Introduction

La visibilité actuelle de la *blockchain* tient à l'intensité du mouvement spéculatif sur les crypto-actifs depuis quelques années et particulièrement depuis 2017. La spéculation liée aux crypto-actifs peut apparaître comme un phénomène grégaire entretenu notamment par les médias et par l'intérêt récent affiché par des institutions ou des entreprises puissantes, souhaitant tirer profit de cette technologie en l'implémentant ou au moins en communiquant dans le sillage de ce phénomène. Cet engouement fortement amplifié ces derniers mois et la fluctuation importante du cours de ces crypto-actifs ont eu pour effet de restreindre la focale liée à la blockchain à la bulle spéculative.

Pour autant, la technologie blockchain et les premiers usages issus de celle-ci méritent une réelle attention et le paradoxe tient au fait que le principal usage de cette technologie est de permettre de réaliser des transactions désintermédiées et donc dans une certaine mesure de spéculer avec une grande fluidité.

Avant d'étudier de manière détaillée les usages issus de la blockchain, il convient de s'intéresser à celle-ci en tant que technologie, de l'inscrire dans une filiation historique technologique et également dans son système technique [GIL 78, GIL 79].

La technologie blockchain s'inscrit notamment dans la lignée des registres sur tablettes d'argile, papyrus ou papier. Les premières formes

d'écriture avaient pour principal objectif de réaliser des registres. Les tablettes d'argile protocunéiformes d'Uruk datées de 3400 ou 3300 avant notre ère, traditionnellement présentées comme les premières traces d'écriture, sont principalement composées de registres, listant bétail et marchandises [GAR 84, KEI 63, LEE 90]. Ces traces d'utilisation de registres sur tablettes d'argile ont permis, par exemple, à des chercheurs de mener des études sur la structure du prix et l'évolution du prix de l'orge par rapport à l'argent dans l'économie néosumérienne à partir de l'analyse de ces tablettes [CRI 17]. Une trace ancienne de registre partage des caractéristiques structurelles et fonctionnelles avec la blockchain [QUI 17], il s'agit du khipu inca. Le khipu est un registre public prenant la forme d'un collier composé de cordes nouées, ordonnançant de l'information de manière cryptée et difficile à altérer, avec, d'après les avancées récentes pour les décoder [MED 18], des codes spécifiques de couleur, pour rajouter des informations à la suite de celles préalablement inscrites.

Au-delà du type de besoin auquel répond structurellement la technologie blockchain, cette technologie appartient au domaine de l'informatique, en tant que système technique. Le mot « bitcoin » est d'ailleurs une référence au bit, c'est-à-dire, en anglais, au *binary digit* ou, en français, au chiffrage binaire, l'unité de mesure de base en informatique, composée de 0 et de 1. Le bit dont il est question dans le bitcoin est celui de la fonction de hachage de blocs de données SHA-256, conçue par la National Security Agency (NSA) et utilisée pour sécuriser le protocole Bitcoin en s'assurant de la validité des blocs grâce à la méthode de *Proof of Work* (PoW) ou « preuve de travail ». Ces systèmes de hachage et de sécurité informatique peuvent se révéler faillibles. Des failles de sécurité du système SHA-256 pourraient avoir des conséquences destructrices pour le bitcoin. En 2005, des chercheurs chinois de l'université de Shandong ont démontré qu'il était possible de contourner la sécurité de l'ancêtre du SHA-256, le SHA-1, en provoquant des collisions, c'est-à-dire en obtenant une même signature (un hash identique, c'est-à-dire une même chaîne de bits) pour deux blocs différents [WAN 05]. En 2017, Google a réussi,

en pratique, avec une puissance de calcul colossale, à réaliser une collision avec le système SHA-1[1].

