Les enjeux de la *Blockchain* pour la Banque de France et l'Autorité de Contrôle prudentiel et de Résolution (ACPR)

Par Nathalie BEAUDEMOULIN
Coordinatrice du Pôle FinTech Innovation de l'Autorité de Contrôle prudentiel et de Résolution
Didier WARZÉE
Ingénieur des mines, expert au Pôle FinTech Innovation de l'Autorité de Contrôle prudentiel et de Résolution
et Thierry BEDOIN
Chief Digital Officer de la Banque de France

L'Autorité de Contrôle prudentiel et de Résolution (qui contrôle les banques et les assurances) ainsi que la Banque de France se sont structurées pour répondre aux défis de la révolution technologique à l'œuvre dans les services financiers. La *blockchain* fait partie des sujets technologiques susceptibles d'optimiser, voire de modifier la manière dont les activités financières peuvent être traitées et fournies. Toutefois, cette technologie reste peu mature et devra dépasser quatre grands dilemmes avant de pouvoir être utilisée pour réaliser des opérations financières.

Une *blockchain* ou des *blockchains* ?

Le terme de *blockchain* (ou d'autres termes proches) est parfois utilisé improprement pour désigner des dispositifs informatiques pouvant être en réalité très différents les uns des autres tant dans leur conception qu'au regard des principes qui les sous-tendent. Au-delà des dénominations, le régulateur s'attachera tout d'abord à examiner les caractéristiques essentielles des solutions présentées pour fonder sa position.

Ainsi, historiquement, le terme « *timestamp server* » a été utilisé pour désigner le protocole sous-tendant le bitcoin, avant que n'apparaisse (peu de temps après) le terme de *blockchain*. Du fait du rôle pionnier de la combinaison de diverses solutions technologiques ayant permis de créer le bitcoin, ce terme est maintenant régulièrement utilisé pour des modèles présentant des similarités avec celui-ci, mais aussi, souvent, pour des modèles présentant avec le bitcoin des différences significatives. Dans certains cas, l'acronyme DLT (pour *Distributed Ledger Technology*) est aussi mis en avant de manière à se démarquer (notamment pour des raisons d'image) de la crypto-monnaie bitcoin.

En effet, le bitcoin, qui n'est pas considéré comme une monnaie ayant cours légal, présente des risques intrinsèques forts tant pour les consommateurs – forte volatilité, risque de fraude avéré – qu'au regard des exigences de lutte contre le blanchiment des capitaux et le financement du terrorisme, notamment du fait de l'anonymat des détenteurs qui se heurte au principe fondamental d'identification du client dans le domaine financier. Le bitcoin a donc légitimement fait l'objet de prises de positions vigoureuses des autorités, tant françaises qu'européennes [1], visant à révéler ces risques au public et à les prévenir autant que possible. Dès lors, les promoteurs de solutions technologiques du type *blockchain* cherchent parfois à se prémunir contre l'assimilation de celles-ci au bitcoin.

Pour autant, certains d'entre eux vont en réalité promouvoir une solution entièrement décentralisée, qu'ils présentent, du fait de la disparition espérée d'intermédiaires, voire de l'autorité centrale d'administration, comme un vecteur majeur de transformation des services financiers, voire même de la Société.

(1) Position 2014-P-01 du 29 janvier 2014 de l'ACPR relative aux opérations sur bitcoins en France. Le fonctionnement du bitcoin, ses risques pour les utilisateurs et les enjeux d'un encadrement réglementaire sont aussi détaillés dans le Focus *n°10 du 5 décembre 2013 publié sur le site Internet de la Banque de France, ainsi que dans le communiqué d'alerte émis le 12 décembre 2013 par l'Autorité bancaire européenne (www.eba.europa.eu).*

La technologie se met alors au service d'une philosophie que l'on peut qualifier de libertaire, qui promet le retour (primitif, bien que numérique) à des relations financières directes entre individus s'appuyant sur un mécanisme transactionnel de confiance entièrement décentralisé.

