Le bitcoin : une nouvelle forme de monnaie ; fruit de la cryptographie

البيتكوين: شكل جديد من المال. ثمرة التشفير

SIAMER Hadjira

Maitre de conférences « B », Université MOULOUD MAMMERI Tizi-Ouzou

siamerhadjira@gmail.com

Received: 06/09/2019

Accepted:02/10/2019

Published:01/01/2020

Résumé

A mesure que se développe la notion fiduciaire, elle se détache peu à peu de celle d'une monnaie adossée à une institution financière ou bancaire, ayant un pouvoir d'achat déterminé. C'est une des étapes de la dématérialisation de la monnaie, et c'est dans ce contexte que le bitcoin est apparu ; a la fois pour réduire le rôle de l'état en matière de fonction monétaire, et pour montrer les progrès que la cryptographie a connu.

Bitcoin en tant que première devise privée a largement ouvert la voie a de nouvelles applications en particulier il peut fortement améliorer l'efficacité du transfert d'argent la ou il y'a le plus besoin, sans passer par des intermédiaires qu'ils soient bureaucratiques ou bancaires.

Mots clés :

Monnaie fiduciaire, bitcoin, cryptographie, monnaie privée, technologie d'information et de communication

Auteur correspondant: Nom et Prénom, Email: auteurC@mail.com

1- Introduction

La monnaie s'est historiquement présentée sous des formes très variées. À l'origine de toute société se trouve une phase où la monnaie s'est présentée sous forme de pièces contenant un poids défini de métal précieux (or ou argent en général). Après une domination de plusieurs siècles ces métaux reculent devant le billet de banque, d'abord convertible puis inconvertible, pour qu'elle devienne une simple inscription sur le registre d'une banque ou d'un service tel que les chèques postaux.

On n'en n'est pas fini ; avec l'avènement de la technologie d'information et de communication et leur introduction dans le secteur bancaire, la monnaie a connu une nouvelle forme électronique contribuant à l'élargissement des moyens de paiement.

Pour cela n'importe quelle mutation monétaire frappée assurant les fonctions de la monnaie (unité de compte ; réserve de valeur, et en état actuelle, instrument politique) est déclarée comme une forme de monnaie

2- Définition de bitcoin

Le bitcoin est une monnaie décentralisée partiellement anonyme sans qu'elle soit soumise à la tutelle d'aucune banque, utilisant à la place, la cryptographie pour la création et le transfert de monnaie, c'est un fichier numérique contenant un registre de la totalité des transactions.

De cette définition on peut déduire des avantages les plus importants de bitcoins qui se résument dans l'inexistence de responsable, et de réserve ; ce qui implique la suppression des coûts de transactions utilisant des méthodes cryptographiques.

Le système mis en place depuis 2009 possède les propriétés suivantes :

- Des nouveaux utilisateurs (comptes) peuvent s'introduire à chaque instant ou se retirer ;

- Les utilisateurs ne sont pas tous contraints de suivre une à une les Operations faites d'un compte a un autres ;
- Les Operations peuvent être plus complexes que le seul versement d'une somme d'argent de compte a compte ;
- Un change flottant de l'unité de compte (le bitcoin) permet a sa valeur d'évoluer : aucune valeur n'est attribuer au départ au bitcoin ; celle-ci s'établit progressivement, puis une fois adoptée, évolue en fonction de l'offre et de la demande ;
- Les pannes de certaines machines de réseau, la coupure et même l'isolement de certaines parties du réseau, de longs délais de transmission entre nœud du réseau, le désaccord de certains nœuds, les tentatives de tricheries (par exemple les doubles dépenses) n'auront pas d'effet sur le fonctionnement général du système.

3- Apparition de bitcoin

3-1- Pourquoi le bitcoin a-t-il vu le jour

La norme monétaire est parfaite lorsque aucune ambiguïté ne pèse sur aucune des fonctions de la monnaie citée auparavant, une telle configuration ne saurait être au mieux qu'éphémère parce que la norme monétaire est porteuse d'une extrême contrainte sur tous les acteurs et leurs stratégies, elle fait l'objet des tentatives afin d'échapper à la rigueur de sa loi.

