# *Blockchain* et DLT
## dans le système bancaire

Imad CHEHADE*

La technologie de la chaîne de blocs (*blockchain*) bouscule depuis quelques années les principes de la finance et ses cadres établis et de l'économie en général. La *blockchain* est une solution décentralisée, transparente et sécurisée permettant à des personnes qui ne se connaissent pas et qui ne se font pas mutuellement confiance de stocker, d'échanger, d'authentifier et de vérifier des transactions à coût réduit et sans tiers de confiance. Dans sa version la plus aboutie, cette technologie assure ainsi certaines fonctions d'intermédiation financière typiquement dévolues au système bancaire.



La *blockchain* pionnière est celle du Bitcoin (système de paiement électronique de pair-à-pair). Elle est apparue en 2009 avec la mise en service d'une monnaie numérique (bitcoin)[1]. Depuis lors, les expérimentations autour des *blockchains* se sont rapidement développées en faisant émerger des technologies aux architectures très différenciées, en termes d'usage et d'implications. Les réseaux *blockchains* diffèrent notamment par leur degré de permissions (publiques, privées et de consortium)[2], tout comme les technologies du registre distribué (*distributed ledger technologies*, DLT), qui sont parfois assimilées à tort à la *blockchain*. Les DLT et les *blockchains* ont le même socle : un registre répliqué entre participants rendant compte en quasi-temps réel d'un

* Doctorant, Laboratoire d'économie Rouen Normandie (LERN), Université de Rouen Normandie. Contact : imad.chehade@univ-rouen.fr.

L'auteur remercie Nicolas Abad, Marie-Laure Cabon-Dhersin et Vincent Iehlé pour leurs commentaires et leurs suggestions.
Ce travail a bénéficié du soutien financier de l'Université de Rouen Normandie dans le cadre du Projet BQRE : « Financement et paiement sous blockchain (2019-2021) ».

ensemble de transactions. Par contre, des différences apparaissent dans la manière dont ces transactions sont validées et par qui elles le sont, la *blockchain* étant la version la plus décentralisée.

La *blockchain* offre potentiellement de nombreuses opportunités au secteur bancaire. Elles concernent la suppression de certains intermédiaires financiers (chambres de compensation ou courtiers) et de leurs coûts, la réduction des coûts d'infrastructure, la réduction des risques d'erreur, l'augmentation de la vitesse d'exécution et de vérification des opérations. La *blockchain* permet aussi aux banques de sécuriser leurs transactions de manière cryptographique et non plus par le biais d'un tiers de confiance, générant ainsi des économies dans la gestion de leurs bases de données. Ces opportunités motivent l'intérêt du secteur bancaire pour les technologies *blockchain*. Dans le même temps, elles posent aussi de nombreux défis ou obstacles à relever pour ce secteur fortement régulé, qu'ils soient d'ordre monétaire, financier, sécuritaire, économique, technique ou juridique. C'est la raison pour laquelle on observe en pratique des choix de technologies orientés vers des DLT qui ne sont pas pour autant des *blockchains*.

L'objet principal de cet article est de déterminer dans quelle mesure les DLT permettent un dépassement des services bancaires traditionnels centralisés. Pour cerner correctement les enjeux associés à cette nouvelle technologie, il faut avant tout en définir les contours et en comprendre le mode de fonctionnement. Dans cet article, nous visons à préciser la forme et le type de technologie la plus adaptée pour le système bancaire.



Nous montrons en particulier en quoi la *blockchain* est une DLT par défaut et en quoi les DLT ne sont pas toutes des *blockchains*. Cette distinction a des implications importantes pour l'utilisation de ces technologies par le système bancaire. Cela nous permet notamment de justifier pourquoi la *blockchain* publique et les crypto-monnaies sont exclues par les banques centrales. Nous montrons aussi que l'usage qui est fait de la *blockchain* bancaire privée n'apporte pas vraiment de changement de paradigme en termes de système d'intermédiation et se résume plutôt à une gestion centralisée et une gouvernance optimisée. Ensuite, nous mettons en lumière les apports des registres avec permission au système bancaire (DLT privée ou de consortium). Les expérimentations effectuées par les consortiums des grandes banques nous aident par ailleurs à mieux comprendre leurs usages. Il ressort que le modèle de DLT de consortium est ainsi vraisemblablement le plus prometteur et celui qui devrait prédominer en pratique dans le système bancaire à l'avenir.

En ce qui concerne le lien entre la *blockchain* et la sphère financière, les contributions académiques se positionnent plutôt sur des aspects

techniques, économiques et de gouvernance qui sont porteurs de freins pour la mise en place de *blockchains* dans le système bancaire. Böheme *et al*. (2015) ainsi que Waelbroeck (2017) considèrent l'exemple du Bitcoin pour illustrer ce propos. Collomb et Sok (2016) considèrent, eux, l'impossibilité de contractualiser l'imprévu et de supprimer les coûts de transactions dans une telle architecture. Guégan (2017b) évalue l'impossibilité de gérer les *bugs* de code inhérents aux *smart contracts* de la *blockchain* Ethereum, tandis que Catalini et Gans (2017) mentionnent l'impossibilité d'identifier les coûts clés affectés par la *blockchain*. Comme le rappelle Wright et de Filippi (2015), la *blockchain* avec permission permet la création de nouveaux systèmes de gouvernance rendant la prise de décision plus participative. Des travaux récents permettent aussi d'observer ce qui est mis en place en pratique depuis quelques années. Verdier (2017) met ainsi en évidence un recours plus courant aux *blockchains* privées au sein des institutions financières. Halaburda (2018) souligne que les contrats intelligents peuvent se mettre en place sans avoir recours à la *blockchain* (par exemple, le projet *Madre* de la Banque de France, BdF). Cette transition technologique (vers des DLT) est supposée améliorer la rentabilité conjointement à une activité plus sécurisée, plus confidentielle et plus contrôlée. Notre contribution s'inscrit plus particulièrement dans la continuité de l'analyse proposée par Verdier (2017) qui identifie déjà les limites de la *blockchain* à l'intérieur de ce marché bancaire très contrôlé. Nous proposons ici de franchir une étape supplémentaire en analysant l'intégration des DLT avec permission dans l'industrie bancaire.



L'article est organisé comme suit : dans la partie 1, nous précisons les points de différence entre *blockchain* et DLT ; dans la partie 2, nous étudions les limites des *blockchains* publiques et les apports des *blockchains* privées ; dans la partie 3, nous nous appuyons sur les perspectives bancaires pour déterminer quel modèle de DLT est le plus approprié pour l'industrie financière ; dans la partie 4, nous comparons trois types d'architectures de DLT utilisés en pratique ; nous concluons dans la partie 5.

## *LES DIFFÉRENCES ENTRE LES DLT*

La crypto-monnaie bitcoin a éveillé l'intérêt des banques pour les registres *blockchain*, puis pour les registres DLT au sens large. La différence entre les deux concepts est importante ; pourtant ces deux termes sont souvent utilisés indistinctement. L'écart entre la littérature académique sur les DLT et son usage à la carte par les banques nous incite à donner un sens précis à ces termes.

En premier lieu, il existe quatre sous-catégories de DLT : *blockchain*, DAG, *hashgraph* et *holochain*. La *blockchain* est une DLT par défaut, mais les DLT ne sont pas toutes des *blockchains*[3]. Comme l'a souligné la Banque des règlements internationaux (BRI, 2017), chaque DLT est une technologie concurrente de la *blockchain* et est spécifiée par des caractéristiques (formes, permissions, structure des données, processus de validation, consensus). Ces caractéristiques sont celles qui déterminent les usages des DLT.

En second lieu, la *blockchain* se différencie des autres DLT non seulement par ses caractéristiques conceptuelles, mais aussi par ses propriétés économiques et ses conditions d'utilisation. Comme souligné par Guégan (2017a), il est donc indispensable de maîtriser l'ensemble des vrais concepts avant de les utiliser.

