Table des matières

Liste des tableaux

Liste des figures

1. Introduction

Comment notre décennie va être retenu par l'histoire de la technologie ? D'ici 50 ans, dans les livres des spécialistes, ce serait marqué : « L'ère de Bitcoin ». C'est la grande invention qui a fait des milliers de personnes s'investir dans des machines pour « miner » la monnaie virtuel. Le grand engouement médiatique qui a suivi a obligé plusieurs grandes entreprises et figures politiques à prendre connaissance du fameux Bitcoin et déclarer une position. Mais qu'est-ce que c'est véritablement cette invention étrange ?

Définir le Bitcoin n'est surtout pas une tâche facile. C'est un sujet complexe, qui couvre des domaines allant de la cryptographie à l'économie, en passant par le génie logiciel, et qui est devenu le champ de discussion de plusieurs experts technologiques. Pour vous donner une idée : un lecteur lambda qui s'aventure sur le Bitcoin n'arrivera pas à comprendre tout de suite l'objet de l'étude, ni ses éventuelles implications.

Une définition relativement simple pourrait exister : Le Bitcoin est une monnaie digitale qui se caractérise par sa décentralisation, soit le fait qu'aucun Etat ou entité bancaire ne la contrôle. Contrairement à la monnaie ordinaire, comme l'euro ou le franc suisse, le Bitcoin n'est soutenu par aucun métal précieux de l'espèce de l'or. Au premier regard étrange, cette définition soulève la question de la validité d'une monnaie pareille. La réponse est simple : le Bitcoin est qualifié de monnaie mais n'est en réalité qu'un simple programme informatique. Comme chaque programme, le Bitcoin a son propre auteur, dont la vraie identité reste inconnue jusqu'au aujourd'hui ; on se réfère dès lors au pseudonyme qui a été laissé au publique – Satoshi Nakamoto, créateur du Bitcoin.

Le code de Bitcoin est lui sous une licence Open Source ce qui veut dire qu'il appartient au domaine publique et peut être trouvé sous Github. Une autre innovation qui démarque le Bitcoin des autres monnaies est sa base de données appelée blockchain qui est décentralisée, publique et bénéficie d'un certain degré d'anonymat.

Depuis sa création le site blochain.info recense plus 88 millions de transactions Bitcoin entre approximativement 120 millions de comptes. Depuis octobre 2015, il est estimé que chaque jour plus de 136 milles transactions prennent place dans le monde, ce qui représente environ 336 milles bitcoins ; à la valeur du marché actuel cela représente 89 millions de francs.

1.1 La monnaie digital

Avant de s'aventurer sur le sujet du Bitcoin, il faut présenter les différentes monnaies qui existent.

Ci-dessous se trouve un tableau établi par « Deutsche Bundesbank » & « ECUREX ». Il classifie la monnaie en fonction de qui la produit et de ce qui lui donne sa valeur.

Tableau 1 : Différentes monnaies

	Monnaie Non-Etatique / Privée	**Monnaie Publique / Etatique**
Monnaie-fiat	Time Dollars	CHF, USD, EUR, etc.
Monnaie-marchande	Liberty Dollar(1998-2009) Monnaie Digital	Coupons or (1863 – 1993)

. Digital Currencies: Principles, Trends, Opportunities, and Risks - p.26

Monnaie publique ou étatique est une monnaie distribuée exclusivement par un Etat. Elle est reconnue comme un moyen de paiement valide et ne peut juridiquement pas être refusée dans le cadre de l'extinction d'une dette privée ou publique.

Monnaie non-étatique ou privée est une monnaie distribuée par une autorité ou communauté qui n'est pas soutenue par un gouvernement. Elle peut être centralisée ou décentralisée.

Les monnaie-fiat est une monnaie décrétée par un Etat. En soi, elle ne présente pas de valeur, mais dérive celle-ci des lois et des réglementations gouvernementales. Il appartient à l'Etat de garantir que la monnaie gardera son pouvoir d'achat.

Monnaie-marchandise – Ce type de monnaie est basé sur un bien spécifique, qui est le plus souvent un matériau précieux, tel que l'or ou l'argent.

Selon cette classification, le Bitcoin, en tant que monnaie digitale, tombe sous la catégorie de monnaie marchandise et privée. C'est principalement ces caractéristiques qui vont nous intéresser dans la suite de la présente contribution.

1.1.1 Les moyens de paiement électronique les plus repandus en entreprise

Pour pouvoir mieux comprendre les avantages du Bitcoin, il convient de mettre la monnaie virtuelle en comparaison avec les moyens de paiement les plus répandus en pratique.

1.1.1.1 Carte de crédit / débit :

Le moyen de paiement le plus utilisé de nos jours est celui moyennant une carte de crédit ou de débit. Pour permettre de telles transactions, une entreprise doit se munir d'un Terminal de paiement électronique (TPE). Le TPE est acquis auprès d'une entreprise tierce qui exerce la fonction d'intermédiaire entre la banque émettant le terminal et la société commerciale utilisatrice (ci-après appelé « le commerce »).

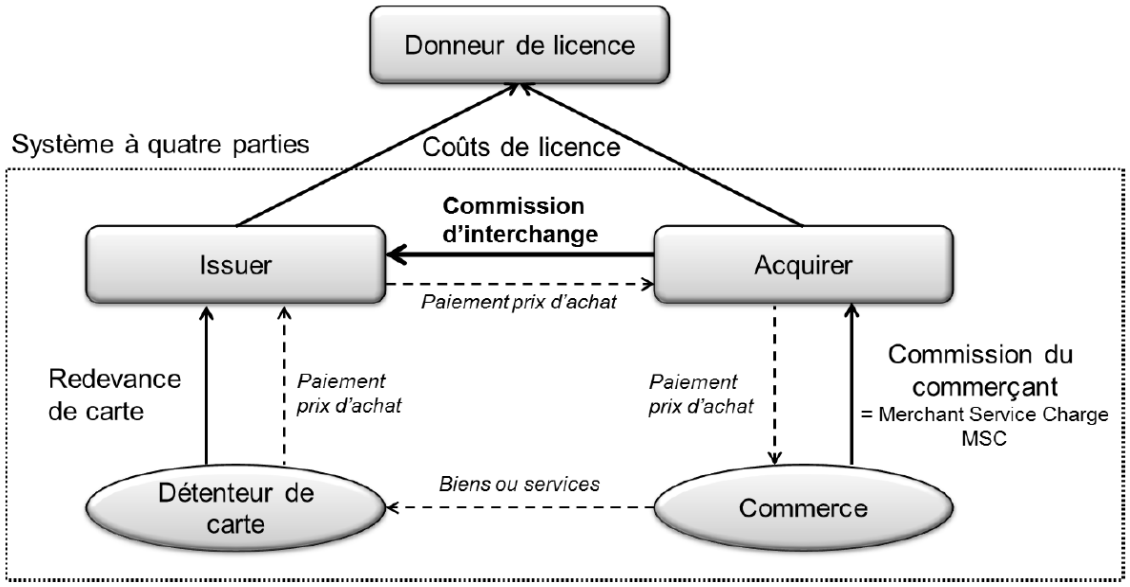


Figure 1 : Documentation pour la conférence de presse concernant le cas des commissions domestiques d'interchange pour les cartes de crédit II (KKDMIF II), p. 1

Lors de chaque transaction effectuée au moyen d'une carte de crédit, le commerce verse un pourcentage du prix d'achat à l'entreprise tierce fournisseur du Terminal. Ce pourcentage est nommé dans la pratique « Commission d'interchange » ou encore « Frais d'interchange » et s'élève aujourd'hui à 0,7% depuis le 1er août 2015. Selon la COMCO (Commission fédérale de la concurrence), le pourcentage va baisser jusqu'à 0,44% à partir de 2017.

Il y a principalement 4 entreprises qui exercent aujourd'hui la fonction intermédiaire : Aduno, B+S Card Service, ConCardis et SIX Payment Services. C'est ces 4 sociétés qui accumulent le bénéfice fait sur toutes les transactions dans les commerces.

Quant aux cartes de débit, leur usage n'est pas soumis à la COMCO et par conséquent, elles ne font pas objet de la même réglementation. L'utilisation de ce type de cartes est régie par les règles internes de la banque émettrice.

1.1.1.2 PayPal :

Paypal est une entreprise américaine, spécialisée dans le transfert d'argent en ligne. Fondée en 1998, l'entreprise a transféré en 2014 plus de 228 milliard de dollars répartis sur 26 monnaies dans plus de 190 pays du monde.