En effet certains agents peuvent thésauriser la monnaie ou chercher à réaliser leurs échanges sans avoir recours a la monnaie, et cette possibilité d'une altération endogène des règles monétaires s'est imposée a partir de l'observation des crises économiques et l'augmentation des couts.

Le bitcoin est apparu pour tenter d'unifier la monnaie qui a pour cible les conditions d'accès à la monnaie qu'il cherche a transformer au niveau des

intérêts des uns et des autres et qui peut conduire à l'éviction de la monnaie ancienne et à son remplacement par une monnaie universelle. Il nous sera possible de penser les transformations monétaires comme des évolutions endogènes à travers lesquelles se trouve exprimée l'essence même d'un rapport monétaire, ces évolutions et ces inachèvements sont une conséquence du caractère violent des relations marchandes et du fait que cette violence ne disparaît jamais. Et l'émergence d'une monnaie unanimement reconnue ne signifie pas l'éradication de la violence mais son extériorisation en un principe médiateur. Considérons les transactions monétaires de base à savoir les ventes et les achats de marchandises et leur fonctionnement idéal met en jeu les trois fonctions de la monnaie : il suppose que les prix de marchandises soient déclarés en monnaie (unité de compte), que l'acquisition de marchandises se fasse à l'apport d'argent (moyen de circulation) et que les encaisses monétaires soient détenues jusqu'à la prochaine transaction (moyen de réserve).

3-2- La création de bitcoins

En 2008 un certain Satoshi Nakamoto, publia un article de recherche dans un mailing list concernant la cryptographie dont le titre : bitcoin : a peer to peer . En particulier ce concept ou autrement dit « preuve de travail » c'est un programme ou un travail informatique doit être résolu par un ordinateur pour valider une tâche. Utilisant la cryptographie dans la création des signatures non falsifiable et implémenter des fonctions à sens unique. Autrement dit il est tout à fait possible à tout un chacun de consulter le registre des transactions ayant eu lieu. Ce programme sert à la fois de résoudre le problème du double paiement et garantit l'identité des participants.

Ces améliorations faisant passer du model simplifié au model réel de bitcoin se fondent sur une série de protocoles particuliers qui font la nouveauté du système des bitcoins et qui aboutissent a un montage subtil et complexes –si non il aurait été inventé bien avant –mais qui rend la monnaie bitcoin résistante a toute sorte de dysfonctionnements en même temps qu’a toute sorte de tentatives de manipulation de la monnaie.

Toute fois la création de nouveaux bitcoins n’a rien avoir avec celle des monnaie classique ; la masse monétaire ne s’adapte pas a la richesse échangée par son biais ; il se rapprochait plutôt a des métaux précieux comme l’or ; ce qui a poussé certain a définir le bitcoin comme l’or numérique, ils sont émis de manière régulière a chaque validation d’un nouveau bloc de transaction.

4- Est-il rare comme l’or

Le nombre de bitcoin créés à chaque validation diminue dans le temps. A l’origine du système 50 bitcoins étaient créés a chaque validation d’un bloc ; autrement dit toutes les dix minutes, et qui se fait par un processus cryptographique qui en assure la parfaite et surtout une totale imprévisibilité et infalsifiable. Ce tirage au sort se fait selon un procédé qui donne d’autant plus de chance de gagner en disposant de plus de puissance de calcul.

Cette puissance nécessaire pour gagner fait qu’il devient impossible même pour un acteur très puissant de s’emparer de tous les gains .l’analyse générale du protocole des bitcoins , effectuée des 2008 par Nakamoto , montre précisément que si un acteur pouvait disposer de la moitié de la puissance consacré au minage , alors il serait en mesure de perturber gravement le fonctionnement de la monnaie bitcoin .l’accroissement des efforts faits pour miner des bitcoin rend de plus en plus difficile de réunir ces 50% , et indirectement renforce donc la monnaie bitcoin . Le système conçu par Nakamoto se consolide au fur et a mesure que des

gens s'y intéressent : plus le cours de biton monte, plus il devient intéressant de miner des bitcoins ; plus nombreux sont ceux qui minent, plus le bitcoin devient robuste y compris aux attaques d'acteurs très puissants, et donc plus son cours a des chances de monter. Ajoutant a cela que le bitcoins ou plutôt le fichier est programmé afin que son nombre soit divisé par deux tous les quatre ans ; et ce jusqu'à finir par être nul. D'ici quelques années (en 2040). À cette date le nombre de bitcoins en circulation sera de 21 millions, et plus aucun bitcoin ne sera plus et ne pourra plus jamais être créé.

