avancée, car il a permis de démontrer deux choses : il est possible de tenir à jour un grand livre d'informations échangées entre des parties de telle façon que, d'une part, aucune surveillance ne soit exercée et que, d'autre part, les membres du système Bitcoin parviennent, de manière crédible, à actualiser le grand livre et à en valider les transactions même si aucun d'entre eux ne s'en remet à un tiers de confiance.

Le grand livre partagé est mis à jour sans qu'il soit fait appel à un tiers de confiance. Pour y parvenir, des mineurs sont mis en concurrence : ceux-ci doivent résoudre une énigme mathématique afin d'acquérir le droit de valider des blocs de transactions. Le premier mineur à trouver la clé d'une nouvelle énigme diffuse le bloc ainsi que la solution auprès du reste des mineurs et « récolte » en échange de nouveaux bitcoins créés avec ce bloc. Le problème soumis aux mineurs est difficile à résoudre, mais sa solution se vérifie facilement. Lorsque les autres nœuds ont vu et vérifié une nouvelle solution, le nouveau bloc est ajouté à la chaîne et les transactions à l'intérieur du bloc sont réputées réglées. Dès lors, les mineurs amorcent la validation d'un autre groupe de transactions. On appelle « méthode de consensus » le protocole par lequel les nœuds s'entendent sur le choix d'un nouveau bloc, et « preuve de travail », l'énigme.

Si le système Bitcoin a prouvé qu'il était particulièrement résilient, plusieurs aspects le rendent néanmoins mal adapté aux besoins des infrastructures de marchés financiers : en effet, 1) les transactions peuvent être vues de tous; or, cette propriété pourrait, par exemple, contrevenir à la législation bancaire et désavantager certaines parties aux transactions; 2) les preuves de travail demandent énormément de temps et d'énergie à produire et apportent des bénéfices dont n'ont généralement pas besoin les environnements où intervient un tiers de confiance; enfin, 3) le système peut être intégré par tous ceux qui le souhaitent, et les participants sont anonymes.

Pour surmonter ces difficultés, les sociétés de technologie financière ont entrepris de mettre au point des systèmes concurrents du Bitcoin. Ces nouveaux systèmes à grand livre partagé limitent l'accès à un nombre restreint de contreparties de confiance. Dans certains systèmes, des protocoles de concertation différents remplacent la méthode de consensus. Par exemple, sur Corda, la plateforme utilisée dans la seconde phase du projet Jasper, un nœud auquel tous les participants accordent leur confiance remplit une fonction notariale et se substitue ainsi à la preuve de travail. Pour finir, ces systèmes font l'impasse sur la chaîne de blocs et remplacent ce concept par un grand livre. Ce grand livre demeure partagé entre les nœuds, mais chaque nœud n'a accès qu'aux données qui lui sont nécessaires. Le dispositif offre moins de transparence à l'intérieur du système et plus de confidentialité aux participants.

Parmi les innovations financières qui recèlent un fort potentiel figure la technologie du grand livre partagé — encore appelée « chaîne de blocs », selon le nom donné à l'une de ses applications bien connues (**Encadré 1**). Cette technologie, introduite en 2008 en même temps que la cryptomonnaie bitcoin (Nakamoto, 2008), permet de valider et d'enregistrer les transactions en toute sûreté. Un grand livre partagé est une base de données à laquelle ont accès un certain nombre de parties. Il permet à ces parties d'exécuter des transactions qu'elles ont convenu et de s'entendre sur les modifications à apporter à la base de données. Ainsi, le livre assure l'uniformité des opérations entre les parties. L'atout majeur de pareil registre tient à ce que

les parties autorisées disposent, grâce à une méthode de consensus, de versions identiques des données sans devoir faire appel à une base de données ou à un administrateur centraux[4].

D'usage plus général, la plateforme à grand livre partagé appelée Ethereum a été lancée en 2013. Elle sert à définir, créer et échanger tout type d'actifs numériques. Elle permet en outre d'exécuter automatiquement les modalités de contrats intelligents, ce qui offre une plus grande praticité que de simplement transférer un type particulier d'actif (Buterin, 2013). Ces évolutions ont suscité un vif intérêt dans le secteur financier. La nature partagée du livre sous-jacent pourrait être source de nombreux avantages : amélioration de l'efficience des processus, réduction des coûts, résilience, interopérabilité, etc. Cependant, l'adaptation de la technologie du grand livre partagé aux besoins du secteur financier comporte aussi son lot de défis. Qu'on pense à la vitesse d'exécution des transactions et à leur confidentialité ainsi qu'à l'irrévocabilité des règlements. De jeunes entreprises de technologies financières ont mis au point des systèmes à registre décentralisé plus généraux — comme la plateforme Corda[5], élaborée par R3 — pour répondre aux besoins du secteur financier.

Les participants au secteur financier s'intéressent à la technologie du grand livre partagé pour plusieurs raisons. Elle est susceptible de réduire les coûts des activités post-marché par l'automatisation de divers processus de règlement. Elle peut améliorer la fiabilité et la traçabilité de l'information stockée dans le grand livre, étant donné que la méthode de consensus restreint le nombre de participants habilités à modifier le livre partagé et le type de modifications qu'ils sont en droit d'y apporter. Enfin, le recours à des processus décentralisés pourrait accélérer le règlement des transactions, qui se compterait éventuellement en heures ou en minutes plutôt qu'en jours.

