OPINIONS
& DÉBATS

N°15 - Mai 2016

Blockchain et autres registres distribués : quel avenir pour les marchés financiers ?

Blockchain and distributed ledger technologies (DLT): what impact on financial markets ?

Alexis Collomb & Klara Sok

INVESTISSEMENTS D'AVENIR

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

LABEX Louis Bachelier

SOMMAIRE

CONTENTS

Opinions & Débats N° 15 Mai 2016

Publication de l'Institut Louis Bachelier

Palais Brongniart - 28 place de la Bourse 75002 Paris ◆ Tél. : 01 73 01 93 40 ◆ www.institutlouisbachelier.org

http://www.labexlouisbachelier.org

DIRECTEUR DE LA PUBLICATION : Jean-Michel Beacco ◆ CHEF DE PROJETS : Noémie Dié ◆ COORDINATION ÉDITORIALE : Karol Alhaire

CONTACT : noemie.die@institutlouisbachelier.org

CONCEPTION GRAPHIQUE : Vega Conseil 01 48 85 92 01

Les articles publiés dans la série "Opinions & Débats" offrent aux spécialistes, aux universitaires et aux décideurs économiques un accès aux travaux de recherche les plus récents. Ils abordent les principales questions d'actualité économique et financière et fournissent des recommandations en termes de politiques publiques.

The Opinion and Debates series sheds scientific light on current topics in economics and finance. Bringing together several types of expertise (from mathematicians, statisticians, economists, lawyers, etc.) this publication makes recommendations in the formulation and implementation of public economic policy.

EDITO

Par Jean-Michel Beacco
Directeur général de l'Institut Louis Bachelier

En mars dernier, la valeur des 15,5 millions de bitcoins en circulation dans le monde dépassait 6 milliards de dollars. Guère étonnant, dès lors, qu'une possible saturation du système d'échange inquiète bien au-delà du cercle d'initiés maîtrisant les défis technologiques en jeu.

La véritable question est la capacité de cette innovation à évoluer, à s'adapter à un nombre croissant d'utilisateurs et de transactions. Derrière le cas emblématique du bitcoin et de sa base d'enregistrement de données, la Blockchain, l'économie mondiale s'interroge sur les bouleversements qui vont naître de l'avènement des crypto-monnaies et des chaînes de blocs.

Se passer d'intermédiaires, recourir, n'importe où, à un système monétaire et d'échange décentralisé, telle est la promesse des chaînes de blocs, promesse dont nous n'imaginons pas encore toutes les applications. Cependant, comme le montrent les initiatives en cours, gouvernements, entreprises, régulateurs, aucun acteur ne peut faire l'économie d'une réflexion sur le sujet.

Déjà, des applications concrètes voient le jour, présentées dans cet article par les chercheurs Alexis Collomb et Klara Sok. Ce ne sont toutefois que les prémisses de bouleversements plus importants, notamment dans le secteur de la banque et de la finance. La fameuse Blockchain n'est plus seule sur le marché, concurrencée par des chaînes de blocs privées ou publiques. Des solutions de substitution à des métiers traditionnels se dessinent et ne se cantonnent pas au domaine des transactions. Les possibilités d'enregistrement des données qu'offrent ces chaînes pourraient bouleverser le secteur financier.

Prouver la solvabilité des acteurs dans un contexte réglementaire toujours plus pointu, améliorer la confiance dans les marchés, raccourcir les délais nécessaires à certaines opérations, automatiser l'émission d'actions ou la distribution de dividendes en espèces... Ce ne sont que quelques exemples des petites révolutions que les chaînes de blocs pourraient entraîner dans la finance.

Les querelles actuelles sur les modifications à apporter à la Blockchain prouvent qu'une voie unique est loin d'être tracée, d'autant plus que les intérêts en jeu divergent, des investisseurs aux entreprises, des traders aux régulateurs, tandis que des questions importantes demeurent. L'aspect sécuritaire ne saurait souffrir de compromis, mais transparence et collaboration ne sont pas pour autant garanties dans cette course à l'innovation.

In March, the value of the 15.5 million bitcoins in circulation worldwide was more than $6 billion. Little wonder, therefore, that a possible saturation of the exchange system is causing concern well beyond the inner circle who have mastered the technological challenges involved.

The real issue is the capacity of this innovation to evolve and adapt to the growing number of users and transactions. Behind the special case of bitcoin and its transaction recording database, the Blockchain, the global economy is wondering about the changes that will ensue from the advent of crypto-currencies and blockchains.

Being able to dispense with intermediaries and having recourse anywhere to a monetary system and decentralized exchange – such is the prospect offered by blockchains, a prospect whose full range of applications remains unknown. However, as shown by the initiatives already underway, no government, business, regulator or other actor can afford not to think about it.

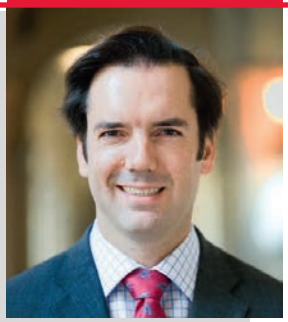
Concrete applications are already emerging, and are introduced in this article by the researchers Alexis Collomb and Klara Sok. These, however, are only the most important indicators of upheavals, especially in the banking and finance sector. The celebrated Blockchain is no longer alone in the market, and faces competition from private or public blockchains. Alternative solutions to traditional professions are emerging – and they are not confined to the area of transactions. The possibilities of recording data offered by these channels could disrupt the financial sector.

Testing actors' solvency in an increasingly strict regulatory environment, improving confidence in markets, shortening the time needed for certain operations, automating the issuance of shares or the distribution of cash dividends... These are just a few examples of the radical changes that blockchains could give rise to in finance.

The current disputes over the changes to be made to the Blockchain show that there is no single track to be followed, especially as the interests in play diverge, from investors to companies, from traders to regulators, and that major issues remain unresolved. The security aspect cannot be subject to compromise, but transparency and collaboration are far from guaranteed in this race to innovate.

BIOGRAPHIE

Alexis Collomb



Après une carrière initiale en banque d'investissement à New York, et en salle de marché comme stratégiste dérivés actions puis *cross-asset* à Londres, Alexis Collomb a rejoint le Cnam en 2011 pour reprendre la responsabilité de la chaire de finance, et de son master. Il assure également aujourd'hui la direction du département Economie Finance Assurance Banque (EFAB) qui comprend notamment l'Ecole nationale d'assurances (Enass). Ingénieur réseaux de formation initiale, il est aussi titulaire d'un master en économie des systèmes et d'un doctorat en sciences de gestion de l'université de Stanford. Il a également étudié l'intelligence artificielle au Japon. Membre du LIRSA (EA 4603), il siège par ailleurs au conseil scientifique du Labex Refi.

Ses recherches portent sur les crypto-monnaies telles que le Bitcoin, et leurs registres distribués comme la Blockchain. Plus particulièrement intéressé par la transformation digitale de l'industrie financière, en particulier ses infrastructures post-marché, et du secteur de l'assurance, il étudie notamment l'impact des nouvelles applications distribuées et des *smart contracts* sur le financement digital de l'économie (finance participative, prêts entre particuliers).

Alexis Collomb began his career in the financial services industry, first as an investment banker in New York, then as an equity derivatives and cross-asset strategist in London. He joined the Cnam in 2011 as Professor of Finance and was appointed chair of Cnam's Department of Economics, Finance, Insurance and Banking and its Ecole nationale d'assurances (Enass). After an initial French degree in network engineering, Alexis graduated with a Master's in Engineering-Economics Systems and a PhD in Management Science from Stanford University. He has also studied artificial intelligence in Japan. Alexis is a member of Cnam's LIRSA (EA 4603) research center and sits on Labex Refi's Scientific Advisory Board.

He is particularly interested in the digital transformation of financial services and the insurance industry. His research focuses on cryptocurrencies and their distributed ledgers, such as Bitcoin and the Blockchain, and on how emerging distributed leger technologies (DLT) and smart contracts could impact the transformation of poste-trade infrastructure and facilitate the development of digital financing (crowdfunding, peer-to-peer lending).

Klara Sok

Klara Sok est chercheuse et doctorante au laboratoire Dicen-IDF du Conservatoire National des Arts et Métiers où elle mène une thèse sur le Bitcoin. Elle s'intéresse tout particulièrement aux changements sociologiques et organisationnels induits par l'utilisation de la blockchain Bitcoin et au développement parallèle d'autres types de blockchains comme alternatives organisationnelles aux structures existantes, notamment pour le secteur financier. Elle porte également un grand intérêt aux transformations et aux évolutions du système financier et monétaire.

Après une première expérience pour le Boston Consulting Group en tant qu'analyste en design organisationnel, Klara a également travaillé pendant plusieurs années comme gérante de portefeuille chez Edmond de Rothschild Asset Management, focalisée sur l'Asie du Sud-Est. Elle a également effectué plusieurs missions de recherche au Cambodge pour le compte des Nations Unies (CNUCED, UNIFEM), La Banque Mondiale (International Finance Corporation), et le Forum Economique Mondial.

Klara est diplômée d'Audencia et du mastère recherche en sociologie des organisations de Sciences Po Paris.

Klara Sok is a research fellow at the Conservatoire National des Arts et Métier's Dicen-IDF research center. She is currently preparing her PhD thesis in Information and Communication on crypto-currencies and Bitcoin. Klara is particularly interested in the sociological and organizational changes generated by the introduction of Bitcoin and other blockchain-based information schemes as alternatives to existing legacy systems, namely for the financial services industry, and in the evolution and transformation of financial and monetary systems.

After a first experience as organizational analyst for the Boston Consulting Group, Klara spent several years working as an Asian equity portfolio manager for Edmond de Rothschild Asset Management. She also worked in Cambodia as a consultant for the United Nations (UNCTAD, UNIFEM), the World Bank (International Finance Corporation), and the World Economic Forum.

Klara graduated from Audencia Business School and holds a Master's in organizational sociology from Sciences Po Paris.

Blockchain et autres registres distribués : quel avenir pour les marchés financiers ?

Alexis Collomb
Professeur du Cnam – Finance

Klara Sok
Doctorante au Cnam, Laboratoire Dicen-IDF

Avant-propos

Les fondements du protocole Bitcoin et de sa crypto-monnaie ont vu le jour en 2008 dans un livre blanc intitulé "*Bitcoin : A Peer-to-Peer Electronic Cash System"* envoyé à une liste de diffusion de cryptographie par un certain Satoshi Nakamoto. La première transaction bitcoin a été réalisée peu de temps après, en janvier 2009 sur la Blockchain[1], une base de données organisée sous forme de chaîne de blocs d'information, distribuée au sein d'un réseau pair-à-pair. Aujourd'hui, plus de sept ans après cette première transaction, la Blockchain est devenue un sujet très médiatique et de nombreux articles et publications traitent du Bitcoin et de son avatar générique, désormais communément appelé la technologie des registres distribués ou Distributed Ledger Technology (DLT).

Si l'on regarde les couvertures de presse consacrées au Bitcoin et à la Blockchain au cours des six derniers mois, nous pourrions être tentés de dire qu'il ne s'agit là que d'une simple mode passagère, manifestation de l'instinct grégaire des esprits animaux de Keynes, ou d'un fonctionnement mimétique à la Girard. Face à cette frénésie, certains économistes de renom ont même déclaré que le Bitcoin/la Blockchain constituaient "le parfait exemple d'une bulle" [2]. Et pourtant, si l'on s'en tient aux faits, on constate que le Bitcoin et ses émules se sont montrés plutôt résilients et continuent à susciter l'intérêt et les investissements. Et sans nous risquer à prévoir l'avenir du Bitcoin et des autres crypto-monnaies, nous pensons que celui-ci s'annonce bien plus prometteur que certains ne voudraient le croire.

Il est aujourd'hui clair que les concepts qui constituent les fondements du Bitcoin et de son registre distribué sous-jacent, appelé la Blockchain, incitent de nombreuses institutions à porter un regard critique sur leurs systèmes d'information et leurs processus de gestion, voire à les repenser. Et le secteur financier en particulier, qui gère un volume important de paiements et de transactions multiformes, porte une attention soutenue à la question de savoir comment utiliser la DLT pour améliorer ou optimiser l'infrastructure des marchés financiers et des capitaux.

Dans ce rapport, nous tenterons de résumer les principales questions et enjeux concernant les registres distribués de données, et nous explorerons comment la DLT pourrait être intégrée à l'infrastructure des marchés financiers, notamment au niveau post-marché. Notre approche sera nécessairement non-exhaustive et pluri-disciplinaire, avec une certaine dose d'anticipations prospectives. Nous ne prétendons pas, bien entendu, avoir fait le tour du sujet : il est bien trop vaste et complexe, et la vague de transformation qu'il a déclenchée trop rapide pour qu'un rapport se voulant général et synthétique comme celui-ci suffise. Mais notre travail de recherche nous a convaincus que la puissance perturbatrice du Bitcoin et de la Blockchain est bien réelle. Nous espérons que ce rapport constituera une synthèse utile pour les fournisseurs d'infrastructure de marché, et tous ceux qui réfléchissent actuellement aux risques et opportunités que pourrait représenter cette technologie pour leurs secteurs d'activité respectifs.

Les opinions exprimées dans cette publication sont celles des auteurs et ne reflètent pas nécessairement celles de l'AMF, du Cnam, du Laboratoire d'Excellence Louis Bachelier Finance et Croissance Durable, ou de leurs affiliés.

Résumé

Dans la première moitié de ce rapport, nous proposerons une brève histoire des crypto-monnaies et un résumé des caractéristiques clés du protocole Bitcoin et de sa base de données distribuée, la Blockchain. Nous évoquerons ensuite quelques-unes des questions techniques qui ont récemment divisé la communauté Bitcoin, avant de présenter une typologie des registres distribués, nécessaire pour comprendre les différents domaines d'application possibles de la DLT. Puis, nous aborderons les aspects de fiabilité et de sécurité des registres distribués, un sujet qui a suscité inquiétude et scepticisme par le passé, et qui reste clairement une question centrale pour l'industrie financière.

Dans la deuxième moitié du rapport, nous détaillerons quelques-unes des principales applications potentielles de la DLT, en particulier pour le secteur financier. Nous regarderons ensuite comment le marché financier pourrait intégrer la DLT dans l'infrastructure post-marché. Et nous terminerons en présentant quelques exemples concrets de mise en œuvre de cette technologie, ainsi qu'un ensemble de réflexions et de recommandations sur le sujet.

1. Distributed Ledger Technology (DLT) : une révolution ou une diversion ?

1.1. L'intérêt pour la blockchain touche tous les secteurs d'activité : de l'industrie financière au secteur public, en passant par l'éducation

L'engouement pour la blockchain a gagné tous les secteurs de l'économie. À travers le monde, des organisations publiques et privées ont manifesté un intérêt grandissant et exprimé leur enthousiasme pour cette nouvelle technologie. Nous constatons une prolifération d'initiatives et, depuis fin 2015, de nombreux rapports ont été publiés par des institutions financières et des organismes publics à un rythme accéléré. Tout en prenant une approche didactique pour expliquer la blockchain au lecteur, la plupart de ces publications encensent les aspects "disruptifs" du phénomène, et soulignent son caractère perturbateur. Nous ne ferons pas ici une liste exhaustive des initiatives actuelles, mais avons choisi de citer quelques-uns des projets les plus significatifs en cours de développement pour donner au lecteur une idée de la nature, de la diversité et de l'importance du phénomène blockchain.

Mais avant d'aborder ces exemples, il est important de noter qu'une sensibilisation accrue du public et le développement concomitant d'innovations comme les *colored coins*, *sidechains* et *smart contracts*, ont enrichi le concept de blockchain d'origine, nourrissant ainsi la construction d'un pôle d'innovation (Schumpeter, 1935) spécifique aux Digital Ledger Technologies (DLT). L'émergence du pôle d'innovation DLT a permis de renforcer la perception du potentiel applicatif de la blockchain, encourageant des initiatives productives les plus diverses, que ce soit sous forme d'investissements ou de travail.

Bien qu'inspiré de technologies existantes, la DLT va bien au-delà des registres partagés (*shared ledgers*) et des bases de données distribuées qui existaient jusqu'alors. En effet, la DLT cumule les avantages d'une base distribuée et la fiabilité du système de registre.

Par ailleurs, on assiste à un foisonnement de réflexions et de débats au sujet de la blockchain : Quel est le degré de distribution souhaitable ? Une blockchain doit-elle être publique ou privée, ou alors une combinaison hybride ? À ce jour, ces questions divisent encore la communauté d'innovation se développant autour de la DLT, et le débat contribue à la richesse et à la diversité du pôle d'innovation lui-même. Mais il faut bien comprendre que ce qui apparaît à première vue comme des choix technologiques simples sont en fait bien plus que cela : ces choix sont indissociables des mécanismes de consensus qui constituent le fondement même de l'organisation et la gouvernance de la blockchain ; en ce sens, ils sont déterminants pour le développement présent et futur de la DLT.

Enfin, les gouvernements et autorités publiques de régulation seront inéluctablement amenés à repenser les systèmes de contrôle et de régulation des activités économiques et sociales en place, que ce soit dans le domaine de la propriété intellectuelle, de l'attribution des licences d'activité ou de la fiscalité. En ce qui concerne la propriété intellectuelle (IP) liée à la DLT, alors que la communauté de développeurs du *Bitcoin Core* a fait du protocole d'origine et de la Blockchain un code source ouvert (*open source code*) à tous, certains acteurs semblent vouloir déposer des demandes de brevets liés à certaines applications de la DLT. Bank of America, par exemple, aurait déjà déposé 15 demandes de brevet auprès du US Patent and Trademark Office[3] et envisagerait d'étendre sa stratégie IP à beaucoup d'autres domaines. Une telle stratégie, qui vise à restreindre les droits de propriété intellectuelle liée à la DLT en les rendant exclusifs, est clairement en contradiction avec la philosophie *open source* ayant favorisé jusqu'alors le développement de cette technologie, et montre à quel point certaines institutions financières cherchent à profiter de la prime au premier entrant (*first mover advantage*) dans l'espace de cette technologie encore en plein développement.

Voici quelques unes des principales initiatives actuelles dans le domaine de la blockchain ; elles démontrent clairement que la portée de cette dernière dépasse largement le monde des *"wallets"* (portefeuilles) et des plateformes de change.

Plusieurs gouvernements ont déjà exprimé leur intérêt pour la DLT. Ainsi, dans son rapport *"Digital Ledger Technology : beyond blockchain"* (janvier 2016), l'*Office for Science* du Royaume-Uni déclare voir en la DLT "le potentiel pour constituer l'une de ces explosions de créativité capable de catalyser un niveau exceptionnel d'innovation." L'*Office for Science* souligne également la nécessité pour le gouvernement du Royaume-Uni d'agir rapidement et énergiquement pour développer et coordonner des ressources dédiées spécifiquement à l'étude et au développement de la DLT afin d'éviter que le Royaume-Uni ne "rate le coche" face à la concurrence internationale. Dans ce contexte, le gouvernement britannique encourage activement des acteurs clés du développement numérique, comme le nouvel *Alan Turing Institute*, le *Digital Catapult Centre*, l'*Open Data Institute* et le *Whitechapel Think Tank*, à travailler ensemble.

Au Ghana, des projets blockchain sont développés afin d'utiliser la blockchain dans le domaine du cadastre foncier[4]. L'Estonie, elle, développe un service public notarial basé sur cette technologie via le programme *Keyless Signature Infrastructur*e. L'île de Man, en collaboration avec la start-up Credits.vision[5], teste actuellement une nouvelle technologie KYC (*know your customer*) développée à partir de DLT et qui sera accessible en *open source* pour ses citoyens.

Dans le secteur de la santé, on teste des systèmes DLT pour l'archivage de dossiers de santé numériques.[6] Des start-ups comme Factom (en partenariat avec HealthNautica) ou BitHealth, offrent d'ores et déjà de tels services. Des archives sécurisées et cryptées, accessibles exclusivement au détenteur de la clé privée correspondant, pourraient bien répondre aux exigences de sécurité et de confidentialité du secteur de la santé. BlockVerify propose une solution d'authentification cryptée basée sur la blockchain pour lutter contre la contrefaçon de médicaments. La rumeur (tweets) dit que Philips Healthcare Group, un acteur majeur

du secteur, collabore avec la start-up Tierion sur un premier projet blockchain. DNA.bits associe big data et DLT pour stocker et partager des données génétiques authentifiées et les dossiers cliniques correspondant tout en garantissant un maintient absolu de l'anonymat.

Dans le secteur de l'éducation, Holberton Software engineering school, basée à San Francisco, et l'École Supérieure d'Ingénieurs Léonard-de-Vinci (ESILV) en France ont annoncé leur intention d'enregistrer et d'authentifier leurs certificats académiques sur la blockchain Bitcoin, tandis que l'Université de Nicosie, à Chypre, a lancé un Master's of Science en Monnaie Digitale dans le cadre de la politique chypriote visant à faire de cet état insulaire une plaque tournante pour "le négoce, le traitement et les activités bancaires libellés en Bitcoin.[7] "

La Blockchain sert également de base à des initiatives dans le secteur humanitaire. Le *Blockchain Emergency ID (BE-ID) Project*, porté par BitNation Refugee Emergency Response (BRER), est une initiative visant à fournir aux réfugiés, Syriens et autres, des documents d'identité numérique conformes aux normes des Nations Unies en matière de documents de voyage destinés aux apatrides. BitNation fournit également d'autres services aux réfugiés, notamment une Carte Visa BitNation permettant le paiement en bitcoins (BitNation Bitcoin Visa Card).

Dans le domaine du commerce électronique, OpenBazaar, une plateforme d'e-commerce venant tout juste d'ouvrir[8], a pour ambition de devenir un concurrent totalement décentralisé d'eBay. A ce jour, OpenBazaar fonctionne exclusivement en bitcoins. Overstock.com, géant américain du commerce électronique, travaille en collaboration avec la start-up CounterParty au lancement de Medici, une plateforme boursière de crypto-monnaies développée sur la blockchain. Visa[9] serait en train de tester la DLT pour ses services de paiement, alors qu'une banque coréenne, KB Kookmin Bank,[10] a fait savoir qu'elle était en train de développer une solution DLT via la Blockchain pour ses opérations de transferts de fonds, actuellement réalisées via SWIFT[11]. Dans le domaine de la logistique et du financement des échanges commerciaux, Skuchain[12] propose des solutions à base de DLT pour le commerce B2B et son financement.

Enfin, la DLT a suscité un énorme intérêt de la part du secteur financier où l'on trouve d'innombrables projets. Une initiative sectorielle comme le groupement bancaire R3 CEV[13], lancé en septembre 2015, développe des prototypes basés sur Ethereum[14] et a engagé des développeurs reconnus comme Richard Brown, ex-directeur de IBM, et Mike Hearn, cité plus haut. R3 CEV est également l'un des 30 membres fondateurs du Hyperledger Project, une initiative intersectorielle de la Linux Foundation, dont la mission est de développer des alternatives aux blockchains Bitcoin et Ethereum[15].

Digital Asset Holdings (DAH), lancée en mars 2015 par Blythe Masters, ancienne directrice du département des matières premières au niveau mondial chez JP Morgan, bâtit actuellement un système de traitement de transactions fondé sur la DLT pour des institutions financières comme la Australian Stock Exchange (ASX)[16]. DAH fait déjà figure d'acteur dominant dans cette industrie naissante, collaborant avec des acteurs d'envergure comme Accenture, PWC and Broadridge, afin de développer ses activités internationales. Il est intéressant de noter qu'en tant que membre fondateur de

l'initiative, Digital Asset Holdings a offert à la Linux Foundation la marque *Hyperledger*, acquis une année auparavant en même temps que la start-up éponyme. Deloitte Canada et Deloitte Luxembourg travaillent ensemble sur Rubix, un projet qui pourrait à terme permettre à leurs clients de développer leurs propres applications DLT reposant sur des *smart contracts*.

Nasdaq propose actuellement un dispositif DLT de vote d'actionnaires pour les e-résidents estoniens et développe par ailleurs un projet DLT pour l'enregistrement et le transfert de valeurs non-cotées, en complément d'ExactEquity, leur solution *cloud* de gestion d'actifs. Intel serait en train de tester la technologie blockchain en développant un jeu vidéo. Les joueurs possèdent des parts dans des équipes de football américain[17] et peuvent se les échanger sur une plateforme blockchain. Ce projet n'est pas commercialisé et sert de prototype dans le cadre du programme Hyperledger.

Les acteurs de l'infrastructure post-marché ont créé le groupe de travail *Post Trade Distributed Ledger Working Group*, dont les membres actuels sont : CME Group, Euroclear, LCH.Clearnet, the London Stock Exchange, Société Générale et UBS. A titre individuel, Euroclear et Depository Trust & Clearing Corporation (DTCC) ont chacun publié leur propre rapport, à quelques jours d'intervalle. DTCC "appelle à une collaboration transversale qui mise sur la DLT pour moderniser, rationaliser et simplifier l'organisation de l'infrastructure du secteur financier et pallier les limitations actuelles du processus post-marché" [18]. Euroclear (février 2016), de son côté, déclare que "l'industrie a besoin de définir une position collective sur le potentiel de cette technologie" et de "travailler avec les innovateurs pour développer des normes tout en préservant les atouts actuels de l'écosystème, et en naviguant dans les mondes complexes de la régulation et du contrôle".

Pour ces acteurs, les principaux avantages de la DLT sont la transparence, la sécurité, la traçabilité et un rapport coût/efficacité favorable. Et comme ces quatre caractéristiques sont également les qualités requises pour une industrie financière solide et efficace, il n'est pas étonnant qu'elles constituent une forte incitation à investir en DLT.

Mais avant d'analyser l'impact de la DLT sur l'infrastructure des marchés financiers et d'évaluer le coût potentiel de la transformation technologique, commençons par regarder les solutions existantes qui s'offrent au secteur.

1.2. Bases de données partagées et protocoles de consensus distribués : un phénomène vraiment nouveau pour le secteur financier ?

Les technologies de l'information ont joué un rôle déterminant dans le développement des services financiers modernes. Comme Shiller le remarque (2003), ce sont bien les innovations informatiques qui ont permis la prolifération de la majorité, sinon de la totalité, des services financiers contemporains. Les nouvelles technologies ont métamorphosé l'infrastructure de l'information et ont changé la donne pour les fournisseurs de services financiers et les marchés des capitaux, en transformant les innombrables piles de papier (difficiles à trier, traiter et archiver) en données numériques. Cette capacité à mieux gérer des volumes importants de données et

d'informations a permis au secteur bancaire d'élargir son offre de produits et de services, d'améliorer ses procédures et de suivre le nombre croissant des transactions auquel les institutions doivent faire face[19]. Aujourd'hui, que ce soit dans le domaine de la titrisation, des produits dérivés ou encore au niveau de la banque commerciale, l'activité du secteur financier repose fortement sur les systèmes d'information.

Il n'est donc pas étonnant que les banques mettent l'accent sur la constitution d'équipes informatiques performantes, surtout dans un monde où la *cybersécurité* est vitale pour le fonctionnement du système bancaire. Jusqu'à présent, le secteur financier privilégiait des architectures informatiques centralisées, devenues un genre de choix par défaut. Des banques centrales jusqu'aux agences de détail, ce paradigme a produit une succession de relations client-serveur, où à chaque niveau, un serveur centralisé (ou ensemble de serveurs fédérés[20]) prend en charge de multiples clients et leurs opérations. Ce choix est logique : une banque centrale veut pouvoir suivre les banques agréées auxquelles elle donne sa monnaie, tandis qu'une banque de détail veut garder le contrôle sur ses comptes clients et pouvoir suivre leur activité.

Aujourd'hui, le modèle centralisé l'emporte dans tous les contextes où l'on a besoin d'un système de tenue des registres fiable ; et pour lequel la sécurité et le contrôle sont vitaux. Pour prendre un exemple hors secteur bancaire, on constate un accroissement important des données biométriques de part le monde au fur et à mesure que les états remplacent les passeports traditionnels par de nouvelles technologies d'identification des citoyens. Ici aussi, les données sont stockées dans d'immenses bases de données centralisées, bien que les questions de la sécurité de ces données hautement sensibles soient vitales ; en effet, tout vol d'identité pourrait s'avérer catastrophique.

Alors, si les registres de données numériques existent depuis plusieurs décennies[21], qu'est-ce qui explique l'engouement soudain pour la technologie des bases de données distribuées (DLT) ? Les partisans de la Blockchain et de la DLT mettent en avant trois faiblesses potentielles des bases centralisées contrôlées par un *tiers de confiance* : (i) le tiers de confiance pourrait s'avérer moins digne de confiance que l'on escomptait, voire faire l'objet de pots-de-vin ou d'autres formes de corruption; (ii) le contrôleur du registre centralisé pourrait censurer ou rejeter certains acteurs du marché pour des motifs subjectifs et/ou discriminatoires; (iii) des bases de données centralisées ne sont pas à l'abri d'une perte de données. La Blockchain, grâce à sa structure décentralisée, ses protocoles de consensus distribués, son approche *open-source* et les multiples copies de la Blockchain accessible à tous, apporte une réponse à toutes ces questions[22].

Mais au-delà de ces considérations, somme toute opérationnelles, il y a une force à l'œuvre dans le secteur financier qui explique l'intérêt grandissant pour la DLT et la perspective réelle d'un abandon des architectures centralisées en faveur du modèle distribué : la montée du "*shadow banking*" (la finance parallèle) et le phénomène croissant de désintermédiation bancaire qui l'accompagne, incitent certains à proclamer une possible "fin des banques" (McMillan, 2014). Avec la finance numérique, le *crowdfunding* et les prêts P2P, emprunteurs et prêteurs peuvent se rencontrer sans recourir à l'intermédiation bancaire (Collomb, 2015). Mais tous dépendent encore de plateformes centralisées. DLT, en revanche, permet de se passer totalement

d'intermédiaire central, que ce soit une banque ou une plateforme numérique centralisée ! Prenons comme exemple le cas bien connu du marché des taxis et des VTC : si Uber propose à ses clients une plateforme numérique uber-conviviale qui facilite grandement la rencontre de l'offre et de la demande via une application smartphone, toutes les données transactionnelles terminent sur une base de données centralisée, contrôlée par Uber. Avec la Blockchain et la DLT, il n'y a plus de plateforme centralisée.

DLT attire différents acteurs avec la promesse "d'ubériser Uber", c'est-à-dire la perspective de pouvoir abandonner l'architecture centralisée en faveur d'une architecture véritablement décentralisée où le système dans son intégralité joue le rôle de tiers de confiance à la place d'un acteur central dominant. Mais comme la DLT est conceptuellement complexe et encore à ses débuts, les acteurs économiques et financiers ont encore du mal à distinguer entre mythes et réalités, et à y voir clair dans ses applications potentielles.

Mais voilà : si jusqu'à présent, l'idée même que des banques puissent partager des informations via des protocoles de consensus distribués, était considérée comme aberrante par la plupart des interlocuteurs du secteur financier, l'intérêt grandissant pour la DLT a changé la donne. L'industrie porte désormais un regard plus ouvert sur le partage des données via des plateformes distribuées et la perspective d'un changement de paradigme se manifeste dans des initiatives comme R3 CEV et d'autres citées plus haut.