De ce fait le bitcoin est en théorie pas enclin à subir une inflation, et une forte déflation des prix ne ferait que limiter le bitcoin a un rôle de réserve de valeurs plus pratique que l'or. En fait la déflation des prix n'aurait de conséquences économiques néfastes que si les bitcoins étaient la monnaie exclusive d'une aire géographique donnée. Cela n'est absolument pas le cas puisqu'en tant que monnaie complémentaire, les bitcoins coexistent avec la monnaie locale sponsorisée par l'état.

5- La gestion de bitcoins

Contrairement à l'idée naïve qu'on pourrait se faire d'une monnaie virtuelle, un bitcoin ne dispose pas d'un porte monnaie sous forme d'un fichier ou dossier. À la place il accède à un registre qui est un grand livre de compte public, consignait toutes les transactions en bitcoins ayant lieu depuis la mise en place du protocole, c'est a partir de ce registre qu'il peut calculer sa fortune personnelle.

A tout instant chacun peut savoir combien ya-t-il de bitcoins sur chaque compte existant, et participer a la vérification des nouvelles transactions, tout en respectant l'anonymat des mineurs qui ne sont pas tenus à se déclarer. Donc il ne tient que par la cohérence et l'accord général et unanime de ceux qui y participent et s'entendent sur le contenu de chaque compte que rien ne le matérialise, et qu'aucune autorité ne garantit .il faut donc que la construction logicielle

cryptographique assure par elle-même que personne ne peut augmenter le total des bitcoins détenus, ni modifier des comptes sans que tout le monde le découvre dans un délai très court, il n'y a pas de police, la conception même de la monnaie doit empêcher seule la fraude et les dysfonctionnements. Il est géré collectivement sous l'intervention du programme cryptographique qui contient deux clés :

Une clé publique qu'on peut laisser circuler (c'est le numéro de compte)

Et une clé privée qui doit absolument rester secrète (c'est le mot de passe pour accéder au mouvement des comptes) qui constitue une série de chiffres et de lettres difficile à retenir en effet certains mineurs préfèrent gérer le compte à l'aide d'un logiciel « wallet ». et si l'une des deux clés s'efface par mégarde ; alors son contenu sera définitivement perdu, et si une autre personne connaît ces clés, elle peut s'en servir du fait que l'identité des mineurs n'est utile à aucun moment, il faut donc que la construction logicielle cryptographique assure par elle-même que personne ne peut augmenter ni modifier le total des bitcoins détenus. La conception même de la monnaie doit empêcher seule la fraude et les dysfonctionnements.

6- Le déroulement d'une transaction

Si une personne (A) souhaite transférer des bitcoins qu'elle dispose pour une autre personne (B) ; un échange de messages sécurisé par des signatures électronique, est évident.

La personne (B) communique sa clé publique à la personne (A) qui construira un message constituant le montant (N) de bitcoins ; et qui donne son accord pour effectuer ce transfert tout en utilisant sa clé privée pour la signer.

6-1- La sécurisation du registre des transactions

Pour éviter une telle double dépense, l'idée centrale est de rendre coûteuse la validation d'une transaction (ou en réalité d'un bloc contenant les transactions

effectuées en une dizaine de minutes). Ainsi un mineur ne pourra pas aisément ajouter des transactions au registre et ainsi valider l'opération avec un autre mineur.

Pour expliquer ce mécanisme central de bitcoin, on a besoin d'introduire une nouvelle notion : celle de fonction de hachage qui est une opération qui consiste à transformer un texte de longueur arbitraire en un texte de longueur fixe. Dans le cas de bitcoin, une suite de 256bits, mais cette suite (appelée hash du texte) doit vérifier une propriété fondamentale : il est virtuellement impossible de créer un second texte avec le même hache.

Grace a ce mécanisme, mettre a jours le registre des transactions sera plus compliqué, plutôt que de simplement valider la transaction.

6-2- Et si le Protocole de signature du bitcoin était cassé ?