### *Les différences de forme*

La technologie de la *blockchain* est l'infrastructure sous-jacente des crypto-monnaies (bitcoin à l'origine). La *blockchain* et les crypto-monnaies sont *de facto* indissociables même s'il existe des exceptions. De ce point de vue, les *blockchains* sont des registres de transactions distribuées de pair-à-pair, placés sur des blocs horodatés. Ils sont ensuite conservés chronologiquement dans une chaîne traçable rendant leur stockage infalsifiable au moment où un consensus est atteint entre des participants non identifiables. En somme, la *blockchain* est une combinaison de trois concepts : réseau distribué de pair-à-pair, cryptographie asymétrique, consensus décentralisé.



Par contre, les DLT ne sont pas basés sur des architectures de *blockchain*. Dans les DLT, il n'y a ni blocs, ni crypto-monnaies, ni mineurs (nœuds de validation), ni compensation. La DLT est une base de données distribuée, administrée par plusieurs participants dont chacun enregistre les données sur son propre registre auquel il a accès et ajoute des transactions au registre distribué. Les copies des registres distribués sont structurées en chaîne de transactions de façon que chaque modification soit répartie instantanément sur toutes les copies.

### *Les différences de permissions*

Les *blockchains* et plus généralement les DLT peuvent être avec ou sans permission. *A priori*, tous les registres publics (*blockchain*/DLT) sont sans permission. Les registres sans permission (*unpermissioned ledgers*) s'adressent davantage au public au sens où tout agent remplissant les conditions requises par la communauté du réseau peut devenir un mineur et participer à la validation des transactions et à leur ajout sur la chaîne.

En revanche, les registres privés et de consortiums nécessitent des permissions que ce soit en mode de lecture/écriture des données ou de vérification des transactions. Ces registres avec permission (*permissioned ledgers*) s'adressent aux entreprises auxquelles l'accès doit être accordé par un ou quelques opérateurs pour que le participant devienne un nœud de validation.

*Quelles implications de permissions sur le consensus ?*

La mise en place d'un registre sans permission (*blockchain Bitcoin*, *Ethereum*) nécessite l'utilisation d'un mécanisme de consensus qu'on appelle preuve de travail (*proof-of-work*, PoW). Cette preuve permet, à chaque fois, aux mineurs de valider les transactions monétaires et de créer de nouveaux blocs. La preuve de travail est un principe de crypto-économie qui définit les mécanismes d'incitation offerts aux mineurs et décourage la création de fausses identités. Une autre manière de procéder consiste à utiliser la preuve d'enjeu (*proof-of-stake*, PoS). C'est un consensus qui donne à chaque mineur un poids dans le vote de consensus et permet de créer des applications décentralisées (Buterin, 2014). Dans le cadre des consortiums, le consensus est défini par une majorité acquise des participants qui vérifient eux-mêmes la validité des transactions.



## *Propriétés économiques*

Les différences de conceptions entre *blockchain* (publique par défaut) et DLT (privée et consortium) ont des implications importantes sur le niveau de sécurité et sur les propriétés économiques de ces technologies.

En pratique et contrairement à la *blockchain* (*trustless system*), les DLT ont été initialement conçues pour procéder à des transactions dans un contexte de confiance. Comme le rappelle Halaburda (2018), la création de la confiance dans ces réseaux fermés est liée à un tiers de confiance (une institution ou un groupe d'entreprises) chargé de certifier, pour les participants potentiels, l'existence d'un actif sous-jacent et de l'attribuer à un processeur initial. En fait, la DLT n'utilise pas forcément la cryptographie asymétrique (une clé publique et une clé privée permettant de crypter et décrypter les messages transférés), ni des algorithmes sophistiqués pour sécuriser le réseau, mais elle compte plutôt sur le cryptage classique. Contrairement à la *blockchain*, les DLT ne s'appuient sur aucune crypto-monnaie.

En ce qui concerne la *blockchain* publique (*Bitcoin*, *Ethereum*, etc.), la confiance des participants est immédiatement liée aux algorithmes et au protocole de consensus (PoW, PoS) qui décrit les modalités de concurrence entre mineurs au sein d'un réseau décentralisé (Rodriguez, 2017 ; Verdier, 2017). On n'a pas besoin de tiers de confiance pour

stocker les informations relatives aux crypto-monnaies sur les *blockchains* publiques du fait qu'elles sont automatiquement transférées dans celles-ci (Halaburda, 2018).

La sécurité des transactions est une conséquence de l'emploi de cryptographie asymétrique qui permet de protéger et d'authentifier les informations quel que soit l'emplacement physique du serveur qui les contient (Guégan, 2017a ; Halaburda, 2018). Aussi, la crypto-monnaie sous-jacente d'une *blockchain* publique permet de faire fonctionner la plateforme en créant une incitation financière à la participation et à la sécurisation du réseau. Par ailleurs, la sécurité de la *blockchain* publique est renforcée par l'augmentation des pouvoirs de mineurs sur le réseau en termes de puissance de calcul. Cela a pour effet de rendre les attaques (changer l'historique des blocs de transactions en même temps) par des pirates isolés ou par une coalition de mineurs très improbables (Waelbroeck, 2017 ; Sayeed et Marco-Gisbert, 2019). Haeringer et Halaburda (2018) montrent que la falsification de Bitcoin est non seulement extrêmement difficile, mais aussi très coûteuse car il s'agit de reconstruire une chaîne biaisée plus longue que la chaîne principale dans la mesure où les autres mineurs continueront leur exploitation.



### *Les différences d'utilisation*

Les DLT sont ciblées plutôt vers des réseaux BtoB (*business to business*). Ces réseaux se construisent généralement sous la forme de consortiums d'entreprises. L'incitation des participants des DLT avec permission vient de l'automatisation d'une activité ayant des effets économiques d'efficience sur un cas d'usage particulier. Tel est le cas du projet bancaire (Clipeum) qui consiste à créer en 2020 une plateforme KYC (*know your customer*) basée sur une DLT avec permission. Les douze banques participantes dont Unicrédit, Crédit Agricole et La Banque Postale peuvent partager en temps quasi réel des informations sur leurs clients afin de mutualiser certains aspects du KYC. Cela permet de lutter contre le blanchiment d'argent et le financement du terrorisme. Dans ce cas, il y a incontestablement moins de papier, moins de coût (pour la collecte d'informations et de documents du KYC) et des gains de temps. Les propriétés économiques des DLT avec permission sont considérées comme conservatrices (autorité régulatrice, identification obligatoire, autorisation demandée, données confidentielles). La quatrième partie montre des études de cas plus détaillées.

La *blockchain* est un nouveau système transactionnel orienté vers des réseaux BtoC (*business to customer*). Elle sert à remplacer la gouvernance institutionnelle par un algorithme incitant des agents à devenir mineurs pour valider des transactions contre des rémunérations cryptos. Entre

autres, des couches supplémentaires innovantes sont ajoutées à la *blockchain* publique afin de supporter son futur développement. Tel est le cas de l'archivage de la propriété via des crypto-monnaies avec des attributs spéciaux (*colored coins*) ou via des chaînes alternatives (*alt-chains*), de la programmation de contrats auto-exécutifs (*smart contracts*) et aussi de financement des projets via des levées de fonds (*initial coin offering*, ICO) à la suite de la mise en réseau des titres de participation qui correspondent à des cybermonnaies ou à des droits de vote matérialisés par des jetons numériques (*tokens*). Ces propriétés économiques découlant du projet libertaire de *blockchain* publique visent à rendre la sphère financière plus liquide, transparente et décentralisée (Waelbroeck, 2017).