2. Principales caractéristiques de la DLT

2.1. Histoire du Bitcoin / de la Blockchain

Bitcoin est la première crypto-monnaie effectivement mise en circulation sans autorité centrale ni intermédiaire. Bien que d'autres crypto-monnaies circulent depuis des décennies, à l'instar des initiatives eCash et Digicash de David Chaum (1981, 1983), aucune avant le Bitcoin n'avait encore trouvé le moyen de créer un système de paiement sécurisé et une monnaie virtuelle sans recourir à un tiers de confiance. Tous les systèmes antérieurs à Bitcoin sans exception ont eu besoin d'un tiers de confiance pour vérifier que la monnaie numérique en circulation n'avait pas déjà été dépensée, une problématique qui n'existe pas pour une monnaie physique. Dans le livre blanc de 2008 où il présente Bitcoin, Satoshi Nakamoto (un pseudonyme), propose la première solution fonctionnelle au problème de "double dépense" jamais publiée. Il fait référence à plusieurs développements informatiques et cryptographiques de la fin du 20e siècle[23] :

(i) **Les fonctions de hachage cryptographique**, ou ***cryptographic hash functions***, qui ont été rendues possibles par le travail novateur de Diffie et Hellman intitulé *New directions in cryptography* (1976) présentant le concept de cryptographie à clé publique[24] ; la recherche de Rabin sur les signatures numériques, *Digitalized signatures* (1978) ; la réponse de Yuval à Rabin "How to swindle Rabin" (1979) ; et le rapport de Merkle intitulé *Secrecy, Authentication and Public Key Systems* (1979).

(ii) **Le mécanisme d'enchaînement chiffré des blocs**, ou ***cipher block chaining (CBC)***, détaillé dans FIPS PUB 46 (US Federal Information Processing Standards Data Encryption Standard) et approuvé comme norme fédérale (U.S.) en 1976, qui a été développé conjointement par IBM et la National Security Agency (NSA) dans les années 70 en réponse à un appel à projets d'algorithmes cryptographiques du gouvernement des États-Unis. FIPS et DES ont été développés par le gouvernement américain pour protéger les données sensibles mais non-classifiées. Ils sont virtuellement *open-access* (peuvent être utilisés sans payer de redevance) ce qui s'approche de la philosophie à la base du protocole Bitcoin.

(iii) **La preuve de travail**, ou ***proof-of-work***, qui a été introduite par Cynthia Dwork et Moni Naor dans un rapport publié en 1993, *Pricing via Processing or Combatting Junk Mail*, où elles proposent de combattre le *spam* (courrier indésirable) en augmentant son coût. "L'idée principale est d'obliger un utilisateur à résoudre une fonction suffisamment difficile mais pas insoluble avant d'accéder à la ressource, ce qui décourage une exploitation futile ou malicieuse [de la ressource]." Adam Back a poussé le concept plus loin avec son système *proof-of-work* Hashcash dont le but est de limiter le *spam* et les attaques DoS (*denial-of-service* ou par déni de service). Adam Back a annoncé Hashcash en mai 1997 à la liste de diffusion cypherpunks@toad.com[25] avant de le publier officiellement en 2002.

(iv) **Le mécanisme de compression par l'arbre de Merkle,** ou ***Merkle Tree compression* mechanism**, qui a été inventé en 1979 par Ralph Merkle. Il est utilisé pour stocker et vérifier un grand volume de données efficacement et de manière sécurisée, et employé par le protocole Bitcoin pour calculer la racine de Merkle de toutes les transactions contenues dans un bloc de données.

(v) **L'horodatage**, ou ***timestamping***, qui est une pratique séculaire dans sa forme physique. Son avatar numérique a été mis au point dans les années 90 pour les besoins des protocoles de sécurité informatique (Une, 2001).

(vi) **La technologie pair-à-pair,** ou **peer-to-peer (P2P) *technology***, dont la mise en application par Shawn Fanning en juin 1999 pour la plateforme de partage de fichiers audio Napster est bien connue. Malheureusement, Napster fonctionnait avec un serveur central (appelé *farm*) qui jouait le rôle d'un registre centralisé de tous les fichiers appartenant à, ou demandés par les pairs. Ce système centralisé constituait le point unique de défaillance (*Single Point of Failure-SPOF*) de Napster et le site a été fermé par le FBI en 2001 pour violation des droits de propriété intellectuelle. Gnutella[26], un protocole de transfert de fichiers P2P, et la première plateforme complètement distribuée de son genre, a été développé en 2000 par Tom Pepper et Justin Frankel pour Nullsoft.

L'innovation apportée par le Bitcoin réside fondamentalement dans l'association qu'il opère entre diverses avancées technologiques du domaine informatique, comme les protocoles pair-à-pair et les fonctions cryptographiques. S'il est vrai que le Bitcoin et la Blockchain constituent un phénomène encore récent, nous pensons néanmoins que les développements de la technologie des registres distribués amèneront un changement de paradigme ouvrant la voie à de nouvelles structures autonomes pour l'échange, l'authentification, la certification, et le règlement de données transactionnelles.

Le Bitcoin, base de données distribuée, transférable et immuable, a ouvert la voie à la multiplication d'applications pratiques et d'innovations technologiques complémentaires enrichissant régulièrement l'espace de la DLT. Le développement des *smart contracts, colored coins, sidechains*, ou de mécanismes d'incitation alternatifs au *proof-of-work*, tel le *proof-of-stake*, en sont des exemples. Certains de ces développements ont déjà été déployés chez des acteurs économiques traditionnels. Ainsi, la plateforme Ethereum, proposant un protocole de gestion de registres distribués, une chaîne de blocs et une crypto-monnaie alternatifs à celle du Bitcoin, a déjà forgé des partenariats avec des acteurs technologiques établis comme Microsoft, pour le développement de sa Machine Virtuelle (*Virtual Machine*).

Curieusement, certaines innovations existent depuis des décennies. Par exemple, Nick Szabo travaille au développement des *smart contracts* et des *colored coins* depuis 1998[27], et a publié un premier papier sur le sujet en 2001[28, 29]. Il explique que les *smart contracts* peuvent rendre des contrats pratiquement inviolables : si les *smart contracts* étaient "embarqués un peu partout", c'est-à-dire dans le "matériel informatique et dans les logiciels dont nous nous servons", ils "augmenteraient le coût du non-respect contractuel jusqu'à le rendre prohibitif pour la partie en défaut". Szabo appelle les *colored coins* "*proplets*" ou "dispositifs pour contrôler des actifs" ; il pense que ces mécanismes forment "le système de sécurité de base nécessaire pour le recueil de preuves, le respect, et la négociation des droits [de propriété, contractuels, et de responsabilité civile]".

Un certain nombre d'Organisations Autonomes Distribuées ou DAOs (*Distributed Autonomous Organizations*) sont actuellement en cours de déploiement. Le concept de DAO a été présenté par Vitalik Buterin, co-fondateur d'Ethereum, en 2014, basé sur l'idéal utopiste de Friedrich von Hayek (1979) et sa théorie de l'ordre spontané (Zacklad, Sok, 2015). Il procède également d'une conception alternative de la sécurité selon laquelle un système autonome offre toujours une protection supérieure à celle que procure traditionnellement une autorité centrale – comme un gouvernement – aux citoyens et aux organisations qu'elle gouverne. Ainsi, dans sa publication sur les *proplets* (2001), Nick Szabo affirma que "le terme *tiers de confiance* est un joli synonyme de faille de sécurité béante qu'un développeur choisit d'ignorer. En développant des proplets, nous nous attachons tout particulièrement à éliminer ces risques."

2.2. DLT : concepts clés

Dans cette section, nous présentons les concepts clés qui sous-tendent la DLT dans sa manifestation la plus usitée, le réseau Bitcoin et sa Blockchain.

Un réseau distribué et décentralisé à la place d'une autorité centrale

Le réseau Bitcoin est composé de milliers de nœuds certifiant la validité de ses transactions. Ils communiquent à travers un protocole pair à pair (P2P) permettant à n'importe quel ordinateur du réseau d'échanger des informations, directement ou indirectement. La distribution du réseau lui donne plus de résilience qu'une base de données centralisée ne pourrait en avoir : si une partie des nœuds du réseau venaient à être défectueux, cela n'affecterait pas son fonctionnement général. Ce qui n'est pas le cas d'une architecture client-serveur qui serait impactée par le dysfonctionnement du serveur central. Notons qu'une clé privée est générée par une fonction aléatoire sécurisée de façon cryptographique de 256 bits[30]. Ce n'est pas anodin. La probabilité que deux utilisateurs finissent par avoir la même adresse est ainsi quasi nulle, malgré le fait que ces adresses soient générées de façon décentralisée[31].

Un système pseudonyme

Le réseau Bitcoin est souvent critiqué du fait qu'il permette à ses utilisateurs d'être anonymes, caractéristique perçue comme facilitant le blanchiment d'argent et l'évasion fiscale. Il est important de comprendre que chaque nouvelle adresse bitcoin générée est dérivée d'une clé publique, elle-même résultant d'une clé privée via une transformation cryptographique. Et donc remonter de l'adresse bitcoin à son propriétaire n'est pas simple, même si ce n'est pas non plus impossible.[32] Et aujourd'hui si la plupart des places d'échange bitcoin demandent pièces d'identité et justificatifs de domicile à leurs clients, il est encore facile de créer des adresses bitcoin dans un e-wallet, auquel cas relier l'adresse bitcoin ainsi créée à son propriétaire n'est pas aisé.[33]

Irréversibilité des transactions

Cet aspect de la DLT est à la fois perçu comme un avantage et la source de nombreuses critiques. Une fois validée dans la Blockchain, une transaction bitcoin ne peut pas être annulée. Cette irréversibilité des transactions est considérée comme un point positif par les commerçants acceptant les bitcoins. En effet, elle élimine le risque que des clients malveillants annulent leur transaction alors qu'ils ont reçu le bien ou service vendu. En un sens, ce système est une façon d'éliminer potentiellement le risque de contrepartie, puisqu'une transaction ne sera validée qu'à condition que l'acheteur payant en bitcoins ait effectivement les fonds disponibles à transférer au vendeur de biens ou services. Une bonne pratique consiste à attendre la validation de six blocs (ce qui prend environ une heure) avant de considérer une transaction comme entérinée de façon irréversible.

Une génération monétaire programmée et limitée

Le Bitcoin est une crypto-monnaie dont la génération est déterminée à l'avance et dont le montant total est limité à 21 millions d'unités. La "création monétaire" est programmée dans le protocole même du Bitcoin. Elle n'est donc pas le fruit du jugement d'une banque centrale et de ses projections macro-économiques. Jusqu'en 2016, 25 bitcoins seront générés par bloc de transactions validé, et le rythme de création sera divisé par deux environ tous les quatre ans : ainsi, nous aurons 12,5 bitcoins par bloc de 2016 à 2020, et ainsi de suite, jusqu'à ce que la limite des 21 millions de bitcoins soit atteinte. C'est pourquoi le minage de bitcoins, rémunéré par ces nouvelles unités créées est souvent comparé à l'extraction aurifère dont les

ressources en or sont limitées et dont le coût marginal d'extraction augmente avec le temps : le travail d'extraction aurifère devient de plus en plus difficile, et de plus en plus coûteux, alors que les réserves de minerai diminuent.

Cryptographie

La cryptographie est utilisée à différents niveaux. Au sein du protocole Bitcoin, des procédés cryptographiques sont utilisés pour : (i) générer les clés publiques à partir des clés privées par l'utilisation de courbes elliptiques de chiffrage, à partir du standard secp256k1 tel que défini par le *National Institute of Standards and Technology* (NIST) ; (ii) calculer l'adresse bitcoin de la clé publique par un double hachage de cette dernière, via la fonction à sens unique SHA256 puis RIPEMD160 ; (iii) fournir une signature digitale qui sera utilisée dans un script débloquant la transaction permettant le transfert des fonds vers une adresse bitcoin spécifique ; (iv) calculer l'empreinte (*hash*) d'un bloc valide en faisant varier un *nonce* – étape clé du "minage" ; (v) dans d'autres situations où des empreintes doivent être calculées, notamment lors de la génération de la racine de Merkle d'un ensemble de transactions.

Mécanismes de consensus et d'authentification

Le protocole Bitcoin a permis de résoudre un problème ancien en informatique distribuée qui est le problème des généraux byzantins (Lamport et al., 1982). En bref, ce problème consiste à voir si, et dans quelles conditions, différents généraux seront capables de s'accorder sur un plan coordonné (un "consensus") sachant qu'il peut y avoir des traîtres parmi eux et que leurs communications peuvent être potentiellement interceptées et corrompues.
Il existe différents paradigmes d'authentification de la validité des transactions, utilisés pour établir un consensus et s'assurer de l'immuabilité de la chaîne de blocs, parmi lesquels :

- La *proof-of-work (PoW)*, ou preuve de travail (utilisée pour le minage bitcoin) ;
- La *proof-of-stake (PoS)*, ou preuve de participation ;
- La *zero-knowledge-proof*, ou preuve à divulgation minimale.

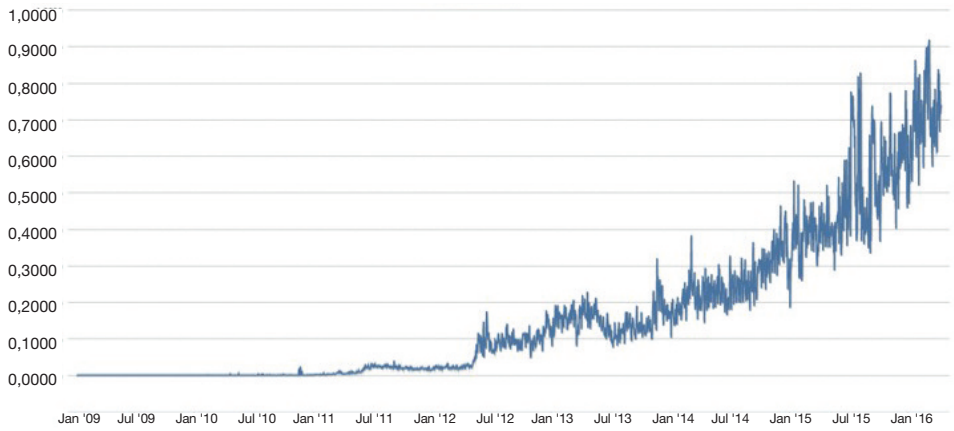
La *proof-of-work* est l'approche la plus commune. Elle est utilisée dans le protocole Bitcoin et permet de vérifier que tout mineur ajoutant un bloc à la Blockchain a résolu un problème cryptographique au préalable. Le mineur, afin de voir son bloc validé dans la chaîne, doit prouver que ce travail a été réalisé. La difficulté du problème à résoudre s'ajuste de façon dynamique par le protocole Bitcoin. Le travail consiste à faire varier tous les nonces possibles afin de trouver l'empreinte (*hash*) correspondant au bloc que le mineur cherche à certifier. Cette empreinte prendra la forme d'une suite de chiffres commençant par un certain nombre de zéros (ce qui revient à trouver un hash plus petit qu'une certaine valeur donnée). Plus il y a de zéros, plus la difficulté à miner est grande, et *vice versa*. La *proof-of-stake (PoS)* est une méthode qui demande aux utilisateurs souhaitant valider des transactions la preuve qu'ils possèdent un certain montant, une certaine part (*stake*), de la crypto-monnaie circulant sur le réseau. Enfin, la *zero-knowledge proof* est une méthode reposant sur la capacité d'une partie (le *prover*) à prouver à une autre contrepartie (le *verifier*) qu'une déclaration est vraie, en ne donnant aucune autre information que le fait que cette déclaration est vraie. Nous n'élaborerons pas sur les avantages et les inconvénients de ces approches. Il est cependant important de comprendre que le Bitcoin utilise la PoW et qu'Ethereum, actuellement en PoW, a déclaré considérer une transition vers la PoS.

3. Débats technologiques

3.1. La controverse de la taille du bloc

La question de la taille du bloc a donné lieu à un débat très vif au sein de la communauté Bitcoin, cette problématique étant étroitement liée pour beaucoup au débit potentiel et aux perspectives de croissance du réseau. Le protocole Bitcoin actuel définit la taille d'un bloc à 1 Mo. Jusqu'à fin 2012, les blocs n'excédaient en général pas 200 ko, mais la taille moyenne d'un bloc a progressivement commencé à augmenter à partir de début 2013. A l'heure de la rédaction de ce rapport, la moyenne glissante sur 7 jours était à 0,75 Mo, avec un nombre croissant de blocs de taille excédant 0,9 Mo. Cette tendance n'est pas passée inaperçue aux yeux de certains développeurs, qui ont commencé à craindre une saturation du réseau.

Figure 1 : Average block size



Il y a essentiellement deux façons de mettre à jour le protocole Bitcoin : les *hard forks* (une "fourche", au sens d'embranchement ou d'évolution, abrupte) et les *soft forks* (une évolution graduelle). Une *hard fork* est un changement fondamental du protocole tel qu'une reconfiguration du format des blocs, ou une nouvelle spécification des transactions admissibles par le réseau. Une *hard fork* ne permettra pas aux anciennes versions du protocole de fonctionner avec les nouveaux standards, forçant tous les utilisateurs du réseau désireux de continuer à participer à cette mise à jour. Une *soft fork*, à l'opposé, permettra une telle compatibilité entre l'ancien et le nouveau : les nœuds du réseau fonctionnant encore sur la version précédente pourront continuer à valider de nouvelles transactions (les nœuds du réseau fonctionnant avec le nouveau protocole rejetteront par contre l'ancien format). Une *soft fork* se mettra donc progressivement en place avec une mise à jour des différents nœuds du réseau et le

fonctionnement du réseau ne sera pas perturbé puisqu'ancienne et nouvelle versions pourront coexister jusqu'à ce que tous les nœuds basculent finalement vers le nouveau format[34]. Une *hard fork*, ne permettant pas cette dissémination progressive du nouveau au sein de l'ancien, nécessitera un *upgrade* simultané de tous les acteurs du réseau une fois le nouveau format décidé.

En juin 2015, Gavin Andresen, l'un des développeurs Bitcoin, publia une nouvelle proposition d'amélioration du protocole (un *Bitcoin Improvement Proposal* ou *BIP 101*) en faveur du remplacement de la taille maximale de bloc à 1 Mo par une taille maximale qui croîtrait au cours du temps avec un taux de croissance prédéterminé (la taille maximale serait passée à 8 Mo en janvier 2016, et aurait doublé tous les 2 ans par la suite jusqu'en 2036 pour arriver à environ 8,1 Go). Lui, et d'autres développeurs actifs de la communauté suggérèrent que les *mineurs* pourraient choisir d'installer la nouvelle version du protocole jusqu'à ce qu'elle soit disséminée sur 75% du réseau (seuil à partir duquel on donnerait deux semaines supplémentaires aux derniers 25% du réseau pour *upgrader* ou bien sortir du réseau - une *hard fork* à ce stade). Cette proposition de changement ne fut pas suivie par la majorité de la communauté, amenant une figure connue des cercles Bitcoin qui lui était favorable, Mike Hearn, à déclarer publiquement que l'expérience "Bitcoin était un échec".

Ce sont surtout les arguments avancés par chaque partie dans ce débat qui sont intéressants, ainsi que ce que cette controverse révèle sur la gouvernance du réseau Bitcoin.

D'un côté, les partisans d'une augmentation de la taille des blocs avancent que sans une telle action, le réseau risque de saturer rapidement, et qu'il faut de plus augmenter la capacité transactionnelle du réseau si l'on veut espérer pouvoir lui permettre un jour de concurrencer les réseaux de cartes de crédit[35].

D'un autre côté, les partisans du status quo invoquent le besoin de préserver la stabilité du réseau, et la nécessité d'éviter tout changement qui risquerait d'augmenter la concentration du *minage*. Beaucoup pensent qu'une augmentation de la taille du bloc, avec l'augmentation des ressources de mémoire et de calcul qu'elle induirait pour les nœuds du réseau, se traduirait par davantage de concentration du *minage* à un moment où certains s'inquiètent déjà des collusions dues au développement croissant des *pools* de minage. D'autres avanceront que le réseau Bitcoin ne devrait pas être utilisé pour des micro-paiements triviaux, et que le cœur des données de la Blockchain devrait porter sur l'authentification et la certification des actes et des documents. Enfin, d'autres encore rappelleront qu'il vaut mieux garder cette contrainte de taille de bloc comme un obstacle devant stimuler la créativité des développeurs, plutôt que d'enlever cette contrainte. [36]

Cette controverse technique est complexe mais nous pensons pour notre part qu'il est encore essentiel à ce stade de préserver une certaine unité dans la communauté Bitcoin, elle-même essentielle pour préserver la crédibilité du réseau. Il est également important de maintenir un niveau minimum de décentralisation qui est un concept essentiel de ce réseau qui prétend justement n'être contrôlé par personne et se passer de tiers de confiance.

3.2. Une brève typologie des registres distribués et des crypto-monnaies

Il paraît tout à fait normal qu'un protocole *open source* tel que Bitcoin, mis en place à partir du livre blanc de Satoshi Nakamoto, inspirerait d'autres initiatives similaires. Et effectivement, une multitude de crypto-monnaies alternatives (à Bitcoin), des *alt coins*, virent le jour dans le sillage du protocole Bitcoin.[37] Mais malgré la prolifération des initiatives, la valeur de marché des crypto-monnaies demeure très concentrée avec un total de €7,8 milliards au 4 avril 2016. Parmi plus de 700 crypto-monnaies listées sur Coinmarketcap, seules quatre disposaient d'une capitalisation supérieure à €100 millions : Bitcoin, Ethereum, Ripple et Litecoin. Ensemble elles représentaient €6,8 milliards ou environ 95% du total des crypto-monnaies. Et parmi ces quatre crypto-monnaies, Bitcoin avait la part du lion (79% du total) suivie par Ethereum (11%), Ripple (3%) et Litecoin (2%)[38].

Nous suivons pour l'essentiel de la suite de cette section la taxonomie proposée par Antonopoulos (2015) pour classer ces différentes crypto-monnaies, et les registres distribués dans lesquels elles s'inscrivent.

Les plateformes de *meta-coins*

Plusieurs couches protocolaires ont été implémentées au-dessus du Bitcoin, permettant d'avoir une "crypto-monnaie à l'intérieur d'une crypto-monnaie", ou un méta-niveau. Ainsi les *colored coins* ("des jetons de couleur") sont définis à partir de méta-protocoles qui surimposent de l'information dans des transactions de petits montants bitcoins, cette information désignant et renvoyant en fait à un autre type d'actif digital.

Jetons alternatifs (*alt coins*) et chaînes/registres alternatifs (*alt chains*)

Ce sont pour l'essentiel des alternatives aux jetons bitcoins, qui utilisent leurs propres registres distribués, complètement séparés de la Blockchain. La plupart de ces *alt coins* ont vu le jour suite à des bifurcations (des *forks*) par rapport au code source du Bitcoin même si certains ont été codés de zéro, le plus souvent lorsqu'ils ont été pensés pour des applications spécifiques. La distinction principale à garder en tête est qu'en général un *alt coin* sera principalement utilisé comme une crypto-monnaie alternative au Bitcoin, alors que des chaînes/registres alternatifs auront été conçus pour des applications spécifiques.

Parmi les registres alternatifs, nous mentionnerons ici Namecoin et Ethereum. Namecoin est considéré comme la première bifurcation du Bitcoin et suit pour l'essentiel les mêmes paramètres. Namecoin est "un registre décentralisé et une plate-forme de transferts qui se sert d'une blockchain", et est aujourd'hui utilisé comme système d'administration des noms de domaines ayant pour suffixe ".bit" (Antonopoulos, 2015). Ethereum de son côté est une "plate-forme décentralisée qui permet l'exécution de *smart contracts* : des applications qui s'exécutent exactement comme elles sont programmées, sans possibilité de temps mort, de censure, de fraude ou d'interférence d'un tiers[39]." Ethereum ambitionne de devenir une machine virtuelle globale et utilise l'*ether* comme crypto-monnaie.

Registres publics ou privés

Il est important de différencier les registres distribués publics, tels que la Blockchain, des registres dont l'utilisation nécessite une autorisation, aussi appelés chaînes privées. En suivant la typologie fournie par Vitalik Buterin (2015)[40], l'un des co-fondateurs d'Ethereum, nous distinguerons entre des chaînes publiques, des chaînes dites de consortium, et des chaînes privées. Les chaînes/registres publics sont ouverts à tous pour lire/écrire des transactions valides, et participer au mécanisme de consensus. Les blockchains de consortium sont des blockchains où le consensus est établi et contrôlé par un ensemble pré-sélectionné de nœuds du réseau ; "le droit de lire la blockchain peut être ouvert à tous, ou restreint aux participants [du consortium], et il peut aussi y avoir des situations hybrides où les empreintes racines des blocs seront publiques, avec une API qui permettra au public externe d'effectuer un nombre limité de requêtes et d'obtenir des preuves cryptographiques de certains contenus de la blockchain." Quant à une blockchain complètement privée, il s'agira "d'une blockchain où les permissions d'écriture sont réservées à une organisation centrale, les permissions de lecture pouvant être accordées au public ou limitées à divers degrés." Une entreprise pourra souhaiter utiliser une blockchain privée pour des applications de gestion de base de données ou d'audit interne, et par conséquent il sera en général inutile dans ces contextes d'avoir des droits de lecture ouverts au public, même si d'ouvrir la blockchain à la consultation extérieure sera parfois souhaitable dans certaines situations où l'entreprise voudra par exemple mettre en valeur la transparence de ses comptes ou de ses opérations.

Nous n'approfondirons pas dans cette étude la distinction entre blockchain de consortium et blockchain privée mais le lecteur devrait garder en tête qu'une blockchain de consortium semble un bon compromis entre le modèle décentralisé et sans confiance d'une chaîne publique, et le paradigme centralisé et dépendant d'un tiers de confiance d'une chaîne privée. Il faut aussi remarquer que les avantages d'avoir une structure de blockchain dans un contexte complètement privé ne sont pas évidents ; ils semblent essentiellement limités à la protection des données qu'un chaînage cryptographié de blocs permet[41].

Sur le débat entre blockchain privée et blockchain publique, Buterin identifie cinq avantages des registres privés par rapport aux registres publics: (i) ils permettent la réversibilité des transactions, l'ajustement dynamique des règles, et l'annulation des transactions indésirables (par exemple criminelles) ; (ii) ils débarrassent du risque d'attaque des 51% puisque les *mineurs/nœuds validateurs* du réseau sont identifiés ; (iii) ils diminuent les coûts de transaction, puisque les transactions doivent simplement être vérifiées par quelques nœuds présélectionnés ; (iv) comme les nœuds du réseau sont a priori de confiance et très bien connectés entre eux, les participants d'une chaîne privée devraient être capables de corriger rapidement des erreurs via une intervention manuelle, et l'établissement du consensus devrait être obtenu après des temps beaucoup plus courts ; (v) si les droits de lecture sont restreints, les registres privés protègent la confidentialité des données.

Cela étant dit, les avantages d'une chaîne publique sur une chaîne privée sont en général de deux types : (i) les chaînes publiques résistent à la censure et protègent leurs utilisateurs de toute forme de contrôle centralisé, et des malversations toujours possibles des agents du tiers centralisé ; (ii) les chaînes publiques sont ouvertes, et donc susceptibles d'être utilisées par le plus grand nombre et de bénéficier d'un fort effet de réseau.

Il est aussi possible de créer des combinaisons hybrides entre des blockchains publiques et privées, par exemple en utilisant des *smart contracts* administrés de manière privée sur des blockchains publiques, ou en établissant des interfaces d'échange trans-chaîne entre blockchains privée et publique. De manière générale, il est difficile de trancher sur le type de blockchain à mettre en place : cela dépend essentiellement du secteur industriel et du type d'application considérés, et bien sûr du degré de confidentialité nécessaire pour les données manipulées.

Sidechains

Les *sidechains* (ou chaînes auxiliaires) existent et fonctionnent de pair avec la blockchain principale, à ce jour la Blockchain, plutôt que d'être indépendantes. Elles bénéficient du réseau de la blockchain principale, à laquelle elles s'adossent, en établissant une correspondance fixe entre les actifs digitaux qu'elles portent et leurs valeurs en bitcoins (on parle alors de *pegged assets*). Ces sidechains doivent "permettre aux bitcoins et autres actifs digitaux inscrits sur les registres d'être échangés entre plusieurs blockchains" et "donner aux utilisateurs l'accès à d'autres crypto-monnaies à partir de celles qu'ils possèdent déjà". En se référençant au bitcoin comme crypto-monnaie d'échange, ces systèmes "peuvent interagir entre eux plus facilement, et avec le réseau Bitcoin, et réduire les problèmes de liquidité et les fluctuations de marché associées avec les nouvelles crypto-monnaies les moins utilisées. Comme ces sidechains sont des systèmes séparés, ils permettent l'innovation technique et économique. Et malgré la possibilité de transferts bi-directionnels, elles isolent les risques : en effet, dans le cas d'une faille de sécurité (cryptographique ou d'architecture), les dégâts restent confinés à la sidechain elle-même" (Back et al., 2014)[42]. Il faut noter qu'aujourd'hui des plateformes de développement *open source* existent pour mettre en place des *sidechains,* ou des blockchains privées capables d'interagir avec le réseau Bitcoin[43].

Ethereum

Ce système de registre distribué a été conçu complètement séparément du Bitcoin même si bien sûr il reprend certains concepts clés du protocole. Ethereum se présente comme "une plate-forme décentralisée sur laquelle tournent des smart contracts : des applications qui s'exécutent exactement comme elles ont été programmées, sans possibilité de temps mort, de censure, de fraude ou d'interférence d'un tiers[44]." Ethereum a "sa propre crypto-monnaie, ou unité de compte appelée l'ether qui doit être dépensée au fur et à mesure de l'exécution du *smart contract*, avec une facturation progressive par le réseau du nombre d'opérations de calcul utilisées par le *smart contract*. La blockchain d'Ethereum enregistre les contrats, exprimés comme un ensemble d'instructions de bas niveau, et dans un langage Turing-complet. En résumé, un contrat est un programme qui tourne sur tous les nœuds du réseau Ethereum. Les contrats portés par Ethereum peuvent stocker des données, envoyer ou recevoir des paiements, stocker de l'ether et exécuter un ensemble infini d'actions de calcul (d'où le système Turing-complet), en opérant comme des agents décentralisés autonomes" (Antonopoulos, 2015). L'une des caractéristiques saillantes d'Ethereum, et qui a généré beaucoup d'intérêt pour cette approche, est que le système offre un environnement de programmation générique de haut niveau, et capable d'exécuter comme un simple *smart contract* ce qui pourrait être fait sinon par une chaîne alternative dédiée.

Ripple

Ce système utilise un mécanisme de consensus différent de la preuve de travail ou de la preuve d'intérêt. L'un des concepts fondateurs est toujours l'idée de se passer d'un intermédiaire qui centraliserait les transactions. Ripple se définit comme une technologie financière distribuée qui "permet aux banques à travers le monde d'effectuer des transactions directement entre elles sans avoir besoin d'une contrepartie centrale ou d'un correspondant intermédiaire[45]." Ripple ambitionne de permettre aux banques de "réduire leurs coûts opérationnels et d'offrir de nouveaux services de paiement transfrontaliers [Ibid]." L'une des caractéristiques clés du système est de permettre un règlement instantané des paiements de banque-à-banque.