Si le protocole de signature venait d'être cassé et que quelqu'un disposant d'une clef publique $A_{(pub)}$ sache calculer facilement la clef privée associée $A_{(pri)}$, alors cette personne serait en mesure de dépenser le contenu de tous les comptes. A condition de le faire progressivement pour ne pas se faire repérer, et les détenteurs de comptes ne s'en apercevraient que lorsque, consultant la somme liée a leur compte (et dont allant lire la blockchain¹), ils découvriraient que leur compte est vide.

Cependant si la personne ne disposera pas du moyen pratique de calculer $A_{(pri)}$ a partir de $A_{(pub)}$, ou que si cela se produit, la faiblesse du protocole de signature aura été repérée avant qu'elle soit devenue réellement utilisable, et donc, que la communauté des développeurs bitcoin aura opéré a temps le changement de cette

¹ Blockchain est le fichier de compte de model simplifié .il ne sera pas modifié a chaque opération, mais seulement toutes les dix minutes .et qui est complété progressivement par ajout de nouvelles pages de transactions (nommés block).

partie du protocole bitcoin. La possibilité d'adapter est donc de corriger des faiblesses qu'on repérerait dans le protocole bitcoin. Mais cette éventuelle réparation d'une défaillance du protocole de signature n'est envisageable que si on s'en aperçoit.

7- Bitcoin contre la monnaie électronique :

La monnaie électronique est généralement définie comme une valeur stockée sous forme électronique émise après réception de fonds dans le montant ne doit pas être inférieur à la valeur de l'unité monétaire émise acceptée comme moyen de paiement par des tiers autres que l'émetteur. Dans le cadre de programme de monnaie électronique, le lien entre la monnaie électronique et la monnaie fiduciaire sur laquelle elle se base reste intact, et les fonds sont exprimés en unités de cette devise.

Dans un programme de monnaie virtuelle en revanche, l'unité de compte n'a aucune contre partie en monnaie fiduciaire.

En dehors du format numérique, il existe peut de similarité entre le bitcoin et la monnaie électronique. La monnaie électronique comme beaucoup d'autres formes numériques de monnaie fiduciaire comme les cartes de crédit et de débit, et les virements bancaires, est simplement un mécanisme permettant d'interagir avec cette monnaie fiduciaire. Afin d'atténuer les risques systémiques et les risques liés à la protection des consommateurs, un montant en espèces correspondant à la valeur de la monnaie électronique émise doit être déposé auprès d'une institution financière soumise à des règles prudentielles. Contrairement au bitcoin la monnaie électronique n'est pas une nouvelle monnaie et elle sous la supervision de la même autorité centrale que la monnaie nationale sous-jacente.

Tableau N° 1 : comparaison entre la monnaie électronique et le bitcoin

	Monnaie électronique	bitcoin
Format	numérique	numérique
Unité de compte	Monnaie fiduciaire	Bitcoin (BTC)
Identification des clients	Les normes des groupes d'action financière s'appliquent en matière d'identification des clients (elles prévoient toutefois des mesures simplifiées pour les produits a faible risque)	Anonyme
Moyen de production	Emission électronique par rapport a la monnaie fiduciaire d'une autorité centrale	Miné/généré mathématiquement
émetteur	Emetteur de monnaie électronique juridiquement constitué (peut être une institution financière)	Communauté de personnes mineurs

Source : données adoptées de banque centrale

européenne http://ec.europa.eu/internal_market/payments/emonney/text/index_.htm.

8- Le bitcoin est il une monnaie ?

Le système mis en fonctionnement, il ya 10ans tient solidement. Dans un premier temps, le cours de bitcoin était dérisoire ; il valait environ 10euros en janvier 2013 ; il atteint 200euro le 9 avril 2013 ; il a ensuite chuté. Et en décembre 2013 le bitcoin est monté jusqu'a près de 900 euros. Depuis il est revenu a 390 euros le 27 aout 2014. En effet certain ont fait d'excellentes affaires, soit en achetant quand le bitcoin ne valait rien, soit en minant les bitcoins quand c'était facile.

D'ou cette capacité de le convertir vers les autres monnaies qui a fait de lui une unité de compte.

En effet il est nécessaire de porter des analyses² qui tentent d'intégrer le bitcoin, et qui essaient de réconcilier deux réalités qui sont absolument contradictoires a savoir monnaie et valeur .Il s'agit de penser du bitcoin a partir des mêmes outils que ceux qui ont permis avec succès de rendre intelligibles les choix individuels en matière de détention de bitcoin à savoir la théorie de la valeur et le calcul marginaliste.