L'un des centres d'intérêt se rapporte aux conséquences possibles de la technologie du grand livre partagé pour les infrastructures de marchés financiers. Ces infrastructures tiennent lieu de tiers de confiance entre les institutions financières : elles suivent les transactions et les enregistrent dans les registres centralisés. Les exploitants d'infrastructures de marché, les participants et les banques centrales portent tous un intérêt aux gains d'efficience et aux possibilités qu'un système à grand livre partagé pourrait leur apporter par rapport aux systèmes centralisés actuels. Il s'ensuit que beaucoup d'avancées récentes dans ce domaine s'articulent autour des moyens qui permettraient aux exploitants traditionnels de systèmes centralisés de cristalliser les avantages de cette technologie et d'obvier à ses inconvénients. Par exemple, l'une des pratiques courantes consiste à créer des systèmes à grand livre partagé dont l'accès n'est autorisé qu'à un groupe d'entités de confiance, ce qui contraste avec les réseaux ouverts tel Bitcoin, auxquels toute entité peut participer. Jusqu'ici, les banques centrales n'ont mis en œuvre la technologie du grand livre partagé que dans des prototypes, et on peut s'attendre à ce qu'elles approfondissent leur examen des applications possibles de cette technologie.

4 Pour avoir un aperçu de la technologie du grand livre partagé et des questions qu'elles soulèvent pour les politiques, voir le cadre analytique du Comité sur les paiements et les infrastructures de marché (2017). Pour lire une introduction technique mais accessible portant sur certaines des notions traitées dans le présent article, voir Narayanan et autres (2016).

5 Corda est une plateforme libre à grand livre partagé servant à enregistrer, à gérer et à automatiser des contrats juridiques interentreprises.

L'une des questions à l'étude est l'application potentielle de la technologie du grand livre partagé aux systèmes de paiement de gros. Le Système de transfert de paiements de grande valeur (STPGV), exploité par Paiements Canada, est le système de paiement de gros utilisé au Canada. Le STPGV traite chaque jour ouvrable des transactions qui représentent 175 milliards de dollars en moyenne. Il a été désigné comme une infrastructure de marché financier d'importance systémique et est encadré par la Banque du Canada conformément aux Principes pour les infrastructures de marchés financiers[6].

Parce qu'ils sont relativement simples, les systèmes de paiement de gros offrent logiquement une première possibilité d'adaptation de la technologie du grand livre partagé. Ils jouent également un rôle essentiel dans le maintien de la stabilité du système financier. Par conséquent, il importe que les autorités d'encadrement, comme la Banque du Canada, comprennent en quoi l'utilisation de cette technologie pourrait modifier la structure et le fonctionnement des systèmes centralisés, s'attachent à déterminer si un système fondé sur un livre partagé peut répondre aux normes internationales en vigueur et découvrent quelles seraient les incidences de ce type de plateforme sur les politiques régissant les systèmes de paiement.

En 2016, Paiements Canada, conjointement avec la Banque du Canada, R3 et des banques commerciales canadiennes qui sont membres du consortium de R3, a lancé un projet expérimental appelé « Jasper » afin d'étudier un système de paiement de gros faisant appel à la technologie du grand livre partagé[7]. Le but premier de Jasper consistait à mettre au point un prototype (sans aucune intention de passer ensuite à un système de production) utilisant un actif de règlement émis et contrôlé par une banque centrale. À la première phase, les participants au projet ont mis au point un dispositif de règlement sur une plateforme Ethereum et démontré que ce dispositif leur permettait d'échanger un actif de règlement entre eux. La deuxième phase repose sur une plateforme Corda munie d'un mécanisme d'économie des liquidités grâce auquel les participants peuvent coordonner leurs paiements pour réduire leurs besoins en liquidité. Dans le cadre de cette phase, les participants préparent en ce moment un document d'orientation plus long, qui sera publié d'ici la fin de juin 2017. Ce document exposera dans le détail les incidences des travaux du point de vue technique et sur le plan des politiques publiques.

Le projet a notamment fait ressortir que, en fait de paiements interbancaires, les différentes versions de la technologie du grand livre partagé pourraient ne pas procurer, globalement, un avantage net par rapport aux systèmes centralisés en place. Les systèmes de base de paiement de gros fonctionnent assez efficacement. Cela dit, un système de paiement de gros fondé sur la technologie du grand livre partagé est susceptible d'apporter un avantage net au plus large groupe des participants des systèmes de paiement et à l'ensemble du système financier, si l'on considère les économies qui découleraient d'un allègement des opérations de rapprochement par les services post-marché et d'une meilleure interaction avec un plus

6 Les Principes forment un ensemble de normes internationales encadrant les systèmes de paiement d'importance systémique. Ils ont été établis par la Banque des Règlements Internationaux (Comité sur les systèmes de paiement et de règlement et Organisation internationale des commissions de valeurs, 2012).