Figure 2 : PayPal

En Suisse le site-web de l'Administration fédérale, dans sa partie qui traite le cas des petites et moyennes entreprise (appelé encore Portail PME) présente les avantages de PayPal comme suit[1] :

> « Les services du type PayPal peuvent s'avérer avantageux pour une boutique en ligne qui débute dans le e-commerce. Ils ne demandent aucun frais d'installation et sont faciles et rapides à mettre en place par le bais d'un plugin sécurisé. Le service se paie à la transaction. Son coût se compose des éléments suivants:
>
> - Un montant fixe par transaction (par exemple CHF 0.55)
> - Une commission sur le montant de la transaction (actuellement entre 1,9% à 3,4% chez PayPal) »

1.1.1.3 Comparatif :

Dans le but d'entrer dans les caractéristiques du Bitcoin, nous effectuerons tout d'abord une comparaison détaillée entre cette monnaie virtuelle et le moyen le plus fréquent du paiement – les cartes de crédit. Le PayPal étant un moyen plus spécifique, il serait utilisé dans la suite du travail, quand il s'agira de présenter la pratique économique du Bitcoin. Aux fins de cette contribution, nous allons nous baser pour la comparaison principalement sur les rapports et informations données par la société Ecurex.

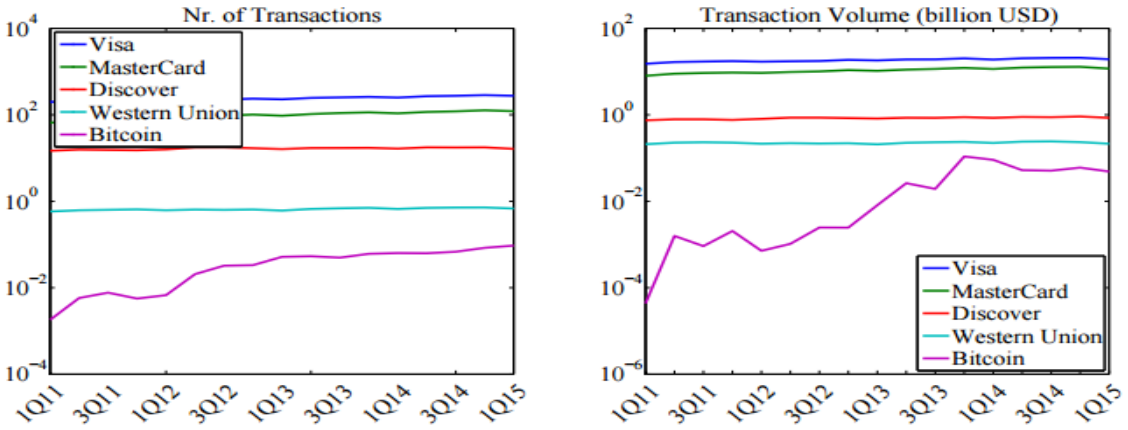
Ecurex est le premier marché digital basé en Suisse qui se spécialise dans les marchés financiers et le trading professionnel. Cette entreprise est en respect des normes des banques Suisse, ainsi que les standards américains et la FATCA[2]. Basée à Zurich, en 2015, elle a mis à disposition, en collaboration avec la « Deutsche

[1] http://goo.gl/YqKFVr - E-commerce: autres services de paiement en ligne – kmu.admin.ch
[2] The Federal Account Tax Compliance Act – Loi Fédérale des Etats-Unis, en vigueur depuis le 28 mars 2010.

Bundesbank », un guide complet sur les monnaies digital qui traite en profondeur du marché du Bitcoin. Les informations qui suivent sont tirées de ce guide, intitulé « Digital Currencies: Principles, Trends, Opportunities, and Risks » (Monnaies virtuelles : Principes, Tendances, Opportunités et Risques).

Afin de démontrer l'évolution du Bitcoin sur le marché ces dernières années, une extraction des données des différents réseaux de paiement a été effectuée à l'aide des rapports trimestriels. Parmi les entreprises qui ont été utilisées dans le cadre de cette étude, nous trouvons les leaders du monde des services financiers, comme VISA, Mastercard, Western Union, et Discover. Les données concernant le Bitcoin ont été prises directement du site Blockchain.info.

Tableau 2 & 3
Nombres de transactions & Volumes de transactions



(Digital Currencies: Principles, Trends,Opportunities, and Risks p.20)

Axe x représente les trimestres. L'axe y représente les transactions en millions

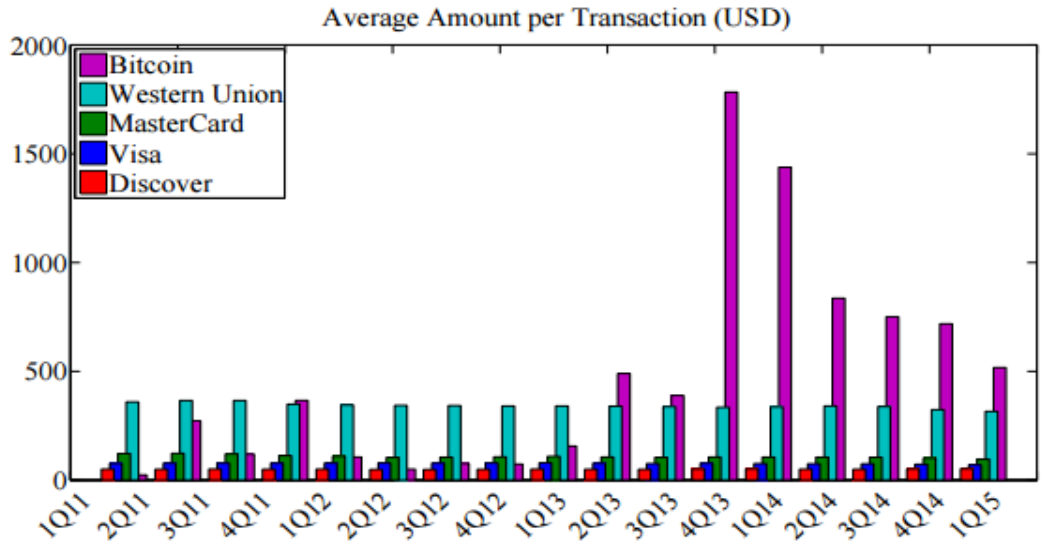
Le graphique ci-dessus démontre l'évolution des monnaies bien implantées sur le marché en comparaison avec le Bitcoin. Nous pouvons constater une augmentation du nombre de transactions avec la monnaie virtuelle. Pendant le premier trimestre de 2014, quand le Bitcoin a pris une popularité parmi les utilisateurs, le Bitcoin a presque atteint le même volume de transactions que le leader Western Union. Depuis, on constate une petite baisse mais qui reste sans grandes fluctuations.

Ci-dessous se trouve en outre un tableau récapitulatif de toutes les données extraites pour produire les graphiques, de façon à permettre une visualisation plus complète des volumes de transactions.

Tableau 4 :
Volume en millions de Dollars (vol) & millions de transaction (Tx)

Year	VISA		MasterCard		Discover		Western Union		Bitcoin	
	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)
1Q11	15,153.8	198.3	8,011.0	65.6	746.5	14.7	208.8	0.6	0.04	0.002
2Q11	16,604.4	213.2	8,934.1	72.5	787.0	15.7	226.4	0.62	1.6	0.006
3Q11	17,033.0	217.7	9,285.7	77.1	787.0	15.4	231.9	0.63	0.92	0.008
4Q11	17,450.5	223.6	9,505.5	84.4	761.3	15.1	226.4	0.65	2.1	0.006
1Q12	16,934.1	215.7	9,329.7	84.8	804.3	15.8	214.3	0.62	0.7	0.007
2Q12	17,252.7	218.7	9,780.2	93.8	861.1	17.5	220.9	0.64	1.04	0.021
3Q12	17,582.4	225.3	10,087.9	95.4	860.9	17.6	216.5	0.63	2.47	0.032
4Q12	18,648.4	236.8	10,835.2	101.3	840.1	16.8	219.8	0.64	2.45	0.033
1Q13	18,120.9	227.9	10,406.6	95.1	819.2	16.1	207.7	0.61	8.12	0.052
2Q13	19,109.9	245.6	11,087.9	104.1	856.1	17.0	225.3	0.66	26.2	0.053
3Q13	19,175.8	252.1	11,494.5	109.9	850.5	17.1	231.9	0.69	19.3	0.050
4Q13	20,197.8	259.9	12,142.9	114.0	883.8	17.2	236.3	0.71	108.65	0.061
1Q14	19,011.0	249.9	11,483.5	108.2	850.4	16.5	223.1	0.66	91.01	0.063
2Q14	20,274.7	269.6	12,351.6	116.6	892.2	17.6	239.6	0.70	52.35	0.063
3Q14	20,703.3	275.9	12,714.3	120.5	881.0	17.5	242.9	0.72	51.07	0.068
4Q14	20,879.1	285.4	12,879.1	127.1	912.0	17.7	233.0	0.72	60.1	0.084
1Q15	19,263.74	275.6	11,681.32	121.3	852.32	16.3	214.29	0.68	48.80	0.094

Tableau 5 :
Montant moyen par transactions en millions d'USD



La transaction moyenne en bitcoins depuis le milieu de l'année 2013 dépasse celles des 4 compagnies de services financiers. Une explication qui est mise en avant à ce sujet est que c'est pendant cette période que le Bitcoin a gagné sa popularité et des milliers de personnes sont entrés dans le processus d'achat-vente. Pourtant, bien que la tendance soit dépassée, on constate que les transactions en moyenne gardent un montant plus élevé que celui atteint par les entreprises de services financiers, malgré le déclin facile à observer du nombre des transactions.