## *BLOCKCHAINS : QUELS OBSTACLES POUR LES BANQUES ?*

Comme nous l'avons vu précédemment dans la première partie, la *blockchain* va bien au-delà de son utilisation comme une simple DLT. Dans le même temps, les apports fonctionnels des *blockchains* créent des contraintes difficilement supportables pour l'infrastructure du marché bancaire à l'heure actuelle.



### *L'infrastructure bancaire et l'impossible mise en place des blockchains publiques*

Comme cela est soutenu par Iansiti et Lakhani (2017), la *blockchain* publique reste une technologie prématurée que l'on ne peut pas appliquer directement dans la sphère financière. Cette technologie très disruptive pour l'organisation actuelle présente en effet des défis variés qu'ils soient monétaires, financiers, sécuritaires, économiques, gouvernementaux, techniques, environnementaux et juridiques.

#### *Défis monétaires*

Les crypto-monnaies sont fortement critiquées par la BdF. Elle les considère comme des crypto-actifs qui ne remplissent pas les fonctions dévolues à la monnaie ayant cours légal[4]. Sur le plan monétaire, les cours des crypto-monnaies sont d'abord très volatils, ce qui ne permet pas d'en faire des moyens de paiement[5]. Ensuite, les plateformes dédiées ne proposent aucune garantie de remboursement en cas de piratage des portefeuilles électroniques stockés sur ces plateformes[6]. Dans ce cas, la détention de crypto-monnaies est exposée à des cyber-risques majeurs (BdF, 2018). Enfin, ils ne reposent sur aucun sous-jacent réel stable (l'or ou le dollar par exemple), ce qui en fait des actifs spéculatifs.

*Défis financiers et sécuritaires*

Les crypto-monnaies sont classées comme des vecteurs de risque majeurs (BdF, 2018). Cela signifie que le cœur de la *blockchain* publique basée sur l'émission de crypto-monnaies met en péril le marché financier pour deux raisons principales. En premier lieu, la possession de crypto-monnaies expose les investisseurs à des risques de perte financière en cas de piratage ou de défaillances. En second lieu, la propriété anonyme des crypto-monnaies (au niveau d'émission, de stockage et de transfert) crée une large faille de sécurité car elle augmente le risque de blanchiment des capitaux, le financement du terrorisme et les activités illicites (armes, drogue, évasion fiscale, etc.). Afin de prévenir un risque d'instabilité financière et sécuritaire, plusieurs banques centrales, y compris la BdF, ont alerté les banques commerciales sur les risques associés aux dépôts, aux prêts ainsi qu'à la commercialisation des produits financiers (titres, contrats) en crypto-monnaies. Les banques commerciales ont néanmoins commencé à développer des outils alternatifs aux crypto-monnaies pour définir, par exemple, des monnaies électroniques stables[7].

*Défis économiques et de gouvernance*



L'Autorité de contrôle prudentiel et de résolution (ACPR) considère que les concepts libertariens associés à la *blockchain* (décentralisation, liberté d'accès, transparence, anonymat) posent des défis économiques à l'infrastructure bancaire (Beaudemoulin *et al.*, 2017). Selon Catalini et Gans (2017), les aspects de la *blockchain* publique s'opposent frontalement au cœur de la finance intermédiée centralisée qui est fondée sur la responsabilité des acteurs, l'indépendance des fonctions, la confidentialité des activités et la reconnaissance juridique des opérations. Yermack (2017) montre que les propriétés de la *blockchain* publique changent en profondeur le pouvoir relatif des parties prenantes qui interagissent dans la gouvernance d'entreprise. L'ouverture conceptuelle du réseau bancaire à de nouveaux entrants pour procéder à la validation des transactions s'oppose au principe du secret bancaire et menace la confidentialité des données financières.

*Défis techniques et externalités environnementales*

En contradiction avec la perspective du comité technique ISO/TC 307, considérant le Bitcoin comme un système de paiement électronique parfaitement anonyme, les programmeurs ont montré qu'une analyse minutieuse des références croisées avec d'autres informations stockées sur le réseau pourrait permettre d'identifier certains utilisateurs (Gramoli et Staples, 2018). En plus, les mineurs peuvent détecter, à partir d'une

adresse IP originelle, des informations privées sur leurs utilisateurs (par exemple, l'emplacement géographique). Ces effets mettent en cause la garantie absolue de l'anonymat (Reid et Harrigan, 2013) et viennent contredire le fait que les utilisateurs sont exclusivement identifiés par leurs pseudonymes.

Selon Pavel (2017), les protocoles de consensus (surtout Bitcoin) souffrent actuellement du problème de scalabilité (passage à grande échelle) et d'un temps long de latence (temps de propagation d'un bloc des transactions à l'ensemble du réseau) par rapport aux systèmes de paiement mondiaux déployés par carte comme PayPal, Visa ou MasterCard.

En outre, la consommation d'électricité annuelle des *blockchains* publiques résultante des opérations du minage des crypto-monnaies (selon le calcul minimal) s'élève à 46,5 TWh/an[8]. Cette consommation énergétique (sept fois plus élevée que la production moyenne d'un réacteur nucléaire) a un impact très préjudiciable sur l'environnement. Cet impact devient de plus en plus significatif avec l'augmentation du nombre de mineurs sur le réseau.

*Défis juridiques*



La réalisation de transactions sous une couverture anonyme, la possibilité d'insertion de données illégales et l'exercice d'activités frauduleuses ou criminelles incitent la BdF et l'ACPR à imposer un statut de prestataires de services en crypto-monnaies aux plateformes convertissant des bitcoins en monnaie légale[9]. D'ailleurs, la CNIL (Commission nationale de l'informatique et des libertés) a mentionné dans ses premières analyses que la *blockchain* publique est non compatible avec le RGPD (voir le rapport de la CNIL, 2018)[10, 11]. En amont, selon de Filippi et Reymond (2016), la CNIL insiste aussi sur différentes exigences de conformité comme l'identification d'un responsable du traitement, le droit à la rectification, le droit à l'oubli ou à l'effacement des données. Notons que ces aspects sont par nature en contradiction frontale avec la *blockchain* publique. Enfin, il paraît difficile d'appliquer sur un protocole décentralisé et fonctionnant sous pseudonyme des codes juridiques taillés pour des institutions centralisées (Bonneau et Renard, 2017).

**Remarque 1.** On peut noter que les DLT publiques, à savoir des registres distribués sécurisés à travers un système d'incitations économiques, génèrent les mêmes types d'obstacles pour les banques.

### *Quelle blockchain privée pour les banques en pratique ?*

Les obstacles créés par les *blockchains* publiques incitent les banques à repenser la réalisation des transactions sur des *blockchains* privées.

En opposition aux *blockchains* publiques inhérentes aux crypto-monnaies, la technologie dite de *blockchain* privée utilisée par les banques peut fonctionner sans crypto-monnaie. Elle est maintenue sous le contrôle d'une autorité centralisatrice décidant les conditions d'accès au réseau, la validation des transactions émises par les participants. Les projets expérimentés par les banques ne respectent pas les piliers architecturaux de la *blockchain* comme le bloc (date, heure, identifiant, hachage, fonction de hachage, nonce), la signature cryptographique et d'autres paramètres décentralisés (Zheng *et al.*, 2017). L'identification de ces variables permet d'afficher les différentes options architecturales de la *blockchain*. En effet, comme l'ont souligné Collomb et Sok (2016), il est incohérent d'avoir une plateforme centralisée appelée *blockchain* étant donné que la *blockchain* est une technologie originellement décentralisée.

L'idée de mettre en place des registres internes ou partagés entre une banque et ses entités semble économiquement très avantageuse en termes de gain de temps, de réduction de coûts et d'efficacité du système (limitation du nombre des intermédiaires et fluidité de la circulation d'informations). Pour toutes ces raisons, l'application de la *blockchain* privée par les banques relève plutôt d'une sorte d'optimisation des processus internes.