7 R3 est un consortium international de grandes banques qui a pour but d'étudier des applications à grand livre partagé et d'en élaborer pour le secteur financier. Les membres canadiens du consortium sont les suivants : BMO Banque de Montréal, Banque Canadienne Impériale de Commerce, HSBC, Banque Nationale du Canada, Banque Royale du Canada, Banque Scotia et TD Canada Trust. Ces sept institutions sont aussi membres de Paiements Canada, et toutes participent au STPGV.

grand écosystème d'infrastructures de marchés financiers reposant sur la technologie du livre partagé. Les sections qui suivent donnent un aperçu général du projet et présentent les premières constatations.

Principales caractéristiques du projet Jasper

Grâce au projet Jasper, on a maintenant une bien meilleure idée de la façon dont une banque centrale et les institutions financières participantes peuvent effectuer des paiements interbancaires à l'aide d'un livre partagé[8]. Le projet a aussi permis de mieux comprendre le fonctionnement d'un système de paiement de gros utilisant différentes plateformes à grand livre partagé, et aidé à déterminer comment y intégrer des caractéristiques des systèmes de paiement modernes, par exemple les files d'attente, pour accroître l'efficience en réduisant les besoins en sûretés. Enfin, l'élaboration d'un prototype fonctionnel a permis de mieux saisir les risques potentiels associés aux systèmes à grand livre partagé et les moyens de les atténuer.

Lors de l'élaboration du projet Jasper, le premier grand défi a été d'établir le mode de transfert des fonds. Les Principes exigent qu'une infrastructure de marché financier effectue ses règlements en monnaie de banque centrale si possible, généralement au moyen de comptes ouverts auprès de la banque centrale. Ainsi, on a retenu l'idée de certificats numériques de dépôt émis par une banque centrale pour représenter les dépôts à la Banque du Canada. Ces certificats sont un symbole numérique de la monnaie émise par la Banque du Canada; ils pourraient constituer un moyen de généraliser l'utilisation de la monnaie de banque centrale (Garratt, 2017). C'est la Banque qui injecte les certificats dans le système et ils sont garantis au pair par des espèces que les participants lui remettent en nantissement. L'échange de certificats contre de la monnaie de banque centrale n'augmente donc en rien la monnaie en circulation dans le système bancaire.

Les participants se servent des certificats pour procéder, dans le système, à l'échange et au règlement de paiements interbancaires. Dans le cycle de traitement du projet Jasper, le règlement atteint l'irrévocabilité par une inscription dans les livres de la Banque du Canada, après que les participants ont échangé avec celle-ci des certificats contre des dollars canadiens transférés dans leurs comptes de règlement respectifs. En fait, ces certificats font fonction d'espèces dans le système.

Le deuxième grand défi a été de déterminer comment régler les paiements le plus efficacement possible avec un minimum de certificats ou de liquidités. Pendant longtemps, le règlement des paiements interbancaires s'est fait au moyen de systèmes qui procédaient, à la fin de la journée, à la compensation entre les participants. Le volume et la valeur des opérations allant crescendo dans ces systèmes, les banques centrales ont commencé à s'inquiéter des risques inhérents à la compensation. En réaction, la plupart des banques centrales ont décidé de mettre en œuvre des systèmes de règlement brut en temps réel (RBTR) (voir Bech et Hobijn, 2007), dans lesquels les paiements sont traités un par un, sans délai, tout au long de la journée, et sont irrévocables. Le prototype de la première phase du projet Jasper était un pur système RBTR : chaque paiement du registre a été préfinancé par des certificats numériques de dépôt portés au compte des participants.

8 Pour en savoir plus au sujet des recherches que mène la Banque du Canada sur la monnaie électronique, consultez son site Web.

Les systèmes RBTR éliminent le risque de règlement au prix d'un besoin de liquidité accru. Dans ces systèmes, les besoins de liquidité peuvent être énormes vu la grande valeur des transactions qui y sont réglées — habituellement jusqu'à un cinquième du produit intérieur brut d'un pays tous les jours. Pour rendre ces systèmes moins demandeurs de liquidité, des exploitants dans diverses parties du monde se sont dotés de mécanismes d'économie des liquidités[9]. Les mécanismes les plus efficaces sont ceux qui favorisent le règlement en appariant périodiquement les paiements de compensation dirigés vers une file d'attente centrale et en ne réglant que les obligations nettes[10]. Toutefois, les algorithmes de compensation causent des délais de règlement, ce qui s'avère inacceptable dans le cas de certains types de paiements. Aussi les banques ont-elles besoin d'un moyen pour effectuer les paiements à délai de règlement critique. La deuxième phase du projet Jasper visait à examiner la possibilité de donner aux banques le choix de demander le règlement immédiat des paiements ou de les placer dans une file d'attente en vue de la compensation et d'un règlement différé. Il semble que le projet Jasper soit le premier cas où une institution publique intègre un algorithme destiné à opérer une économie de liquidités à une plateforme utilisant un grand livre partagé.