1.2 Traitement juridique du Bitcoin en Suisse

1.2.1 Conseil fédéral

Le 25 juin 2014, le Conseil fédéral a émis un rapport traitant du Bitcoin intitulé : « Rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070) ».

Le rapport en question examine certains aspects de l'utilisation des monnaies virtuelles, tout en se basant sur l'importance économique, leurs traitements juridiques et le risque qu'elles comportent.

En règle générale, l'utilisation du Bitcoin en Suisse n'est pas réglementée par une loi spécifique, étant donné que le nombre d'utilisateurs sur le territoire du pays n'est pas suffisamment important. Comme tout moyen de paiement, le Bitcoin est couvert par le Code des obligations[3] et son article 1 et peut être intégré dans n'importe quelle transaction du droit privé. En cas d'exécution entière du contrat, le paiement par Bitcoin ne pose pas de problèmes. Des troubles peuvent être générés en cas de litige, puisque souvent les utilisateurs du Bitcoin se trouvent dans des pays différents et dans ce cas, les règles sur le droit international privé doivent intervenir. Il est impossible de dire sous quel droit et quel tribunal sera compétent pour statuer sur de tels litiges, vu la complexité du moyen de paiement et sa répartition dans le monde entier. Des cas pareils devant les tribunaux suisses ne sont pas intervenus à ce jour.

On peut donc conclure qu'en Suisse, l'utilisation du Bitcoin n'est pas vue aujourd'hui comme une matière spéciale, nécessitant une intervention parlementaire et son traitement correspond à celui de tous les autres moyens de paiement.

1.2.2 FINMA

L'Autorité fédérale de surveillance des marchés financiers (FINMA), l'organe responsable de la régulation financière en Suisse, a publié en juin 2014 un rapport au sujet du Bitcoin et la réglementation y applicable. Toutes informations qui suivent sont tirées de ce rapport.

Figure 3 : Finma

Tout d'abord, le Bitcoin ne fait objet d'aucune réglementation spécifique en Suisse ; la loi ne prévoit pas le besoin d'une autorisation pour acheter ou vendre des biens et des services au moyen du Bitcoin. Pourtant, la situation peut être différente selon le modèle

[3] Code des obligations du 30 mars 1911 ; RS 220.

Clicours.COM

business qui a été choisi par l'entreprise. Dans certains secteurs spécifiques, une autorisation de la part de la FINMA est nécessaire ; à défaut d'une telle autorisation, l'activité peut être dénoncée comme illégale et peut faire objet d'une enquête pénale. Si une entreprise ne respecte pas les exigences légales posées par la FINMA, elle peut subir de différentes sanctions, y compris une liquidation totale.

Ces secteurs spécifiques incluent en principe les entreprises qui assument une fonction de genre « bancaire », en proposant aux clients des comptes spécifiques pour garder leurs Bitcoin et/ou pour les faire administrer par des professionnels. Dans de tels cas, l'entreprise doit être en possession d'une autorisation bancaire, fournie par la FINMA.

Un autre exemple sont toutes les actions qui peuvent tomber sous la Loi fédérale sur le blanchiment d'argent, soit des plateformes internationales proposant un échange de Bitcoin « en cachette » de la loi. Dans cette situation, les créateurs de la plateforme doivent aussi faire une demande auprès de la FINMA pour légaliser leur activité.

Le rapport note encore que pour l'instant l'utilisation du Bitcoin reste très insignifiante en Suisse, mais n'exclut pas les risques, énumérés dans le rapport du Conseil fédéral présenté plus haut.

Par conséquent, on peut conclure que le Bitcoin n'est pratiquement pas contrôlé par la FINMA et ne tombe pas sous les exigences générales. Dès lors, l'usage du Bitcoin et son implémentation dans l'entreprise ne nécessitent pas des mesures spécifiques de la part des gérants.

1.2.3 Taxation

La question de la taxation est un des problèmes plus spécifiques concernant le Bitcoin. Pour pouvoir présenter des réponses complètes, une recherche assidue a été effectué auprès de l'Administration fiscale cantonale et la Fédération des Entreprises Romandes (FER), au moyen de leurs sites-web. Etant donné que ces deux sources présentent peu d'informations sur le sujet, une prise de contact avec Monsieur Godel Roland, Secrétaire Général adjoint chargé de la communication du Département des finances (DF) a eu lieu, afin de comprendre mieux comment les transactions avec le Bitcoin et les achats de la monnaie elle-même sont traités sous l'angle fiscal.

1.2.3.1 Comptabilité

A ce jour, le Bitcoin est considéré, de point de vue de l'Administration fiscale suisse et au regard de la réglementation fiscale, comme une monnaie étrangère. Cela implique qu'à la fin de chaque année civile, dans la comptabilité des entreprises utilisatrices, les bitcoins doivent être convertis et présentés en Francs Suisses. Le taux applicable à cette conversion est celui au jour du 31 décembre et l'Administration fiscale est chargée de mettre à disposition la liste des cours des devises étrangères. A cette étape, le Bitcoin ne figure pas encore dans les listes qui sont disponibles au public.

1.2.3.2 TVA

Quand il s'agit de l'achat de bitcoins, on applique les règles générales sur les achats des devises étrangères. Ce type de transactions est exempté de la TVA.

En revanche, lorsqu'il s'agit de l'achat de biens ou de services moyennant le Bitcoin, en tant que monnaie, ces opérations sont soumises à la TVA ordinaire.

On peut conclure, au regard de peu d'informations qu'on a à ce sujet, que la taxation du Bitcoin n'a pas encore pris grande importance dans les milieux fiscales, à cause du nombre insignifiant d'utilisateurs en Suisse. Pour cette raison, il est difficile de présenter un régime complet. Il est peu probable que la situation concernant le traitement juridique et financier du Bitcoin va changer, puisque la tendance a petit à petit perdu de l'importance.

Tous les échanges avec Monsieur Godel peuvent être trouvés en annexe du présent travail (Annexe II).

1.3 Bitcoin expliqué

Le Bitcoin avec un B majuscule est une crypto-monnaie crée par Satoshi Nakamoto. Les protocoles furent publiés en 2008 sur un site spécialisé de la cryptographie. Le projet fut implémenté et la première version stable fut mise en marche le 3 janvier 2009.

Figure 4 : Bitcoin logo

Les paiements sont effectués en bitcoin (BTC) avec un b minuscule qui représentent des pièces digitales transféré par le réseau du Bitcoin.

Les protocoles du Bitcoin sont codés de façon à ce qu'il y ait au maximum 21 millions de Bitcoin jamais crées. De leur côté, les bitcoin sont émis par le système de façon stable, définie et dégressive. Le processus se déroule sur une durée de 4 ans ; une fois la durée écoulée, le nombre de bitcoins émises est réduit à moitié. Prenons l'exemple suivant : l'algorithme en 2009 émettait 50 bitcoins toutes les 10 minutes. 4 ans plus tard, en 2013, ce même algorithme émettait 25 bitcoins. Ainsi, en 2017, il va descendre à 12,5 et ainsi de suite. Ce procédé sera répété jusqu'à ce que l'on arrive au 21 millions de bitcoins maximum, évènement qui devrait se situer aux alentours de l'année 2140.

Le début de l'année 2016 marque l'entrée de 15 millions de bitcoins en circulation.

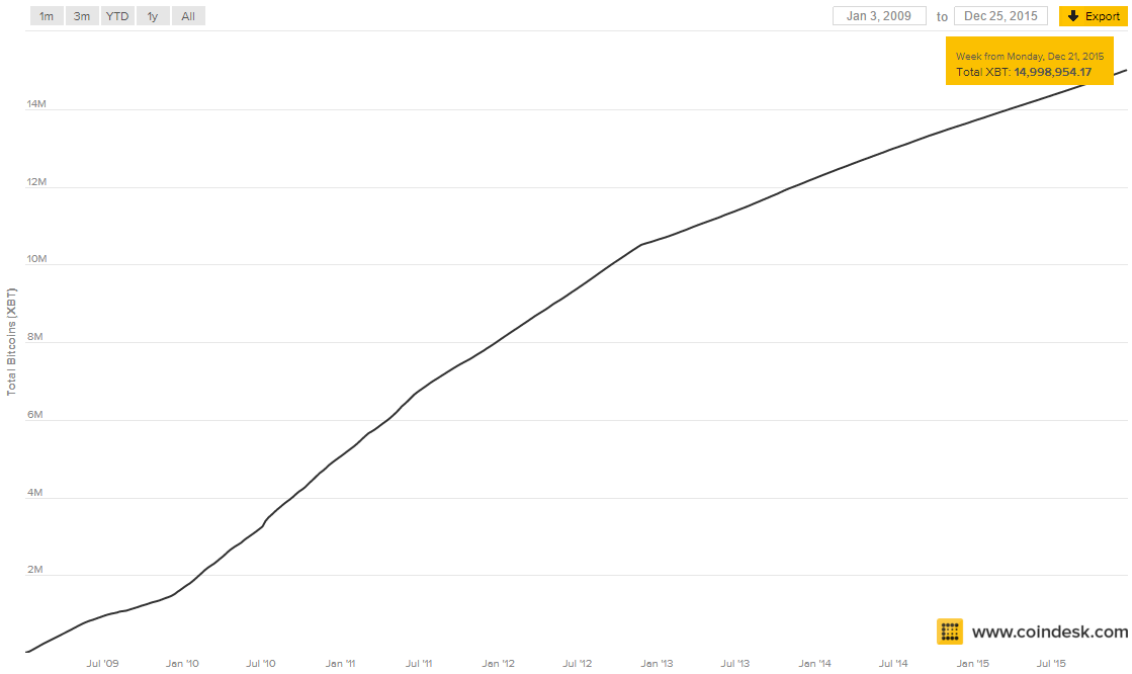


Figure 5 : Nombre de Bitcoin actuel en circulation, www.coindesk.com

Il est important de noter que toutes les transactions, qui ont été effectuées dès la création du Bitcoin sont disponibles sur internet mais restent pseudo-anonyme tout de même (un de grands avantages du Bitcoin est exactement le fait que la monnaie n'est pas nominative et assure l'anonymat).

