REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DES SCIENCES ECONOMIQUES, COMMERCIALES ET DE GESTION

DEPARTEMENT DES SCIENCES FINANCIERE ET DE GESTION

Mémoire de fin d'étude en vue de l'obtention d'un diplôme de master en sciences financières et comptabilité

Option : Finance et Banque

Thème :

Block Chain et crypto-monnaie : Emergences, enjeux et perspectives

Présentées par :

BOUAROUR Thileli

CHAOUCHE Melissa

Dirigée par :

Madame AMIAR Lila

Devant le jury composé de :

Présidente : M^me^ SI MANSOUR Farida

Rapporteur : M^m^ AMIAR Lila

Examinateur : M^r^ HABBAS Boubekeur

Date de soutenance :13/02/2022

Remerciements

En premier, on tient tout d'abord à remercier le bon Dieu le tout puissant et miséricordieux, qui nous a donné la force, la volonté et la patience d'accomplir et de réaliser ce modeste travail qui nous tenait à cœur.

En second lieu, ce travail n'aurait pas pu avoir le jour sans l'aide et l'encadrement de MADAME AMIAR LILA, on la remercie pour la qualité de son encadrement exceptionnel, pour sa patience, sa rigueur, ses conseils et ses efforts.

Nos remerciements s'adressent également à tous nos proches, amis(es) et à toute personne qui a participé de près ou de loin et qui nous a soutenu et encouragé au cours de la réalisation de ce mémoire.

Dédicaces

Je dédie ce travail a :

A la personne devant laquelle tous les mots de l'univers sont incapables d'exprimer mon amour et mon affection pour elle, a l'être qui m'est le plus cher, à ma douce mère.

Du fond du cœur, merci

A mon cher père qui a payé des années d'amour et sacrifie le prix de ma façon de penser. Père, je te remercie d'avoir fait de moi une femme.

A mes chers frères et sœurs que dieu les protèges.

A toute la famille BOUAROUR.

A tous mes amis (es) et tous ceux qui ont cru en moi.

Thilelli

Dédicaces

Je dédie ce modeste travail à mes très chers parents qui ont consacré leur existence pour bâtir la mienne, pour leur soutien, leur patience, et pour tout ce qu'ils ont fait pour que je sois là où je suis aujourd'hui.

Papa, Maman,

Vous me manquez très fort, mais je vous promets que je vais tenir ma promesse,

Je vais réussir.

A mes très chers frères Mastene et Mayes.

A mes grands parents.

A mes oncles Hakim, Mouloud, Mohammed et Nabil.

A mes chères tantes Naima, Malika, Manel, Nabila, Nacira, Samia et Fariza.

A tonton Mourad et Massi, tata Kahina et Noura

A mes cousines Lina, Maya, Nabila et Sarah.

A mes colocs Sarah, Lydia et Aldjia.

A tout ceux qui ont cru en moi.

J

Melissa

ACPR : Autorité Chargée de la supervision des secteurs bancaires et d'assurance

BCE : Banque Centrale Européenne

CPU : Central Processing Unit, processeur

CDS : Credit Default Swap

DLT : Distributed Ledger Technologies, un registre distribué

DAO : Decentralized Autonomous Organization, Organisation autonome décentralisée

DTCC : Depository Trust & Clearing Corporation

ECN : Electronic Compensation Networks

FED : Federal Reserve System, réserve fédérale des États-Unis

FFA : Féderation Française de l'assurance

ISDA : International Swaps and Derivatives Association, association internationale des swaps et dérivés

ICO : Information Commissioner's Office

ICS : Identifiants Créanciers

KYC : Know Your Customer, connaissance du client

PwC : PricewaterhouseCoopers

P2P : Peer to Peer

PoW Proof of Work

RGPT : Règlement Général pour la Protection du Travail

SEPA : Single Euro Payments Area

Sommaire

Sommaire

Sommaire

Introduction Générale

Introduction générale :

A l'origine des temps, l'homme se procure directement ce dont il a besoin par la chasse, la pêche et la cueillette. Au fur et à mesure que la civilisation progresse, il ne peut plus satisfaire la totalité de ses besoins qui deviennent de plus en plus variés. Il doit donc échanger les biens qu'il produit contre d'autres biens fabriqués par ses semblables.

Pour que l'échange puisse avoir lieu, la double coïncidence des désirs d'échange doit être réalisée et le désir d'échange d'un individu doit coïncider avec le souhait d'échange d'un autre individu.

Lorsque les sociétés évoluent peu, chaque individu échange sa production respective dans le cadre d'un rapport d'échange stable. Cette opération présente cependant de nombreux inconvénients : elle est toujours particularisée, n'a pas de valeur universelle et supporte des coûts d'information et de transaction. Elle ne permet pas, en définitive, d'atteindre une expression unique de l'ensemble des relations d'échange de tous les biens. Ainsi, tandis qu'il se généralise, le troc exige qu'un élément pris parmi tous les autres servent de référence. Cet étalon de valeurs, à ce stade du raisonnement, ne peut être qu'une monnaie abstraite c'est à dire qui ne donne pas lieu à une représentation concrète.

Avec l'apparition de la monnaie matérielle, nous sommes en présence d'un bien qui brise le troc et qui intervient réellement dans les échanges. Plusieurs phases se sont succédé : la monnaie marchande, la monnaie métallique, le bimétallisme.

L'histoire économique nous enseigne que la monnaie est passée progressivement d'un support ayant une certaine valeur en soi (or, argent) à un objet sans valeur intrinsèque ou purement symbolique fixée par l'Etat, se présentant sous une forme de plus en plus dématérialisée.

L'évolution économique, a été un support pour l'innovation monétaire notamment avec la création des plateformes et des registres de transactions qui ont permit le passage d'une monnaie matérielle contrôlée par l'Etat et la banque centrale à une monnaie virtuelle.

La plupart des systèmes monétaires non métalliques ne s'appuyant pas sur un bien tangible, reposent sur la confiance, accordée par ses utilisateurs, à la monnaie en tant qu'unité de compte et instrument de paiement, et, dans une moindre mesure, en tant qu'intermédiaire dans les échanges et réserve de valeur. Cette confiance s'appuie sur un principe de garantie

incarné par une institution centralisée (États, banques centrales ou instances locales dans le cas des monnaies complémentaires locales).

La volonté de ses créateurs est de donner naissance à une monnaie échappant au contrôle des États et donc non soumise à la tentation de la « planche à billets », un mal selon eux à l'origine de crises telles que celle des subprimes. En d'autres termes, selon une vision libertaire, les adeptes des crypto monnaies voient, dans la fin du monopole des banques centrales sur l'offre de la monnaie et la « débancarisation », l'assurance que les citoyens se réapproprient leur devise.

Aujourd'hui, alors que leur valeur est passée de quelques centimes en 2009 à des milliers d'euros, une évolution qui a commencé en décembre 2017, les crypto monnaies sont considérées par certains comme une menace et reconnues par d'autres comme une occasion de renouveler le système financier. Derrière ces cryptomonnaie aux caractères assez controversés, se cache une nouvelle technologie « la Blockchain », cette technologie permet d'éliminer les intermédiaires et de se débarrasser de tout opérateur de confiance dans le monde de la finance.

Si les crypto monnaies se présentent comme des monnaies électroniques pouvant s'échanger entre pairs par une banque ou autre intermédiaire financier, la blockchain se caractérise quant à elle par un registre de transactions distribué, une base de données décentralisée qui repose sur un réseau pair à pair destiné au stockage et au transfert de données.

Grâce à la cryptographie, la blockchain permet le transfert de ressources en format numérique sans passer par un intermédiaire de confiance, contrairement aux bases de données traditionnelles, administrées par des opérateurs centralisés, la blockchain est administrée de manière collective par tous les nœuds du réseau. Ces nœuds obéissent tous à un même protocole informatique, qui définit les procédures à suivre, ainsi que les conditions à respecter pour mettre à jour cette base de données.

Aujourd'hui, la blockchain est parfois assimilée à une révolution équivalente à celle de l'invention d'Internet. Mais quelles seront les répercussions réelles de cette technologie sur nos modes de vies ? Si Bitcoin nous permet d'échanger des crypto monnaies de façon décentralisée et parfaitement sécurisée, les nouvelles applications fondées sur la blockchain nous offrent des possibilités beaucoup plus larges. Certaines de ces applications nous

permettent de certifier et d'authentifier des documents, sans que soit requise la présence d'un notaire. D'autres applications nous permettent d'automatiser des transactions, de créer de nouvelles formes d'organisation ou même de nous coordonner sans recourir à aucune autorité de confiance. C'est bien là la promesse de la blockchain : Désintermédier la confiance.

La blockchain marque ainsi le passage d'un système fondé sur la confiance vers un système fondé sur la preuve : tant qu'on fait confiance à la technologie sous-jacente, on n'a besoin de faire confiance à personne.

Les banques et les investisseurs, les startups et les grandes entreprises, et même les États, tous veulent participer à cette innovation pour tenter de survivre à la vague de décentralisation et de désintermédiation, la Blockchain intéresse désormais de nouveaux acteurs qui visent à explorer d'autres types d'applications rendues possibles grâce à elle, notamment les acteurs du secteur bancaire et du secteur des assurances qui ont commencé à envisager la pratique de cette nouvelle technologie dans leurs fonctions.

La problématique :

Face à ce paradoxe, il nous est semblé pertinent de s'interroger sur la problématique suivante :

- ***Y a-t-il des perspectives de projections des technologies de la Blockchain et des crypto monnaies dans le secteur bancaire et financier ?***

De cette question principale découlent les questions secondaires suivantes :

- Comment la monnaie est passée d'un système de troc à un système de monnaie dématérialisée avec une création monétaire désintermédiée ?
- Qu'est ce que la crypto monnaie et quels sont ses enjeux ?
- Qu'est ce que la Blockchain et qu'elle est sa relation avec les crypto monnaies ?
- Est ce qu'une projection de la blockchain et des crypto monnaies sur le secteur financier et bancaire est possible et envisageable ?

Les hypothèses :

Pour répondre à cette problématique nous posons les hypothèses suivantes :

- Les technologies de la Blockchain et des crypto monnaie peuvent êtres projetées dans le secteur bancaire et financier ?

- Les technologies de la Blockchain et des crypto monnaies sont encore très récentes et méconnues, et peuvent êtres risquées et inadaptées à un secteur très sensible comme le secteur bancaire et financier ?

Motif de choix du sujet :

Bien que l'utilisation des crypto monnaies soit limitée, le potentiel qu'elles offrent est énorme, et bien qu'elles soient encore méconnues, elles constituent la monnaie du futur, c'est de là que vient notre passion pour ce sujet.

Objectif principal de recherche :

L'objectif de ce travail de recherche est d'expliquer cette nouvelle technologie de la Blockchain et des crypto monnaies, de s'approfondir sur la notion de la monnaie et son évolution à travers l'histoire jusqu'à sa dématérialisation et la désintermédiation de sa création et de s'interroger sur la possibilité de sa projection dans le secteur bancaire et financier.

La méthodologie :

L'étude en question entre dans le cadre d'un essaie de compréhension de la nouvelle technologie de la Blockchain et des monnaies chiffrées dites crypto monnaies, qui ont connu un essor phénoménale ces dernières années, en particulier depuis l'apparition de Bitcoin. Un phénomène qui change chaque jour, chaque heure, chaque minute voir chaque seconde et qui a bouleversé le secteur bancaire et financier. Une évolution historique relativement rapide à l'échelle de l'histoire des monnaies.

Ce qui nous a amené à opter pour une démarche méthodologique d'analyse descriptive basée sur la recherche documentaire à travers la consultation d'ouvrages, recherches, revues, textes réglementaires et sites internet relatifs à ce sujet, afin d'analyser et de vérifier les perspectives d'une projection de cette nouvelle technologie dans le secteur bancaire et financier.

La structure de mémoire :

A partir des hypothèses et des questions qui ont découlé, nous allons entamer notre travail de recherche à travers un raisonnement et une argumentation qui seront développés et structurés en quatre chapitres réalisés suivant un cadre théorique.

Chapitre I : Au cœur du problème, la monnaie et sa définition

Dans ce chapitre, nous allons nous introduire dans notre sujet en définissant la monnaie, en parlant de son évolution à travers l'histoire jusqu'à sa dématérialisation complète, de l'évolution économique qui a permit l'innovation monétaire et financière, des mécanismes traditionnels de la création monétaire et de sa désintermédiation.

Chapitre II : La crypto monnaie

Ce chapitre sera consacré à la crypto monnaie, sa présentation, évolution, enjeux et avenir.

Chapitre III : Le registre des transactions en crypto monnaies « Blockchain »

Le troisième chapitre sera consacré au registre de transactions « Blockchain », à sa définition, types et fonctionnement, mais aussi à la relation entre la blockchain et les crypto monnaies, et aux enjeux techniques de cette plateforme de transactions.

Chapitre IV: Crypto monnaies et blockchain : Perspectives de projection dans le secteur bancaire et financier

Dans le quatrième chapitre, nous allons étudier et analyser les perspectives de projection de ces nouvelles technologies dans le secteur bancaire et financier, leurs perspectives d'application par les acteurs du secteur financier, dans le secteur bancaire et dans le secteur de l'assurance.

Chapitre I

AU CŒUR DU PROBLEME, LA MONNAIE ET SA DEFINITION

Chapitre I : Au cœur du problème, la monnaie et sa définition.

Introduction :

Les échanges entre les hommes visent à se procurer les biens nécessaires à la survie. Un homme seul ne pouvant se procurer tout ce qui est nécessaire à sa survie, il échangera donc ce qu'il a en trop contre les objets qui lui manquent. En ce sens, l'échange est l'un des piliers de la vie en société. Ces échanges ont été facilités par la mise en place d'un instrument appelé la monnaie.

En effet, la monnaie a une fonction d'unité de compte dans le sens où elle permet d'exprimer la valeur des biens et des services dans une unité commune ; elle permet de fixer les prix et de tenir la comptabilité. Elle est la condition pour rentrer sur le marché, car l'agent économique qui désire acquérir un bien doit posséder, soit la quantité de monnaie nécessaire, soit le moyen d'obtenir cette quantité de monnaie nécessaire.

Depuis son avènement, ses formes ont évolué jusqu'à leur dématérialisation grâce aux différentes évolutions économiques et financières.

Grâce à ces évolutions, la création monétaire est passée d'une création contrôlée par la banque centrale à une création dématérialisée.

Dans ce chapitre, nous définissons, dans la première section, la monnaie et son évolution à travers l'histoire, ensuite, dans la deuxième section nous verrons que la monnaie est devenue un produit très complexe et qu'avec l'évolution économique et technologique qui ont transformé les transactions vers des transactions complètement dématérialisées, le temps est devenu d'une importance très considérable en matière monétaire, et dans la troisième et dernière section, nous allons nous pencher sur la mutation des mécanismes de la création monétaire, d'une création contrôlée par l'état et la banque centrale vers une création désintermédiée.

Section 01 : Le passage de l'économie de troc à la monnaie dématérialisée.

1. La définition de la monnaie :

Selon M. Morgues, il existe 3 définitions de la monnaie[1] :

- ***Une définition institutionnelle :*** La monnaie est l'instrument d'échange qui permet l'achat immédiat de tous les biens, services et titres sans coûts de transactions ni coûts de recherche et qui conserve la valeur entre deux échanges. C'est un phénomène social car elle repose sur la confiance des agents dans le système qui la produit.
- ***Une définition fonctionnelle :*** La monnaie est, par nature, l'instrument d'échange universel dont l'existence préalable est la condition de l'échange. Sa détention est rationnellement justifiée par la nécessité soit de rompre les relations de troc soit de différer l'échange en situation d'incertitude. Son utilisation comme numéraire conduit à simplifier le système de prix relatifs.
- ***Une définition qui se réfère aux propriétés de la monnaie :*** Dans un monde dominé par l'incertitude et la peur du risque la monnaie est le bien dont la valeur relative est la plus stable et qui présente une supériorité absolue sur les autres biens pour conserver le pouvoir d'achat en minimisant les risques. C'est la raison pour laquelle elle sera toujours acceptée dans l'échange contre n'importe quel bien.

La monnaie est l'un des instruments les plus utilisés dans notre vie quotidienne. En ce sens, elle peut être définie comme une institution caractérisant l'économie d'échange. Il est également possible de la présenter en insistant soit sur ses fonctions spécifiques, soit sur les propriétés qu'elle doit nécessairement remplir pour jouer complètement son rôle. Ces approches, non exclusives les unes des autres, sont complémentaires. Montrant la complexité du phénomène monétaire, chacune d'elles met l'accent notamment sur la manière dont celui-ci joue son rôle dans l'économie.

Plus récemment, les nouvelles technologies ont fait émerger de nouveaux instruments de circulation, tels que la monnaie virtuelle, qui présente de nouveaux défis, de nature différente, au système bancaire et aux banques centrales.

[1] Ruimy M., Dembik C., « La monnaie, fonctions, mécanismes et évolutions », édition ellipses, Paris, 2017

2. L'évolution de la monnaie à travers l'histoire[2] :

Nous pouvons distinguer historiquement plusieurs formes de la monnaie qui ont pu coexister ou se succéder. La succession chronologique des formes d'échanges monétaires, utilisée à des fins pédagogiques, ne correspond pas à une réalité historique en ce sens que le troc pur et simple ne semble pas avoir existé, les échanges dans les sociétés primitives ayant en fait des formes complexes : les opérations de comptes courants et l'usage du chèque sont connus à Babylone au VIIe siècle avant J.- C., le bimétallisme (or-argent) existe en Lydie où il fut introduit par Crésus au VIe siècle avant J.- C., le papier-monnaie est émis en Chine au IIIe siècle avant J.- C.

1.1. De l'économie de troc à la monnaie abstraite :

A l'origine des temps, l'homme se procure directement ce dont il a besoin par la chasse, la pêche et la cueillette. Au fur et à mesure que la civilisation progresse, il ne peut plus satisfaire la totalité de ses besoins qui deviennent de plus en plus variés. Il doit donc échanger les biens qu'il produit contre d'autres biens fabriqués par ses semblables. Pour que l'échange puisse avoir lieu, la double coïncidence des désirs d'échange doit être réalisée et le désir d'échange d'un individu doit coïncider avec le souhait d'échange d'un autre individu.

Lorsque les sociétés évoluent peu, chaque individu échange sa production respective dans le cadre d'un rapport d'échange stable. Cette opération présente cependant de nombreux inconvénients : elle est toujours particularisée, n'a pas de valeur universelle et supporte des coûts d'information et de transaction. Elle ne permet pas, en définitive, d'atteindre une expression unique de l'ensemble des relations d'échange de tous les biens. Ainsi, tandis qu'il se généralise, le troc exige qu'un élément pris parmi tous les autres servent de référence. Cet étalon de valeurs, à ce stade du raisonnement, ne peut être qu'une monnaie abstraite c'est à dire qui ne donne pas lieu à une représentation concrète.

1.2. De la monnaie abstraite à la monnaie concrète :

Avec l'apparition de la monnaie matérielle, nous sommes en présence d'un bien qui brise le troc et qui intervient réellement dans les échanges. Plusieurs phases se sont succédé :

1.1.1 La monnaie-marchandise :

[2] Ruimy M., Dembik C., « La monnaie, fonctions, mécanismes et évolutions », Op, cit, p3.

Il s'agit d'un bien divisible (sel, coquillages, thé, tissus, tabac, hachettes de cuivre en Gaule, arachides et mil en Afrique...etc.) pouvant se conserver, inspirant confiance, facilement cessible, accepté comme ayant une certaine valeur d'usage.

1.2.2. La monnaie métallique :

Les biens de consommation utilisés ont été rapidement remplacés par des métaux précieux (or et argent) qui avaient toutes les qualités pour être universellement acceptés (désirés pour leur rareté et leur beauté) et pour être conservés:

- Homogènes, donc facilement divisibles ;
- Inaltérables, leur durée de vie étant presque infinie ;
- Grande valeur, du fait de leur rareté, pour un poids et un volume assez ;
- Aisément transportables.

D'abord « pesée » (on remettait une certaine quantité de métal), puis « comptée » (boules de métal avec risque de fourrage), la monnaie métallique a rapidement été « frappée ». En effet, devant la puissance qui s'attache à sa détention et, par conséquent, à sa création, à sa fabrication et à sa mise en circulation, le pouvoir politique s'est réservé le droit d'émettre des signes monétaires et de définir l'étalon monétaire (pouvoir régalien de « battre la monnaie »). Cette monnaie, émise par le Prince (l'État), avait, pour valeur nominale, son contenu garanti en métal et possédait un pouvoir libératoire. Il s'agit là d'une présentation relativement idéale de la monnaie métallique car, en pratique, le souverain peut avoir intérêt à altérer le contenu métallique des pièces. Il impose alors leur utilisation pour une valeur nominale supérieure à sa valeur intrinsèque en diminuant la teneur en métaux précieux des pièces.

Cette dissociation entre valeur intrinsèque de la pièce et valeur conférée par le pouvoir politique nous amène à la logique qui prévaut à l'émission de la plupart des pièces contemporaines. Celles-ci ne constituent plus de la monnaie métallique. Il s'agit, en fait, d'une monnaie divisionnaire qui ne subsiste plus qu'à titre d'appoint. Elles sont frappées dans un métal de faible valeur et l'État leur donne une valeur légale qui les conduit à être acceptées dans les paiements.

1.2.3. La loi de Gresham (relative au bimétallisme) :

Trois métaux (or, argent et, plus rarement, cuivre) étaient traditionnellement utilisés pour frapper des pièces de monnaie qui circulaient parallèlement. Au Moyen Âge, en France, on

payait ainsi indifféremment en deniers d'argent ou en écus d'or, ces derniers restant toutefois beaucoup moins nombreux. Le régime du bimétallisme établissait, quelques siècles plus tard, un rapport légal fixe entre les valeurs des monnaies d'or et d'argent.

Cependant, le bimétallisme ne peut perdurer que si la valeur commerciale des métaux reste très proche de leur valeur officielle. Mais, si le prix de l'un des deux métaux varie, par exemple à la suite de la découverte de nouveaux gisements miniers, le métal dont la valeur s'apprécie disparaît très vite de la circulation. Il est thésaurisé, fondu ou réservé aux paiements à l'étranger. C'est la loi de Gresham, selon laquelle « la mauvaise monnaie chasse la bonne ».

Ce système monétaire, fondé sur les deux étalons métalliques, était pratiquement en vigueur partout dans le monde jusqu'au milieu du XIX siècle. Les découvertes d'importantes mines d'or (Californie en 1848, Australie en 1851), puis de mines d'argent au Nevada (États-Unis), ont déclenché de fortes divergences dans l'évolution de la valeur de ces deux métaux, troublant ainsi le fonctionnement du système bimétalliste provoquant son abandon progressif.

1.3. De la monnaie matérielle à la monnaie dématérialisée :

L'histoire économique nous enseigne que la monnaie est passée progressivement d'un support ayant une certaine valeur en soi (or, argent) à un objet sans valeur intrinsèque ou purement symbolique fixée par l'Etat, se présentant sous une forme de plus en plus dématérialisée.

1. Les billets (monnaie fiduciaire) :

D'un point de vue historique, il conviendrait de distinguer précisément deux catégories de billets: le billet d'État et le billet de banque.

Le billet d'Etat est un papier-monnaie émis par la puissance publique, ou en son nom, avec comme contrepartie des créances sur l'État.

Le billet de banque, quant à lui, n'est, à l'origine, qu'un simple certificat représentatif d'un dépôt de monnaie métallique (le montant des billets ne dépasse pas celui du stock de métal sous-jacent). L'idée en revient à Palmstruch, banquier suédois, qui avait pris l'habitude, depuis 1656, d'en remettre en échange des effets de commerce escomptés. Il est donc une monnaie de papier émise par une banque privée, ou un organisme de ce type, à partir d'une contrepartie, intégrale ou partielle, en or dans un premier temps, et à l'occasion d'octrois de crédit par la suite.

Avec le temps, estimant que la confiance régnait et donc que leur conversion en métal ne sera pas demandée, en même temps, par l'ensemble des détenteurs, l'émetteur a émis plus de billets qu'il ne conservait de métal S'ajoutant à la monnaie métallique, ces supports ont été, dès lors, progressivement consacrés comme une véritable monnaie fiduciaire. Le même type de processus a été mis en œuvre par les *Goldsmiths* londoniens (orfèvres) puis par la Banque d'Angleterre, à l'origine banque privée concurrente, qui s'imposera par la suite.

La confiance dans le billet de banque n'a été cependant totale que lorsque l'État lui conféra le cours légal. Ce fut le cas, en France, en 1870. Dès lors, tout créancier fut obligé de l'accepter en paiement dans les limites du pouvoir libératoire qui lui était accordé.

Cette idée d'une émission de billets plus ou moins indépendante des encaisses métalliques fut au cœur d'une controverse au XIX^{e} siècle.

D'un côté, les tenants de la *Currency School*, dont David Ricardo est le principal représentant, regroupés sous le nom d'École de la circulation, considèrent que dans un monde où l'idée de monnaie est encore très largement associée au métal, un morceau de papier ne peut pas être monnaie. Si une banque émet ce document sur lequel est inscrite une somme, elle doit donc en posséder l'équivalent en or ou en argent, en réserve, dans ses coffres. Dans cette optique, la monnaie reste le métal et le billet, un substitut commode au métal, permettant de faciliter la circulation.

D'un autre côté, l'École de la banque (*Banking School*), représentée par *Tooke* et *Thornton*, remet en question cette vision archaïque de la nature du billet. L'or continue, certes, à jouer un rôle prépondérant puisque le billet est convertible, mais la banque peut émettre des billets pour une valeur supérieure à son encaisse métallique. En effet, ce sont les besoins de l'économie qui appellent la création de billets. Lorsque l'activité se développe, le montant des crédits commerciaux tend à s'accroître. Or, c'est en contrepartie de ces crédits accordés que la banque émet des billets.

Ces deux analyses de la nature des billets de banque conduisent chaque école à prôner une politique différente en matière d'émission.

Les partisans du « *currency principle* », appliqué en Grande-Bretagne, voient dans l'intervention de l'État un moyen de limiter l'émission de billets pour assurer la stabilité monétaire. Une banque peut, en effet, être conduite à procéder à de nombreuses émissions. Le

surplus de billets dans la circulation peut perturber l'activité économique, en provoquant une hausse des prix. Il revient alors à l'État d'empêcher les déséquilibres en réglementant l'émission.

Les défenseurs du « *banking principle* », appliqué en France, refusent, au contraire, toute réglementation étatique. La liberté d'émission peut être compatible avec la stabilité: l'excès de billets n'est pas à redouter puisque l'émission est rythmée par le mouvement des affaires. La banque ne décide pas arbitrairement du montant à injecter dans le circuit économique. Elle diffuse ces billets en satisfaisant les demandes de crédit émanant des commerçants qui lui fournissent, en contrepartie, des effets. Il ne peut donc pas y avoir un accroissement de billets en circulation puisque ceux-ci font l'objet d'une demande. En outre, le remboursement du crédit se traduit par un retour des billets à la banque ou par un afflux de métal. Si le montant déremboursements l'emporte sur celui des crédits nouvellement consentis, la quantité de monnaie en circulation diminue. La circulation monétaire se réduit ainsi automatiquement quand l'activité économique se ralentit.

Aujourd'hui, la distinction est peut-être de moindre importance mais non pour autant dénuée de portée.

2. Le compte (monnaie scripturale) :

De même que la mise en dépôt de métaux précieux avait conduit à l'émission de billets, celle des billets conduira à l'utilisation des dépôts pour opérer des règlements par écritures. Le risque que la conversion des dépôts en soit demandée, en même temps, par tous les déposants étant minimes, les banques créent la monnaie scripturale, l'alimentation des comptes s'effectuant par l'octroi de crédits.

Jusqu'au début de la seconde moitié du XX^{e} siècle, le système de paiement en France n'a évolué que très lentement, les instruments utilisés pour transférer la monnaie scripturale étant en nombre limité. La recherche et la mise au point, au cours de la seconde du siècle, de nouveaux moyens d'échange se sont accélérées, modifiant profondément la situation observée auparavant.

Tous les règlements scripturaux reposent sur le même principe : L'ordre doit être donné par le titulaire du compte au gestionnaire de son dépôt de remettre des fonds à une personne déterminée qui, d'ailleurs, peut être le titulaire du compte s'il s'agit, par exemple, d'un retrait de billets. Au-delà de cette fonction consistant à être le support de flux financiers, l'instrument

de paiement a, le plus souvent, vocation à transporter deux autres types de flux: D'une part, un flux « commercial » d'informations entre le débiteur et le créancier (motif de l'opération, référence de facture ou de contrat...) d'autre part, un flux « juridique » permettant au banquier de disposer d'une autorisation de débit du compte (signature manuscrite, référence à une autorisation de débit préexistante autorisation de prélèvement, contrat porteur « CB »...).

S'il n'existe que deux formes principales de monnaie (fiduciaire ou scripturale), les moyens de règlement se sont, eux, multipliés et perfectionnés.

Peu répandu en France jusqu'à la Seconde Guerre mondiale, le chèque a commencé à se développer lorsque les pouvoirs publics ont rendu obligatoire le règlement par chèque ou par virement de sommes supérieures à un certain montant. Toutefois, son utilisation tend à régresser depuis plusieurs années, au bénéfice principalement des moyens de paiement électroniques (notamment la carte, le virement ou encore le télé règlement). Il a connu ainsi, en France, en 2014, un recul de près de 5 % en volume par rapport a 2013 pour atteindre 2,49 milliards de transactions (13 % des paiements scripturaux). En Europe, l'Hexagone reste de loin le pays qui utilise le plus le chèque (68,5 % des chèques émis dans l'Union européenne), loin devant le Royaume-Uni (17,8 %) et l'Italie (6,4 %). En montant, elle occupe la première place avec 32,6 % du montant total des chèques échangés devant le Royaume-Uni (23,1 %) et l'Italie (14,3 %).

Le virement, à caractère commercial et financier, permet d'effectuer des transferts de fonds entre comptes bancaires sur ordre du débiteur. Relativement peu utilisé jusqu'aux années 1960, il était essentiellement un instrument de règlement pour les opérations financières. Il est apparu progressivement comme un moyen souple automatisé de versement de salaires et de pensions.

Dans l'Union européenne, l'Allemagne détient, en 2014, la première place en nombre de virements émis avec 21,9 %. La France arrive en 3ème position tant en volume (12,6 %), derrière le Royaume-Uni (14,6 %), qu'en valeur (10,2 %) derrière le Royaume-Uni (37,5 %) et l'Allemagne (22,4 %).

L'avis de prélèvement est utilisé par certains créanciers dont l'activité conduit à procéder à des recouvrements périodiques. Il a connu, depuis sa création, un développement relativement rapide. Entièrement automatisé dans les relations interbancaires, il donne, en effet, satisfaction aux entreprises en leur procurant des facilités de gestion, et aux banquiers en raison des

faibles coûts de traitement. En revanche, il n'a connu qu'un succès relatif auprès des particuliers pour des motifs essentiellement Il est vrai qu'il s'agit de moyens de règlement, à l'initiative du créancier, qui retire toute possibilité de modulation des dates d'imputation aux débiteurs. Ceux-ci peuvent craindre, en outre, de ne pouvoir faire valoir leur bon droit, auprès de l'émetteur, en cas de litige avec ce dernier.

L'Allemagne reste, de loin, en 2014, le premier pays émetteur de prélève ment dans l'Union européenne avec 39,4 % des prélèvements émis. La France arrive à la 3ème position (16,1 %) des émetteurs de prélèvement en volume de l'Union européenne, juste après le Royaume-Uni (16,7 %). En valeur, la France occupe la 2ème position dans l'Union européenne avec 7,7 % du montant total des prélèvements, loin derrière l'Allemagne (42,1%) et devant le Royaume-Uni (7,2 %).