Aspects techniques du projet Jasper

La montée du bitcoin a attisé l'intérêt des développeurs d'infrastructures de marchés financiers pour la technologie du grand livre partagé. Le réseau Bitcoin recourt à un protocole de preuve de travail qui assure une validation décentralisée des transactions. Ce protocole sert à dissuader les participants qui chercheraient à prendre le contrôle d'un système à grand livre partagé ouvert pour y inscrire en double des dépenses ou falsifier le registre. Pour empêcher ces fraudes, le protocole impose à chaque nœud vérifiant les transactions de produire un travail coûteux. Ce protocole peut cependant être très onéreux sur le plan de la puissance de calcul. De plus, il nécessite un certain degré de transparence à l'égard de toutes les transactions. Dans la chaîne de blocs de Bitcoin, par exemple, l'identité des participants est masquée, mais tous voient les transactions. Les coûts engendrés et cette transparence découlent de la nature anonyme et ouverte des grands livres partagés comme Bitcoin.

La première phase du projet Jasper se fondait sur la plateforme Ethereum, dont la méthode de consensus est une preuve de travail. La version publique d'Ethereum est un système sans restriction d'accès : tous les participants disposent d'une copie intégrale du registre. Pour le projet Jasper, on s'est servi d'une version ne donnant accès au registre qu'aux seuls membres de R3. Dans un réseau privé fermé, comme c'est le cas d'un système de paiement de gros, les preuves de travail ne sont ni nécessaires ni souhaitées. N'autoriser l'accès qu'aux contreparties de confiance permet aux développeurs de protocoles pour les grands livres partagés d'employer d'autres protocoles efficaces pour exécuter les fonctions de validation et d'enregistrement.

9 Au début des années 1990, environ 3 % des grands systèmes de paiement dans le monde utilisaient des mécanismes d'économie des liquidités; en 2005, cette proportion s'élevait à 32 % (Bech, Preisig et Soramäki, 2008). Cette tendance s'est poursuivie, à tel point que la quasi-totalité des principaux systèmes de paiement fait appel à ce mécanisme, sous une forme ou une autre.

10 Les économies de liquidité générées par les algorithmes de compensation viennent de ce que les liquidités ne sont alors nécessaires que pour combler la différence nette entre les paiements et ainsi permettre le règlement. Supposons que la banque A doive verser une somme de 100 dollars à la banque B, et celle-ci, une somme de 90 dollars à la banque A. Dans ce cas, le montant nécessaire pour régler ces deux paiements, s'ils étaient mis dans une file d'attente dotée d'un algorithme de compensation, serait de 10 dollars. À l'inverse, sans mécanisme d'économie des liquidités, il faudrait au moins 100 dollars pour régler ces deux paiements.

La deuxième phase du projet Jasper reposait sur la plateforme Corda, qui a recours à une fonction notariale plutôt qu'à une preuve de travail. La principale caractéristique de Corda a trait à l'actualisation du registre; celle-ci fait intervenir deux fonctions : une fonction de validation et une fonction d'unicité[11]. La fonction de validation, exécutée par les parties à la transaction, permet de vérifier que tous les renseignements concernant la transaction sont exacts et que l'expéditeur dispose des fonds nécessaires. La fonction d'unicité, pour sa part, est exécutée par un notaire. Dans le cas du système du projet Jasper, il s'agit de la Banque du Canada, qui, à ce titre, a accès à l'intégralité du registre et peut donc vérifier que les fonds d'une transaction sont disponibles.

Mécanismes d'économie des liquidités dans le cadre du projet Jasper

Le mécanisme d'économie des liquidités utilisé dans le projet Jasper prend la forme d'une file d'attente de paiements pourvue d'un dispositif de compensation multilatérale périodique. Du point de vue conceptuel, son fonctionnement est très simple. Si une banque doit effectuer un paiement non urgent, elle peut le placer dans une file d'attente. Après qu'elle a envoyé un avis de paiement à la file, le paiement en question est mis en attente avec d'autres jusqu'au début d'un cycle d'appariement. La file d'attente est alors verrouillée temporairement pendant qu'un algorithme apparie tous les paiements soumis, détermine les obligations nettes de chaque banque et évalue la position de liquidité de chacune[12].

Par nature, une file d'attente de paiements est centralisée. L'un des grands défis a été de mettre en œuvre une file dans un système à grand livre partagé au lieu de recourir à un système de grand livre traditionnel centralisé fondé sur des comptes. Ce problème technique a été source d'une grande complexité et a mis en lumière les difficultés inhérentes à l'élaboration de systèmes décentralisés qui nécessitent une certain centralisation du contrôle ou d'une partie de l'information.

La solution novatrice mise au point pour le projet Jasper a été l'intégration d'une séquence de « flux-reflux » dans la plateforme Corda. Avant le début du cycle d'appariement, les banques sont autorisées à placer des paiements dans la file d'attente. Toutefois, ces paiements ne passent pas immédiatement par le double test de validation et d'unicité nécessaire pour inscrire une transaction au registre du système Corda. Les instructions de paiement attendent plutôt dans la file jusqu'au début du cycle, après quoi se produit une série d'opérations. D'abord, durant la phase de flux, un avis est adressé à toutes les banques participant au cycle pour leur demander d'envoyer à la Banque du Canada des certificats numériques de dépôt. Chacun de ces paiements est alors validé, puis inscrit au registre. Ensuite, durant la phase de reflux, l'algorithme d'appariement génère, en fonction des fonds disponibles, un sous-ensemble de paiements à compenser, calculés en valeur nette. La Banque du Canada renvoie à chacune des banques participantes un paiement en certificats numériques d'une valeur égale au montant qu'elles ont versé, somme à laquelle est ajoutée ou retranchée tout montant qui leur est dû ou qu'elles doivent, suivant les résultats des calculs de l'algorithme d'appariement.