Actuellement, la *blockchain* privée des banques se résume plutôt à des bases de données partagées et des contrats intelligents personnalisés. On observe ainsi une digitalisation de mécanismes qui s'associent à une technologie alternative à la *blockchain* Bitcoin (Guégan, 2018). Tout cela peut se résumer à un registre distribué privé régi par des modes de gestion centralisée.

#### *Quelle est la vraie blockchain privée ?*

La vraie *blockchain* privée est celle qui est distribuée sur le plan architectural et fonctionnant sans tierce partie sur le plan transactionnel. L'aspect privé de la *blockchain* signifie seulement que le degré d'ouverture du réseau est restreint à des acteurs accrédités pour participer aux processus de gestion, de partage, de validation des transactions et d'addition des blocs à la chaîne suivant des protocoles de consensus définis par l'opérateur du réseau. La vraie *blockchain* privée nécessite une crypto-monnaie stable garantie par une réserve d'actifs réels, un réseau de pair-à-pair, un écosystème horizontalisé, une gestion partagée et une gouvernance décentralisée (collégiale) où la décision

doit être prise par tous les acteurs. Cela permet d'avoir une infrastructure financière (désignée par une plateforme des contrats intelligents) durable, interopérable et fiable ainsi qu'un protocole évolutif, résilient, sécurisé et transparent[12].

## *PERSPECTIVES BANCAIRES AUTOUR DES DLT AVEC PERMISSION*

Le secteur bancaire a besoin de technologies avec permission qui sont principalement de deux types dans le cas des DLT : privée ou de consortium. Ces deux modalités sont privilégiées par le secteur bancaire comme nous le verrons à travers de nombreux exemples. Dans le cas privé où le contrôle des transactions est assuré par un seul opérateur, le champ d'action est nécessairement réduit. Dans le cas d'un consortium qui met en relation plusieurs acteurs pour la validation des transactions, toute la difficulté consiste à trouver le bon équilibre entre une gouvernance fiable et l'intégration de nouveaux participants.

### *L'adoption de la DLT privée par les banques*

De nombreuses DLT bancaires ont été mises en place pour des cas d'usages variés avec des objectifs différents, créant ainsi une galaxie de registres avec permission. En Europe, ce mouvement est encouragé par la Commission européenne qui a créé, en février 2018, l'Observatoire-Forum des DLT afin d'accroître la place de l'Europe dans l'expérimentation des projets surtout en matière de technologie financière[13].



À titre d'exemple, BBVA et Indra développent la première DLT privée pour l'octroi de prêts aux entreprises, depuis la négociation de l'accord jusqu'à sa signature. De même, BNP Paribas lance en partenariat avec la startup Pikciochain, une DLT privée dédiée à l'enregistrement et à la sécurisation des données personnelles des clients dans une logique de KYC. L'objectif est de fournir des informations en temps réel sur les clients, ce qui leur permet en retour de surmonter la lenteur habituelle du processus KYC. La Société Générale a procédé avec Forge à l'émission de la première obligation sécurisée de financement d'habitat (OFH) sous forme de *security tokens* directement enregistrés sur la *blockchain* Ethereum. Les avantages de ce projet sont d'augmenter la transparence, la vitesse et l'efficacité de transfert et de règlement des titres, de diminuer les coûts et de s'affranchir de certains intermédiaires ainsi que de proposer un circuit automatisé d'émission et de négociation sur le marché secondaire. On trouve aussi des projets de DLT qui traitent de la gestion clientèle. Tel est le cas du projet du groupe bancaire Crédit Mutuel Arkéa qui collabore avec IBM pour mettre en place un mécanisme permettant via la DLT de partager en quasi temps réel des identifiants clients avec l'ensemble des filiales du

groupe. Il existe d'autres projets qui concernent les transferts d'argent et les opérations de change, à l'instar de celui testé par le Crédit Agricole qui adopte en interne certains apports de la DLT Ripple dans le cadre de ses services alternatifs xCurrent Ripple lui permettant d'effectuer instantanément des transferts interbancaires à faibles coûts ainsi que de faciliter les virements interdevises selon un taux de change transparent. Par ailleurs, on observe des projets basés sur les ICO qui permettent de lever des fonds. Tel est le cas du projet Tezos qui a réussi à créer un protocole d'échange supportant la création d'applications décentralisées (dApps). Tezos est une DLT privée fonctionnant selon le protocole PoS et permettant une gouvernance participative où n'importe quel participant au protocole peut proposer des perfectionnements.

Des banques centrales (Riksbank, MAS, Banque Populaire Occitane, Banque du Canada, BdF et Nederlandsche Bank) expérimentent l'émission d'une monnaie digitale de banque centrale (MDBC). Le motif essentiel d'émission d'une MDBC est d'offrir un instrument de paiement sécurisé parfaitement liquide, adapté à l'évolution technologique de la DLT. L'apport commun de ces projets est non seulement d'effectuer des transactions en *tokens*, mais aussi de réduire les coûts sociaux des paiements de détail, lutter contre le blanchiment d'argent et le financement du terrorisme.



Dans le monde du post-marché, la bourse Australian Securities Exchanges (ASX) a remplacé son système de sous-registre électronique du centre d'échange CHESS par une solution fondée sur la DLT dans le cadre de règlement-livraison des titres. Ce projet vise à automatiser la gestion de l'achat et la vente des actions afin de réduire les coûts de transactions, ces transactions étant enregistrées de manière immuable. En Europe continentale, la bourse Euronext, en collaboration avec des banques européennes, cherche à moderniser le marché des PME avec une nouvelle infrastructure DLT de post-marché.

### *L'émergence d'un modèle de DLT de consortium*

Les difficultés rencontrées par les banques pour mettre en place des projets *blockchains* privées dans le cadre de leurs services financiers ont incité plusieurs banques à se rediriger vers les DLT de consortium (c'est-à-dire les DLT hybrides sous contrôle).

Ce type hybride est distribué de pair-à-pair au niveau architectural et est quasi décentralisé selon son protocole de fonctionnement, surtout en termes de permissions d'accès au réseau et de protocoles de consensus (seulement certains participants peuvent contribuer à la validation des transactions).

Les progiciels de gestion intégrée (*enterprise ressource planning*, ERP) existants sont largement inefficaces, cloisonnés et partiellement à base

de papier. Ils introduisent des goulets d'étranglement et créent des coûts, des retards, de la complexité et des risques. Pour cette raison, une myriade de consortiums basés sur les technologies de registre distribué s'est développée. D'une part, il existe des consortiums combinant des institutions financières, des clients corporatifs et des partenaires technologiques. Tel est le cas du réseau Marco Polo qui s'engage à offrir de nouveaux types de solutions et une connectivité transparente en matière de financement du commercial. On peut aussi mentionner le réseau Komgo dont la plateforme est consacrée au financement des matières premières. D'autre part, il existe des consortiums intégralement bancaires. Les trois initiatives suivantes en sont de bons exemples. Le réseau We.trade combine douze banques d'affaires européennes dont Deutsche Bank, HSBC, Unicredit, Société Générale et Santander. Il s'agit d'une plateforme de commerce international qui s'appuie sur le registre Hyperledger Fabric lancé par IBM permettant le partage et la sécurisation des données. Le consortium bancaire Voltron s'engage dans la numérisation des tâches relatives au crédit documentaire. Le consortium R3 développe la plateforme Corda pour les applications de DLT au sein de contrats financiers.