La carte de paiement a connu un faible engouement au début de sa mise en place. Toutefois, sous l'effet des efforts de promotion menés par les établissements de crédit au cours de ces dernières années, les cartes permettant le paiement chez les commerçants et le retrait d'espèces auprès des distributeurs automatiques de billets ont été diffusées à un rythme rapide auprès du public.

La carte de paiement, qui reste le moyen de paiement le plus utilisé a France, a atteint la barre de 50 % des paiements en 2014 avec 9,47 milliards en de paiements effectués par cartes interbancaires ou privatives en France La France représente 19,9 % du nombre de paiements par carte de l'Union européenne, et occupe la deuxième place dans l'Union européenne, après le Royaume-Uni (27,4 %) et devant l'Allemagne (7 %).

En valeur, la carte de paiement, en France, voit son montant global de paiements augmenter de manière modérée (+ 1,5% en 2014). En effet, malgré une utilisation de plus en plus répandue, la carte reste réservée pour des paiements de petit montant (47 euros par transaction en moyenne), et est de plus en plus utilisée pour des montants plus faibles à la faveur du développe ment du paiement en mode sans contact (Ce mode de paiement représente, en 2014, un montant global de 537 millions d'euros, soit 0,12 % du total des paiements par carte).

En 2014, le nombre de paiements en monnaie électronique reste, en France, relativement modeste (55 millions de paiements, 0,28 % des paiements en monnaie électronique de l'Union européenne). Le Luxembourg, hébergeant l'acteur le plus important du marché européen,

PayPal, détient de loin la première place (89 %). En valeur, elle reste utilisée pour des opérations de montants très faible (4,6 euros en moyenne par paiement). Le Luxembourg occupe largement la première place dans l'Union européenne avec 78 % du montant total des échanges de monnaie électronique devant l'Italie (18,4 %), la France détenant la 6ème place avec 0,3 %.

De nouvelles manières de payer se sont développées au cours de la dernière décennie tirant profit de l'essor de l'Internet et des technologies de l'information. Ces nouveaux services visent à apporter des fonctionnalités inédites aux utilisateurs de services de paiement. Il s'agit notamment des paiements sans contact, qui permettent de payer rapidement, sans saisir un code confidentiel pour des petits montants, en approchant une carte ou un téléphone mobile d'un terminal de paiement (Ils sont appréciés tant des commerçants que des utilisateurs car ils permettent davantage de fluidité en caisse et garantissent un confort d'utilisation accru par rapport à un paiement par carte classique) et des portefeuilles électroniques, qui permettent d'effectuer des paiements sur l'internet rapidement et simplement, sans avoir à saisir des numéros sensibles (Le numéro de carte de paiement, sa date de validité et on cryptogramme visuel).

On peut noter, par ailleurs, que les facilités de caisse, les lignes automatiques de crédit, les crédits confirmés permettent également d'effectuer des achats ou de régler une dette de la même manière que les billets ou les avoirs en compte préexistants. La frontière entre crédit automatique et monnaie devient dès lors floue.

Le système de paiement français est caractérisé, en définitive, par la faiblesse relative du nombre de paiements en espèces, et corrélativement, par le grand nombre de paiements scripturaux (par construction de l'agrégat M1).

Ce poids de la monnaie scripturale influence de façon déterminante les choix des agents économiques en matière de paiements scripturaux tant du point de vue de l'efficacité des instruments que de celui de leur coût d'utilisation.

Une telle situation trouve son origine dans la forte « bancarisation » de la population (96%). Elle résulte, à la fois :

- Des actions législatives et réglementaires des Pouvoirs publics, qui ont imposé l'utilisation des règlements scripturaux pour certaines transactions (contrôle fiscal, lutte contre le blanchiment des capitaux...).

- De la constitution par les établissements de crédit, dans les années 1970, de réseaux d'agences très denses sur l'ensemble du territoire et,
- Dans une moindre mesure, de la reconnaissance du « droit au compte » qui n'est pas assimilable à un droit au carnet de chèques dans une banque de son choix pour toute personne physique résidant en France.

Le développement rapide de la monnaie scripturale s'explique également par des qualités de commodité, les règlements par jeux d'écriture évitant les déplacements et de sécurité puisque la preuve du paiement apparaît dans la comptabilité des organismes gestionnaires des comptes.

On estime, par ailleurs, que 80 % des instruments de paiement sont échangés entre banques dans les systèmes d'échange interbancaire, les 20 % restants relevant d'un traitement intrabancaire (le débiteur et le créancier ont leur compte dans le même établissement) ou par accords bilatéraux. On évalue à plus 10 milliards le nombre annuel de paiements scripturaux, le nombre de transactions en billets ou extrêmement difficile à évaluer ressortant, selon les estimations, entre 20 et 40 milliards par an.

3. Les cartes pré chargées (monnaie électronique) :

Un grand nombre d'interrogations se pose autour de ce nouveau moyen de paiement. Elles s'inscrivent dans un spectre analytique très large allant des problèmes techniques les plus concrets (sécurisation des paiements) à des problématiques plus raffinées (impact sur la politique monétaire, véritable nature de la monnaie électronique).

Apparu, il y a un peu plus d'une dizaine d'années, le concept de monnaie électronique s'apparente à un nouveau type de moyen de paiement, soumis aux mêmes règles générales que les instruments existants, et non à une forme spécifique de monnaie. Cette monnaie est une réserve de valeur pré payée, stockée sur un support généralement électronique. De nombreux pays européens mettent actuellement en place des solutions de paiement utilisatrices de monnaie électronique. En France, la disparition des billets et des pièces en francs a suscité un certain regain d'intérêt notamment pour l'implantation du « porte-monnaie électronique », utilisable, pour des petites sommes d'argent, comme moyen de paiement auprès des tiers.

L'encours stocké dans une carte prépayée présente une différence essentielle avec la monnaie scripturale puisque le siège de la monnaie n'est plus un dépôt à vue individualisé, mais bien la carte elle-même dont la simple détention est la preuve de la créance du porteur

sur l'émetteur. Cette caractéristique rapproche cet encours stocké, des espèces dont il se différencie pourtant à deux égards: il n'a pas cours légal et il n'est pas réutilisable en tant que tel (alors qu'un billet peut servir à effectuer plusieurs règlements successifs).

Ainsi, à la lumière des caractéristiques principales d'une monnaie, la monnaie électronique n'est pas une nouvelle forme juridique qui viendrait s'ajouter aux deux formes habituelles (monnaie fiduciaire, monnaie scripturale). En effet, ne bénéficiant pas du régime du cours légal ou forcé et, même si les unités de monnaie électronique peuvent changer de mains sans être systématiquement converties en monnaies traditionnelles, elle est toujours assortie d'un droit de créance sur l'émetteur. En d'autres termes, leur valeur demeure liée à la créance qu'elles représentent sur de la monnaie scripturale. Elle n'est pas, de ce fait, un instrument monétaire.

De surcroît, elle implique davantage d'acteurs que l'échange de la monnaie fiduciaire puisque, outre le commerçant et le consommateur, l'émetteur intervient à plusieurs reprises : Au moment de la conversion des unités électroniques en somme d'argent et au moment du chargement de la carte. La monnaie électronique peut être alors définie comme un titre de créance dont la « puce », supplantant le papier, est l'instrument électronique.

Le « rattachement » de la monnaie électronique à la monnaie scripturale ou fiduciaire apparaît, au total, conditionnel à l'obligation ou non qui sera faite de recycler automatiquement les unités électroniques en monnaie bancaire traditionnelle. L'émergence d'une « société sans cash » n'est pas imminente.

La loi bancaire française a clarifié, par ailleurs, que seuls les établissements de crédit ont la possibilité d'émettre et de gérer la monnaie électronique. Elle présente donc des défis de nature différente au système bancaire et aux banques centrales.

Dans la mesure où seules les banques ont le droit de gérer cet instrument de paiement, celui-ci doit être pris en considération par les autorités de surveillance prudentielle (Autorité de Contrôle Prudentiel et de Résolution en France). Ainsi, toute fraude sérieuse sur ce moyen de transaction pourrait avoir des conséquences prudentielles importantes si elle est à l'origine d'une baisse substantielle de la rentabilité bancaire. Dans la même optique, les établissements de crédit sont requis de déposer des réserves obligatoires à la banque centrale pour le volume de monnaie électronique émis. Enfin, ils doivent adhérer au Fonds de garantie des dépôts, destiné à garantir le remboursement des fonds figurant sur le porte-monnaie.

En outre, si une importante substitution de la monnaie électronique aux pièces et billets survenait, une perte de seigneuriage constituerait un problème majeur pour l'équilibre budgétaire des banques centrales. Improbable à court terme, cette hypothèse n'est pourtant pas à écarter sur un horizon temporel plus lointain.

Mais, plutôt que de remettre en cause les banques centrales, la monnaie électronique a des implications sur la politique monétaire. La théorie économique, qui refuse d'attribuer à la monnaie la fonction de « bien public », la considère comme un instrument concurrençant les billets et pièces émis par l'Institut d'Émission. Certains experts évoquent même la possibilité, à terme, d'une éviction de la monnaie fiduciaire au bénéfice de la monnaie électronique car cette dernière nie les frontières et présente des caractéristiques complètes permettant un règlement de tout montant. Mais le faible succès, pour l'instant, du porte-monnaie électronique, quel que soit le pays, témoigne de l'avenir du métier de banquier central.

Si, la monnaie électronique venait toutefois à se développer, elle pourrait être à l'origine d'une création monétaire qui mettrait en danger la stabilité des prix, tâche assignée, pour la zone euro, à la Banque centrale européenne. En effet, son déploiement n'est pas neutre sur la quantification de la monnaie et rend in fine plus délicat la définition (et donc le contrôle) des agrégats. Il induit, en outre, une contraction de la base monétaire limitant ainsi les capacités d'actions des autorités et, par voie de conséquence, les leviers de la politique monétaire.

L'essor de la monnaie électronique sera, au final, vraisemblablement l'occasion d'une évolution des formes d'interbancarité et s'inscrit, en tout cas, dans un important contexte de mutations des technologies bancaires. Outre ces enjeux, il va mobiliser les pouvoirs publics qui auront la double tâche de veiller à l'intégrité du système de paiement et de ne pas voir diluer leur capacité de régulation macroéconomique.

En définitive, des monnaies fiduciaires ou scripturales se sont imposées peu à peu comme des instruments de paiements ayant la même valeur que les monnaies marchandise. Il est ainsi possible de donner une première définition, institutionnelle, de la monnaie, Elle est l'instrument d'échange qui permet l'achat immédiat de tous les biens, services et titres, sans coûts de transaction, ni coûts de recherche et qui conserve la valeur entre deux échanges. C'est un phénomène social car elle repose sur la confiance des individus dans les systèmes qui la produisent.

4. La monnaie virtuelle :

La plupart des systèmes monétaires non métalliques ne s'appuyant pas sur un bien tangible, reposent sur la confiance, accordée par ses utilisateurs, à la monnaie en tant qu'unité de compte et instrument de paiement, et, dans une moindre mesure, en tant qu'intermédiaire dans les échanges et réserve de valeur. Cette confiance s'appuie sur un principe de garantie incarné par une institution centralisée (États, banques centrales ou instances locales dans le cas des monnaies complémentaires locales).

Avec la généralisation de l'Internet, se sont développés de nombreux systèmes d'échanges décentralisés offrant la possibilité de s'émanciper de contraintes légales. Des échanges de films, de morceaux de musique on pu ainsi s'effectuer de manière privative, sans passer par un tiers, d'un ordinateur à l'autre (*peer to peer*). Dès lors, si de telles opérations ont eu lieu, pourquoi de tels échanges monétaires et échanges ne s'effectueraient pas ? Cette situation ouvre la voie à une large réflexion sur la création de monnaies digitales, non conventionnelles indépendantes des autorités centralisées traditionnelles, dont un exemple est le bitcoin.

L'expression « monnaie virtuelle » désigne une monnaie créée, non pas par un État ou une union monétaire, mais par un groupe de personnes (physiques ou morales) et destinée à comptabiliser, sur un support virtuel, les échanges multilatéraux de biens ou des services au sein de ce groupe. Le système peut être fermé (sans convertibilité avec la monnaie officielle) ou ouvert (avec possibilité de convertir les fonds virtuels en monnaie officielle).

Le logiciel bitcoin est une application dite open source, son code informatique est public, son acquisition et son utilisation sont gratuites. La publication du code vise à permettre à tout à chacun de le vérifier et de le modifier pour l'optimiser et ajouter des fonctionnalités. Son objectif est de réaliser des échanges directs, anonymes et sûrs grâce à un système de cryptographie. La complexité, mais aussi l'intérêt de la technologie, est de permettre d'entériner et de répertorier les transactions réalisées partout dans le monde.

Cette devise serait donc, à la fois, une monnaie et un protocole de paiement. Cependant, si elle n'a rien d'illégal, elle n'est ni émise, ni tracée par une autorité centrale.

Son essor trouve son fondement théorique notamment dans l'École autrichienne, dont une des figures emblématiques est Friedrich Hayek. Le tenants de ce courant de pensée économique considèrent que la monnaie, est bien trop importante et précieuse pour être confiée aux hommes politiques qui seront, par nature, enclins à abuser de leurs pouvoirs et

créeront de l'inflation, et aux banques, qui octroient et réduisent le volume de crédit de manière disproportionnée, accentuant ainsi les cycles économiques.

La volonté de ses créateurs est de donner naissance à une monnaie échappant au contrôle des États et donc non soumise à la tentation de la « planche à billets », un mal selon eux à l'origine de crises telles que celle des subprimes. En d'autres termes, selon une vision libertaire, les adeptes des bitcoins voient, dans la fin du monopole des banques centrales sur l'offre de la monnaie et la « débancarisation », l'assurance que les citoyens se réapproprient leur devise.

Le bitcoin échappe ainsi à toutes les règles monétaires traditionnelles. Sachant qu'il n'est utilisé que sur l'Internet, sa valeur est fragile puisqu'il n'est relié ni à un décret gouvernemental, ni à une marchandise susceptible de renforcer la confiance que ses utilisateurs pourraient avoir en lui. En d'autres termes il n'a pas de « valeur tangible » mais uniquement une « valeur d'usage » celle que veulent bien lui reconnaître les personnes qui l'utilisent, qui repose exclusivement sur la certitude que d'autres individus/entreprises accepteront le bitcoin comme moyen de paiement. Cette devise peut donc à tout moment être concurrencée par une autre monnaie virtuelle qui, si elle obtient la préférence des utilisateurs, lui ferait alors perdre toute sa valeur.

L'existence d'une base publique de données, consultable à tout moment, permet à l'usager de suivre les opérations qu'il a réalisées. Cette qualité confère à cette monnaie un statut de porte-monnaie virtuel.

Créé automatiquement, il n'est pas généré par le cycle traditionnel des prêts bancaires Plus de 11 millions de bitcoins pour une contre-valeur d'environ 6,5 milliards USD circulent, à l'heure actuelle, dans le monde. Principalement échangé contre des yuans, des dollars et/ou des euros, il peut également s'échanger contre des cryptomonnaies (Ethereum, Litecoin...) sur une dizaine de plates-formes mais sous certaines contraintes. Il est actuellement impossible pour des raisons de sécurité, de régler les transactions à l'aide de cartes de débit/crédit ou via le système Paypal. Les offreurs de bitcoin ne souhaitent pas, en effet, être payés via ces moyens de paiement car il est relativement aisé, dans certaines zones géographiques, d'annuler une opération payée par carte bancaire alors qu'une transaction en bitcoin est définitive. Cependant, certains sites autorisent leur clientèle à utiliser des moyens de paiement alternatifs - cartes prépayées, portefeuilles électroniques, espèces, comptes Paypal vérifiés, cartes bancaires avec vérification 3D Secure, etc.

Jusqu'en novembre 2013, il était habituel de considérer le cours pratiqué sur la plateforme Mount Gox (Japon) comme représentatif du marché du fait de l'important volume de transactions s'y effectuant. Sa faillite (février 2014) n'a pas affecté le cours observé sur les autres sites. Aujourd'hui, www.bitcoinaverage.com, intégrant près d'une quarantaine de plateformes pour établir un indice pondéré du cours du bitcoin, joue ce rôle de référence.

Mais déjà, il n'est plus besoin d'aller sur l'Internet ou de se rencontrer physiquement pour s'échanger cette monnaie. Au Canada (Vancouver), les utilisateurs peuvent désormais en acheter ou en vendre grâce à des distributeurs automatiques! Pour effectuer une transaction, un individu qui détient un compte en bitcoins devra s'identifier par le biais d'un contrôle biométrique. Une fois authentifié, il pourra commander quotidiennement la somme de son choix, à condition de ne pas dépasser 3000 dollars canadiens (près de 2100 euros) pour que cette opération ne soit pas qualifiée de blanchiment d'argent. Le distributeur (Robocoins) lui envoie un code QR dans le porte monnaie électronique de son smartphone et imprime un ticket.

Cependant, en dépit de sa progression globale sur le long terme, cette monnaie apparaît malgré tout intrinsèquement instable et sujette à toute une série de pathologies récurrentes (forte variation dans sa liquidité, extrême volatilité de son cours: 175 % par an entre juillet 2010 et juillet 2013; emballements spéculatifs: rendement annuel moyen de près de 400 %, effondre ment du cours début 2015...). Est-ce un effet de rareté, prompt à nourrir la spéculation ? À la différence d'un marché conventionnel, où une banque centrale n'hésite pas à intervenir pour défendre une monnaie et limiter sa volatilité, le bitcoin est laissé libre à la spéculation.

Au total, la perte de valeur entre son cours le plus haut et celui d'aujourd'hui est d'environ 80 %, éliminant ainsi la vocation du bitcoin à être une monnaie de réserve substitutive, parfois alléguée lorsque son cours était proche de ses sommets. Par ailleurs, la très faible utilisation comme moyen de paiement de transactions commerciales licites en fait un instrument de spéculation et de contournement des lois qu'une monnaie de plein exercice.

Mais, dès l'origine, de nombreux risques techniques ont été invoqués à l'encontre du bitcoin:

- Risque lié à l'irréversibilité des transactions.

- Risques opérationnels liés au logiciel et à l'environnement informatique (fichier wallet mal protégé, banque passante requise pour charger les blocs, etc.).
- Risque de change (sa relative jeunesse l'expose à de fortes fluctuations de cours).
- Risque technologique (il est souvent avancé que le réseau ne pourrait pas monter en puissance pour traiter toutes les transactions en mode *peer to peer*).

Au plan économique, il a fait également l'objet de critiques:

- Une « bulle» bien réelle pour cette devise virtuelle pourrait se produire. La difficulté de lui assigner une « valeur fondamentale » comme pour toute monnaie traditionnelle, fait d'elle le terreau du boursicotage et autres manipulations comme en atteste son parcours heurté.

- Selon Dorit Ron et Ami Shamir, chercheurs de l'Institut Weizmann (Israel), le livre public des bitcoins montre qu'à fin 2012, 78 % des unités étaient restées bloquées sur les comptes (thesaurisation). Prenons garde à spéculer car l'observation de l'évolution du cours de cette devise semble favoriser les premiers acquéreurs de la monnaie (*early adopters*). Cette situation, si elle était avérée, pourrait laisser penser à un schéma de Ponzi (montage financier frauduleux qui consiste à rémunérer les investissements des premiers clients essentiellement par les fonds procurés par les nouveaux entrants) voire à une « tulipomanie » (nom donné à « crise de la tulipe », période de très forte hausse suivie de l'effondrement du cours de l'oignon de tulipe aux Pays-Bas au milieu du XVIIe siècle. Au plus fort de cet engouement, en février 1637, des promesses de vente pour un bulbe se négociaient pour un montant égal à dix fois le salaire annuel d'un artisan spécialisé. Certains historiens ont qualifié cette crise de « première bulle spéculative» de l'histoire économique).

- L'engouement pour cette monnaie pourrait d'une part, avoir un impact sur la stabilité des prix et sur celle des systèmes financiers et d'autre part, perturber la politique monétaire (vitesse et quantité de monnaie en circulation) et, in fine, l'efficacité et la transmission de celle-ci.

- Si les monnaies virtuelles se substituent aux réelles, le bilan de la banque centrale diminuerait et les décisions qu'elle aurait à prendre n'auraient pas l'impact attendu.

Dans les pays où de telles devises ont pris un poids non négligeable, les pouvoirs publics ont rapide ment réagi. Ainsi, la société des télécoms chinoise Tencent avait lancé pour le compte de sa clientèle sa propre monnaie, Q-coin, dont le taux de change était fixé par rapport au yuan renminbi. Devant le succès de cette initiative, les autorités chinoises ont décidé d'y mettre unilatéralement fin, en juin 2009, arguant de son possible impact sur le système financier réel. Au total, « si elles ne semblent pas encore, à ce jour, menacer la stabilité financière compte tenu de leurs liens limités avec l'économie réelle, de leurs faibles volumes, leur développement doit être attentivement surveillé ».

3. La dématérialisation complète de la monnaie[3] :

La monnaie métallique est devenue marginale, et les banques ne contrôlent plus la monnaie fiduciaire, malgré des textes épars et désuets qui leur attribuent encore le monopole du crédit. La monnaie est portée par d'autres entités, au delà d'un simple territoire ou d'une zone monétaire, de sorte que la perception de sa réalité est perdue des systèmes statistiques actuels fonctionnant dans le cadre de normes juridiques nationales ou européennes. C'est le phénomène de création monétaire, en dehors du système bancaire traditionnel, que nous avons décrit dans cet ouvrage.

Avec la numérisation de l'information se développent de nouvelles formes de comptabilisation des échanges. Celles-ci ne sont plus adossées directement à des références monétaires classiques (dollars, euros, yen), mais à d'autres unités de mesure dont la seule limite est celle de l'imagination (crédits carbone, indices etc.), avec pour corollaire la prolifération de plates formes d'échanges électroniques spécialisées. Ces instruments ont une composante transactionnelle, et constituent un actif liquide dont la création a totalement échappé aux banques centrales.

Ce mode de comptabilisation des échanges est une forme moderne du troc ancestral, à ceci près que les transactions étaient le plus sou vent suivies d'un échange réel et non pas d'une écriture. Qui plus est même pour ces monnaies d'échange, le prince pouvait jouer un rôle de banquier de dernier ressort. Aujourd'hui, comme dans le cas de la titrisation, le facteur amplificateur est celui de la multiplication des transactions sans échanges physiques, rendue

[3] Serval J.F., Tranté J.P., « Monnaie virtuelle qui nous fait vivre, l'économie à l'épreuve de l'innovation financière », édition EYROLLES, deuxième tirage, Paris, 2011.

possible par les technologies de l'information plates-formes informatiques et réseaux interconnectés qui parachèvent la dématérialisation de la monnaie.

Le développement des technologies de l'information et des réseaux contribue à l'explosion du volume des transactions financières sur un produit donné, sans réalisation d'une livraison physique. Ainsi, il n'est pas rare qu'un container change de propriétaire plusieurs fois avant son arrivée au port de destination. Les transactions sur les marchés peuvent être dénouées entre deux compensations avant même d'être comptabilisées, ce qui pose le problème connu depuis long temps de ce qui se trouve dans les tuyaux en cas de défaillance et de l'affichage des volumes habituellement échangés. Le volume des transactions financières réalisées sur les seuls index des principaux marchés de matières premières (DJ. SP, S&P) est passé de 13 milliards de dollars fin 2003 à 260 milliards en mars 2008.

Désormais enfin, grâce aux CDS et autres contrats de garantie, les créances émises par les entreprises, constituées de simples factures virtuelles, d'un débit, ont les mêmes caractéristiques que la monnaie scripturale des banques et constituent de la monnaie fiduciaire. C'est pourquoi il est indispensable que les banques centrales ou d'autres organes de supervision puissent avoir connaissance des éléments de fonctionnement de ces instruments fonctionnement et la sécurité des transactions. Ceci implique pour mettre en encore une fois place les mesures de contrôle garantissant le bon Instruments d'échange et d'épargne et à tous les émetteurs que la notion de monnaie soit étendue à tous les instruments d'échange et d'épargne et à tous les émetteurs.

Section 02 : L'évolution économique support de l'innovation monétaire

1. La mutation de la monnaie vers un produit complexe à consistance indéfinie

La monnaie remplit trois fonctions économiques: unité de mesure des prix, elle permet d'évaluer la valeur des biens; moyen d'échange et de commerce, elle possède un pouvoir libératoire, réserve de valeur, elle détermine le pouvoir d'achat.

Sa première fonction d'unité de compte rend toutes les marchandises commensurables, c'est-à-dire mesurables entre elles, et constitue un référentiel simple là où l'économie de troc nécessitait une grille d'analyse complexe et constituait un handicap au développement des échanges. Sa deuxième fonction de moyen de paiement appelle un certain nombre de qualités pour en assurer un usage fluide : l'acceptabilité (d'où le succès des métaux précieux « désirables », l'inaltérabilité (l'or ne s'oxyde pas), la facilité d'usage (poids et volume limité) et la divisibilité. Enfin, sa troisième fonction suppose de pouvoir garder un certain temps, sans risque de perte, la monnaie obtenue en échange de la vente de produits.

La monnaie permet ainsi de mesurer la plupart des activités économiques, assimilables à une addition de transactions réelles ou virtuelles, mais elle ne suffit plus à en décrire la complexité croissante nécessitant de faire appel à l'information financière et à la comptabilité. Les transactions simples, immédiates entre deux parties (par exemple paiement comptant contre remise de la marchandise) ont évolué dans le temps. Au XIVe siècle sont apparues la lettre de des moyens change (qui reporte la transaction métallique comme de nos jours le chèque, lui-même en cours de remplacement par électroniques) et les compensations sur livre de comptes des banquiers (soldant actifs et passifs entre deux établissements sans transferts matériels). Ainsi, pour accompagner l'évolution de l'activité économique, la monnaie s'est progressivement étendue à des moyens de paiement scripturaux (c'est-à-dire correspondant à des écritures comptables). Aujourd'hui se pose la question des limites de la monnaie. À titre d'exemple, la question s'est posée de savoir si les programmes de fidélisation Internet (inspirés des « miles » des compagnies aériennes) devaient être soumis à la réglementation des banques centrales (échangeables sur des sites « *peer to peer* », monétisables en devises, et accumulables en l'absence de péremption).

Pour mieux comprendre la nature des problèmes soulevés par la complexification des échanges et leur transcription dans le langage comptable, examinons les composantes de ces transactions: le prix, l'objet, les parties, le temps, étant souligné que ces variables, elles-mêmes de plus en plus complexes, peuvent remettre en cause la valeur ou les fondements desdites transactions selon l'interprétation qui leur est donnée.

- **Le prix: la monnaie, une source d'informations, en est l'étalon de mesure :**

Le prix de l'échange. C'est-à-dire l'expression monétaire, est le premier facteur de l'échange pour les deux parties. Les monnaies étalons grecques puis romaines, ne comportaient pas d'expression nominal de leur valeur (aureus, denier, sesterce, as...): leur contenu métallique rendait leur valeur libératoire implicite. Après que l'Empereur Auguste (63 avant J.-C.-14 après J.-C.) eut procédé à l'unification monétaire, sous le règne d'Aurélien (270-275), l'État romain, après avoir joué pendant près d'un siècle sur l'aloi et les poids, décide en 274 d'émettre une monnaie garantie avec l'inscription sur la pièce elle-même de son poids et de son titre. La monnaie métallique restera la référence à travers les siècles, mais l'apparition d'une valeur d'échange déconnectée de la valeur métal ouvrait la voie vers d'autres formats (en particulier le billet papier apparu en Chine au VIII siècle) et la création de la monnaie fiduciaire'. La monnaie fiduciaire (du latin *fides*, confiance) repose fondamentalement sur la confiance dans l'émetteur, celui-ci garantissant la valeur faciale des pièces et billets en circulation, comme l'indique la mention figurant sur le billet actuel de 100 roupies en Inde: *I promise to pay the bearer the sum of hundred roupies*, avec la signature en fac-similé du gouverneur de la banque centrale, dont peu de porteurs sont susceptibles de connaitre la véritable contrepartie...

En effet, la nature de cette garantie a évolué depuis la disparition de convertibilité-or de la plupart des devises dans les années 1930.

- L'or, un étalon universel: de la valeur intrinsèque de la monnaie métallique à l'Or étalon puis à la réserve :

  De Gaulle à Ron Paul, nombre de politiques et d'économistes ont salué les vertus de l'or, métal neutre, impérissable et n'appartenant à personne, là où on vient de retrouver des pièces byzantines en état neuf, la monnaie papier du FED serait dans un pitoyable état si elle avait été enterrée il y a quinze siècles. Le facteur confiance dont bénéficie l'or, métal par excellence de la bijouterie, incite à l'épargne de précaution ou de spéculation. En

réponse à la thésaurisation des espèces métallique dont le coût devenait supérieur à la valeur faciale, la monnaie a progressivement cessé d'être émise en or

Depuis lors s'est posée la question du lien à l'or métal en volume disponible fini, que ce soit par une convertibilité directe (dite *universal gold standard*) auprès de son émetteur, ou par un mécanisme de contrepartie s'échangeant entre banques centrales (dit *gold exchange standard*). A défaut de revenir à une définition pondérale de la monnaie (x grammes d'or comme l'avait fait le franc germinal pus l'accord monétaire dit de la convention de Paris créant en 1865 l'Union latine durera en fait jusqu'à la Première Guerre mondiale), rien ne permet de penser que si cet or était détenu par une banque centrale mondiale qui réglerait les déséquilibres des paiements entre les nations, celle-ci livrerait effectivement son métal précieux

C'est le constat qui a présidé au décrochage du dollar en 1971 Ord devenu une simple réserve de valeur pour les banques centrales comme po particuliers, insignifiante par rapport aux masses monétaires circulantes.

Les banques centrales conservent toutefois en or dans or role de large fraction de leur encaisses, entre 65 et 80 % environ pour les in Allemagne, la France et Italie. Font exception à cette règle la Chine 0,9% elle Royaume-Uni avec 18,7 % Cette position évolue avec Fo monétaire européenne prévoyant des réserves en devises et la monnaie chinc qui reste non convertible à ce jour.

La monnaie a change de nature elle est désormais dynamique (les flux l'emportent sur les stocks, d'où l'importance de la vitesse de circulation, dématérialisée transactions virtuelles), conventionnelle (avec le support de la comptable to confiance, qui constitue le critère fondamental de la pérennité d'une monnaie peut plus se fonder sur l'or, produit physique inadapté à une économie devenue partiellement immatérielle (numérique notamment), mais sur une régulation adaptée (droit commercial pour les échanges, droit des règlements monétaires entre Ex pour autant que l'émetteur soit capable d'entretenir cette confiance par la solde de son économie et donc la valeur des titres (monnaie) qu'il émet.

Un système intermédiaire remplaçant la convertibilité universelle et fixé par les accords de Gêne en mai 1922 établissait un «gold exchange standard» entre banques centrales basé sur le dollar et la livre. Il ne vivra que brièvement. Secoué par la crise de 1929, il sera abandonné avant la Seconde Guerre mondiale.

Les accords de Bretton Woods de juillet 1944 visaient à rétablir un système universel protégeant les Etats avec la convertibilité entre devises (et le maintien de taux de changes relativement fixes) et la convertibilité-or du dollar et de la livre sterling qualifiées de monnaies de réserve.

Il ne fonctionnera lui-même que pendant quelques décennies. Du fait des déficits accumulés de leur balance des paiements, les Etats Unis finissent par renoncer le 15 août 1971 à la convertibilité-or qu'ils n'étaient plus en mesure d'assurer au regard de leurs réserves. Le métal cesse d'être une référence universelle et la valeur de la monnaie trouve désormais son unique source dans les échanges immédiats ou les crédits. La valeur du crédit, équivalent nominal de la monnaie, se justifie désormais soit par la production disponible de la nation concernée, soit par la capacité de l'État émetteur à équilibrer ses comptes, c'est-à-dire à lever des impôts sur cette production, ou à imposer les termes de l'échange pour des raisons militaires et/ou politiques, soit enfin dans la capacité du détenteur de la créance à obtenir des biens en échange.