---

11 Voir le document d'orientation non technique sur Corda.

12 Le concept est semblable au mécanisme d'économie des liquidités intégré en avril 2013 au Système de paiement interbancaire automatisé avec règlement le jour même (CHAPS), le système de paiement de gros du Royaume-Uni. Dans ce système, le temps écoulé entre chaque cycle d'appariement est de deux minutes, et, dans chaque cycle, les paiements sont gelés pendant les 20 secondes durant lesquelles s'exécute l'algorithme d'appariement. Le Royaume-Uni fait état d'économie de liquidités de l'ordre de 20 % (Davey et Gray, 2014).

Supposons, à titre d'illustration, que deux banques seulement — A et B — placent dans la file des paiements mutuels d'une valeur de 100 et 90 dollars respectivement, et que chacune ait déjà envoyé à la file 15 dollars dans le cadre de la phase de flux. Après compensation des deux paiements, l'algorithme débiterait 10 dollars à la banque A et créditerait 10 dollars à la banque B. Compte tenu du montant qu'elles ont versé lors de la phase de flux, les banques A et B recevraient respectivement, lors de la phase de reflux, 5 et 25 dollars.

Ces transactions sont alors validées, puis inscrites au registre. Les paiements non appariés par l'algorithme restent dans la file. À cette étape, un nouveau cycle d'appariement commence. Les banques ont la possibilité de mettre des paiements dans la file ou d'en retirer jusqu'à la fin du cycle suivant, et le processus se répète en boucle.

Efficience du projet Jasper et risques pour la stabilité du système financier

L'efficience du projet Jasper et les risques pour la stabilité du système financier qui s'y rattachent ont été évalués au regard des Principes qui s'appliquent à l'exploitation d'un système de paiement de gros. Seuls ont été considérés les principes pertinents pour un prototype. On a exclu les principes s'appliquant uniquement aux aspects des infrastructures de marchés financiers pertinents pour un système de production, par exemple ceux ayant principalement trait à la gouvernance et aux questions juridiques[13]. Ainsi, les principes examinés peuvent être groupés selon les risques qu'ils encadrent : risque de crédit et de liquidité, risque de règlement et risque opérationnel.

Risque de crédit et de liquidité

Sur les plateformes du projet Jasper, le risque de crédit est nul parce que tous les paiements représentent une créance sur les dépôts effectués auprès de la banque centrale, ces dépôts étant un actif sans risque. Les participants transfèrent des fonds à la Banque du Canada par l'intermédiaire du STPGV, et la Banque crée en retour des certificats numériques de dépôt pouvant être échangés sur la plateforme à grand livre partagé. Dans l'ensemble, aucun aspect du prototype ne s'est révélé fondamentalement incompatible avec le principe relatif au risque de crédit.

Comme expliqué précédemment, les systèmes du projet Jasper intègrent un mécanisme d'économie des liquidités qui reproduit les fonctionnalités des systèmes RBTR existants afin d'atténuer le risque de liquidité, c'est-à-dire le risque qu'un participant n'ait pas suffisamment de certificats numériques pour effectuer un paiement. On met actuellement à l'essai l'efficacité de ce mécanisme à partir de données simulées. Quoiqu'il soit trop tôt pour prédire les résultats de ces simulations, nous pouvons dire que, jusqu'à maintenant, rien n'indique qu'un pareil mécanisme intégré à un grand livre partagé pourrait avoir des performances ou une efficacité différentes de celles d'un mécanisme similaire dans un système centralisé. Selon toute vraisemblance, le mécanisme mis en œuvre pour le projet Jasper générerait des économies de liquidité analogues à celles des mécanismes en place.

13 Ont aussi été exclues d'autres questions juridiques qui sortent du cadre des Principes, par exemple les exigences imposées par la lutte contre le blanchiment d'argent.

Risque de règlement

Le règlement désigne le transfert irrévocable et inconditionnel d'un actif. Poser les conditions qui définissent la finalité d'un règlement est un acte essentiel pour la stabilité d'un système financier.

Deux dimensions de la finalité des règlements intéressent les dispositifs inspirés de la technologie du grand livre partagé, comme ceux mis en œuvre dans le projet Jasper : le règlement opérationnel (qui renvoie au degré de certitude de la procédure d'actualisation d'un registre décentralisé) et le règlement légal (à savoir, la finalité du règlement telle qu'elle est définie par les règles d'un système et les textes de loi y afférents).

Dans le projet Jasper, le transfert d'un certificat numérique de dépôt s'apparente au transfert intégral et irrévocable de la créance sous-jacente exigible sur les fonds déposés auprès de la banque centrale, ce qui assure la finalité du règlement légal. Cette caractéristique concerne l'émission des certificats : elle n'est donc pas liée aux plateformes sur lesquelles repose le projet Jasper.