Dans la même logique, certains chercheurs se sont intéressés à l'augmentation de la puissance de calcul liée aux avancées dans le domaine des ordinateurs quantiques fonctionnant avec des quantum bits (qubits) sur la pérennité du système de PoW du bitcoin [AGG 18]. Il est d'ailleurs à noter que le système de PoW a été abandonné par plusieurs projets blockchain se tournant notamment vers le *Proof of Stake* (PoS), comme Ethereum. Le *Proof of Stake*, ou « preuve d'enjeu », accorde, généralement selon un système de tirage aléatoire pondéré, le droit de créer le prochain bloc à un validateur actif sur le réseau ayant mis en dépôt des unités de la cryptomonnaie de cette blockchain. Plusieurs projets de blockchain, comme le projet Particl, étudient des techniques pour rendre des blockchains résistantes à des attaques d'ordinateurs quantiques en renforçant la sécurité de la méthode de validation des blocs *Proof of Stake*.

Au sein du système technique de l'informatique, la blockchain peut être qualifiée de sous-catégorie des technologies de registres distribués (*distributed ledger technology*). Ces registres informatisés ont pour spécificités de ne pas avoir d'administrateur central et de ne pas dépendre d'une seule entité de stockage. Afin de garantir la cohérence des données stockées, des systèmes de consensus sont nécessaires, en tant que technologie de registre distribué, la blockchain a pour spécificité d'utiliser un système de consensus fonctionnant avec des chaînes de bloc. La blockchain permet ainsi la certification d'historiques et la validation de flux.

La technologie blockchain répond à un besoin d'enregistrement permettant d'inscrire des données et informations dans des registres pour réaliser des transactions. Cette technologie, dont les principaux fondements ont été conçus, brevetés[2] et partiellement expérimentés

1. Détails de l'expérience disponibles aux adresses : https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html et https://shattered.io/.

2. Voir notamment le brevet du 14 novembre 1989 (déposé le 30 juillet 1987), accordé à Ralph C. Merkle pour « Digital signature system and method based on a conventional

[PRE 96] dans les années 1990, a été popularisée avec le bitcoin, en pratique, à partir de 2009, à une période où les consommateurs étaient très réfractaires à l'utilisation de leur numéro de carte bancaire pour réaliser des achats sur Internet, de peur d'être piratés. L'article fondateur du bitcoin publié en 2009, intitulé « Bitcoin : A Peer-to-Peer Electronic Cash System » [NAK 09], est, comme son titre l'indique, focalisé sur le déploiement d'un système de monnaie électronique en pair-à-pair. Cet article n'est pas un manifeste cypherpunk, mais bien un article scientifique en informatique, portant principalement sur la présentation d'un procédé de sécurisation à mettre en place pour les paiements par signature électronique.

Des solutions, comme celles de PayPal, société créée en 1998 et rachetée par eBay en 2002, existaient déjà lors de la création du bitcoin en 2009. Dans un débat sur la chaîne CNBC le 14 août 2018, l'ancien Président de PayPal, Bill Harris, qualifiait la blockchain et l'ensemble des cryptomonnaies de « totalement inutiles », en insistant sur le fait que d'autres technologies étaient plus performantes pour répondre au besoin de transfert d'argent et que le seul critère à prendre en compte était la vitesse du réseau[3].

La différence avec ces solutions techniques de transfert de devises tient au fait que la blockchain, y compris celle de Bitcoin, en raison de

---

encryption function », le brevet du 4 août 1992 accordé à Stuart A. Haber et Wakefield S. Stornetta Jr. pour « Digital document time-stamping with catenate certificate » ou encore le brevet du 25 novembre 1986 accordé à Tatsuaki Okamoto, Shoji Miyaguchi, Akira Shiraishi, Tsukasa Kawaoka, « Signed document transmission system ». Les brevets ont une durée de validité maximale de 20 ans à compter de la date de dépôt, les principales innovations en matière de cryptage, horodatage et registre distribué sont donc dans le domaine public depuis l'émergence de l'écosystème blockchain. Il est donc en grande partie erroné de présenter les premières innovations en matière de technologie blockchain comme *open source*, elles sont en réalité tombées dans le domaine public.