Cette démarche consiste à élargir l'approche wallisienne du consommateur pour y intégrer le bitcoin lui-même, autrement dit on se propose à traiter le bitcoin d'une marchandise comme les autres, c'est-à-dire un objet .pour ce faire il faut démontrer qu'il a une utilité.

Donc il est possible de faire entrer le bitcoin dans la fonction d'utilité au même titre que les marchandises, ce qui rend légitime le recours aux techniques habituelles de maximisation pour déterminer des demandes individuelles de bitcoin. Ce faisant du bitcoin fétichisé au sens que Marx donne a terme lorsqu'a propos des marchandises, il observe d'un rapport social déterminé des hommes entre eux.

Pour eux la forme fantastique d'un rapport des choses entre elles, en effet réduire la relation monétaire a la recherche individuelle d'une utilité intrinsèque, c'est avant tout refuser de voir le bitcoin, est d'abord une relation entre acteurs

² L'approche est inspirée de l'idée de don patinkin, l'une des plus intéressantes en ce qu'elle entreprend de reconstruire théoriquement d'une manière qui se veut absolument rigoureuse, il cherche pour reprendre son heureuse formule , une intégration de la théorie monétaire et la théorie des valeurs

économiques qui repose sur la confiance des mineurs et des attentes stratégiques, cette dimension sociale disparaît totalement derrière l'utilité.

9- De quelle utilité s'agit-il ?

Le bitcoin est utile d'une manière indirecte à travers son pouvoir de le convertir en d'autres monnaies et à travers les marchandises qu'il permet d'acquérir et qui sont directement utiles.

Mais nous nous intéressons à l'utilité de détenir des bitcoins et pas à l'utilité de les dépenser, donc son utilité découle de son aptitude à éviter les désagréments que causent temporairement la désynchronisation entre dépenses et recettes et la monnaie légale.

Cette désynchronisation qui se traduit par un manque provisoire de liquidité, dans cette optique le service de bitcoin ce serait donc la liquidité.

Dans un tel cadre l'utilité du bitcoin est pensée comme étant totalement indépendante du comportement des autres individus, il s'agit d'une donnée intrinsèque qui ne dépend que des préférences particulières de l'individu considéré, en l'occurrence de son aversion plus au moins grande pour le désagrément qu'engendre la liquidité, par conséquent la demande sur le bitcoin résulte d'un calcul purement privé où chaque individu compare l'utilité marginale d'un bitcoin, qu'il détient aux utilités marginales des autres monnaies et marchandises, il s'ensuit que le recours aux mêmes outils que ceux traditionnellement utilisés pour les marchandises permet d'analyser la demande de bitcoin.

On comprend en vertu de ce qui est dit que cette approche a fait du bitcoin un pur objet dont chacun peut appréhender les qualités sans tenir compte de regard d'autrui, elle intègre théorie de la monnaie et théorie de la valeur, mais en niant la spécificité de bitcoin en tant que relation des hommes entre eux pour le réduire

a un bien banal , il s'agit de faire de la relation monétaire un rapport du type objectal compatible avec l'individualisme marchand.

A l'évidence le choix de détenir le bitcoin est fortement conditionné par ce que pensent les autres et s'ils refusent d'accepter cette monnaie alors celle-ci n'a plus aucune utilité elle cesse d'être liquidier ; c'est la un fait incontournable , le nier n'est guère réaliste , autrement dit si un mineur de bitcoin sait que ses bitcoins seront refusés par tous les échangistes alors il ne les acceptera pas pour cette raison de fond , il est impossible de réduire le rapport de la monnaie a une relation purement privée de type objectal , indépendante des choix des autres , ce qui condamne non seulement l'approche précédente mais également et plus fondamentalement la notion même de valeur appliquée au bitcoin .pour le dire autrement la liquidité repose sur le fait que les autres échangistes acceptent cette monnaie dans leurs échanges.