Au niveau de la forme, les consortiums bancaires excluent implicitement l'usage de la *blockchain* car les données ne sont pas regroupées dans des blocs (Khan *et al.*, 2017). Au niveau du fond, ils détournent les particularités qui caractérisent la *blockchain* comme l'absence de tierce partie, la gouvernance décentralisée, l'anonymat et la transparence complète (Tapscott et Tapscott, 2016 ; O'Leary, 2017). Les consortiums affichent néanmoins un bilan ambitieux et inclusif permettant aux banques d'innover dans les limites de la réglementation existante.



### *Les avantages pour les banques liés au développement de DLT de consortium*

Le secteur bancaire cherche à profiter des avantages potentiels relatifs aux DLT de consortium. Parmi ces avantages, on trouve, d'une part, ceux qui contribuent à l'efficacité de l'infrastructure financière, comme la minimisation des coûts de transactions, la réduction des risques financiers et opérationnels, la numérisation et la simplification des circuits financiers complexes surtout pour les virements internationaux multilatéraux, l'augmentation de la vitesse de traitement des transactions de détail et les gains d'efficience résultant des contrats intelligents notamment pour les activités de post-marché et les crédits documentaires (Deloitte, 2016 ; Brühl, 2017). D'autre part, on observe certains avantages sécuritaires internes directement liés à la DLT de consortium. Ces avantages sont réalisés sur le plan consensuel pour lequel le

consortium nécessite l'unanimité des participants connus, tandis que le registre public sollicite l'accord de la majorité des participants anonymes (y compris des mineurs malveillants). Le consortium est aussi un réseau autorisé qui excelle par sa capacité à empêcher les risques de fraude et les cyber-attaques en rendant l'identification des participants obligatoire et vérifiable.

À titre d'exemple, on peut considérer la nouvelle norme du registre mondial de messagerie financière (SWIFT GPI) qui est le système de référence pour les virements internationaux. Malgré sa capacité de créditer des transactions aux bénéficiaires finaux en moins d'une heure et son amélioration de la sécurité et de la traçabilité, la société technologique Ripple, inspirée de sa DLT, stimule l'innovation dans les paiements. Concrètement, elle offre aux banques un système global de règlement brut en temps réel (RTGS, *real time gross settlement system*). Ce réseau de change et de transfert de fonds testé depuis 2016 par plusieurs banques est susceptible d'effectuer des transactions financières transfrontalières non seulement moins chères et plus sûres, mais aussi quasi instantanées et sécurisées (Khan *et al.*, 2017). Ces aspects peuvent donner aux acteurs bancaires rejoignant ce système de paiement, basé sur la DLT de Ripple (c'est-à-dire xCurrent Ripple), la possibilité d'échanger entre eux des micropaiements et des microvirements à faibles commissions et à grande vitesse.



D'autres RTGS sont apparus, tels que le système de règlement-livraison de titres (TARGET2-Securities, T2S). En juin 2015, T2S a été exploité par l'Eurosystème après l'adoption de la DLT de consortium. T2S a remplacé les systèmes nets à règlement différé de titres transfrontaliers. Actuellement, les banques commerciales paient les titres sur la plateforme T2S en utilisant le compte qu'elles ont auprès de leur banque centrale, ce qui réduit considérablement le risque de règlement de la transaction et accroit ainsi la stabilité financière.

De manière prospective, la DLT de consortium peut être aussi vue comme un nouvel outil de suivi du risque systémique (Collomb et Sok, 2016). La traçabilité transactionnelle sûre et immuable d'une DLT de consortium permet d'atténuer, en cas de crise bancaire, les effets de contagion sur les marchés financiers et l'économie en général. Cette traçabilité est assurée par l'archivage de référentiels complets des transactions surtout sur des produits dérivés (options, *futures, forwards, swaps*) via une infrastructure bancaire commune et partagée à grande échelle.

Par ailleurs, il existe des avantages communs correspondant au registre distribué quel que soit son type privé ou de consortium. Il s'agit notamment de l'augmentation de la transparence, l'immuabilité des données, l'automatisation des processus, l'activation des fonctionnali-

tés d'audit intelligent, la gestion des garanties, la dématérialisation des rapports financiers et les procédures de conformité[14]. Ces avantages peuvent éliminer la plupart des tâches manuelles actuellement nécessaires pour maintenir la synchronisation des registres bancaires (Brown *et al.*, 2016).

## *EXPÉRIMENTATIONS BANCAIRES DE DLT AVEC PERMISSION*

Dans cette partie, nous procédons à une comparaison des technologies concurrentes dans le cadre de grands projets à usage bancaire (Madre, Corda et Libra). Elle permet de mettre en lumière les concepts les plus pertinents pour les banques lors de la mise en place d'une DLT.

### *La DLT privée « Madre » de la BdF*

Mis en place en avril 2018, il s'agit de l'un des premiers projets de *blockchain* privée proposé par une banque centrale. L'expérimentation du projet Madre vise à créer un registre distribué et décentralisé des identifiants créanciers SEPA (ICS)[15] en termes de partage et de gestion, en collaboration avec quelques banques commerciales[16]. Il permet de réduire drastiquement le coût, le papier, le personnel et le délai de traitement des demandes d'ICS envoyées par les banques participantes à la BdF, de plusieurs jours à quelques minutes. Le point clé repose sur la décentralisation des fonctions de gérant du référentiel en donnant aux participants la permission de lire en temps réel les référencements transmis sur le registre[17].



Pour ce faire, la BdF personnalise le protocole de la *blockchain* publique Ethereum (PoW) dans un espace privatif, afin de bénéficier des possibilités ouvertes par les contrats intelligents. En examinant son fonctionnement de plus près, on observe que le projet Madre ne constitue pas vraiment une *blockchain* privée pour plusieurs raisons. Premièrement, il s'agit d'un simple registre distribué d'identifiants et non d'une chaîne de blocs de transactions financières. Deuxièmement, même si la procédure de supervision suivie est automatisée, la gouvernance reste totalement centralisée sur le plan opérationnel car la BdF est le seul acteur qui peut recevoir des requêtes, analyser des informations et attribuer des identifiants. Donc Madre n'est pas structuré dans un réseau de pair-à-pair puisque les banques ne sont pas habilitées à partager des identifiants créanciers entre elles, contrairement à une modalité de type *blockchain* qui nécessite une gestion par les participants au réseau. Troisièmement, la BdF représentée par son centre d'alerte et de réaction aux attaques informatiques (CERT) intervient pour vérifier l'exécution du dispositif automatisé « *central bank as a code* ». Cela signifie que la BdF est loin du concept « *code is law* » où le

contrat intelligent doit être auto-exécutif sans l'implication d'une décision humaine. Quatrièmement, le registre expérimenté par la BdF n'élimine pas le rôle de *front* et de *middle office* comme intermédiaire à l'opposé de l'idée originelle de la *blockchain* qui repose sur l'absence de tiers de confiance.

La technologie utilisée par la BdF est donc bien différente de ce que l'on peut attendre d'une *blockchain*. Madre repose exclusivement sur des modalités provenant des DLT privées (données stockées sur plusieurs serveurs et dans différents lieux) et des contrats intelligents personnalisés.

### *La DLT de consortium Corda pour les banques*

De nombreuses banques internationales ont exprimé leur disposition à coopérer afin de réduire leurs coûts et leurs risques. Cela a encouragé la Fintech newyorkaise R3 à lancer à la fin de 2015 une initiative portant sur la mise en place d'un registre distribué (plateforme Corda) fédéré par et pour les banques. Corda est un réseau de pair-à-pair distribué sur le plan architectural, décentralisé sur le plan technologique et quasi décentralisé sur le plan transactionnel (permission, stockage, partage, gestion, validation des transactions, consensus). Elle associe actuellement environ deux cents institutions financières dont l'accès exige un certificat d'entrée auprès de l'opérateur du réseau R3. Cette initiative à finalité sectorielle permet de développer des prototypes DLT inspirés de la *blockchain* Ethereum pour l'utilisation de contrats intelligents au sein des activités bancaires et post-marché (Hearn, 2016).