La brève typologie précédente montre la diversité des initiatives autour des techniques de registres distribués. Il nous paraît clair à ce jour que ce paysage technologique n'a pas encore atteint sa phase de maturité, et qu'il va continuer à évoluer rapidement à court terme.

4. Peut-on se fier à la technologie des registres distribués ?

La sécurité est un aspect central à traiter dans l'étude de la DLT. Et ce, tout particulièrement pour ses applications dans le domaine financier. Nous distinguerons ici le cas où les registres sont distribués au sein de chaînes de blocs publiques de celui où ils sont distribués au sein d'une chaîne privée.

4.1. Le réseau Bitcoin et la blockchain sont-ils sûrs ?

En termes de sécurité, deux aspects essentiels posent question : (i) l'utilisation de la Blockchain du Bitcoin pour des activités frauduleuses, voire criminelles – une question centrale en matière de mise en application de la loi pour les autorités régulatrices en charge, et (ii) le niveau de sécurité qu'elle offre à ses utilisateurs légitimes.

Le Bitcoin a souffert d'une mauvaise réputation du fait de plusieurs affaires de fraude qui lui ont été associées. Certains ont même annoncé sa fin, du fait de ce marquage négatif. Pour autant, le réseau de transactions électroniques a survécu à ces attaques et s'en est sorti non seulement intact, mais renforcé, puisque ce n'est pas le protocole en soi qui fit défaut, mais plutôt son utilisation[46].

L'histoire des premières monnaies numériques, qui n'utilisaient pas encore la DLT, a probablement aussi contribué à cette image négative, associée "à des affaires de fraude, de blanchiment d'argent et en lien avec des groupes criminels" (Frunza, 2015), comme en témoignent la suspension de systèmes comme E-Gold en 2008 ou Liberty Reserve en 2013. Par la suite, des plateformes d'échange en ligne utilisant le Bitcoin

et la Blockchain, comme Silk Road ou Sheep Momentum, ont fait la une des journaux pour les activités criminelles qu'elles facilitaient, comme la vente de drogues et d'armes. Silk Road a été saisie par le FBI en octobre 2013. Sheep Momentum, ayant pris de l'ampleur suite à la clôture de Silk Road, fut, elle, fermée peu après en décembre 2013. Ces scandales ont largement contribué à la perception négative que l'opinion publique se forma du Bitcoin. Surnommé par certains *Bitcon* (un jeu de mots entre *Bit*, l'unité binaire, et *con*, escroquerie en anglais), le Bitcoin prit rapidement l'allure du dispositif idéal pour le blanchiment d'argent et la facilitation d'activités criminelles.

L'effondrement dramatique de Mt Gox au début de l'année 2014 finit par alimenter la couverture médiatique plus que jamais négative du Bitcoin. Mt Gox était une plateforme d'échange de bitcoins ayant couvert jusqu'à près de 80% du trading global de cette monnaie numérique[47]. La plateforme dût mettre la clé sous la porte suite à la découverte de la disparition estimée de 744 000 bitcoins, représentant alors environ 350 millions de dollars, soit environ 6% du volume total de bitcoins alors en circulation. Mt Gox ne fut pas un cas isolé. De nombreuses plateformes d'échange ont vu leur fermeture forcée (Moore and Cristin, 2013). Cependant, elle fut, de loin, la plus importante et la plus visible. Il y eut, par ailleurs, plusieurs autres arnaques liées à l'utilisation de bitcoins. Cependant, il semblerait qu'elles furent plus le résultat de manipulations d'escrocs que liées à des faiblesses technologiques du réseau. Par exemple, aux Etats-Unis, une enquête au niveau fédéral mit fin en 2014 à un système de Ponzi. Son organisateur avait réussi à réunir près de 765,000 bitcoins en un an et a finalement été arrêté pour fraude financière[48].

Risque majeur pour toute monnaie numérique décentralisée, le blanchiment d'argent par l'utilisation du réseau Bitcoin peut être réalisé de deux manières : (i) directement, à travers la mise en place d'une opération importante de minage, un investissement financé par de l'argent gagné de façon illicite qui générera des bitcoins à travers la collecte de nouveaux bitcoins créés d'une part et des frais de transaction d'autre part ; indirectement, en échangeant cet argent sale contre des bitcoins à un complice non identifiable. Il est en effet aisé de créer des adresses bitcoins n'ayant pas de lien direct avec son identité à partir d'un ordinateur ou même d'un smartphone. Aujourd'hui, dans les pays où la réglementation est effective, la plupart des plateformes d'échange demanderont une pièce d'identité aux clients souhaitant acheter de la monnaie numérique contre de la monnaie nationale. Cependant, la plupart du temps, les procédures *Know Your Customer* (KYC), visant à identifier ses clients, demeurent assez basiques. Il existe encore des moyens d'échanger des bitcoins contre des espèces de monnaie nationale sans vérification d'identité.

Quid du niveau de sécurité offert aux utilisateurs légitimes ? Tout dépend de l'utilisation faite des clés privées et publiques, et de la bonne garde de la clé privée, qui doit demeurer absolument confidentielle[49]. Le comportement de l'utilisateur est crucial pour le maintien de cette confidentialité et le niveau de sécurité des actifs détenus. Diverses solutions de stockage sécurisé des clés privées ont été développées ces dernières années. En France, on peut citer Ledger, par exemple, qui propose des solutions de stockage de clés privées via une carte à puce connectée en USB ou NFC (sans contact) à son ordinateur ou son smartphone. Puisque la probabilité qu'un appareil électronique connecté soit piraté un jour ou l'autre est loin d'être nulle, il est primordial de s'assurer que ses clés privées soient gardées dans un endroit séparé

du portefeuille électronique, et de ne pas les perdre ! Ce principe de ségrégation des données très sensibles de tout appareil connecté à Internet est appelé *cold storage*.

Un utilisateur prudent suivra donc plusieurs bonnes pratiques afin de garantir un niveau de sécurité élevé : par exemple, l'allocation de petits montants à plusieurs adresses bitcoin, plutôt que l'utilisation d'une seule adresse pour un gros montant. Par ailleurs, comme l'a montré l'affaire Mt Gox, il est plus que recommandé de faire une *due diligence* et de procéder à toutes les vérifications nécessaires avant d'avoir recours à une plateforme d'échange de bitcoins. Le système bancaire a mis des procédures en place ne permettant pas à ses employés d'accéder aux données clients. Il n'est pas encore sûr que toutes les plateformes d'échange de bitcoins suivent les mêmes pratiques.

Un autre aspect important affectant le niveau de sécurité d'un réseau ouvert, fondé sur une confiance décentralisée[50], est lié à la question du niveau de distribution du contrôle de ce dernier. Le réseau ne doit en effet pas tomber sous le joug d'un groupe mal intentionné et se prémunir d'une collusion de mineurs formant une coalition majoritaire. Nous avons précédemment mentionné la menace potentielle d'*attaque des 51%*. Il est intéressant de noter qu'il arriva qu'un pool de mineurs ait atteint un niveau cumulé de force de calcul de 51%. Cependant, la rumeur dit que le pool se désagrégea naturellement pour redescendre à un niveau inférieur, suivant une logique d'autogestion guidée par la volonté de ne pas affaiblir le réseau. En effet, la menace d'attaque des 51% est sérieusement considérée comme une faiblesse potentielle du réseau et est suivie de près par ses participants et par les régulateurs[51]. Ceci étant dit, il n'est pas aisé de suivre l'évolution de la distribution de la force de calcul du réseau de façon précise aujourd'hui et donc d'anticiper une telle attaque. Certains pays, comme la Chine par exemple[52], ont mis en place des systèmes de *firewalls* brouillant le passage de données vers l'extérieur, et rendant ainsi cette analyse tronquée. Il est aussi important de comprendre qu'une attaque des 51% ne permettrait pas aux attaquants de réécrire l'histoire des transactions : ils pourraient contrôler la validation de nouveaux blocs de transactions et ainsi permettre une double dépense de bitcoins, mais ils n'auraient pas, à ce jour, assez de force de calcul pour réécrire les transactions passées en l'espace des 10 minutes nécessaires à l'ajout d'un nouveau bloc dans la blockchain.

4.2. Quid des chaînes privées ?

Différents niveaux de droit (de lecture simple ou de modification par exemple) peuvent être attribués à une chaîne de blocs privée. Dans le cas d'un réseau fermé regroupant les membres d'un consortium, le nombre de nœuds peut être grandement réduit (de l'ordre de plusieurs milliers à quelques centaines) et l'on peut donner à chaque nœud un niveau spécifique d'autorisation à agir sur le réseau, selon le rôle et la fonction que l'on souhaite attribuer à ce nœud. Dans certains cas, il pourrait être envisageable de n'utiliser ni *proof-of-work,* ni *proof-of-stake.*

L'intégrité des données transactionnelles pourrait être garantie par un système de hachage périodique (comme la production d'une racine de Merkle de toutes les transactions du jour par exemple) et la mise en place de procédures de *cold storage*. Le fait que l'ensemble des données soit distribué au sein d'un réseau pair-à-pair

augmente la difficulté qu'un étranger au réseau puisse s'infiltrer et modifier les données transactionnelles.

Des procédures de conformité et de reporting automatiques à des entités extérieures, comme les autorités régulatrices par exemple (utilisant peut-être aujourd'hui les référentiels centraux de données, communément appelés *trade repositories*), pourraient aussi renforcer la solidité du système.

4.3. Résilience des algorithmes cryptographiques existants

La cryptographie est un autre – si ce n'est le plus important – aspect du niveau de sécurité général du système. Le niveau requis de chiffrage (incluant, bien entendu, celui lié au minage dans le cas du Bitcoin) et les risques posés par le progrès informatique est une question récurrente. En effet, on pourrait imaginer qu'il soit un jour possible d'inverser les fonctions à sens unique (par exemple, RIPEMD160 après SHA256 pour la génération d'adresses bitcoin). C'est une question légitime, lorsque l'on observe que certains algorithmes considérés comme sûrs dans le passé sont aujourd'hui obsolètes[53].

Le protocole Bitcoin, cependant, utilise une combinaison de fonctions cryptographiques (par exemple, lors de la génération d'une adresse bitcoin, SHA 256 est d'abord appliquée, puis RIPEMD160). Cela augmente tant la difficulté à déduire une clé publique d'une adresse bitcoin, et une clé privée d'une clé publique que de nombreux experts considèrent qu'il est aujourd'hui impossible ou infaisable de trouver une clé privée à partir d'une adresse bitcoin. Néanmoins, il nous semble très important de garder un œil attentif au développement des ordinateurs quantiques, du fait des effets multiplicateurs qu'ils pourraient avoir sur la capacité de calcul, rendant potentiellement ainsi plus accessible la solution à des problèmes de fonctions de chiffrage combinées[54].

4.4. Risques liés à l'automatisation

Le fonctionnement des marchés financiers est aujourd'hui encore fondé sur de nombreuses interventions manuelles, plus particulièrement au niveau du *middle-office* pour la capture de données et du *back-office* pour leur traitement. L'introduction de la technologie des registres distribués s'accompagnera probablement de beaucoup plus d'automatisation. Cette dernière peut être perçue comme une façon de réduire le risque opérationnel dans des circonstances de fonctionnement normal. Certains opérateurs de marché soulignent cependant les risques inhérents liés à une dépendance accrue aux systèmes automatisés. Ainsi, l'intégration de la technologie des registres distribués demandera probablement un niveau de sophistication plus élevé des fonctions de *middle* et *back-office* et la mise en place de procédures de contrôle d'urgence.

5. Domaines clés d'application de la DLT

5.1. Certification, horodatage et services de certification : vers un nouveau modèle de notarisation ?

Comme mentionné dans la partie 1.1, la certification par horodatage crypté et irréversible a été testée à travers la mise en place de solutions de registres distribués dans de nombreux secteurs économiques. Les applications de la blockchain sont nombreuses. Parmi les plus significatives : des services de cadastre, de notarisation, de gestion de dossiers médicaux anonymes, de certification de médicaments (pour lutter contre la contrefaçon), de certification des diplômes, de gestion de cartes d'identités électroniques pour les réfugiés, de gestion logistique…

Il est donc logique de regarder du côté de la technologie blockchain pour sa capacité à faciliter les services de certification, c'est à dire, "toute sorte de service, lié au traitement, au classement, et à l'enregistrement de documents, à des services notariaux (validation), et à de la protection de propriété intellectuelle" (Swan, 2015). Ces services bénéficieront de la capacité de la blockchain à utiliser des "hash cryptographiques comme façon permanente et publique d'enregistrer et de stocker de l'information, disponible via un explorateur de blocs". En ce sens, la blockchain serre de centre d'archives universel. *Proof of Existence* fut une des premières plateformes web à offrir une certification par la Blockchain[55]. "Vous pouvez utiliser nos services pour chiffrer de l'art ou des logiciels, par exemple, dans le but de prouver que vous en êtes l'auteur par le biais d'un mécanisme fiable d'horodatage", qui n'existait pas avant que la Blockchain ne soit mise en place avec le Bitcoin. Ce service "démontre la propriété d'un document sans en révéler l'information contenue, et fournit la preuve qu'un document a été créé par un auteur particulier à un temps donné" (Swan, 2015). Divers autres services de notarisation, comme Virtual Notary[56] ou Bitproof[57] ont depuis vu le jour.

Factom[58], spécialisé dans la sécurisation et le stockage de données, utilise une approche intéressante. Son produit phare, la *Factom Proof*, combine trois types de preuve : la preuve d'existence ("le document existait sous cette forme à cette date"), la preuve de processus ("tel document est lié à tel autre version mise à jour") et la preuve d'audit ("vérifiant les modifications opérées dans un document mis à jour"). De même, Stratumn[59], basée à Paris, offre une plateforme capable de traiter des processus de travail (*workflows)* en décrivant chacune de ses étapes et en lui ajoutant une vérification cryptographique.

La capacité à stocker des données de façon immuable, chiffrée et sûre de la DLT pourrait être à la base d'un nouveau paradigme d'authentification et de certification de documents, avec valeur de preuve pour la justice (Blanchette, 2012). Par ailleurs, le système de multi-signatures facilitant l'étape d'approbation ou de rejet d'un document ou d'une transaction avant certification dans la Blockchain donne une dimension collaborative intéressante à cette technologie. A terme, pourquoi ne pas

imaginer son utilisation pour l'authentification de certains documents, directement de pair à pair, sans nécessairement passer par les services légaux d'un tiers ? Il faut aussi remarquer qu'on peut conditionner l'exécution de transactions ou de *smart contracts* portés par une blockchain grâce à un "oracle", i.e. un serveur extérieur à la blockchain dédié précisément à la vérification de ces contingences exogènes.

Cela signifie-t-il pour autant que la profession de notaire risque de voir son activité d'authentification et de certification perdre son monopole ? Probablement pas à court terme. La profession verra, elle-même, sans doute ses pratiques évoluer avec les avancées technologiques et potentielles révolutions réglementaires. Si l'on reprend les travaux de Porter (1979), la DLT peut être aussi bien considérée comme une menace qu'une opportunité d'évolution de la profession, qui pourrait bien se saisir cette technologie et ainsi proposer de nouveaux services. Par ailleurs, la dimension de conseil juridique du notariat (dans des pays de droit civil) rend son périmètre d'activité bien plus large que celui de la pure certification.

5.2 DLT et systèmes de paiements

Dans son livre blanc de 2008, Satoshi Nakamoto décrit le protocole Bitcoin comme "une version de monnaie électronique purement pair-à-pair permettant d'effectuer des paiements en ligne directement d'un parti à un autre sans passer par une institution financière". De fait, le Bitcoin a prouvé son efficacité comme système d'échange de transactions numériques, en permettant l'envoi et la réception de bitcoins directement d'une personne à une autre, sans qu'il ne soit nécessaire de passer par un intermédiaire. En pratique, les utilisateurs peuvent choisir entre différents types d'interfaces numériques afin de procéder à leurs paiements. Celles-ci sont communément appelées des *wallets* (portefeuilles) et peuvent aisément être installées sur des appareils mobiles comme les *smartphones* et les tablettes (comme c'est le cas de Mycelium, par exemple), des ordinateurs (comme le logiciel Bitcoin Core) ou via une interface web (comme Coinbase).

Une série d'accessoires s'est développée, permettant à l'utilisateur d'ajouter une couche de sécurité supplémentaire à sa gestion de bitcoins, comme les *smartcards* (Ledger par exemple[60]) permettant la garde de ses clés privées séparément du terminal procédant au paiement. La Figure 2 présente comment une transaction standard de bitcoins fonctionne. Les bitcoins sont fongibles et peuvent être échangés contre de la monnaie nationale. En France, par exemple, on peut notamment trouver ces services chez Paymium[61], plateforme française d'échanges en ligne ou encore à La Maison du Bitcoin[62], ayant une présence physique à Paris avec un comptoir de change et un distributeur automatique de bitcoins[63]. Basée à Chicago, la start-up Glidera propose même un service permettant de lier son *wallet* Bitcoin directement à ses comptes bancaires traditionnels, à travers le développement d'APIs.

Figure 2 : Comment s'échange-t-on des bitcoins ?

Récemment, la France a modifié sa réglementation monétaire et financière et introduit le statut d'établissement de paiements, défini comme tel dans l'article L522-1 du Code monétaire et financier (ordonnance n°2009-866 du 15 juillet 2009 – art 12) : "les établissements de paiement sont des personnes morales, autres que les établissements de crédit et autres que les personnes mentionnées au II de l'article L. 521-1, qui fournissent à titre de profession habituelle les services de paiement mentionnés à l'article L. 314-1[64] ". Les plateformes d'échange de bitcoins comme Paymium entrent dans ce champ. Régulés par l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) de la Banque de France, ces établissements de paiement peuvent obtenir l'autorisation d'offrir leurs services à l'échelle européenne sur autorisation de cette première[65].

Comme mentionné dans la partie 1.1, les principaux acteurs du secteur des paiements, comme Visa, Mastercard, Paypal[66], pour ne pas tous les citer, ont déclaré être en phase d'exploration et d'évaluation de la faisabilité en matière de DLT. La banque coréenne KB Kookmin Bank a officiellement annoncé son intention d'explorer la blockchain comme une solution potentielle lui permettant de baisser la structure de coûts de son service de transfert de fonds internationaux (*remittances*), qui fait aujourd'hui appel à SWIFT. Nous observons trois principaux segments se développer aujourd'hui autour des services de paiement :

(i) Les *wallets* (portefeuilles) offrant des services de paiement P2P décentralisés (comme Mycelium, BitPay et bien d'autres)

(ii) Les plateformes d'échange de bitcoins et d'autres monnaies numériques (comme par exemple Coinbase, Paymium, la Maison du Bitcoin, Medici d'Overstock)

(iii) Les services de transferts de fonds internationaux (comme BitPesa, Abra, Rebit, ArtaBit, Coincove, etc.)

Aujourd'hui, les principaux fournisseurs de services de paiement, qui souhaitent intégrer à leurs solutions de paiement actuelles de la DLT, doivent développer leurs propres API ou faire appel aux services de programmation qu'offre Glidera, par exemple. Comme mentionné plus haut, Glidera permet un accès direct à ses comptes bancaires via son *wallet*. Le développement de ce type d'API devrait encourager et faciliter le processus d'intégration de la DLT dans ce secteur.

Ceci étant dit, comme discuté en partie 3.1., avant de devenir une alternative de grande envergure, la DLT devra avoir résolu la question de la stabilité du réseau. Dans leur article *On Scaling Decentralized Blockchains* (IC3, 2016) au sujet de la mise en échelle de blockchains décentralisées, le groupe IC3 (*Initiative for CryptoCurrencies and Contracts*[67]), note que le débit de validation de transactions maximal du Bitcoin est aujourd'hui de 3.3-7 transactions par seconde. "En comparaison, un organisme de traitement des paiements comme Visa […] traite en moyenne 2 000 transactions par seconde, et peut culminer à 56 000 transactions par seconde si nécessaire." S'il est certainement probable que les évolutions technologiques en cours et à venir rendent ces performances similaires, à terme, il est important de souligner la question du déploiement à grande échelle de la DLT[68].

En fait, divers experts du Bitcoin partagent leurs doutes sur l'utilisation du réseau Bitcoin, et toute la puissance de calcul qu'il requiert, pour l'authentification de micro-transactions, servant par exemple à l'achat d'un café ou d'un journal[69]. En effet, il peut paraître inadéquat d'utiliser la puissance de calcul de tout le réseau et le processus de *proof-of-work* de façon systématique. Beaucoup pensent que la combinaison de blockchains privées pour de petites transactions et l'utilisation de la Blockchain du Bitcoin pour le solde journalier des transactions serait plus raisonnable. En d'autres termes, la Blockchain pourrait ou devrait être utilisée de façon modérée pour l'enregistrement d'agrégats d'informations présentes sur d'autres chaînes parallèles (*sidechains*), mais pas nécessairement pour l'enregistrement de n'importe quelle transaction.

Une telle configuration pourrait en effet représenter une utilisation optimale de la DLT, maximisant la sécurisation de la certification des transactions à travers la Blockchain et minimisant les ressources de calcul nécessaires à cette action. On pourrait imaginer l'utilisation de chaînes fermées pour des transactions inférieures à un certain montant.

La start-up Blockstream et le *Bitcoin Lightning network* développent des solutions allant en ce sens. Blockstream a annoncé avoir levé 55 millions de dollars en Février 2016 pour le développement de *sidechains* interopérables[70] et permettant la combinaison de chaines privées et publiques de données. Le *Bitcoin Lightning network*, comme expliqué par Poon et Dryja[71] dans leur livre blanc, propose une solution hors blockchain pour augmenter la capacité de traitement du réseau Bitcoin sans en augmenter le risque de centralisation. Ils suggèrent de "décaler dans le temps le fait d'informer le monde entier de chaque transaction [et] de laisser la confirmation qu'une transaction est liée à une autre à une date ultérieure". L'utilisation de micro-canaux de diffusion "permet aux utilisateurs Bitcoin d'échanger autant de transactions qu'ils le souhaitent sans bloquer pour autant la Blockchain ni faire appel à un tiers de confiance central". L'utilisation de "*time locks* [c'est à dire le décalage dans le temps programmé] comme composants d'un consensus global" pourrait, selon eux, permettre la création d'une structure efficace ne nécessitant pas l'intervention de la

notion de confiance. Cela passerait par la “mise en place d’une relation entre les deux parties de telle sorte qu’ils soient perpétuellement à la recherche de l’équilibre des soldes”, actions qui seraient faites de façon routinière hors blockchain. Ainsi, comme développé précédemment dans la partie 3.1, il semblerait possible de combiner mise en grande échelle avec le maintien de la décentralisation du réseau, ce qui pourrait donner à la DLT une certaine place dans l’univers des paiements.

5.3. DLT, marché des capitaux et finance d’entreprise

Nombreuses sont les applications de la DLT pour l’industrie financière, comme en témoignent les investissements importants qu’ont réalisé certains grands acteurs du secteur ces derniers mois. Pour autant, une telle intégration devra se faire avec prudence. En effet, du fait des enjeux, les services financiers n’ont que très peu de marge d’erreur possible, dans un contexte où les infrastructures existantes sont capables de traiter des millions de transactions par jour.

L’opérateur boursier ASX (*Australian Stock Exchange*) a annoncé récemment avoir acheté 5% de la société Digital Asset Holding pour 14,9 millions de dollars australiens et son intention de tester la DLT pour ses services de post-marché[72]. ASX utilise actuellement une plateforme de compensation et de règlement nommé CHESS. Cette dernière “continuera d’opérer normalement, en parallèle aux développements faits en DLT. Cela laissera aux différents acteurs d’évaluer les bénéfices et les conséquences [de cette technologie] avant une prise de décision finale concernant la technologie à utiliser pour le post-marché en 2017.”

Parmi les nombreuses applications possibles de la DLT, nous voyons un potentiel de développement particulièrement intéressant pour les *smart contracts* ou contrats intelligents. Un *smart contract* est un programme informatique dans lequel les clauses contractuelles sont codées sous forme de règles et qui est capable de s’exécuter automatiquement. Les *smart contracts* ont de nombreuses applications et pourraient être notamment utilisés pour la distribution de dividendes, l’émission de nouvelles actions, la division d’actions en plusieurs unités. Tout en appliquant automatiquement les règles menant au dénouement de la position de sortie d’une opération financière (ou, dans le cas d’une option, à son exercice), à partir du moment où certaines conditions programmées à l’avance sont mises en place, le code rédigé dans les *smart contracts* imite la logique d’exécution des clauses contractuelles. L’ambition derrière les *smart contracts* est de fournir un niveau de sécurité d’exécution supérieur à celui proposé actuellement par le droit des contrats en diminuant les frais de transactions et les coûts légaux liés à la formalisation d’obligations contractuelles. Wright et De Filippi (2015) avancent d’ailleurs que le déploiement à grande échelle de la DLT devrait déboucher sur un ensemble de lois, nommé *lex cryptographia*, défini comme une collection de “règles administrées par des *smart contracts* auto-exécutables et des organisations (autonomes) décentralisées”.

La blockchain d’Ethereum serait une des plateformes les plus prometteuses dans sa capacité à accueillir le développement de *smart contracts*. D’autres plateformes existent, comme Nxt[73], et il ne serait pas étonnant de voir le rythme d’innovations se multiplier au cours de la prochaine année dans ce domaine. Conscients que cette technologie en est encore à ses débuts et sous environnement de test, nous proposons un aperçu

synthétique de ce que nous considérons comme étant les principaux mécanismes et applications potentielles de ces *smart contracts* pour l'industrie financière.

Prenons quelques exemples. Dans le cas d'une distribution de dividendes, nous pourrions programmer dans le contrat qu'un certain pourcentage des bénéfices par action annoncés soit envoyé directement aux actionnaires à la fin de chaque année, par exemple. Cet envoi pourrait se faire sous forme de monnaie nationale ou par son équivalent en crypto-monnaie. De même, de nombreux produits dérivés standardisés, tels que les options vanilles, pourraient tout aussi bien être programmés dans des *smart contracts*, avec la possibilité de préprogrammer des caractéristiques de couverture dynamique[74] ou le dénouement automatique de positions. Les appels de marge, eux-mêmes fonctions du cours de l'actif sous-jacent, pourraient eux aussi être automatiquement générés et gérés par l'intermédiaire d'un *smart contract*. De plus, les titres financiers, traduits de façon numérique dans les *smart contracts,* eux-mêmes enregistrés sur une blockchain, pourraient incorporer leur règlement-livraison automatique auprès des comptes de l'acheteur et du vendeur. En effet, tout changement de propriété, partielle ou complète d'un actif numérique inscrit dans un registre distribué sera automatiquement enregistré et lié à son nouveau propriétaire et à la chaine de transactions précédentes. Si cela menait au raccourcissement de la procédure de règlement-livraison, il n'est pas exclu que ce système se substitut au moins partiellement à des solutions d'identification des négociations, comme notamment offerts par SWIFT.

L'application de certaines règles prudentielles, telles que les ratios de fonds propres pour les banques, ou encore les covenants financiers pour les emprunteurs, pourrait être suivie à travers la mise en place de *smart contracts* sur une blockchain. Les bilans comptables des parties concernées pourraient être inscrits de façon cryptée dans un registre distribué, et liés aux transactions réalisées par ces parties. En un sens, l'adoption générale d'une blockchain commune, ou d'un ensemble de chaînes capables d'interopérabilité, pourrait être l'architecture de base d'un système "incontestable" de preuves de solvabilité. En "injectant de la confiance" entre les participants, ces dernières pourraient bien mener à l'augmentation du niveau d'échanges commerciaux, à plus de liquidité de marché, et à l'encouragement des prêts interbancaires. Point d'autant plus important dans un contexte où ces derniers se sont réduits comme peau de chagrin, au plus profond de la dernière crise économique mondiale, les banques se montrant de plus en plus prudentes vis à vis du risque de contrepartie. Un registre, partagé et distribué à tous les participants, capable de fournir des preuves de solvabilité fiables, aurait alors sans doute trouvé son utilité.

Par ailleurs, la traçabilité rendue possible par une blockchain pourrait grandement faciliter la gouvernance d'entreprise en général (Yermack, 2015), et la gestion financière. La DLT, par sa capacité à gérer les transferts de propriété de façon transparente, pourrait s'avérer intéressante à mobiliser dans les situations où les entreprises doivent contacter leurs investisseurs, que ce soit dans le cadre d'une fusion ou d'une acquisition, pour une élection interne ou pour toute décision où le vote des actionnaires est requis. Le vote des actionnaires, s'il se faisait par le biais de cette technologie, pourrait donner davantage de précision aux services de vote par procuration (*proxy services*) existant : les actionnaires pourraient être contactés plus rapidement et efficacement. On peut aussi imaginer une utilisation en comptabilité d'entreprise et pour le *reporting* financier. Certains auteurs vont même jusqu'à affirmer que les entreprises pourraient tout à fait volontairement inscrire toutes leurs transactions sur une blockchain, menant à une

comptabilité financière en quasi temps réel (Lazanis, 2015). Alors que tous ne partagent probablement pas le même enthousiasme, la mise en place d'une politique d'inscription systématique sur une blockchain pourrait apporter trois bénéfices : (i) une image claire de la solvabilité d'une organisation, à travers la récupération possible de ses données comptables (bilan, compte de résultats, flux de trésorerie) par tout investisseur ou débiteur de cette même entité ; menant à la facilitation de (ii) procédures d'audit et (iii) des fonctions de *reporting*.

Cette liste de potentielles applications de la DLT n'est, bien entendu, pas exhaustive. Nous pourrions aussi mentionner, par exemple, les opportunités significatives que la DLT représente pour le financement des échanges commerciaux (*trade finance*)[75]. Au final, quelque soit le domaine d'application dans le secteur financier, il est clair que la DLT sera utilisée pour bousculer les situations de *status quo*. Explorons désormais le potentiel de cette technologie dans son application pour les infrastructures de marché, avec un regard particulier sur le post-marché.

6. DLT et potentiel d'intégration au sein de l'infrastructure des marchés financiers

La chaîne de valeur des infrastructures de marché est communément divisée en trois grandes parties : (i) *pre-trade* ou pré-négociation, (ii) *trade* ou transaction and (iii) *post-trade* ou post-marché.

Dans quelle mesure la DLT, dont les dispositifs sont capables d'enregistrer et de transférer de la valeur, d'un propriétaire à un autre, pourrait-elle perturber cette chaîne de valeur ? Négocier un titre sur les marchés financiers, l'acheter ou le vendre, résulte au transfert de propriété d'un actif à un prix négocié. Les transferts doivent donc être enregistrés de façon sûre, et l'actif traité, gardé en toute sécurité, et transféré vers son nouveau propriétaire de manière efficace et fiable.