Le protocole de communication mis en place au sein du programme est le peer-to-peer qui est utilisé pour faciliter la mise à jour du blockchain sur le réseau et assurer les transactions entre les utilisateurs, sans faire appel à un intermédiaire. Le peer-to-peer est très important puisque le Bitcoin est basé sur l'anonymat. Tout de même, cela peut et a déjà posé des problèmes. L'exemple phare est le site Silk road, un site sur le marché noir, qui permettait d'utiliser les bitcoins afin de se procurer des produits illégaux. Le site a été fermé en 2013 par le FBI, car c'était impossible de retrouver les utilisateurs. L'anonymat du Bitcoin crée aussi des situations conflictuelles dans le domaine du blanchiment d'argent.

1.3.1 Adresse

Bitcoin fonctionne sur le principe cryptographique de clé publique et clé privée. Ce couple de clés sont générées ensemble et sont liées.

La clé publique est originalement générée par l'algorithme « Elliptic curve digital signature algorithme » (ECDSA). Après plusieurs hachages avec SHA256 & RIPEMD160, on arrive enfin à une chaine de caractères qu'on appellera adresse et sur laquelle une personne peut envoyer des bitcoins. La raison des multiples hachages est de diminuer la taille de l'adresse tout en prévenant certain type d'attaques.

Cette adresse pourra être affichée publiquement sur un site internet ou à côté d'une caisse de paiement dans un magasin sans crainte.

La clé privée est générée en au moment du ECDSA et permet de dépenser les bitcoins de la clé publique correspondante. Il est très important de ne pas divulguer cette clé et de la garder en sécurité.

Figure 6 : Exemple QR code adresse

L'obtention de cette clé permettra à la personne qui la possède de se servir des Bitcoin correspondant à l'adresse publique.

Chaque clé privée correspond à une clé publique ; néanmoins il est possible qu'une seul clé privée soit utilisée pour l'ensemble des clés publiques. Il est aussi possible d'associer n clés privées à une clé publique - ceci s'appelle une « signature multiple ».

Une adresse est simplement un identifiant alphanumérique aléatoire de 26 à 35 caractères commençant par les caractères « 1 » ou « 3 ». Le 1 et le 3 étant rajoutés après les hachages, ils ont l'utilité d'indiquer si ce sont des adresses avec signature simple (1) ou signature multiple (3). Une adresse peut être générée sans coûts par n'importe qui. Une personne n'est pas limitée par le nombre d'adresses.

Un exemple d'une adresse : **`1ErMy5qaJgWUSzyySYYt1VWDmW3VchfvC1`**

Une clé privée est généralement un nombre de 256 bits. Certains porte-monnaie varient entre 128 et 512 bits. 256 bits en hexadécimal reviens à 32 bytes. 256 bits représente 2^{256} combinaison différents ; pour mettre ce nombre en perspectif cela représente 1 suivie de 77 zéros de possibilités.

Figure 7 : Exemple QR code clé privé

Imaginons qu'on génère 1 trillion de clés privées par seconde ; dans une telle hypothèse, on dépassera l'âge de l'univers avant d'avoir énuméré toutes les combinaisons éventuelles. Ces 10^{76} possibilités jouent un rôle fondamental dans la sécurité du Bitcoin. Pour comparaison, il y a environ 10^{50} molécules sur terre et entre 10^{78} et 10^{80} atomes dans l'univers observable.

Un exemple de clé privée :

`5J6DUP2N3mBctcVjHN4tbPE2hA2PJ8YBS9D4jY2E4wKhdcSQY4K`

Toutes ces adresses sont générées et gérées par le software Bitcoin, appelé porte-monnaie. A la création d'un porte-monnaie une adresse et une clé privée sont mis en place.

Une bonne pratique du Bitcoin est d'utiliser qu'une seul fois son adresse. Cette pratique n'est pas obligatoire mais fortement conseillée pour augmenter son niveau d'anonymat ainsi que pour des questions de sécurité. En effet si au moment d'acheter un bien ou service avec des bitcoins un nom, prénom, adresse ou entreprise est demandé l'anonymat disparaît. Pour cette raison, c'est conseillé d'utiliser qu'une fois l'adresse. Normalement un porte-monnaie est tout à fait capable de régénérer une

adresse et si ce n'est pas le cas, il suffit de se renvoyer les bitcoins sur une nouvelle adresse.

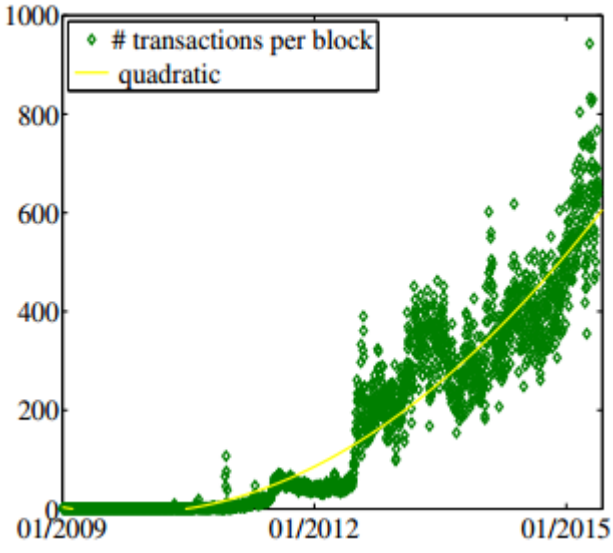
Les adresses sont sensibles à la case et la chance qu'une adresse avec une erreur soit acceptée est de 1 chance sur 2^{32} ce qui représente 1 chance sur 4,29 milliards. Pour des raisons de sécurité et d'ambiguïté les caractères suivants sont remplacés lors de la création de l'adresse : « O » majuscule, « I » majuscule, « l » minuscule, et le numéro « 0 ».

En outre, afin de simplifier la tâche aux utilisateurs les adresses sont transformées en QR Code pour un partage rapide et efficace. Ceci permet aussi d'éviter les erreurs de retranscription.

1.3.2 Blockchain

Une des grandes innovations du Bitcoin est le « blockchain » aussi appelé « block chain ». Le blockchain n'as pas de traduction française officielle mais peut être traduit par « registre des transactions numériques». Le blockchain est aussi appelé « Ledger » qui est traduisible par « journal de transactions ».

Ce registre est une base de données décentralisée de toutes les transactions qui ont été effectuées sur le réseau Bitcoin depuis sa création. Partagé par tous les ordinateurs communiquant par nœuds dans un système Bitcoin, ce blockchain est en constante augmentation étant donné que de nouveaux blocks sont ajoutés au fur et à mesure. Sa mise à jour est automatique et constante sur tout le réseau toutes les 10 minutes.



Nombre moyen de transaction dans un block - Blockchain.info

Au jour du 1 janvier 2016 le nombre de block s'élevait à approximativement 391'000. Un block contient potentiellement des milliers de transactions ; le nombre de transactions par block n'est pas limité mais au niveau de la taille, un block n'excèdera jamais 1 Mb. De plus un block n'aura jamais plus de 20'000 signatures. Il est important de souligner que dans le blockchain chaque adresse et le montant y contenu est visible par tout le monde mais

aucun nom, prénom ou informations permettant de désigner une personne ou organisation ne peuvent en être tirées.

Le blockchain est théoriquement sûr et infalsifiable étant donné que la notion de confiance n'est pas implémentée, c'est-à-dire qu'aucune autorité centrale n'est mise en place pour vérifier les blocks. Un algorithme en assure le bon fonctionnement. Cet algorithme est exécuté par les mineurs.