Corda vise les transferts d'argent, l'achat et la vente d'actifs numériques. Les banques participantes au réseau Corda sont chargées d'exécuter son logiciel et de développer des applications distribuées (*CorDapps*) destinées à leurs clients sur la base d'un registre bancaire mondial (Brown *et al.*, 2016 ; Khan *et al.*, 2017). Corda consiste à automatiser le stockage et le partage des accords financiers ainsi qu'à mettre en place une infrastructure standardisée partagée (Guo et Liang, 2016). Afin de protéger leurs données et le secret des affaires, la participation des banques à Corda s'accompagne de l'application de normes confidentielles très strictes au niveau de la validation des transactions partagées et de l'obtention d'un consensus.

La dernière version de Corda impose que le partage des données soit effectué de manière chiffrée entre des parties juridiquement identifiées[18]. Dans ce cadre, les banques partageant des données, portant sur une transaction précise, enregistrent et administrent leurs propres registres, puis distribuent le registre, sous forme d'une copie cryptée, à l'ensemble des banques participantes au réseau. Cela permet aux parties

contractantes d'assurer une gestion de la confidentialité pour chaque état transféré (actif ou donnée structurée insérés dans une transaction). Le partage des données dans Corda se fait donc immédiatement au niveau transactionnel dans le but de conserver le secret des portefeuilles bancaires. Une fois le partage des données réalisé, chaque banque dans Corda accède à un sous-ensemble des états partagés. Le consortium bancaire est ainsi un réseau semi-privé où les données sont stockées de façon quasi décentralisées.

Dans Corda, le consensus est restreint aux banques disposant d'une sous-partie des données gérées par le réseau dans son intégralité. Le consensus s'applique sur la base d'une transaction nouvellement proposée qui utilise des états d'entrée historiques et crée des états de sortie actualisés. Chaque banque faisant partie du consensus doit vérifier que la transaction proposée, via un rapprochement bilatéral, constitue une mise à jour valide du registre distribué. Cela exige deux consensus consécutifs : consensus de validité et consensus d'unicité.

En premier lieu, le consensus sur la validité d'une transaction nécessite la vérification de chaque état d'entrée et de sortie de la transaction proposée à l'aide d'un contrat intelligent, puis la signature de cette transaction par les acteurs participants au consensus, qui sont les validateurs des états finals de la transaction reçue et les contrôleurs du code référencé dans celle-ci. En fait, la validation d'une transaction nécessite de vérifier toutes les transactions y aboutissant.



En second lieu, le consensus de l'unicité vise à vérifier que les entrées de la transaction proposée n'ont pas déjà été utilisées auparavant. Ce consensus est accompli par les notaires[19]. Ces derniers signent la transaction proposée sans divulguer son contenu. Une fois le consensus de l'unicité atteint, la transaction proposée est directement ajoutée au registre partagé de manière immuable. La coopération des banques nécessite une tierce partie indépendante qui contrôle la responsabilité des traitements. À cet effet, les banques favorisent la confidentialité plutôt que la transparence complète lors de l'exécution des transactions (Santo *et al.*, 2016). La confidentialité mutuelle demandée par les banques permet au protocole de consensus Corda d'offrir un débit de transaction élevé, un faible temps de latence et une économie d'énergie.

### *La DLT de consortium Libra*

Le réseau Libra (projet développé par la Bigtech Facebook en juin 2019) a été originellement conçu comme une infrastructure financière mondiale permettant à toute personne possédant un smartphone d'acquérir, de stocker et de payer des produits et des services exclusivement avec la pièce numérique multidevises appelée Diem (anciennement Libra ou ≋LBR). L'objectif est d'améliorer l'inclusion

financière de plus de 1,7 milliard de personnes non bancarisées ou sous-bancarisées dans le monde. En mars 2020, signe de changement, Facebook a présenté des aménagements de son projet initial. Selon le rapport *The Information,* le projet Libra se concentrera dans sa nouvelle version sur la prise en charge d'un réseau fermé plus traditionnel de paiement. Le réseau Libra fait appel à un panier de pièces stables adossées à une seule monnaie, en plus de la Libra, en commençant par certaines pièces dans le panier proposé (par exemple, LibraUSD ou ≋USD et LibraEUR ou ≋EUR) prêt à être lancé en 2020 selon le livre blanc de Libra Association. Cela permettra aux particuliers et aux entreprises des pays d'accéder directement à une pièce stable dans leur monnaie.

Sur le plan architectural, contrairement à la *blockchain* définie comme une séquence de blocs de transactions, le système de paiement Libra est construit sur une structure de données unique qui enregistre l'historique des transactions et des états au fil du temps. Libra et les autres pièces de monnaie sont architecturées selon les graphes acycliques dirigés (*directed acyclic graph*, DAG)[20]. Ce type de DLT simplifie le travail du réseau en donnant un cadre unifié à la vérification de l'intégrité des données. La DLT de consortium Libra permet à ses partenaires commerciaux (dont Mastercard, Visa et PayPal) de garder conjointement un registre de données numériques et donc de parvenir collectivement à un consensus sur l'acceptation ou le rejet d'une transaction.



Sur le plan monétaire, contrairement aux crypto-monnaies publiques et volatiles (exemples de Bitcoin et de l'Ether) utilisées sans permission à des fins de spéculation, d'investissement et de thésaurisation, les pièces circulant sur le réseau Libra sont permissionnées (c'est-à-dire gardées par quelques entités de confiance), stables et à faible volatilité. Libra et les autres pièces stables sont principalement utilisées dans les paiements transfrontaliers et les transferts d'argent et sont attachées à des portefeuilles détenus sous pseudonymes. Les détenteurs de pièces stables sont incités à les consommer et à ne pas les thésauriser. Néanmoins les pièces stables peuvent être un moyen de protéger l'épargne dans les économies fragiles. L'offre de ces pièces n'est pas limitée. Pour créer de nouvelles pièces, il doit y avoir un achat équivalent en monnaies fiduciaires et le transfert de cette monnaie à la réserve. La réserve évolue en réponse à des contextes défavorables au niveau des conditions du marché pour assurer la stabilité de sa valeur (Catalini *et al.*, 2019). La réserve ainsi créée est investie dans des actifs sous-jacents à faible risque de crédit et à liquidité élevée.

Sur le plan économique, les intérêts générés par la réserve doivent être utilisés pour couvrir les coûts du réseau, garantir les frais de

transaction bas et augmenter le capital requis. Afin d'assurer la stabilité et la croissance du réseau, l'association Libra crée un cadre de fonds propres réglementaires pour absorber les pertes qui pourraient apparaître dans des situations économiques extrêmes (cas de changements rapides des taux d'intérêt). Ces fonds propres permettent de faire face aux risques de crédit, de marché et opérationnels. La conception économique de la DLT de consortium Libra rend son mode de paiement, créateur de valeur, confidentiel, transparent et interopérable.

Sur le plan technique, le protocole du Libra est à double modalité. D'une part, il s'agit d'une preuve à zéro connaissance (*zero knowledge proof*, ZKP) permettant un temps de vérification succinct et une taille de preuve réduite[21]. D'autre part, il s'agit d'une preuve de la tolérance des pannes byzantines (*byzantine fault tolerance*, BFT) permettant un passage à grande échelle (Baudet *et al.*, 2019). Ces deux modalités contribuent à améliorer l'efficacité du réseau.