Mais au-delà de ces cas assez utopiques, la technologie *blockchain* présente des caractéristiques suffisamment remarquables pour que les acteurs financiers (qu'ils soient récents ou davantage établis) et les autorités financières (dont la Banque de France et l'Autorité de Contrôle prudentiel et de Résolution) s'y intéressent de très près.

Quel est le potentiel de la *blockchain* publique décentralisée pour le domaine financier ?

Au-delà du bitcoin en tant que monnaie virtuelle, c'est l'ensemble du mécanisme de confiance mis en œuvre par celui-ci qui a soulevé l'enthousiasme et aiguisé la créativité d'acteurs financiers, notamment de nombreuses *start-ups* qui y voient une façon de concurrencer les établissements financiers.

En effet, le – ou les – créateurs du bitcoin ont pensé sa *blockchain* originelle comme un système décentralisé ne faisant appel à aucun tiers de confiance et se fondant sur des techniques cryptographiques pour assurer simultanément la transparence, la sécurité et l'anonymat de transactions numériques directes de pair-à-pair. Ainsi, un registre entièrement transparent de transactions directes de pair-à-pair distribué sur un nombre important de nœuds d'un réseau est, de ce fait, présenté comme indestructible. De plus, son intégrité est garantie par un mécanisme impliquant, à chaque validation d'un nouveau bloc de transactions (sécurisée par le protocole de consensus par « preuve de travail »), l'intégration de l'empreinte numérique de la chaîne de blocs précédente.

Une qualité que souhaitent fréquemment utiliser des porteurs de projet est l'inaltérabilité de la base de données distribuée, avec la confiance qu'elle est censée générer afin de sous-tendre des projets de registres d'informations ou de transactions – *via* l'utilisation de *tokens* – dans le monde réel.

Toutefois, au-delà de ces atouts, des limitations significatives sont rapidement apparues ne serait-ce qu'en matière de volumes de transactions traitables ou de délais nécessaires à ce traitement, qui ont donné naissance à d'autres dispositifs visant à compenser ces lacunes. C'est ainsi que d'autres *blockchains* publiques ont vu le jour, telle la *blockchain* Ethereum, qui intègre des contrats s'exécutant de manière automatisée (les *smart contracts*) dès lors qu'une information externe (appelée oracle) en déclenche la réalisation, le projet de *blockchain* Hyperledger dédiée au *business*, ou encore la *blockchain* Tangle/IOTA spécialisée dans les problématiques d'objets connectés.

Les *smart contracts* permettraient, en interagissant « intelligemment » avec le monde réel, d'envisager des actions plus sophistiquées qu'une simple transaction réalisée en crypto-monnaie (y compris améliorée par la possibilité d'y associer quelques octets de caractères, dans le cas du bitcoin). Ainsi, par exemple, certains modèles assurantiels sont fondés sur ce type de mécanisme, proposant une indemnisation automatique sur le fondement d'un *smart contract* se référant au tableau des arrivées des avions d'un aéroport (assurance retard).

Toutefois, la nature même de la *blockchain* utilisée et de ses caractéristiques fondatrices (le fait d'être à la fois publique et décentralisée) continue de poser des difficultés importantes (voire rédhibitoires) pour une application à grande échelle au domaine financier.

Ces difficultés peuvent être appréhendées sous la forme de quatre dilemmes :