Nous avons vu précédemment (partie 5.3) que les *smart contracts* peuvent automatiser n'importe quelle action que l'on peut traduire en fonctions algorithmiques. Dans cette section, nous irons plus loin et nous concentrerons sur les principaux processus structurant aujourd'hui l'infrastructure des marchés financiers et le potentiel de la DLT à se substituer de façon raisonnable aux systèmes hérités.

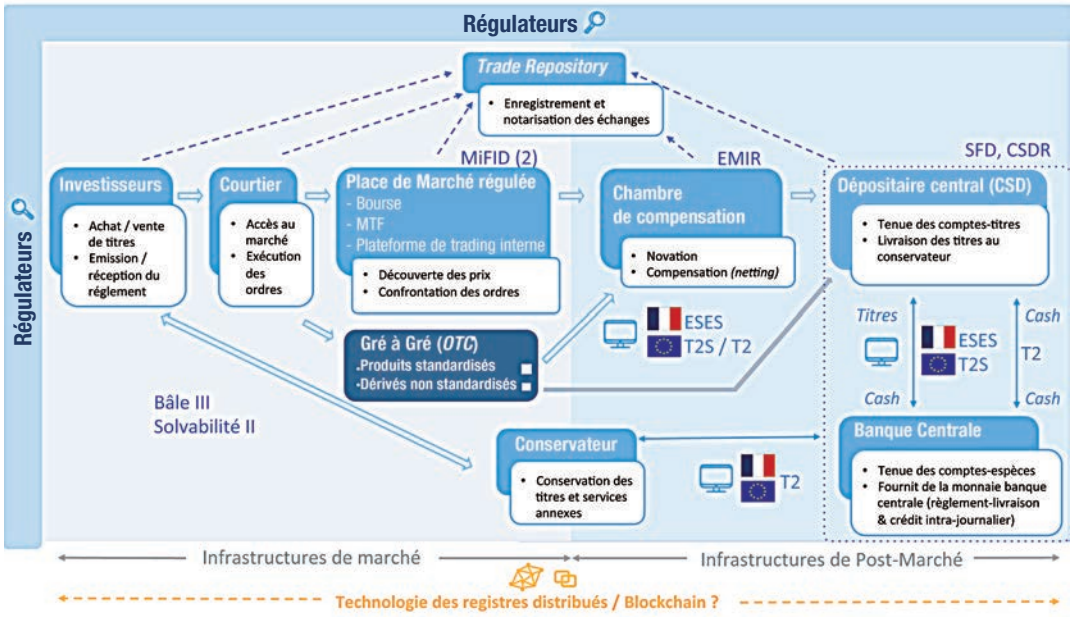
6.1. Les infrastructures de marchés financiers européens : des changements réglementaires et de l'introduction des systèmes RTGS à travers l'Europe.

La dernière grande crise financière mondiale a eu un impact significatif sur la réglementation bancaire et sur les marchés financiers. De façon globale, la gestion du risque systémique est devenue centrale. L'espace bancaire européen a vu les règles

prudentielles telles que Bâle III augmenter les niveaux de fonds propres estimés comme nécessaires à leur solvabilité. La réglementation EMIR (*European Markets Infrastructure Regulation*) a introduit l'obligation de passer par une chambre de compensation centrale (CCP) pour les transactions faites de gré-à-gré (*OTC*) de dérivés standardisés, "ce qui a érigé les CCP en piliers de la nouvelle architecture financière mondiale" (Cont, 2015). Aux Etats-Unis, le *Dodd-Frank Act* de juillet 2010 augmenta, de façon similaire, les obligations prudentielles et de *reporting* des institutions financières y exerçant.

Le renforcement des règles prudentielles et des obligations de *reporting*, combiné à la contraction de liquidité conséquente à l'effondrement de Lehman, a rendu les besoins de financement du secteur privé européen encore plus aigus. Et par conséquence, encore plus importante l'efficacité des marchés financiers européens à accomplir leur mission de financement de l'économie. En effet, comme souligné par le plan d'action de la Commission Européenne pour construire une union des marchés des capitaux ("*Action Plan on Building a Capital Markets Union", September 2015*[76]) : "Comparées aux Etats-Unis, les PME européennes reçoivent cinq fois moins de financement de la part des marchés financiers". Le recours à la titrisation est une autre recommandation contenue dans ce plan d'action. Perçue comme une façon fiable d'augmenter la liquidité, elle pourrait soutenir le renouvellement des marchés de crédit européens.

Figure 3 : Quel niveau d'intégration pour la DLT au sein de l'infrastructure des marchés financiers ?



Dans ce contexte, la sécurité et l'efficacité des infrastructures de post-marché sont fondamentales pour la mise en place d'une croissance économique durable en Europe. Les systèmes informatiques et la réglementation ont évolué en parallèle. Comme développé dans le plan d'action européen mentionné plus en amont (Septembre 2015), "la législation européenne, telle qu'EMIR, CSDR (*Central Securities Depositories Regulation*) et MiFID II, a levé les barrières du règlement-livraison des titres [sur les marchés financiers]". Les efforts d'harmonisation se sont inspirés des recommandations du Groupe Giovannini (2001, 2003), à travers certaines initiatives telles que le *European Post Trade Group* (EPTG), composé de la Commission européenne, la Banque Centrale Européenne (BCE), l'ESMA (*European Securities and Markets Authority*) et des représentants du secteur privé.

Des systèmes de règlement en lien continu (*Continuous link settlement*, CLS) et de règlement brut en temps réel (*real-time gross settlement*, RTGS) ont remplacé les procédures de règlement net différé (Deferred Net Settlement, DNS) au niveau européen pour les paiements et crédits intra-journaliers (TARGET puis TARGET 2, ou T2, à partir de Novembre 2007), et plus récemment pour la livraison de titres (TARGET2-Securities, ouT2S, est actuellement en phase de déploiement dans l'Eurosystem). Ces systèmes de règlement brut en temps réel utilisent le système de messagerie SWIFT pour le traitement des flux d'information.

La conception de nouveaux systèmes utilisant la DLT doit être réalisée en prenant en compte les changements auxquels les utilisateurs vont faire face, notamment en matière de gestion des risques et de structure de coûts. Le design de systèmes de règlement-livraison va de pair avec, d'un côté, la volonté de réduire le risque de liquidité en effectuant le règlement-livraison le plus tôt possible, et de l'autre côté, le souci de réduire les coûts de liquidité liés à l'immobilisation des actifs durant la période la plus courte possible.

Les dispositifs de règlement-livraison brut en temps réel RTGS sont généralement considérés comme plus sûrs que les systèmes nets différés DNS (Hervo, 2008), puisque chaque transaction y est réglée "dès qu'elle entre dans le système". De l'autre côté, "une des externalités négatives de la modalité RTGS réside en le fait qu'ils ont des besoins de liquidité intra-journaliers […] plus importants que dans un environnement DNS".

Des caractéristiques d'économie de liquidité ont été introduites dans les systèmes RTGS afin de permettre "une compensation bilatérale ou multilatérale avec une fonctionnalité de règlement-livraison en temps réel (par exemple, CHIPS aux Etats-Unis, TARGET 2 dans l'Union européenne)." D'autres fonctionnalités en temps réel ont été ajoutées afin de réduire les coûts d'opportunité de liquidité, comme la capacité, par exemple, de modifier l'ordre de traitement d'une transaction, le moment auquel le règlement-livraison doit être effectué ou la mise en place de certaines limites de crédit permettant de contrôler le flux de fonds sortant.

Par ailleurs, les dépositaires centraux (CSD) ont introduit des fonctionnalités d'auto-collatéralisation, permettant de faire face au besoin de collatéralisation plus important des systèmes RTGS. Par exemple, le système ESES d'Euroclear fournit des services de règlement-livraison en temps réel avec des procédures d'auto-collatéralisation

automatiques. Ces services permettent l'utilisation de titres "étant en cours d'achat comme collatéral pour le crédit intra-journalier" (Hervo 2008). Une fois complètement déployé, le système T2S devrait avoir des caractéristiques similaires.

Par ailleurs, dans le but d'augmenter la sécurité et la fiabilité des infrastructures RTGS, les systèmes avec révocabilité des opérations ont été remplacés par des systèmes de règlement-livraison irrévocables (En France, Relit+ a ainsi été remplacé par ESES en 2007)[77].

La gestion des flux de règlement-livraison en période de pointe, le besoin accru de diversification du collatéral et l'augmentation de l'utilisation de la monnaie de banque commerciale à la place de monnaie banque centrale pour les règlements en multidevises sont autant de défis auxquels les infrastructures des marchés financiers doivent faire face (Hervo, 2008).

En dernier lieu, il est important de rappeler l'envergure des opérations que doit traiter l'infrastructure post-marché européenne. Le système RTGS T2S est encore en phase de déploiement et nous n'avons donc pas encore de statistiques permettant de mesurer l'échelle de son activité. Selon la Banque de France[78], le système RTGS TARGET2, considéré comme un système de paiement de montant élevé (*Large Value Payment System*, LVPS), a traité 364 000 transactions par jour, pour un montant total de 1 935 milliards d'euros en 2013. Dans ce contexte, il est légitime de s'interroger sur la capacité de la DLT à faire face à la complexité et l'échelle des processus gérés par les infrastructures post-marché.

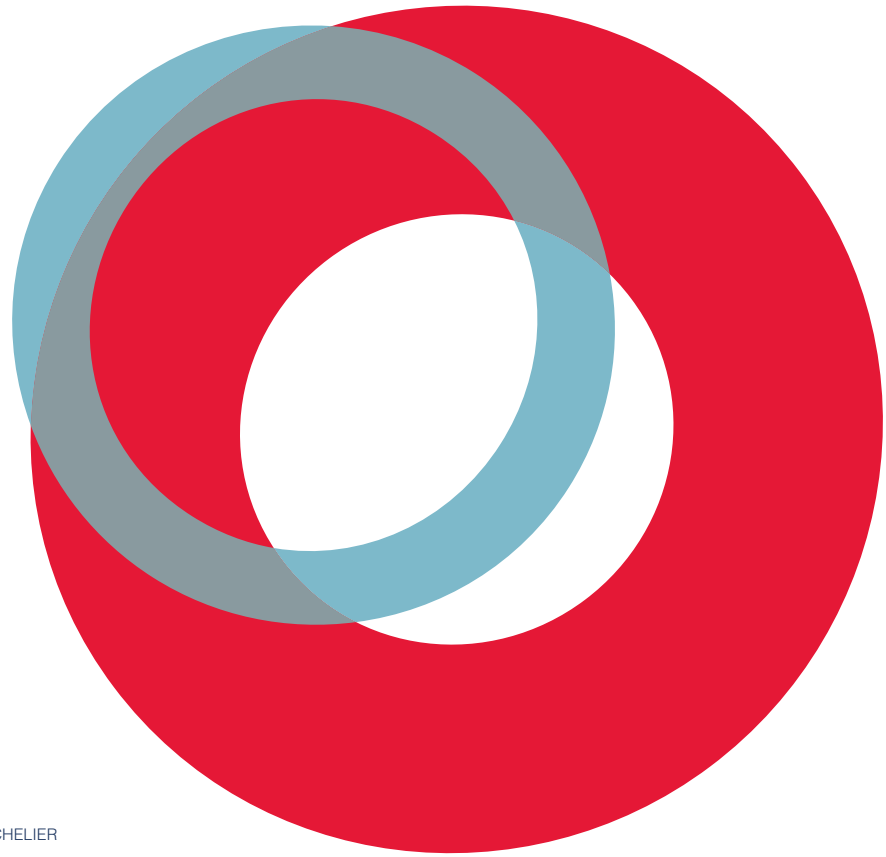
6.2. La DLT : un nouveau paradigme pour le post-marché ?

Les partenariats entre start-ups DLT et grandes institutions financières ont bousculé la perception que l'on a de la façon, souvent perçue comme traditionnelle, dont les banques opèrent. Est-ce que ces jeunes entreprises de la DLT auront la capacité de transformer l'industrie financière au même titre que certaines start-ups (qu'on appelle communément les *unicorns*[79]) ont déjà modifié le paysage concurrentiel de nombreux secteurs comme le transport de personnes, l'immobilier, l'hôtellerie, et même l'exploration spatiale ? Comme mentionné dans la partie 1.1, des cadres dirigeants de l'industrie financière, comme Blythe Masters, ancienne directrice de la branche matières premières de JP Morgan au niveau mondial, ou Peter Randall, fondateur de la plateforme de trading Chi-X, se sont clairement impliqués dans la DLT, qu'ils perçoivent comme une technologie extrêmement prometteuse. Sir David Walker, notamment ancien directeur exécutif de Bank of England, a aussi rejoint le mouvement DLT en s'associant à la start-up SETL.io.

SETL est une start-up dont l'objectif est de développer des solutions de règlement-livraison fondées sur la DLT à destination de l'industrie financière. Elle a annoncé, à l'automne 2015, être en capacité de traiter jusqu'à 100 000 transactions par seconde (5 000 en mode test et 100 000 dans un contexte réel). Ces chiffres sont comparables à ceux de Visa. La posture de SETL est d'utiliser "l'informatique pour simplifier les processus" et perçoivent la DLT comme très prometteuse sur ce front. "Lorsque nous avons lancé Chi-X, cela a fonctionné car, au lieu de prendre un tas de procédures

manuelles à informatiser, on a fait l'inverse – on a commencé avec l'outil informatique, on l'a mis au centre et on a construit les procédures à partir de ça […] La réconciliation est, traditionnellement, très onéreuse – on finit par avoir à réconcilier de nombreuses fois à cause de la diversité des systèmes. Mais la blockchain […] nous permet de ne le faire qu'une seule fois. Le potentiel est énorme[80] ". Clearmatics, une autre start-up DLT qui travaille avec UBS serait, elle aussi, en train d'avancer à grands pas dans ses développements[81].

Dans ce contexte, vu les développements entamés par SETL et, plus généralement, vu la dynamique de recherche et développement en cours travaillant actuellement au déploiement de la DLT à grande échelle, nous posons l'hypothèse que cette question sera à terme techniquement réglée et ne devrait pas être un frein majeur au futur développement de cette technologie. Le suivi de la mise en place d'applications DLT pour des institutions traitant à grande échelle comme Nasdaq ou encore ASX sera un moyen de suivre les progrès effectifs de la DLT en matière de mise en grande échelle. A court terme, nous ne pensons pas que la DLT sera capable de se substituer pleinement à une chambre de compensation (CCP) ou à un dépositaire central (CSD) ; cependant, sur le long terme, une intégration verticale semble possible, à condition que le cadre réglementaire le permette. La DLT pourrait bien présenter l'opportunité d'unifier (et de simplifier) la réglementation existante à travers l'établissement d'un nouveau cadre règlementaire adapté.



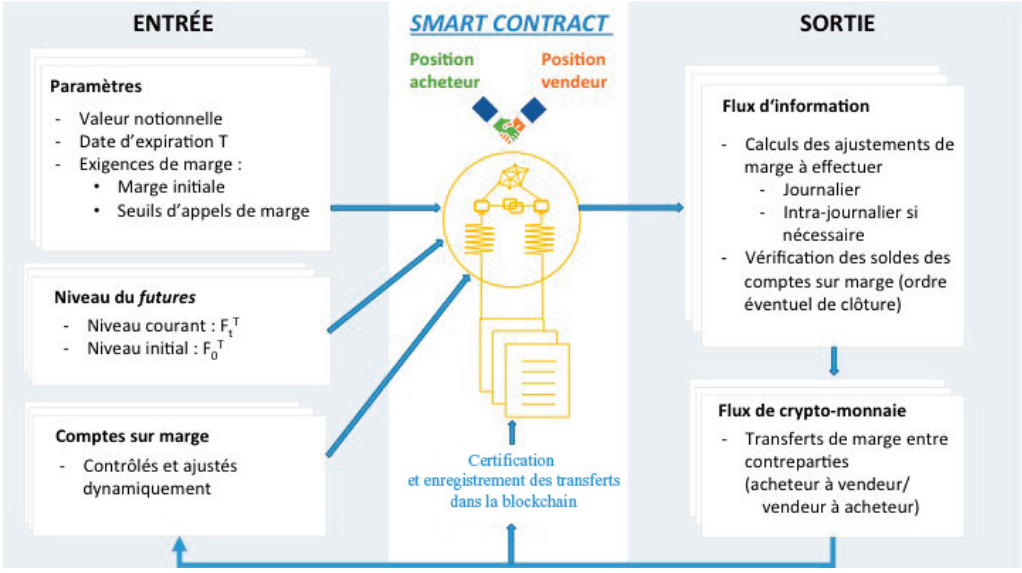
VII. Exemples concrets

En faisant l'hypothèse que les problèmes éventuels de déploiement opérationnel des *smart contracts* seront résolus, nous allons évaluer maintenant deux exemples concrets en prenant une approche prospective dans cette partie de notre article.

7.1. Un *futures* comme *smart contract*

Dans cet exemple, illustré en Figure 4, nous décrivons comment programmer un *futures* comme *smart contract*.

Figure 4 : Un *futures* EUR/USD programmé comme un smart contract



Dans ce simple exemple, on décompose un *futures* sur le taux de change EUR/USD comme un simple *smart contract*. Ce qui est essentiel est de s'assurer que les appels de marge seront bien exécutés, par défaut quotidiennement après la clôture des marchés mais également durant une session (en *intra-day*) si le niveau courant du futures F_t^T fluctue de manière significative durant la journée. S'il est avéré que l'une des contreparties n'a pas les fonds suffisants en crypto-monnaies pour répondre à ses appels de marge, le contrat est immédiatement fermé.

Il est important de remarquer qu'un *smart contract* génère non seulement des flux informationnels, comme les niveaux de marge ou les soldes des comptes de l'acheteur et du vendeur, mais aussi des flux financiers dénominés dans la crypto-monnaie concernée. Dans cet exemple, les marges peuvent être réglées automatiquement et

directement entre les deux parties. En fait, l'intérêt essentiel d'avoir un *futures* géré comme un smart contract sur une plate-forme de registres distribués est que les flux financiers (en crypto-monnaie) entre les contreparties peuvent être complétement automatisés. Une simple API fournissant le niveau du futures F_t^T suffit à automatiser le traitement des appels de marge. Avant que Nakamoto (2008) ne propose sa solution au problème de la double dépense, il n'était pas possible de coupler directement les flux financiers aux flux informationnels sans passer par un tiers de confiance. Cela illustre l'importance du mécanisme de consensus et du protocole de certification (avec ses composantes cryptographiques) utilisés pour la Blockchain dans sa fonction de vecteur des *smart contracts*. Ces derniers mécanismes sont au cœur de la résolution du problème de double dépense, et donc primordiaux pour la sûreté de la technologie des registres distribués.

D'autres exemples plus sophistiqués pourraient être considérés, comprenant par exemple des règles de dénouement anticipé ou bien de *roll-over* des dits contrats. Si nous comparons ces *smart contracts* à d'autres programmes de trading automatisés, leur valeur ajoutée essentielle réside dans le fait qu'ils peuvent donner lieu à des transferts fiduciers automatisés en crypto-monnaie entre les deux contreparties sans passer par un tiers de confiance, ou ici une chambre de compensation. Un point important est que la crypto-monnaie utilisée peut être attachée à un réseau distribué spécifique et programmée pour être utilisée seulement dans un certain nombre de situations anticipées, telles que par exemple les appels de marge ou la gestion du collatéral (comme l'exemple précédent du contrat à terme *futures* l'a illustré). Ainsi l'utilisation de *smart contracts*, pour des transactions de titres financiers primaires ou leurs produits dérivés, devrait permettre une gestion préprogrammée et sans heurt du collatéral requis, et rendre très difficile l'utilisation du même collatéral pour différents engagements simultanés.

De plus, la possibilité de définir et de programmer les contraintes d'utilisation de la crypto-monnaie, et ses tenants et aboutissants, devrait permettre de séparer ou d'isoler les dépôts collatéraux requis pour n'importe quelle transaction. Ainsi les *smart contracts* pourraient représenter une manière sûre et efficace de gérer le collatéral, en l'isolant le cas échéant, pourvu que ce dernier soit directement ou indirectement manipulable par le réseau principal de registres distribués portant ces mêmes *smart contracts*.

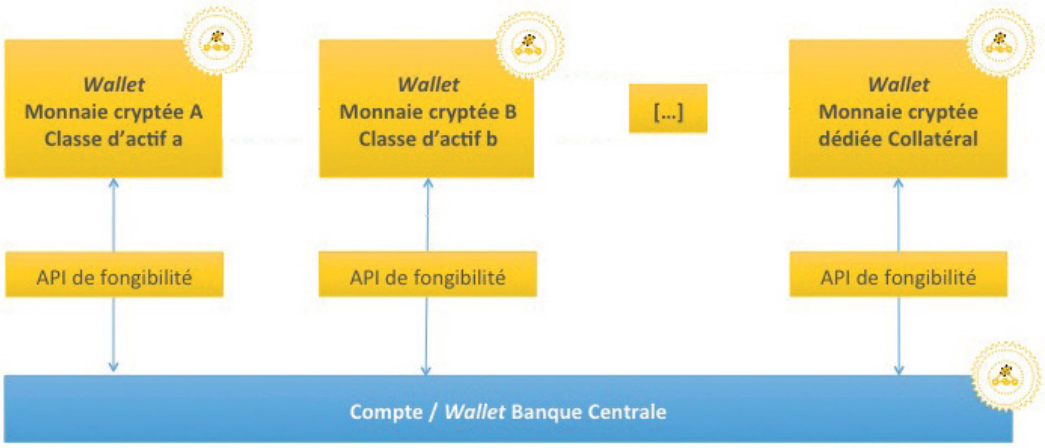
Enfin, nous pensons que la technologie des registres distribués pourrait être exploitée pour gérer des produits structurés complexes tels que des obligations adossées à des actifs (les *collateralized debt obligations* ou CDO). On peut en effet imaginer une blockchain dédiée à un type de CDO donné, gérant ses flux de paiement via un smart contract, à partir d'une mise à jour automatique des informations recueillies sur les actifs sous-jacents. Cela pourrait simplifier la gestion souvent coûteuse et compliquée de l'arrangement des CDOs, tout en facilitant la gestion de leurs risques. Nous estimons en tout cas que le potentiel prometteur de la DLT pour émettre et gérer des produits structurés mérite davantage de recherches et d'investigations.

7.2. Crypto-monnaie collatérale

Le concept de crypto-monnaie collatérale, dédiée à un type unique de transactions et impossible à utiliser hors de ce cadre, pourrait s'avérer particulièrement intéressant pour la gestion du collatéral. Un portefeuille de crypto-monnaie collatérale pourrait être approvisionné avant une transaction. Cette crypto-monnaie collatérale serait portée/stockée par une chaîne dédiée, et transférable uniquement sur cette chaîne afin de garantir la gestion séparée du collatéral. Une telle crypto-monnaie collatérale pourrait être fongible en monnaie régalienne suivant un taux de conversion pré-fixé.

En particulier de telles crypto-monnaies devraient pouvoir être convertibles en monnaie banque centrale, non pour la remplacer mais pour faciliter les mécanismes monétaires. Même si durant certaines périodes un découplement a été observé entre les agrégats M0 et M1 et entre M1 et le taux de refinancement de la Banque Centrale (Giraud, 2012), la monnaie banque centrale demeure bien sûr un élément clé de la politique monétaire. Et nous pensons qu'un système de crypto-monnaies dédiées, non convertibles directement entre elles mais par contre toutes fongibles en monnaie banque centrale, pourrait faciliter la gestion du collatéral et des risques liés aux opérations de refinancement. Une attention particulière devrait être accordée au mécanisme de convertibilité de chaque crypto-monnaie en monnaie banque centrale.

Figure 5 : Crypto-monnaies collatérales dédiées



L'architecture illustrée en Figure 5 n'aurait de sens que si les blockchains envisagées sont capables d'interfacer avec la monnaie banque centrale. C'est pour cela que nous pensons que la technologie des registres distribués ne pourra exprimer son plein potentiel que si les banques centrales, et la BCE au niveau européen, décidaient d'ajuster leurs infrastructures actuelles (T2 et T2S) afin de leur permettre d'interfacer avec les blockchains envisagées. Nous pensons que des prototypes pourraient être mis en place à partir d'APIs dits de fongibilité.

VIII. Recommandations de politique publique

Il est évident d'après la fréquence et la multiplicité des annonces qu'il y a aujourd'hui une course à l'étude et à l'exploitation de la *DLT*. Nous pensons qu'alors que cette technologie présente des attraits potentiels multiples pour les marchés financiers en général, l'implémentation nécessitera un mélange de prudence et d'audace. Il paraîtrait en effet très prématuré de délaisser les infrastructures de marché actuelles pour des alternatives qui n'ont pas encore fait leurs preuves ; mais il semble également très probable que quiconque ignorerait aujourd'hui la DLT risquerait de prendre un retard dangereux par rapport à une concurrence marchant d'un pas décidé.

D'un côté la prudence est nécessaire car l'engouement actuel pour la Blockchain/*DLT* est alimenté par des idées générales sur ce que c'est, comment la technologie fonctionne et ce qu'elle pourrait faire ; cependant, pour la plupart des applications évoquées, peu de propositions détaillées de mise en place ont été fournies, sans même parler de preuves de concept ou de prototypes qui fonctionneraient. De tous les registres distribués, la Blockchain est probablement celui qui a été le plus testé et utilisé. Ethereum semble très prometteur mais en est encore à ses balbutiements. Certaines initiatives de blockchains privées ou de consortium, telles que SETL, sont en phase de test mais peu sont déjà opérationnelles, à l'exception de Ripple. Pour résumer, nous sommes encore au début d'une vague d'innovations et il paraît raisonnable d'attendre encore quelques mois, voire années, avant de se prononcer sur la réussite de telle ou telle initiative.

D'un autre côté, l'audace paraît indispensable car les choses avancent très rapidement et les leaders de demain seront probablement ceux qui seront les plus agressifs aujourd'hui dans l'étude de la technologie, et dans leurs politiques de R&D et d'investissement. Comme nous l'avons souligné au début de cette étude, il est clair que les institutions financières comme les gouvernements sont aux aguets et suivent de près l'évolution des différentes initiatives DLT afin de défendre le cas échéant leurs intérêts commerciaux ou souverains.

En se focalisant sur l'infrastructure des marchés européens, on constate qu'elle est encore essentiellement fondée sur des systèmes parfois assez anciens, avec une implémentation qui dépend encore des juridictions nationales, et que de nombreuses spécificités fiscales ou légales demeurent et compliquent les flux transfrontaliers. Cependant, si l'on regarde les deux dernières décennies, les coûts post-marché ont été grandement diminués et l'intégration des marchés financiers est devenue une réalité favorisée par les plateformes transfrontalières comme T2 (et bientôt T2S). Ainsi, en Europe en particulier, la DLT est en train d'émerger dans le sillage d'un effort transfrontalier récent et majeur d'intégration des marchés de capitaux, effort qui s'est notamment soldé par la mise en place de T2 (et bientôt de T2S). Faire évoluer l'infrastructure financière à cause de la DLT ne prendra tout son sens que si cette technologie est capable de prouver son triple intérêt, à la fois comme outil d'amélioration du fonctionnement des marchés, comme vecteur de renforcement de

la gestion du risque systémique, et comme moteur de simplification de la règlementation financière aujourd'hui devenue très complexe. Et il faudra que les bénéfices de la technologie soient perçus à la fois par les institutions financières et les régulateurs.

Comme cela fut prôné par le Groupe Giovannini, une réglementation destinée à améliorer l'innovation, l'efficience et la sécurité des marchés dans un contexte transfrontalier, devrait être d'autant plus efficace qu'elle sera déployée par paliers et qu'elle arrivera à mobiliser toutes les parties prenantes : les acteurs du marché, les régulateurs, les gouvernements et les instances supra-nationales. De par sa position stratégique d'interlocuteur incontournable, et de par l'intérêt déjà évoqué de pouvoir interfacer des crypto-monnaies dédiées avec la monnaie banque centrale, nous pensons que la BCE a un rôle clé à jouer, avec l'ESMA, pour l'adoption à terme de la technologie.

Nous résumons ci-dessous nos diverses recommandations concernant le déploiement de la technologie, et les thèmes de recherche qu'ils nous semblent indispensables de creuser à l'heure où l'environnement français a été en particulier décrié comme manquant de recherche dédiée sur le sujet :

R1 – Un cadre européen pour les technologies de registres distribués : nous recommandons qu'un groupe conjoint constitué des banques centrales des pays membres de l'Union européenne, et des autorités de marché correspondantes, se saisisse du sujet et fournisse un cadre pan-européen d'étude et d'expérimentation, disponible pour l'ensemble des institutions financières européennes. La coordination d'un tel groupe pourrait être assurée par la Commission européenne.

R2 – Observatoire européen Blockchain/DLT : dans l'esprit de la recommandation précédente, nous pensons qu'un observatoire Blockchain/DLT pan-européen pourrait être mis en place par la Commission européenne. De tels observatoires peuvent bien sûr être mis en place au niveau national mais nous pensons qu'une coordination européenne forte est indispensable pour un déploiement efficace de la technologie, surtout lorsque des interfaces avec les monnaies banque centrale sont à envisager.

R3 – Programmes d'investissement : étant donnée la vitesse de mise en place de nouvelles initiatives de type blockchain au niveau global, nous pensons qu'il est essentiel que l'Union européenne investisse de manière vigoureuse dans la technologie. Là aussi, différents programmes d'investissement peuvent être mis en place au niveau national[82], et le sont déjà dans certains cas, mais nous pensons que la plupart des applications auront besoin d'être développées à une échelle internationale pour être vraiment crédibles. Nous pensons que l'Union européenne pourrait décider de faire de cette technologie une de ses priorités stratégiques, et l'envisager comme une priorité d'infrastructure éligible au Fonds européen pour les investissements stratégiques (EFSI[83]).

R4 – Programmes pilotes : en termes tactiques, nous pensons qu'il serait judicieux de suivre des approches de déploiement prudentes comme l'ASX ou le Nasdaq sont en train de le faire. Ainsi la bourse australienne ASX a déployé une blockchain prototype qui coexiste avec les infrastructures en place, et réduit ainsi le risque d'une transition

prématurée. Une approche de programme pilote est suivie par l'initiative Nasdaq Linq qui se focalise sur des titres privés, évitant ainsi de commencer par des marchés cotés avec de forts volumes transactionnels. Nous pensons que des titres privés non cotés, ou des produits OTC peu liquides, constituent une bonne classe de sous-jacents pour la mise en place d'une blockchain dédiée ou la transposition de leur marché sur une chaîne publique. Il est aussi intéressant de remarquer que les plateformes de finance participative seraient des candidats naturels pour l'enregistrement de leurs transactions sur une blockchain.

R5 – Cadre réglementaire élaboré sur une base internationale : nous pensons qu'il est important de réfléchir dès maintenant à une réglementation qui serait harmonisée sur le plan international. Cependant il est essentiel de ne pas juguler l'innovation par trop de réglementation trop tôt, et de risquer de créer en France en particulier un environnement règlementaire qui serait défavorable à l'innovation et risquerait de pousser les entrepreneurs à l'exil[84]. Il paraît en même temps intéressant de faire avancer dès aujourd'hui certains aspects légaux.