**Remarque 2.** Il est intéressant d'identifier les différences entre les initiatives technologiques examinées dans cette partie : Madre, Corda et Libra. On observe notamment que Madre, créée par une banque centrale, est une DLT privée où la gestion des données est hybride : l'enregistrement est décentralisé et la transmission est centralisée. Dans le cadre de Madre, il n'y a pas de consensus sur l'état du registre dont le contrôle et la gouvernance sont assurés par une entité centrale jouant le rôle d'intermédiaire entre les participants. À l'inverse, Corda, lancée par une Fintech, est une DLT de consortium partiellement distribuée qui fonctionne sans tiers de confiance. Finalement, Libra, conçu par une Bigtech, est une DLT de consortium totalement distribuée qui nécessite un consensus entre tous ses participants. Ce prototype excelle par sa gouvernance répartie, son cadre de conformité robuste et ses protections solides dans la conception de la réserve.



## *CONCLUSION*

Les monnaies virtuelles, les protocoles de consensus, la cryptographie asymétrique, les réseaux de pair-à-pair sans tiers de confiance, les *smart contracts*, les ICO, les *tokens*, les modèles de gouvernance partagée sont tous des éléments originellement issus de la révolution *blockchain* (Wright et de Filippi, 2015). La *blockchain* a introduit une technologie de rupture qui vient modifier en profondeur les pratiques centralisées en matière de gestion et de contrôle même si, dans la plupart des cas, les projets bancaires relèvent plutôt des registres distribués. Comme le souligne d'ailleurs Halaburda (2018) dans un article

au titre volontairement provocateur (« Blockchain Revolution Without the Blockchain »), les modalités d'utilisation que l'on observe en pratique ne nécessitent pas la mise en place d'une *blockchain*.

Nous avons décrit comment les apports disruptifs des *blockchains* et des crypto-monnaies poussent l'industrie bancaire à basculer vers un nouveau paradigme alternatif et équilibré qui associe les avantages des systèmes distribués autonomes et la réglementation juridique existante. En cela, les consortiums bancaires et leurs plateformes (c'est-à-dire Corda) sont de bonnes illustrations de ce type d'applications. Ces projets sont des protocoles de stockage et d'échange auditables fondés sur des DLT, permettant d'améliorer le système transactionnel actuel en intégrant de nouvelles pratiques de contrôle des informations financières.

En conclusion de ce constat sur les formes de technologies les plus adaptées, il est légitime de se demander dans quelle mesure les DLT de consortium peuvent aboutir à une (R)-évolution pour l'infrastructure du marché bancaire. Pour y répondre, il est important de mettre l'accent sur les applications et les modèles de ces DLT, que ce soit pour des activités de post-marché (compensation, livraison, règlement des titres) ou pour des produits et des services bancaires. Dans ce sens, deux scénarios sont évoqués par la Banque centrale européenne (BCE) dans son rapport (BCE, 2016). Le premier scénario est évolutionnaire. Il est tourné vers des attentes spécifiques du secteur financier comme la digitalisation de certaines activités bancaires ou l'amélioration de la vitesse de traitement des transactions par les infrastructures du marché. Ces attentes ne mettent pas en question les fondements économiques actuels. Le deuxième scénario est plus révolutionnaire puisqu'il s'agit d'appliquer une DLT de pair-à-pair entre tous les acteurs du marché (émetteurs, investisseurs, dépositaires de services, fournisseurs d'infrastructures, banques commerciales, places financières) avec mise à disposition d'outils complètement décentralisés, désintermédiés et automatisés.



Les expérimentations de DLT de consortium sont nombreuses, mais leurs mises en place restent encore difficiles, comme nous l'avons vu. Le passage de la situation actuelle (bases de données centralisées) à la mise en œuvre de DLT de consortium bancaire nécessite l'identification d'un plan de gouvernance clair et l'établissement des standards juridiques applicables. Deux évolutions sont attendues. À court terme, un modèle de DLT de consortium peu évolué serait harmonisé techniquement et juridiquement avec l'infrastructure du marché financier. À moyen terme, la DLT de consortium pourrait constituer un maillon essentiel d'une nouvelle infrastructure bancaire, digitale et plus décentralisée.

# *NOTES*

1. Bitcoin avec (« B » majuscule désigne le protocole (première application de la *blockchain*) alors qu'avec « b » minuscule, bitcoin indique la crypto-monnaie. Pour en savoir plus, voir Nakamoto (2008).

2. Pour comprendre le fonctionnement et les applications de la *blockchain*, on renvoie le lecteur au rapport de Finyear (2016), par exemple. Voir le site : https://www.finyear.com/attachment/648901/.

3. Source : https://101blockchains.com/blockchain-vs-hashgraph-vs-dag-vs-holochain/.

4. Selon l'article L 111-1 du Code monétaire et financier (CMF), la monnaie de la France est l'euro.

5. Pour un regard sur le marché des monnaies alternatives, voir le site : https://coinmarketcap.com/.

6. La première plateforme d'échange de bitcoin (MtGox) est tombée en faillite en janvier 2015 à la suite d'une fraude interne de 360 M$ (soit 650 000 bitcoins). Plus récemment, en 8 mai 2019, le géant de crypto-monnaie (Binance) a été piraté pour 41 M$ (7 000 bitcoins).

7. Récemment, de nombreuses initiatives bancaires ont néanmoins été lancées pour créer une crypto-monnaie stable (c'est-à-dire JPM Coin) ou une monnaie digitale de banque centrale (MDBC ; en anglais, *central bank digital currency*, CBDC). La MDBC est différente des diverses formes de monnaie numérique décentralisée comme le bitcoin. Elle est centralisée, stable et au pair avec une monnaie fiduciaire comme l'euro ou le dollar.

8. Source : https://bitcoin.fr/quelle-est-la-consommation-electrique-du-reseau-bitcoin/.

9. Le Parlement a adopté le 11 avril 2019 la loi Pacte qui vise à créer un cadre réglementaire pour les prestataires de services des crypto-actifs et pour les levées de fonds par émission de *tokens*.

10. Le RGPD (Règlement général de la protection des données) est entré en application le 25 mai 2018 dans l'Union européenne. Il vise à appliquer des mesures de conformité dès que le produit ou le service est créé « *privacy by design* ».

11. La CNIL considère que le protocole de la *blockchain* publique n'est pas responsable des traitements. Ses participants (personne physique et morale) sont les vrais responsables de gestion des données selon leurs activités professionnelles ou commerciales. Ce point de vue n'est pas partagé par tous les acteurs ou observateurs de la *blockchain*.



12. Source : http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf.

13. Source : https://www.bankobserver-wavestone.com/point-initiatives-blockchain-bancaires-europe/.

14. Source : Rapport de l'ESMA, *Blockchain and Securities Markets*.

15. L'identifiant des créanciers SEPA (ICS) est un numéro de référence unique composé de treize caractères. Ce numéro identifie chaque émetteur souhaitant mettre en place un prélèvement.

16. Ce registre est un produit centralisé qui ne répond pas à l'exigence architecturale d'une DLT (présence d'un tiers de confiance) et ne peut pas être comparé avec des solutions décentralisées.

17. Source : www.revue-banque.fr/risques-reglementations/article/blockchain-banque-france-entre-en-production.

18. La dernière version du consensus (Corda 4) adopte l'approche *Byzantine Fault Tolerance* (*BFT*). Corda peut fonctionner correctement, même en cas d'échec de certains nœuds de validation.

19. Dans la terminologie employée par les spécialistes du domaine, le notaire est un vérificateur interne au réseau Corda. Son rôle est d'éviter la double dépense d'un montant transféré. Par exemple, il certifie que la somme reçue par une banque n'est pas utilisée à un autre emploi.

20. Les DAG représentent la cohabitation de plusieurs chaînes de transactions dont chaque transaction est un nœud du graphe. Les fonctionnalités de ce type dépassent la *blockchain*. Par exemple, les DAG offrent un système de micropaiement entre ses machines (Popov, 2018).

21. Le *zero-knowledge proof* est un protocole sécurisé entre deux entités : un fournisseur de preuve et un vérificateur. Le fournisseur de preuve doit convaincre mathématiquement le vérificateur de la validité d'une proposition sans divulguer aucune information supplémentaire au-delà du fait que la proposition est vraie.