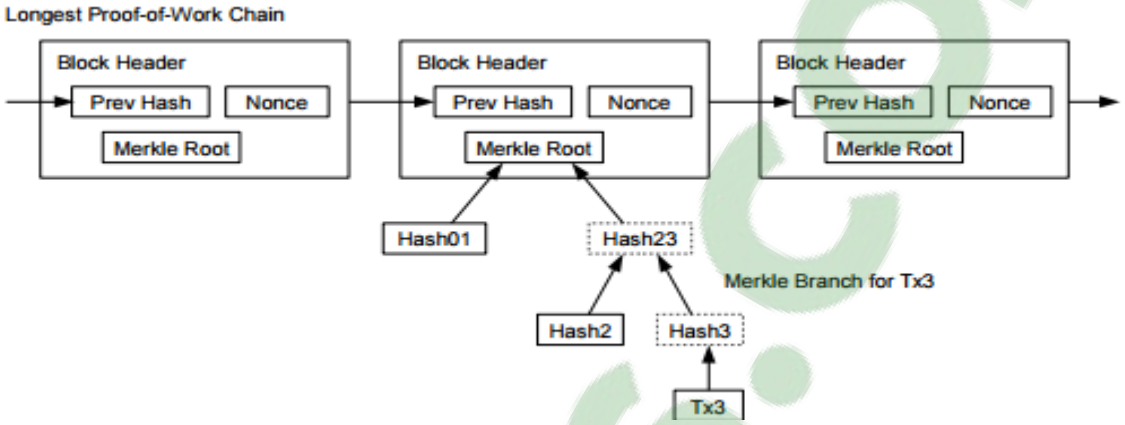


Figure 8 : Blockchain expliqué: chain

Bitcoin: A Peer-to-Peer Electronic Cash System p .5

Toutes les 10 minutes un mineur gagne une sorte de loto compétitif qui lui permet de de valider le block en cours. Il rassemble un maximum de transactions, il les combine et ensuite il hache les id de toutes ces transactions ensemble ; le résultat sera un nœud de Merkel. Le nœud de Merkel sera combiné avec le Timestamp (date et heure de la création du block), le hash précédent et plusieurs autres éléments : nonce (numéro gagnant du « loto compétitif »), taille et difficulté. Le fait que chaque nouveau block contient le hash général du block précédent est ce qui lie le blockchain ensemble d'où le mot chaine.

Le blockchain alors met à jour le registre en validant les transactions. Cette mise à jour est ensuite propagée à tous les nœuds proches qui à leur tour propagent aux nœuds proches jusqu'à ce que le réseau complet soit mis à jour.

Toutes les transactions vérifiées sont inclues dans ce registre. Une version complète du registre permet de savoir combien de Bitcoin contient chaque adresse à n'importe quel moment dans le temps.

Au jour du 1 janvier 2016 le site bitinfocharts.com estime avec précision le taille du blockchain à 64.91 Gigabyte (GB).

1.3.3 Transaction

Une des particularités de Bitcoin est que la monnaie n'existe pas physiquement. Ce n'est que des transactions entre différentes adresses avec le solde des bitcoins qui augmente et diminue. La théorie veut que personne n'a de bitcoins ; tous les bitcoins créés et à créer sont simplement des adresses dans un registre et le seul moyen de les utiliser est de connaitre la clé privée.

A la création de bitcoins le mineur créateur du block se voit attribuer 25 bitcoins en plus de toutes les commissions du block. Il pourra alors envoyer ces bitcoins sur une adresse qui lui est propre. Toutes les transactions Bitcoin sont reçues et envoyées par un porte-monnaie.

Prenons un exemple :

Fred et Charles ont envoyé des bitcoins à Alice. Alice décide d'envoyer ses 5 bitcoins à Bob. 3 informations importantes sont à tirer :

- Un **input** : un ou plusieurs records d'information qui contient toutes les informations sur la provenance des bitcoins.
- Un **montant** : Le montant qu'Alice souhaite envoyé à Bob.
- Un **output** : L'adresse de Bob.

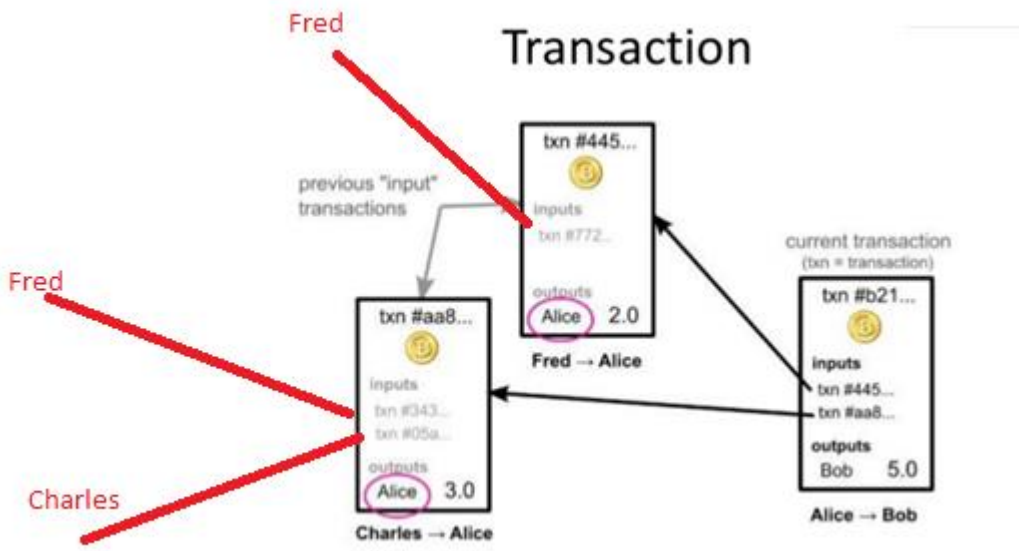


Figure 9 : Exemple de transaction Bitcoin simple

Chaque transaction est un message signé avec une clé privée et contient les transactions précédentes.

Prenons le cas où Bob doit envoyer 15 bitcoins à Ted mais n'as qu'une adresse de 20 bitcoins. Cette adresse de 20 sera envoyée à Ted et la transaction s'occupe de splitter les 20 bitcoins en 2 adresses composées : 15 bitcoins qui seront transmis à Ted et 5 bitcoins qui seront transférés sur une nouvelle adresse de Bob que le porte-monnaie aura généré automatiquement.

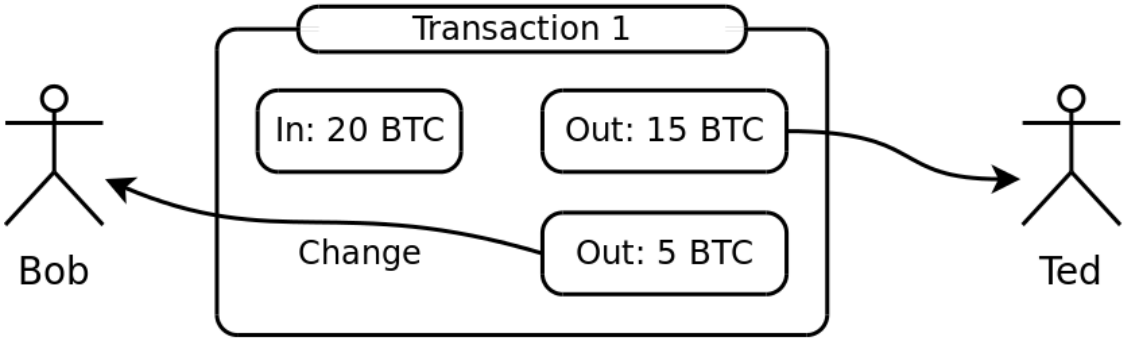


Figure 10 : Explication du retour de monnaie

Prenons maintenant 2 autres exemples plus concrets, qui sont des exemples réels, tirés du blockchain (ces informations ont été tirées du block 391'240 à l'aide site blockexplorer.com).

Création de bitcoins dans le blockchain

Le numéro de la transaction est 3d8f4413c (…).

Un mineur a généré 25 bitcoins pour avoir résolu le block et a reçu 0.22 bitcoins qui représente la somme de toutes les commissions. Le mineur s'est envoyé les bitcoins sur 2 adresses séparées.

Clicours.COM

Figure 11 : Exemple de création de bitcoins dans le blockchain

Exemple d'envoi de de bitcoins d'un particulier à une autre

Ci-dessous ce trouve une transaction tiré du block 391'240.

Dans ce cas, nous ne pouvons que supposer qu'une personne a acheté un bien ou service à 3 bitcoin. Son porte-monnaie a combiné 0.22 et 0.08 pour former les 3 bitcoins. Le 0.01136 représente sûrement sa somme de retour de monnaie.

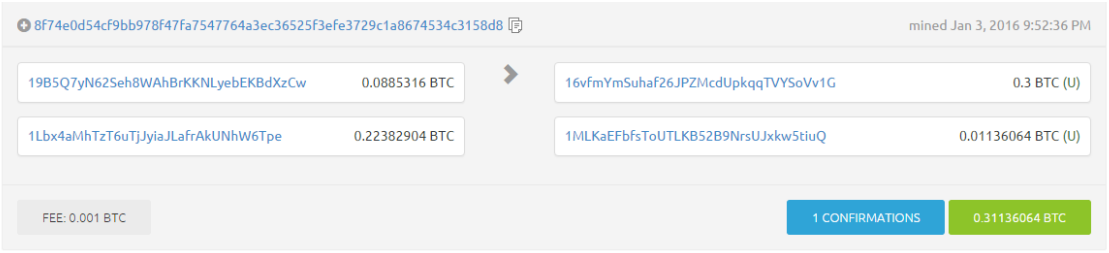


Figure 12 : Exemple de transaction avec un retour de monnaie dans le blockchain

1.3.3.1 Commission

En règle générale il n'y a pas de commission lors des transactions, mais il n'est pas impossible d'en rencontrer. Généralement une commission sera demandée que pour certaines transactions bien précises ; le motif est souvent un empêchement d'attaque par Spam ou Dénis de service (DoS). Ces commissions sont en moyenne fixées au maximum à 0.0001 bitcoins qui représente 0.03 CHF. Bitcoinarmory[4] est un porte-monnaie Bitcoin qui comporte une documentation très complète et dénombre 3 cas théoriques de la commission :

Transaction de moins de 0.01 bitcoin.