En janvier 1976, les accords internationaux dits « de la Jamaïque » entérinaient définitivement pour une longue période la fin d'une recherche d'un système de changes fixes.

La déconnection du stock de métaux précieux à quantité disponible finie, recommandée par l'économiste américain Robert Triffin[1] a donné un formidable élan au développement de la monnaie fiduciaire. Mais elle rendait nécessaire une meilleure caractérisation de la santé des États émetteurs et de leurs économies sous-jacentes puisque leur dette n'était plus limitée par l'encaisse de leur banque centrale. D'un autre côté, la monnaie pouvait désormais plus facile ment et indépendamment de la dette s'adapter en volume aux besoins des échanges et donc à la taille des économies c'est-à-dire à leur croissance. La monnaie avait changé de nature. La notion de dette correspondant à une définition comptable de leur montant, mode et les règles d'établissement des états financiers prenaient de lors une importance nouvelle perçue par Hjalmar H. Schach auteur du redressement économique de l'Allemagne après la déroute financière qui a suivi la Première Guerre mondiale. Le pouvoir libératoire des actifs et passifs dans les bilans, y compris ceux des Etats est désormais lié à la liquidité, à la profondeur des marchés financiers et à d'autres facteurs à la connaissance variable comme la qualité de contreparties, dont la perception s'est révélée essentielle en août 2008 Conscients de leur dépendance, les principaux États établisse même des comptes très proches dans leur système conceptuel d ceux d'une entreprise privée et, pour recueillir la confiance des marchés financiers, les soumettent à un audit externe comparable.

- **Le dollar monnaie de référence :**

L'histoire de l'humanité met en lumière le rôle central de la monnaie de l'état dos nant, crédité d'un capital confiance par les utilisateurs de cette monnaie, que de sa puissance économique, politique et souvent militaire. Le dollar, monnaie de l'État dominant contemporain n'échappe pas à cette règle. Cependant, cette facilité porte en elle-même sa propre perte. La demande de dollars par les acteurs économiques étrangers encourage la création de déficits commerciaux finançables po l'émission monétaire. Comment résister à la facilité de faire fabriquer en Chine produits à bas prix qui satisferont le citoyen américain, en faisant fonctionner une planche à billets indolore. Tant que la monnaie reste dominante, les déficits s'accroissent, ainsi que l'émission monétaire, et les *Asia dollars* accumulés alimentent la thésaurisation ou des financements locaux. Qui plus est, en cédant la facilité des importations, l'État dominant enregistre une dégradation de la compétitivité industrielle sur laquelle avait été bâtie sa puissance. Le problème survient lorsque la confiance disparait et les demandes de remboursement (ou de conversion dans d'autres devises commencent à affluer à la Banque centrale. C'est le problème de l'économie américaine qui doit trouver un mode de règlement de sa dette extérieure et redynamiser sa compétitivité industrielle pour redresser sa balance commerciale, ou abandonner sa suprématie internationale. En tout état de cause il est difficile à une monnaie dominante de conserver sa place dans la durée

En synthèse, le prix de la transaction exprimée dans une monnaie n'a pas de caractère absolu (en raison notamment de la fluctuation des monnaies entre elles) et le détenteur de la monnaie supporte le risque de la perception par les autres acteurs du marché de la solvabilité de son émetteur. Toute expression monétaire n'a donc qu'une valeur relative et fluctuante. Dès lors, et c'est sa qualité, elle soumet à d'éventuelles sanctions ses émetteurs, pour autant qu'ils soient clairement identifiés, ses régulateurs, pour autant qu'ils soient compétents, et enfin, toujours, ses usagers. Ces derniers peuvent être classés en deux catégories, avec des effets des jeux monétaires différents : ceux situés dans l'espace de souveraineté (États-Unis pour le dollar ou eurozone pour l'euro...) et ceux situés en dehors de ces zones (banques centrales externes contreparties des échanges et épargnants).

Nous reviendrons sur la question, déjà abordée par les rédacteurs de la Constitution américaine, du pouvoir de contrôle du citoyen sur sa monnaie et donc sur la définition du champ de celle-ci. La dépréciation monétaire peut être l'équivalent d'un impôt (pour le détenteur d'obligations à valeur de remboursement nominale par exemple) ou d'une prime (par exemple pour les industriels ou les bénéficiaires d'emprunts).

2. L’importance du temps en matière monétaire :

Tout comme le prix, le temps est une variable dont l'influence et la lisibilité est essentielle à la sécurité financière. En effet, la multiplication des transactions sur un même support physique ne permet plus de quantifier les risques sur le paiement différé de la transaction.

Le commerce antique était peu développé en matière de crédit et de conditions d'exécution. L'échange couvert par le Code Napoléon est qualifié par l'accord sur la chose et sur le prix, éludant implicite ment l'interférence avec le temps. La réalisation des conditions devait simplement s'inscrire dans un calendrier choisi par l'homme mais non modifiable ou transformable en tant que tel. La traduction comptable de l'échange ne soulevait pas de problème. Au plus élevé de la sophistication, il suffisait de classer créances ou dettes en ordre croissant ou décroissant en fonction du degré d'éloignement de l'échéance pour vérifier la correspondance des totaux. Si le bilan était bien l'addition d'actifs et de passifs divers dont les totaux s'équilibraient, le lecteur pouvait aussi en faire une analyse poste à poste. L'orthodoxie comptable conduit à comparer l'actif circulant au passif circulant, les capitaux propres et les dettes à long terme aux immobilisations et au besoin en fonds de roulement. La technologie et les ambitions de l'homme ont fait évoluer ce contexte où régnait une certaine égal devant l'information. Les transactions peuvent désormais se faire en l'espace d'une fraction de seconde, entre les parties, sans être transcrites publiquement C'est le problème du *flash trading* et des *black pools* sur les marchés boursiers où certains opérateurs privilégiés accèdent à l'image des transactions. Les mémoires électroniques permettent d'amplifier ce phénomène en retenant l'information. Conscients de cette interférence avec le temps, opérateurs et régulateurs ont néanmoins cherché à en produire une description dans des écritures comptables Celles-ci n'étant pas adaptées, ils ont recherché d'autres modes d'expression, tels que l'actualisation des créances qui rend comparables tous les soldes, quelle que soit leur échéance d'exigibilité.

La présentation simplificatrice des opérations d'un acteur donné par leur solde pose un problème sérieux : la compensation ne reflète pas l'ampleur des volumes et des montants traités, qui n'apparaîtra qu'en cas de défaillance. Le solde non dénoué peut être considérable, comme l'ont montré les défaillances de la succursale en Asie de la banque anglaise Baring et celle des CDS de Lehman. Ceci illustre, au delà de la réglementation générale sur les instruments et places de marché, la nécessité de promouvoir des chambres de compensation avec des plates-formes de règlement-livraison pour tous les produits plus généralement, la

valeur comptable de la transaction perd son caractère immuable. L'avenir de la solvabilité et de l'adossement juridique (gage ou autre) est par nature incertain. Le taux d'actualisation à choisir doit lui-même inclure des hypothèses de volatilité de durée et de risques. L'allongement des échéances, qui du temps de la Grèce antique correspondaient aux quelques mois d'un crédit sur cargaison à livrer par bateau, peut aujourd'hui atteindre plu sieurs années. Le sous-jacent et la capacité des parties initiales à exécuter un contrat largement peut être remis en cause dans le temps. In fine, l'actualisation des créances ne résout ni la question comptable ni les questions de sécurité.

Ainsi, la lisibilité des états financiers en termes d'échéances de dettes, de créances et de risques a disparu. Cette disparition n'est pas seule ment conceptuelle. Elle résulte également de la possibilité qu'ont les marchés financiers d'acheter et de vendre tout actif ou passif non immobilisé pour le transformer en instrument liquide d'échéance variable. Si la liquidité de ces marchés était réellement permanente, la question de l'écriture bilancielle serait moins cruciale, car la valeur des titres serait connue en permanence. Ce n'est malheureusement pas le cas. Du fait de la complexité des transactions avec une variation continue des taux, un éventuel adossement des opérations directement, lorsque emprunts et dettes sont de mêmes échéances, ou indirectement, par exemple lors de la vente de produits à sous-jacent implicite, et de la coupure arbitraire du temps comptable (année civile au 31 décembre), une autre voie a dû être envisagée pour essayer de rendre compte à chaque clôture de la situation.

De cette interférence du temps et de l'état financier naîtra l'idée de corriger les valeurs en incluant dès l'instant de la transaction une estimation de la valeur du temps (par l'escompte). C'est l'extension du concept de la « juste valeur » dont il sera question au-delà de son champ naturel des instruments financiers liquides à court terme. Cette méthode engendre une volatilité des comptes. Il faut notamment intégrer l'effet des variations de taux d'intérêts sur la valeur des actifs et l'évolution du risque, lequel ne suit pas dans le temps un tracé linéaire. Le temps des comptes n'est plus celui qui a été pris en compte au moment de la décision d'investissement ou de production. L'entrepreneur devient dépendant d'un temps, devenu variable exogène. Ce temps corrigé est nécessairement imparfait puisqu'il n'a plus de lien avec celui de l'entreprise (désintermédiation). En substituant une variable temps exogène à l'entreprise, les marchés ont retenu une solution comparable à égards à celle des économies soviétiques. Les entreprises y déterminaient leurs choix d'investissements en fonction du taux annoncé par r le ministère du Plan. Il est vrai que ce dernier régulait dans une logique d'intérêt collectif alors que les marchés ont des logiques propres et indépendantes, hétérogènes entre

elles et sans lien avec les besoins des entreprises du fait de cycles économiques de durée et de risque différents. Par ailleurs, le temps est indissociable de la masse monétaire et de sa vitesse de circulation (voir chapitre 10). La liquidité doit être clairement définie par rapport à l'horizon temporel. Un horizon rapproché peut avoir des conséquences fondamentalement différentes de celles d'une cessibilité immédiate. Quelle valeur enfin accorder au calcul effectué par modélisation (dite mark to model) pour substituer à la valorisation en valeur de marché, lorsque celle-ci n'existe pas? Les comptes comme les écritures constituent des documents juridiques. Ils peuvent par le biais de la fausse information financière engager la responsabilité de ceux qui les arrêtent et les contrôlent. Le taux d'actualisation des modèles de valorisation repose sur des hypo thèses par nature incertaines et nécessairement non accessibles au lecteur du fait de l'hétérogénéité des situations. Si la description des comptes par l'information peut en permanence être améliorée, ce que le normalisateur s'attache à faire par un programme continu de révision de ses textes (par exemple IASB n° 7[1]), la correction des soldes par le temps doit être extrêmement limité à des catégories dont les contreparties sont certaines et la négociabilité assurée par ces dernières. Nous ne sommes pas dans le domaine de l'information mais de la substance à laquelle l'information ne pourra remédier.

3. Les transactions d'aujourd'hui

L'évolution de la nature des biens échangés, tant en termes de péremption que de contenu, a fondamentalement modifié le champ des transactions.

Les échanges couvrent aujourd'hui tout le spectre des marchandises et intègrent désormais une part croissante de services complexes dont la valeur peut être chiffrée différemment par les bénéficiaires ou les garants (par exemple garanties pièces et main d'œuvre). Par fois même, on est confronté à des flux complexes qui trouvent leur source dans l'échange de biens incorporels infiniment complexes contre des droits de propriété ou des titres variés (actions, obligations et tous leurs dérivés).

Ce phénomène est bien connu, mais ses évolutions sont très mal appréhendées, notamment en raison de l'absence de mesure de la désintermédiation dans les systèmes statistiques des gouvernements et des banques centrales.

- **Les acteurs de l'échange (les parties) :**

Les parties à l'échange ont perdu leur relation bilatérale avec l'apparition des places de marché, forme évoluée des foires ancestrales, qui favorisent les échanges et organisent les règlements. Dans les foires et marchés de l'Antiquité, le contenu de l'information était largement visuel pour des biens échangés sur place, et le prix pouvait être fixé entre l'acheteur et le vendeur. Les échanges se sont compliqués avec la généralisation de la monnaie scripturale et l'émergence d'un nouvel acteur intermédiaire spécialisé entre les parties: la place de marché. La transaction devenait multilatérale, la place assurant non seulement les échanges mais aussi la compensation des soldes et organisant les règlements.

Les parties ne se rencontrent plus nécessairement physiquement et les volumes échangés deviennent indépendants des transactions physiques. Par les conditions qu'elle organise à l'admission des acheteurs et vendeurs, la place de marché assure désormais la garantie de bonne fin. Cette évolution marque une étape importante de la financiarisation de l'économie en autorisant des opérations «virtuelles », par le décalage dans le temps entre la transaction, la livraison et son règlement. Cette transformation va notamment permettre de sécuriser les prix de vente des producteurs, céréales par exemple, mais aussi des transformateurs et distributeurs puisqu'elle va ouvrir la voie à des ventes « à livrer ». Les acheteurs et les vendeurs physiques ne se connaissent plus. Ils sont interchangeables. Les relations deviennent purement financières. Les livraisons et réceptions physiques, si elles sont nécessaires, peuvent intervenir totalement indépendamment et au moment opportun choisi par l'opérateur à l'origine des ordres. Le prix pour l'opérateur est en effet garanti par rapport au cours à la livraison ou à la réception, par le règlement du solde de ses transactions sur le marché. Cette organisation favorise le développe ment d'une catégorie d'agents économiques purement financiers, les courtiers » (brokers), indépendamment des agriculteurs, des industriels et des distributeurs.

Suivant la voie ouverte en 1971 par le NASDAQ, première bourse électronique, de nombreux marchés électroniques, dits ECN (*electronic compensation networks*) ont émergé ces vingt dernières années avec la révolution des technologies de l'information qui comprime les coûts d'infrastructure, et du Web qui offre un accès universel aux utilisateurs. Ces nouvelles places de négociation, dont les volumes rivalisent avec ceux des Bourses classiques, sont mal ou peu réglementées en raison de leur libre localisation, de l'effet de fractionnement des marchés et d'un mode opératoire rendu opaque par le souhait de liquéfier les marchés en admettant le maximum d'opérations dont les volumes serviront de contrepartie. S'il faut bien permettre aux opérateurs d'entrer leurs transactions sur des écrans délocalisés, il n'en reste pas moins que le fractionnement des marchés a un effet contraire à la bonne application du

principe d'égalité de traitement des opérateurs et des ordres. Ces nouvelles places de marché assurent désormais l'essentiel des transactions et enregistrent les opérations y compris de gré à gré, les Bourses traditionnelles ne constatant plus toujours des cours représentatifs puisque l'on ne sait pas, en l'absence d'homogénéité, définir ce concept de façon indiscutable.

Les mouvements monétaires en jeu prennent désormais des proportions supérieures aux budgets des États. Pour perpétrer la stabilité du système, il est nécessaire de pouvoir garantir la bonne fin des engagements sur les places de marché ou les marchés de gré à gré, indépendamment de la réalité physique ou même monétaire. Cette contrainte a présidé à l'émergence des contrats de garantie d'échanges fiduciaires, les CDS, qui assurent la garantie des bilans des opérateurs financiers et de leurs engagements. Le cercle était bouclé. Un système nouveau s'était construit de lui-même, sans rapport nécessaire avec l'économie dite réelle et auto garantie (par les CDS échangés). À l'instar des banques centrales qui certifient le caractère libératoire de la monnaie, les CDS assurent la garantie des titres échangés, ce qui confère à leur émetteur un pouvoir d'émission comparable à celui d'une banque centrale, mis à part les privilèges de souveraineté. En dépit de leurs volumes très importants, les encours de CDs sont largement dépassés par les swaps de taux d'intérêt et de durées (environ 10 fois plus importants), illustrant l'ampleur de masses financières hors de contrôle qui alimentent la spéculation.

Section 03 : Les mutations des mécanismes de la création monétaire

1. Les mécanismes classiques de création monétaire

La notion de financement a évolué avec les besoins de l'économie. Malgré plusieurs échecs, dont la faillite de Law au siècle précédent, l'innovation majeure qui a nourri la révolution industrielle et permis l'essor du système bancaire a été la monnaie scripturale. Elle représente aujourd'hui entre 80 et 90% de la monnaie des pays occidentaux selon les définitions de la BCE, et permet des transferts de fonds (cartes, chèques, virements, prélèvements, etc.) qui restent réservés en France, sauf dérogation, à des opérateurs bancaires ou assimilés, pour le compte de leurs clients.

Le mécanisme de création est initié par les banques commerciales, habilitées à prêter les montants qui leur sont confiés (les dépôts créent les crédits) mais surtout ceux qu'ils n'ont pas encore (les crédits font les dépôts). Dans ce dernier cas, le plus intéressant, que se passe t-il quand la banque prête 1 euro à un client? Elle crée un titre de 1 euro comptabilisé à son actif,

et inscrit 1 euro sur le compte de l'emprunteur, comptabilisé à son passif. Au final, elle a augmenté son actif et son passif de I euro (qu'elle a créé ex nihilo à l'occasion de l'opération). Cet euro disparaitra au fur et à mesure des remboursements de l'emprunteur. Si les banques cessaient d'accorder c dits, la monnaie scripturale telle qu'actuellement définie disparaitrait, Il va de soi que cette création monétaire repose fondamentale ment sur la confiance, car le montant des prêts dans les bilans d'une banque est un multiple de ses fonds propres, et celle-ci ne pourrait faire face à une demande généralisée de retrait des avoirs de ses épargnants en espèces. Le phénomène de panique collective constaté lors de la crise de 1929, a encore été observé en 2008 dans le cas de Northern Rock (une banque britannique de crédit immobilier), Les États tentent de limiter cette création monétaire à travers un arsenal de mesures, dont la principale est l'encadre ment du crédit par la constitution de réserves fractionnaires.

- **Le multiplicateur du crédit :**

Lorsqu'un dépôt est fait à la banque par un particulier ou une entreprise, celle-ci e lorsqu'un dépôt est fait à la banque par un particulier ou une dispose sous réserve des règles que lui imposent ses organes de surveillance d'en conserver toujours une partie (ou fraction <F> selon le vocabulaire officiel, par exemple 10% d'un dépôt initial de 1000 euros) disponible pour des retraits d déposant. La banque peut alors prêter le solde disponible (dans notre exemple 900 euros) au même déposant ou à d'autres clients. Mais cette utilisation générera un dépôt bancaire équivalent et donc une nouvelle capacité de prêt de 90% de ces 900 euros, soit 810 euros. En répétant ce phénomène, le calcul monte que la banque pourra distribuer un total de prêts de 1000 (1-f/f), soit dans note cas 9000 euros alors que le dépôt initial d'un épargnant n'était que de mouvement la banque transforme des dépôts en crédit, opération qui s'appelle transformation et elle gagne de l'argent par la différence entre le taux qu'elle accorde à son client sur ses dépôts et le taux auquel elle lui prête

Ce multiplicateur pourrait avoir un effet quasi illimité si les emprunteurs ne voulaient conserver une partie de la masse d'argent disponible sous forme de liquidité ou si la banque centrale n'avait élaboré des obligations limitatives comme l'obligation de lui en remettre une partie sous forme de dépôt.

Les autres mesures de contrôle sont les règles prudentielles que la régulation impose aux banques et les ratios que ces dernières doivent respecter: minimum de fonds propres dont elles doivent disposer pour distribuer des prêts, compensation journalière entre banques en

monnaie banque centrale des soldes des échanges, taux de rémunération des dépôts, interventions de la banque centrale pour assurer la liquidité de refinancement sur les marchés ou par le réescompte (sur la base d'un taux d'intérêt déduit par la banque centrale des effets qui lui sont remis avant échéance par les banques commerciales). Les législateurs entendent en outre ajouter un contrôle de l'effet de levier utilisé par les banques en mettant sous contrainte le rapport des capitaux qu'elles utilisent et la dette à laquelle elles-mêmes recourent.

Les autres acteurs habilités à créer de la monnaie scripturale sont les banques centrales. Elles peuvent intervenir dans trois cas: en reprenant des créances bancaires par un jeu d'écritures, en consentant des avances au Trésor public (ou en achetant des bons du Trésor), enfin en achetant des devises en échange de monnaie nationale créée pour l'occasion (par exemple pour la reprise de dollars apportés à la banque centrale par les banques à la suite des dépôts de leurs clients).

En résumé, le mécanisme de création monétaire est un acte met tant en relation un agent financier ou non, particulier, entreprise, collectivité publique, et une institution disposant d'un pouvoir monétaire, c'est-à-dire émettant une créance sur elle-même qui sera acceptée comme moyen de paiement. Ce mécanisme est processus continu de création (crédits accordés, achats d'actifs réels et financiers réalisés par les banques, entrées de devises dans le pays) et de destruction (remboursements de crédit, ventes effectuées par les banques et des sorties de devises) de monnaie, le solde étant généralement positif en période de croissance économique.

2. L’idée d’absence de banque centrale ou de l’indépendance de la banque centrale

Les Etats ont toujours été soupçonnés de se servir de la monnaie pour satisfaire leurs propres besoins. Si la gestion publique sépare depuis l'Antiquité les biens privés du souverain de ceux collectifs du peuple, le prince est soupçonné à juste titre de se servir de la monnaie pour satisfaire ses besoins privés (le train de vie) ou collectifs (la guerre ou les grands travaux par exemple). La séparation des patrimoines, si elle crée une limite, peut au contraire autoriser tous les débordements au nom de l'intérêt collectif. Le contrôle parlementaire sur les dépenses et les recettes de l'État n'a été que progressif et souvent trop tardif, comme l'illustre la réunion des États généraux en 1787[1] faite par le monarque sous la menace d'une banqueroute d'État, devant l'impossibilité d'obtenir une réforme fiscale que ses prédécesseurs avaient déjà tentée.

De nombreux auteurs dénient à l'État le privilège de battre monnaie, y compris au nom de la collectivité?, et prônent l'absence de banque centrale, fût-elle indépendante, de sorte que l'Etat soit réduit à la situation d'un simple agent économique dont le crédit puisse être remis en cause par ses créanciers. Ceci a été le cas de Madison et celui de Jefferson, un des plus brillants présidents des États-Unis, très proche de Samuel Dupont, ce qui explique la création tardive d'une banque centrale, d'abord privée puis publique aux États-Unis[1]. La raison économique et plus précisément la contribution positive d'une monnaie unique au développement des échanges a progressive ment permis la généralisation de ce modèle. Il reste alors à résoudre la question du statut institutionnel. La création de banques centrales d'abord privées puis publiques au XIXe siècle avait pour objectif d'instaurer la confiance dans la monnaie, par l'indépendance vis-à-vis du souverain. Aujourd'hui encore, la banque centrale doit être structurée pour être neutre, avec des comptes séparés de ceux du budget de l'État.

Pourtant, cette indépendance, même inscrite dans la Constitution, ne peut être absolue. La banque centrale ne peut pas s'abstraire des besoins de l'économie puisqu'elle est censée la servir en assurant le bon fonctionnement du système bancaire. Ainsi, lorsque la liquidité des banques disparaît avec un risque de défaillance en chaîne ou que les prix s'effondrent sur les marchés financiers comme conséquence de politiques étatiques qui n'ont pas veillé au respect de certains équilibres macroéconomiques (déficit de l'État, commerce extérieur, inflation...), la banque centrale est contrainte d'intervenir. Alors, défiant parfois ses propres statuts, elle achète des actifs pour soutenir les valeurs, comme le ferait une banque commerciale. Ce sont les politiques dites « non conventionnelles », consistant par exemple à en acheter des papiers de dettes publiques pour notamment les prix d'émission. Le besoin fait loi.

3. La désintermédiation de la création monétaire[4]

Le dispositif de régulation monétaire au travers des crédits et des dépôts ne fonctionne que si lesdites transactions se font par l'intermédiaire d'une banque commerciale reconnue et autorisée par la banque centrale. Or, le développement des marchés financiers, notamment de gré à gré, c'est-à-dire passant par un intermédiaire, a ouvert aux agents économiques la possibilité de se financer auprès d'autres sources que les banques, en dehors de leur zone monétaire et éventuellement dans une autre devise. Ce phénomène de « désintermédiation »

[4] Serval J.F., Tranté J.P., « Monnaie virtuelle qui nous fait vivre, l'économie à l'épreuve de l'innovation financière », Op. cit. p19

permet aux entreprises de ne plus passer par les canaux bancaires traditionnels pour se financer ou pour faire transiter leurs paiements.

Si nous revenons à la définition du concept, une opération de crédit entre deux agents non financiers n'est pas source de création monétaire, car la créance en résultant ne peut servir à effectuer des achats. Ce n'est que si cette créance est revendue dans un second temps à une institution monétaire (par voie d'escompte, par exemple), qu'il y aura création monétaire. Or, en quelques années, les volumes de ces financements « désintermédiés », notamment les crédits interentreprises, ont significativement dépassé ceux qui sont issus de la création monétaire, et ne sont pas comptabilisés dans la masse monétaire. Cette désintermédiation n'apparait pas clairement dans les bilans appréhendés statistiquement par le système de surveillance des banques centrales. Cette carence réduit significativement la pertinence du contrôle monétaire, dès lors que le recours au financement ne passe plus par les banques commerciales, mais par des investisseurs non régulés au plan bancaire (fonds de pension, entreprises, etc.), par des agents non domiciliés dans la même zone monétaire ou par des marchés financiers non régulés, dont l'encours peut être financé par des capitaux offshore. Une partie de la masse des déficits extérieurs non recyclés par la souscription de bons du Trésor (ou papiers souverains de tous ordres) est ainsi financée par des canaux extérieurs qui alimentent l'émission monétaire.

A la seul, le crédit interentreprises, mode historique de financement désintermédié (puisqu'échappant aux banques) représente l’équivalent d'un tiers de M3 en France avec un total de créances clients de 528 milliards d'euros fin 2007, selon la Banque de France.

Une deuxième source de financement est apparue avec le développement des échanges internationaux et l'ouverture de lignes de crédit par des établissements non soumis à la régulation de l'institut d’émission de la monnaie concernée (les eurodollars des années 1980), Associée à l'essor des places de marché qui démultiplient les échanges financiers sur un même sous-jacent, sans échanges physiques, cette nouvelle forme de crédit et donc de monnaie a ouvert une brèche dans les dispositifs nationaux de régulation.

Plus récemment, la titrisation a permis de diffuser des titres de financement échangeables, en volumes considérables, en offrant la faculté de transformer toute forme d'actif en produit financier.

Enfin, la vente en ligne de produits ou de crédits et la disparition du monopole des moyens de paiement favorisent cette désintermédiation au travers de mécanismes de compensation informatisés et purement comptables, auxquelles sont associées des plates formes logistiques de livraison (uniquement nécessaire en cas de biens matériels).

Dès lors, l'échange entre agents économiques n'a plus besoin d'être compensé par l'argent des émissions monétaires, et le support universel que constitue la combinaison des nouvelles formes de communication avec les plates-formes logistiques assure un avenir aux échanges non soldés, mettant ainsi à mal le monopole d'émission monétaire. Au-delà même de la possibilité de créer des monnaies privées dites implicites sous forme de points ou autres (« miles »...), ces mécanismes d'échange s'apparentent à une forme moderne de troc, sans l'inconvénient (pour la rapidité d'exécution) de la rencontre physique.

Ainsi, cette désintermédiation bancaire, favorisée par la souplesse des marchés, a toutes les chances de s'amplifier dans le futur avec les réglementations de plus en plus astreignantes (comme Bale Il et surtout Bâle III) auxquelles sont soumises les banques, puisque les papiers titrisés souscrits par des tiers au système sont pour les banques des dépôts leur procurant de la liquidité.

Il faut cependant se garder de généraliser le sens du mot «désintermédiation»: L'exclusivité bancaire s'est réduite mais les emprunteurs doivent aller sur d'autres marchés pour trouver des financements qui impliqueront des compétences, banquiers d'affaires ou autres arrangeurs et des moyens de communication techniques ou une Bourse où inscrire le papier émis en représentation de l'emprunt (par exemple obligataire).

Malgré sa définition, l'échange économique et financier apparemment désintermédié implique une intervention humaine et technique pour la rencontre des parties, même si la forme de la rencontre a évolué et si la rapidité des échanges et leur volume peuvent changer de dimension et concerner un nombre simplement illimité d'acteurs. La désintermédiation désigne en réalité la fin des monopoles monétaires et bancaires.

Au final, la politique de désintermédiation commencée en 1984 pendant l'ère Reagan aux États-Unis et en 1985 en Europe a abouti à ce que 75 % de l'économie des États-Unis soient financés hors système bancaire régulé et seulement 25 % en Europe. La différence tient notamment à l'absence en France du système des fonds de pension. Cette situation réduit la

portée de la régulation du système bancaire et accroît sans raison les risques d'effet pervers et de divergence.

Il s'agit donc aujourd'hui, avant de prendre le risque d'installer une régulation à portée inconnue, de regarder dans quelle mesure pourrait être mis en place un outil d'observation des agrégats financiers adapté à ce nouveau contexte, pour suivre l'évolution des masses monétaires en circulation.

Conclusion :

La monnaie est l'instrument d'échange qui permet l'achat immédiat de tous les biens, services et titres sans coûts de transactions ni coûts de recherche et qui conserve la valeur entre deux échanges.

Historiquement, plusieurs formes de la monnaie ont pu coexister ou se succéder. Elle est passée progressivement d'un support ayant une certaine valeur en soi (or, argent) à un objet sans valeur intrinsèque ou purement symbolique fixée par l'Etat, se présentant sous une forme de plus en plus dématérialisée.

La plupart des systèmes monétaires non métalliques ne s'appuyant pas sur un bien tangible, reposent sur la confiance, accordée par ses utilisateurs à la monnaie en tant qu'unité de compte et instrument de paiement, et, dans une moindre mesure, en tant qu'intermédiaire dans les échanges et réserve de valeur. Cette confiance s'appuie sur un principe de garantie incarné par une institution centralisée (États, banques centrales ou instances locales dans le cas des monnaies complémentaires locales).

Avec la généralisation de l'Internet, se sont développés de nombreux systèmes d'échanges décentralisés offrant la possibilité de s'émanciper de contraintes légales. Des échanges de films, de morceaux de musique on pu ainsi s'effectuer de manière privative, sans passer par un tiers, d'un ordinateur à l'autre (*peer to peer*).

La volonté de ces créateurs est de donner naissance à une monnaie échappant au contrôle des États et donc non soumise à la tentation de la « planche à billets », un mal selon eux à l'origine de crises telles que celle des subprimes. En d'autres termes, selon une vision libertaire, les adeptes des bitcoins voient, dans la fin du monopole des banques centrales sur l'offre de la monnaie et la « débancarisation », l'assurance que les citoyens se réapproprient leur devise. Et que cette dernière échappe à toutes les règles monétaires traditionnelles.

Chapitre II

La genèse de la crypto monnaie

Chapitre II : La genèse de la crypto monnaie

Introduction

Le monde de la finance est sur le point de changer drastiquement. Un nouvel arrivant vient de pénétrer ce gigantesque marché de plusieurs milliers de milliards de dollars et il entend s'imposer. Les monnaies du monde entier, et avec elle le reste du système financier ont été réglementées et gérées de façon centralisée depuis bien longtemps. Cependant, là où étaient attendues stabilité économique et prospérité, on a souvent vu naître des crises économiques, des krachs boursiers, voir même des guerres[1]. Le besoin d'un refuge capable de soutenir les futurs chocs économiques se fait clairement sentir.

La demande croissante de transaction à la fois plus rapide et plus sécurisée pourrait bien, à l'heure d'internet, trouver sa réponse dans les cryptomonnaies. Un large écosystème se développe autour de cette monnaie. Elle mobilise une population importante et active de startups et d'investisseurs. Elles perturbent potentiellement les banques et intermédiaires financiers traditionnels, à la fois soucieux d'en tirer les bénéfices technologiques et ne pas déstabiliser leur modèle de fonctionnement.

Le dynamisme des crypto-monnaies et l'engouement dont elles bénéficient résultent d'une triple évolution : un progrès technologique réel, un profond mouvement de société et, plus conjoncturellement, des conditions financières très accommodantes.