R6 – Attribuer la valeur de preuve aux données de la Blockchain : comme certaines juridictions l'ont déjà fait, il paraît très opportun de permettre aux données qui ont été certifiées sur la Blockchain d'avoir valeur de preuve au regard de la loi[85]. Idéalement, nous pensons que cela devrait être fait par exemple au niveau européen, mais nous recommandons également des initiatives nationales, surtout que ces dernières risquent d'être plus faciles et rapides à mettre en place dans un premier temps[86].

R7 – Micro-crédit, finance participative, et financement de l'économie : la DLT pourrait favoriser le développement de la finance participative et des prêts entre particuliers sans intermédiation par une plate-forme propriétaire comme c'est le cas actuellement. L'essor de ces modes de financement digitaux pourrait s'avérer particulièrement utile si le contexte de taux d'intérêt parfois négatifs, et d'un financement de l'économie difficile, voire en berne, venait à perdurer. La DLT n'est pas conçue comme place de marché ou de négociations, où l'on construit un carnet d'ordres. Mais nous pensons que la technologie pourrait être utilisée comme infrastructure post-marché par les plateformes de finance participative ou de prêt entre particuliers, en offrant à ces derniers le bénéfice de transactions pseudonymes. La législation de la finance participative devra également évoluer afin de refléter l'intégration probable, en aval de ces plateformes, des technologies de registres distribués.

R8 – Comptabilité, audit, conformité, information financière et gouvernance : c'est notre conviction que la DLT devrait s'avérer créatrice de valeur ajoutée à la fois pour les institutions régulées et pour les régulateurs. Nous estimons que la DLT devrait faciliter de nombreuses fonctions d'information financière, de *reporting* et de conformité, et la gouvernance des entreprises en général. Cependant aujourd'hui, et c'est tout à fait normal, la DLT est complètement ignorée par les règles et procédures de conformité. Nous pensons que les associations et organismes professionnels, régissant notamment les normes comptables et les sciences de gestion[87], devraient financer la recherche sur la manière d'intégrer la DLT dans leurs procédures et standards.

R9 – *Big data* et Internet des Objets (IoD) : nous estimons que l'usage croissant des registres distribués devrait alimenter des flux toujours plus importants de données dans tous les secteurs d'activité concernés, tout comme les réseaux sociaux ont créé un foisonnement de données sur les préférences et pratiques des particuliers. Il nous paraît clair que l'intégration de la DLT ne pourra être bien pensée que dans son articulation avec l'Internet des objets (dont elle pourrait être une des courroies de transmission), et la gestion des données massives qu'elle devrait produire. Nous pensons qu'il y a une place importante pour des partenariats de recherche entre industriels, académiques et pouvoirs publics[88] sur ces sujets.

R10 – Cryptographie et signatures digitales : alors que les systèmes utilisant les crypto-monnaies sont susceptibles de se multiplier, il paraît essentiel d'avoir une veille soutenue sur les avancées de la cryptographie. Le système bancaire actuel est déjà très tributaire de procédures cryptographiques et de sûreté informatique, mais la décennie à venir pourrait voir le développement de nouvelles technologies, comme l'avénement de l'ordinateur quantique, susceptibles de fragiliser les systèmes en place, ou en développement comme la DLT. En particulier, nos consultations d'experts nous laissent également penser que plus de recherche est nécessaire en chiffrement homomorphe[89]. En France, nous recommandons que la législation actuelle sur les signatures digitales soit adaptée pour refléter les procédures de multi-signatures qui devraient proliférer avec le développement de la DLT.

R11 – Emploi et métiers : l'impact potentiel de la DLT sur les emplois du secteur financier, en particulier les fonctions des back et middle offices, risque d'être important à moyen ou long terme. Nous ne pensons bien heureusement pas que l'introduction de blockchains devrait être synonyme à long terme de pertes d'emplois importantes dans ces secteurs, mais par contre elle devrait amener une évolution de certains métiers. Nous recommandons la mise en place, sur une base sectorielle, de groupes de travail chargés de suivre l'évolution des métiers potentiellement impactés, coordonnées soit par des instances professionnelles comme la FBF et ses partenaires sociaux pour le secteur bancaire français, soit par un établissement public de recherche comme le CEE[90]. Il nous paraît en tout cas important d'avoir tôt le souci de la formation des personnels concernés afin de familiariser chacun avec les avantages potentiels de la technologie.

R12 – Macro-économie et droits de tirage spéciaux (DTS) : comme nous l'avons précédemment évoqué, nous pensons que la DLT ne montrera son plein potentiel que si elle peut être liée aux, et utilisée par les banques centrales[91]. Une application qu'il nous semblerait particulièrement pertinent d'envisager serait d'utiliser la technologie pour l'émission et la gestion des DTS, tels qu'opérés aujourd'hui par le FMI. Même si nous pensons que cela ne serait envisageable qu'à long terme, une crypto-monnaie avec un fonctionnement similaire à celui des DTS pourrait devenir une référence monétaire internationale dans le futur.

NOTES

[1] Dans ce rapport, nous utiliserons Blockchain avec un b majuscule pour désigner la base de données distribuée du protocole Bitcoin, et utiliserons un b minuscule dans tous les autres cas.

[2] Citation de Robert Shiller, prix Nobel d'économie 2013, lors de sa participation à une table ronde sur le numérique et les marchés financiers au Forum économique mondial de Davos le 24 janvier 2014. Il a néanmoins également qualifié "d'inspiration" cette technologie à cause de sa maîtrise informatique. Source : http://www.businessinsider.com/robert-shiller-bitcoin-2014-1?IR=T

[3] http://www.cnbc.com/2016/01/28/bank-of-america-is-going-big-on-blockchain-plans-to-file-20-patents.html

[4] Selon la rumeur, le Honduras avait également l'intention de développer un système basé sur la Blockchain pour leur cadastre en 2015 ; mais le projet a été abandonné pour motifs politiques, selon la start-up DLT CounterParty, qui aurait été retenue pour le projet - http://www.coindesk.com/debate-factom-land-title-honduras/

[5] http://www.ibtimes.co.uk/credits-testing-kyc-blockchain-isle-man-1520923

6 http://blogs.csc.com/2015/10/30/blockchain-in-healthcare-from-theory-to-reality/

[7] http://www.unic.ac.cy/digitalcurrency

[8] http://www.coindesk.com/openbazaar-live-version-bitcoin-market/

[9] http://www.coindesk.com/visa-europe-remittances-bitcoin-blockchain/

[10] http://www.coindesk.com/korean-bank-developing-blockchain-solution-foreign-exchange/

[11] SWIFT (*Society for Worldwide Interbank Financial Telecommunication* - https://www.swift.com) est un service de messagerie sécurisé entre les institutions financières.

[12] http://www.skuchain.com

[13] Lancé en septembre 2015, R3 CEV a pour mission de collaborer "à la recherche, l'expérimentation, la conception et l'ingénierie […] de solutions [blockchain] pour répondre aux exigences bancaires en termes de sécurité, de fiabilité, de performance, d'évolutivité et de contrôle" (cf. communiqué de presse). Au 22 février 2016, R3 CEV comprenait 43 membres : Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J.P. Morgan, Royal Bank of Scotland, State Street, UBS, Bank of America, BNY Mellon, Citi, Commerzbank, Deutsche Bank, HSBC, Mitsubishi UFJ Financial Group, Morgan Stanley, National Australia Bank, Royal Bank of Canada, Skandinaviska Enskilda Banken, Société Générale, Toronto-Dominion Bank, Mizuho Bank, Nordea, UniCredit, BNP Paribas, Wells Fargo, ING, MacQuarie, the Canadian Imperial Bank of Commerce, BMO Financial Group, Danske Bank, Intesa Sanpaolo, Natixis, Nomura, Northern Trust, OP Financial Group, Banco Santander, Scotiabank, Sumitomo Mitsui Banking Corporation, U.S. Bancorp and Westpac Banking Corporation.

[14] En février 2016.

[15] Les 30 membres fondateurs de Hyperledger sont: ABN AMRO, Accenture, ANZ Bank, Blockchain, BNY Mellon, Calastone, Cisco, CLS, CME Group, ConsenSys, Credits, The Depository Trust & Clearing Corporation (DTCC), Deutsche Börse Group, Digital Asset Holdings, Fujitsu Limited, Guardtime, Hitachi, IBM, Intel, IntellectEU, J.P. Morgan, NEC, NTT DATA, R3, Red Hat, State Street, SWIFT, Symbiont, VMware et Wells Fargo.

[16] ASX a investi dans Digital Asset Holdings, en compagnie de ABN AMRO, Accenture, BNP Paribas, Broadridge Financial Solutions, Inc., Citi, CME Ventures, Deutsche Börse Group, ICAP, J.P. Morgan, Santander InnoVentures, The Depository Trust & Clearing Corporation (DTCC) et PNC Financial Services Group, Inc.

[17] http://www.coindesk.com/intel-testing-blockchain-built-fantasy-sports-game/

[18] Communiqué de Presse DTCC Press, 25 janvier, 2016 : "New DTCC White Paper Calls for Leveraging Distributed Ledger Technology to Solve Certain Long-Standing Operational Challenges" – accessible depuis le 22 février 2016 à : http://www.dtcc.com/news/2016/january/25/new-dtcc-white-paper-calls-for-leveraging-distributed-ledger-technology

[19] Rien qu'en France, la part des créations d'emploi liée à la gestion des transactions et au IT est en croissance constante depuis plusieurs années (2015, Observatoire des métiers dans la banque).

[20] Dans le cas d'un ensemble de serveurs fédérés, les données à traiter sont divisées horizontalement entre les serveurs qui partagent le travail. Les serveurs sont gérés séparément mais collaborent en réseau. Comme les différents serveurs participant au réseau sont généralement tous programmés par une même autorité centrale, cette configuration doit être considérée comme une architecture centralisée.

[21] Il est intéressant de remarquer qu'aujourd'hui encore, COBOL, un langage de programmation créé en 1959, est très utilisé dans le secteur financier.

[22] Pour une illustration de ce type de raisonnement voir DFIN-511 / Session 2, Introduction to Digital Currencies, University of Nicosia, 2015.

[23] Nous indiquons des références pour chaque développement cité, y compris ceux qui ne figurent pas dans le livre blanc de Nakamoto.

[24] Le cryptologue français Jacques Stern écrit dans "La science du secret" (1998) , que ce rapport est tellement fondamental à la cryptographie que l'on peut dire qu'il y a un "avant" et un "après" l'introduction de ce concept clé.

[25] http://hashcash.org/papers/announce.txt

[26] http://www.dsi.unive.it/~marek/files/04.55%20-%20peertopeer.pdf

[27] Comme Nick Szabo l'a dit lui-même Durant la conférence DevCon1 Ethereum Developer Conference le 13 novembre 2015; vous trouverez le vidéo à : https://www.youtube.com/watch?v=YpSeOU1VVj4

[28] À propos des smart contracts : http://szabo.best.vwh.net/formalize.html

[29] À propos de colored coins/proplets: http://szabo.best.vwh.net/proplets.html

[30] Cela donne 2^{256} combinaisons potentielles, soit 10^{77}, ce qui représente bien plus que le nombre d'atomes sur Terre, estimé à environ 10^{50}, et un peu moins que le nombre d'atomes composant l'univers, estimé à 10^{81}.

[31] Afin de changer la graine (*seed* en anglais) d'un générateur de nombres aléatoires (afin de s'assurer que deux adresses bitcoin générées soient différentes), on crée de l'entropie, en demandant, par exemple, aux utilisateurs de déplacer leur souris de façon aléatoire, comme c'est le cas sur le site générateur d'adresses bitaddress.org.

[32] On pourra à ce sujet consulter: "Mapping the Bitcoin Economy Could Reveal Users' Identities", par Tom Simonite, MIT Technological Review, September 5, 2013.

[33] Les e-wallets bitcoin sont le plus souvent implémentés sur des smart phones, et les adresses bitcoin qu'ils créent ne sont pas toujours facilement traçables aux propriétaires de smart phones correspondants.

[34] Par exemple, une approche de type *soft fork* a été adoptée lors de l'introduction des transactions Pay-to-script-hash (P2SH) par le *Bitcoin Improvement Proposal* (*BIP*) *16*. Ces transactions permettent l'envoi de bitcoins vers des adresses de type *script hash* (commençant par un 3) au lieu des addresses de type *public key hash* (commençant par 1).

[35] On estime la capacité maximale du réseau Bitcoin à 7 transactions/seconde. En comparaison, le réseau Visa peut supporter des pics d'activité d'environ 56,000 transactions/seconde.

[36] Par exemple, la *soft fork* "Segregated Witness" (segwit), devrait permettre une augmentation dans la capacité du réseau Bitcoin : https://bitcoincore.org/en/2016/01/26/segwit-benefits/

[37] Une représentation visuelle de l'histoire des crypto-monnaies est disponible sur http://www.mapofcoins.com

[38] Le lecteur pourra consulter le site http://www.coinmarketcap.com pour une liste des crypto-monnaies et leurs capitalisations respectives.

[39] Source : http://www.ethereum.org

[40] "*On public and private blockchains*", article posté sur le Crypto Renaissance Salon, le 7 août 2015.

[41] Certains experts informatiques comme Vitalik Buterin semblent se demander, cependant, si d'autres techniques cryptographiques comme les preuves à divulgation nulle de connaissance ne seraient pas plus efficaces dans un context privé. Sur les procédés de certification cryptographique, Buterin déclare "qu'il n'y a pas de raison de croire qu'un procédé optimal d'authentification devrait consister en une série de paquets de données liés par leurs empreintes et contenant des racines de Merkle ; de manière générale, les preuves à divulgation nulle de connaissance offrent une gamme de possibilités très stimulantes pour permettre les garanties cryptographiques que les utilisateurs sont en droit d'attendre de leurs applications."

[42] Ce livre blanc peut être trouvé sur http://www.blockstream.com. Blockstream, qui offre des solutions de *sidechains*, a récemment annoncé une levee de fonds de $55 millions.

[43] On pourra par exemple consulter Multichain, une plate-forme *open source* de développement de blockchains privées, compatibles avec Bitcoin Core. Son livre blanc peut être consulté sur http://www.multichain.com.

[44] Source : http://www.ethereum.org

[45] Source : http://www.ripple.com

[46] Nous pourrions citer comme exemple le cas de la faillite de la bourse d'échange de bitcoins Mt Gox. Le responsable de la plateforme a prétendu que la "disparition" des bitcoins dont ses clients ont souffert était due à un défaut technique du protocole Bitcoin, que l'on appelle la "malléabilité des transactions" (*transaction malleability*). Il s'avéra, au final, que cette faiblesse sécuritaire, existante dans la première version du protocole Bitcoin, avait en fait déjà été traitée et n'était pas la cause de la disparition des fonds (d'autres plateformes avaient déjà corrigé le problème).

[47] Source: Financial Times, "Mt Gox founder Mark Karpelès charged with embezzlement", article de Leo Lewis, 11 September 2015.

[48] http://www.bloomberg.com/news/articles/2015-09-21/bitcoin-firm-chief-pleads-guilty-to-first-of-its-kind-ponzi-scam

[49] La clé privée à partir de laquelle une adresse bitcoin est générée permet à quiconque la possédant de contrôler les bitcoins lui étant associés. Il est important de savoir que ne pas partager la clé publique correspondante augmente aussi le niveau de sécurité. En effet, les adresses bitcoin sont générées par les clés publiques (via l'utilisation de fonctions à sens unique), elles-mêmes générées par les clés privées.

[50] Certains auteurs utilisent le terme de "réseau sans confiance", une expression qui ne nous semble pas juste car les utilisateurs de Bitcoin doivent précisément avoir confiance en l'intégrité du protocole et d'une majorité des nœuds du réseau.

[51] Dr. Dirk Haubrich, à la tête du département de protection des consommateurs et de l'innovation financière de l'Autorité bancaire européenne (ABE), déclara que l'attaque des 51% représentait un des risques qu'il percevait comme les plus importants dans le cas d'une adoption de masse des monnaies numériques. Source: http://www.newsbtc.com/2015/06/17/eba-sees-51-attack-as-bitcoin-s-biggest-threat/

[52] Une carte mondiale des nœuds de minage est disponible sur : http://bitnodes.21.co/

[53] Comme SHA-1 par exemple

[54] Par ailleurs, il est important de noter que te tels développements ne compromettraient malheureusement pas uniquement l'intégrité des protocoles de monnaies cryptées comme le Bitcoin mais pourraient, malheureusement, affecter l'intégrité du système bancaire actuel.

[55] http://www.proofofexistence.com/

[56] http://virtual-notary.org

[57] https://bitproof.io/

[58] See factom.com or factom.org

[59] See stratumn.com

[60] Voir ledgerwallet.com

[61] https://paymium.com

[62] http://lamaisondubitcoin.fr

[63] Pour une cartographie des distributeurs automatiques de bitcoins dans le monde, voir Coindesk: http://www.coindesk.com/bitcoin-atm-map/

[64] https://www.legifrance.gouv.fr/affichCode.do;jsessionid=6EB229C62D0DBC17A2BAF3350E6DFCB3.tpdjo11v_3?idSectionTA=LEGISCTA000020869628&cidTexte=LEGITEXT000006072026&dateTexte=20110624

[65] En exerçant à l'échele européenne sous "Libre Prestation de Service": https://acpr.banque-france.fr/fileadmin/user.../form_LPS_EP.doc

[66] http://www.coindesk.com/how-payment-giants-are-embracing-bitcoin-and-blockchain/

[67] IC3 initiative (en mars 2016) : Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, Dawn Song, et Roger Wattenhofer des institutions suivantes : Cornell, Jacobs, Cornell Tech, UMD, ETH, Berkeley, NUS.

[68] Une contrainte à garder en tête pour les systèmes distribués est le théorème CAP (ou de Brewer) qui affirme qu'il est impossible à un système informatique de calcul distribué de garantir de manière synchrone (i) la cohérence des données, (ii) la disponibilité (afin de garantir que toutes les requêtes recevront une réponse) et (iii) la tolérance au partitionnement du réseau.

[69] Un des experts rencontrés s'est amusé à comparer l'utilisation du réseau Bitcoin pour se payer un café à prendre une voiture de Formule 1 pour se rendre au coin de la rue.

[70] Le livre blanc de Blockstream sur les *sidechains* est disponible à: https://blockstream.com/wp-content/uploads/2014/10/sidechains.pdf

[71] In Poon, J., & Dryja, T. The Bitcoin Lightning Network : https://lightning.network/lightning-network-paper.pdf

[72] L'annonce a été faite le 22 Janvier 2016.

[73] https://nxt.org

[74] Par exemple, des niveaux spécifiques de delta hedging pourraient être pré-programmés dans un *smart contract*, forçant l'achat ou la vente d'une certaine quantité pré-définie du sous-jacent, lorsque son cours atteindrait certains niveaux décidés à l'avance. Les positions de sortie pourraient aussi être programmées dans l'optique d'un dénouement de position.

[75] Par exemple, Skuchain (www.skuchain.com) propose d'utiliser la DLT pour faciliter et désintermédier le commerce B2B et la gestion de la chaîne logistique.

[76] http://ec.europa.eu/finance/capital-markets-union/docs/building-cmu-action-plan_en.pdf

[77] https://www.banque-france.fr/stabilite-financiere/infrastructures-des-marches-financiers-et-moyens-de-paiement-scripturaux/infrastructures-des-marches-financiers/traitantlestitres.html

[78] https://www.banque-france.fr/stabilite-financiere/infrastructures-des-marches-financiers-et-moyens-de-paiement-scripturaux/target2-banque-de-france.html

[79] http://www.ibtimes.com/real-reason-everyone-calls-billion-dollar-startups-unicorns-2079596

[80] http://www.bankingtech.com/348852/blockchain-based-setl-plans-to-revolutionise-payment-and-settlement/

[81] http://www.bloomberg.com/news/articles/2015-11-18/ubs-blockchain-partner-clearmatics-raises-funds-for-digital-coin

[82] Par exemple dans "*Les enjeux des chaînes de consensus pour la place financière de Paris*" (Mars 2016), le think tank CroissancePlus recommande l'allocation de €500 millions à la technologie Blockchain (à financer à partir des €10 milliards attendus pour le PIA3).

[83] *European Fund for Strategic Investments*, aussi appelé communément "Plan Juncker".

[84] En France, un colloque organisé le 24 mars 2016 dans les locaux de l'Assemblée Nationale par le CSSPPCE et le CHECy aura souligné la peur de certains participants d'avoir "trop de régulation trop tôt", ce qui risquerait d'inciter les startups françaises travaillant sur la DLT à s'exiler.

[85] L'État du Vermont est actuellement en train d'étudier une proposition de loi qui demande l'octroi de la valeur de preuve devant un tribunal aux données de la Blockchain. Réf. http://legislature.vermont.gov/bill/status/2016/H.737

[86] En ce qui concerne la France, nous soutenons la recommandation de CroissancePlus sur le sujet. Source : “Les enjeux des chaînes de consensus pour la place de financière de Paris” @ www.croissanceplus.com

[87] Par exemple l’Autorité des Normes Comptables (ANC - http://www.anc.gouv.fr) ou la Fondation Nationale pour l’Enseignement de la Gestion des Entreprises (FNEGE - http://www.fnege.org) en France.

[88] Par exemple l’Agence de l’Environnement et de la Maîtrise de l’Énergie (ADEME - http://www.ademe.fr/) en France, lorsque ces projets favorisent des “pratiques énergétiques intelligentes” et la transition écologique.

[89] Le chiffrement homomorphe permet à un tiers de faire des calculs sur des messages chiffrés sans les déchiffrer mais tout en ayant un résultat utilisable. En France, nous pensons que le CHECy (http://checy.org/) serait un candidat naturel pour assurer une veille des techniques de chiffrement applicables aux blockchains/DLT.

[90] The Centre d’études de l’emploi (CEE) is a public research organization focused on employment.

[91] Il est intéressant de remarquer que les banques centrales de Chine (http://www.ibtimes.co.uk/chinese-central-bank-launch-its-own-digital-currency-1539279), du Royaume-Uni (http://cointelegraph.com/news/bank-of-england-to-launch-its-own-cryptocurrency) et des Pays-Bas (http://www.coindesk.com/dutch-central-bank-to-create-dnbcoin-prototype/) ont déjà annoncé en 2016 vouloir lancer leur propre crypto-monnaie (ou s’intéresser de près à la question).

Blockchain and distributed ledger technologies (DLT): what impact on financial markets ?

Alexis Collomb
Professor at Cnam – Finance

Klara Sok
PhD Candidate at Cnam, Dicen-IDF research center

Foreword

The foundations of the Bitcoin protocol and the crypto-currency it supports first emerged in 2008 via a white paper circulated on a cryptography mailing list by a certain Satoshi Nakamoto. Soon thereafter, in January 2009, the first bitcoin transaction was recorded on the Blockchain[1], a distributed ledger that is essentially a chain of blocks of information. Today, over seven years later, the Blockchain has become a hot topic of discussion and numerous reports have recently been published on its generic affiliate known as Distributed Ledger Technology (DLT).

If we look at the significant press coverage devoted to Bitcoin and Blockchain over the last six months, our initial reaction could be to discount the phenomenon as an example of Keynes's animal spirits' herding instinct, Girard's mimetic forces, or as a simple fad. The craze has even prompted some prominent economists to call Bitcoin/Blockchain an "amazing example of a bubble".[2] Yet, there is significant factual evidence to show that the Bitcoin network and its derivatives have not only been resilient, but are continuing to draw interest and investors. Although we will avoid the quagmire of forecasting the future of Bitcoin and similar crypto-currencies, we believe that it is probably brighter than many think.

It is clear that the conceptual foundations of Bitcoin and its underlying distributed ledger, commonly referred to as the Blockchain, are now prompting many institutions to rethink their existing information systems and business processes. The financial services industry in particular, with its manifold payments and transactions, is currently investigating how distributed ledgers could be used to improve or optimize existing market infrastructure.

This report attempts to summarize the key issues of distributed ledgers and take a look at how they could be integrated into financial markets, especially at the post-trade level. Our approach is non-exhaustive and necessarily cross-disciplinary with a certain dose of foresight. We certainly do not claim to have mastered the subject: it is far too vast and complex and the wave of transformation too fast-moving to be addressed in a single general paper. But our investigation has convinced us that the disruptive potential of the technology is real. We hope that this report will provide a useful compendium on the subject for market infrastructure providers and many others who are considering the risks and opportunities that DLT could represent.

The views expressed in this paper are those of the authors and do not necessarily reflect those of the AMF, the Cnam, the Louis Bachelier "Finance and Sustainable Growth" Laboratory, or any of their affiliates.

Abstract

In the first half of this report, we provide a brief history of the emergence of crypto-currencies and summarize the key features of the Bitcoin protocol and its underlying distributed ledger, the Blockchain. We then discuss some of the recent technological issues that have split the Bitcoin community before introducing a typology of distributed ledgers necessary to understand their various contexts of application. Next, we focus on the safety and security of distributed ledgers, an aspect that has sparked angst and skepticism in the past, and clearly remains a focal point for the financial services industry.

In the second half of this paper, we list some of DLT's main potential applications, in particular for the financial services industry. We then focus on how DLT could be integrated into the existing post-trade infrastructure. In the final sections, we present some concrete examples and finish with a set of policy recommendations and various considerations for those contemplating implementing this technology.

1. Distributed Ledger Technology (DLT): A tsunami for change or a red herring?

1.1. The blockchain hype: from financial services to education and government

The blockchain hype has reached every sector of the economy. Both private and public sector organizations across the globe have publicly demonstrated an increased interest in the technology, and shared their clear enthusiasm for it. Initiatives have flourished and numerous reports have been published by financial institutions and public agencies at an accelerated pace from the end of 2015. As a matter of fact, most of these publications praise the disruptive aspects of the technology while taking a didactic approach designed to educate the reader on blockchain. While it is not the aim of this report to provide an exhaustive list of existing initiatives, the authors have chosen to cite some of the more significant projects under development in order to give the reader a sense of the nature, the diversity and the magnitude of the blockchain phenomenon.

Before mentioning any specific initiative, it is important to note that increased public awareness and the concomitant development of complementary innovations such as colored coins, sidechains and smart contracts, have enriched the original blockchain concept, feeding an innovation cluster (Schumpeter, 1935) in Digital Ledger Technologies (DLT). The DLT cluster, has significantly increased the original Bitcoin/Blockchain's perceived potential (Nakamoto, 2008), attracting incremental productive efforts from many more sources, both in the form of investments and labor.

Although it is inspired by existing technologies, DLT goes beyond shared ledgers on the one hand and distributed database solutions on the other hand. In fact, DLT comprises both distribution characteristics and the trustworthiness of ledger records.

Furthermore, there is considerable ongoing cogitation and debate on just how widely distributed blockchains should be and whether they should be public or private, or a hybrid combination. The issue is currently segmenting the DLT innovation landscape, contributing to the diversity and depth of the innovation cluster itself. What appear to be straightforward technological choices are far more than that: they are in fact intertwined with the consensus mechanisms that constitute the very foundation on which the organization and governance of blockchain is built; and they are key to DLT's present and future development.

Last but not least, just as DLT players must answer key questions related to the openness of their network, public authorities may be prompted to re-think the way they supervise and regulate business and productive human organizations, be it for licensing, taxation or intellectual property. In terms of DLT-related intellectual property

rights, while the community of core Bitcoin/Blockchain programmers made the original protocol and its Blockchain an open-source code accessible to the initiated and general public, some players are said to be attempting to file DLT-related patent applications. Bank of America, for example, is reported to have filed 15 patent applications with the US Patent and Trademark Office so far[3] and plans to further develop their intellectual property strategy to cover many more application fields. This IP strategy clearly departs from the open source philosophy of the Bitcoin/Blockchain initial community, and shows how large financial institutions are seeking first mover's advantage in the DLT space.

The following are some of the main initiatives in the area of blockchain, which, as you will see, go far beyond Bitcoin wallets and exchanges.

At the government level, the United Kingdom's Office for Science, in its report "Digital Ledger Technology: beyond blockchain" (January 2016), clearly shares hopes that DLT will be "one of those potential explosions of creative potential that catalyze exceptional levels of innovation." The Office for Science addresses the need for the UK Government to quickly and forcefully provide and coordinate resources in order not to miss out on DLT promises in the face of international competition. And they are actively encouraging key players in digital project development, such as the recently launched Alan Turing Institute, the Digital Catapult Centre, the Open Data Institute and the Whitechapel Think Tank, to work together towards this goal.

Ghana is developing blockchain projects for land registry[4] while Estonia is working on offering a blockchain-based public notary service to e-residents through their Keyless Signature Infrastructure program. The Isle of Man is testing a KYC blockchain with the Credits[5] start-up and fostering DLT with the intent that it should be openly available to its citizens.

In the healthcare sector, electronic health records are being tested using DLT.[6] Start-ups such as Factom (with healthcare player HealthNautica) or BitHealth, already provide such services. Secured encrypted records available only to private key holders might indeed fit the healthcare sector's needs for privacy and confidentiality. Bloc Verify offers certification through encryption in a blockchain designed to combat counterfeit drugs. Large player Philips Healthcare Group is said (twitted) to be partnering with the start-up Tierion on an initial blockchain project. DNA.bits combines Big Data and DLT to store and share authenticated genetic data with correlated clinical records while securely maintaining anonymity for that data.

In education, the San Francisco based Holberton Software engineering school and the French Ecole Supérieure d'Ingénieurs Léonard-de-Vinci (ESILV) announced that they would store and authenticate their academic certificates on the Bitcoin blockchain while the University of Nicosia in Cyprus launched their MSc Degree in Digital Currency as part of the island state's clearly-stated goal of becoming a hub for "Bitcoin trading, processing and banking."[7]

In the Humanitarian sector, the Blockchain Emergency ID (BE-ID) project, part of the BitNation Refugee Emergency Response (BRER), is an identification project that uses blockchain technology to provide refugees, Syrian and others, with a digital identity

that meets UN travel documentation standards. Moreover, BitNation is also providing refugees with other services, including a Bitnation Bitcoin Visa Card.

On the e-commerce front, OpenBazaar, a recently launched e-commerce platform,[8] aims at becoming a totally decentralized competitor to eBay. Once operational, the platform will accept only bitcoin as payment. While US e-commerce giant Overstock.com still relies on an off-blockchain trading platform, it has announced that it is developing a blockchain-based securities exchange, Medici, with DLT start-up Counterparty. Visa[9] is also said to be testing DLT for their payment services, while the Korean KB Kookmin Bank[10] has announced that they are developing DLT solutions using the Blockchain to support their remittance business, currently intermediated by SWIFT.[11] In logistics and trade finance, Skuchain[12] offers blockchain-based products for B2B trade and supply chain finance.