Le réseau Bitcoin considère que ces montants sont presque insignifiants (0.01 BTC représente en moyenne 3 CHF). Pour décourager les utilisateurs de faire ces transactions, les développeurs de l'algorithme ont pris la décision de mettre une

[4] https://bitcoinarmory.com/faq/

commission. Une autre raison est aussi d'empêcher une personne de scinder une transaction de bitcoins : au moment d'envoyer 1 bitcoin, un utilisateur décide de scinder ce bitcoin pour en faire 1'000'000 de transactions à 0.000001 bitcoins et cela gratuitement ; cela aura comme conséquences de surcharger le réseau et il est préférable de l'éviter.

Transaction comportant des bitcoins qui sont « trop nouveau ».

Chaque fois qu'une personne envoie des bitcoins sur le réseau, il envoie des bitcoins dit « vieux » qui ont une certaine durée de vie. Une fois ces « vieux » bitcoins envoyés à une personne, ils sont détruits et sont recréés pour la personne bénéficiaire. Ces nouveaux bitcoins devront attendre une certaine durée de temps pour être considérés comme vieux. La théorie est relativement obscure ; certaines personnes ont leurs pièces confirmé comme vieux après un bloc et d'autres doivent attendre plusieurs jours avant que soit considéré comme vieux. Ce temps d'attente est lié en parti au volume de transaction sur le réseau ainsi qu'au niveau d'altruisme des mineurs. Cette commission est mise en place pour empêcher que des spammeur puissent s'envoyer un aller-retour de Bitcoin qui résulterait en surcharge de réseau.

Transaction qui combine beaucoup de plus petit montant.

Cette commission concerne des personnes qui reçoivent généralement beaucoup de petites transactions. Prenons par exemple une personne qui reçoit 100 transactions de 0.0001 BTC puis envoie 0.01 BTC (la taille minimum qui ne nécessite pas de commissions). Bien que ce montant soit relativement petit, le fait de prendre en compte ces 100 transactions s'additionnera et sera très grande en terme de kilobyte (kB) ; cela nécessitera une commission de 0.0001 BTC par kB utilisé.

1.3.4 Porte-monnaie

Un porte-monnaie ou « wallet » en anglais est l'endroit où une personne conserve toutes ses adresses ainsi que ses clés privées. Un porte-monnaie s'occupe de la génération d'adresses ainsi que de l'envoie des bitcoins et présente le total des bitcoins sur la machine. Lors de l'installation d'un porte-monnaie de type Mobile & Desktop le blockchain sera téléchargé. Selon les versions une partie du blockchain sera incluse mais une mise à jour sera obligatoire du fait que la création de block arrive toutes les 10 minutes.

Il existe 3 types de porte-monnaie :

- Web
- Mobile
- Desktop

1.3.4.1 Porte-monnaie Web

Le porte-monnaie « Web » est un service web qui propose de stocker tout en ligne sur les serveurs du provider. Il est extrêmement facile de le mettre en place, très intuitive et facile d'accès, peu importe si on utilise un browser quelconque ou un smartphone avec une connexion internet. Certains porte-monnaie web permettent d'encrypter ses clés privées. Bien que ces porte-monnaie soient idéaux pour les gens qui souhaitent s'aventurer sur la technologie, elles présentent certains risques.

Le risque le plus dominant est que le service contrôle toutes les informations sensibles (adresses et clé privées) ainsi que l'adresse email, ce qui enlève une couche d'anonymat. Si le site ferme ou qu'une fuite arrive, il n'y a pas de solutions de secours. Il est quand même possible de faire des backups des adresses et clés. Si un tel porte-monnaie est utilisé, il faut avoir de la confiance au fournisseur.

1.3.4.2 Porte-monnaie mobile

Le porte-monnaie « **mobile** » est le plus facile à transporter et est très souvent utilisé, notamment grâce à son utilisation intuitive et sa facilité d'accès. En outre, il est très populaire quand il s'agit de faire des achats dans un magasin, grâce aux fonctionnalités de génération de QR Code et son scannage. Ces fonctionnalités sont natives au smartphones.

Pour utiliser ce type de porte-monnaie un smartphone est obligatoire et une connexion internet de type 3G est requise pour pouvoir profiter pleinement de toutes ces fonctionnalités. Etant donné que le blockchain doit être mis à jour souvent il se peut que la consommation du data du téléphone s'épuise très vite.

1.3.4.3 Porte-monnaie Desktop

Le porte-monnaie Desktop est une application à installer sur l'ordinateur. Ce porte-monnaie a le meilleur niveau de sécurité de par le fait qu'il permet de stocker les clés privées et les adresses offline tout en les encryptant et les hachant. Son seul inconvénient est qu'il n'est pas aussi facile à utiliser par une personne débutant dans le domaine du Bitcoin.

1.3.5 Mineurs

« Miners » en anglais ou mineurs sont des personnes qui utilisent des ordinateurs pour principalement 2 raisons : la création de nouveau bitcoin et la vérification du réseau. Le Bitcoin génère sa propre monnaie via un algorithme. Cet algorithme indique comment faire ce processus et à quelle vitesse l'effectuer. Les mineurs utilisent du software spécial qui a comme but de vérifier les transactions ainsi que de résoudre l'algorithme de génération des bitcoins.

Une prime monétaire mise en place récompense leurs efforts dans la résolution de ces algorithmes : principalement la création de monnaie (bitcoin block / block rewarding) et les frais de transactions. Actuellement les frais de transaction son négligeables. De ce fait la majorité des profits que les mineurs en tirent proviennent de la création de monnaie. Pour chaque bloc de bitcoin résolu actuellement 25 bitcoins sont récompensés à un mineur. Cette récompense est divisée par 2 tous les 4 ans jusqu'à l'arrivé au 21 millions de bitcoins. Une fois les 21 millions de bitcoins crées il n'y aura plus de Bitcoin à miner. A ce moment-là les mineurs se verront obligés de se tourner envers leurs secondes sources de revenu potentiel, c'est-à-dire les frais de transactions.

Au moment d'envoyer une somme de bitcoins un acheteur peut prendre l'initiative d'inclure une commission qui rendra la transaction plus rapide ; plus grande la commissions, plus rapidement le paiement sera pris en compte. Cette commission est totalement optionnelle mais en 2015 plus de 97% des transactions comportaient une commission par défaut qui s'élevait à 0.0001 BTC soit 0.04 CHF.

Etant donné que chaque block doit être résolu tous les 10 minutes, cela va de soi que l'algorithme se voit dans l'obligation d'augmenter sa difficulté tous les 2016 blocks. Il serait théoriquement possible qu'un groupe de supers ordinateurs rentrent en lise pour le minage et qu'ils arrivent à miner plus vite, c'est-à-dire plus de 1 block par 10 minutes mais après les 2016 blocks la difficulté sera ajustée. Si ces ordinateurs une fois la difficulté augmentée décident de partir, le réseau se verrait dans l'impossibilité de produire un block tous les 10 minutes et de ce fait la difficulté pourrait théoriquement redescendre pour s'ajuster.

De surcroît, les mineurs peuvent s'associer pour miner plus vite, puisque la nature même du minage dans Bitcoin est très compétitive. C'est ce que l'on appelle des « pool » de minage. Aujourd'hui le réseau est dominé par 8 pools. Chaque ordinateur dans un pool a une tâche particulière et la combinaison de ces petites tâches permet d'augmenter la vitesse de minage.

2. Enterprise à Genève qui utilise le bitcoin

Une rigoureuse étude mener de ma part sur le marché économique de Genève démontre aujourd'hui que près d'une dizaine d'entreprises ont décidé d'intégrer le Bitcoin dans leur fonctionnement. Certaines de ces entreprises ne sont plus existantes et ne peuvent faire objet d'analyse. D'autres, que nous allons vous présenter dans la suite, ont utilisé le Bitcoin comme moyen de paiement, alternative qui présente un nombre d'avantages considérables. C'est intéressant de noter que ces entreprises offrent des services dans des domaines très diverses, ce qui démontre bien le caractère multifonctionnel et adaptable du Bitcoin.