Dans ce deuxième chapitre, nous allons parler de la genèse de la crypromonnaie, de son évolution et de ses enjeux.

En effet, ce chapitre sera divisé en trois sections, dans la première section nous allons aborder l'histoire de la monnaie (préhistoire, naissance et évolution), dans la deuxième, la combinaison des techniques qui a permit l'existence d'une telle technologie innovatrice et dans la troisième ses enjeux et son avenir.

[1] Delahaye J.P., « Les preuves de travail » revue Pour la science, N°60, Avril 2014, consulté en ligne sur (www.pourlascience.fr) le 20/11/2021.

Section 01 : Histoire de la crypto monnaie

1. Préhistoire[2] :

L'origine de la blockchain date des années 1990, alors que différents groupes d'informaticiens s'efforçaient de comprendre et de perfectionner le potentiel des nouvelles technologies numériques et des avancées en cryptographie, et ce, afin de développer des outils qui permettraient de mieux protéger la vie privée des individus.

Le mouvement des *cypherpunks*, un groupe ayant pour ambition de démocratiser l'accès aux nouvelles technologies de chiffrement, y apporte une contribution importante. Avec l'invention de la cryptographie asymétrique (à double clé) et grâce au développement du système de chiffrement RSA en 1977 développé par trois chercheurs du MIT (Ronald Rivest, Adi Shamir et Leonard Adleman, dont les initiales sont à la base de l'acronyme), la cryptographie est progressivement devenue un outil accessible à toute personne désirant communiquer de façon sécurisée sur un réseau ouvert tel qu'internet. La cryptographie à double clé permet en effet de garantir non seulement la confidentialité, mais aussi l'authenticité et l'intégrité des communications en ligne. Les *cypherpunks* se sont ainsi approprié ces nouvelles technologies dans le but de préserver la vie privée et la liberté d'expression et même d'en promouvoir la défense, dans un environnement numérique qui commençait déjà à remettre en question un certain nombre de libertés fondamentales.

Dans un monde où toute activité laisse une trace toute trace permettant potentiellement de remonter à un individu, la vie privée des internautes se trouve toujours plus à la merci des grands opérateurs du réseau qui contrôlent les infrastructures de communication. Ces opérateurs peuvent de fait surveiller toutes les informations qui transitent sur leurs plateformes, et ils peuvent librement sauvegarder, analyser, ou même censurer ces informations. Il devient dès lors crucial de développer des outils permettant aux internautes de se protéger contre ce nouveau type de surveillance, et de leur redonner le pouvoir de décider quelles sont les informations les concernant qui peuvent être dévoilées aux autres acteurs du réseau. Il en va de même pour la liberté d'expression, il est délicat de s'exprimer librement dans un contexte où les communications sont gérées, et potentiellement censurées, par les opérateurs des grandes plates-formes sur internet. La cryptographie est donc un outil

[2]De Filippi P., « Blockchain et cryptomonnaies », Que sais-je ?, Paris, novembre 2012.

fondamental qui permet aux individus de communiquer de façon confidentielle, sans courir le risque d'être écoutés ou interceptés.

Cependant, dans un réseau connecté, les méthodes utilisées pour la protection de la vie privée ne peuvent être effectives qui si elles sont utilisées de manière collective. En effet, si un individu communique avec un autre individu qui n'emploie pas les mêmes techniques de protection, la communication pourra être potentiellement interceptée par des tiers. La confidentialité des communications n'existe alors que tous les internautes ont accès à ces mêmes outils de protection et les utilisent en continu. C'est pour cela que les *cypherpunks*, armés de leurs ordinateurs et de leurs logiciels, ont développé de nouveaux systèmes informatiques, accessibles à un plus grand nombre d'individus, pour faciliter une communication sécurisée et authentifiée.

Mais au sein du mouvement des *rypberpunks*, certains individus avaient des motivations qui s'étendaient bien au-delà de la protection des libertés fondamentales, animés non seulement par le désir de préserver la vie privée et la liberté d'expression des internautes, mais non moins fortement par le désir d'échapper au contrôle étatique, ainsi qu'au contrôle exercé par les grandes entreprises qui s'installaient sur le réseau. C'est le cas, notamment, des « crypto-anarchistes », qui s'inscrivent dans un courant de pensée beaucoup plus politisé, avec des tendances souvent anarcho-capitalistes. Ces individus revendiquent la suprématie du marché et recherchent une complète indépendance à l'égard de toute institution étatique ou gouvernementale. Les crypto-anarchistes refusent de se soumettre aux lois des Etats et n'obéissent qu'à leurs propres systèmes de règles, qui sont à fois définies et appliquées par le code informatique. Les idéologies sous jacentes à ce mouvement ont été analysées et décrites en détail par Timothy C. May, auteur du Manifeste de la crypto-anarchie, rédigé en 1989 mais toujours d'actualité, où il résume les problématiques soulevées par le développement de ces nouvelles technologies de communication décentralisée et de chiffrement :

« Tout comme la technologie de l'imprimerie a modifié et réduit le pouvoir des guildes médiévales et la structure du pouvoir social, les méthodes cryptologiques vont fondamentalement modifier la nature des sociétés et l'ingérence du gouvernement dans les transactions économiques. [...] Et juste comme une invention apparemment mineure comme le fil de fer barbelé rendu possible la clôture de vastes ranchs et de fermes changeant ainsi pour toujours les concepts de terre et de droits de propriété en Occident, la découverte

apparemment mineure d'une branche mystérieuse des mathématiques deviendra le coupe-file qui démantèlera les barbelés autour de la propriété intellectuelle »[3].

De façon générale, quelle que soit leur appartenance politique, les *cypherpunks* soutenaient un idéal de société plus libre et décentralisée, une société où la technologie permettrait aux internautes d'interagir et de communiquer librement sans être soumis à aucune forme d'intimidation ou de représailles éventuelles de la part des États ou d'autres institutions, publiques ou privées.

Toutefois, pour que cet idéal puisse se réaliser pleinement, il manquait un système de paiement anonyme et décentralisé qui permettrait de protéger la sphère privée financière des individus. En effet, qui dit protection des données personnelles dit aussi protection des informations relatives aux transactions financières, susceptibles de dévoiler des informations sensibles et privées sur les modes de vie de chacun.

Aussi bien pour les *cypherpunks* que pour les anarchistes, la désintermédiation des transactions finales cryptocières représentait l'un des fondements de l'établissement d'un nouvel idéal de société. Alors que les *cypberpunk* voyaient dans les intermédiaires financiers une menace à la vie privée, les crypto-anarchistes revendiquaient le besoin d'un système monétaire déconnecté de toute institution étatique, afin de permettre l'émergence d'une société de marché entièrement dérégulée.

Plusieurs initiatives ont eu lieu au cours de ces dernières années dans le but de créer des monnaies virtuelles, anonymes, et dont les transactions ne peuvent pas être tracées. L'un des premiers exemples était le projet Digi-Cash lancé en 1989 par David Chaum, un cryptographe dont les idées ont fortement influencé le mouvement cypherpunk. DigiCash était un système de paiement électronique pouvant s'intégrer au sein du système financier traditionnel et permettant aux individus de retirer des billets électroniques auprès de leur banque. Le système s'appuyait sur un système de « signature aveugle » (une primitive cryptographique inventée par Chaum lui-même). Ce système donnait la possibilité aux individus d'effectuer des transactions sécurisées de façon complète ment anonyme. Il mettait ainsi fin à la surveillance et au contrôle exercé par les banques et autres institutions financières. Pour ces opérations, DigiCash utilisait cependant un serveur centralisé géré par une entreprise privée. Ainsi, lorsque l'entreprise a fait faillite en 1998, le système a dû être interrompu.

[3] De Filippi P., conférence des hackers, 1988, 1989 et 1990.

Une autre initiative qui a fortement contribué au développement de Bitcoin est le projet Hashcash, proposé en 1997 par Adam Back et qui n'avait pourtant rien d'une cryptomonnaie. Hashcash utilisait la puissance de calcul des ordinateurs (autrement dit les ressources CPU) pour créer de la rareté dans le monde numérique. Tout individu désireux d'utiliser un service en ligne devait ainsi prouver avoir effectué une certaine quantité de « travail » par l'intermédiaire de son ordinateur afin de pouvoir accéder au service. Le but n'était donc pas de créer une monnaie virtuelle, mais plutôt de décourager certains comportements néfastes, tels que les courriels indésirables (*spam*) dénis de service (*denial of service*), en augmentant leurs coûts d'exécution. Malgré son adoption limitée à l'époque, ce modèle a inspiré plusieurs systèmes de paiement électronique fondés sur la preuve de travail (*proof of work*), dont Bitcoin est l'exemple le plus important.

Un projet qui mérite d'être mentionné à cet égard est celui de Wei Dai, un ingénieur informatique participant au mouvement *cypherpunk*, qui a publié en 1998 un article dans lequel il proposait de mettre en place un système de paiement électronique décentralisé et anonyme, opérant sur un réseau pair à pair. Ce système, qu'il avait nommé B-money, s'appuyait sur le même mécanisme de proof of work proposé par Hashcash, utilisé cette fois-ci dans le but de réguler l'émission d'une nouvelle monnaie virtuelle.

Dans cet article, Wei Dai expliquait que tout individu pouvant prouver qu'il a effectué une certaine quantité de « travail avec son ordinateur serait récompensé avec de la monnaie virtuelle. Pour transférer cette monnaie, il suffirait de communiquer la transaction aux autres membres du réseau pour mettre à jour les comptes des individus concernés. Ce système souffrait cependant d'une limite majeure. En effet, sans un moyen de communication synchrone qui ne puisse pas être brouillé, le système pouvait être manipulé par des individus malveillants qui tenteraient de dépenser plusieurs fois la même unité de monnaie virtuelle.

Bien que ce système de paiement n'ait jamais été développé, B-money est cependant considéré comme un il a d'ailleurs été cité comme référence dans l'article où précurseur de Bitcoin Satoshi Nakamoto décrit le protocole de Bitcoin.

La même année, Nick Szabo, un cryptographe appartenant lui aussi au mouvement *cypherpunk*, décrit un modèle alternatif de monnaie virtuelle qu'il appellera BitGold. Conçu en 1998, BitGold présentait déjà la plupart des briques techniques sur lesquelles Bitcoin s'est construit. Comme dans le cas de B-money, l'émission de BitGold est déterminée par la puissance de calcul dépensée pour résoudre une équation mathématique. Cependant, à la

différence de B-money, qui ne peut fonctionner que dans un réseau synchrone, BitGold intro duit un nouvel élément qui permet au réseau de fonctionner de façon asynchrone : la solution de chaque équation devient une partie intégrante de la prochaine équation à résoudre, produisant ainsi une série de transactions qui s'enchaînent les unes les autres de façon chronologique (un élément qui rappelle fortement le modèle de Bitcoin). Ce mécanisme permet d'horodater l'émission de nouvelle monnaie. Ainsi, les nœuds du réseau peuvent vérifier à tout moment la validité d'une transaction par rapport à son exécution dans le temps. Cela permet de résoudre le problème de la «double dépense » qui affecte la plupart des systèmes de paiements électroniques décentralisés. Cependant, le système tel qu'il avait été conçu par Nick Szabo était incapable de contrer les attaques dites Sybil (*Sybil attack,* en anglais), une attaques qui consistent à créer un grand nombre de fausses identités sur un réseau pair à pair, afin d'en détourner le fonctionnement. Malgré ces limitations, BitGold n'en est pas moins le précurseur le plus important de Bitcoin, ce qui a conduit Nick Szabo à être plusieurs fois soupçonné d'être le mystérieux Satoshi Nakamoto.

Ces idées ont contribué à alimenter les discussions des *cypherpunks*, qui voyaient dans ces systèmes informatiques une occasion de limiter, voire d'éliminer l'emprise des institutions financières sur la vie économique des citoyens. Et pourtant, en dépit du potentiel qu'ils présentent, aucun de ces systèmes de paiement électronique n'a jusqu'à présent été traduit dans un code informatique.

Le premier prototype fonctionnel de monnaie virtuelle a été développé en 2004 par Hal Finney, l'un des membres les plus éminents du mouvement *cypherpunk*. Ce système, bien qu'il dépende d'un serveur centralisé, est directement inspiré du fonctionnement de B-money et de BitGold. Il s'appuie sur des preuves de travail réutilisables (*reusable proofs of works*) afin de permettre à tout individu d'obtenir une unité de monnaie virtuelle en fournissant la preuve qu'il a effectué une certaine quantité de travail sur son ordinateur. Ce jeton (ou *token,* en anglais) est alors enregistré sur un serveur comme appartenant à cet individu. L'individu peut ensuite transférer son token à une autre personne en informant le serveur de cette transaction.

Ce système résolvait donc le problème de la double dépense en s'appuyant sur un serveur centralisé responsable de s'assurer que personne ne dépense plus d'argent qu'il n'en possède réellement. Il répondait aussi aux exigences des *cypherpunks* relatives à la protection de la vie privée. En effet, les membres du réseau ne pouvaient être identifiés que par l'intermédiaire de

leurs clés cryptographiques, lesquelles n'étaient associées à aucune identité spécifique (tout individu pouvait d'ailleurs détenir un nombre de clés indéfini). Cette solution, cependant, ne satisfaisait pas les critères d'autonomie ou d'indépendance souhaités par les crypto-anarchistes, qui jugeaient primordial de créer un système dont le fonctionnement ne s'appuierait sur aucune autorité de confiance. C'est précisément ce problème que Bitcoin souhaitait résoudre.

2. Première apparition[4] :

Bitcoin a été conçu en 2008 par un individu (ou un groupe d'individus) caché sous le pseudonyme de Satoshi Nakamoto. Le 31 octobre 2008, Nakamoto publiait un livre blanc intitulé Bitcoin: A Peer-to-Peer Electronic Cash System sur une liste de diffusion orientée crypto graphie (metzdowd.com). Le livre blanc décrivait un système de paiement décentralisé accompagné d'une monnaie virtuelle pouvant être échangée entre pairs, et ce, sans qu'il soit nécessaire de passer par aucune banque ni aucun intermédiaire financier. L'idée assez ambitieuse consistait à créer un système de paiement décentralisé capable de fonctionner indépendamment de toute autorité de confiance, et qui serait en mesure de répliquer, voire de remplacer, le rôle des institutions financières.

Quelques mois plus tard, les idées décrites au sein de ce livre blanc seraient traduites en un logiciel informatique à l'origine de la création du réseau Bitcoin. Le 3 janvier 2009, le logiciel est lancé et le premier bloc de la blockchain de Bitcoin est créé (le soi-disant Genesis block) générant ainsi les 50 premiers Bitcoins attribués à l'adresse de Nakamoto. Incorporé au sein de cette première transaction apparaissait le titre d'un article du journal The Times paru le même jour : « *Chancellor on Brink of Second Bailout for Banks* », un message révélant les motivations sous-jacentes à la création de Bitcoin, ainsi qu'une preuve concernant la date de lancement du réseau.

Bitcoin est tout d'abord un système de paiement pair à pair permettant le transfert de valeur sur Internet de façon sécurisée et complètement décentralisée. Pour son fonctionnement, Bitcoin utilise un réseau de communication pair à pair avec des mécanismes de stockage réparti qui lui permettent de fonctionner sans opérateur centralisé. Il emploie aussi des techniques cryptographiques qui, combinées les unes avec les autres, ont permis l'établissement d'un système extrêmement fiable et sécurisé qui n'a toujours pas été piraté

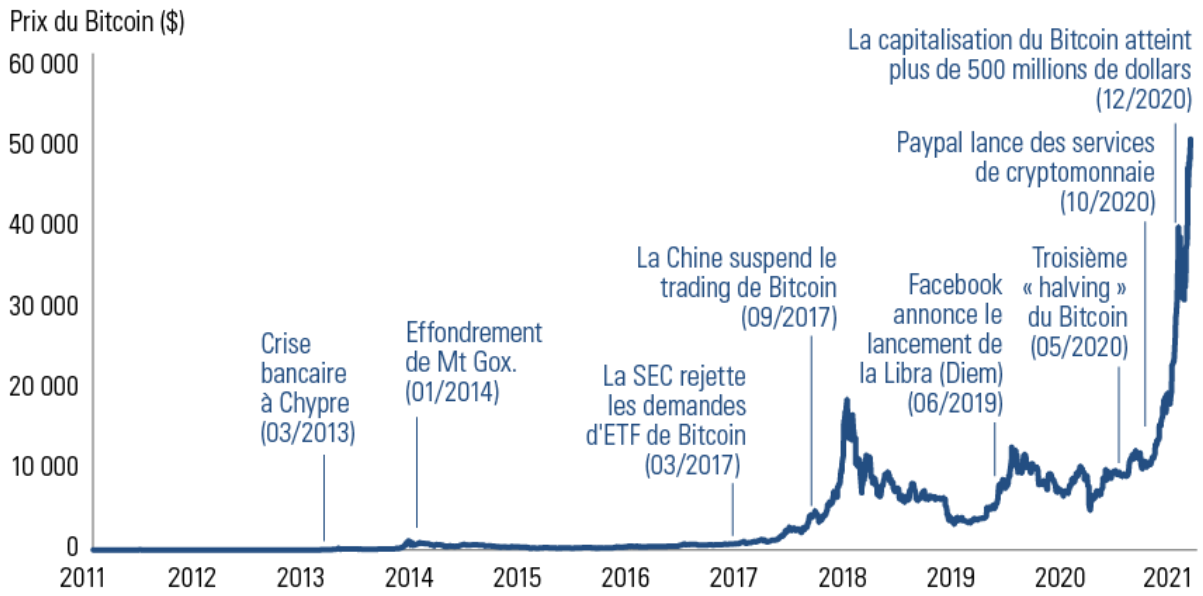
[4] De Filippi P., « Blockchain et cryptomonnaies », Op, cit.

depuis qu'il existe. Cela étant, même si Bitcoin est considéré par certains comme une innovation de rupture, une technologie sans précédent susceptible de dépasser les paradigmes établis, cette innovation s'appuie tout de même sur un certain nombre de technologies préexistantes, sans lesquelles Bitcoin n'aurait jamais vu le jour.

3. Evolution[5] :

Les crypto monnaies ont de nouveau suscité l'intérêt des investisseurs, avec de solides performances en 2020. Une spéculation accrue, les espoirs de pouvoir se couvrir contre les baisses des marchés actions et le risque inflationniste ainsi que le développement des actifs numériques sont autant de raisons pouvant expliquer les nouveaux sommets atteints par les cours des cryptomonnaies. Les risques demeurent toutefois élevés, et même si certains hedge funds peuvent trouver intéressant d'investir dans une forte volatilité, nous ne sommes pas convaincus par l'allocation aux monnaies numériques au sein d'un portefeuille stratégique.

Figure 01 : Evolution du cours de bitcoin..



Source : Bloomberg et GSAM. Au 17 février 2021.

La technologie qui sous-tend la plupart des cryptomonnaies est la Blockchain, mais cette dernière peut être utilisée pour d'autres applications. La base de données partagée et sécurisée

[5] Suivre l'évolution des cryptomonnaies (gsam.com), consulté le 14/11/2021

qui stocke l'information de manière efficace et vérifiable dispose du potentiel nécessaire pour être intégré dans divers secteurs. À l'image du développement des chemins de fer au 19e siècle, ou des entreprises du secteur de l'Internet à la fin du 2ème siècle, la technologie de la Blockchain est potentiellement révolutionnaire, mais le choix des gagnants au fil de l'évolution de la technologie peut s'avérer décevant.

- **La spéculation a été un puissant élément du prix :**

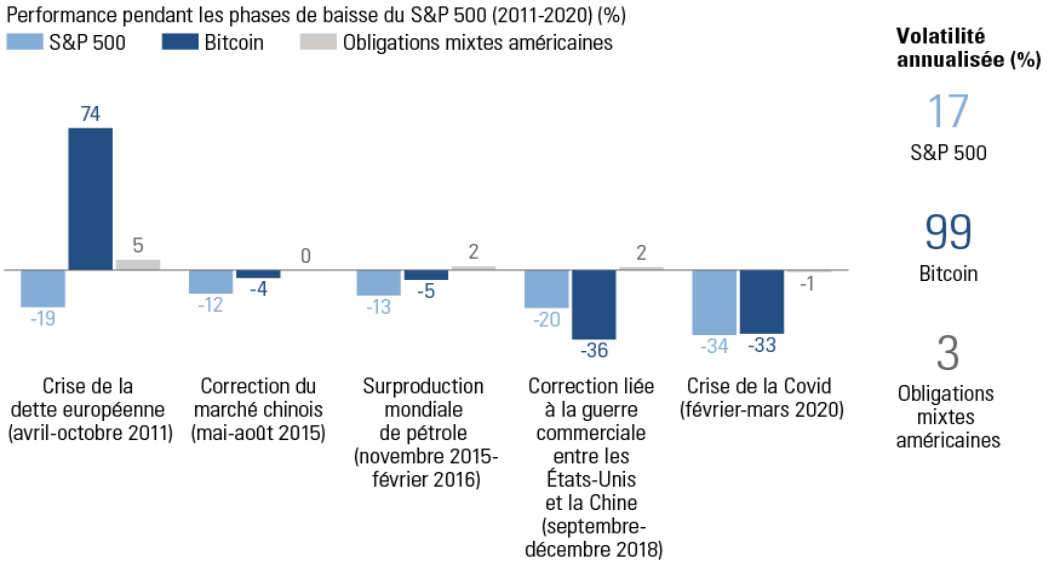
Le cours du Bitcoin ayant fait un bond, passant de 5 000 dollars en mars 2020 à 50 000 dollars en février 2021, l'activité sur le marché des cryptomonnaies a doublé. En outre, sur une année où la masse monétaire mondiale a augmenté de près de 20 %, la masse restreinte des cryptomonnaies a alimenté la spéculation d'autant plus.

L'émission de Bitcoin, par exemple, est limitée à 21 millions d'unités. Les Bitcoins nouvellement émis entrent dans le système grâce à un procédé appelé « minage », par lequel les « mineurs » vérifient les transactions de la Blockchain en résolvant des problèmes mathématiques complexes, appelés fonctions de hachage. Pourtant, le montant des Bitcoins récupérés en résolvant ces fonctions est divisé par deux tous les quatre ans, dans le but de ralentir le rythme de minage ou de circulation des Bitcoins.

- **Les acheteurs se sont tournés vers les cryptomonnaies comme outil de couverture éventuel :**

Les taux très bas et la politique monétaire accommodante ont poussé les investisseurs à trouver d'autres moyens pour gérer les risques baissiers de leurs portefeuilles. Certains ont vu dans les cryptomonnaies une alternative possible, considérant que leurs corrélations fluctuantes avec les classes d'actifs traditionnelles constituent une source de diversification efficace. Comme l'illustre le graphique 2, il existe toutefois peu d'éléments indiquant que les cryptomonnaies sont une source de diversification fiable au cours des corrections des marchés actions, notamment par rapport à l'indice *Bloomberg Barclays US Aggregate Bond*, dont la volatilité est bien plus faible.

Figure 02 : Performance et volatilité pendant les corrections DU S&P 500 (2011-2020) (%)



Source : Bloomberg et GSAM. Au 17 février 2021.

Lorsque l'indice S&P 500 a chuté de -19 % au cours de la crise de la dette européenne de 2011, le Bitcoin a fait un bond de 74 %. Mais lors de la correction liée à la guerre commerciale entre les États-Unis et la Chine (en 2018) et de la pandémie de COVID-19 (en 2020), le Bitcoin a connu des corrections similaires à celles des actions, voire plus importantes. En outre, la volatilité du Bitcoin a de loin surpassé celle des actions américaines, à respectivement 99 % contre 17 %. Pour un moyen censé réduire ou couvrir les baisses, le risque reste important. De plus, compte tenu de leur historique récent, aucun exemple ne montre comment les cryptomonnaies se comportent dans des environnements d'inflation ou de taux plus élevés. En outre, au cours des périodes où les performances du Bitcoin étaient les plus impressionnantes par rapport à celles des actions, la taille du marché du Bitcoin était insignifiante.

Section 02 : La crypto monnaie, une innovation fondée sur une combinaison de techniques préexistantes[6]

1. Une base de données décentralisée :

Pour enregistrer les transactions effectuées sur le réseau, Bitcoin s'appuie sur une base de données assez standardisée de type clé-valeur (key-value database). Ces bases de données sont organisées sous la forme d'un dictionnaire de clés auxquelles sont associées des valeurs.

Alors qu'il est possible de stocker tout type d'information dans le champ des valeurs, on ne peut y accéder que si l'on connaît la clé qui lui est associée. Étant donné la simplicité de ces systèmes, les bases de données de type clé-valeur sont généralement plus rapides que les autres bases de données de nature plus structurée, et peuvent gérer plusieurs millions de requêtes avec un temps de réponse très court. Base de données ne connaît pas la nature, ni la structure. Cependant, puisque la base des données stockées dans le champ de valeurs,

Elle est incapable de les traiter ou de les manipuler par elle-même. Tout traitement doit se faire par l'intermédiaire d'un système externe à la base de données.

La blockchain de Bitcoin se distingue des bases de données traditionnelles (gérées par des opérateurs centralisés), car elle est administrée de manière collective par l'ensemble des membres qui interagissent sur le système. Bitcoin s'appuie sur un protocole informatique qui va dicter les règles et les procédures à suivre afin de permettre l'enregistrement des transactions de manière sécurisée et décentralisée.

Tant que la plupart des participants respectent ces règles, aucune autorité de confiance n'est requise pour garantir la bonne exécution des transactions. Plus besoin d'un opérateur centralisé chargé d'autoriser les transactions, l'historique de toutes les transactions étant détenu en sa totalité, par tous les membres du réseau, qui participent tous à la validation et la vérification des transactions. Et c'est le fait qu'elles soient partagées en réseau qui les rend infalsifiables, car toute tentative de modifier ne serait-ce que l'une de ses transactions sera immédiatement détectée par les autres membres de réseau.

[6] De Filippi P., « Blockchain et cryptomonnaies », Op, cit.

2. Le chiffrement à double clé :

L'une des briques les plus importantes utilisées par Bitcoin pour assurer la sécurité du réseau est la cryptographie asymétrique à pour assurer double clé. Alors que les mécanismes de cryptographie symétrique impliquent que les individus qui communiquent entre eux se soient accordés sur une clé de chiffrement commune, la cryptographie asymétrique est une méthode qui permet à plusieurs individus de communiquer sur un réseau non sécurisé sans avoir besoin de transmettre une clé de chiffrement.

Chaque individu génère une paire de clés, une clé privée qu'il ne dévoile à personne, et une clé publique qu'il peut communiquer librement sur le réseau. Le système est sécurisé car, même s'il est toujours possible de générer une clé publique à partir d'une clé privée, il est cependant impossible de récupérer une clé privée à partir d'une clé publique. Ainsi, lorsqu'un individu désire communiquer de façon confidentielle avec un autre individu, il lui suffira de chiffrer le message avec la clé publique de ce même individu et d'envoyer le message chiffré sur le réseau. Même si le message est intercepté, seul le destinataire pourra accéder au contenu du message, puisque le message ne pourra être déchiffré qu'avec sa propre clé privée.

La cryptographie à double clé avait initialement été conçue pour assurer la confidentialité des communications dans un réseau non sécurisé, où il serait dangereux de transmettre une clé de chiffrement symétrique. Toutefois, ce mécanisme peut aussi être utilisé pour garantir la source ou l'authenticité des communications numériques. En chiffrant un message avec sa clé privée, un individu peut authentifier le message avant de le partager sur le réseau. Son contenu pourra ensuite être déchiffré par tous ceux qui ont accès à la clé publique de l'expéditeur.

Ce mécanisme permet d'obtenir deux résultats distincts. En premier lieu, il permet de vérifier message provient bien d'un individu donné. En second que le lieu, il rend la répudiation de ce message impossible, car le message ainsi chiffré ne peut avoir été constitué que par la personne qui détient la clé privée. Cette technique est utilisée aujourd'hui dans un grand nombre de systèmes de signature électronique.

Inventé en 1970 par un cryptographe britannique, James H. Ellis, le concept de chiffrement à double clé n'a été rendu public qu'en 1976, à la suite d'un article rédigé par Whitfield Diffie et Martin Hellman. Il a fallu attendre deux ans pour voir la première implémentation opérationnelle de ce concept, avec l'élaboration du système RSA. Bien que le

système RSA demeure aujourd'hui le système le plus communément utilisé, Bitcoin a opté pour un système alternatif (SECP256k1) qui permet d'obtenir le même niveau de sécurité avec des clés de tailles inférieures.

Dans le modèle de Bitcoin, le chiffrement à double clé a pour fonction de prouver que toute personne commençant une transaction est bien la propriétaire des fonds à transférer. Avant d'être communiquée au réseau, chaque transaction est signée avec la clé privée de l'émetteur. Les membres du réseau responsables de la vérification des transactions pourront alors contrôler que la transaction a bien été signée avec la clé privée associée à l'adresse qui émet cette transaction, et que cette adresse détient suffisamment de bitcoins pour assurer cette transaction. Si ces deux conditions sont remplies, la transaction sera validée avant d'être enregistrée au sein de la blockchain de Bitcoin.

3. Hachage et protocole de consensus distribué :

3.1. Les fonctions de Hashage :

Une fois validées, les transactions sont enregistrées, de façon chronologique, au sein d'un bloc de transactions, qui incorpore une référence aux blocs précédents. Cette référence, créée par le biais d'une fonction de hachage cryptographique (*hash function*, en anglais), joue un rôle fondamental pour garantir l'intégrité de toute la chaîne de transactions.

Une fonction de hachage est une fonction particulière qui prend une chaîne de caractères (ou un fichier numérique) comme paramètre d'entrée, et qui produit une nouvelle chaîne de caractères, de longueur prédéfinie, comme paramètre de sortie. Cette chaîne représente l'empreinte numérique (*digital fingerprint*) du fichier, elle permet de l'identifier de façon unique. Une particularité essentielle de toute fonction de hachage est qu'il est pratiquement impossible de générer la même empreinte numérique pour deux paramètres d'entrée différents (et le risque de « collision » peut être réduit rapidement en augmentant la longueur de la chaîne de caractères en sortie). Une autre caractéristique importante liée à la fonction de hachage est que toute modification apportée à un paramètre à l'entrée, si minime soit-elle, générera une chaîne de caractères complète ment différente à la sortie. Il est donc impossible de dériver ou de déduire des informations concernant un fichier à partir de sa seule empreinte numérique.

L'empreinte d'un fichier permet donc non seulement d'identifier des documents ou des fichiers numériques, mais aussi d'en vérifier l'intégrité. Bien qu'il soit impossible de

renverser la fonction de hachage pour récupérer le contenu d'un fichier à partir de son empreinte numérique (à moins de procéder à une attaque en force, en essayant toutes les possibilités), l'empreinte numérique peut tout de même être utilisée pour vérifier qu'un document correspond effectivement au fichier précédemment «haché ». Cela est très utile pour la transmission de fichiers sur un réseau non sécurisé, puisqu'il est possible de comparer les empreintes d'un fichier avant et après la transmission afin de s'assurer que la communication s'est bien déroulée et de vérifier que le fichier n'a pas été altéré entre-temps.