- Premier dilemme : décentralisation *versus* responsabilité. La décentralisation du système de confiance (qui présente des avantages notamment en termes de sécurité du dispositif partagé par un plus grand nombre) ne permet pas d'identifier un acteur juridiquement responsable de sa sécurité, qui rendrait compte aux clients (par exemple en cas de défaillance, pour assurer la continuité du dispositif, le remboursement, etc.) et aux autorités de régulation.
- Deuxième dilemme : liberté *versus* dépendance. La *blockchain* publique s'affiche comme un bien collectif autogéré auquel tout un chacun peut (en principe) contribuer. Or, dans la pratique, elle s'avère très dépendante de quelques codeurs. Elle est aussi très dépendante vis-à-vis de fermes de minage extrêmement concentrées sur le plan géographique et économiquement incitées à se regrouper (jusqu'à un certain point [2]). L'emprise de ces parties prenantes sur le fonctionnement des *blockchains* publiques défie le caractère « démocratique » affiché et elle peut provoquer de vrais schismes dans les communautés, qui se traduisent parfois par des scissions de la *blockchain* elle-même (*hard fork*). Elle pose *in fine* la question de leur gouvernance, car les tiers de confiance auxquels ces *blockchains* sont censées se substituer ne font, dans ces conditions, que se « déplacer » et revenir sous d'autres formes (développeurs, mineurs), d'une manière beaucoup moins transparente, et en ayant des objectifs souvent divergents.
- Troisième dilemme : transparence *versus* confidentialité. La *blockchain* publique est transparente et efficace en termes de traçabilité des opérations. En effet, elle permet de connaître l'ensemble des transactions ou des enregistrements réalisés, à la manière d'une piste d'audit présentée comme unique et intangible. Néanmoins, cette caractéristique se heurte assez rapidement au principe du secret des affaires, chaque établissement participant ne souhaitant pas exposer (notamment à la concurrence) les transactions qu'il réaliserait en l'utilisant.
- Quatrième dilemme : anonymat *versus* identification. Le

(2) Il faut qu'elles restent en deçà de 50 % de la capacité de traitement en termes de puissance de calcul mise en œuvre, sinon elles mettent en danger l'efficacité du protocole de « preuve de travail », et donc la confiance dans le bitcoin – confiance dont elles tirent leur richesse (étant donné qu'elles sont rémunérées… en bitcoins).

principe libertaire qui sous-tend la *blockchain* implique l'usage de pseudonymes, ce qui ne permet pas l'identification des acteurs. Cette opacité n'est pas acceptable au regard des objectifs de la lutte contre le blanchiment des capitaux et le financement du terrorisme.

En raison de ces limitations, l'usage des *blockchains* publiques pour des activités régulées n'apparaît pas approprié à ce stade – sauf à concevoir une *blockchain* publique nativement construite pour répondre aux problématiques du secteur financier, incluant les enjeux de supervision.

Conséquence : on envisage de réintégrer une autorité centrale dans des protocoles de registres distribués

Les acteurs financiers ont donc cherché à recréer des systèmes inspirés des *blockchains* publiques, à ceci près qu'ils en resteraient l'autorité centralisatrice tiers de confiance, permettant ainsi de résoudre certains des problèmes susmentionnés – tout en conservant dans le système ainsi créé une position privilégiée s'inscrivant dans la continuité de leurs fonctions actuelles.

Le cas le plus orthogonal aux *blockchains* publiques est celui de registres distribués entièrement privés. Dans la pratique, ils correspondent plutôt à des bases de données de transactions répliquées sur plusieurs sites physiques et bénéficiant des mécanismes cryptographiques assurant leur intégrité, sans toutefois se fonder sur des mécanismes de minage. Ceux-ci sont en effet rendus superflus par une confiance *a priori* forte entre des nœuds exhaustivement contrôlés par le même acteur.

Ces *blockchains* privées sont notamment utilisables pour optimiser des procédures internes, au sein de groupes. Elles peuvent ainsi permettre de disposer d'un outil d'enregistrement immédiat et partagé d'informations et de transactions entre différentes sociétés d'un même groupe, ou entre différentes unités d'une même entreprise. Le rôle du superviseur consistera alors à surveiller les risques opérationnels (dont les problèmes de cybersécurité, les risques liés à l'utilisation éventuelle du *cloud*, etc.) que ces solutions font éventuellement courir aux établissements financiers, et ce de la même manière que pour toute autre utilisation de nouvelles technologies de gestion de l'information, sans que cela ne soit uniquement et spécifiquement lié au recours à la *blockchain*.