Pour bien comprendre l'analyse sur l'usage du Bitcoin dans la réalité économique, il convient d'abord d'adopter une approche théorique et ensuite, suivre l'application de cette théorie en pratique. Pour cette raison, nous avons choisi de vous présenter en premier lieu un tableau d'avantages et d'inconvénients du Bitcoin, mis en comparaison avec d'autres moyens de paiement largement utilisés en ligne, comme les cartes de crédit ou le paiement par internet (le service PayPal) (cf. Chapitre 1.1).

Une fois la comparaison effectuée, nous allons examiner l'implémentation de la monnaie virtuelle dans la pratique, en se basant sur la recherche effectuée auprès des entreprises et les questionnaires détaillés qu'on leur a présenté et dont les réponses on a reçu de façon orale (cf. annexe I). Nous allons utiliser 2 théories principales : la possibilité de faire appel à une entreprise tierce qui assure l'implémentation, le maintien et le fonctionnement du service ou le « do it yourself » approche, qui suppose des minimales connaissances préalables dans le domaine. Dans cet examen, nous allons nous pencher aussi sur les diverses méthodes d'installer le système.

2.1 Nombre d'utilisateurs de Bitcoin

2.1.1 En Suisse

En pratique, il est très difficile, voire quasi-impossible, de déterminer le nombre exact de personnes qui utilisent le Bitcoin en Suisse. Des essaies ont quand même été faits, par exemple par l'Ecole Polytechnique Fédérale de Zurich (EPFZ) qui monitore quotidiennement le réseau d'utilisateurs Bitcoin à des fins scientifiques. En avril 2014, sur demande du Conseil Fédéral, l'EPFZ a fourni un chiffre estimatif d'environ 3'825 adresses IP actives sur ce réseau à une date donnée. Ceci n'est qu'un nombre approximatif, mais démontre quand même que le Bitcoin s'est bien introduit dans la réalité économique de la Suisse.

2.2 L'utilisation pratique du Bitcoin

2.2.1 Les avantages pour les entreprises, utilisateurs du Bitcoin

2.2.1.1 Un taux de transaction avantageux

Comme déjà vu précédemment, tous les moyens de paiement usuels impliquent un taux de transaction quelconque. Le Bitcoin se diffère sur ce point, en assurant une utilisation qui est sur le long terme beaucoup moins coûteuse. Cette monnaie présente des choix devant l'entreprise – on peut l'intégrer sur un site d'e-commerce ou bien physiquement dans les magasins de l'entreprise. L'installation et le maintien du système n'exigent pas un investissement coûteux – il suffit d'avoir une impression papier du QR Code du compte auquel l'argent doit être transféré par le client et un porte-monnaie qui se crée gratuitement. Cela implique par conséquence aussi un ordinateur, tablette voire smartphone pour pouvoir contrôler l'arrivée de la monnaie et la consultation du compte privé de l'entreprise.

Cela dit, le Bitcoin est sans doute un investissement beaucoup moins coûteux que ce qu'on utilise généralement dans le quotidien.

Le transfert de porte-monnaie à porte-monnaie est gratuit tandis que la conversion du Bitcoin à une monnaie fiat (Franc Suisse, l'Euro…) peut selon le moyen utilisé avoir un taux de conversion mineur dépendant du moyen utilisé.

Un papier publié en 2013 par Paypal nommé «Modern Spice Routes : The Cultural Impact and Economic Opportunity of Cross-Border Shopping », prévoit qu'en 2018, 94 millions de consommateurs interviewés sur 6 questionnaires dépenseront au total plus 397 milliards d'USD en achat transfrontalier. Chaque transaction à l'étranger génère des taxes pour la société. En revanche, le Bitcoin lui ne différencie pas un achat

effectué dans le même pays ou à travers le monde, ce qui peut éviter des frais exorbitants.

2.2.1.2 Protection contre les fraudes de cartes de crédit amélioré

La pratique connaît souvent des cas de fraudes sur Internet, ce qui consiste dans l'achat de biens sur des sites, sans l'intention d'effectuer le paiement de la prestation. Au moment de l'expédition du bien par le vendeur, l'acheteur demande généralement l'annulation de la facture et le remboursement direct de l'argent transféré (ce qui est accepté pour la plupart des cartes de crédit, dans une certaine période après l'achat). Dans ce cas, le bien arrive chez le destinataire mais le paiement n'est pas effectué.

Le Bitcoin protège l'entreprise de cette fraude. Au moment où la monnaie est transférée (suite au scan de QR Code par le client et sa confirmation), les bitcoins se trouvent désormais dans le porte-monnaie de l'entreprise et le client ne peut pas annuler l'ordre donné, par une simple demande de remboursement. Le client devra passer par l'entreprise pour récupérer ces bitcoins.

2.2.1.3 Sécurité au moment de dépense

L'implémentation du Bitcoin permet de renforcer la sécurité et d'éviter une mauvaise utilisation des avoirs de l'entreprise par les personnes concernées. Il est possible et largement accepté que plusieurs personnes doivent mettre des signatures (ou des mots de passe respectives) afin de pouvoir se servir du Bitcoin en possession de l'entreprise. C'est très utile en pratique, afin d'assurer que toute dépense des bitcoins a été justifiée et suit l'action voulue de l'entreprise.

2.2.1.4 Anonymat

Le Bitcoin est un moyen qui assure un grand niveau de discrétion et de confidentialité si utilisé correctement. Une entreprise qui veut garder ses transactions privées a le moyen de le faire, puisque les transactions bitcoins sont non nominatives. En principe, tout transfert est inscrit dans le « blockchain », où tous les utilisateurs sont inclus. Cette base de données est extrêmement grande et de ce fait, difficile à déchiffrer et à retrouver des traces personnelles quelconques. Par conséquent, en pratique, les transactions avec des bitcoins sont souvent « cachées » par un rideau d'anonymat. Il est possible de passer que par un réseau TOR[5] pour accroitre son anonymat.

[5] Tor Onion Routing, réseau international lié par des nœuds qui transmettent de façon anonyme le signal.

Clicours.COM

2.2.2 Les inconvénients du Bitcoin

2.2.2.1 Facile à perdre

Le Bitcoin est en principe géré par un porte-monnaie virtuel, propre à chaque utilisateur. Il y a des différents types de porte-monnaie qui ont déjà été présentés plus haut (cf. 1.3.4). En fonction du choix qui a été fait par l'utilisateur, il peut y avoir des pertes irrécupérables du Bitcoin, puisque la virtualité crée toujours un risque. Dans le cas d'un porte-monnaie très sécure, l'utilisateur peut rencontrer des problèmes (p.ex., la perte du mot de passe le laisserait « en dehors » et il perdrait l'accès complet à ses bitcoins, parfois même pour toujours, étant donné que le niveau de sécurité de récupération du mot de passe peut être accru et insistant). Les porte-monnaie moins sécures évitent ce risque, mais ils sont plus susceptibles d'interventions externes. Le choix est donc entre les mains de l'utilisateur.

2.2.2.2 Très volatile

La valeur du bitcoin est très fluctuante et fait souvent objet de modifications drastiques d'un jour à l'autre. Cette volatilité peut présenter un inconvénient, car elle peut provoquer des pertes inattendues dans l'entreprise. En outre, cela oblige souvent les commerçants d'effectuer des changements journaliers dans les prix des produits affichés en bitcoins, afin de pouvoir garder un équilibre financière. En pratique, ce défaut est un problème mineur pour 2 raisons principales. Tout d'abord, il est rare que les utilisateurs gardent les bitcoins en état, sans les échanger pour une monnaie ordinaire (comme le CHF ou l'Euro). De surcroît, il existe des applications notamment web spécifiques qui permet de mettre à jour le prix affiché du produit au moment de la vente.

2.2.3 Porte-monnaie Bitcoin

2.2.3.1 Présentation des plus utilisé

Comme présenter dans la partie théorique il a actuellement 3 différents types de porte-monnaie : Mobile, Web, Desktop. Parmi ces 3 types, nous allons nous concentrer principalement sur 2 des porte-monnaie, au regard du fait que la version mobile n'est pas orientée sur les entreprises mais est destinée plutôt à un usage personnel. Il est malheureusement impossible de dire avec certitude quelles sont les porte-monnaie les plus utilisés, puisqu'une personne peut gratuitement télécharger et utiliser plusieurs différents.

2.2.3.2 Web

Il est difficile de choisir un porte-monnaie pour une entreprise, puisqu'en réalité, tous les porte-monnaie présentent des fonctionnalités similaires:

- Encryption du porte-monnaie avec mot de passe
- Backup
- Multisignature

Parmi les porte-monnaie Web les plus populaires nous trouvons :

- Blockchain
- Bitcoin Core
- StringCoin
- BTCinch

En réalité, le choix effectué par une entreprise est plutôt personnel que lié à des raisons techniques.

2.2.3.3 Desktop

Le téléchargement de ce type de porte-monnaie dépend tout d'abord de l'OS utilisé. En fait, le Dekstop ne présente pas beaucoup de différences au niveau des fonctionnalités que le porte-monnaie Web (elle implémente aussi l'encryption du porte-monnaie avec le mot de passe et les hachages, les backups, la multisignature). Elle a une fonctionnalité plus spécifique qui est l'utilisation du mode offline.