À l'inverse, pour qu'il y ait finalité d'un règlement opérationnel, il faut d'abord que soient résolus les problèmes posés par la technologie sous-jacente des plateformes utilisant le grand livre partagé. Dans le cas d'Ethereum, les paiements sont validés à l'aide d'une preuve de travail, la méthode de consensus employée sur cette plateforme. Or, comme ce genre de règlement subordonné à une preuve de travail est probabiliste, le paiement résultant n'est jamais complètement réglé, car il demeure une légère possibilité qu'il puisse être contrepassé. En fait, le règlement acquiert un degré croissant de certitude dès lors que la transaction inscrite devient plus immuable, mais il n'atteint jamais l'irrévocabilité. Sur la plateforme Corda, le notaire permettrait, dans l'absolu, d'éliminer cette incertitude parce qu'il serait impossible de contrepasser des transactions déjà réalisées. Pour autant, puisque ce système n'a pas été soumis à un test de résistance, la finalité du règlement pourrait rester exposée à un risque.

Dans l'ensemble, adopter Corda à la place d'Ethereum permet de réduire le risque de règlement et de rendre un système de production plus près de répondre aux exigences associées au principe relatif au risque de règlement. Un avis plus définitif nécessitera d'autres tests.

Risque opérationnel

La résilience, la sûreté et la capacité d'évolution sont des considérations essentielles quand il s'agit du risque opérationnel des systèmes de paiement de gros. Dans la mesure où le projet Jasper ne concerne pas une plateforme de production, il n'était pas possible d'évaluer en détail toutes les sources de risque opérationnel. Cela dit, la résilience et la capacité d'évolution étaient des aspects centraux de ce projet.

Sur le plan de la résilience, il était important de savoir si une plateforme de paiement de gros fondée sur un grand registre décentralisé pouvait offrir de la résilience à moindre coût en évitant d'avoir un point de défaillance unique. La première phase du projet Jasper a donné lieu à une réduction des coûts de la haute disponibilité[14], car les nœuds exploités par chacun des participants constituaient en définitive une chaîne de sauvegarde pour les données partagées entre eux. Cette propriété garantissait une haute disponibilité sans qu'un autre rideau de protection anti-risque soit nécessaire

14 Un système de paiement est dit à haute disponibilité s'il fonctionne l'essentiel du temps où il est censé fonctionner, par exemple, 99,99 % du temps.

pour chaque nœud. Mais l'ajout d'une autre fonction, par exemple un mécanisme d'économie des liquidités, peut recréer une exposition de la plateforme à un point de défaillance unique. La résilience est donc un aspect qui doit faire l'objet d'une attention toute particulière lors de la planification de la mise en œuvre, et ce, pour trois raisons.

Tout d'abord, les nouvelles composantes technologiques — par exemple, la gestion des clés, du contrôle de l'identité et de l'accès — sont fondées sur des modèles centralisés et sur l'existence de principe d'un exploitant unique investi de la confiance des participants (des versions décentralisées de ces modèles sont à un stade préliminaire). D'où leur défaut : tout comme les systèmes centralisés actuels, ces importantes composantes sont confrontées à la vulnérabilité que présente un point de défaillance unique. Par exemple, des clés numériques sont assignées à chaque participant et lui servent à prouver qu'il a le droit d'effectuer des transactions sur certains actifs. Tout opérateur d'un nœud de la chaîne de blocs doit pouvoir stocker en toute sécurité ses propres clés numériques dans le système, et il doit éviter de partager ces clés avec d'autres membres du réseau. Il importe donc que les composantes qui servent au stockage des clés numériques aient une haute disponibilité de manière à ce que l'on puisse éviter le risque causé par un point de défaillance unique. Il importe également de créer une copie de ces composantes pour faciliter la reprise après sinistre, étant donné que les informations qu'elles renferment ne peuvent être restituées à partir du nœud d'un autre participant.

La deuxième raison ressort de la poursuite de la comparaison entre les points de défaillance uniques des systèmes à grand livre partagé et ceux d'un système comme la plateforme Corda où existe un notaire. Contrairement à ce qui se passe dans les dispositifs qui font intervenir une preuve de travail, les nœuds utilisés par chacun des participants doivent pouvoir envoyer ou recevoir des paiements. Or, cette caractéristique réduit la résilience du système. Corda, la plateforme à grand livre partagé étudiée dans le cadre du projet Jasper, sépare les données afin que chaque nœud n'ait accès qu'à une partie de l'information et ne puisse assurer que la mise à jour de ce groupe de données. Cette approche, qui a l'avantage de résoudre les problèmes liés à la confidentialité des données, crée des difficultés importantes pour la réplication des données à travers le réseau[15]. Car, à la différence des systèmes avec chaîne de blocs publique, dans lesquels tous les nœuds ont une copie d'une base de données identique (comme dans la première phase du projet Jasper), les systèmes avec restriction d'accès ont autant de points de défaillance qu'il y a de nœuds. Autrement dit, au lieu de participer à la résilience du système comme c'est le cas dans la chaîne de blocs d'Ethereum, chaque nœud requiert plutôt une réplication et un archivage des données pour que les opérations se poursuivent.

Troisième raison : un système avec notaire a plus de chances d'avoir un point de défaillance unique, car les nœuds y sont relativement plus spécialisés que dans un système faisant appel à des preuves de travail. Dans la seconde phase du projet Jasper, le rôle du notaire que l'on retrouve dans Corda est tenu par la Banque du Canada; ainsi une panne à la Banque empêcherait-elle le traitement des paiements. C'est un fait important puisqu'il montre que la résilience des opérations dépend de la fonction accomplie par chaque nœud.