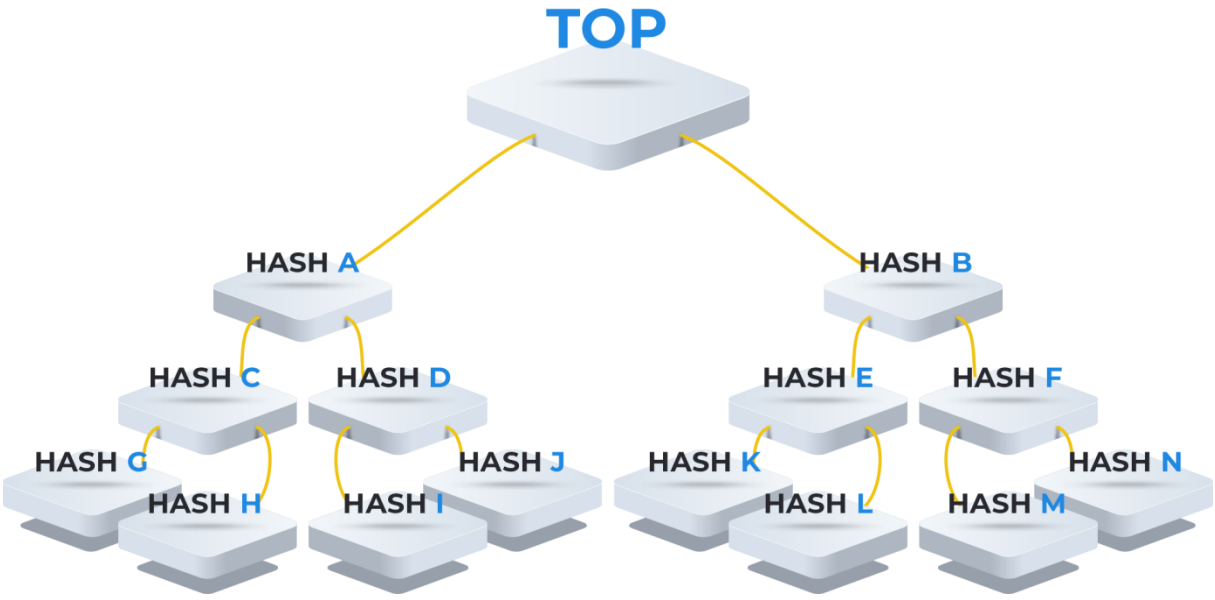
Au cours des dernières années, de nombreuses appli cations ont été rendues possibles grâce aux fonctions spécifiques du hachage cryptographique. Les arbres de hachage (plus connus sous le nom d'arbres de Merkle ou Merkle trees d'après son inventeur) sont une appli cation particulièrement intéressante de cette technologie, elle représente d'ailleurs l'une des briques fondamentales du protocole de Bitcoin. Inventée en 1979, cette technique utilise une fonction de hachage pour créer une structure de données en arborescence, où chaque nœud possède sa propre empreinte numérique, laquelle est générée à partir du « hash » des empreintes numériques de tous les nœuds qui en découlent. Ce mécanisme permet de vérifier de façon plus efficace l'intégrité de larges bases de données. Les arbres de Merkle sont aujourd'hui utilisés par un grand nombre de bases de données distribuées, afin de faci liter, voire d'optimiser la synchronisation des données. Ce même mécanisme permet aussi de faciliter la vérification des données échangées sur un réseau pair à pair non sécurisé, notamment lorsque, pour faciliter la transmission, les fichiers de grandes dimensions doivent être fragmentés en plusieurs pièces ou paquets avant d'être transmis sur le réseau. Grâce à un arbre de Merkle, les membres du réseau peuvent facilement reconstituer ces fichiers, et s'assurer que n'ont pas été modifiés ni altérés lors de la transmission. Ce mécanisme est utilisé notamment par BitTorent, un réseau de partage de fichier entre pairs qui fonetionne de manière complètement décentralisée.

Bitcoin utilise les arbres Merkle pour organiser les transactions au sein de chaque bloc de la chaîne, où chaque transaction peut être identifiée de façon unique grâce à son empreinte numérique. Cela permet de vérifier rapidement si une transaction a bien été enregistrée au sein d'un bloc, mais aussi de s'assurer qu'aucune transaction n'a été manipulée au cours du temps.

Chaque bloc de transactions sera, à son tour, « haché » : il en dérivera une empreinte numérique qui sera, elle, incorporée à l'intérieur du bloc suivant créant ainsi une longue chaîne de blocs qui se référencent les uns après les autres.

Cela permet de garantir l'intégrité du système dans son ensemble. Tous les blocs de transactions validés par le système forment une « chaîne » séquentielle de «blocs » qui contient la liste de toutes les transactions effectuées jusqu'à présent, organisées de manière chronologique. Étant donné les propriétés de la fonction de hachage, l'altération d'une seule de ces transactions entraînerait une modification de l'empreinte numérique (ou « hash ») du bloc de référence ce qui aura des répercussions tout au long de la chaine de blocs. Ainsi, plus longue est la chaîne de blocs, plus grande sera la sécurité du système, puisque toute altération d'une transaction invalidera la référence aux blocs précédents, ce qui brisera inévitablement la chaîne.

Figure 03 : Merkle Tress



Source : merkle-tree.png ((scrive.com), consulté le 21/11/2021

3.2. Le protocole de consensus distribué :

Alors que le processus de minage permet de garantir la sécurité et l'intégrité du réseau, le protocole de « consensus distribué » (*distributed consensus*, en anglais) adopté par Bitcoin permet de s'assurer qu'à tout moment les membres du réseau peuvent se mettre d'accord sur un état donné de la blockchain.

En effet, le réseau étant décentralisé, les transactions peuvent être reçues (et traitées) dans un ordre différent par les différents nœuds du réseau. Si plusieurs blocs de transactions sont validés en même temps par différents mineurs [7], il sera impossible de déterminer

[7] Mineurs : des utilisateurs de la blockchain dont le rôle est de valider les transactions.

objectivement lequel de ces blocs devrait avoir la priorité sur les autres. Cela est d'autant plus critique lorsqu'il existe un conflit potentiel entre les transactions incorporées au sein de ces blocs. Par exemple, un individu avec un solde de 3 Bitcoins pourrait tenter d'effectuer deux transactions de 2 Bitcoins chacune. Ces deux transactions pourraient paraître valides si chaque opération est considérée individuellement. Pourtant, les deux transactions sont mutuellement incompatibles, car leur somme dépasse le solde existant de trois Bitcoins. Il s'agit là d'un problème plus couramment connu sous le nom de la « double dépense ».

Pour résoudre ce problème, Bitcoin a mis en place un protocole de consensus distribué qui permet au réseau de trancher, et de déterminer, en cas de conflit, quel sera le bloc de transactions qui aura la priorité sur les autres. Ce protocole prévoit que les membres du réseau devront toujours sélectionner la chaîne de blocs la plus longue (celle qui a demandé une plus grande puissance de calcul, et donc de « preuve de travail »).

Ainsi, lorsque deux blocs sont attachés simultané ment à la même chaîne, une bifurcation se crée au sein de la blockchain. Étant donné que les deux bifurcations sont de la même longueur, il sera difficile pour le réseau de déterminer lequel de ces deux blocs prévaudra sur l'autre. Ce sera donc aux mineurs de décider, au moment de la création d'un nouveau bloc, lequel de ces deux blocs sera privilégié. Le conflit est résolu dès lors qu'un nouveau bloc de transactions est validé par le réseau et que l'une des deux bifurcations devient ainsi la chaîne la plus longue. Certes, rien n'empêche certains mineurs de continuer à référencer l'autre chaîne, mais cela risquerait de leur coûter cher (en énergie), puisque les blocs appartenant à la chaîne la plus courte seront tout simplement ignorés par la majorité du réseau, y compris les Bitcoins émis lors de la création de ces blocs.

Dans une perspective économique, les mineurs ont donc intérêt à respecter le protocole et à ne référencer que les blocs appartenant à la chaîne la plus longue.

L'avantage de fonder le protocole de consensus distribué sur la quantité de « travail » investi dans le processus de minage réside dans le fait que toute tentative de manipulation du réseau deviendrait extrêmement coûteuse. La modification d'une transaction enregistrée au sein d'un bloc de la chaîne obligerait en effet l'attaquant à résoudre une nouvelle fois l'équation associée à ce bloc (dont l'empreinte numérique aurait nécessairement changé), et à résoudre aussi toutes les équations associées aux blocs suivants. Puisque les membres du réseau ne considèrent que la chaîne la plus longue comme valide, il sera pratiquement impossible pour l'attaquant de « récupérer le retard ». En effet, seul un mineur (ou un groupe

de mineurs) contrôlant plus de 50 % de la puissance de calcul investie dans le réseau sera capable de créer des blocs plus rapidement que le reste du réseau, c'est ce qu'on appelle une attaque à 51 %. C'est grâce à ce système que Bitcoin a résolu le problème de la double dépense, ainsi que le problème des attaques de type Sibylles qui affectent beaucoup de systèmes de paiement décentralisés.

Section 03 : les enjeux et l'avenir de la crypto monnaie

1. Les avantages de la crypto monnaie[8] :

Presque tout le monde connaît aujourd'hui la technologie des crypto-devises et des chaînes de blocs, alors il est impératif de savoir comment ces deux entités vont changer le monde qui nous entoure, pour le mieux. Il est important de connaître certains des avantages d'utiliser ces crypto-monnaies.

1.1. Sécurité et protection contre la fraude : Les crypto-monnaies de particuliers sont numériques et ne peuvent être contrefaites ou annulées arbitrairement par l'expéditeur, comme c'est le cas avec les impayés de cartes de crédit.

1.2. Règlement immédiat : L'achat de biens immobiliers implique généralement des tiers (avocats, notaires), des retards et le paiement des frais. À de nombreux égards, la blockchain est comme une «grande base de données de droits de propriété», Les contrats peuvent être conçus et appliqués pour éliminer ou ajouter des approbations de tiers, des faits externes de référence, ou être complétés à une date ou une heure future pour une fraction des dépenses et du temps requis pour effectuer des transferts d'actifs traditionnels.

1.3. Frais plus bas : Il n'y a généralement pas de frais de transaction pour les échanges de cryptomonnaie parce que les mineurs sont compensés par le réseau. Même sans frais de transaction, beaucoup s'attendent à ce que la plupart des utilisateurs engagent un service tiers pour créer et maintenir leurs portefeuilles de devises numériques. Ces services agissent comme Paypal pour les utilisateurs de cartes de crédit ou de caisse,

[8] Les avantages d'utiliser la crypto-monnaie | CryptoKemet, (www.cryptokemet.com) consulté le 25/11/2021

fournissant le système d'échange en ligne, et à ce titre, ils sont susceptibles de facturer des frais. Il est intéressant de noter que Paypal n'accepte ni ne transfère de bitcoins.

1.4. Protection contre le vol d'identité : Lorsque vous donnez votre carte de crédit à un commerçant, vous lui donnez accès à votre ligne de crédit complète, même si la transaction est pour une petite quantité. Les cartes de crédit fonctionnent sur une base «pull», où le magasin initie le paiement et tire le montant désigné de votre compte. Cryptomonnaie utilise un mécanisme «push» qui permet au détenteur de cryptomonnaie d'envoyer exactement ce qu'il veut au marchand ou au destinataire sans autre information.

1.5. Accès pour tout le monde : Il y a environ 2,5 milliards de personnes ayant accès à Internet ou à des téléphones mobiles et smartphones qui n'ont pas actuellement accès aux échanges traditionnels, ces personnes sont prêtes pour le marché de la cryptomonnaie. Le système M-PESA du Kenya, un service de transfert d'argent basé sur le téléphone portable, et le service de microfinancement ont récemment annoncé un dispositif bitcoin, avec maintenant un Kenyan sur trois possédant un portefeuille bitcoin.

1.6. Décentralisation : Un réseau mondial d'ordinateurs utilise la technologie blockchain pour gérer conjointement la base de données qui enregistre les transactions en Bitcoin. C'est-à-dire que le Bitcoin est géré par son réseau et non par une autorité centrale. La décentralisation signifie que le réseau fonctionne d'utilisateur à utilisateur (ou d'égal à égal). Les formes de collaboration de masse que cela rend possibles commencent tout juste à être étudiées.

1.7. Suivi des paiements : Les systèmes bancaires traditionnels exigent que les expéditeurs ou les destinataires suivent leurs paiements via des systèmes bancaires sur des périodes de trois jours ou plus. Cela crée une incertitude pour l'expéditeur et le destinataire des fonds. Avec les crypto-monnaies, les transactions peuvent être suivies à la seconde et l'heure exacte de la livraison du paiement peut être collectée avec plus de certitude. Cela crée une sécurité pour l'expéditeur et le destinataire

1.8. Confidentialité : Alors que les banques exigent la connaissance complète de toutes vos informations personnelles et de celles du bénéficiaire de votre paiement, la cryptomonnaie n'exige pas plus d'informations que vous ne souhaitez en fournir. Votre paiement est entre vous et votre bénéficiaire. Pour les personnes qui ont besoin de confidentialité et d'anonymat, c'est l'un des plus grands avantages de la cryptomonnaie.

1.9. Reconnaissance au niveau universel : Puisque la cryptomonnaie n'est pas liée par les taux de change, les taux d'intérêt, les frais de transaction ou autres frais de tout pays; par conséquent, elle peut être utilisée au niveau international sans rencontrer de problèmes. Ceci, à son tour, fait gagner beaucoup de temps et d'argent de la part de toute entreprise qui dépense pour transférer de l'argent d'un pays à l'autre. La cryptomonnaie fonctionne au niveau universel et rend donc les transactions assez faciles.

Il n'existe aucun autre système de paiement électronique dans lequel votre compte n'appartient pas à quelqu'un d'autre. Par exemple PayPal : si l'entreprise décide pour une raison quelconque qu'un compte a été mal utilisé, elle a le pouvoir de geler tous les actifs détenus dans le compte. Avec la cryptomonnaie le client possède la clé privée et la clé publique correspondante qui constitue l'adresse de sa cryptomonnaie.

Il est clair que la cryptomonnaie apporte un certain nombre d'avantages nouveaux et passionnants par rapport au système fiduciaire actuel. Alors que cette technologie en est encore à ses balbutiements, il est extrêmement excitant de penser à un système révolutionnaire dans lequel une cryptomonnaie est la principale forme de devise. Un nouveau système plus simple pour tous pourrait répandre la richesse dans le monde entier, faciliter le commerce et préserver les richesses.

2. Les limites de la crypto monnaie[9] :

En dépit de tous ses avantages, la crypto monnaie, comme toute technologie, présente certaines failles. Selon les spécialistes, le principal talon d'Achille de la crypto monnaie réside

[9] Quels sont les principes et les enjeux de la crypto monnaie ? (lamineauxinfos.fr), consulté le 22/11/2021

dans sa volatilité élevée. En effet, la valeur des crypto monnaies est très instable. Aussi, étant une monnaie virtuelle, elle présente des risques élevés de piratage.

Les crypto monnaie peuvent également être utilisées à des fins criminelles en raison de leur confidentialité relativement élevée. Malgré ses limites, la monnaie électronique incarne un énorme potentiel économique pour l'avenir.

3. L'avenir de la crypto monnaie[10] :

Pour l'instant, la crypto monnaie est un écosystème déconnecté et indépendant, bien qu'elle tende à connecter ses veines avec l'économie réelle. Les agents économiques en sont au stade néophyte, commençant à décortiquer le sujet sans en connaitre les véritables intérêts. Il faut surtout se tourner vers ceux qui sont déjà dans son univers pour comprendre quels sont les véritables enjeux des crypto monnaies. Pour les banques centrales par exemple, il s'agit d'un moyen efficace pour baisser le coût de l'émission de billets. En effet, la fabrication d'un dollar américain coûte 0,05 centimes, or une crypto monnaie émis par la banque centrale coûterait 0 centime. Pour les Européens, c'est une solution pour s'affranchir du dollar américain, le dollar qui, depuis la fin de la deuxième guerre mondiale était au centre des rouages économiques internationaux.

Les investisseurs tels que les exportateurs et les importateurs verront en la crypto monnaie, un moyen alternatif pour s'affranchir du dollar. Même les îles Marshall, qui utilisent le dollar au quotidien veulent créer une crypto monnaie locale pour abandonner le dollar. Pour les simples utilisateurs, c'est un moyen d'échapper aux contrôles de l'utilisation des fonds (par exemple sur bitcoin) car ils n'auront pas besoin de compte, ni d'authentification de leur identité pour utiliser leurs actifs, mais seulement d'une clé. C'est pourquoi on associera parfois la crypto monnaie avec le blanchiment d'argent, le trafic d'armes, tel le cas de la cryptomonnaie anonyme Darkcoin.

Quoi qu'il en soit, l'évolution de la crypto monnaie ne peut être plus freinée. Elle existe et grandira toujours. Actuellement, à part les plus connues, comme Bitcoin ou Ripple, on en dénombre plus de 500 crypto monnaies dans le monde. Si l'euro, le dollar et le yen sont liés

[10] Comprendre la crypto monnaie et ses enjeux sur l'économie réelle (crypto-monnaies.xyz), consulté le 22/11/2021

aux territoires géographiques, les crypto monnaies ne posent pas de frontières. Seules les lois et l'évolution des usages des consommateurs qui détermineront son avenir. Il faut d'abord faire entrer le sujet dans les mœurs, établir la confiance, vulgariser l'usage pour que la crypto monnaie fasse partie de la vie de tous les jours.

Conclusion

Au cours de l'année écoulée, certaines entreprises ont commencé à accepter les cryptomonnaies comme moyens de paiement, et de plus en plus de sociétés de services financiers ont mis au point des plates-formes permettant aux utilisateurs d'acheter, de vendre et de transférer des cryptomonnaies.

En outre, les banques centrales du monde ont commencé à se pencher sur les monnaies numériques de banque centrale (MNBC), une version numérique des monnaies traditionnelles. Les adeptes considèrent que les MNBC sont un moyen de répondre au déclin de l'utilisation de l'argent liquide dans la société actuelle, et d'améliorer la transmission de la politique monétaire. Les détracteurs se méfient des attaques informatiques, des contrefaçons et des fraudes potentielles. En particulier, les monnaies numériques de banque centrale peuvent surtout diminuer la valeur ou accroître les risques des monnaies numériques existantes[11].

Il est fort probable que ces moteurs de marchés des cryptomonnaies persisteront vraisemblablement dans les prochaines années, mais cela ne justifie pas forcément l'investissement dans les cryptomonnaies comme actifs à part entière. Les infrastructures sont encore récentes et exposées à divers risques, au-delà des inquiétudes liées à leur adoption, notamment à des risques légaux et réglementaires.

Selon les économistes, les cryptomonnaies coexisteront probablement avec la monnaie liquide, bien installée, émise et contrôlée par les États, mais ne la remplaceront pas. À long terme, ce pourrait être le concept sous-jacent et la technologie de la Blockchain qui se révèleront révolutionnaires.

[11] Suivre l'évolution des cryptomonnaies (gsam.com), consulté le 5/11/2021

Chapitre III

Le registre des transactions « Blockchain »

Chapitre III : Le registre des transactions en crypto monnaies « Blockchain ».

Introduction

La blockchain est assimilée à une révolution équivalente à celle de l'invention d'internet. Si les crypto monnaies nous permettent d'échanger d'une façon décentralisée et parfaitement sécurisée, les nouvelles applications fondées sur la blockchain nous offrent des possibilités beaucoup plus larges.

Certaines de ces informations nous permettent de certifier et d'authentifier des documents sans que soit requise la présence d'un notaire, d'autres applications nous permettent d'automatiser des transactions, de créer de nouvelles formes d'organisation ou même de nous coordonner sans recourir à aucune autorité de confiance et marque le passage d'un système basé sur la confiance vers un système basé sur la preuve

Dans ce chapitre, nous définissons, dans la première section, la monnaie et son évolution à travers l'histoire, ensuite, dans la deuxième section nous verrons que la monnaie est devenue un produit très complexe et qu'avec l'évolution économique et technologique qui ont transformé les transactions vers des transactions complètement dématérialisées, le temps est devenu d'une importance très considérable en matière monétaire, et dans la troisième et dernière section, nous allons nous pencher sur la mutation des mécanismes de la création monétaire, d'une création contrôlée par l'état et la banque centrale vers une création désintermédiée.

Section 01 : Qu'est ce que la Blockchain[1] ?

1. Définition de la Blockchain :

Au plus fort de la crise économique qui toucha le monde en 2008, une nouvelle façon de concevoir la monnaie a été proposée au sein d'un article posté sur internet et intitulé « Bitcoin : A Peer-to-Peer Electronic Cash System ». Dans cet article, un certain Satoshi

[1] Dumas J.G., Lafourcade P., Tichit A., Varrette S., « Les blockchains en 50 questions », édition Dunod, Paris, 2018

Nakamoto décrivait un nouveau système d'émission et de gestion d'unités monétaires, appelé bitcoin, qui reposait sur une structure de données de type DLT et appelée blockchain[2].

En effet, blockchain est un anglicisme composé de deux mots distincts mis bout à bout. Il s'agit de *block* (bloc en français) et de *chain* (chaîne en français). La blockchain représente donc une chaîne de blocs au sein de laquelle les blocs représentent des données numériques et la chaîne une sorte de base de données publique. De manière technique, on dira que la blockchain est un système sécurisé permettant le stockage et la diffusion d'informations sur un réseau public non centralisé[3].

Dans son rapport publié en décembre 2018, la mission d'information commune de l'assemblée nationale sur les usages des chaînes de blocs et autres technologies de certification de registre définit la blockchain comme étant « Un registre, une grande base de données qui a la particularité d'être partagée simultanément avec tous ses utilisateurs, tous également détenteurs de ce registre, et qui ont également tous la capacité d'y inscrire des données, selon des règles spécifiques fixées par un protocole informatique très bien sécurisé grâce à la cryptographie ».

Et selon ce même rapport, l'une des particularités de ce registre est d'enregistrer les données sur des blocs qui contiennent une quantité limitée d'informations. Un bloc validé ne peut plus être modifié, sauf par consensus des détenteurs du registre. Les transactions ou les informations échangées entre les utilisateurs du réseau sont donc regroupées par blocs horodatés et irréversiblement liés les uns aux autres, formant une chaîne. Les écritures enregistrées sur ce bloc et sur tous les précédents sont inaltérables et infalsifiables.

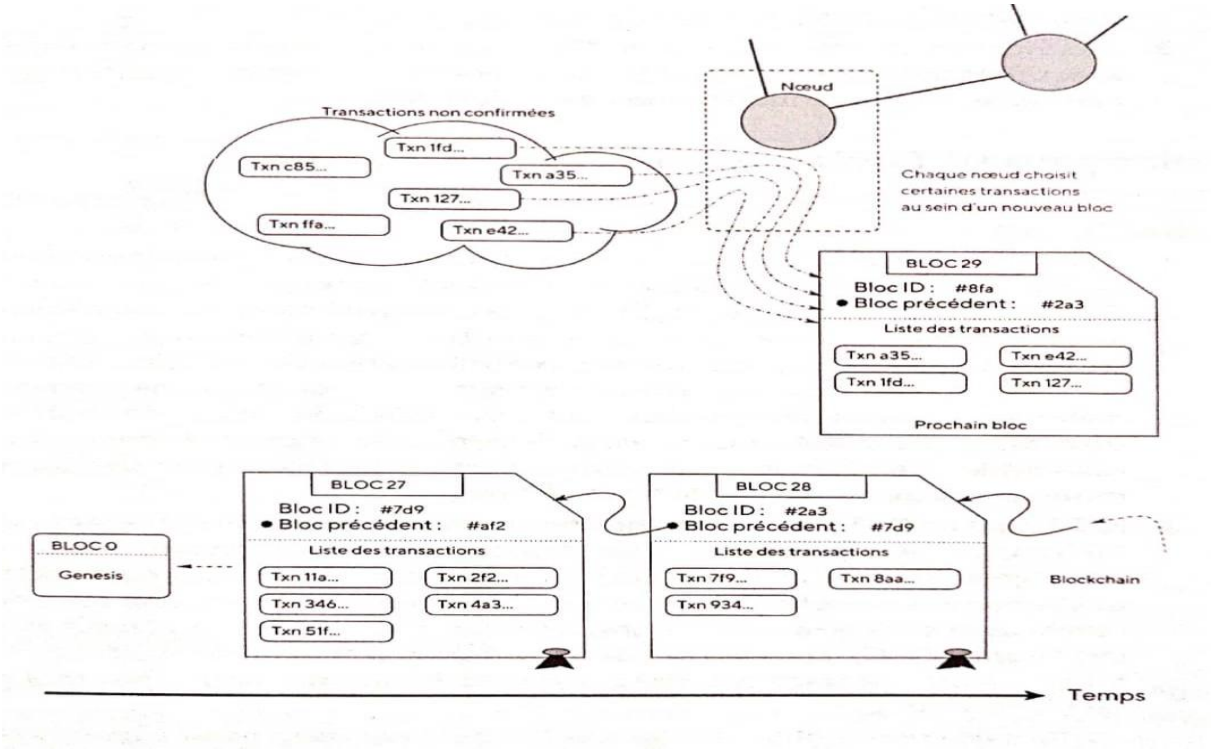
2. Fonctionnement de la blockchain[4] :

Par analogie avec les registres classiques dans lesquels les transactions sont regroupées sur des pages, les transactions sont ici agrégées au sein de blocs digitaux chaînés entre eux. Dans cette structure de données, les transactions confirmées (ou validées) sont intégrées dans des blocs bénéficiant d'un identifiant « unique » dépendant de son contenu, une signature qui

[2] Dumas J.G., Lafourcade P., Tichit A., Varrette S., « Les blockchains en 50 questions », Op.cit.
[3]/ www.astuces-aide-informatique.info, consulté le 02/11/2021.
[4] Dumas J.G., Lafourcade P., Tichit A., Varrette S., « Les blockchains en 50 questions », Op.cit.

est obtenue par une empreinte de hachage[5]. Chaque bloc contient la signature du bloc précédent de la chaine, ce qui permet de garantir l'intégrité de l'ensemble des enregistrements et des données de la blockchain depuis le premier bloc appelé bloc « Genesis ».

Figure 04 : Fonctionnement de la blockchain.



Source : J.G. Dumas, P. Lafourcade, A. Tichit, S. Varrette, « Les blockchains en 50 questions », édition Dunod, Paris, 2018

Ce schéma est un schéma illustrant le fonctionnement de la blockchain, on remarque que lorsqu'une nouvelle transaction est émise pour être validée, elle est propagée parmi les participants pour entrer dans un ensemble de transactions non confirmées. Celles-ci seront choisies pour intégrer un nouveau bloc construit par un mineur[6]. Les mineurs valideront ces transactions selon des techniques dépendant du type de blockchain, par exemple, dans la blockchain utilisée au sein du bitcoin, cette technique est appelée la preuve de travail ou *Proof-of-Work* (PoW).

[5] Hachage : Une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte numérique servant à identifier rapidement la donnée initiale.

[6] Un mineur : C'est un individu vérifiant les transactions et opérations effectuées par les utilisateurs sur le réseau.

Chaque bloc ne contient pas forcément un nombre fixe de transactions. Une fois validé, un bloc est horodaté et ajouté à la blockchain. Cet horodatage n'est pas forcément nécessaire, car l'ordre des blocs n'est pas nécessairement chronologique, mais reste pratique. La valeur proposée est alors celle de l'horloge locale. Au moment de la vérification du bloc, il est suffisant de s'assurer que la valeur du *timestamp* reste cohérente avec les autres temps de la blockchain.

Il existe plusieurs modèles de déploiement de ce type de structure Mais c'est une implémentation distribuée au-dessus d'un réseau Peer-to-Peer (P2P) comme celle proposée dans l'article fondateur de bitcoin qui permet d'obtenir un DLT tel que défini précédemment.

Ainsi, chaque nœud du réseau possède et maintient une copie cohérente et identique de la blockchain.

Il convient alors de définir les mécanismes décentralises permettant de :

- Distribuer de nouveaux blocs a tous les nœuds impliques ;
- Valider les transactions et plus généralement les blocs;
- Assurer la cohérence éventuelle de toutes les copies de la blockchain.

Ces mécanismes sont explicités par la suite et dépendent évidemment du système considéré. Mais en les supposant en place, une blockchain constitue alors une base de données publique, distribuée, c'est-à-dire partagée par ses différents utilisateurs, sans autorité centrale, fiable et inviolable. Ainsi elle peut être assimilée à un grand livre des comptes, public, infalsifiable et vérifiable.

La blockchain est infalsifiable, toute modification d'un bloc de transactions dans la chaine rend celle-ci incohérente. En effet, tout bloc est référencé dans le bloc suivant de la chaine, lui même référencé dans le bloc suivant de la chaîne, etc. Cette référence est entièrement déterminée par le contenu du bloc et totalement différente pour chaque variation, même infime, ceci est assuré par l'usage d'une empreinte de hachage cryptographique de ce bloc.

Pour altérer une partie de la chaîne il faudrait donc être capable d'altérer la totalité des blocs à partir de la modification, et cela tellement rapidement que l'ensemble du réseau mondial (qui scrute, vérifie et augmente la chaine constamment) ne puisse s'en apercevoir.

3. Les types de la blockchain :

Il existe deux types de la blockchain :

- **Les blockchains publiques :**

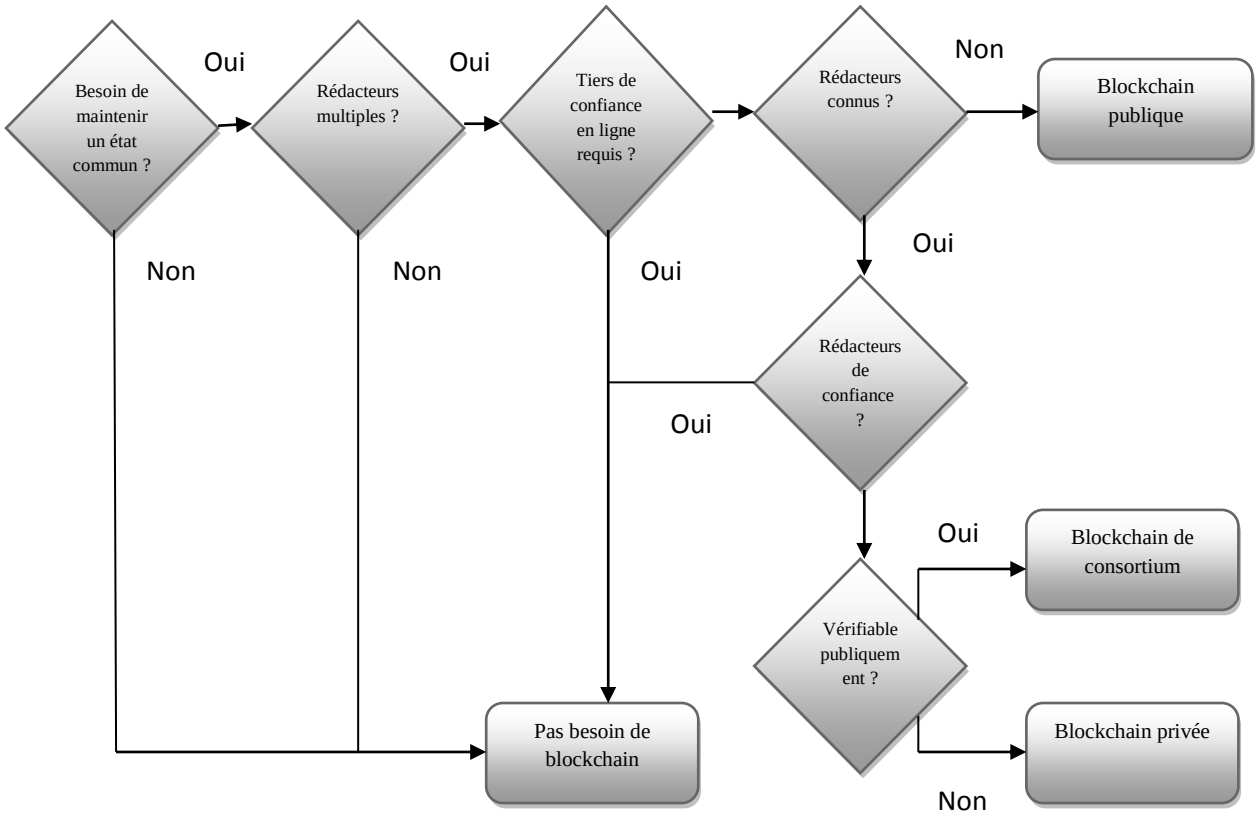
Les blockchains publiques sont par définition ouvertes et accessibles à tous. En particulier, tout le monde peut participer aux transactions (et ainsi espérer les voir incluses dans la blockchain sous réserve de validité), mais aussi collaborer aux opérations de consensus de la blockchain permettant de déterminer quel bloc peut être ajouté à la chaîne et à l'état courant, et cela sans besoin d'une autorisation particulière de la part d'une autorité de contrôle (éventuellement distribuée). En particulier, une blockchain publique peut être assimilée à un grand livre comptable public et infalsifiable.