Les limitations en matière de cas d'usage de ces *blockchains* privées (notamment pour ce qui concernerait des activités BtoC) ont conduit au développement de modèles impliquant une architecture proche de celle des *blockchains* publiques, mais avec des mécanismes conférant à un tiers central la gestion de la gouvernance, du code et des accès au dispositif : elles sont fréquemment appelées « *blockchains* publiques permissionnées ».

L'expression de « *blockchain* publique permissionnée » est toutefois susceptible de recouvrir des systèmes assez différents ; de celui qui n'autorisera que quelques acteurs dans le réseau pair-à-pair en organisant une gouvernance spécifique du code utilisé – système en général dit des *blockchains* de consortium quand ces acteurs sont des sociétés –, à un système d'accès en théorie ouvert utilisant un protocole de consensus calqué sur le mécanisme public, mais intégrant un acteur centralisant les droits d'accès et certaines informations concernant les utilisateurs.

Au regard des cas d'usage, et notamment de la « confiance *a priori* » entre les pairs du réseau, le protocole de consensus sera souvent différent de la « preuve de travail » du bitcoin, ce qui améliorera substantiellement la rentabilité du système (le coût énergétique du « minage » du bitcoin étant en effet très important).

Il y a aussi des projets de systèmes permissionnés qui cherchent à retrouver des propriétés de résilience du registre (intégrité et disponibilité) proches de celles des *blockchains* publiques. Or, ces propriétés sont générées par la taille des réseaux (plus celle-ci est importante et plus il existe de copies du registre) et par l'énergie dépensée par les mineurs pour la validation des blocs, dans le cas du consensus « preuve de travail » : plus celle-ci est importante, plus un éventuel attaquant devra lui-même dépenser d'énergie pour corrompre le système. Une solution envisagée, dite *sidechain*, consiste à ce qu'une *blockchain* publique permissionnée se branche (en quelque sorte) sur une *blockchain* publique non permissionnée afin de pouvoir être sécurisée.

La plupart des cas d'usage envisagés aujourd'hui, que ce soit dans le cadre des ouvertures réglementaires françaises (enregistrement et transactions sur les titres non cotés [3]) ou dans celui d'autres projets liés à la gestion d'actifs, aux paiements, aux transferts de fonds ou à l'assurance, le sont au travers d'un modèle *blockchain* publique permissionnée.

Au vu des différences significatives dans ce que ces modèles recouvrent en réalité, il faudra examiner au cas par cas les projets proposés afin de déterminer de quelle façon ils répondent aux exigences réglementaires.

De manière générale, les dispositifs proposés doivent d'ores et déjà se conformer aux exigences fondamentales que sont la sécurité des transactions, la protection du consommateur et la lutte contre le blanchiment des capitaux et contre le financement du terrorisme. Ainsi, les clients devront toujours être identifiés de manière fiable et documentée (au moyen de mesures d'identification renforcées si l'entrée en relation ne s'effectue pas en face-à-face). Les paiements qui transiteraient par un tel dispositif devront toujours être entourés des mesures de sécurité requises (par exemple, l'authentification renforcée). Les dispositifs doivent aussi respecter les exigences

(3) L'article 120 de la loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique habilite le gouvernement, d'ici le 9 décembre 2017, à réformer le droit applicable aux titres financiers afin de permettre la représentation et la transmission (au moyen d'un dispositif d'enregistrement électronique partagé) des titres financiers qui ne sont ni admis aux opérations d'un dépositaire central ni livrés dans un système de règlement et de livraison de certains instruments financiers.

Photo © Romain Gaillard/REA

La *Fintech Revolution*, événement organisé par France Fintech, le 28 mars 2017 (seconde édition), au théâtre de La Gaîté Lyrique.

« L'Autorité de Contrôle prudentiel et de Résolution s'est dotée en juin 2016 d'un pôle dédié aux *FinTechs* et à l'innovation. »

réglementaires spécifiques applicables aux cas d'usage (comme, les informations précontractuelles, dans le cadre de souscriptions de contrats).