3. « I think the problem statement is correct, for instance one of the thing why people loves Bitcoin or XRP or something like that is look at how difficult it is to get money from one country to cross the border to another, it is slow, it is expensive, it is all these things. Agree. You don't need Bitcoin, you don't need XRP, you don't need any of that to solve that problem. What you need is just a faster network. », Bill Harris, ancien Président de PayPal, 14 août 2018, CNBC.

ses spécificités technologiques, n'est pas limitée au transfert de devises préexistantes, mais propose un nouveau paradigme à la fois non centralisé et distribué. La technologie blockchain répond profondément à la notion de « paradigme » au sens kuhnien[4], en ce qu'elle fédère une communauté de chercheurs (et d'entrepreneurs) autour d'un consensus scientifique. Le consensus est d'ailleurs un aspect central dans le développement même des blockchains, celles-ci étant généralement participatives et leur code ne pouvant être modifié qu'en cas d'accord de la majorité de la communauté.

Actuellement, un écosystème de solutions d'enregistrement de transactions et d'opérations se développe à partir de ces deux grands axes de la blockchain que sont la non-centralisation et la désintermédiation et pourrait transformer les usages. L'émergence de la blockchain, en tant que technologie, modifie très sensiblement les rapports de force économiques et la place centrale occupée actuellement par les intermédiaires (financiers, juridiques, institutionnels, éditoriaux, etc.) qui tentent de se repositionner pour préserver leurs avantages acquis sur ces champs d'activités. Si cette innovation débouchait effectivement sur des usages importants [EDG 98], certains pourraient l'interpréter comme une nouvelle forme de déterminisme technique[5] ou tout au moins un élément déterminant du bouleversement des rapports de force préexistants. Cette technologie est ainsi en voie de « sociabilisation », pour reprendre la notion de l'historien des sciences François Russo[6], ou, pour utiliser un terme plus fréquent, en voie d'adoption par la société et ses institutions.

La désindexation progressive des cryptomonnaies des devises devrait transformer la manière de consommer et d'investir, le comportement

4. « Les hommes dont les recherches sont fondées sur le même paradigme adhèrent aux mêmes règles et aux mêmes normes dans la pratique scientifique. Cet engagement et l'accord apparent qu'il produit sont des préalables nécessaires de la science normale, c'est-à-dire de la genèse et de la continuation d'une tradition particulière de recherche. » [KUH 83, p. 30].

5. Voir par exemple [MAR 94].

6. « Par sociabilisation, nous entendons le processus par lequel une création technique est accueillie au sein de la société, s'y répand et s'y développe. » [RUS 86, p. 225].

d'achat évoluant en fonction du mode de paiement, comme l'ont révélé de nombreuses études de « douleur du paiement » selon lesquelles, par exemple, les personnes achètent plus facilement avec des cartes prépayées ou parient des sommes plus importantes avec des jetons de casino et sont prêtes à payer un prix plus élevé un même produit avec une carte bancaire qu'avec du liquide [MON 97, RAG 08, SOM 01, VAN 13]. Pour l'instant, aucune étude n'a été réalisée sur le comportement comparatif d'achat avec des cryptomonnaies, ce qui peut s'expliquer par la difficulté de payer avec celles-ci dans l'état actuel des choses. Pour autant, sans réaliser d'études approfondies, le comportement lors des ICO a montré que les détenteurs de cryptomonnaies investissaient avec une grande facilité dans des projets leur attribuant de nouveaux jetons. Sans tirer de conclusions hâtives sur ce point, il pourrait être intéressant d'étudier si le fait d'investir avec des cryptomonnaies limite l'aversion au risque par rapport à l'investissement en devises.

La blockchain représente une nouvelle étape dans les transformations liées à Internet, avec l'amélioration des systèmes de cryptage, de partage de données et l'augmentation de la puissance de calcul des ordinateurs individuels. Les usages permis par l'avènement de la blockchain pourraient avoir une portée sociétale notable, en réduisant sensiblement le rôle des intermédiaires de « confiance ».