Last but not least, DLT has garnered tremendous interest in the financial services industry where individual and collaborative initiatives and projects abound. Industry-wide initiatives such as the R3 CEV banking consortium,[13] launched in September 2015, is developing Proof of Concept (PoC) systems using Ethereum[14] and has hired top-tier developers such as former IBM director Richard Brown and former Bitcoin developer Mike Hearn. In parallel, R3 CEV is one of the 30 founding members of the Linux Foundation's cross-industry Hyperledger Project, whose mission is to develop DLT alternatives to the Bitcoin or the Ethereum blockchains.[15]

Digital Asset Holdings (DAH), launched in March 2015 by Blythe Masters, former head of JP Morgan's global commodities unit, is building a DLT-based processing service for financial institutions, such as the Australian Stock Exchange (ASX).[16] DAH is already considered a dominant player in this fledgling industry, partnering with large solution providers and facilitators such as Accenture, PWC and Broadridge to scale their business to common global clients. It is worth mentioning that as a founding member of the DLT initiative, Digital Asset Holdings offered Linux Foundation the *Hyperledger* trademark which they had acquired the previous year along with the Hyperledger start-up. Deloitte Canada and Deloitte Luxembourg are working together on Rubix, a project that should eventually allow clients to create their own smart contract-based DLT applications.

Nasdaq is using a DLT-based shareholder voting system for international Estonian e-residents and is currently developing a DLT project for the transfer and record-keeping of unlisted securities in their Private Market segment, complementing their existing ExactEquity cloud-based equity management solution. Intel is said to be currently testing blockchain technology to exchange shares of videogame-based football teams.[17] The videogame, still an in-house project not yet commercialized, currently serves as a prototype within the framework of the Hyperledger project.

Post-trade infrastructure players formed the *Post Trade Distributed Ledger Working Group*, currently composed of the CME Group, Euroclear, LCH.Clearnet, the London Stock Exchange, Société Générale and UBS. At an individual level, Euroclear and Depository Trust & Clearing Corporation (DTCC) published reports within a few days of each other. DTCC "calls for industry-wide collaboration in leveraging distributed ledger technologies to modernize, streamline and simplify the siloed design of the

financial industry infrastructure and address certain limitations of the current post-trade process",[18] while Euroclear (February 2016) states that "the industry needs to take a collective view on the potential of the technology" and "work with innovators to develop standards, while also preserving the existing strengths of the ecosystem, and navigating the complex worlds of regulation and legal oversight."

These players see transparency, security, traceability and cost efficiency as the main advantages of DLT. And since those four characteristics are desirable features of a sound and efficient financial industry, it is not surprising that they constitute a strong incentive to invest in DLT.

But if we are to assess the impact of DLT on financial market infrastructures and evaluate the potential cost of technological change, it is important to begin by taking stock of existing solutions available to the industry.

1.2. Are shared databases and distributed protocols truly a new phenomenon for the financial services industry?

Information technology has played a key role in the development of modern financial services. As underlined by Shiller (2003), it is the development of information technology that has made possible the proliferation of many, if not all, contemporary financial services. Improvements in information infrastructure have been essential for modern financial plans as they allowed the transformation of countless stacks of paper, hard to classify and archive, into electronic data. Because they are now capable of better managing data and information, banks have been able to expand their product offerings, improve their processes and keep track of the increasing number of transactions.[19] And be it in area of securitization, derivatives, or just plain commercial banking, financial institutions now rely on information systems and databases to do business.

It is therefore not surprising that banks place a strong emphasis on solid IT teams, especially as the subject of cyber-security is of paramount importance to the banking system. Until now, the prevailing default consensus in the industry has been to rely on a centralized IT architecture. And from central banks to retail agencies, this IT paradigm has given rise to a pyramid of successive client-server relationships, whereby at each level, one centralized server, or a set of federated servers,[20] caters to multiple clients. This is perfectly understandable: a national central bank will want to track the licensed banking entities into which it feeds money, while a retail bank will want to retain control over all its client accounts and track their activities.

The centralized ledger model has prevailed in any situation where a trusted record keeper is needed, and where security and control are essential. In a non-banking field for example, there has been a surge of biometrical data around the world as governments try to replace old passport systems with various new identification techniques. There again, the information is kept in large centralized databases, while security for this highly sensitive information is essential as identity theft could have devastating consequences.

So, if digital ledgers have existed in the banking industry for decades,[21] what explains the sudden hype over distributed ledger technology? Proponents of the Blockchain and DLT usually put forward three potential deficiencies of centralized ledgers controlled by a trusted third-party: (i) the trust depository may not really be trustworthy and may be subject to bribery and other forms of corruption; (ii) the controller of the centralized ledger may censor or reject certain market participants on subjective and/or discriminatory grounds; (iii) centralized ledgers are not immune to loss of records. The Blockchain, with its decentralized consensus-reaching mechanism, its open-source approach, and multiple copies of the Blockchain available for all to see, is capable of addressing all these concerns.[22]

Yet beyond these practical motives, there is another force at work in the financial sector that accounts for the growing interest in DLT and a possible switch-over from the current centralized model: the rise of shadow banking and increased bank disintermediation that comes with it, is leading many to speculate on the potential "end of banking" (McMillan, 2014). With digital finance, crowdfunding, and peer-to-peer lending platforms, borrowers and lenders can find each other without bank intermediation (Collomb, 2015). Yet, they still depend on centralized digital platforms. DLT however, raises the prospect of doing without central intermediaries, be it a bank or a centralized digital platform! To use the well-known example of taxi services, although Uber provides an *uber-friendly* digital platform that greatly facilitates matching demand with supply via a simple smartphone application, all the transactional data still ends up on a centralized ledger controlled by Uber. With the Blockchain and DLT, there is no Uber-like centralized platform.

DLT is able to lure various market participants with the promise of potentially "uberizing Uber", i.e. the possibility of switching from a centralized digital database architecture to a genuinely decentralized one where it is the entire system rather than a dominant party that acts as the trusted record-keeper. But because DLT is both relatively complex to understand and still evolving, actors are not yet able to distinguish between fantasy and reality, and there is still a certain cloud of confusion hovering over its potential applications.

But there we have it: if until now the idea of banks sharing their information on common distributed ledgers would have seemed ludicrous to many, the growing interest in DLT has opened up a new line of thinking in the financial services industry as regards sharing and distributing data, and this new paradigm has materialized with consortium initiatives such as R3 CEV and many others previously mentioned.

2. Key features of DLT

2.1. History of Bitcoin/Blockchain

Bitcoin is the first successful cryptocurrency to be put into circulation without the need of an intermediary. While cryptocurrencies have been around for decades, with initiatives such as David Chaum's ecash or DigiCash (1981, 1983), until Bitcoin, none of them had ever found a way to securely by-pass a trusted third party. The trusted third-party had always been needed to check that digital money had not already been spent, an issue that does not exist with physical currency. Satoshi Nakamoto (a pseudonym), in his 2008 white paper introducing Bitcoin, proposed the first working solution to the so-called "double spending" problem ever published. In the white paper, he directly and indirectly cites several core computer science and cryptographic developments of the late twentieth century: [23]

(i) The cryptographic use of hash functions that were made possible by Diffie and Hellman's seminal research on "New directions in cryptography" (1976) that first introduced the concept of public key cryptography,[24] Rabin's work on "Digitalized signatures" (1978), Yuval's answer to Rabin "How to swindle Rabin" (1979), and Merkle's paper on "Secrecy, Authentication and Public Key Systems" (1979);

(ii) Cipher block chaining (CBC), presented in FIPS PUB 46 (US Federal Information Processing Standards Data Encryption Standard) and approved as a Federal Standard in 1976, was co-developed by IBM and the National Security Agency (NSA) in the 1970's in response to a US government request for encryption algorithms (Preneel, 2007). FIPS DES were developed by the US government in order to protect sensitive but unclassified information and can be used by other parties without paying a license fee, which is very close to the original philosophy underlying the Bitcoin protocol;

(iii) Proof of work, introduced by Cynthia Dwork and Moni Naor in their 1993 paper entitled "Pricing via Processing or Combatting Junk Mail" where they propose deterring junk mail by increasing its cost, whereby "the main idea is to require a user to compute a moderately hard, but not intractable, function in order to gain access to the resource, thus preventing frivolous use." The concept was further developed by Adam Back via his Hashcash proof-of-work system designed to limit spam and denial-of-service attacks. Hashcash was first announced in May 1997 to the cypherpunks@toad.com mailing list[25] and formally published in 2002;

(iv) The Merkle Tree compression mechanism (1979), used for saving and secure verification of large data structures, and by the Bitcoin protocol, for calculating the merkle root of all transactions included in a block;

(v) Timestamping, a centuries-old concept in its paper form with a digital avatar that was developed for information technology security applications during the 1990s (Une, 2001);

(vi) Peer-to-peer (P2P) technology, famously put into application by Shawn Fanning in June 1999 for the music-sharing platform Napster. Napster, however, relied on a central server (the "farm") which was used by the network as the central registry for the list of files owned and requested by peers – it constituted Napster's single point of failure and was eventually shut down by the FBI in 2001 for breaching intellectual property law. Gnutella,[26] the first widely used, *fully distributed* P2P file transfer platform, was developed in 2000 by Tom Pepper and Justin Frankel for Nullsoft.

Bitcoin's innovation resides primarily in the original combination it makes of various advances in computer science such as peer-to-peer protocols and cryptographic functions. Admittedly, Bitcoin/Blockchain is a recent phenomenon, but the authors believe that the Bitcoin protocol and its offspring are likely to prove to be a paradigm-changing tipping point in the development of new autonomous organizational forms for exchanging, authenticating, certifying, notarizing and settling transactional information.

Bitcoin, as a distributed transferable and immutable data registry, has paved the way for concrete applications of other innovations that enrich the DLT space such as smart contracts, colored coins, sidechains and alternative incentive systems, such as proof-of-stake mechanisms, and other transactional systems - some of which have been adopted by traditional economic players. Similarly, the distributed ledger Ethereum, based on the ether crypto-currency, has already partnered with traditional technology players such as Microsoft to develop their virtual machine project.

Interestingly enough, some of these developments have been around for decades. For example, Nick Szabo has been working on smart contracts and colored coins since 1998[27] and first published on the subject in 2001.[28, 29] He explained how smart contracts, if "embedded in the world", i.e. in the "hardware and software we deal with" can "make breach of contract expensive (sometimes prohibitively so) for the breacher." Szabo refers to colored coins, as "proplets" or "devices for controlling property"; he believes that they define the "basic security architecture for local evidence gathering, enforcement, and negotiation of [property rights, contracts and tort] laws."

A number of Distributed Autonomous Organizations (DAOs), are currently being rolled-out. DAO is a concept introduced by Ethereum's co-founder Vitalik Buterin (2014), based on Friedrich von Hayek's (1979) utopian ideal of "spontaneous order" (Zacklad, Sok, 2015). DAO is also the product of an alternative view of security, according to which the architecture of a self-reliable system is superior to the protection that central authorities – such as governments – traditionally offer to the organizations and persons they govern. In his 2001 proplet paper, Nick Szabo wrote, "*trusted third party* is a nice-sounding synonym for a wide-open security hole that a designer chooses to overlook. Proplet design places strong emphasis on eliminating such exposures."

2.2. DLT: essential concepts

We will not revisit how the Bitcoin protocol works but rather focus on the key concepts that support DLT in its public format, the Bitcoin network and its Blockchain.

A distributed and decentralized network rather than a central authority

The Bitcoin network is comprised of thousands of full-service nodes capable of certifying its transactions. They communicate through a peer-to-peer (P2P) protocol that enables any two computers in the network to exchange information, directly or indirectly. As for the Internet, this distributed network offers the advantage of resilience over a centralized database given that shutting down a few of its nodes will not affect its overall functioning. This is not true of a standard client-server architecture that will in fact shut down if the central database on the server shuts down. It is worth noting that a private key is generated by a cryptographically-secure random string of 256 bits.[30] This is an important point because different bitcoin addresses can be generated in a decentralized way with a quasi-zero risk of having two different bitcoin users ending up with the same bitcoin address.[31]

A pseudonym system

The anonymity of the Bitcoin network is often criticized for potentially paving the way for money laundering and facilitating tax evasion. It is important to understand that every new bitcoin address generated is derived from a public key, itself derived from a private key via a cryptographic transformation. The ability to use bitcoins attached to a given bitcoin address requires the knowledge of the corresponding private key. While mapping a given bitcoin address back to its physical holder may not be easy, it is not impossible either.[32] To the best of our knowledge, almost all bitcoin-traditional currency exchanges require at the minimum a government-issued photo ID and proof of address before validating an exchange transaction. That being said, it is indeed easy to move bitcoins around on the network given that creating a bitcoin address in an e-wallet is very simple to do and hardly traceable.[33]

Irreversible transactions

This aspect of DLT has been both praised and criticized. One of the main characteristics of a bitcoin transaction is that once it has been validated, it cannot be cancelled. Irreversibility has been hailed as an advantage by merchants who accept bitcoin, because it eliminates the risk of malicious customers cancelling transactions. The system should potentially eliminate counterparty credit risk since a transaction will only go through if the payer has the funds available for transfer to the payee. A rule-of-thumb for a strong validation is to wait for six blocks to be appended to the block in which the transaction is included (about one hour) before the transaction is deemed irreversibly settled.

Finite and scheduled supply

Bitcoin is a cryptocurrency with a finite supply and pre-determined supply schedule. “Monetary creation” is hardwired into the Bitcoin protocol and not subject to the whims of a central bank with its subjective analysis and macro-economic projections. Bitcoin supply is limited to a maximum of 21 million bitcoins. The Blockchain will create 25 bitcoins per block until 2016, then 12.5 bitcoins for the next 4-year period, and half as many per block every 4 years until the maximum limit of 21 million bitcoins issued and in circulation has been reached. This finite bitcoin supply, with its decreasing issuance rate of over time, has led many to compare the creation of bitcoins to the process of extracting gold from a mine where supply is finite: the process is easy early on but becomes increasingly more difficult as the cost of extraction increases and the supply of gold ore in the mine diminishes.

Cryptography

DLT uses cryptography extensively for various functionalities. In the Bitcoin protocol, cryptography is used: (i) to calculate a public key from a private key through elliptic curve cryptography, using the secp256k1 standard defined by the National Institute of Standards and Technology (NIST); (ii) to calculate a public bitcoin address from a public key by double hashing the latter, first using the SHA256 one-way function, followed by the RIPEMD160; (iii) to provide a digital signature that will be used in a transaction's unlocking script to allow the transfer of bitcoins locked to a particular bitcoin address; (iv) to calculate a valid block's hash by varying a nonce, a process called "mining"; (v) in other situations where hashes need to be calculated such as when calculating the Merkle's root of a set of transactions.

Authentication mechanisms

The Bitcoin protocol provided a solution to a previously unsolved problem in distributed computing called the Byzantine generals problem (Lamport et al., 1982). In brief, this problem consists of studying if, and under what conditions, a network of generals can agree on a course of action (reach a "consensus") given that they are potential traitors among them, and they can only exchange information over an unreliable and possibly compromised network.

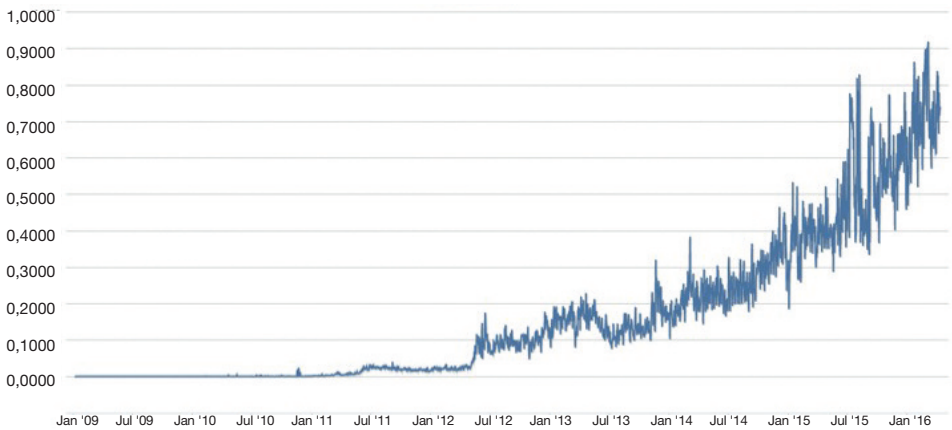
Proof-of-work (or mining), proof-of-stake, and zero-knowledge-proof are different paradigms for authenticating the validity of transactions that all aim to make it impossible to alter the distributed ledger. Proof-of-work (PoW), the first and most common approach, and the one used by Bitcoin, consists of verifying that anyone who adds a block to the Blockchain has first solved a cryptographic problem. The validating node (the "miner") has to prove that work has been done. Mining essentially boils down to solving a cryptographic problem whose difficulty is dynamically adjusted by the Bitcoin protocol. A miner will go through all possible nonces to find a suitable hash code for the block it is trying to "mine". A suitable hash code is a hash code that starts with a certain number of zeroes (which is equivalent to requiring that the hash be smaller than a certain value). The greater the number of zeroes, the greater the mining difficulty, and *vice versa*. Proof-of-stake (PoS) on the other hand, is a method that requires users who wish to validate transactions to prove ownership of a certain amount (their "stake") of currency. Lastly, zero-knowledge proof is a method by which one party (the "prover") can prove to another party (the "verifier") that a given statement is true, but this is done without conveying any information other than the fact that the statement is indeed true. We will not elaborate on the differences between theses approaches or their pros and cons, but it is important to understand that Bitcoin uses proof-of-work and that Ethereum, which is also currently using PoW is considering transitioning to PoS in the future.

3. The various technical debates

3.1. Bitcoin block size and other controversies: is the debate relevant?

One of the most heated debates within the Bitcoin community has been the issue of block size, since it is related to Bitcoin's scalability. The current Bitcoin Core protocol defines the block size as 1Mo. Until late 2012, the actual size of blocks rarely exceeded 200ko, but beginning in 2013 block size began increasing. At the time of writing, the 7-day trailing average stands at around 0.75Mo, with an increasing number of blocks larger than 0.9Mo. This trend has clearly not gone unnoticed and fears of network saturation prompted some developers to worry about block size early on.

Figure 1: Average block size



There are essentially two ways to change and upgrade the Bitcoin protocol: *hard forks* and *soft forks*. Typically, a hard fork is a change to the bitcoin protocol that will require all users to upgrade by making fundamental alterations to the block format (e.g. block hash) or to the set of possible transactions. With a hard fork, there is no possible backward compatibility as old nodes will not be able to cope with new transactions that they will automatically deem invalid. A soft fork, on the other hand, will allow backward compatibility as old nodes will be able to recognize new transactions as valid with only new nodes rejecting old-type transactions. A soft fork will only require a majority of the miners upgrading to enforce the new rules and will allow each active node to choose whether or not to implement the proposed changes. Hence a soft fork will not disrupt the ongoing functioning of the network as new and old versions can coexist for a certain time until a clear consensus for the newer version is reached and old nodes end up rallying the new format.[34] A hard fork does not allow for this phasing in of the newer and phasing out of the older as essentially all nodes need to upgrade at the same time to be able to recognize and deal with the block/transaction formats.

In June 2015, Gavin Andresen, one of the core Bitcoin developers, posted a new Bitcoin Improvement Proposal (BIP 101) in support of replacing the fixed one-megabyte maximum block size with a maximum size that would grow over time at a predictable rate (according to this proposal, the maximum block size was to become 8 Mo in January 2016, and would have doubled every other year until 2036 to finally reach about 8,1 Go). He and other active developers suggested miners could upgrade to Bitcoin XT until 75% of the network opted in, at which point the remaining miners would have had two weeks to upgrade or be left out (a hard fork). This proposed change was effectively voted down by a majority of the Bitcoin community, prompting Bitcoin opinion leader Mike Hearn, until then a prominent developer in the Bitcoin community, to make a climactic public statement saying that Bitcoin had "failed".

What is interesting in this debate is to understand the arguments for and against an upgrade, and what this controversy says about the governance of this decentralized community and its various paradigms and philosophies.

On the one hand, proponents of an increase caution that there are real risks of network saturation and argue that it was necessary to increase the network's transactional capacity in order to compete with other well-established payment systems such as credit card networks.[35]

On the other hand, supporters of the status quo invoke the need to preserve current network stability and avoid engaging in a change that is likely to further increase mining concentration (as changing the block size to 8Mo would risk driving many active nodes out of mining). Some also argue that the Bitcoin network should not be used for trivial micro-payments, and that the core of the Blockchain data should relate to authentication. Last but not least, many partisans of the status quo also believe that it is important to preserve the Bitcoin community's creativity for finding solutions around the existing constraint, rather than removing this constraint.[36]

This is a complex technical issue, with a seeming dilemma between scalability and mining concentration. But we believe that, while many blockchains already coexist and are likely to continue to flourish, preserving the initial Bitcoin/Blockchain is essential at this juncture for keeping up the momentum and credibility of the current wave of initiatives. That implies, at the very least, making sure that the network's current level of decentralization is at least maintained.

3.2. A brief typology of possible coins and chains

It is only natural that an open source such as the Bitcoin protocol developed from Satoshi Nakamoto's white paper, would inspire others to follow suit. In fact, a flurry of alternative coins (aka *alt coins*) and alternative chains have followed in Bitcoin's wake.[37] But despite the proliferation of initiatives, at the time of writing, market capitalization for cryptocurrency players remains exceptionally concentrated. As of April 4th 2016, total market capitalization represented approximately €7.8 billion. Of the 700+ currencies listed on Coinmarketcap, only four players have a market capitalization over €100m: Bitcoin, Ethereum, Ripple and Litecoin. Together they total €6.8 billion, representing 95% of total market capitalization. Of the four, Bitcoin takes the lion's share (79% as of April 4th 2016) followed by Ethereum (11%), Ripple (3%) and Litecoin (2%).[38]

We have adopted Antonopoulos's taxonomy (2015) for our classification but we will also include significant digital currency and payment initiatives such as Ripple, because they are gathering momentum in the financial services industry and cannot be ignored.

Meta-coin platforms

Numerous protocol layers have been implemented on top of the Bitcoin's Blockchain, described as "software layers implemented on top of bitcoin, either implementing a currency-inside-a-currency, or a platform/protocol overlay inside the bitcoin system." *Colored coins*, a meta-protocol that "overlays information on small amounts of bitcoin" and is repurposed to designate another asset, are among the most prevalent.

Alt(ternative) coins and alt(ernative) chains

These are essentially alternative coins and chains to Bitcoin, that use their own distributed ledgers, separate from the Blockchain. The vast majority of these alternative coins came into existence as "forks" of the Bitcoin source code, although some are coded from scratch, in particular alternative chains conceived for specific applications. The main distinction to keep in mind here is that an alternative coin will primarily be used as a currency, whereas an alternative chain will focus on a non-currency purpose.

Among alt chains, we will cite Namecoin and Ethereum. Namecoin is considered the first *fork* from bitcoin and essentially follows Bitcoin's parameters. Namecoin is a "decentralized key-value registration and transfer platform using a blockchain" and is currently used as an alternative domain name service (DNS) for the root-level domain ".bit" (Antonopoulos, 2015). Ethereum on the other hand is a "decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference."[39] Ethereum literally aims to become a global virtual machine and uses *ether* as its digital currency.

Permissioned vs. public chains

It is important to distinguish between public distributed ledgers, such as the Bitcoin Blockchain, and other permissioned distributed ledgers, also called private chains. We will address public blockchains, consortium blockchains and fully private blockchains following the typology provided by Vitalik Buterin (2015),[40] one of Ethereum's co-founders. Public blockchains are open to all for reading and writing valid transactions, and participating in the consensus process. Consortium blockchains are blockchains where the consensus process is controlled by a pre-selected set of nodes; "the right to read the blockchain may be public, or restricted to the participants, and there are also hybrid routes such as the root hashes of the blocks being public together with an API that allows members of the public to make a limited number of queries and get back cryptographic proofs of some parts of the blockchain state." A fully private blockchain is a "blockchain where write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent. Likely applications include database management or auditing internal to a single company, and so public readability may in many cases not be necessary at all, though in other cases public auditability [may be] desired."

The distinction between consortium and private blockchains is beyond the scope of this study but the reader should remember that a consortium blockchain appears to be a good hybrid between the low-trust/decentralized model of a public blockchain, and the high-trust/centralized paradigm of a private blockchain. It should also be noted that the benefits of having a blockchain structure in a completely private setting are not obvious; they would essentially be limited to the cryptographic authentication that a blockchain structure permits.[41]

On the debate between private and permissioned blockchains, Buterin sees five advantages of private blockchains over public blockchains: (i) they allow transaction reversibility, make it possible to change rules over time, and override some undesirable transactions (such as criminal ones); (ii) they remove the risk of a 51% attack since miners/validators are identified; (iii) they decrease transactions costs, since transactions only need to be verified by a few trusted nodes; (iv) since nodes can be trusted and should be very well-connected, private chain participants should be able to quickly correct errors via manual intervention, allowing the use of consensus algorithms that offer finality after much shorter block times; (v) if read permissions are restricted, private blockchains can provide a greater level of privacy.

This being said, the advantages of a public blockchain over a private one fall into two categories: (i) public blockchains are censorship-resistant and protect users from developers and from any form of centralized control; (ii) public blockchains are open, and therefore are likely to be used by very many entities and benefit from network effects.

It is also possible to create hybrid combinations of public and private blockchains for example, by using privately administered smart contracts on public blockchains, or cross-chain exchange layers between public and private blockchains. And Buterin[38] to conclude that the optimal solution for a particular industry depends heavily on the type of industry, and most notably, on the degree of private control and privacy that it requires.

Sidechains

Bitcoin sidechains exist and function alongside the main blockchain rather than creating an independent one. They jointly leverage the network benefits of security and pegged assets to the main Bitcoin Blockchain. They should “allow bitcoins and other ledger assets to be transferred between multiple blockchains” and give “users access to the new and innovative cryptocurrency using the systems they already own. By reusing Bitcoin’s currency, these systems can more easily interoperate with each other and with Bitcoin, avoiding the liquidity shortages and market fluctuations associated with new currencies. Since sidechains are separate systems, technical and economic innovation is not hindered. Despite bidirectional transferability between bitcoin and pegged sidechains, they are isolated: in the case of a cryptographic break (or malicious design) in a sidechain, the damage is entirely confined to the sidechain itself” (Back et al., 2014).[42] Another example of a private chain is the off-the-shelf MultiChain platform.[43]

Ethereum

This blockchain-like ledger and system has a completely independent design and is implemented separately from Bitcoin. Ethereum presents itself as a "decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference."[44] Ethereum has "a built-in currency called ether which is required in order to pay for contract execution. Ethereum's blockchain records contracts, which are expressed in a low-level, byte code-like, Turing-complete language. Essentially, a contract is a program that runs on every node in the Ethereum system. Ethereum contracts can store data, send and receive ether payments, store ether and execute an infinite range (hence Turing-complete) of computable actions, acting as decentralized autonomous software agents" (Antonopoulos, 2015). One of the powerful features of Ethereum is that it is highly generic and able to perform as a particular case of a smart contract what some dedicated alt chains do.

Ripple

Although Ripple uses a consensus algorithm of its own, different from proof-of-work or proof-of-stake, we feel it is important to mention it here as it is a distributed financial technology that "allows for banks around the world to directly transact with each other without the need for a central counterparty or correspondent."[45] Ripple aims to enable banks "to compress operational costs and offer new services for cross-border payments."[Ibid] One of Ripple's key services is to facilitate instant direct bank-to-bank settlement.

This brief taxonomy shows the diversity of DLT initiatives, and we believe the DLT landscape is likely to continue to evolve significantly in the near future as the technology matures.

4. Are distributed ledgers trustworthy?

Security is an obvious and essential aspect of distributed ledgers, especially when it comes to financial applications. We will distinguish here between the case of distributed ledgers that are public, and distributed ledgers belonging to a private or permissioned network.

4.1. Are the Bitcoin network and the Blockchain safe?

When considering the safety of the Bitcoin network and the Blockchain, two important issues come to mind: (i) whether Bitcoin/Blockchain can be used for criminal activities – a key aspect for law enforcement agencies and regulators – and (ii) whether they are secure for legitimate users.

When addressing the first question, it is fair to say that the Bitcoin network has repeatedly drawn negative attention because of highly publicized cases of fraud, announced by some as portending the end of Bitcoin. But Bitcoin has managed to weather the attacks and come out of these predicaments unscathed, and even strengthened, since it was generally recognized that the Bitcoin protocol was not at fault.[46]

The history of the first digital currencies, which were not DLT-based, certainly did not help the cause as it was "shaded with cases of fraud, money laundering, and ties with criminal groups" (Frunza, 2015). Examples of terminated ventures such as E-Gold in 2008 or Liberty Reserve in 2013 speak for themselves. Later, a few websites using Bitcoin and the Blockchain, such as Silk Road or Sheep Momentum, made the headlines for the numerous criminal activities they were facilitating, such as drug dealing or arms smuggling. Silk Road was shut down by the FBI in October 2013 while Sheep Momentum, that gained traction after Silk Road disappeared, was closed shortly thereafter in December 2013. These episodes largely contributed to spreading a negative perception of Bitcoin (dubbed by some "Bitcon") as a perfect tool for laundering money and financing criminal activities.

But the climax in negative press coverage came with the dramatic collapse of Mt Gox in early 2014. Mt Gox was an exchange which at some point in time handled almost 80% of global bitcoin trading.[47] The exchange shut down after it was discovered that an estimated 744,000 bitcoins, representing about US$350 million or 6% of the total volume of bitcoins in circulation, had disappeared. Mt Gox belonged to a long series of exchanges forced to close (Moore and Cristin, 2013), except that it was by far the largest and most visible. There were also various investment scams involving bitcoins, but there again they seem to have had more to do with con artists than intrinsic technological flaws. For instance, in 2014, a U.S. federal investigation indicted the organizer of a bitcoin-based Ponzi scheme that had managed to raise about 765,000 bitcoins over a year via securities fraud.[48]

In the case of Bitcoin, money laundering, a major risk for any decentralized crypto-currency, can be achieved in one of two ways: (i) directly, by setting up a large mining operation financed with illicit money that will earn both mining rewards and transactions fees; (ii) indirectly, by receiving bitcoins that have been purchased by an undetected third-party accomplice. In the latter case, it is very easy to create unregistered bitcoin addresses for this purpose from any laptop or smart phone bit-wallet. Today, almost all exchanges in regulated countries will require clients purchasing crypto-currencies against fiat money to provide positive identification. However, most of the time, KYC procedures remain pretty basic and there are still many bitcoin points of sale where one can simply buy bitcoins for fiat cash, and without any identity check.

Regarding the second question and the level of security provided to legitimate users, it very much depends on making sure that both private and public keys are only used when needed, and that the former are kept absolutely confidential.[49] User behavior is a key component of security and confidentiality. On this front, various startups have emerged providing safe storage services for private keys. Since it is highly likely that all connected devices will be hacked one day or another, an important rule of thumb

is to make sure that private keys are stored away from the electronic wallets where they were created, and not loose them! The principle of segregating highly sensitive data away from any Internet-connected device is called *cold storage*.

Then there are various security paradigms that any prudent user should follow, such as allocating small amounts over multiple addresses, rather than having one large amount attached to a single bitcoin address. Also, learning from the Mt Gox demise, if an exchange is to be used, it is highly recommended to do some serious due diligence prior to choosing an exchange. While banks have put procedures in place to prevent their employees from accessing their clients' sensitive information, it remains to be seen if all bitcoin exchanges have done the same.