Enfin, de telles blockchains sont souvent *permissionless:* les nœuds comme les utilisateurs n'ont pas besoin d'autorisation ni d'être authentifiés.

- **Les blochchains privées et de consortium :**

L'autre grand type de blockchains est celui des blockchains privées dont l'accès et l'utilisation sont limités à un certain nombre d'acteurs qui, par ailleurs, ne se font pas nécessairement entièrement confiance. Ici, il convient de dissocier les blockchains complètement privées, dans lesquelles les droits d'écriture sont restreints et centralisés au sein d'une seule institution, des blockchains de consortium où le processus de consensus est contrôlé par un sous-ensemble de nœuds et de participants présélectionnés (selon une approche centralisée ou non) et disposant ainsi d'un rôle privilégié pour la gestion de la blockchain. Dans les deux cas, l'accès en lecture de la blockchain peut être entièrement public ou restreint, que ce soit au niveau des participants ayant été autorisés ou du nombre de requêtes effectué. Éventuellement, certains systèmes permettent de limiter l'accès aux preuves cryptographiques à seulement une partie de la blockchain. Enfin et de façon générale, une blockchain privée est dite *permissioned*, si les nœuds du réseau, tout comme les utilisateurs, sont authentifiés et autorisés selon des critères prédéfinis, comme sur le schéma suivant.

Figure 05 : Comment choisir un type de la blockchain.



Source : J.G. Dumas, P. Lafourcade, A. Tichit, S. Varrette, « Les blockchains en 50 questions », édition Dunod, Paris, 2018

Section 02 : La relation entre la Blockchain et les crypto monnaies

1. Chaîne des transactions en cryptomonnaies :

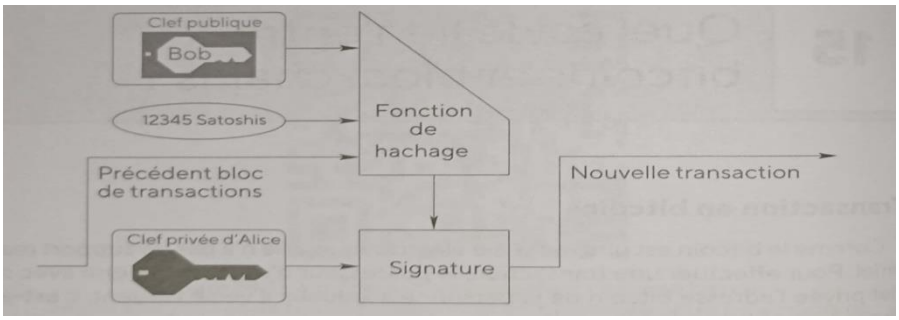
Prenant l'exemple le plus pertinent qui est le bitcoin, Comme le bitcoin est une monnaie électronique, elle n'a pas de support matériel. Pour effectuer une transaction, le possesseur d'un bitcoin signe avec sa clef privée l'adresse bitcoin de la personne à laquelle il verse l'argent c'est-à dire sa clef publique

Ensuite, afin de prouver qu'il possède bien la somme en bitcoins qui est l'objet de la transaction le propriétaire associe dans les données signées l'ensemble des transactions existantes depuis la création du bitcoin Tel quel cela représenterait beaucoup trop de données, c'est pourquoi ces données sont structurées dans une blockchain, dans laquelle les transactions

sont regroupées par blocs. Ces blocs sont eux-mêmes liés par une chaine de hachage arborescente de Merkle (des hachages de blocs simples de la chaîne de blocs).

Pour mieux expliquer la façon dont une transaction est créée, il est nécessaire de donner un exemple :

Figure 06 : Transaction de 12 345 satoshis entre Alice et Bob.



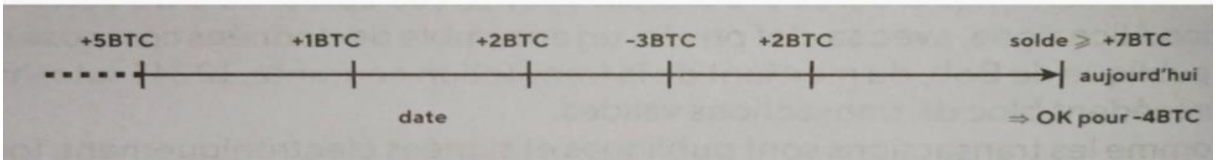
Source : J.G. Dumas, P. Lafourcade, A. Tichit, S. Varrette, « Les blockchains en 50 questions », édition Dunod, Paris, 2018

Par exemple, sur cette figure, Alice paie à Bob la somme de 12 345 satoshis soit environ 12 centimes d'euros si 1 bitcoin vaut 10 000 euros, lors de cette transaction Alice signe avec sa clef privée, un ensemble de données compose de la clef publique de Bob, du montant de la transaction courante, 12 345 satoshis, et du précédent bloc de transactions valides comme les transactions sont publiques et signées électroniquement, tout le monde peut vérifier le bien fondé d'une transaction en vérifiant les signatures à l'aide des clefs publiques précédentes, et ainsi remonter la chaine des transactions.

La propriété fondamentale des bitcoins est qu'aucun découvert n'est autorisé : le montant en bitcoins associé à une adresse bitcoin est toujours positif. Si, par exemple, Alice veut dépenser quatre bitcoins, comme sur la figure 15 2 alors un bitcoin ne pouvant être dépensé avant d'avoir été gagné, les auditeurs vinifieront qu'Alice possède un solde positif d'au moins quatre bitcoins. Comme à chaque instant, tout crédit en bitcoin est positif, la transaction sera validée car l'historique, public, de toutes les transactions d'Alice montre que ses cinq dernières transactions sont quatre gains respectivement de 5, 1, 2 et 2 bitcoins, et une dépense de 3 bitcoins. Alice possède donc au moins 7 bitcoins au moment où elle souhaite faire cette transaction.

A chaque instant, tout crédit en bitcoin est positif, la transaction sera validée car l'historique, public, de toutes les transactions d'Alice montre que ses cinq dernières transactions sont quatre gains respectivement de 5, 1, 2 et 2 bitcoins, et une dépense de 3 bitcoins. Alice possède donc au moins 7 bitcoins au moment où elle souhaite faire cette transaction.

Figure 07 : Précédente transaction d'Alice : une transaction de 4 BTC est validée car Alice possède au moins 7 BTC à la date de la transaction.

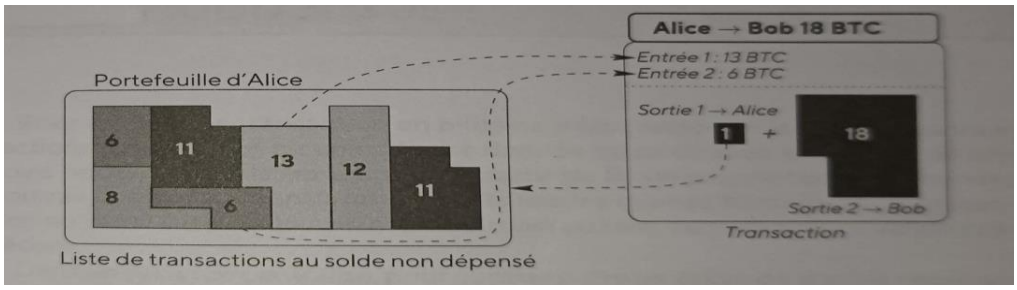


Source : J.G. Dumas, P. Lafourcade, A. Tichit, S. Varrette, « Les blockchains en 50 questions », édition Dunod, Paris, 2018

2. Création d'une crypto monnaie dans un portefeuille :

Lorsqu'une transaction d'une certaine valeur est envisagée, il faut combiner plusieurs bitcoins précédemment reçus pour atteindre au moins cette valeur Ces bitcoins sont potentiellement détenus à des adresses bitcoins distinctes stockées dans des portefeuilles électroniques distincts. De même, la valeur totale de la transaction peut être partagée entre plusieurs destinataires en particulier un des destinataires peut être le possesseur lui-même afin de faire de la monnaie.

Figure 08 : Sélection de bitcoins dans un portefeuille pour réalise une transaction de 18 BTC, avec une monnaie restante de 1 BTC.



Source : J.G. Dumas, P. Lafourcade, A. Tichit, S. Varrette, « Les blockchains en 50 questions », édition Dunod, Paris, 2018

Dans cette figure, Alice possède les sommes suivantes, en bit coins, dans des portefeuilles distincts : 6, 6, 8, 11, 11, 12 et 13 BTC Alice doit 18 BTC à Bob, elle choisit par exemple

deux groupes, l'un de 13 et l'autre de 6 BTC puis crée une transaction avec deux destinataires, Bob pour 18 BTC, et elle-même pour 1 BTC, la monnaie restante. Elle aurait pu choisir 12 et 6 BTC dans ce cas la transaction n'aurait eu qu'un seul destinataire En pratique, afin d'assurer l'anonymat pour chaque transaction, un utilisateur utilise une nouvelle paire de clefs. Ainsi les transactions sont souvent constituées de plusieurs sources pour aller vers plusieurs destinataires. A noter que le format exact d'une transaction bitcoin sera détaille dans la question.

3. Payement en crypto monnaie sur la blockchain :

Une blockchain est une base de données qui comporte tout l'historique des échanges réalisés entre des utilisateurs depuis sa création. On compare souvent la blockchain à un grand livre comptable qui reste anonyme et infalsifiable[7].

On parle souvent de blockchain avec les crypto monnaies telles que le Bitcoin, l'Ethereum ou encore le Ripple. La blockchain permet donc d'échanger des monnaies virtuelles en toute sécurité et toutes les informations disposent d'une parfaite traçabilité.

En effet, la monnaie numérique est gérée par une chaîne de blocs ou blockchain qui répertorie l'ensemble des transactions effectuées en cryptomonnaie depuis sa création. Toute transaction est consultable par tous et l'envoie de cryptomonnaie n'est pas si simple. En effet, cet échange fait jouer un processus complexe comprenant une large série d'étape permettant de transférer la cryptomonnaie d'un portefeuille à un autre.

Comment se passe une transaction en crypto monnaie[8] :

Prenant l'exemple le plus pertinent Bitcoin, Pour envoyer une certaine somme de Bitcoin, on doit publier notre intention de transférer une certaine somme. Les nœuds de vérification vont ensuite venir scanner l'entièreté du réseau afin de s'assurer qu'on possède bien la somme et qu'on ne l'a pas déjà transféré à quelqu'un d'autre.

Une fois que ces informations ont été confirmées, la transaction sera incluse dans un «bloc». Ce bloc se rattache au bloc précédent, d'où le terme blockchain, qui signifie, chaîne de blocs. Les transactions ne peuvent pas être modifiées a posteriori parce que cela signifierait qu'il faudrait reproduire chaque bloc qui est venu s'y rattacher ensuite.

[7] Qu'est-ce que la blockchain et la cryptomonnaie ? (journalducm.com), consulté le 06/11/2021
[8] Payer en bitcoin : comment faire ? (pouruneautreeconomie.fr), consulté le 06/11/2021

Chaque transaction est vérifiée et incluse dans un bloc, ce qui sécurise les informations des échanges.

Exemple [9]***:***

Par exemple, prenons un commerce nommé A, acceptant la cryptomonnaie et un particulier B souhaitant payer A en bitcoin.

Avant tout, il faudra que A et B détiennent bien tous les deux un portefeuille bitcoin, un fichier électronique contenant plusieurs adresses bitcoin. Celles-ci pourraient être assimilées à un sous compte bancaire : chaque adresse détient une somme de bitcoin associée. Néanmoins le concept de l'adresse bitcoin diverge du sous compte bancaire classique de part :

- Un portefeuille peut avoir (et cela est même encouragé) de nombreuses adresses ;
- Il est préférable de créer une nouvelle adresse pour chaque nouvelle transaction, cela permet de conserver un certain anonymat ;
- Cette adresse est une série de 34 lettres et chiffres.

Pour démarrer la transaction, A va créer une nouvelle adresse pour réaliser la transaction avec le particulier B. L'adresse va générer l'apparition d'une clé publique et d'une clé privée.

Cette paire de clé est intrinsèquement liées. La clé publique est, comme son nom l'indique, publique et correspond à l'adresse bitcoin. Tout un chacun peut la connaître sans vous faire courir de risque. Toute clé publique a pour corolaire une « clé privée » qui lui correspond. Il s'agit là de 64 chiffres et lettres. Celle-ci est donc privée, et il est très important que de la garder confidentielle pour protéger ses bitcoins. Les deux clés sont certes associées, mais cela ne signifie pas que qui que ce soit puisse deviner une clé privée d'après une clé publique, bien au contraire.

Ce système de double clé, privée et publique, permet de protéger son portefeuille et ses bitcoins.

La clé privée permet de signée chaque transaction et fait office de preuve d'origine de transaction. Une fois la transaction, aussi appelée message signée par A, l'adresse, ou clé publique est envoyer à B pour lui soumettre la demande de paiement sous forme de QR code.

[9] Payer en bitcoin : comment faire ? (pouruneautreeconomie.fr), consulté le 06/11/2021

Figure 09 : Un QR-code représentant l'adresse bitcoin 3Npnd9AEj9CJoSde7nC5dJjUCHmB18MbdM

Source : J.G. Dumas, P. Lafourcade, A. Tichit, S. Varrette, « Les blockchains en 50 questions », édition Dunod, Paris, 2018

B va communiquer la clé publique envoyée par A ainsi que le montant de la transaction à son client bitcoin (ou logiciel de portefeuille). B va choisir ou créer dans son portefeuille, l'adresse depuis laquelle il souhaite envoyer à A la cryptomonnaie nécessaire à sa transaction. Le client bitcoin va alors signer sa demande de transaction avec la clé privée de l'adresse de B choisie pour la transaction de bitcoin.

Tout le monde peut alors vérifier que la demande de transaction provient bien du bon propriétaire de compte grâce à la clé publique de la transaction.

Le contrôle de la transaction se fait grâce aux mineurs via le cloud mining. En réalité, tout le réseau bitcoin fonctionne grâce aux mineurs. Vous l'aurez bien compris, il ne s'agit pas de creuser la terre pour trouver des bitcoins. Au contraire, ce sont des individus, mais le plus souvent des groupes d'individus, qui mettent à disposition du réseau la puissance de calcul de leur ordinateur. N'importe qui peut devenir mineur de bitcoin. Pour en savoir plus sur comment être mineur, n'hésitez pas à lire notre article sur le cloud mining.

Ce sont eux qui récupèrent les transactions de chacun et les mettent en bloc. Afin de décider qui des mineurs pourra ajoute

Section 03 : Enjeux techniques[10].

Malgré le potentiel de cette nouvelle technologie, une grande majorité des applications de la blockchain sont encore en phase expérimentale et n'ont pas encore atteint une acceptation et utilisation de masse. Cette technologie soulève des interrogations importantes, notamment en

[10] De Filippi P., « Blockchain et cryptomonnaies », Que sais-je, Paris, novembre 2018

ce qui concerne la sécurité des réseaux et des applications fondées sur la blockchain, ainsi que leur capacité de mise à l'échelle.

1. L'immaturité et la complexité :

Tout d'abord, l'immaturité et la complexité de cette nouvelle technologie sont telles qu'il n'existe aujourd'hui qu'un petit nombre d'experts capables de comprendre le fonctionnement et d'analyser les potentielles failles de sécurité de ces systèmes. Ce problème est exacerbé par le fait qu'une fois déployé, le protocole d'une blockchain ou le code des applications déployées sur cette blockchain ne peut pas facilement être mis à jour.

2. Failles de sécurité :

L'exécution des applications sur la blockchain se faisant de façon automatique (et autonome), aucun opérateur ne peut (à lui seul) intervenir pour en arrêter le fonctionnement. Il est donc fondamental de s'assurer que ces applications soient développées de façon simple et sécurisée, afin d'éviter le risque de se retrouver avec une application dysfonctionnelle, dont le code ne pourra plus être modifié ni altéré. L'occasion s'est déjà présentée d'observer les implications de certaines failles de sécurité au sein d'une application blockchain. Un premier incident de grande envergure est survenu en juin 2016, lorsqu'un individu a identifié une vulnérabilité dans le code d'un *smart contract* déployé sur la blockchain d'Ethereum, qui détenait alors plus de 150 millions de dollars (en Ethers). Cet individu a exploité cette vulnérabilité afin de transférer un tiers de ce montant vers un autre smart contract sur lequel il détenait le contrôle. Seule une action coordonnée des membres du réseau a permis d'apporter une altération au protocole d'Ethereum afin de récupérer les cryptomonnaies ainsi détournées.

Un autre incident qui hante encore la communauté d'Ethereum a été causé par certaines failles de sécurité dans le code d'une librairie informatique qui régissait à l'époque un grand nombre de contrats à signature multiple (multi-sig). Une première faille a été exploitée pour détourner l'équivalent de 30 millions de dollars de ces contrats; puis une deuxième a permis de rendre cette librairie complètement inopérante, entraînant ainsi l'immobilisation de plus d'un million d'Ethers (dont la valeur est équivalente à plus de 700 millions de dollars aujourd'hui).

Mais les enjeux de sécurité ne se limitent pas uniquement aux failles informatiques. Comme nous l'avons vu auparavant, le mécanisme de « preuve de travail » (proof of work) permet d'administrer une blockchain de manière décentralisée, en utilisant des incitations

économiques afin d'encourager les mineurs à investir les ressources informatiques nécessaires pour administrer et sécuriser le réseau. Cependant, ce mécanisme n'est capable d'assurer la sécurité du réseau que si aucun acteur (ou groupe d'acteurs) investie dans ce réseau. Une fois ce seuil de 50% contrôle sur ne détient le plus de 50 % de la puissance de calcul atteint, cet acteur (ou groupe d'acteurs) pourrait potentiellement censurer certaines transactions, ou même manipuler des transactions passées.

Ce danger n'est pas uniquement théorique. Malgré leur caractère initialement décentralisé, on observe déjà une tendance à la centralisation de plusieurs blockchains. Par exemple, après neuf ans de fonctionnement, une grande partie de la puissance de calcul investie dans le réseau Bitcoin est contrôlée aujourd'hui par quatre grandes coopératives de mineurs (mining pools), administrées par des entreprises privées en Chine. Cette configuration constitue une véritable menace pour la sécurité du réseau, puisqu'une collusion entre ces différents acteurs leur permettrait de prendre le contrôle du réseau. Même si ces acteurs n'ont pas forcément intérêt à s'associer de cette façon (car cela risquerait de compromettre la sécurité, et donc la crédibilité du réseau), ils fragilisent néanmoins l'inviolabilité de la blockchain sur laquelle ils opèrent. Ces grandes coopératives de mineurs opèrent sur un territoire donné, et sont donc soumises aux lois qui régissent ce territoire. Un gouvernement serait à même de les obliger à coopérer les unes avec les autres, afin de faire appliquer certaines règles de droit : il pourrait ainsi réguler ces opérateurs en leur demandant de censurer certaines informations stockées sur la blockchain, ou d'ignorer des transactions considérées illicites.

3. La lenteur et les risques de congestion :

Un autre enjeu important est lié à la lenteur et aux risques de congestion qui se présentent pour une grande majorité des systèmes fondés sur la blockchain. La plupart des blockchains publiques de gérer qu'un nombre limité de transactions. Pu ne sont capables exemple, le réseau Bitcoin ne peut traiter que 240 000 transactions par jour environ bien inférieur aux 150 millions de transactions traitées -un nombre chaque jour par des sociétés telles que VISA. Etant donné le nombre croissant de transactions effectuées chaque jour sur la blockchain de Bitcoin, le réseau est désormais incapable d'en traiter la totalité. Cette incapacité a entraîné une forte augmentation des coûts de transaction dans les dernières années, avec des coûts arrivant au-delà des 50 euros en décembre 2017. Ainsi, de nombreuses transactions (dont les coûts ne sont pas suffisamment élevés) sont désormais ignorées par le réseau.

Ces blockchains sont aussi beaucoup plus lentes que la plupart des bases de données existantes. Il faut environ sept minutes pour qu'une transaction soit enregistrée sur la blockchain de Bitcoin. Et pour éviter le risque que le bloc dans lequel cette transaction a été enregistrée ne soit successivement remplacé par un nouveau bloc (qui appartiendrait à une chaîne ayant requis une quantité de puissance de calcul supérieure), de nombreux opérateurs ne reconnaissent la validité de ces transactions qu'après avoir reçu un certain nombre de « confirmations » (c'est-à-dire à la suite de l'enregistrement d'un certain nombre de blocs à la suite de la chaîne de référence). D'autres blockchains ont des délais relativement plus rapides, comme la blockchain d'Ethereum par exemple, capable d'enregistrer de nouveaux blocs, en moyenne, toutes les 10 ou 20 secondes. Ces chiffres restent cependant assez limités, comparés aux fractions de seconde requises pour enregistrer des informations sur des bases de données traditionnelles.

Afin de pouvoir effectivement bénéficier d'une adoption de masse, la performance de ces blockchains doit encore largement s'améliorer. Alors que certains opérateurs commerciaux commencent tout juste à expérimenter ces nouvelles technologies, il est important d'identifier les moyens qui permettraient à ces blockchains de grandir et d'évoluer, afin de pouvoir être utilisées comme base pour le développement de nouvelles applications, aussi bien dans le secteur public que privé.

Cependant, malgré les enjeux importants que cela représente, aucune solution définitive n'a encore été identifiée pour résoudre le problème lié à la congestion et à la saturation d'une blockchain. En raison de son irréversibilité, chaque nouvelle transaction enregistrée sur une blockchain provoque un accroissement de la taille de sa base de données à tel point que cela risque de compromettre le caractère décentralisé de ces réseaux. Car plus la taille d'une blockchain est grande, plus elle va nécessiter des ressources importantes en termes de stockage, de puissance de calcul, et de bande passante. Si ces exigences deviennent trop lourdes, le nombre d'acteurs pouvant contribuer aux opérations du réseau sera de plus en plus faible. Ce processus pourrait fragiliser la sécurité du réseau, puisqu'une réduction du nombre de mineurs comporte un risque plus élevé de collusion entre les acteurs responsables d'en assurer le fonctionnement.

Certaines propositions ont émergé pour faciliter la « scalabilité » de ces comportent, par exemple, l'élaboration de plus rapides et plus sophistiqués, le déplacement de applications. Elles certaines opérations hors de la blockchain, ou encore l'établissement de nouvelles

techniques de données permettant le traitement des transactions en gestion des protocoles parallèle. Une proposition particulièrement prometteuse à cet égard est le Lightning Network: un réseau de transaction haute fréquence qui permettrait d'effectuer des paiements instantanés entre les utilisateurs de Bitcoin ou d'autres cryptomonnaies (telles que Litecoin). La fondation Ethereum est aussi très impliquée dans ces efforts de scalabilité avec le développe ment d'un nouveau mécanisme de « proof of stake » (Casper) qui permettrait de réduire les coûts énergétiques impliqués dans la sécurisation du réseau. Les universités jouent également un rôle fondamental avec la mise en place de recherches coordonnées entre plu sieurs experts du secteur (par exemple, le Blockchain Lab de l'University College of London, et l'IC3 de Cornell University aux États-Unis). Toutes les pro positions développées jusqu'à présent restent à un niveau théorique et doivent encore être mises en appli cation. Leur réussite sera l'un des facteurs déterminants pour l'adoption en masse de ces technologies.

Conclusion

Au plus fort de la crise économique qui toucha le monde en 2008, une nouvelle façon de concevoir la monnaie a été proposée au sein d'un article posté sur internet et intitulé « Bitcoin : A Peer-to-Peer Electronic Cash System ».

La blockchain ou « chaîne de blocs » est une technologie de stockage et de transmission d'informations. Cette technologie permet à des personnes connectées en réseau qui ne se connaissent pas, de réaliser des transactions en quasi-temps réel à partir d'une même application.

Par analogie avec les registres classiques dans lesquels les transactions sont regroupées sur des pages, les transactions sont ici agrégées au sein de blocs digitaux chaînés entre eux.

Il existe deux types de blockchain, les blockchains publiques qui par définition sont ouvertes et accessibles à tous et les blockchains privées dont l'accès et l'utilisation sont limités à un certain nombre d'acteurs qui, par ailleurs, ne se font pas nécessairement entièrement confiance.

On parle souvent de blockchain avec les cryptomonnaies telles que le Bitcoin, l'Ethereum ou encore le Ripple. La blockchain permet donc d'échanger des monnaies virtuelles en toute sécurité et toutes les informations disposent d'une parfaite traçabilité.

Malgré le potentiel de cette nouvelle technologie, une grande majorité des applications de la blockchain sont encore en phase expérimentale et n'ont pas encore atteint une acceptation et utilisation de masse. Cette technologie soulève des interrogations importantes, notamment en ce qui concerne la sécurité des réseaux et des applications fondées sur la blockchain, ainsi que leur capacité de mise à l'échelle.

Chapitre IV

Crypto monnaies et blockchain : perspectives de projection dans le secteur bancaire et financier

Chapitre IV : Crypto monnaies et blockchain : perspectives de projection dans le secteur bancaire et financier

Introduction :

La blockchain pourrait devenir incontournable dans de nombreux domaines de l'économie. Dans le secteur financier, ses potentialités « disruptives » attisent autant les convoitises qu'elles ne troublent les esprits. Elle annoncerait la fin des intermédiaires[1] et ouvre des horizons pour les acteurs de la finance.

Nous serions aujourd'hui en matière de blockchain à l'équivalent des années 1990 pour l'internet, la blockchain se montre sous un jour incroyablement vertueux, elle offre à ses utilisateurs des fonctions de stockage, de transmission, de partage et de traçage avec une promesse de transparence et de fiabilité grâce au contrôle exercé par l'ensemble des membres de la chaine (blockchain publique) ou par celui qui la gère (blockchain privée).

Dans ce quatrième et dernier chapitre, nous allons présenter les perspectives de projection des technologies de la blockchain et des crypto monnaies dans le secteur bancaire financier. Nous allons commencer par une première section, qui abordera les applications communes aux acteurs de secteur financier (KYC, Reporting, et lutte contre la fraude), dans une deuxième section nous allons aborder les applications de la blockchain développées ou envisagées dans le secteur bancaire et financier (Au service de paiement, au service de financement et au service d'investissement) et dans une troisième section les applications développées ou envisagées dans le secteur de l'assurance (dans la gestion de la vie du contrat d'assurance, les produits d'assurance et dans la réassurance).

Section 01 : Applications communes aux acteurs du secteur financier

1. Know Your Customer (KYC) :

Le Know Your Customer consiste, pour une banque ou une grande entreprise, à vérifier l'identité et l'intégrité de ses clients[2]**.** La réglementation européenne impose cette vérification

[1] Vamparys Xavier, « La blockchain au service de la finance : Cadre juridique et applications pratiques », édition RB, Paris, septembre 2018.

[2] Connaître votre client (KYC) - Aperçu, importance et avantages, processus (corporatefinanceinstitute.com), consulté le 25/11/2021

afin de prévenir notamment la corruption, le blanchiment d'argent, la fraude fiscale et le financement du terrorisme. Elle contribue par ailleurs à garantir la stabilité du système financier[3].

Le processus consiste à :

- Collecter et analyser les données liées au client et valider son identité.
- Examiner les transactions et le comportement du client.
- Evaluer le niveau de risque d'un client, et ce depuis l'entrée en relation.

Toutes les sociétés qui exercent des activités de conseil, d'investissement ou de crédit (Banques, assurances, entreprises d'investissement, etc.) effectuent le KYC à chaque ouverture de compte, notamment les banque qui, de part leur particularité, nécessitent des standards de sécurité très élevés[4].

Ce mécanisme de contrôle est difficilement compatible avec les exigences de réactivité qu'impose l'ère numérique, la collecte de documents est très coûteuse et retarde l'acquisition de clients (Customer Onboarding) alors que l'examen et le contrôle en temps réel deviennent progressivement impératifs[5].

En effet, la blockchain peut résoudre ce problème, elles ne seront inscrites sur le registre que des informations vérifiées et validées, qui restent sous le contrôle des clients qui décideront d'y donner accès ou non. Par ailleurs, l'information ne devra plus être collectée, saisie et contrôlée par chaque banque ou intermédiaire, elle sera centralisée et accessible, avec l'accord du client, par tout membre de la chaine[6].

2. Reporting / Conformité [7]

Les obligations de reporting est un questionnaire sur la protection de la clientèle et les pratiques commerciales demandé par une autorité chargée de la supervision des secteurs bancaires et d'assurance appelée l'ACPR (Autorité de contrôle prudentiel et de résolution) aux professionnels[8].

[3] KYC : la connaissance client au service du secteur financier (infolegale.fr) consulté le 25/11/2021
[4] Le KYC à l'ère de l'intelligence artificielle : Quels atouts pour les institutions ? | SKAIZen Group, consulté le 25/11/2021
[5] Qu'est-ce que le KYC (Know your customer) à l'heure de l'IA ? (microsoft.fr) consulté le 04/11/2021
[6] Xavier Vamparys, « La blockchain au service de la finance : Cadre juridique et applications pratiques », Op, cit.
[7] Ibid.
[8] https://acpr.banque-france.fr/proteger-la-clientele/vous-etes-un-professionnel-du-secteur-de-la-banque-ou-de-lassurance/les-obligations-de-reporting, consulté le 04/11/2021

Les obligations de reporting des établissements bancaires et des assureurs ont connu une formidable inflation ces dernières années avec comme motivation une meilleure connaissance par les dirigeants, et notamment les membres des conseils d'administration, les actionnaires, le marché et les régulateurs, des risques supportés ou générés par des acteurs à l'importance de plus en plus systémique.

Le calcul des besoins en fonds propres requis par la réglementation Bâle III ou la directive Solvabilité II suppose la collecte et l'analyse d'innombrables données sur les risques supportés par les acteurs qui y sont assujettis. De même, les exigences de liquidité de Bale III demandent la mise en œuvre d'algorithmes de calcul et de reportings quotidiens. Autre illustration avec la réglementation SFTR (Securities Financing Transactions Regulation)[9], les sociétés de gestion qui pratiquent le financement sur titres ou les contrats d'échange sur rendement global doivent désormais fournir des informations sur chaque opération, ses contreparties, leurs risques et garanties.

Le corollaire de cette inflation réglementaire est le coût de plus en plus élevé pour les acteurs concernés de la mise en conformité de leurs activités d'ailleurs concomitant à une hausse très significative du montant des sanctions imposées en cas de non-conformité. Ainsi entre 2009 et 2017, les banques auraient payé 345 milliards de dollars aux divers régulateurs pour des défauts de conformité et plus de 100 milliards de dollars auraient été dépensés par les établissements financiers dans des programmes de conformité sur l'année 2017 uniquement.

La blockchain, parce qu'elle permet un enregistrement fiable et pérenne d'informations partagées et validées, constitue un outil intéressant pour la collecte des données utiles à la préparation de ces rapports et analyses et forme une piste d'audit exploitable par tout contrôleur. Par ailleurs, elle pourrait autoriser une vérification directe et permanente du régulateur à qui un accès est donné à cette blockchain.

Certaines start-up se sont positionnées sur ce segment d'activité, parfois dénommé RegTech, qui comprend les acteurs innovants s'appuyant sur les nouvelles technologies, dont la blockchain, pour aider les institutions financières à se mettre en conformité avec la réglementation qui leur est applicable[10].

[9] Règlement UE n° 2015/2365 relatif à la transparence des opérations de financement sur titres et de la réutilisation (Securities Financing Transactions Regulation ou SFTR), 23 décembre 2015. Consulté le 04/11/2021

[10] Vamparys X., « La blockchain au service de la finance : Cadre juridique et applications pratiques », Op, cit.