Tout au fois même si le bitcoin a la confiance que l'on peut lui accorder de pouvoir l'échanger contre des biens et services , et l'échanger auprès d'une communauté a expansion ; mais il risque de le perdre a tout moment, l'absence de la frappe sur cette monnaie remet en cause cette dernière si on part du principe que c'est pas les pièces et les billets qui font la monnaie mais c'est la frappe qui l'a faite , de fait que cette dernière n'est pas libre et elle est soumise a un monopole politique qui a fait de la monnaie un privilège régulier et attribut de la souveraineté , ainsi la fausse monnaie est un crime de l'ère –majesté.

Conclusion

A chacune des grandes étapes de l'évolution ; la valeur de la monnaie repose en définition sur la croyance et la foi sociales, que le bitcoin a son tour les a gagnés en raison de ce système très sécurisé anonyme que personne ne peut y utiliser sans être un mineur en effet de ce système cryptographique qui empêche toutes modifications dans le registre électronique, c'est d'ailleurs dans ce point que le

bitcoin a montré sa robustesse. Et la participation au contrôle ne sera menée que par les nœuds du réseau qui le souhaitent. Pour éviter que trop peu de nœuds du réseau participent de contrôle un système de rémunération est prévu. Ce délicat agencement étonne les spécialistes et prouve que l'auteur anonyme qui a conçu les bitcoins est ; très probablement un cryptographe averti ou un groupe incluant au moins un cryptographe averti.

Le bitcoin se veut une monnaie universelle ; il a ce pouvoir de conversion vers toutes les monnaies ; à l'instar du dollar et de l'euro sans qu'il soit contrôlé par l'état, ce qui fragilise la souveraineté et qui peut être affaiblie ou détruite , l'unanimité que le bitcoin a engendré peut se déliter et les conflits qu'il avait réussi à faire taire peuvent renaître ; se trouve alors mis en question la prétention à la monnaie à être radicalement différente des actifs financiers et des marchandises profanes , une différence qui fonde son autorité. Elle doit rivaliser avec des monnaies partielles et qui prétendent vouloir la remplacer à l'instar du bitcoin .pour le dire autrement la monnaie ne résulte pas du libre assentiment des sociétaires en tant qu'elle exerce une contrainte extrêmement forte sur les intérêts privés et elle est le lieu de conflits incessants.

Ce qui favorise le blanchiment d'argent sale, la fraude fiscale, et la séparation entre la sphère monétaire et la réelle. De ce fait le bitcoin est économiquement très petit à côté des autres monnaies internationales auquel il ne peut pas prendre sa place.

Cette expérience inédite d'un cryptographe nous a montré que les problèmes économiques et sociaux ne trouvent pas forcément de solutions dans la technologie.

Bibliographie

1- Livres

- Olivier bomsel ; gratuit de déploiement de l'économie numérique édition gollimard, 2007.
- Philippe HERLIN, la révolution du bitcoin et des monnaies complémentaires, édition Eyrolles 2013 ;
- Jaun-luis BESSON, monnaie et finance, office des publications universitaires, Ben Aknoun .ALGER
- P.SALLES, initiation économique et sociale ; DUNOD, PARIS 1970
- Sid-Ali BOUKRAMI, Vade-mecum de la finance, office des publications universitaires, Ben Aknoun, ALGER 1991.
- ZOLLINGER Lamarque, e-marketing et stratégie de la banque ; DUNOD, paris 1999.
- Zunayr, MIKDASHI ; les banques a l'ère de la mondialisation, éd economica, paris 1998.

2- Article du journal :

- David bounie ; quelques incidences bancaire et monétaires des systèmes de paiement électronique ; revue-économique 2001/0vol ;
- JEAN-PAUL Delahaye ; le bitcoin, première crypto-monnaie ; bulletin de la société informatique de France, numero4, octobre2014,pp67-104 .
- Le bitcoin : nature et fonctionnement ; banque et droit N°159 janvier 2015 sur : <http://www.revue-banque.fr/medias/content/users/christine/1423573965130.pdf>.

3- Sites web :

- Bastien VIALLA, fonctionnement d'une crypto-monnaie : le bitcoin sur <https://www.lirmm.fr/content/download/7214/123889/file/bitcoib.pdf>
- ec.europa.eu/internal_market/payments/emoney/text/index_fr.htm.
- Remy CHRETIEN et Stéphanie DELAUNE, le bitcoin, une monnaie 100% numérique sur :
<http://people.irisa.fr/Stephanie.Delaune/PUBLICATIONS/CD-interstices14.pdf>