15 Il convient de souligner que, dans Corda, les demandes en suspens adressées aux nœuds sont mises dans la file d'attente. De la sorte, il est toujours possible de traiter les transactions dès qu'un participant reprend ses opérations après une panne.

Selon les données d'évaluation, les grands livres partagés munis d'un mécanisme de restriction d'accès pourraient, en regard des deux plateformes centralisées et d'une plateforme ouverte avec grand livre partagé, amoindrir la résilience des opérations s'ils étaient mal conçus. Cet impératif de résilience opérationnelle pourrait faire monter le coût d'une mise en conformité d'un système basé sur Corda (système de la seconde phase du projet Jasper) avec les Principes pour les infrastructures de marchés financiers, par rapport au coût de conformité associé au système centralisé existant. Il est par conséquent probable que chaque participant devra se doter d'un nœud à haute disponibilité afin de réduire le risque de panne.

La capacité d'évolution est une autre considération essentielle du risque opérationnel qui est énoncée dans les Principes. À l'heure actuelle, le STPGV traite 32 000 opérations journalières et atteint un volume maximal d'environ 10 opérations à la seconde. Le caractère décentralisé des grands livres partagés s'accompagne d'un coût sur le plan de la puissance de calcul. Les plateformes qui, à l'exemple d'Ethereum, utilisent une preuve de travail ont une capacité d'évolution limitée. Pour la première phase, la capacité de traitement était d'environ 14 opérations à la seconde, car Ethereum a été conçue pour un réseau public Internet où le plafonnement du débit pourrait compromettre la circulation de l'information entre les nœuds. Même si cette capacité de traitement suffit pour prendre en charge les volumes quotidiens du STPGV, elle pourrait causer des contraintes futures en ce qui concerne les volumes, par exemple dans des périodes de tensions ou de volatilité sur les marchés. À l'inverse, la capacité d'évolution ne représenterait pas une contrainte sur la plateforme Corda, car la méthode de consensus n'y repose pas sur un délai précis et la vérification des transactions ne fait intervenir que les nœuds des parties concernées et le notaire.

Transparence et confidentialité

Préserver la confidentialité des opérations qu'effectuent les participants entre eux est une exigence cardinale pour les systèmes de paiement de gros. C'est un impératif pour éviter que les participants qui ne sont pas partie aux opérations profitent des informations livrées par ces transactions. Ce type de confidentialité pourrait aussi être privilégié ou exigé par les clients d'un participant. Dans ces conditions, les plateformes qui utilisent des preuves de travail seraient mal adaptées à ce genre de systèmes de paiement de gros puisqu'elles reposent sur l'idée que toutes les transactions réalisées en leur sein peuvent, à terme, être vues publiquement.

À l'opposé, des systèmes à grand livre partagé comme Corda, qui s'appuient sur un notaire, permettent de renforcer la confidentialité, car une tierce partie légitime (par exemple, la Banque du Canada) facilite la vérification de toutes les transactions. L'opacité d'un système comme Corda signifie en revanche qu'aucun des nœuds, si ce n'est peut-être le notaire, n'est en possession de l'ensemble des informations. Partant, la corruption de données au niveau d'un ou de plusieurs nœuds pourrait rendre impossible la reconstitution du réseau tout entier, dans la mesure où le tiers de confiance lui-même ne dispose pas d'une copie complète du grand livre. Cette situation rend indispensables les dispositifs de sauvegarde pour chacun des nœuds et entraîne la perte des économies d'échelle associées aux systèmes centralisés. Elle nous amène aussi à nous demander si les bénéfices proposés sur le plan de la résilience par la technologie du grand livre partagé sont envisageables dans un contexte où la protection de la confidentialité des transactions est un impératif.

Conclusion

Le projet Jasper nous a permis de mieux comprendre les fonctions et les responsabilités de l'exploitant d'un système de paiement de gros fondé sur un grand livre partagé, des participants au système et de la banque centrale. Le rôle de l'exploitant d'une plateforme à grand livre partagé s'apparenterait davantage au rôle d'un faiseur de règles ou d'un producteur de normes qu'à celui d'un exploitant traditionnel d'infrastructure TI. La technologie du grand livre partagé a des retombées sur les fonctions des exploitants aussi bien que sur l'application ou la modification des Principes. Il pourrait être nécessaire à terme d'actualiser les Principes afin que les autorités réglementaires y incluent des principes portant sur l'organisation d'une infrastructure de marché fondée sur un grand livre partagé.

Par ailleurs, le travail accompli dans le cadre du projet Jasper a permis aux parties prenantes du système de paiement de gros d'élaborer ensemble la plateforme du projet. Grâce à ce projet, les partenaires du privé et du public ont pu en apprendre beaucoup plus sur les volets techniques. Ils ont ainsi reconnu de part et d'autre la complexité des processus en jeu, et ont surmonté les obstacles techniques en cultivant la collégialité. Le projet Jasper a également permis de procéder à une comparaison complète des différentes technologies du grand livre partagé, en confrontant tous les points de vue (à savoir, ceux de l'autorité de surveillance, de l'exploitant et du participant).