3. Lutte contre la fraude

La blockchain est souvent présentée comme un outil efficace de lutte contre le risque de fraude. En matière d'assurance, elle permet notamment d'assurer la traçabilité (lieu et date de production, transferts de propriété successifs, etc.) de certains biens, biens précieux ou œuvres d'art par exemple[11]. La valeur ou l'authenticité de ces biens pourra ainsi être aisément vérifiée. La certification des factures via une application permettrait d'éviter la fraude à l'assurance basée sur l'émission de factures[12].

Au-delà de la lutte contre la fraude, les informations figurant sur la chaîne permettront aux assureurs d'adapter la prise en charge des sinistres. En matière d'assurance automobile par exemple, on peut imaginer que des voitures connectées pourraient, en fonction de la nature de leur panne, déclencher l'intervention d'un dépanneur ou la mise en relation avec un garage adhérent à un réseau, pour que la prise en charge soit adaptée et justement tarifée. On pourrait également imaginer des actions préventives permettant de devancer la survenance d'une panne à partir des informations transmises par ces véhicules[13]. C'est aussi l'historique du véhicule et du conducteur qui, sous réserve de compatibilité avec les restrictions sur la transmission des données personnelles, pourra être partagé entre assureurs. On peut aisément imaginer des applications équivalentes en matière d'assurance habitation[14].

Section 02 : Applications de la blockchain développée ou envisagée dans le secteur bancaire et financier

1. Au service de paiement

La blockchain semble offrir des perspectives prometteuses en matière de paiement, notamment international.

Les commissions qui y sont pratiquées sont en effet très élevées et les délais d'exécution très lents. Comme le reconnaît la Société Générale « les paiements internationaux doivent évoluer, surtout en dehors de la zone SEPA (Single Euro Payments Area), car les clients

[11] W. Davtian, « Blockchain et assurance : espérance démesurée ou nouvelle ère », Revue Banque & Stratégie, n° 369, mai 2018, p. 33-38
[12] Vamparys X., « La blockchain au service de la finance : Cadre juridique et applications pratiques » Op, cit.
[13] W. Davtian, «Blockchain et assurance : espérance démesurée ou nouvelle ère», Revue Banque & Stratégie Op, cit.
[14] Vamparys X., « La blockchain au service de la finance : Cadre juridique et applications pratiques » Op, cit.

exigent un traitement de plus en plus rapide, des rapprochements facilités et une plus grande transparence en ce qui concerne les tarifs (...) Dérivée de blockchain, la DLT (distributed ledger technology) est à présent étudiée et évoquée dans le secteur des paiements internationaux, car elle pourrait introduire des améliorations aux méthodes de traitement des paiements, ce qui permettrait de satisfaire en conséquence les exigences des clients »[15].

En rendant inutile le recours à un tiers de confiance, les virements sont effectués rapidement et pour un coût plus faible. Toutefois, pour la Société Générale, deux conditions restent à remplir pour que la blockchain devienne une technologie de référence en matière de paiements. Tout d'abord, il faudra adopter des normes communes aux diverses crypto-monnaies, Ensuite, la technologie doit être développée et les acteurs raccordés entre eux tout en assurant la conformité du dispositif aux contraintes réglementaires, notamment en termes de lutte contre le blanchiment d'argent et de régimes des sanctions[16].

Certaines banques semblent toutefois plus optimistes et offrent désormais un service de virement international rapide et sécurisé basé sur le Ripple[17], qui fonctionne comme une monnaie universelle d'échange.

L'utilisation de la blockchain va par ailleurs pousser certains acteurs pourtant établis comme la messagerie internationale Swift, acteur incontournable des transferts de fonds internationaux, à réagir. Ainsi, Swift propose désormais un service de suivi des virements transfrontaliers, virements dont la réalisation a été accélérée puisqu'avec ce service les paiements sont crédités dans la journée, voire pour une part significative d'entre eux en quelques secondes ou minutes[18]. Ce service sera amélioré pour permettre à un client d'arrêter un virement avant d'atteindre le compte cible. En outre, Swift compte développer son service de paiement instantané et a rejoint le consortium Hyperledger, un projet open source et open gouverance qui offre à ses membres une structure technologique pour developper un projet reposant sur une blockchain (le protocole, la blockchain et les smart contracts) mais également un environnement et les outils nécessaires pour développer le projet et mettre en

[15] Société Générale, « blockchain et paiements- Enseignement tirés er perspectives d'avenir », https://www.societegenerale.com/fr/temoignages-entrepreuneurs/evenements/sibos-2017/blockchain-paiements, consulté le 05/11/2021

[16] Ibid.

[17] Ripple est un système de règlement brut en temps réel (RBTR), un marché des changes et un réseau d'envois de fonds par la société Ripple.

[18] Charlie Perreau, « menacé par Ripple, Swift contre attaque » Jounal du net, 29/04/2018 Menacé par Ripple, Swift contre-attaque (journaldunet.com) consulté le 05/11/2021

relation les différentes parties au projet [19] pour y expérimenter des paiements via la blockchain[20].

L'utilisation du Ripple comme cryptomonnaie de compensation pour les transferts de fonds internationaux fait écho à l'expérience menée par UBS, avec l'Utility Settlement Coin, équivalent numérique de chacune des principales devises permettant des transferts d'argent rapides et fiables[21].

BNP Paribas propose de son côté le service de transfert de cash international Cash Without Borders, qui repose également sur la blockchain et permet des virements entre comptes BNP Paribas auprès de banques étrangères correspondantes en deux heures, sans qu'il soit nécessaire, comme c'est le cas des transferts Ripple, de mobiliser du collatéral[22]

L'accélération des paiements, qu'ils soient nationaux ou internationaux, répond à une demande d'instantanéité de plus en plus forte des consommateurs[23], demande pour laquelle la blockchain peut offrir des solutions intéressantes.

Enfin, l'initiative suivante mérite d'être relevée : la Banque de France a lancé une étude sur les opportunités offertes par la technologie blockchain pour le registre des Identifiants Créanciers SEPA (ICS), dont elle assure la gestion[24] en qualité de tiers de confiance. Le choix de ce registre était motivé par la faiblesse des enjeux de sécurité il s'agit d'un registre d'identification et non de transferts de valeurs et d'un cadre réglementaire favorable [25]. L'application, qui prend la forme d'un smart contract, a été développée avec 7 établissements partenaires représentant 95 % des demandes SEPA[26]. Désormais, les modifications du registre SEPA sont assurées directement par les banques participantes, membres d'une chaîne privée

[19]https://www.blockchainsexpert.com/ .
[20]Charlie Perreau, « menacé par Ripple, Swift contre attaque » Journal du net, 24/04/2018 Menacé par Ripple, Swift contre-attaque (journaldunet.com) consulté le 05/11/2021
[21] How UBS Could Change the Way the World's Biggest Banks Do Business – Bitcoin Isle (www.bitcoinisle.com), consulté le 05/11/2021
[22] Interview de P. Denis « il faut déceler les cas d'usage les plus pertinents de la blockchain », revue Banque, n°811, 30/08/2017 (http://www.revue-banque.fr/revue-banque/numero-811), consultée en ligne le 05/11/2021
[23] https://www.boursorama-com.cdn.ampproject.org/c/s/www.boursorama.com/actualite-economique/actualites-amp/tgv-du-virement-bancaire-le-paiement-instantane-debarque-en-france-eeadbc19940d9abe2046d399b527588f, consulté le 05/11/2021
[24] Communiqué de presse Banque de France « La banque de France mène une expérimentation de blockchain interbancaire » 15 décembre 2016.
[25] S. Leboucher, « blockchain, la banque de France entre entre en production, revue Banque, n° 811, 30/08/2017(http://www.revue-banque.fr/revue-banque/numero-811), consulté en ligne le 05/11/2021
[26] Ibid

constituée à partir du protocole Ethereum. La période de test a permis d'identifier certains sujets, certes classiques, liés à la décentralisation des registres : la confidentialité des opérations, à préserver pour les membres de la chaîne non concernés, la capacité à gérer un grand nombre de transactions, la faculté de mettre en œuvre le droit à l'oubli[27].

2. Au service de financement

- **Crowdfunding :** La blockchain peut être utilisée pour faciliter la mise en place de financement, en capital ou en dette, en particulier pour le financement participatif (crowdfunding). Une ordonnance du 30 mai 2014[28] a créé deux statuts pour les plateformes de crowdfunding, en fonction de la forme du financement proposé : titres ou dons/prêts.

Pour les financements sous forme de titres, les plateformes doivent obtenir la qualification de conseiller en investissement participatif[29], et pour ceux sous forme de dons ou prêts, c'est le statut d'intermédiaire en financement participatif qui s'applique, Les sponsors de toute opération de crowdfunding sur la blockchain devront donc tenir compte de ce cadre réglementaire. Il convient toutefois de noter qu'il concerne des personnes morales exerçant une activité de levée de fonds à titre de profession habituelle, ce qui ne serait pas le cas d'une opération de financement isolée initiée par une communauté de membres d'une blockchain ou d'une DAO[30].

BNP Paribas a développé avec SmartAngels [31]une plateforme de financement participatif en fonds propres (crowdequity) qui repose sur la blockchain[32] Le registre distribué gère les souscriptions, constatées instantanément sur paiement avec l'émission d'un certificat électronique, mais aussi certains aspects de la vie sociale des sociétés financées, comme les convocations aux assemblées générales. Il est constitué d'un réseau privé dont les principaux nœuds sont pilotés par BNP Paribas, avec une règle de consensus basée sur la preuve d'enjeu. Le processus permet un traitement fiable, rapide et peu coûteux des opérations sur titres, ce qui in fine va contribuer à un accès facilité des start-up à des financements de croissance.

Depuis l'adoption de l'ordonnance du 28 avril 2016 sur les minibons, BNP Paribas utilise également la blockchain pour le financement participatif en dette (crowdlending).

[27] S. Leboucher, « blockchain, la banque de France entre entre en production, Op. cit.
[28] Ordonnance n° 2014-559 du 30 mai 2014 relative au financement participatif du droit français.
[29] Interview de P. Denis « il faut déceler les cas d'usage les plus pertinents de la blockchain », Op cit.
[30] Ibid.
[31] https://allianz.smartangels.fr/
[32] Interview de P. Denis « il faut déceler les cas d'usage les plus pertinents de la blockchain », Op cit.

La Caisse des Dépôts et l'association Financement Participatif France collaborent de leur côté autour d'une blockchain dédiée au financement participatif au profit des PME et à laquelle participent certaines plateformes comme Crédit.fr, Unilend, Lumo ou Enerfip[33].

- **Financement pair à pair :** En fait, la blockchain pourrait concurrencer fortement les plateformes de crowdfunding en mettant les prêteurs en lien direct avec les entreprises, les porteurs de projets ou les particuliers. Là encore, l'intérêt de la blockchain est de rendre inutile le recours à tout intermédiaire spécialisé Bitbond [34] permet par exemple à des particuliers de financer des prêts en bitcoins d'autres particuliers.

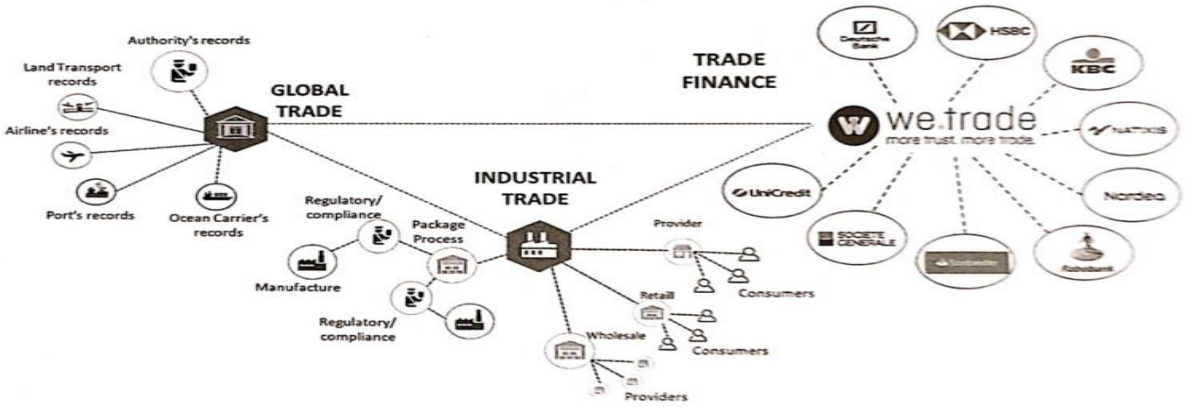
On peut par ailleurs envisager que les prêts consentis par des particuliers soient transférables à d'autres, créant ainsi un marché secondaire.

- **Trade finance :** Le trade finance recouvre les activités de financement des opérations de commerce international, sur lesquelles les banques françaises sont très présentes. Le nombre de parties et le volume de documentation impliqués dans chaque opération de trade finance en font un candidat idéal pour des applications blockchain. Les banques Wells Fargo et Commonwealth Bank of Australia, qui prétendent avoir réalisé une première mondiale en ce domaine en 2016, ont ainsi souligné que l'« utilisation de la technologie Blockchain apporte de la transparence pour l'acheteur et le vendeur, un niveau plus élevé de sécurité et la possibilité de suivre une livraison en temps réel (..). réduit les erreurs et réalise en quelques minutes ce qui prenait auparavant des jours »[35]

L'application de la blockchain proposée par le consortium Digital Trade Chain, devenu « We Trade », associe neuf banques (Deutsche Bank, HSBC, KBC, Natixis, Nordea, Rabobank, Santander, Société Générale, UniCredit) pour le commerce frontalier et met en réseau sur la blockchain vendeur, acheteur, banques, transporteurs et autres intermédiaires[36].

[33] Communiqué de presse CDC, http://www.caissedesdepots.fr/sites/default/files/medias/cp_et_dp/cp_minibons.pdf consulté le06/11/2021
[34] https://www.bitbond.com, consulté le 06/11/2021
[35] D. Cuny « La caisse des dépots teste la blockchain dans le prêt de titres », La Tribune, 4 novembre 2016
[36] https://www.we-trade.com/ consulté le 06/11/2021

Figure 10 : Financement avec la blockchain



Source : Xavier Vamparys, « La blockchain au service de la finance : Cadre juridique et applications pratiques », édition RB, Paris, 2018

Toujours en matière de commerce international, Hyperledger, projet blockchain piloté par IBM, met les cocontractants et leur banque en réseau et assure l'exécution automatique de certains engagements et garanties via des smart contracts.

Enfin, Euler Hermes et HSBC ont testé la blockchain pour proposer à leurs clients une solution d'assurance-crédit et d'affacturage plus efficace, avec un suivi de la facture et de son paiement plus transparent et fluide[37].

- **Prêt-emprunt de titres :** Certains investisseurs institutionnels (banques, assureurs, sociétés de gestion) disposent de portefeuilles de titres qu'ils mettent à disposition d'autres investisseurs (banques, hedge funds) pratiquant la vente à découvert. Ces opérations font l'objet de garanties sous forme d'actifs (collatéral) qui imposent un monitoring précis. La transparence, la sécurité et la rapidité de la blockchain en font un bon candidat pour assurer ce monitoring. Ainsi, certains institutionnels ont développé avec la Caisse des Dépôts une plateforme de gestion du collatéral non cash pour les prêts emprunts de titres constituée sur la base du protocole Ethereum et de smart contracts[38].
- **Titrisation** : La titrisation est une technique financière qui consiste à regrouper certains actifs peu liquides dans un véhicule dont les titres sont proposés à des investisseurs. Par extension, cette technique couvre toute opération rendant la propriété ou d'autres droits

[37] Communiqué de presse Euler Hermes, http://www.eulerhermes.fr/medicacenter/actualites/Pages/blockchain-hsbc.aspx, consulté le 06/11/2021
[38] Ibid

sur un bien ou des actifs plus liquides ». La blockchain constitue un outil intéressant en matière de titrisation. Elle facilite en effet l'émission et l'échange de droits « numériques » portant sur un actif matériel ou immatériel. En fait, tout bien pourra faire l'objet de droits de propriété ou d'usage numériques, droits « liquides » et négociables en raison de leur inscription sur une chaîne de blocs[39]. Ainsi, on pourrait imaginer qu'une entreprise disposant d'une classe d'actifs particulière (véhicules, immeubles par exemple) en propose le partage de la propriété, ou de l'usage, sous forme de jetons qui seraient échangeables sur une chaîne de blocs.

- **Autres financements :** BBVA a été la première banque à utiliser la blockchain pour consentir un prêt commercial, d'un montant de 75 millions d'euros. Cette technologie a notamment facilité la négociation, dont le temps s'est réduit à quelques heures[40].

Comme on a pu le voir, la blockchain est testée en matière de lettre de crédit (solution Hyperledger) ou de crédits documentaires (solution Corda), mais également d'émission obligataire.

3. Au service d'investissement

- **Tenue de registre des titres non cotés[41] :** Les titres non cotés ne font pas l'objet d'une tenue auprès d'un intermédiaire habilité. Ainsi, ces titres, lorsqu'ils sont émis par une société ou un organisme de placement collectif, peuvent être tenus par cette société ou cet organisme, ou la tenue peut être confiée à un tiers mandataire. Cette tenue, assez largement manuelle, pourrait être optimisée (notamment en termes de fiabilité) par l'utilisation de la technologie blockchain, et ce à moindre coût, par des prestataires spécialisés dans la gestion de titres, secteur sur lequel les banques sont bien positionnées.

La start-up Utocat propose un outil de gestion numérique des titres non cotés dénommé «Catalizr » utilisable par les émetteurs, les intermédiaires financiers et les investisseurs.

- **Titres cotés : activités de marché[42] :** Les opérations mises en œuvre lorsqu'un instrument financier est acheté ou cédé sur un marché réglementé ou sur un système multilatéral de négociation sont complexes, font intervenir de nombreux acteurs (intermédiaires financiers, Bourse, chambre de compensation, dépositaire central, dépositaire

[39] Vamparys X., « La blockchain au service de la finance : Cadre juridique et applications pratiques », Op cit.
[40] Ibid.
[41] https:/www.utocat.com/ consulté le 06/11/2021
[42] Vamparys X., « La blockchain au service de la finance : Cadre juridique et applications pratiques », Op cit.

local) et prennent donc du temps. Dans le cadre d'une opération sur action, l'inscription en compte intervient normalement deux jours après la transmission de l'ordre d'achat de l'action Ce processus génère par ailleurs des erreurs, estimées à 20 %, qui doivent être corrigées manuellement.

C'est cette mécanique complexe et lente que la blockchain pourrait bouleverser en remplaçant l'intermédiaire financier, la Bourse, la chambre de compensation et le dépositaire central. L'immédiateté de l'ensemble du cycle de d'achat/vente de titres sur la blockchain rend l'intervention de ces intermédiaires/rouages de l'infrastructure de marché inutile. Il faut peut-être réserver le cas particulier de la fixation du prix qui suppose une centralisation des intérêts de vente et d'achat qui bute sur le caractère décentralise de la blockchain. Le groupe FinTech de Paris Europlace sur les impacts des réseaux distribués et de la technologie blockchain dans les activités de marché relève d'ailleurs que les carnets d'ordres des bourses de crypto monnaies sont tenus en dehors de la blockchain.

L'agence de notation Moody's[43] considère que la blockchain pourrait transformer de nombreux aspects du trading des actions, permettant potentiellement aux institutions financières de réduire les coûts et d'augmenter la vitesse de règlement des opérations sur titres. Il est relevé que le nombre d'intervenants impliqués dans les opérations post-marché, jusqu'à une douzaine « des chambres de compensation, aux banques chargées de la conservation, puis aux acteurs en charge du règlement et de la livraisons, mais aussi le fait que ces acteurs ne partagent aucune base de données, sont sources d'inefficacité. Ainsi, pour Moody's, « plutôt que chaque participant aux échanges post-marché conserve les mêmes données dans son registre individuel de transactions, un registre principal partagé entre ces participants éliminerait la nécessité de processus de conciliation coûteux ».

Pour Moody's toutefois, il est probable qu'à moyen terme les acteurs actuels du post-marché ne cèdent pas la place à de nouveaux entrants car le secteur reste très réglementé. La chambre de compensation doit, en qualité d'établissement de crédit, être agréée par l'ACPR, après avis de l'AMF et de la Banque de France. Le dépositaire central est supervisé par l'AMF. Une blockchain ne pourrait donc en l'état agir comme dépositaire central sans agrément de cette autorité. L'inscription en compte auprès d'un dépositaire central est prévue pour tout titre négocié sur une plateforme d'échange, Quant à l'activité de tenue de compte-

[43] V. D. Cuny « La blockchain a le potentiel de transformer le trading d'actions selon Moody's », La Tribune, 14 avril 2017.

conservation, elle doit être assurée par l'émetteur ou par un des intermédiaires visés à l'article L. 542-1 du Code monétaire et financier (établissements de crédit ou entreprises d'investissement). Les teneurs de compte sont tenus à certaines obligations prévues par le Code monétaire et financier et le règlement général AMF et doivent notamment apporter tous leurs soins à la conservation des instruments financiers, à leur comptabilisation et à l'exercice des droits qui y sont attachés, L'adoption de la blockchain pour les échanges de titres cotés impliquerait donc une modification très significative de la réglementation française et européenne. Certains suggèrent par exemple que les nœuds des blockchains titres fassent l'objet d'un agrément[44].

Pourtant, on voit bien que la raison d'être de l'intervention de certains acteurs, et notamment la chambre de compensation, disparait avec is blockchain, puisque l'instantanéité de l'échange titres-espèces qu'elle permet supprime les risques de contrepartie et de marché, Toutefois, certains craignent que ce mode d'échange des titres ne concoure pas à une fixation neutre et juste du cours des titres[45].

C'est donc d'abord dans le domaine des titres non cotés que la technologie blockchain pourra s'imposer. Pour ces titres, le transfert de propriété intervient à la date convenue entre les parties, conformément aux dispositions de l'article R. 228-10 du Code de commerce. Elle a d'ailleurs fait l'objet d'une première reconnaissance avec l'ordonnance du 8 décembre 2017.

Liquidshare, FinTech constituée par BNP Paribas, CACEIS, la Caisse des Dépôts, Euroclear, Euronext, S2iEM et Société Générale, a pour ambition de développer un outil pour les opérations post-marché pour le segment des PME. La blockchain a, selon les promoteurs de cette FinTech, « le potentiel de simplifier significativement la chaîne des opérations de post-négociation, en garantissant et facilitant la consolidation des registres de titres, tout en permettant une rapidité d'exécution avec un règlement-livraison en temps réel à T+0 ». La rapidité d'exécution et de circulation de l'information est obtenue en mettant sur la même chaîne les investisseurs, les brokers, le dépositaire et les PME émettant des titres. L'investisseur qui souhaite acheter des titres envoie un ordre sur la chaîne, ordre reçu par le broker qui est également sur la chaîne, puis à la Bourse pour exécution. Cette exécution entraine immédiatement, via un smart contract, le règlement du vendeur via la banque dépositaire, membre également de la chaîne, et le règlement du vendeur. La PME concernée,

[44] Vamparys X., « La blockchain au service de la finance : Cadre juridique et applications pratiques », Op cit.
[45] Ibid.

qui appartient à la chaîne, est immédiatement avisée du changement d'actionnaires. L'opération peut ensuite être contrôlée par le régulateur ou toute autorité, l'ensemble des opérations ci-dessus étant enregistrées de façon immuable sur la chaine. L'accélération des opérations est facilitée par la disparition des livraisons physiques » de titres et numéraire désormais remplacées par des écritures électroniques « dématérialisées » (virement et inscription en compte)[46].

Aux Etats-Unis, DTCC (Depository Trust and Clearing Company), qui intervient comme dépositaire et chambre de compensation pour tous les titres cotés sur les marchés américains, a adopté la technologie blockchain pour les opérations de compensation de l'ensemble des dérivés de crédit (credit default swap) 46. Il est ainsi prévu que les entreprises participantes aient accès au registre distribué des opérations en tant que « nœuds » du réseau. A terme, chacun de ces participants n'aura plus à se reposer sur des infrastructures et bases de données qui lui sont propres. La blockchain servira à la fois pour l'enregistrement des opérations et la gestion des opérations « post-marché ». La technologie retenue par DTCC est celle développée par le consortium R3.

Autre illustration, la Bourse australienne prévoit de passer toutes ses operations de compensation et de règlement sur la blockchain d'ici 2021, à partir d'une technologie proposée par une start-up, Digital Assets Holding[47].

- **Gestion d'actifs[48] :** La gestion d'actifs fait, comme les activités de marché, intervenir beaucoup d'intermédiaires qui, sociétés de gestion mises à part, relèvent principalement du secteur bancaire: centralisateur, dépositaire, teneur de compte, chambre de compensation, agent de transfert... autant d'acteurs qui peuvent être source d'erreurs, d'inefficacité ou de délais.

La mise en place d'une chaîne de blocs pour gérer les souscriptions et rachats de parts permettrait de réduire le temps d'exécution de quelques minutes et économiserait les commissions de quelques intermédiaires, et ce sans fragiliser la sécurité des opérations s'agissant notamment du risque de contrepartie.

[46] Communiqué de presse, « Liquidshare, la fintech blockchain européenne pour le post-marché des PME, est lancée », Société Générale, 11 juillet 2017
[47] http://www.coindesk.com/australian-securities-exchange-eyes-end-2020-dit-rollout/consulté le 06/11/2021
[48] Vamparys X., « La blockchain au service de la finance : Cadre juridique et applications pratiques », Op cit.

La blockchain permettra un suivi en temps réel des actifs gérés et de leur valeur. Par ailleurs les événements affectant ces actifs pourront, lorsqu'ils ont des conséquences juridiques ou commerciales, faire l'objet de mises en œeuvre automatiques, comme en matière de dérivés ou de levée d'options[49].

Ainsi, en 2017, la société de gestion Natixis Asset Management a mis en place une plateforme dénommée FundsDLT en collaboration avec Fundsquare, filiale de la Bourse du Luxembourg, permettant aux investisseurs de souscrire des parts de fonds via une application mobile connectée à la chaîne de blocs à laquelle participaient la société de gestion CACEIS en qualité d'agent de transfert, la banque de l'investisseur et celle de l'organisme de placement collectif concerné.

Bien évidemment, les questions relatives au choix de la blockchain, à la compatibilité avec le règlement RGPD, à l'identification, etc., évoquées ci-dessus restent pertinentes pour l'activité de gestion d'actifs.

- **Trading de crypto-monnaies :** Les banques d'affaires ont rapidement compris que l'émergence des monnaies virtuelles pouvait constituer un nouvel are d'activités.

Ainsi, la banque Goldman Sachs s'est récemment lancée dans une activité d'achat-vente (trading) de contrats indexés sur les crypto-monnaies pour ses clients. L'étape suivante pour cette banque, comme pour celles qui ne manqueront pas de se lancer elles aussi dans cette activité, pourrait être l'achat-vente de crypto-monnaies en direct pour ses clients, voire la mise sur le marché de ses propres contrats indexés sur ces monnaies et l'achat-vente de celles-ci pour compte propre[50].

Alors que les banques françaises ont déclaré se tenir à l'écart des cryptomonnaies, il semblerait que la réalité soit plus nuancée.

Au-delà du secteur bancaire au sens strict, certains fonds d'investissement se sont constitués autour des crypto-monnaies. Il y aurait ainsi aujourd'hui plus de 200 fonds dédiés à ces actifs dans le monde, contre seulement une trentaine en 2016. Le montant des actifs sous gestion de ces fonds serait inférieur à 5 milliards d'euros, somme relativement faible au

[49] Interview de B. Denis « la blockchain dans le secteur de l'assurance », Wolters Kluwer, 21 septembre 2017.
[50] R. Bloch, Goldman Sachs prêt à investir dans les cryptomonnaies », Les Echos, 3 mai 2018, https://www.lesechos.fr/2018/05/goldman-sachs-pret-a-investir-dans-les-cryptomonnaies-989857, consulté le 07/11/2021

regard de la valorisation totale des crypto-monnaies. L'intérêt croissant des principaux acteurs du secteur financier, comme les banques d'affaires, pour les crypto monnaies et la recherche par les investisseurs d'actifs permettant d'espérer des taux de rendement élevés devraient être favorables au développement de ce type de fonds. Une étude 56 portant sur les neuf plus importants fonds a montré que ces taux s'élevaient en moyenne à près de 1500 % en 2017… Par ailleurs, la valeur des crypto-monnaies n'est pas corrélée à l'état de l'économie, ce qui en fait une bonne source de diversification dans un portefeuille… si on oublie que leur valeur d'usage et leurs perspectives de revenus sont nulles et leur liquidité faible[51]

Les stratégies d'investissement de ces fonds sont assez diversifiées, certains prenant des positions sur l'une ou l'autre des crypto-monnaies, d'autres investissant dans des paniers de monnaies et d'autres encore profitant des écarts de change sur ces crypto-monnaies entre les différentes plateformes.

En France, la société Tobam, qui compte environ 10 milliards de dollars d'actifs sous gestion, a lancé fin 2017 un fonds alternatif non régulé investi en Bitcoins, le Tobam Bitcoin Fund[52].

L'univers de la blockchain donnera également naissance à des fonds qui investiront dans les ICO ou les acteurs du secteur. Certains de ces fonds, comme ceux proposés par la société de gestion Trecento, sont déjà en cours de constitution, sous une forme originale qui est celle d'une DAO où les décisions d'investissement sont prises à la fois par les membres et la société de gestion, les profits tirés de ces investissements étant ensuite partagés. La chaine est ainsi bouclée : un d'organisation et de fonctionnement qui repose sur la blockchain pour investir dans des produits ou acteurs de cette même blockchain[53].

Le rapport Landau préconise de dissuader les banques de s'engager dans l'activité de trading pour compte propre de crypto-monnaies, pour éviter toute diffusion à l'économie réelle d'une crise dans l'écosystème des crypto monnaies, et d'encadrer la pour les gestionnaires de portefeuilles d'y inclure de tels actifs.

[51] https://www.crypto-france.com/societe-generale-bitcoin-aucun-avenir-caractere-anonyme/ consulté le 07/11/2021
[52] https://www.tobam.fr/ consulté le 07/11/2021
[53] https://trecento-blockchain.capital/consulté le 07/11/2021

- **Produits dérivés**[54] **:** La blockchain et les smart contracts constituent des outils intéressants pour l'activité «dérivés » des banques.

L'ISDA a indiqué que la blockchain pouvait jouer un rôle significatif dans la mise en place de pratiques de marché standardisées et efficaces. Elle recommande notamment de mettre les accords-cadres (ISDA Master Agreements) sur une chaîne de blocs. L'exécution automatique de certaines clauses (appels de marge, transmission d'informations) pourra être rendue possible avec des smart contracts, qui ont fait l'objet d'une étude publiée par l'ISDA en août 2017.

En pratique, on a vu que DTCC allait utiliser la blockchain pour la compensation des opérations de swap de défaut de crédit. Autre illustration pratique : la plateforme Variabl qui permet les transactions de dérivés sur crypto-actifs au moyen d'un smart contract, mettant face à face sur la blockchain deux parties qui font un pari contraire sur l'évolution d'une crypto-monnaie (pour le moment l'ether).

- **Conseil :** La multiplication des projets d'ICO a permis l'émergence d'acteurs nouveaux, venant concurrencer les banques d'affaires généralement mandatées pour assister un émetteur dans l'émission et le placement de valeurs mobilières.

Ainsi, les sociétés Blockchain Partner et Coinhouse proposent désormais d'accompagner les entrepreneurs souhaitant lever des fonds en crypto monnaies. Blockchain Partner s'est par ailleurs associée à Havas pour accompagner les sociétés ayant émis des tokens dans leur communication « cryptofinancière ».

- **Autres activités :** Toutes les activités d'investissement ou de négoce impliquant des volumes importants de documentation et l'intervention de plusieurs intermédiaires pourront voir un avantage dans la blockchain. On pensera notamment au négoce de matières premières[55].