Certains intermédiaires, dont la valeur ajoutée tenait plus à la mise en relation sélective stricte à partir de bases de données internalisées qu'à la confiance inspirée, ont été fragilisés par les premiers usages de l'Internet grand public puis des smartphones. La place des agents immobiliers ou des agences matrimoniales a par exemple été largement affaiblie avec l'apparition des plateformes de mise en relation entre particuliers puis d'applications du type *swip and match*, c'est-à-dire de sélection à la volée. Certains intermédiaires entre entreprises et consommateurs ont également été fragilisés ou remplacés, comme les agences de voyages ou les centrales de réservation de taxis.

La place des intermédiaires de confiance ou des tiers de confiance pourrait être affaiblie avec la blockchain, dont une des fonctions est de

constituer massivement des preuves en remplaçant la confiance interindividuelle par une confiance systémique [LUH 06] ou plus spécifiquement par une confiance algorithmique. Dans de nombreux pays, ou plus exactement dans de nombreux systèmes juridiques, les intermédiaires ou tiers de confiance sont des institutions publiques, des entreprises puissantes au cœur d'écosystèmes et des professions réglementées (agents, représentants, avocats, notaires, intermédiaires en financement, institution de dépôt de droits de propriété intellectuelle, etc.).

Pour autant, une acculturation importante serait nécessaire pour que les opérations désintermédiées par preuve numérique *via* blockchain se substituent, même en partie, aux opérations réalisées en s'appuyant sur la confiance interindividuelle ou sur celle accordée à certaines institutions ou professions. Une transition du contrat écrit au *smartcontract*, c'est-à-dire au contrat algorithmique fonctionnant sur un protocole blockchain, pourrait être encore plus difficile que la transition du contrat oral vers le contrat écrit. La pratique ne s'aligne pas systématiquement sur les possibilités techniques et les traditions ou habitus peuvent perdurer en raison d'enracinements culturels et civilisationnels.

En raisonnant selon une perspective occidentale, où le contrat écrit tient une place centrale dans les interactions, opérations et transactions et où la confiance est plus liée aux instances chargées d'authentifier les actes ou d'en assurer la force exécutoire, les freins à l'adoption de la blockchain tiennent principalement à la reconnaissance de la force exécutoire des opérations hors du monde virtuel.

Selon une perspective asiatique, particulièrement selon une perspective chinoise, des freins culturels pourraient limiter l'usage de *smartcontracts* autoexécutés. En effet, la société chinoise reste très attachée à la relation de confiance interindividuelle, transcrite notamment par la notion de *Guanxi* 关系 (réseau de confiance) [GRE 06, LIU 12, LUB 06, LUO 07, TRA 12, TUC 11]. Certains commentateurs occidentaux ont pu notamment indiquer cette différence culturelle au stade de la formalisation contractuelle et de l'exécution des contrats. Ainsi, un éminent spécialiste américain du droit chinois,

Stanley Lubmann, indiquait par exemple que « les affaires en Chine reposent plus sur les relations que sur du droit. Le contrat écrit ne vaut pas plus que le papier sur lequel il est écrit ; le vrai contrat est celui qui existe dans l'esprit des parties, sa force est fonction de leur relation et de leur confiance réciproque »[7]. Si cette position peut paraître radicale et si la société chinoise évolue et adopte certaines pratiques d'affaires occidentales avec l'ouverture du pays à la mondialisation et son développement économique, il n'en reste pas moins que la désintermédiation portée par la blockchain pourrait ne pas être compatible avec certains aspects de la culture d'affaires chinoise ou avec le maoïsme et avec les aspects autoritaires et de planification de l'économie socialiste de marché.

Dès lors, il paraît utile d'identifier les mutations d'usage en cours ou potentielles liées à la blockchain et les résistances sociales, économiques, juridiques et administratives susceptibles de se manifester.

Ce livre a ainsi pour objectif de discuter les usages susceptibles de découler de la technologie blockchain à partir d'une analyse de deux de ses caractéristiques fondamentales, la désintermédiation et la non-centralisation (partie 1) et de cas concrets dans plusieurs secteurs permettant de dessiner un nouveau paradigme socio-économique (partie 2).

7. « Chinese businesses rely on relationships rather than legal bonds. A contract is worth only the paper it is written on; the real contract exists in the minds of the parties and its strength consists in their relationship and whether they believe they can trust each other. » [LUB 06].