Les établissements doivent en outre tenir compte des réglementations trans-sectorielles susceptibles de s'appliquer, telles les nouvelles règles européennes liées à la protection des données personnelles [4] (dont le recueil du consentement du client avant tout traitement, le droit à l'oubli – qui apparaîtrait difficile à respecter si la *blockchain* restait immuable – ou encore les dispositions européennes liées à l'utilisation de la signature électronique [5]).

Une question attentivement suivie par le Pôle FinTech Innovation de l'ACPR et par la Banque de France

Afin d'être en phase avec la révolution numérique actuellement à l'œuvre dans les services financiers (dont la *blockchain* est l'une des manifestations) et de préparer la supervision d'une finance toujours plus digitale, l'Autorité de Contrôle prudentiel et de Résolution s'est dotée en juin 2016 d'un pôle dédié aux FinTech et à l'innovation.

Ce pôle travaille étroitement avec l'Autorité des Marchés Financiers, avec laquelle l'ACPR anime un Forum FinTech, qui réunit des FinTech, des banques et des assurances, ainsi que d'autres partenaires de l'écosystème de l'innovation financière, et les pouvoirs publics. Les sujets abordés portent sur la régulation de l'innovation et sur les problématiques réglementaires liées à la *blockchain*, telle que (par exemple) la valeur juridique des opérations enregistrées sous une *blockchain* ou encore les *smart contracts*.

En tant qu'autorité indépendante adossée à la Banque de France, l'ACPR entretient un dialogue constant avec les experts de la Banque centrale sur les enjeux liés à la *blockchain*. En effet, ayant rapidement perçu les enjeux de cette nouvelle technologie pour certaines de ses missions (systèmes de paiement et infrastructure de marchés, politique monétaire, services bancaires), la Banque de France a décidé de tester la *blockchain* afin d'être en mesure de juger par elle-même des potentialités de cette technologie.

Ainsi, la Banque de France conduit actuellement, sous l'égide de son *Chief Digital Officer,* plusieurs expérimen-

(4) Règlement (UE) 2016/679 du 27 avril 2016 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
(5) Règlement (UE) 910/2014 du 23 juillet 2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS ».

tations de la technologie *blockchain*, dont l'une, menée avec des banques de la place, vise à maintenir de manière décentralisée un registre d'identifiants ICS (identifiant créancier SEPA remplaçant le TIP depuis le 1er août 2014) utilisés dans les prélèvements SEPA (projet MADRE). Si les banques françaises s'échangent actuellement l'identité de leurs clients créanciers (ICS) grâce à l'intervention opérationnelle de la Banque de France qui centralise les demandes, génère et dissémine l'ensemble de ces identifiants, l'utilisation de la *blockchain* permet la tenue de ce registre dans les *smart contracts* d'une *blockchain* à laquelle les banques participent directement. La Banque de France réussit ainsi à exercer son rôle d'opérateur du service ICS au travers de traitements automatiques qui s'exécutent selon des règles prédéfinies qu'elle a déployées dans la *blockchain*. Dans la gouvernance du dispositif, elle conserve uniquement un rôle d'accréditation initiale des banques participantes, tout en renforçant sa qualité de tiers de confiance.

Cette expérimentation a confirmé une capacité de la technologie *blockchain* à relever des défis réels, notamment en matière de tenue de registre. Son extension à une *blockchain* interbancaire multiservices et son utilisation éventuelle dans des traitements critiques du monde de la finance dépendront néanmoins d'avancées restant à démontrer sur les aspects liés à la capacité de traitement de masse (*scalabilité*), à la confidentialité des transactions, à la sécurisation et, surtout, à la mise en place de dispositifs de gouvernance assurant son bon fonctionnement dans la durée.

Conclusion

Si certaines caractéristiques de la technologie sous-jacente à la *blockchain* peuvent être prometteuses, son application à des activités impliquant le traitement de flux financiers importants exigera que l'on ait au préalable relevé des défis notables dans les domaines technique et réglementaire.