# *BIBLIOGRAPHIE*


Baudet M., Ching A., Chursin A., Danezis G., Garillot F., Li Z., Malkhi D., Naor O., Perelman D. et Sonnino A. (2019), « State Machine Replication in the Libra Blockchain ».

BCE (Banque centrale européenne) (2016), *Distributed Ledger Technology: Role and Relevance of the ECB*, Rapport.

BdF (Banque de France) (2018), « L'émergence du bitcoin et autres crypto-actifs : enjeux, risques et perspectives », *Focus*, nº 16.

Beaudemoulin N., Warzée D. et Bedoin T. (2017), « Les enjeux de la Blockchain pour la Banque de France et l'Autorité de contrôle prudentiel et de résolution (ACPR) », *Annales des mines réalités industrielles*, vol. 3, pp. 29-33.

Berentsen A. et Schar F. (2018), « The Case for Central Bank Electronic Money and the Non-Case for Central Bank Cryptocurrencies », *Federal Reserve Bank of St. Louis Review*, vol. 100, nº 2, pp. 97-106.

Böheme R., Christin N. et Edelman B. (2015), « Bitcoin: Economics, Technology, Governance », *Journal of Economics Perspectives*, vol. 29, nº 2, pp. 213-238.

Bonneau T. et Renard I. (2017), « Fonctionnement de la blockchain – Compatibilité avec un environnement réglementé : que peut-on et que doit-on réglementer dans une blockchain ? », *Revue de droit bancaire et financier*, nº 1, dossier 3.

BRI (Banque des règlements internationaux) (2017), *Distributed Ledger Tchnology in Payment, Clearing and Settlement*, Rapport.

Brown R. G., Carlyle J., Grigg I. et Hearn M. (2016), « Corda: an Introduction », *Document de travail*.

Brühl V. (2017), « Virtual Currencies, Distributed Ledgers and the Future of Financial Services », *Intereconomics*, pp. 370-378.

Buterin V. (2014), « A Next Generation Smart Contract & Decentralized Application Platform », *Document de travail*.

Catalini C. et Gans J. (2017), « Some Simple Economics of the Blockchain », Rotman School of Management, *Working Paper*, nº 2874598 ; *MIT Sloan Research Paper*, nº 5191-16.

Catalini C., Gratry O., Mark Hou J., Parasuraman S. et Wernerflet N. (2019), « The Libra Reserve », *Document de travail.*

Cecchetti S. G. et Schoenholtz K. L. (2017), « Fintech, Central Banking and Digital Currency », *Money and Banking Blog*.

Collomb A. et Sok C. (2016), « Blockchain/Distributed Ledger Technology (DLT): What Impact on the Financial Sector? », *Communication & Strategies*, vol. 103.

De Filippi P. et Reymond M. (2016), « La Blockchain : comment réguler sans autorité », in Nitot T. (dir.) et Cercy N., *Numérique : reprendre le contrôle*, Framabook, pp. 81-96.

Deloitte (2016), *The Future of Financial Infrastructure. An Ambitious Look at How Blockchain Can Reshape Financial Services*, Rapport.

ESMA (European Securities Markets Authority) (2017), *The Distributed Ledger Technology Applied to Securities Markets*, Rapport.

Gramoli V. et Staples M. (2018), « Blockchain Standards: Can We Reach Consensus? », IEEE, *Communications Standards Magazine*, vol. 2, nº 3, pp. 16-21.

Guégan D. (2017a), « Blockchain publique versus Blockchain privée : enjeux et limites », Centre d'économie de la Sorbonne, *Document de travail*.

Guégan D. (2017b), « Blockchain publique et contrats intelligents (*Smart Contrats*). Les possibilités ouvertes par Ethéreum... et ses limites », Centre d'économie de la Sorbonne, *Document de travail*.

Guégan D. (2018), « The Digital World: II – Alternatives to the Bitcoin Blockchain? », Centre d'économie de la Sorbonne, *Document de travail*.

Guo Y. et Liang C. (2016), « Blockchain Application and Outlook in the Banking Industry », *Financial Innovation*, pp. 2-24.

HAERINGER G. et HALABURDA H. (2018), « Bitcoin: a Revolution? », in Ganuza J. et Llobert G. (éd.), *Economic Analysis of the Digital Revolution*, FUNCAS.

HALABURDA H. (2018), « Blockchain Revolution without the Blockchain? », Communications of the ACM, vol. 61, nº 7, juillet, pp. 27-29.

HEARN M. (2016), « Corda: a Distributed Ledger », *Document de travail*.

IANSITI M. et LAKHANI K. R. (2017), « The Truth about Blockchain », *Harvard Business Review*, vol. 95, nº 1, pp. 118-127.

KHAN C., LEWIS A., RUTLAND E., WAN C., RUTTER K. et THOMPSON C. (2017), « A Distributed Ledger Consortium Model for Collaborative Innovation », The IEEE Computer Society.

NAKAMOTO S. (2008), « Bitcoin: a Peer-to-Peer Electronic Cash System », *Document de travail*.

O'LEARY D. E. (2017), « Configuring Blockchain Architectures for Transaction Information in Blockchain Consortiums: the Case of Accounting and Supply Chain Systems », *Intelligent Systems in Accounting, Finance and Management*, vol. 24, nº 4, pp. 138-147.

PAVEL I. (2017), « La blockchain - Les défis de son implémentation », *Annales des mines réalités industrielles*, nº 11, pp. 20-24.

POPOV S. (2018), « The Tangle », *Document de travail*.

REID F. et HARRIGAN M. (2013), « An Analysis of Anonymity in the Bitcoin System », in Altchuler Y., Elovici Y., Cremers A. B. *et al*. (éd.), *Security and Privacy in Social Networks*, Springer, pp. 197-223.

RICKS M., CRAWFORD J. et MENAND L. (2018), « A Public Option for Bank Accounts (or Central Banking for All) », *Vanderbilt Law Research Paper*, nº 18-33 ; *UC Hastings Research Paper*, nº 287.

RODRIGUEZ P. (2017), *La révolution blockchain : algorithmes ou institutions, à qui donnerez-vous votre confiance ?*, Dunod, 177 p.

SANTO A., MINOWA I., HOSAKA G., HAYAKAWA S., KONDO M., ICHIKI S. et KANEKO Y. (2016), « Applicability of Distributed Ledger Technology to Capital Market Infrastructure », *JPX Working Paper*, vol. 15.

SAYEED S. et MARCO GISBERT H. (2019), « Assessing Blockchain Consensus and Security Mechanisms Against the 51% Attack », *Applied Sciences*.

TAPSCOTT D. et TAPSCOTT A. (2016), *Blockchain Revolution: How the Technology Behind Bitcoin and other Cryptocurrencies Is Changing the World*, London: Penguin Books.

THE LIBRA ASSOCIATION (2020), « An Introduction to Libra », *Document de travail*.

VERDIER M. (2017), « La blockchain et l'intermédiation financière », *Revue d'économie financière*, nº 129, pp. 67-87.

WAELBROECK P. (2017), « La blockchain : les enjeux économiques de la Blockchain », *Annales des mines réalités industrielles*, nº 10, pp. 10-19.

WRIGHT A. et DE FILIPPI P. (2015), « Decentralized Blockchain Technology and the Rise of Lex Cryptographia », *Working Paper*.

YERMACK D. (2017), « Corporate Governance and Blockchains », *Review of Finance*, vol. 21, nº 1, pp. 7-31.

ZHENG Z., XIE S., DAI H., CHEN X. et WAND H. (2017), « An Overview of Blockchain Technology: Architecture, Consensus and Future Trends », IEEE, 6th International Congress on Big Data.