Another important security aspect of public chains based on decentralized trust[50] is that the network should not fall into the hands of a malicious party, or any collusion thereof. We already referred to this so-called "51% attack" scenario. Interestingly enough, there have been instances in the past where it is believed that a mining pool almost very nearly seized the majority of the network computing power. However, because the risk of a 51% attack is considered a serious potential threat to the network, and is closely monitored (including by regulators[51]), it is also believed that, in the very rare cases where it could have happened, the responsible mining pool self-regulated to avoid attaining the 51% bar. However, since it is difficult to track the distribution of network computing power precisely, it is also not possible to ensure beyond the shadow of a doubt that a 51% attack can be avoided or thwarted. Certain countries, such as China,[52] have firewalls capable of fudging this analysis. It is also important to understand that, even if it were to occur, a 51% attack would not allow attackers to rewrite history: they could control the validation of new blocks, and double spend existing bitcoins, but they would not have the necessary computing power to rewrite past blocks within the average ten-minute interval it takes to add a new block to the chain.

4.2. What about permissioned/private chains?

Different rights (e.g. read or write) can be attributed to different nodes of a permissioned distributed ledger. In the case of a private or consortium chain, the number of nodes can be greatly reduced (from thousands to hundreds) and each node can be given specific permissions profiled according to the node's role and function. In some cases, proof-of-work or proof-of-stake could be eliminated altogether.

The integrity of transactional data against intruding attacks could be maintained by periodic hashing (such as producing a Merkle tree root of all transactions that happened on a given day) and regular cold storage procedures. The peer-to-peer approach and distributed ledger architecture should make it much more difficult for intruders to modify transactional data.

Automated compliance and reporting procedures to external entities such as regulators (possibly using current trade repositories) should also increase the system's robustness.

4.3. Resilience of current cryptographic algorithms

Cryptography is another, if not THE, essential aspect of the system's overall security. A recurrent question from crypto-currency skeptics relates to the amount of required cryptography (including of course for mining in the case of Bitcoin) and the risks posed by any computing breakthrough that would make it possible to crack some of the current one-way functions (for instance RIPEMD160 after SHA256 for generating bitcoin addresses). This is a legitimate question given that some algorithms deemed safe yesterday are considered obsolete today.[53]

The Bitcoin protocol however, uses compounded cryptographic functions (for instance, when generating a bitcoin address from a public key, first SHA256 is applied and then RIPEMD160) that so greatly increase the difficulty of tracing back the public key from the bitcoin address, and the private key from the public key, that many experts consider that it is currently impossible or unfeasible to trace back a private key from a bitcoin address. Nonetheless, we believe close attention should be paid to the advent of so-called quantum computers and the multiplying effect they could have on processing power, making it far easier to break compound encryption functions.[54]

4.4. Automation risks

Today, financial markets still function using some manual procedures, especially in middle-office functions for data capture and in back-office data processing. The introduction of DLT is likely to significantly increase the level of automated data processing. While under normal circumstances some may view increased automation as a way of reducing operational risk, some market operators also underline the risks inherent in increasing dependency on automated processes. DLT integration will probably require a greater degree of sophistication from middle and back-offices and the establishment of emergency control procedures.

5. Key areas of application for DLT

5.1. Certification, time-stamping and attestation services: towards a new notarization model?

As mentioned in section 1.1, numerous sectors of the economy have already implemented blockchain applications for certification through irreversible, encrypted time-stamping. Land registries, public notary services, electronic health records, drug authentication (fighting counterfeits), anonymous medical research data storage and transfer, issuing, storing and authenticating academic certificates, registering and providing IDs to refugees, inventory and supply-chain management are just a few examples of current blockchain applications.

It is only logical to look to the Blockchain to facilitate certification services, i.e. "all manner of services related to document filing, storage and registry, notary services (validation) and IP protection" (Swan, 2015). Such services take advantage of the Blockchain's ability to use "cryptographic hashes as a permanent and public way to record and store information, and also to find it later with a block explorer." In this case, the Blockchain acts as a central universal repository. Proof of Existence is one of the first web services to offer blockchain certification.[55] "People can use the web-based service to hash things such as art or software to prove authorship of the works [with] a trusted timestamping mechanism" that did not exist before the Blockchain was put in place. This service "demonstrates document ownership without revealing the information it contains, and it provides proof that a document was authored at a particular time" (Swan, 2015). Various other notarization services, such as Virtual Notary[56] or Bitproof,[57] are now up-and-running.

Factom,[58] a service specialized in securing data and record keeping, uses another approach worth mentioning. This leading DLT start-up's product, Factom Proof, combines three types of proof: proof-of-existence (the "document existed in this form at a certain time"), proof-of-process (the "document is linked to this new updated document"), and proof-of-audit ("verifying the changes in the updated document"). Similarly, Stratumn,[59] based out of Paris, offers a platform for processing workflows and an open standard script, Chainscript, for describing each step of a workflow and adding cryptographic verification to business processes.

Because the data it stores is immutable, encrypted and secure, DLT could provide a new paradigm for efficient and secure document authentication and certification, admissible as evidence in court (Blanchette, 2012). Moreover, it has a certain advantage over traditional systems: multiple digital signatures facilitate document approval or contest prior to "admission" to the Blockchain. Hence, using public blockchains could eventually become a system of choice for authenticating documents drafted by individuals without the assistance of legal council. It is also worth noting that it is possible to condition the execution of transactions or smart contracts to be carried out or executed on a blockchain via the use of an "oracle", that is a server external to the blockchain, and able to interface with it, whose role is precisely to check for the realization of exogenous contingencies.

Does this mean that notaries are in danger of loosing their monopoly on authentication and certification? Probably not in the short term, but it does mean that the profession will have to evolve along with technology and real-world practices. Porter's work (1979) on how new technologies are adopted shows that depending on how the technology is embraced by the profession, Blockchain/DLT could be considered either as a threat to the notary profession or as an opportunity for the profession to increase its added-value as an advisory service above and beyond authentication.

5.2 DLT and existing payment systems

In his 2008 white paper, Satoshi Nakamoto described the Bitcoin protocol as a "purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution." As a

matter of fact, Bitcoin has proven its efficiency as a digital transactional payment system allowing bitcoin transactions to be directly sent from one person to another without any third party intermediation, contrary to standard banking-based transactions. In practice, users can choose between different types of digital interfaces to process their payments. These interfaces are commonly called *wallets* and can be installed on mobile devices such as smartphones and tablets (e.g. Mycelium), laptop and desktop computers (the original Bitcoin Core software), or can be web-based (e.g. Coinbase). Payment systems can also include hardware components (such as Ledger's smartcards[60]) that provide users with supplemental layers of security allowing them to keep their private keys separate from the device used to process payments. Figure 2 explains how such a standard bitcoin transaction is done in practice.

Bitcoins are fungible and can be exchanged against fiat currencies on Bitcoin exchanges (for example, Paymium,[61] a French online exchange, or La Maison du Bitcoin,[62] a Paris-based exchange counter with a brick-and-mortar storefront). One can also withdraw bitcoins directly from ATMs.[63] The Chicago-based start-up Glidera even offers a bitcoin exchange service embedded in existing bitcoin wallets directly linked to the user's traditional bank account through an integrated API.

Figure 2: How a bitcoin payment works

In France, monetary and financial regulations were modified in 2008 making it possible for Bitcoin payment companies such as Paymium to operate under French jurisdiction. Specifically, articles L522-1 and L522-2 of the French *Code monétaire et financier*[64] (Monetary and Financial Code) of July 15th 2009 established the legal status of payment institution (*établissement de paiements*) and authorized such institutions to provide both payment and payment-related services. Article L522-1 defines payment

institutions as "legal entities other than credit institutions and others cited in article L.521-1 that provide professional payment services as defined in article L. 314-1, Title II." The *Autorité de Contrôle Prudentiel et de Résolution* (ACPR) is France's main regulatory authority for payment activities, and a French payment institution can offer its services at the European level if authorized to do so by the ACPR.[65]

As mentioned in section 1.1, major players such as Visa, Mastercard, Paypal,[66] to cite only a few, are said to be exploring the feasibility of offering DLT solutions to their customers. KB Kookmin Bank officially announced its intention to explore DLT as a potential solution for decreasing the cost structure of its remittance business, currently operating via SWIFT. At the present time, three main areas of DLT-supported payment services are growing:

(i) Wallets offering decentralized P2P payment services (such as Mycelium, BitPay and many more)

(ii) Bitcoin and other altcoin exchanges, and street counters (e.g. Coinbase, Paymium, Maison du Bitcoin, Medici from Overstock)

(iii) International money transfers and remittance operations (e.g. BitPesa, Abra, Rebit, ArtaBit, Coincove, etc.)

Today, major payment service providers who wish to connect their existing payment solutions to DLT must choose between developing their own APIs in-house or using the services of DLT-linked API developers such as Glidera. As mentioned earlier, Glidera links fiat currency bank accounts to bitcoin wallets directly. This type of API development could encourage leading payment service providers to jump the DLT hurdle faster.

This being said, as discussed in section 3.1., before DLT becomes the technology of choice for the world's premier payment service providers, it will have to address the issue of network scalability. In their paper "On Scaling Decentralized Blockchains" (IC3, 2016), the IC3 group (Initiative for CryptoCurrencies and Contracts[67]), notes that at the present time, Bitcoin's maximum throughput, i.e. the maximum rate at which the network can validate transactions, is estimated at 3.3-7 transactions per second. "In comparison, a mainstream payment processor such as Visa confirms a transaction within seconds, and processes 2,000 transactions/sec on average, with a peak rate of 56,000 transactions/sec." While the authors believe that technological advancements could close this gap overtime, such discrepancies clearly lead us to ask the question of network usage optimization[68].

In fact, various Bitcoin experts wonder whether a powerful transaction verification system such as the Bitcoin network should really be used to authenticate trivial transactions, such as paying for coffee or buying a newspaper.[69] It does indeed seem inappropriate to use the network's enormous computing power and proof-of-work mining process indiscriminately. Many believe that a savvier route would be to combine permissioned blockchains for small transactions with the use of the Bitcoin blockchain for aggregated daily balances. In other words, the Blockchain could and should be used for storing carefully sampled aggregate information from sidechain activities, but not necessarily for recording trivial transactions.

The aforementioned configuration could indeed represent an optimal use of DLT, offering a good tradeoff between maximizing authentication and security by ultimately encrypting pools of transactions on the Blockchain and the need to minimize power and computing resources for doing so. This would entail using permissioned blockchains for transactions inferior to a certain threshold. The DLT-based start-up Blockstream and the Bitcoin Lightning network are currently developing interesting services along this paradigm.

Blockstream, which announced a US$55 million fundraising in February 2016, is developing interoperable sidechains[70] that would be able to combine the use of private and public blockchains. The Bitcoin Lightning network, as explained by Poon and Dryja[71] in their white paper, proposes another off-blockchain solution for increasing the Bitcoin network's scalability while not increasing the risk of node centralization. They suggest that by "by deferring telling the entire world about every transaction [and] doing net settlement of their relationship at a later date", the use of micropayment channels "enables Bitcoin users to conduct many transactions without bloating up the Blockchain or creating trust in a centralized counterparty." The use of "time locks as a component to global consensus" could, in their view, achieve the creation of an "effectively trustless structure", by "creat[ing] a relationship between two parties to perpetually update balances" that are routinely conducted off-blockchain.

Hence, as previously developed in section 3.1**.,** it may be possible to dodge the trade-off between scalability and node decentralization therefore making DLT a potentially disruptive force in the payment system universe.

5.3. DLT's multi-faceted potential for capital markets and corporate finance

We believe that there are numerous potential applications for DLT in the financial industry as evidenced by leading financial players' considerable investments in the area. Yet, because there is little margin for error in financial services and current infrastructures do the job churning away millions of transactions a day, financial infrastructure providers have to be very careful when integrating DLT.

The Australian stock exchange operator ASX recently announced that it had paid AU$14.9 million for a 5% equity stake in New York-based Digital Asset Holdings and that they plan to test DLT for post-trade services.[72] ASX currently uses a clearing and settlement platform called CHESS. ASX announced that "the [DLT-based] development will take place alongside CHESS, which will continue to operate as normal. This will allow all stakeholders to assess the benefits and implications before a final decision is made on Australia's post-trade technology in 2017."

Out of all potential DLT applications, the one that is most promising is smart contracts. A smart contract is essentially a program into which contractual clauses are encoded and that is self-executing or self-enforcing. Smart contracts can for instance be used to automate the distribution of cash dividends, the issuance of new shares, perform share splits and automatically execute the unwinding or the closing of an existing position (or, in the case of an option, its rule-based exercise) if some predetermined

conditions are met. The code embedded into smart contracts will usually emulate the logic of contractual clauses. The ambition of smart contracts is to provide a level of security superior to traditional contract law while reducing the transaction costs and legal fees associated with contracting. Wright and De Filippi (2015) even argue that DLT widespread deployment should lead to a new subset of law, termed *lex cryptographia*, defined as " rules administered through self-executing smart contracts and decentralized (autonomous) organizations".

Ethereum's blockchain is said to be one of the most promising DLT platforms able to host smart contracts, but there are others, such as Nxt,[73] and it is clear that further innovations will follow at a rapid pace over the coming year. While the technology is still in its infancy and under test, we summarize below what we view as the main mechanisms and potential applications of smart contracts for the financial market industry.

Let's take a look at several practical examples: for a smart contract to generate the distribution of cash dividends to shareholders, it would simply need to be programmed to automatically send shareholders a percentage of announced earnings per share at the end of each fiscal year in cash, or more precisely in its crypto-currency equivalent. Similarly, many standard financial derivatives such as plain vanilla options could also be straightforwardly programmed into smart contracts, with potentially sophisticated features such as pre-programmed dynamic hedging[74] or automated position unwinding. Margin calls, as functions of the underlying asset price, could also be automatically generated and managed through the use of smart contracts. The same holds for repurchase agreements ("repos"). More generally, any financial contract that could be translated into a combination of algorithmic rules could be implemented through the execution of a smart contract.

Furthermore, securities digitally translated into smart contracts hosted by a blockchain would be automatically settled in the buyers' and sellers' accounts. Indeed, digital ledger assets are by definition embedded in a blockchain, and any change of total or partial ownership would be automatically recorded in this digital ledger. Shortening the settlement process could also eventually lead to replacing trade identification services, currently offered by the SWIFT system, with a blockchain-based service, leveraging its unique encryption and authentication capabilities.

Prudential rules, such as tier-one ratios for banks, or debt covenants for credit holders, could also be tracked through smart contracts embedded into a blockchain, encrypting the balance sheets of banks and corporations in general (and by derivation, their solvency). In a sense, broad adoption of a common blockchain, or a set of interoperable blockchains, running smart contracts could be the architectural basis for incontestable proofs of solvency. By creating trust among market participants, such proofs of solvency could in turn increase trade and market liquidity and facilitate interbank lending. It is worth noting that this last activity nearly came to a halt during the worst days of the recent financial crisis as banks became increasingly weary of one another. A shared and reliable distributed ledger able to provide proofs of solvency would have been particularly welcome in this situation.

In addition, the traceability made possible by a blockchain could greatly facilitate corporate governance in general (Yermack, 2015), and corporate finance in particular. The transparency of ownership that DLT offers could be very useful to corporate managers who need to reach out to investors in a variety of situations, such as a merger or an acquisition, or for any corporate election or decision where shareholder voting is required. DLT-based voting could achieve much greater accuracy than is currently available with proxy services, allowing all shareholders to be contacted quickly and efficiently. DLT could also be leveraged for corporate accounting and financial reporting. Some authors go as far as to suggest that a firm could voluntarily include all its transactions on a blockchain, leading to real-time financial accounting (Lazanis, 2015). Though many firms would probably be reluctant to follow this route initially, a systematic blockchain posting policy, if implemented, would bring three benefits: (i) corporate shareholders or creditors could easily reconstruct the firm's balance sheet, income and cash flow statements (providing a clear picture of the firm's solvency) which would in turn facilitate (ii) auditing and (iii) reporting functions.

The aforementioned list of potential DLT applications is clearly not exhaustive. We should also point out, for example, that DLT represents significant opportunities for trade finance.[75] And all in all, it is clear to us that whatever the field of financial applications considered, DLT will be used to challenge the current status quo. One particular area of interest that we will now explore is market infrastructure, and in particular post-trade market infrastructure.

6. How can DLT be integrated into financial market infrastructures?

Financial market infrastructures are commonly broken down into three main value chain components: (i) pre-trade, (ii) trade and (iii) post-trade processes. This segmentation results primarily from the fact that infrastructures were built on legacy systems and have evolved slowly over time.

To what extent could DLT, as a means to both store and transfer ownership of digital ledger assets, change the value chain of financial markets? Trading results in transferring the ownership of an asset at a negotiated price. Transfers then need to be registered properly and safely, while the asset must be stored safely and efficiently for the new owner.

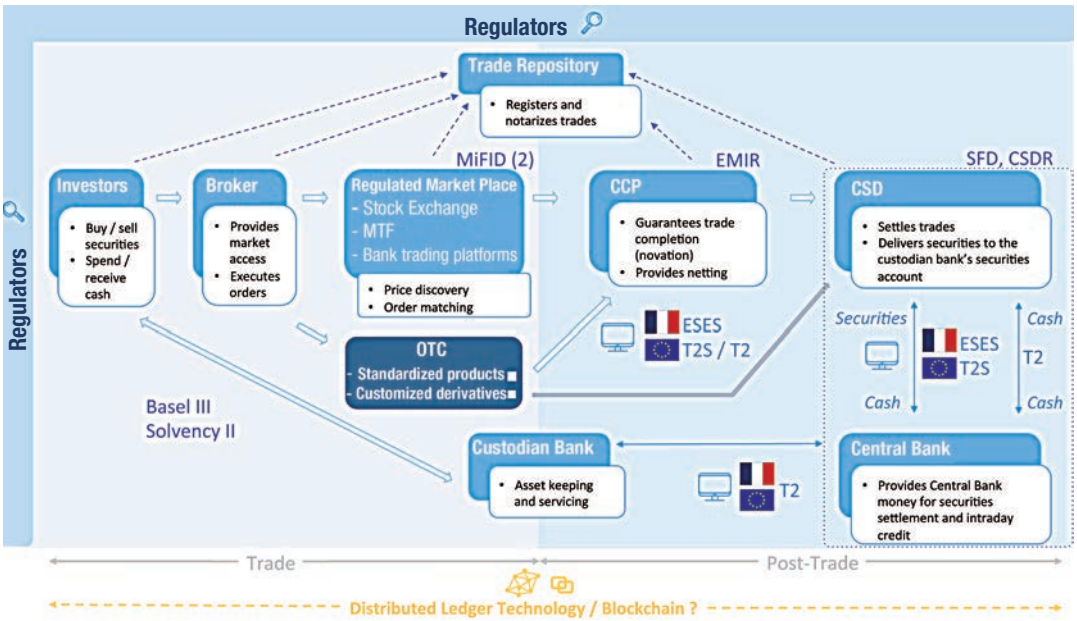
We've seen in section 5.3 that smart contracts can basically automate any contractual process that can be translated into algorithmic functions. In this section, we will go further and focus on key processes flowing through the financial market infrastructure and assess the extent to which DLT could be deemed a reasonable substitute for existing legacy systems.

6.1. Current European financial market infrastructures: regulatory changes and the introduction of pan-European RTGS systems

The recent global financial market crisis has significantly impacted the regulatory space of both banks and financial markets. Across the globe, systemic risk management has become a primary focus. European banking has seen prudential rules such as Basel III increase their solvability requirements. The European Markets Infrastructure Regulation (EMIR) introduced reporting requirements to trade repositories for OTC derivatives and expanded the obligation for regulated financial institutions to use a central counterparty (CCP) clearing house for standardized over-the-counter (OTC) derivative transactions, "casting CCPs as pillars of the new global financial architecture" (Cont, 2015). Similarly, in the United States, the Dodd-Frank Act enacted in July 2010 increased the importance of prudential and reporting requirements for financial institutions.

More stringent prudential rules and reporting requirements, combined with the liquidity contraction that took place in the wake of Lehman's demise, made the European private sector's funding needs even more acute. And this in turn shifted the spotlight onto the importance of fostering an efficient development of European financial markets, all the more so given that they seemed to lag behind their US counterparts in terms of financing the economy. Indeed, as underlined by the European Commission's "Action Plan on Building a Capital Markets Union" (September 2015),[76] "compared with the US, European SME receive five times less funding from capital markets." Another solution that was recommended by the Action Plan was securitization, perceived as a reliable way to increase liquidity and support the renewal of European credit markets.

Figure 3: What level of integration for DLT in financial market infrastructures?



In this context, safe and efficient post-trade infrastructures are key to achieving secure and sustainable economic growth across Europe. Both regulation and IT systems have evolved and are constantly being upgraded in parallel. As stated in the European Commission's "Action Plan on Building a Capital Markets Union" (September 2015), "EU legislation, such as European Markets Infrastructure Regulation (EMIR), Central Securities Depositories Regulation (CSDR) and MiFID II, has removed many of the barriers to the cross-border clearing and settlement of securities." Harmonization efforts have been made in line with the Giovannini Group's recommendations (2001, 2003), through pan-European initiatives such as the European Post Trade Group (EPTG) composed of the European Commission, the European Central Bank (ECB), the European Securities and Markets Authority (ESMA), and industry representatives.

Continuous link settlement (CLS) and real-time gross settlement (RTGS) systems have been set up to replace deferred net settlement (DNS) procedures at the European level for both intraday payment and credit (TARGET2, or T2, replaced RTGS TARGET in November 2007) and most recently for securities settlement (TARGET2-Securities, or T2S, is currently being rolled out in the Eurosystem). RTGS systems use and rely on the SWIFT messaging system.

The design of any new DLT-based system should take into account this trade-off between (i) aiming to provide settlement as early as possible to decrease liquidity risks on the one hand (this should be quasi-instantaneous with DLT) and (ii) minimizing the collateral requirements which can be costly.

RTGS is generally considered safer than DNS (Hervo, 2008) as each transaction is settled "as soon as it enters the system." Yet, "a side effect of settlement in RTGS mode is that the associated intraday liquidity needs required to settle an equivalent of underlying payment obligations are higher than in a DNS environment" while it also creates an increased need for "collateralization to support liquidity demand."

Liquidity-saving features have been introduced into RTGS systems in order to allow "bilateral or multilateral compensation with real-time settlement functionality (for instance, CHIPS in the United States, T2 in the EU)." Other types of commands based on real-time information have been added in order to lower users' liquidity-related opportunity costs, such as the ability to modify the order of a transaction in the backlog, the time at which it should settle or some credit limits controlling how much funds are going out.

As for dealing with the increased collateralization generated by RTGS, it should be noted that central securities depositories (CSD) have introduced automated self-collateralization features. For example, Euroclear's ESES settlement system provides real-time delivery versus payment (DVP) services with embedded automated self-collateralization procedures whereby securities "being purchased can be used as collateral for intra-day credit in order to fund the purchase" (Hervo 2008). Once roll-out is complete, T2S should provide similar features.

Moreover, in order to increase security and trust, RTGS systems have prompted the dismantlement of revocable operational systems (in France, ESES began replacing Relit+ in 2007) in favor of irrevocable settlement systems for the delivery-versus-payment of securities.[77]

Peak hours in payment and settlement flows, increased need for diversified collateral, multicurrency settlement and the increased use of commercial bank money instead of central bank money for multicurrency settlement are so many challenges financial market infrastructures need to take into consideration (Hervo, 2008). Last but not least, is the question of the European post-trade infrastructure's scale of operations. RTGS system T2S is still in test mode and therefore, no statistics related to its operations are as yet available. According to the Banque de France,[78] RTGS system T2, considered a Large Value Payment System (LVPS), treated on average 364,000 transactions per day, for a total amount of 1,935 billion euros in 2013. In this context, it is legitimate to wonder whether or not DLT would be able to address the complexity and the scale of post-trade infrastructure processes.

6.2. Could DLT be the new paradigm for post-trade processes?

Partnerships between DLT start-ups and large financial institutions have shaken up the perception of traditional banking. Could DLT start-ups trigger the transformation of the financial industry in the same way *unicorns*[79] changed the course of history for traditional industries such as transportation, hospitality, or space exploration, creating what appears to be billion-dollar business fairy tales? As discussed in section 1.1, seasoned financial executives such as former JP Morgan global head of commodities, Blythe Masters, or the founder of the Chi-X trading platform, Peter Randall, clearly believe that it will. Even former Bank of England Executive Director Sir David Walker has joined the DLT movement under the SETL.io banner.

SETL, a start-up focused on developing DLT-based settlement solutions for the financial industry, has announced that they expect to be able to process as many as 100,000 transactions per second (5,000 in test mode and 100,000 in enterprise context), numbers comparable to those of payment services provider Visa. SETL's stance is to "use computing to simplify processes." They envision DLT as very promising on this front. "When we launched Chi-X, that worked because instead of taking a bunch of manual processes and computerizing them, we did it the other way round – we started with the computer, put that at the center and built the processes around it […] Reconciliation is traditionally very expensive – you end up having to reconcile multiple times due to differing systems. But the blockchain is a golden record that allows us to do it only once. The potential is enormous."[80] Clearmatics, working alongside Swiss banking giant UBS is rumored to be making other significant advances.[81]

Given SETL's advances and the active research underway to address DLT's scalability issue, the authors believe that scalability issues should not constitute a major impediment to the technology's future development. The implementation of professional DLT applications such as Nasdaq's Link or ASX's DLT-based clearing and settlement solution will provide good proxies for tracking what can effectively be accomplished in terms of scale.

With respect to the general post-trade infrastructure, we do not believe that DLT will be able to act as a full substitute to CCP or CSD in the short term; however, a fully integrated vertical substitution may be possible in the longer term, provided the regulatory framework evolves. In fact, DLT may provide an opportunity, through the establishment of a new and adapted regulatory framework, to unify (and simplify) current regulation.

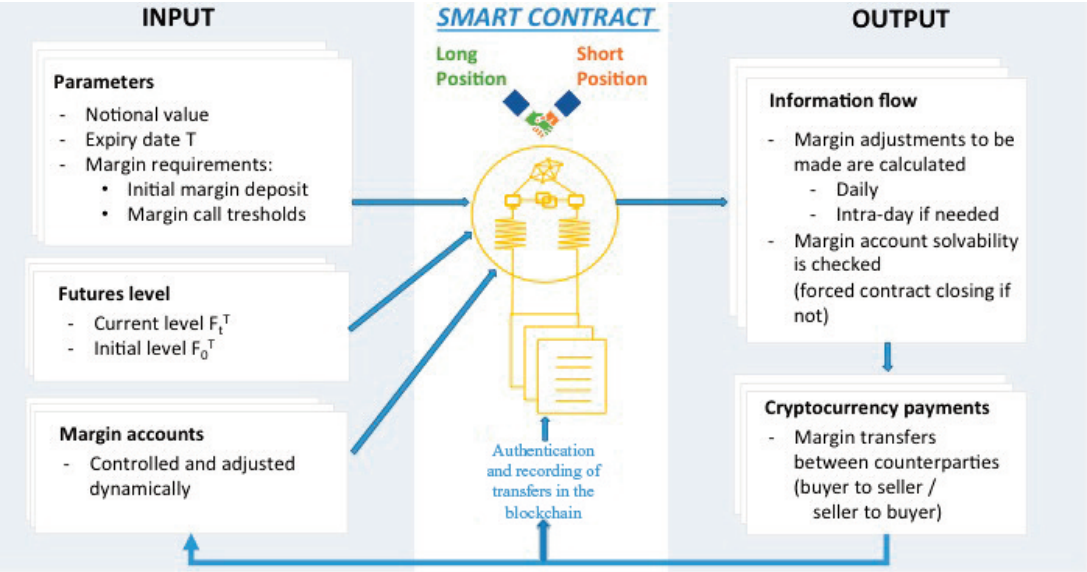
VII. Concrete examples

Assuming that operational scale issues are resolved and that most financial securities or derivatives can be programmed in the form of smart contracts, we shall now look at concrete examples by taking a prospective approach in the following section of this paper.

7.1. Futures as a smart contract

In this example, illustrated in Figure 4 below, we will first look at how programming a futures into a smart contract would work, considering that only the minimum features would be embedded in the smart contract technology.

Figure 4: How would a smart contract for a EUR/USD futures contract work?



In this simple example, we break down the necessary steps for programming a futures on the EUR/USD rate as a smart contract. What matters most is to make sure that margin calls will be thoroughly executed, by default on a daily basis, but also intra-day if the futures' current level F_t^T varies significantly during the day. If it turns out that one counterparty does not have the necessary crypto-currency funds, the *futures* contract is immediately closed.

It is important to note that a smart contract not only generates information flows, i.e. the resulting margin call levels and account balances, but concomitantly also generates financial flows denominated in cryptocurrencies. In this example, once

transferred from one party to the other, margins are settled automatically and directly. In fact, what truly adds value to the existing algorithmic functions is the fact that in a DLT-based system, smart contracts make it possible to send cryptocurrency flows automatically to the different parties involved. A simple API providing the current futures level F_t^T is enough to automate margin calls. Before Nakamoto (2008) proposed his solution to the double spending problem, it was not possible to couple financial flows directly to informational flows without the services of a trusted third party. This highlights the prime importance of DLT's consensus mechanism and authentication protocol (with its key cryptographic components) for the blockchain used to register smart contracts. As a matter of fact, they are at the core of the solution to the double spending problem, and therefore primordial to DLT's safety.

We could offer more sophisticated examples, incorporating early termination of a derivative contract or its programed roll-over. If compared to other automation systems, the cryptocurrency transfer component embedded in smart contracts is where their added value resides. An important point is that the cryptocurrency can be attached to one specific distributed network and be programmed to be usable only for pre-programmed anticipated cases, such as margin requirements and collateral management as illustrated in our previous futures contract example. In this sense, using smart contracts for trading securities and derivatives should have the technical advantage of making it possible to actively and seamlessly manage collateral via pre-programing. Multi-collateralization should become in turn much harder.

Additionally, the possibility of programming for what, to whom and under what circumstances this cryptocurrency should be used is a way to securely segregate collateral money. Hence smart contracts could represent a safe and efficient way to segregate financial assets and manage collateral, whichever its form, provided it is linked to the main distributed ledger operating the smart contracts.