[54] https://www.isda.org/a/6EKDE/smart-contrats-and-distribued-ledger-a-legal-perspective.pdf, consulté le 07/11/2021

[55] https://www.the--blochchain-com.cdn.ampproject.org/, consulté le 11/11/2021

Section 03 : Applications de la blockchain développées ou envisagées dans le secteur de l'assurance

Le secteur de l'assurance s'intéresse de plus en plus à la blockchain : comme 'illustre une étude de PwC, si en 2016 seuls 17 % des assureurs reconnaissaient un intérêt à cette technologie, ils étaient plus de la moitié en 2017[56].

1. La gestion de la vie du contrat d'assurance

Tarification [57] : En leur donnant accès à un ensemble d'informations fiables et régulièrement mises à jour, les assureurs pourront proposer à leurs clients une tarification adaptée. Ceci va à l'encontre du principe de mutualisation des risques, mais ce mouvement est déjà bien enclenché, indépendamment même du développement de la blockchain. Pour un auteur, avec cette technologie, on entrerait « dans l'ère de la personnalisation des primes, avec une prévention des négligences par l'augmentation de prime qui oblige l'assuré à la responsabilité, et le risque de voir des assurés fragiles laissés pour compte ».

Le recours en temps réel à des oracles ou à des objets connectés autorisera un ajustement permanent des risques couverts et donc de la tarification. Des applications sont déjà imaginées, en matière d'assurance maritime par exemple. Par ailleurs, ces risques seraient mieux connus, notamment grâce à l'historique infalsifiable de l'assuré ou du bien assuré, et à la juste valorisation de ce dernier. Enfin, la désintermédiation inhérente à la blockchain permettrait aux assurés d'être directement mis en contact avec les assureurs, réduisant de fait les coûts d'acquisition de la clientèle.

Gestion des contrats[58] : Même si des progrès ont été accomplis en ce domaine, via notamment la dématérialisation des documents, la gestion administrative des polices reste coûteuse pour les assureurs. Un certain nombre de tâches pourront être automatisées, de la souscription au paiement des sinistres, via notamment la mise en place de *smart contracts*. Assureurs et assurés pourront ainsi se dispenser du recours aux contrats ou documents papier, parfois égarés ou non remis. L'ensemble des événements qui marqueront la vie du contrat

[56] https://www.pwc.com/gx/en/financial-services/fintech/assets/fintech-2-0-insurance.pdf, consulté le 11/11/2021
[57] Ibid.
[58] www.blocksure.com, consulté le 11/11/2021

seront fidèlement retranscrits dans la chaîne, ce qui sera source de transparence pour les assurés et de preuve pour les assureurs. Plus globalement la rapidité d'exécution, et notamment de règlement des sinistres, devrait être favorable aux assurés.

Pour un auteur, le risque pour les employés des compagnies d'assurance est de voir la blockchain remplacer l'activité de tarification des actuaires, la distribution et surtout le conseil de vente de nombreux produits, la gestion des sinistres, le pilotage comptable, etc. Tout en suscitant de nouveaux métiers

À plus brève échéance, la blockchain permettra le partage d'informations et de bases de données entre assureurs, réassureurs, courtiers et autres intermédiaires et l'automatisation au moins partielle de certaines conventions de marché, comme la Convention d'Indemnisation directe de l'assuré et de recours entre sociétés d'assurance automobile « IRSA » ou la Convention d'Indemnisation et de recours corporel automobile « IRCA » .

Le consortium B3i- qui réunit certains assureurs et réassureurs dans une blockchain pour faciliter leurs échanges, de la souscription du contrat au paiement des sinistres – estime que le gain en coûts de gestion pour les assureurs pourrait être de l'ordre de 30 %. Ceci suppose bien évidemment que des acteurs, même concurrents, acceptent de coopérer. C'est à ce prix que la blockchain aura un impact très significatif sur le secteur. BCG évalue quant à lui les gains potentiels en marge technique pour le secteur à 200 milliards de dollars.

Microsoft considère que l'assurance de biens à valeur élevée (assurance maritime ou assurance aéronautique par exemple) est un bon cas d'application de la blockchain car ce secteur se caractérise par des informations en «silo» non partagées entre acteurs, une documentation aux formats différents et souvent irréconciliables, un recours encore intensif au papier, un pricing complexe, notamment en raison d'une information imparfaite, et une occurrence élevée de fraudes. Microsoft a ainsi mis en place une plateforme avec E&Y et Guardtime en matière d'assurance maritime »[59].

La start-up ChainThat propose une application basée sur la blockchain pour rendre plus efficaces les échanges entre assureurs ou réassureurs tout au long de la vie d'un contrat. Les inefficacités identifiées sont de plusieurs ordres et notamment : données incohérentes, fausses ou non partagées entre les différents acteurs (assuré, assureur, courtier, réassureur), traitement

[59] https://www.bcg.com/fr-fr/publications/2018/first-all-blockchain-insurer.aspx , consulté le 11/11/2021

de ces données par des intermédiaires avant transmission (source de coûts et d'erreurs), délais importants dans le placement d'un risque ou la gestion d'un sinistre. En connectant l'ensemble des acteurs à une même chaîne, l'information est partagée en temps réel et non dupliquée. Le même type de services et de gains dans les coûts de gestion sont proposés par la start-up Blocksure[60].

Autre illustration : la société Stratumn a accompagné quatorze assureurs du groupe de travail blockchain de la Commission numérique de la Fédération française de l'assurance (FFA) autour d'un projet d'échange de données entre assureurs, dans un objectif de réduction des coûts mais aussi de facilitation de la résiliation des contrats d'assurance automobile et habitation, permise par la loi Hamon[61].

2. Les produits d'assurance

Assurance à la demande/microassurance : Le développement de l'assurance à la demande ou pay as you go sera facilité par l'outil blockchain et la connexion à la chaîne d'outils divers comme la voiture, le logement, l'équipement ménager, etc.

Ceci devrait favoriser l'émergence d'un marché de la micro-assurance dont la caractéristique est de couvrir des besoins précis sur une durée déterminée, généralement courte (la voiture le temps d'une location, un équipement ménager le temps d'une utilisation, des biens le temps d'un voyage, etc.).

Assurance pair à pair ou collaborative[62] : La blockchain met les membres d'un réseau en lien les uns avec les autres, soit de façon universelle, soit en sous-groupes constitués en DAO, Ces sous-groupes peuvent pratiquer l'auto assurance : les « primes » versées par chaque membre du groupe servent à couvrir les sinistres des autres membres, le cas échéant via l'exécution d'un smart contract, selon des règles définies entre ces membres.

La start-up Dynamis propose ainsi une assurance-chômage collaborative reposant sur le protocole Ethereum et sur un oracle constitué du réseau LinkedIn, qui permet de vérifier la situation professionnelle des membres de la communauté. La nature juridique de la

[60] www.blocksure.com, consulté le 11/11/2021
[61] « Stratumn veut sécuriser les relations entre assureurs », Banque & Stratégie, n°368, avril 2018, p. 26-27
[62] Vamparys X., « La blockchain au service de la finance : Cadre juridique et applications pratiques », Op cit.

communauté et l'encadrement de ce type d'assurance comportent encore de nombreuses incertitudes.

La start-up Teambrella fonctionne sur le même principe de mutualisation des risques entre pairs. Elle a testé des produits de couverture des risques liés aux bicyclettes, voitures et animaux. Les dirigeants de la start-up considèrent que leur modèle d'affaires ne nécessite aucun agrément dans la plupart des pays et que la réglementation constitue un « obstacle à la disruption du secteur de l'assurance ». Par conséquent, ils indiquent que leur plateforme ne propose pas de produits d'assurance, mais offre une solution permettant de s'en dispenser.

Dernière illustration la plateforme Yakman qui permet la constitution de communautés qui s'auto-assurent. Cette plateforme précise également que les contrats mis en place ne constituent pas des produits d'assurance mais une mise en commun de fonds.

On retiendra que les diverses initiatives en matière d'assurance collaborative (assurance santé, assurance responsabilité civile) pourraient utilement s'appuyer sur la blockchain pour se développer. Ces initiatives qui sont souvent l'œuvre de start-up doivent interroger les compagnies d'assurance : est-il opportun qu'elles se proposent de les « faciliter » (réassurance, gestion des contrats par exemple) ? Ou doivent-elles développer une offre d'assurance « affinitaire », au sens originel de ce mot, c'est-à-dire au profit de groupes de personnes partageant un centre d'intérêt ou une activité (motards, cyclistes, voyageurs, golfeurs, etc.) ? Et selon quelles modalités : seules ou en partenariat avec des start-up ?

Pour certains auteurs, l'assurance collaborative se résume à la constitution une cagnotte » et n'est pas à proprement parler une activité d'assurance. Pour d'autres, il s'agit d'un retour «aux prémices de l'assurance, au temps des tontines et du prêt à la grosse aventure » en l'absence de transfert de risques, risques pris en charge par une communauté sans personnalité morale. La qualification juridique de cette activité et des communautés qui l'exercent este donc incertaine.

Assurance indicielle ou paramétrique[63] : Le smart contract le plus connu en matière d'assurance est le contrat « Fizzy » proposé par Axa, Les souscripteurs de ce contrat sont couverts contre tout retard de leur vol de plus de deux heures, quelle qu'en soit la cause. Si le

[63] https://www.axa.com/fr/newsroom/actualites/axa-se-lance-sur-la-blocchain-avec-fizzy, consulté le 11/11/2021

retard est constaté, le remboursement du billet est automatique et instantané, c'est-à-dire sans que l'assuré ait à engager une quelconque démarche. Le montant de l'indemnisation est par ailleurs connu par avance. En termes techniques, le contrat, qui repose sur la chaine Ethereum, est connecté à un oracle, en l'espèce un fournisseur de données sur l'état du trafic aérien mondial. Le paiement est effectué via un prestataire spécialisé.

Ce produit appartient à la famille de l'assurance « paramétrique » ou « indicielle », qui automatise une indemnisation dès lors qu'un paramètre ou un indice est atteint. Cette automaticité s'accommode très bien du mode de fonctionnement des smart contracts.

Axa est un acteur important dans ce domaine, ayant développé une assurance contre les risques climatiques pour les agriculteurs, notamment dans les pays en voie de développement. Cette couverture permet de sécuriser les revenus des agriculteurs qui sont indemnisés automatiquement dès lors que certaines données météorologiques (vitesse du vent, pluviométrie, etc.) sont objectivement constatées. Cette couverture semble, pour Axa, déclinable à toutes les activités économiques sensibles aux variations météorologiques (transport et énergies renouvelables par exemple). Elle est aujourd'hui en capacité d'utiliser « des données satellitaires de haute résolution permettant de mesurer l'humidité des sols ou le développement des plantes lui permettant ainsi de fournir une couverture d'assurance fondée sur des indices météo ou de croissance de la végétation »

On pourrait également imaginer d'autres types de couvertures individuelles donnant droit à une indemnisation dès lors que certaines mesures captées par des objets connectés, sur l'état de santé d'un porteur de risques ou son activité physique par exemple, ou encore sur l'état d'un véhicule accidenté (déclenchant l'intervention d'une dépanneuse ou la location d'un véhicule de remplacement), sont constatées .Ainsi, à Singapour, Metlife teste une couverture d'assurance contre le risque de diabète gestationnel qui repose sur un smart contract déclenchant un paiement vers l'assurée dès que le diabète est diagnostiqué.

En dehors d'Axa, plusieurs assureurs proposent une assurance « retard de vol ». On citera notamment les sociétés Policypal à Singapour ou Etherise 20 au Royaume-Uni.

Assurance internationale. En matière de police d'assurance internationale, l'utilisation de la blockchain entre les divers assureurs qui contribuent à la couverture (dans un exemple simple, un assureur par pays) permet un partage d'informations en temps réel, contribuant de

la sorte à une meilleure gestion du contrat. AIG a ainsi testé une solution blockchain proposée par IBM pour ce type de produits[64].

Innovation en matière de produits. La blockchain créé globalement un écosystème propice à l'innovation en matière de produits d'assurance. C'est ce qu'essaie d'exploiter la start-up Aigang Network[65] en proposant aux experts ou plus globalement aux personnes intéressées par l'assurance de partager leurs idées en matière de produits innovants. Ce partage va de la prédiction sur l'usage d'un produit d'assurance à la tarification et la profitabilité de ce produit. Si le produit est rentable, ceux qui en sont à l'origine en touchent les fruits via les tokens émis par la plateforme. Aigang a ainsi mis sur le marché une assurance contre l'obsolescence des batteries de téléphones portables qui repose sur un smart contract et un logiciel chargé dans le téléphone mesurant l'état de la batterie. En dessous d'un certain seuil, l'indemnisation est déclenchée automatiquement. Aigang souhaite prochainement lancer des produits d'assurance dans le domaine des drones et des voitures sans chauffeur.

Autre illustration la société Buzzvault s'appuie sur la blockchain pour proposer une assurance qui prend précisément en compte les biens qu'une personne souhaite assurer, en temps réel à partir de l'inventaire qui en est fait par un outil vidéo permettant l'identification et l'estimation de la valeur des wens. Chaque assuré dispose ainsi d'un inventaire digitalisé de ses biens, biens qu'il peut choisir ou non d'inclure dans sa couverture d'assurance.

La société Monuma 24 offre une solution d'inventaire dématérialisé du patrimoine qui repose sur la blockchain, avec une expertise de la valeur des biens à partir de photographies. L'existence et la propriété des biens font T'objet d'une certification par l'enregistrement des photos sur la blockchain. Le patrimoine d'un propriétaire est ainsi répertorié et valorisé, ce qui est utile en cas de vol ou de sinistre.

En outre, la blockchain donnera naissance à des couvertures spécifiques pour l'activité qui lui est liée. C'est donc un nouveau marché qui s'ouvre pour les assureurs. On a ainsi pu

[64] « AIG teams with IBM to use blockchain for « smart » insurance police », The Business Times, 15 juin 2017
[65] https://aigang.network/ consulté le 11/11/2021

relever que XL Catlin avait fourni une police à la société BitGo, fournisseur de portefeuilles de crypto-monnaies sécurisés, contre le val de ces crypto-monnaies[66].

3. La réassurance [67]

Ce qui a été exposé ci-dessus en matière de partage d'informations et de rapidité d'exécution des contrats est applicable également au secteur de la réassurance. Ainsi, la plateforme conçue par le consortium B3i permet aux assureurs, réassureurs et courtiers d'enregistrer sur une chaîne toutes leurs opérations contractuelles relatives à des couvertures « catastrophes naturelles », avec un accès différencié à l'information en fonction de la participation ou non d'un acteur à telle ou telle opération.

En matière d'obligations « catastrophes» (ou cat bonds) qui permettent aux assureurs ou réassureurs de transférer à des investisseurs tout ou partie des risques de catastrophe naturelle qu'ils ont accepté de couvrir, la blockchain a déjà pu être testée par le groupe Allianz pour la négociation des obligations et l'exécution de leurs conditions contractuelle via des *smart contracts*.

Conclusion

Le secteur financier s'est rapidement intéressé à la blockchain. Ses acteurs, banquiers, assureurs ou intermédiaires, ont commencé à étudier de réelles perspectives de projection de ces nouvelles technologies dans leurs différents services (KYC, Reporting et lutte contre la fraude pour les acteurs du secteur financier, service de financement, de paiement et d'investissement pour les banques, assurance et réassurance pour les assurances).

Selon un rapport de la banque Santander, l'utilisation de la blockchain pourrait être source d'économies pour le secteur bancaire, estimées à 15 à 20 milliards de dollars par an d'ici 2022

[66] https://bitcoinmagazine.com/articles/breaking-news-bitgo-unleashes-fdic-likes-insurance-ushering-new-era-bitcoin-security-1424894391/ consulté le 18/11/2021
[67] S. Acedo, « La blockchain expérimentée dans la titrisation des risques », l'Argus, 15 juin 2016

grâce à la réduction des coûts d'infrastructure liés aux paiements internationaux, au *trading* et à la mise en conformité[68].

Le secteur de l'assurance aussi s'intéresse de plus en plus à la blockchain, comme illustre une étude de PwC, si en 2016 seuls 17 % des assureurs reconnaissaient un intérêt à cette technologie, 2017[69].

D'après les statistiques et les données collectées, les acteurs du secteur financier, sont actuellement dans une démarche d'étude d'une potentielle utilisation de la technologie de la Blockchain et des crypto monnaies dans ce secteur, et ce pour ce qu'elle offre comme avantages et ce qu'elle pourrait apporter à l'économie.

[68] Vamparys X., « La blockchain au service de la finance : Cadre juridique et applications pratiques », édition RB, Paris, 2018

[69] https://www.pwc.com/gx/en/financial-services/finetech/assets/fintech/assets/fintech-2-0-insurancepdf consulté le 18/11/2021

Conclusion générale

Conclusion générale :

L'évolution technologique, et surtout l'avènement de l'internet, a conduit à la création et à l'émergence d'une nouvelle forme de monnaie : la monnaie virtuelle ou digitale, baptisée aussi cryptomonnaie ou monnaie numérique. Les monnaies électroniques, sont crées à partir d'un protocole cryptographique de pair à pair, donc sans banque centrale, comme c'est le cas habituellement.

La volonté de ses créateurs est de donner naissance à une monnaie échappant au contrôle des Etats et des banques centrales, selon eux, origine de tous les maux et de toutes les crises. En d'autres termes, selon une vision libertaire, les adeptes des cryptomonnaies voient, dans la fin du monopole des banques centrales sur l'offre de la monnaie et la débancarisation, l'assurance que les citoyens se réapproprient leur devise. Et que cette dernière échappe à toutes les règles monétaires traditionnelles qui sont derrière les multiples crises financières qui ont bouleversé l'histoire.

La création d'une monnaie virtuelle ou d'une monnaie chiffrée, vient donc d'une idée de créer et d'utiliser une monnaie sans autorité de confiance, de pouvoir vérifier soit même le bon déroulement de la création monétaire et de concevoir un mécanisme qui permet d'enregistrer de manière distribuée des informations dans un registre irréversible et vérifiable par tous ses utilisateurs, qui a été appelé « blochchain ».

Ainsi, cette technologie, apportant plus de transparence, de fiabilité et de rapidité, pourrait entrainer la disparition de certains intermédiaires dont l'utilité est remise en question en raison du lien direct crée par la blockchain entre acteurs économiques et clients et entre clients eux-mêmes.

Aujourd'hui, l'utilisation d'une telle technologie permettrait aux banques et autres acteurs du secteur financier de monter sur la vague d'innovation, de survivre à la désintermédiation et de regagner la confiance des clients et en tirer les multiples avantages qu'elle offre, au service d'une efficacité renforcée, d'une maîtrise des coûts et d'une plus grande pertinence dans les produits et services proposés à leurs clients, ça confirme notre première hypothèse sur la possibilité de projection des technologies de la blockchain et des crypto monnaies dans le secteur bancaire et financier.

D'ailleurs, huit banques européennes ont récemment annoncé vouloir créer une coentreprise en vue de lancer une plateforme commerciale en ligne, reposant sur la

technologie Blockchain. Il s'agit de Deutsche Bank, de Natixis, de KBC, de Rabobank et de HSBC. Société Générale, Banco Santander et Unicredit rejoignent également la liste[1].

Cependant, les caractéristiques des crypto monnaies comme la volatilité, la décentralisation et la difficulté de suivre les traces des utilisateurs soulèvent de plus en plus la question de danger de leur application dans un secteur sensible tel que le secteur financier. Néanmoins, l'étude de cette technologie a montré qu'en matière de sécurité, les limites techniques liées à sa modernité rendent sa menace pour les banques a priori assez limitée à court terme, en particulier, seules sept transactions par seconde maximum sont aujourd'hui possibles sur toute la blockchain Bitcoin, loin des milliers du réseau Visa.

Par ailleurs, la volatilité, peut rendre complexe leur utilisation dans un certain nombre d'opérations financières dans la mesure où les atouts de la blockchain se composent d'une réduction des délais de transaction et d'une réduction des coûts, ne pas pouvoir s'assurer de la stabilité de la monnaie peut obliger à des surcoûts importants qui menacent cet avantage. Cependant là encore, des solutions pour couvrir ce risque sont en cours de développement, par exemple à base de *smart contracts*, ça infirme notre hypothèse liée au danger que peut présenter cette technologie en cas de son application dans le secteur bancaire et financier.

[1] Les banques optent pour la technologie Blockchain - MeilleureBanque.com (meilleurtaux.com), consulté le 01/12/2021.

Références bibliographiques

1. Ouvrages :

- RUIMY Michel, DEMBIK Christopher, « La monnaie, fonctions, mécanismes et évolutions », édition ellipses, Paris, 2017
- SERVAL Jean-François, TRANTE Jean-Pascal, « Monnaie virtuelle qui nous fait vivre, l'économie à l'épreuve de l'innovation financière », édition EYROLLES, deuxième tirage, Paris, 2011.
- DE FILIPPI Primavera, « Blockchain et cryptomonnaies », Que sais-je ?, Paris, novembre 2012.
- DUMAS J.G, LAFOURCADE P, TICHIT A, VARRETTE S, « Les blockchains en 50 questions », édition Dunod, Paris, 2018
- VAMPARYS Xavier, « La blockchain au service de la finance : Cadre juridique et applications pratiques », édition RB, Paris, septembre 2018.

2. Revues, périodiques et rapports:

- Delahaye Jean Paul, « Les preuves de travail » revue Pour la science, N°60, Avril 2014, consulté en ligne sur (www.pourlascience.fr) le 20/11/2021.
- Interview de P. Denis « il faut déceler les cas d'usage les plus pertinents de la blockchain », revue Banque, n°811, 30/08/2017 (http://www.revue-banque.fr/revue-banque/numero-811), consultée en ligne le 29/11/2021
- W. Davtian, « Blockchain et assurance : espérance démesurée ou nouvelle ère », Revue Banque & Stratégie, n° 369, mai 2018, p. 33-38
- S. Leboucher, « blockchain, la banque de France entre entre en production, revue Banque, n° 811, 30/08/2017(http://www.revue-banque.fr/revue-banque/numero-811), consulté en ligne le 29/11/2021.
- « Stratumn veut sécuriser les relations entre assureurs », Banque & Stratégie, n°368, avril 2018, p. 26-27.
- Communiqué de presse, « Liquidshare, la fintech blockchain européenne pour le post-marché des PME, est lancée », Société Générale, 11 juillet 2017.
- Communiqué de presse Banque de France « La banque de France mène une expérimentation de blockchain interbancaire » 15 décembre 2016.

- Communiqué de presse Euler Hermes, consulté en ligne (www.eulerhermes.fr) le 27/11/2021.
- D. Cuny « La caisse des dépôts teste la blockchain dans le prêt de titres », La Tribune, 4 novembre 2016.
- « AIG teams with IBM to use blockchain for « smart » insurance police », The Business Times, 15 juin 2017.
- S. Acedo, « La blockchain expérimentée dans la titrisation des risques », l'Argus, 15 juin 2016.
- R. Bloch, Goldman Sachs prêt à investir dans les cryptomonnaies », Les Echos, 3 mai 2018, (www.lesechos.fr) le 29/11/2021.
- Interview de B. Denis « la blockchain dans le secteur de l'assurance », Wolters Kluwer, 21 septembre 2017.

3. Loi et règlements :

- Ordonnance n° 2014-559 du 30 mai 2014 relative au financement participatif du droit français.
- Règlement UE n° 2015/2365 relatif à la transparence des opérations de financement sur titres et de la réutilisation (Securities Financing Transactions Regulation ou SFTR), 23 décembre 2015. Consulté le 26/11/2021.

4. Thèses et mémoires :

- SIDHOUM Nacira, « La crypto-monnaie : Emergence, Enjeux et Perspectives », mémoire de fin d'études en vue d'obtention du diplôme de Master option économie monétaire et bancaire, Université Mouloud MAMMERI, 2018/2019.
- MOUAZER Abdelmalek, CHEKINI Sabrina, « Les cryptomonnaies, au-delà de la dématérialisation des moyens de paiement, cas d'Algérie », mémoire de fin d'études en vue d'obtention du diplôme de Master filière techniques bancaires et monétaires, Université Mouloud MAMMERI 2016/2017

5. Sites Web :

- www.gsam.com, consulté le 14/11/2021
- www.cryptokemet.com, consulté le 25/11/2021
- www.lamineauxinfos.fr, consulté le 22/11/2021

- www.crypto-monnaies.xyz, consulté le 22/11/2021
- www.astuces-aide-informatique.info, consulté le 02/11/2021.
- www.journalducm.com, consulté le 06/11/2021
- www.pouruneautreeconomie.fr, consulté le 06/11/2021
- www.corporatefinanceinstitute.com, consulté le 25/11/2021
- www.infolegale.fr; consulté le 25/11/2021
- www.skaizengroup.eu, consulté le 25/11/2021
- www.microsoft.fr, consulté le 25/11/2021 à 17h50
- www.acpr.banque-france.fr , consulté le 26/11/2021
- www.societegenerale.com , consulté le 29/11/2021
- www. journaldunet.com, consulté le 01/12/2021
- www.blockchainsexpert.com, consulté le 01/12/2021
- www.bitcoinisle.com, consulté le 29/11/2021
- www.allianz.smartangels.fr, consulté le 02/12/2021
- www.caissedesdepots.fr, consulté le 02/12/2021
- www.bitbond.com, consulté le 02/12/2021
- www.utocat.com, consulté le 02/12/2021
- www.coindesk.com, consulté le 02/12/2021
- www.crypto-france.com, consulté le 03/12/2021
- www.tobam.fr, consulté le 03/12/2021
- www.trecento-blockchain.capital, consulté le 03/12/2021
- www.isda.org, consulté le 03/12/2021
- www.the--blochchain-com.cdn.ampproject.org 03/12/2021
- www.pwc.com, consulté le 03/12/2021
- www.axa.com, consulté le 03/12/2021
- www.aigang.network, consulté le 03/12/2021

Lexique

Bitcoin (BTC) : crypto-monnaie créée en 2009 qui fonctionne grâce à la blockchain et constitue un moyen de paiement pair à pair. Lorsque le terme bitcoin est utilisé avec un «b» minuscule, il désigne la crypto-monnaie, avec un B» majuscule le protocole Bitcoin.

Bloc : regroupement de transactions et d'informations validées ensemble et ajoutées à une chaîne avec l'identifiant numérique du bloc précédent.

Blockchain ou chaîne de blocs: technologie qui sert de support à la tenue de registres partagés en ligne, distribués auprès des membres d'un réseau qui en sont les gardiens, registres portant sur des informations ou opérations stockées indéfiniment et de façon intangible.

Chiffrement ou cryptographie asymétrique : méthode de chiffrement qui repose sur la distinction entre une clé publique, partagée, et une clé privée, connue de son seul propriétaire, par opposition au chiffrement symétrique ou une clé privée est partagée par plusieurs personnes.

Consensus: règles de validation des opérations ou informations d'une chaine de blocs définies par le protocole qui lui est applicable. Les règles de consensus les plus courantes sont la preuve de travail (proof of work) et la preuve d'enjeu (proof of stake).

Crypto-actif: terme équivalent à celui de jeton ou token.

Crypto-monnaie : application la plus populaire de la blockchain qui fonctionne comme un moyen de paiement conventionnel. Le bitcoin est la crypto monnaie la plus connue. Dans le cas du bitcoin, la crypto-monnaie est émise pour rétribuer les mineurs.

Ether (ETH) : crypto-monnaie qui fonctionne grâce à la blockchain Ethereum.
Ethereum: au sens large, plateforme blockchain qui permet notamment la création de smart contracts, avec un langage simplifié, Solidity. Au sens strict, protocole qui régit la chaîne. C'est vraisemblablement la blockchain la plus utilisée par les développeurs.

Fork: création d'une nouvelle branche sur une chaîne qui résulte d'un désaccord entre membres de la chaîne.

Hachage : fonction cryptographique utilisée pour sécuriser les chaines de blocs et qui a la particularité de ne pas donner de résultats prédictibles. Dans le cas du bitcoin, la fonction retenue pour le minage est la fonction SHA-256.

ICO ou initial Coin Offering: offre de jetons à des investisseurs.

Mineur : ordinateur ou ensemble d'ordinateurs connectés au réseau qui mettent leur puissance de calcul au service de la validation des transactions d'une blockchain et dont les propriétaires sont rémunérés pour les tâches ainsi effectuées, par de l'émission de crypto-monnaies et des commissions dans le cas du bitcoin.

Nœud : ordinateur ou ensemble d'ordinateurs connectés au réseau qui participent à la validation et la conservation des données partagées. Chaque nœud détient une copie de la blockchain. Les nœuds ne sont en principe pas rémunérés pour le travail effectué au profit de la chaine, alors que les mineurs le sont.

Open source : s'agissant d'un code ou d'un protocole, signifie qu'il peut être librement copié et utilisé.

Pair à pair : réseau dans lequel les utilisateurs peuvent communiquer ou échanger des données ou valeurs sans intermédiaire.

Preuve d'enjeu ou proof of stake : mode de validation des blocs qui repose sur un tirage au sort du mineur récompensé, mais où chaque membre de la chaine a une chance d'être désigné proportionnelle à son intérêt dans la chaine.

Preuve de travail ou proof of work : mode de validation des blocs qui repose sur une récompense du mineur qui aura résolu des énigmes mathématiques complexes le plus rapidement.

Protocole : ensemble des règles qui gouvernent une blockchain. Smart contract : programme informatique permettant l'exécution automatique de stipulations contractuelles lorsque certaines conditions sont remplies.

Token : représentation numérique de valeur émise par des sociétés ou des communautés d'utilisateurs dont la fonction varie: instrument de paiement, souscription à un service, quote-part d'un bien ou investissement par exemple. Les crypto-monnaies sont un type particulier de jeton, à la fois actif et représentation numérique de cet actif.

Wallet : portefeuille électronique permettant de stocker des crypto-monnaies, souvent sous forme d'une simple clé cryptographique.

Whitepaper : document d'offre utilisé dans les ICO.

Liste des figures

Table des matières

Table des matières

Table des matières

Table des matières

Résumé

L'innovation financière a entrainé la création d'une immense quantité d'argent non contrôlée par les banques centrales appelées « les crypto monnaies », une monnaie qui circule virtuellement sur un réseau appelé « blockchain », un registre de transactions distribué, une base de données décentralisée qui repose sur un réseau pair à pair destiné au stockage et au transfert de données.

Aujourd'hui, alors que leur valeur est passée de quelques centimes en 2009 à des milliers d'euros, les crypto monnaies sont considérées par certains comme une menace et reconnues par d'autres comme une occasion de renouveler le système financier.

Cette nouvelle technologie intéresse désormais les banques, les assurances et les autres auteurs du secteur financier qui tentent de monter sur la vague d'innovation pour survivre à la désintermédiation et pour regagner la confiance des clients et en tirer les multiples avantages qu'elle offre au service d'une efficacité renforcée, d'une maîtrise des coûts et d'une plus grande pertinence dans les produits et services proposés à leurs clients.

Mots clés :

Blockchain, registre de transactions, innovation financière, innovation technologique, monnaie, monnaie numérique, monnaie virtuelle crypto monnaie, cryptographique, système de paiement, banque, confiance, unité de compte, réserve de valeur, moyen de paiement, système décentralisé, anonymat, pair à pair.

Abstract

Financial innovation has led to the creation of a huge amount of money not controlled by central banks called "cryptocurrencies", a currency that circulates virtually on a network called "blockchain", a distributed transaction register, a decentralized database based on a peer-to-peer network for data storage and transfer.

Today, while their value has gone from a few cents in 2009 to thousands of euros, cryptocurrencies are considered by some as a threat and recognized by others as an opportunity to renew the financial system.

This new technology interest now banks, insurance companies and the other authors in the financial sector who are trying to ride the wave of innovation to survive disintermediation and to regain customer trust and reap the multiple benefits it offers in the service of increased efficiency, cost control and greater relevance in the products and services offered to their customers.

Word keys :

Blockchain, transaction register, financial innovation, technological innovation, currency, digital currency, cryptocurrency, cryptographic, payment system, bank, trust, unit of account, value reserve, means of payment, decentralized system, anonymity, peer to peer.