Un système de paiement de gros fondé sur un registre totalement décentralisé a, tout compte fait, peu de chances d'offrir les mêmes avantages qu'un système de paiement de gros centralisé. Et cela parce que certaines des composantes des systèmes viables de paiement de gros sont intrinsèquement centralisées : c'est le cas par exemple du mécanisme d'économie des liquidités examiné plus haut. Cette complexification pourrait accentuer le risque opérationnel par rapport à ce que l'on observe dans les systèmes centralisés actuels.

Les avantages d'un système de paiement de gros fondé sur la technologie du grand livre partagé résident selon toute apparence dans les liens qui existent entre ce genre de plateforme et l'écosystème plus large des infrastructures de marchés financiers. Il est possible d'aboutir à de tels avantages en intégrant au grand livre d'autres actifs de paiement : l'intégration des systèmes de post-marché créerait des économies d'échelle et ferait baisser les coûts pour les participants, et cette approche pourrait d'ailleurs grandement simplifier le nantissement ainsi que la cession d'actifs.

Des économies ou des gains d'efficience seraient également possibles au niveau sectoriel si, par exemple, un système de paiement interbancaire de base fondé sur un grand livre partagé servait de soubassement à d'autres systèmes dotés d'un grand livre partagé afin d'améliorer la compensation et le règlement de toute une série d'actifs financiers. Ainsi, les actifs échangés en bourse sont déjà compensés et réglés au sein de systèmes sûrs et efficients. Or, il serait possible d'obtenir des améliorations si ces systèmes pouvaient être intégrés de telle façon que les espèces qui servent de moyen de paiement pour le volet espèces des transactions figureraient dans le même livre. Les marchés de gré à gré (pour actions, obligations ou instruments dérivés), les prêts consortiaux et le crédit commercial fonctionnent de manière beaucoup plus décentralisée dans des systèmes où l'échéance de règlement est longue. Une plateforme fondée sur un grand livre partagé permettrait une sensible amélioration si ces marchés et ces instruments de

crédit étaient intégrés à un système de base de paiement de gros qui assurerait le transfert des paiements en espèces dans de la monnaie de banque centrale.

Les plateformes dotées d'un grand livre partagé peuvent offrir des économies par la baisse des coûts de réconciliation qu'elles permettent. En donnant aux banques la possibilité de valider leurs transactions dès le début, un système fondé sur un grand livre partagé pourrait réduire le travail de réconciliation comptable et offrir des économies importantes pour le secteur financier. Ces économies dépendent de la nature de la technologie du grand livre partagé : un système avec preuve de travail comme Ethereum, par exemple, serait, par comparaison, plus onéreux à faire fonctionner en raison du coût engendré par la méthode de consensus sur le plan de la puissance de calcul.

Le projet Jasper a apporté à toutes les parties des enseignements. Plusieurs pistes de réflexion pourraient être poursuivies. L'une d'entre elles concernerait le remplacement des garanties en espèces déposées auprès de la Banque du Canada par des titres. Une autre piste consisterait à explorer les possibilités d'intégration entre le projet Jasper et d'autres types de grands registres décentralisés, au Canada ou à l'étranger. Cette réflexion pourrait nous aider à cerner les gains d'efficience que seraient susceptibles d'offrir l'amélioration des connexions, l'amélioration de l'automatisation des paiements transfrontières ou l'emploi de dispositifs permettant le règlement de plusieurs actifs (par exemple, obligations ou instruments du marché monétaire) dans le même livre.

Bibliographie

Bech, M. L., et B. Hobijn (2007). « Technology Diffusion Within Central Banking: The Case of Real-Time Gross Settlement », *International Journal of Central Banking*, vol. 3, nº 3, p. 147-181.

Bech, M. L., C. Preisig et K. Soramäki (2008). « Global Trends in Large-Value Payments », *Economic Policy Review*, Banque fédérale de réserve de New York, septembre, p. 59-81.

Buterin, V. (2013). *A Next-Generation Smart Contract and Decentralized Application Platform*, document d'orientation sur la plateforme Ethereum. Internet : https://github.com/ethereum/wiki/wiki/White-Paper.

Comité sur les paiements et les infrastructures de marché (2017). *Distributed Ledger Technology in Payment, Clearing and Settlement: An Analytical Framework*, Banque des Règlements Internationaux, février.

Comité sur les systèmes de paiement et de règlement et Comité technique de l'Organisation internationale des commissions de valeurs (2012). *Principes pour les infrastructures de marchés financiers*, Banque des Règlements Internationaux, 16 avril.

Davey, N., et D. Gray (2014). « How Has the Liquidity Saving Mechanism Reduced Banks' Intraday Liquidity Costs in CHAPS », *Quarterly Bulletin*, Banque d'Angleterre, deuxième trimestre, p. 180-189.

Garratt, R. (2017). *CAD-Coin versus Fedcoin*, rapport du R3, 5 avril.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Internet : https://bitcoin.org/bitcoin.pdf.

Narayanan, A., J. Bonneau, E. Felten, A. Miller et S. Goldfeder (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton (New Jersey), Princeton University Press.

Schindler, J. (à paraître). *FinTech and Financial Innovation: Drivers and Depth*, Conseil des gouverneurs de la Réserve fédérale, Washington.