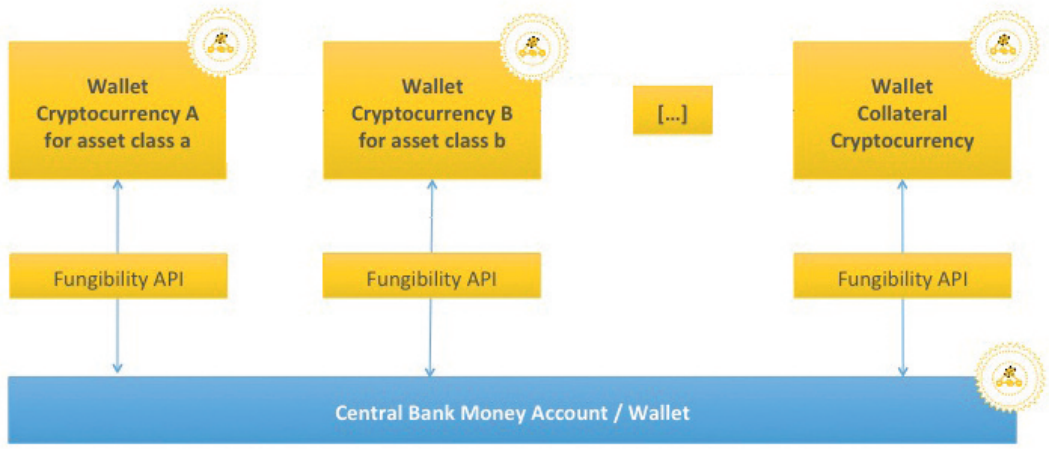
Last but not least, we believe that DLT could be designed and exploited to manage complex structured products such as collateralized debt obligations (CDO). Indeed, one can imagine a dedicated CDO blockchain linked to its underlying mortgage-backed securities (MBS), and operating the CDO as a smart contract. This could automate and simplify the costly and complex task of servicing CDOs (and other structured products) while improving their risk management. Given the above, we believe the use of DLT for securitized products is worth further investigation.

7.2. Collateral cryptocurrency

The concept of collateral cryptocurrency, segregated by design in its possible uses from any other purpose, could prove interesting for efficient collateral management. One could imagine that a collateral cryptocurrency wallet could be used and filled, when relevant, prior to a trade. The cryptocurrency would be stored and transferred on a specific chain, in order to guarantee segregation. Such cryptocurrency-based collateral management, would require the same level of financial analysis and risk management skills as currently needed by clearinghouse members. It is also important to note that a cryptocurrency could also be denominated in fiat currency. The concept of cryptocurrency is a technical device, a token, reflecting some agreed upon value, whether through supply and demand mechanisms or by reflection of fiat money value.

Furthermore, while collateral currency with embedded proof of solvency could, to some extent, appear as a potential substitute to central bank money, it is the authors' view that in the current system, central bank money is key to managing monetary policy, and thus should not be substituted by private money. While during specific time-periods we have observed decoupling between M0 and M1 and between M1 and interest rates (Giraud, 2012), central bank money clearly remains an essential tool for monetary policy in the current system at large. However, one could imagine a system whereby segregated-by-purpose cryptocurrencies would not be fungible among themselves but only fungible with central bank money. Cryptocurrency exchange with central bank money could be assisted by smart-contract-based automated systems and monitored by dedicated risk managers. The following Figure 5 is an illustration of how cryptocurrencies could be used in combination with central bank money for collateral management and asset segregation.

Figure 5: Segregated-by-purpose cryptocurrencies



The architecture illustrated in Figure 5 would only be possible if blockchains are able to interface with central bank money. This is why we believe that DLT will unleash its full potential only if central banks, and the ECB at the European level, decide to adjust their current infrastructure (T2/T2S) to allow it to interface with new and dedicated blockchains. We believe that pilot tests could be conducted using fungibility APIs.

VIII. Policy recommendations

It is evident from the growing number of initiatives that there is currently a global rush for studying and exploiting DLT. We believe that while DLT presents multiple opportunities for financial markets in general, implementation will require a mix of prudence and audaciousness. It is indeed premature to discard current market infrastructures for unproven alternatives; but it is equally clear that whoever ignores DLT today is very likely to be left behind in the longer term.

Prudence is required because the current excitement around Blockchain/DLT is fuelled by general ideas about what it is, how it works and what it could do; however, for many of its targeted applications, it has produced few detailed proposals for implementation, let alone proofs of concept or working prototypes. Of all distributed ledgers, the Blockchain is probably the one that is the most tried and tested. Ethereum appears very promising, but is still in its infancy. Some private/consortium distributed ledger initiatives, such as SETL, are currently in the test-stage, but few are already operational, with the exception of Ripple. To sum it up, we're in the middle of a wave of innovation and we need to wait for the dust to… settle.

Audacity, on the other hand, is absolutely necessary because things are moving very rapidly and tomorrow's key players will probably be those who invest aggressively and on a large scale today. As we pointed out in our first section, it is clear that financial institutions and governments are on the lookout. And it is our conviction that distributed ledgers may provide significant benefits for global economies if properly used.

Limiting our focus to European financial market infrastructure, we see that it is still based on a mix of legacy systems, implementation depends to a large extent on national jurisdictions, and there are still many tax and legal specificities complicating the flow of cross-border transactions. Nonetheless, if we look at recent history, post-trade costs have been greatly reduced and financial market integration has become a reality fuelled by successful deployment of cross-border platforms such as T2 (and soon T2S). Hence, in Europe in particular, DLT is emerging in the wake of a significant cross-border push for capital markets union and DLT introduction could bring yet another wave of transformation (probably more disruptive this time around). Our perceived ideal would be for DLT to make capital markets more efficient while improving and simplifying financial regulation, and strengthening risk management. It is in fact our conviction that DLT will successfully deploy in financial markets provided it is able to show its longer-term benefits for regulation and regulators.

As advocated by the Giovannini Group, regulation aimed at improving the industry's innovativeness, efficiency, and safety in a cross-border context, is likely to be most effective if it is conducted in a staged approach and is able to involve all stakeholders: market participants, regulators, governments and supra-national instances. And among the many private and public initiatives mentioned before, and as shown by the last graph illustrating the key role played by central bank money, we consider that it is the ECB that is best positioned to play this pivotal role at the European level in coordination with ESMA.

Below, we detail our various recommendations regarding DLT deployment and future research topics:

R1 – European DLT framework: we recommend that European Union members' central banks, and their corresponding financial market regulators, jointly define a framework for prototyping and testing DLT, an initiative that should be open and available to all European Union financial institutions. Such a framework could be coordinated by the European Commission.

R2 – European Blockchain/DLT Steering Group: in the spirit of the previous recommendation, we believe that a pan-European DLT observatory should be put in place by the European Commission. Observatories could of course be implemented at the national level, but we believe that a strong European coordination is necessary for an efficient deployment of the technology, especially when interaction with central bank money is contemplated.

R3 – Investment programs: given the pace of DLT initiatives around the globe, we believe it is essential for the European Union to invest in DLT. Here again, programs could be implemented at the national level[82] but we believe that blockchains require international scale to be credible. We further believe that DLT should be a strategic concern for the European Union and as such, included as an infrastructure priority in the European Fund for Strategic Investments.[83]

R4 – Pilot programs: in terms of deployment tactics, we believe that it would be wise to follow the prudent ASX or Nasdaq approaches. Following ASX's example, implementing a blockchain prototype that coexists with the current system until substitution can be achieved, would reduce the risks of a premature transition. An approach similar to the Nasdaq Linq approach that focuses on private securities, will yield a smoother learning curve than if initial efforts were to focus on riskier public securities with high trading volumes. We recommend pilot programs involving private securities, such as equity shares of SMEs looking to raise capital, or relatively simple OTC products such as convertible notes. It is worth noting that in the former case, establishing an equity-ownership blockchain could also be achieved by focusing on a crowdfunding platform.

R5 – An international regulatory framework: we believe it is important to begin drawing up an international regulatory framework that would be robust to regulatory arbitrage. However, because the technology is still in its early development stages, it is also essential that regulatory efforts should not stifle innovation, or result in driving DLT-centric startups out of regulated jurisdictions.[84]

R6 – Blockchain data as legal evidence: as it is already the case in some jurisdictions, it is urgent to permit data properly authenticated on the Blockchain to be admissible as legal evidence in court proceedings.[85] Ideally, we believe that this should be done at the European level, but also advocate national initiatives, especially since they may be easier and faster to pass into law.[86]

R7 – Microcredit, crowdfunding and financing the economy: DLT could support further development of crowdfunding and peer-to-peer lending without a proprietary platform acting as intermediary. This is particularly valuable in the current environment of negative interest rates and not-so-effective bank lending. The microcredit potential of crypto-currencies and distributed ledgers is also considerable. However, as we have mentioned before, in terms of market infrastructures, DLT is not designed to act as a substitute for a market place where lenders can meet borrowers, where an order book can be built or prices negotiated. But we believe that DLT could act as a perfect post-trade infrastructure for crowdfunding or peer-to-peer lending platforms, giving users the full benefits of pseudonym transacting. Crowdfunding legislation will also need to evolve to take into account the likely integration of DLT downstream of these digital platforms.

R8 – Accounting, auditing, compliance, financial reporting and corporate governance: it is our firm opinion that DLT will prove itself a win-win opportunity for both the regulated and the regulator. DLT should in the end facilitate many corporate reporting and compliance functions, and corporate governance in general. Yet, and understandably so, current compliance rules and procedures are completely oblivious to DLT. It is our opinion that professional bodies, in the field of accounting or management for instance,[87] should finance research on how DLT is likely to impact their current procedures and standards.

R9 – Big data & IoT: we expect that the growing use of distributed ledgers will bring about ever-increasing volumes of data for many economic sectors, just like social networks did for individual consumers. It is also clear that certain DLT applications, such as property tech, will feed upon the Internet of Things and various sensors controlled by it. Hence, we believe there is a need for cross-disciplinary research projects to be conducted on these topics by industrial and academic partners, and public bodies.[88]

R10 – Cryptology and digital signatures: as cryptocurrencies are likely to continue spreading, growing attention should be given to cryptographic advancements. The current banking system already depends heavily on cryptography and IT security, but the potential development of quantum computing over the next decade is likely to challenge the safety of existing algorithms. We also believe that more research is needed on homographic encryption.[89] In France, we recommend that the current legislation on digital signatures be adapted to reflect multiple signatures as this type of scheme is likely to flourish with DLT.

R11 – Employment: the potential impact of DLT on financial sector employment, especially on middle and back-office functions, is likely to be significant in the medium or longer term. We do not believe that the introduction of DLT will necessarily imply redundancies in financial services or other sectors. But it is clear that DLT will force certain functions to evolve. We recommend that a task force on job evolution be put in place on a sectorial basis, for instance by the FBF for the French banking sector, or by research units such as the CEE.[90] It is also clear that education and training programs need to be further developed to facilitate DLT transition.

R12 – Macro-economics and SDR: as we discussed in the previous section, we believe DLT will only show its full potential if it can be linked to central banks, and used by them[91]. One potential application that we recommend investigating is using DLT for special drawing rights (SDR) as currently operated by the IMF. Though we believe this could only become reality in the long term, a DLT-based cryptocurrency with a functioning similar to SDR's could be used as an international reference money in the future.

NOTES

[1] We will refer to the Blockchain, with a capital b, or the Bitcoin Blockchain, when alluding to the distributed ledger used by the Bitcoin protocol, and will use a small b in all other instances.

[2] This quote is from Nobel Laureate Robert Shiller during a panel discussion about digital trends in financial markets at the Davos World Economic Forum on January 24th, 2014.
Shiller also called it an "inspiration" because of its embedded computer technology. Source : http://www.businessinsider.com/robert-shiller-bitcoin-2014-1?IR=T

[3] http://www.cnbc.com/2016/01/28/bank-of-america-is-going-big-on-blockchain-plans-to-file-20-patents.html

[4] There had been rumors that Honduras also intended to use the Blockchain for their land registry in 2015, but the project was canceled for political reasons, according to the DLT start-up Counterparty, who was allegedly hired to complete the work - http://www.coindesk.com/debate-factom-land-title-honduras/

[5] http://www.ibtimes.co.uk/credits-testing-kyc-blockchain-isle-man-1520923

[6] http://blogs.csc.com/2015/10/30/blockchain-in-healthcare-from-theory-to-reality/

[7] http://www.unic.ac.cy/digitalcurrency

[8] http://www.coindesk.com/openbazaar-live-version-bitcoin-market/

[9] http://www.coindesk.com/visa-europe-remittances-bitcoin-blockchain/

[10] http://www.coindesk.com/korean-bank-developing-blockchain-solution-foreign-exchange/

[11] The Society for Worldwide Interbank Financial Telecommunication (SWIFT - https://www.swift.com) allows financial institutions across the globe to send and receive information about financial transactions in a secure, standardized and reliable environment.

[12] http://www.skuchain.com

[13] As of February 22nd, 2016, R3 CEV comprises 42 members: Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J.P. Morgan,[7] Royal Bank of Scotland, State Street, UBS, Bank of America, BNY Mellon, Citi, Commerzbank, Deutsche Bank, HSBC, Mitsubishi UFJ Financial Group, Morgan Stanley, National Australia Bank, Royal Bank of Canada, Skandinaviska Enskilda Banken, Société Générale, Toronto-Dominion Bank, Mizuho Bank, Nordea, UniCredit, BNP Paribas, Wells Fargo, ING, MacQuarie, the Canadian Imperial Bank of Commerce, BMO Financial Group, Danske Bank, Intesa Sanpaolo, Natixis, Nomura, Northern Trust, OP Financial Group, Banco Santander, Scotiabank, Sumitomo Mitsui Banking Corporation, U.S. Bancorp and Westpac Banking Corporation.

[14] As of February 2016.

[15] Hyperledger's 30 founding members are: ABN AMRO, Accenture, ANZ Bank, Blockchain, BNY Mellon, Calastone, Cisco, CLS, CME Group, ConsenSys, Credits, The Depository Trust & Clearing Corporation (DTCC), Deutsche Börse Group, Digital Asset Holdings, Fujitsu Limited, Guardtime, Hitachi, IBM, Intel, IntellectEU, J.P. Morgan, NEC, NTT DATA, R3, Red Hat, State Street, SWIFT, Symbiont, VMware and Wells Fargo.

[16] SX invested in Digital Asset Holdings, along with ABN AMRO, Accenture, BNP Paribas, Broadridge Financial Solutions, Inc., Citi, CME Ventures, Deutsche Börse Group, ICAP, J.P. Morgan, Santander InnoVentures, The Depository Trust & Clearing Corporation (DTCC) and PNC Financial Services Group, Inc.

[17] http://www.coindesk.com/intel-testing-blockchain-built-fantasy-sports-game/

[18] DTCC's Press Release, January 25, 2016 : "New DTCC White Paper Calls for Leveraging Distributed Ledger Technology to Solve Certain Long-Standing Operational Challenges" – available as of February 22, 2016 on the Internet at: http://www.dtcc.com/news/2016/january/25/new-dtcc-white-paper-calls-for-leveraging-distributed-ledger-technology

[19] In France alone, the share of new jobs related to transaction management and IT has been steadily increasing over the last few years (2015, Observatoire des métiers dans la banque).

[20] In this case, the database processing load is shared across a group of servers by horizontally partitioning the data. The federated servers are managed independently but cooperate to process the database requests from the applications. As cooperation between servers is typically programmed by a central authority, the case of federated servers still falls into the central architecture paradigm previously described.

[21] As evidence that "old" information technology can still satisfy its users, it is interesting to remark that COBOL, a language first created in 1959, is still very much used in the financial industry.

[22] An illustration of this typical set of rationales can be found in DFIN-511 / Session 2, Introduction to Digital Currencies, University of Nicosia, 2015.

[23] For each development covered in this paper, we also provide references not necessarily included in Nakamoto's original paper.

[24] The French crytpologist Jacques Stern writes in "La science du secret", (1998) that this paper is so important in cryptography that it is fair to say there is a "before" and an "after" the introduction of this key concept.

[25] http://hashcash.org/papers/announce.txt

[26] http://www.dsi.unive.it/~marek/files/04.55%20-%20peertopeer.pdf

[27] As mentioned by Nick Szabo himself during the DevCon1 Ethereum Developer Conference on November 13th 2015; the video can be found at: https://www.youtube.com/watch?v=YpSeOU1VVj4

[28] On smart contracts: http://szabo.best.vwh.net/formalize.html

[29] On colored coins/proplets: http://szabo.best.vwh.net/proplets.html

[30] This gives 2^{256} potential combinations, about 10^{77}, which is much more than the estimated number of atoms on earth (c. 10^{50}) and slightly less than the estimated number of atoms in the universe (c. 10^{81}).

[31] To change the *seed* of the random number generator (to make sure that any two bitcoin addresses generated will be different), users will typically be asked to move a mouse around randomly.

[32] See: "Mapping the Bitcoin Economy Could Reveal Users' Identities", by Tom Simonite, MIT Technological Review, September 5, 2013.

[33] Bitcoin wallets are usually implemented on smart phones, and the bitcoin addresses they create are hard to trace back to the smart phone owner/user.

[34] The soft fork approach was how Pay-to-script-hash (P2SH) transactions (standardized in BIP 16) were introduced to the Bitcoin network. These transactions allow bitcoins to be sent to script hash addresses (that start with 3) instead of public key hash addresses (that start with 1).

[35] A rough estimate of Bitcoin's current capacity is 7 transactions per second. In comparison, the Visa network can cope with peak volumes of about 56,000 transactions per second.

[36] For instance, Bitcoin's Segregated Witness soft-fork (segwit), while including a wide range of features, should allow an increase in the capacity of the Blockchain: https://bitcoincore.org/en/2016/01/26/segwit-benefits/

[37] A visualized history of cryptocurrencies can be found at http://www.mapofcoins.com

[38] The reader can consult the site http://www.coinmarketcap.com for a list of the various cryptocurrencies and market capitalization.

[39] Source : http://www.ethereum.org

[40] "On public and private blockchains", post in Crypto Renaissance Salon, August 7th, 2015.

[41] Some computer experts such as Vitalik Buterin seem to wonder, however, whether other techniques such as zero-proof algorithms would not be more efficient in a private context. On cryptographic authentication, Buterin states that "there is no reason to believe that the optimal format of such authentication provision should consist of a series of hash-linked data packets containing Merkle tree roots; generalized zero knowledge proof technology provides a much broader array of exciting possibilities about the kinds of cryptographic assurances that applications can provide their users."

[42] This white paper can be found at : http://www.blockstream.com. Blockstream, that offers sidechain solutions, recently announced it had raised $55 million in a Series A round of financing.

[43] Multichain is an open source private blockchain platform, backward-compatible with Bitcoin Core. Its white paper can be found at http://www.multichain.com.

[44] Source : http://www.ethereum.org

[45] Source: http://www.ripple.com

[46] For example, in the Mt Gox bankruptcy, the exchange first claimed that its problems were due to "transaction malleability". It turned out this flaw in the original Bitcoin protocol could easily be fixed (other exchanges had already corrected the problem) and was not responsible for the Mt Gox demise.

[47] Source: Financial Times, "Mt Gox founder Mark Karpelès charged with embezzlement", article by Leo Lewis, September 11th, 2015.

[48] http://www.bloomberg.com/news/articles/2015-09-21/bitcoin-firm-chief-pleads-guilty-to-first-of-its-kind-ponzi-scam

[49] Possessing the private key from which a bitcoin address is derived allows one to control any bitcoins attached to it. It should be noted that not sharing the corresponding public key also reinforces security. Indeed, bitcoin addresses are derived (using one-way functions) from public keys, themselves derived from private keys.

[50] Many authors will use the term *trustless network*, a term we deem inappropriate because we believe that on the contrary transacting on the Blockchain implies trust in its architecture, and in the majority of its nodes.

[51] Dr. Dirk Haubrich, the head of the EBA's consumer protection and financial innovation department, stated that the 51% attack was one of his foremost concerns in case the digital currency gained mass mainstream adoption. Source : http://www.newsbtc.com/2015/06/17/eba-sees-51-attack-as-bitcoin-s-biggest-threat/

[52] A global map of mining nodes can be found at http://bitnodes.21.co/

[53] A good example of this is SHA-1

[54] It is unfortunate to note that in such a case, it is not just the integrity of crypto-currency protocols such as Bitcoin that could be threatened, but more importantly the integrity of the entire current banking system.

[55] http://www.proofofexistence.com/

[56] http://virtual-notary.org

[57] https://bitproof.io/

[58] See http://factom.org

[59] See http://stratumn.com

[60] See ledgerwallet.com

[61] https://paymium.com

[62] http://lamaisondubitcoin.fr

[63] For a map of existing Bitcoin ATMs around the world, as referenced by Coindesk: http://www.coindesk.com/bitcoin-atm-map/

[64] Made law by Ordonnance n°2009-866 of July 15th 2009 - art. 12, available at: https://www.legifrance.gouv.fr/affichCode.do;jsessionid=6EB229C62D0DBC17A2BAF3350E6DFCB3.tpdjo11v_3?idSectionTA=LEGISCTA000020869628&cidTexte=LEGITEXT000006072026&dateTexte=20110624

[65] If the request is for "Libre Prestation de Service", the request can be submitted by filling out a form, available at: https://acpr.banque-france.fr/fileadmin/user.../form_LPS_EP.doc

[66] http://www.coindesk.com/how-payment-giants-are-embracing-bitcoin-and-blockchain/

[67] At the time of writing, the IC3 initiative was composed of Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, Dawn Song, and Roger Wattenhofer from the following institutions: Cornell, Jacobs, Cornell Tech, UMD, ETH, Berkeley, NUS.

[68] One of the limitations of a distributed network to keep in mind is the CAP (or Brewer's) theorem that states that it is not possible for a distributed computer system to simultaneously guarantee (i) data consistency, (ii) availability (to respond to all requests) and (iii) partition tolerance (in case of partial network failures).

[69] One of the experts we talked to joked that paying for a drink at the local store with Bitcoin was like using a Formula one racing car to go to the street corner.

[70] Blockstream's white paper on sidechains is available at: https://blockstream.com/wp-content/uploads/2014/10/sidechains.pdf

[71] Poon, J. & T. Dryja, "The Bitcoin Lightning Network", available at: https://lightning.network/lightning-network-paper.pdf

[72] The announcement was made on January 22nd, 2016.

[73] https://nxt.org

[74] To illustrate this point, discrete levels of delta-hedging could be pre-programmed into the smart contract, forcing the buying or selling of certain amounts of the underlying security when its price crosses certain pre-programmed thresholds. Closing conditions could also be pre-programmed for unwinding a position.

[75] A good example in this field is the work of www.skuchain.com that focuses on building blockchain-based products for B2B trade and supply chain finance.

[76] http://ec.europa.eu/finance/capital-markets-union/docs/building-cmu-action-plan_en.pdf

[77] https://www.banque-france.fr/stabilite-financiere/infrastructures-des-marches-financiers-et-moyens-de-paiement-scripturaux/infrastructures-des-marches-financiers/traitantlestitres.html

[78] https://www.banque-france.fr/stabilite-financiere/infrastructures-des-marches-financiers-et-moyens-de-paiement-scripturaux/target2-banque-de-france.html

[79] "Unicorns " are privately held companies valued at more than US$ 1 billion. The term "unicorn" was first used by venture capitalist Aileen Lee on November 2, 2013, in a Techcrunch article titled "Welcome to the Unicorn Club: Learning from Billion-Dollar Startups." Aileen Lee used the term "unicorn" to show how rare the phenomenon was. Aileen Lee was doing due diligence research on the tech sector in order to check that there were no bubbles when she came up with this now standard term. Source: http://www.ibtimes.com/real-reason-everyone-calls-billion-dollar-startups-unicorns-2079596

[80] http://www.bankingtech.com/348852/blockchain-based-setl-plans-to-revolutionise-payment-and-settlement/

[81] http://www.bloomberg.com/news/articles/2015-11-18/ubs-blockchain-partner-clearmatics-raises-funds-for-digital-coin

[82] For instance, in "*Les enjeux des chaînes de consensus pour la place financière de Paris*" (March 2016), the French think tank, CroissancePlus, advocates dedicating €500 million of the expected €10 billion PIA3 (a French program for investing in the future) to Blockchain.

[83] The current EFSI program, running until the end of 2017, has mobilized approx. €315 billion over three years.

[84] In the case of France, a recent colloquium organized at the Assemblée Nationale by the CSSPPCE and the CHECy has underlined the fear of many participants that "too much regulation too soon" would risk driving DLT startups out of the country.

[85] The State of Vermont is currently studying a draft bill on recognizing blockchain-based data as admissible evidence in a court of law. Source: http://legislature.vermont.gov/bill/status/2016/H.737

[86] As regards France, we fully back CroissancePlus' recommendation on the subject. Source: "Les enjeux des chaînes de consensus pour la place de financière de Paris" at www.croissanceplus.com

[87] Such as the ANC (http://www.anc.gouv.fr) or FNEGE (http://www.fnege.org) in France.

[88] Such as the *Agence de l'Environnement et de la Maîtrise de l'Énergie* (ADEME - http://www.ademe.fr/) in France where DLT-based applications could foster "smart energy practices" and the ecological transition in general.

[89] Homographic encryption allows computations to be carried out on ciphered information producing usable results without deciphering/revealing the underlying information. In France, the CHECy would be a natural candidate for monitoring DLT-centric cryptographic advancements.

[90] The *Centre d'études de l'emploi* (CEE) is a public research organization focused on employment.

[91] It is worth noticing that various central banks, in China (http://www.ibtimes.co.uk/chinese-central-bank-launch-its-own-digital-currency-1539279), in the UK (http://cointelegraph.com/news/bank-of-england-to-launch-its-own-cryptocurrency) and in the Netherlands (http://www.coindesk.com/dutch-central-bank-to-create-dnbcoin-prototype/), have recently announced their ambition to launch their own cryptocurrency.

REFERENCES

AFME (2015), *Building a Capital Markets Union*, Consultation Response.

Agre, P. (1997), *Computation and human experience*, Cambridge University Press.

Antonopoulos, A. M. (2015), *Mastering Bitcoin – Unlocking Digital Cryptocurrencies*, O'Reilly.

Back A. (2002), *Hashcash - A Denial of Service Counter-Measure*. Disponible @ http://www.hashcash.org/papers/hashcash.pdf

Blanchette, J.F. (2012), *Burdens of Proof – Cryptographic Culture and Evidence Law in the Age of Electronic Documents*, The MIT Press.

Buterin V. (2014), *DAOs, DACs, DAs and More: An Incomplete Terminology Guide*. Ethereum blog @ https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/, last retrieved April 6th, 2016.

Chaum, D. (1981), *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*, Communications of the ACM 24(2), pp. 84–88.

Chaum, D. (1983), *Blind Signatures for Untraceable Payments*, in Advances in Cryptology: Proceedings of CRYPTO 82, Plenum Press, pp. 199–203.

Chaum, D. (1984), *Blind Signature System*, in Advances in Cryptology: Proceedings of CRYPTO 83, Plenum Press, p. 153.

Chaum, D. (1985), *Security Without Identification: Transaction Systems to Make Big Brother Obsolete*, Communications of the ACM 28(10), pp. 1030–1044.

Chaum, D. (1988), *The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability*, Journal of Cryptology 1, pp. 65–75.

Chaum, D., A. Fiat & M. Naor (1988), *Untraceable Electronic Cash*, in Advances in Cryptology — CRYPTO '88 Proceedings, Springer-Verlag, pp. 319–327.

Collomb, A. (2015), chapitre sur *Les nouvelles formes digitales du shadow banking : du crowdfunding au bitcoin*, dans l'ouvrage *Le Shadow Banking*, Cercle Turgot et Laboratoire sur la Régulation Financière, Eyrolles, pp. 79-98.

Cont, R. (2015), *Les ressources des chambres de compensation face aux scénarios extrêmes*, Opinions & Débats, N° 11, Juillet/Août 2015, Publication de l'Institut Louis Bachelier.

Diffie, W. & M.E. Hellman (1976), *New directions in cryptography*, IEEE Trans. on Information Theory, Vol. IT-22, No. 6, pp. 644-654.

Dwork, C. & M. Naor (1993), *Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology*, CRYPTO'92: Lecture Notes in Computer Science No. 740 (Springer): 139–147.

Frunza, M.-C. (2016), *Solving Modern Crime in Financial Markets – Analytics and Case Studies*, Academic Press.

Giovannini Group (November 2001), *Cross-Border Clearing and Settlement Arrangements in the European Union*, Brussels.

Giovannini Group (April 2003), *Second Report on EU Clearing and Settlement Arrangements*, Brussels.

Giraud G. (2012), *Rendre le monopole de la création monétaire aux banques centrales ?*, *dans* La réglementation financière décryptée par Labex Réfi, Revue-Banque, numéro du 25/9/2012.

Hervo, F. (2008), *Évolutions récentes de la liquidité intrajournalière dans les systèmes de paiement et de réglement*, dans Banque de France, Revue de la Stabilité Financière, N° 11, Numéro spécial liquidité, Février.

IC3, Initiative for CryptoCurrencies and Contracts (2016), *On scaling decentralized blockchains*, disponible @ http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf

Lamport, L., Shostak, R. & M. Pease (1982), *The Byzantine Generals Problem*, ACM Transactions on Programming Languages and Systems, Vol.4, No. 3, July 1982, Pages 382-401.

Lazanis, R. (2015), *How technology behind Bitcoin could transform accounting as we know it*, TechVibes.

McMillan, J. (2014). *The End of Banking – Money, Credit and the Digital Revolution*, Editions Zero/One Economics GmbH.

Merkle, R.C. (1979), *Secrecy, Authentication and Public Key Systems*, Information Systems Laboratory, Technical Report No. 1979-1, Stanford University.

Moore, T. & N. Christin (2013), *Beware the middleman: empirical analysis of Bitcoin-exchange risk*, in Financial Cryptography and Data Security, Springer, Berlin, pp. 25-33.

Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Poon, J. & T. Dryja. The bitcoin lightning network, disponible @ https://lightning.network/lightning-network-paper.pdf

Porter, M. (1979), *How Competitive Forces Shape Strategy*, Harvard Business Review, March-April, pp. 137-145.

Preneel, B. (2007), *The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition*, Dept. Electrical Engineering-ESAT/COSIC, Katholieke Universiteit Leuven et IBBT.

Rabin, M.O. (1978), *Digitalized signatures*, in Foundations of Secure Computation, R. Lipton and R. DeMillo, Eds., Academic Press, New York, pp. 155-166.

Shiller, R. J. (2003), *The new financial order: Risk in the 21st century*, Princeton University Press, p. 71.

Stern, J. (1998), *La science du secret*, Odile Jacob.

Swan, M. (2015), *Blockchain – Blueprint for a new economy*, O'Reilly.

Une, M. (2001), *The Security Evaluation of Time Stamping Schemes: The Present Situation and Studies*, Institute for Monetary and Economic Studies (IMES), Bank of Japan, Discussion Paper Series, Discussion Paper No. 2001-E-18.

Wright, A. & P. De Filippi (2015), *Decentralized Blockchain Technology and the rise of Lex Crytpographia*, manuscrit inédit.

Yermack, D. (2015), *Corporate Governance and Blockchains*, Working paper, NYU Stern School of Business and National Bureau of Economics Research.

Yuval, G. (1979), *How to swindle Rabin*, Cryptologia, Volume 3, Issue 3, pp. 187-191.

Zacklad, M. & K. Sok (2015), *Les organisations autonomes distribuées : innovation socio-technique ou utopie technocentrée ?*, dans Actes du Colloque Org&Co, 17-19 juin 2015 pp. 286-294.

Institut Louis Bachelier
Palais Brongniart
28, place de la Bourse
75002 Paris
Tél. : +33 (0)1 73 01 93 40
Fax : +33 (0)1 73 01 93 28
contact@institutlouisbachelier.org

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DE L'INDUSTRIE ET DE L'EMPLOI

LABEX
Louis Bachelier

CONCEPTION GRAPHIQUE : VEGA CONSEIL 01 48 86 92 01