Les porte-monnaie Dekstop les plus populaires selon l'OS sont :

PC: • Bitcoin-QT the official client • Armory • Electrum • Multibit	Mac: • Bitcoin-QT the official client • Armory • Electrum • Multibit
Linux: • Armory • Electrum • Multibit	Ubuntu: • Armory

2.3 Comment intégrer Bitcoin a son Entreprise

La première étape obligatoire avant de se lancer dans la création du porte-monnaie est de définir la stratégie actuelle et future dans l'entreprise s'agissant du comment les biens et services seront vendus. Dans cette étude nous allons nous baser sur les 2 principaux canaux de vente. La vente sur internet ainsi que la vente dans un lieu propre à l'entreprise (point de vente). Il faut aussi décider si les bitcoins seront convertis en monnaie fiat ou gardés en tant que bitcoins. Comme expliqué plus haut, garder ces bitcoin en état est fortement risqué étant donnée la volatilité de la monnaie.

Dans tous les cas un porte-monnaie est obligatoire si l'usage du Bitcoin est souhaité. La création du porte-monnaie est gratuite.

Si l'entreprise est spécialisée dans la vente sur internet via un magasin le mode de fonctionnement restera la même.

Il est important de ne pas oublier de référencer son entreprise sur les différents sites qui récence les magasins qui acceptes les bitcoins. Les 2 plus connue étant Bitcoin.travel et coinmap.org.

2.3.1 Physiquement

Mettre en place le Bitcoin dans un point de vente ne présente pas de complexité et n'exige pas de connaissances spécifiques. Le plus compliqué est de choisir le porte-monnaie adéquat. Une fois le porte-monnaie installé, il suffit d'imprimer son QR code et le tour est joué.

2.3.2 Site de vente sur internet

Comme pour le point de vente, choisir son porte-monnaie est très important. Ensuite, la mise en place du Bitcoin sur un site-web de vente dépendra principalement de la technologie voulue. Si un CMS (Content management system) est utilisé tel que WordPress, un plugin aura de très grande chance d'exister. WordPress en l'occurrence propose un plugin développé par Bitpay.com[6]. Malgré ses petites spécificités, le choix est complètement laissé aux utilisateurs. Le site de Bitpay.com est spécialisé dans les plugins avec plus de 15 plugins open source ou encore 10 CMS intégrant de base leurs solutions. Pour les plus téméraires Bitpay a en plus mis à disponibilité leurs librairies : PHP, Node.js et Ruby. Pour un contrôle total, leur API est disponible.

[6] https://bitpay.com/bitcoin-for-ecommerce

2.4 Présentation des entreprises

Pour pouvoir dresser un bilan de pratique, nous nous sommes d'abord penchés sur la recherche des entreprises à Genève qui utilisent le Bitcoin comme moyen de paiement dans leur activité journalière. Il est important de noter qu'il n'existe pas une liste de toutes les entreprises utilisatrices qui est tenue à jour ou qui est complète. Cependant, nous nous sommes servis de deux sites-web qui présentent des données sur des sociétés qui ont implémentée la monnaie virtuelle.

2.4.1 bitcoin.travel

Bitcoin.Travel est le plus vieil annuaire de Bitcoin mondial. Il a été créé en 2011 et est géré par une entreprise externe. Le site est basé sur le principe que chaque entreprise peut soumettre sa candidature pour être ajoutée aux listes officielles. La seule exigence posée est que l'entreprise en question ait affiché sur son propre site web que le Bitcoin est accepté dans ses affaires. Tous les 3 mois, une procédure de re-listing est lancée par bitcoin.travel pour que la base de données soit toujours à jour. En novembre 2015 (date de la dernière consultation), aucune entreprise, basée à Genève, n'était indiquée sur les listes. En outre, seulement 2 sociétés Suisses étaient présentes. Malgré cela, bitcoin.travel est l'endroit populaire pour toute entreprise qui a envie de s'ajouter au réseau Bitcoin et affirmer l'utilisation de la monnaie.

Figure 13 : Bitcoin.travel

2.4.2 Coinmap.org

Coinmap.org fut déployé en mai 2013 et à la différence des autres sites, il est basé sur OpenStreetMap, ce qui signifie que toute personne est libre et encouragée à collaborer pour le développement. Le site fonctionne sur le support de la communauté et donc la notion de confiance joue un rôle important. Il répertorie une dizaine d'entreprises à Genève dont nous avons effectué la vérification. Une partie de ces sociétés n'existe plus depuis octobre 2015. Le site présente plus de 7300 sociétés & bancomats à travers le monde et ce nombre ne fait que croitre chaque jour. Le site compte approximativement 130 entreprises et bancomats en Suisse seulement.

Figure 14 : Coinmap.org 2.0

Ci-dessous ce trouve un liste non exhaustive des entreprise qui utilisent le Bitcoin à Genève. Ces entreprises ont été repérées sur le site coinmap.org. Dix entreprises à Genève sont recensées ; parmi elles, trois sont probablement des plateformes d'échange de Bitcoin.

2.4.3 Café Moka

Présentation : Café à côté de la gare

Adresse : La Voie-Creuse 3

Date d'entrée du Bitcoin : 7/6/2013

Nombre de clients par mois : Environ 1 client par mois

Figure 15 : Café Moka

2.4.4 Venuisa

Présentation : Salon érotique

Adresse : Rue Rodo 2, 1205 Genève

Date d'entrée du Bitcoin : juin 2014

Nombre de clients par mois : 1-2

Figure 16 : Venuisa

2.4.5 Magicom

Présentation : Petit magasin de vente, spécialisé dans la vente de portables, gadgets et appareils électroniques.

Adresse : Rue Paul-Bouchet 6, 1201 Genève

Date d'entrée du Bitcoin : Juin 2014 - Septembre 2015

Nombre de clients par mois : 3-4

Figure 17 : Magicom

2.4.6 Zurich 6

Présentation : Café bar au Paquis.

Adresse : Rue de Zurich 6, 1201 Genève

Date d'entrée du Bitcoin : Décembre 2013

Nombre de clients par mois : 0

Figure 18 : Zurich 6

2.4.7 Meeting Point

Présentation : Café bar à Rive

Adresse : Carrefour de Rive 1, 1207 Genève

Date d'entrée du Bitcoin : Janvier 2014

Nombre de clients par mois : 1-2

Figure 19 : Meeting Point

2.4.8 Tokyonama

Présentation : Boutique Japonaise

Adresse : Rue de Carouge 75, 1205 Genève

Date d'entrée du Bitcoin : Juin 2014

Nombre de clients par mois : 0-1

Figure 20 : Tokyonama

2.4.9 EverdreamSoft

Présentation : Entreprise spécialisé dans le développement de jeux vidéo

Adresse : Rue de la Muse 2, 1205 Genève

Date d'entrée du Bitcoin : Janvier 2014

Nombre de clients par mois : Inconnu

Figure 21 : EverdreamSoft

2.4.10 Bitcoin Suisse SA

Présentation : Entreprise de courtage possédant un réseau de bancomat Bitcoin. Spécialisé dans l'achat-vente de Bitcoin ainsi que le consulting.

Adresse : Lättichstrasse 1, 6340 Bâle

Figure 22 : Bitcoin Suisse SA

2.5 Synthèse des entretiens

Toutes les entreprises présentées ci-dessus ont fait objet d'un entretien personnalisé portant sur l'implémentation, le fonctionnement et l'usage du Bitcoin dans leur domaine. Le questionnaire détaillé utilisé lors de ces entretiens se trouve en annexe de la présente contribution.

Par conséquent nous pouvons synthétiser les résultats de la manière suivante :

- Un manque de connaissance sur la présence et l'utilisation du Bitcoin se manifeste parmi le personnel dans la grande majorité des entreprises. Cela est généralement dû à deux raisons principales. D'abord, les travailleurs sont souvent mal informés du fait que l'entreprise accepte et traite avec des bitcoins et ne présentent pas cette possibilité au client lors du paiement des services. A cela s'ajoute le fait que très peu de personnes en Suisse et plus particulièrement à Genève font usage de cette monnaie virtuelle pour leurs transactions. La non-popularité du Bitcoin est aussi une des raisons principales du nombre bas des entreprises utilisatrices.

- Un grand nombre des entreprises interviewées ne mettent pas l'accent sur la possibilité de payer avec des bitcoins. Seulement trois parmi eux ont décidé d'afficher un mini panneau statuant sur l'usage de la monnaie virtuelle dans l'entreprise (en pratique, cela fonctionne par un autocollant sur le même principe que l'autocollant pour les cartes de crédit, que nous pouvons facilement trouver sur les vitrines des commerces). Cela démontre que le but principal de l'usage du Bitcoin n'est pas la vraie prise de connaissance des clients avec cette monnaie, mais plutôt une façon de provoquer de la publicité en faveur de l'entreprise, par l'implémentation de cette mode de paiement inhabituel.

- C'est intéressant de noter que les entreprises qui ont servi à la recherche sont toutes des petits commerces qui ne disposent pas d'un magasin en ligne et toute transaction se passe sur place, dans les locaux, après l'accomplissement de leurs services.

- Toutes les entreprises, à l'exception d'une, opèrent une conversion des bitcoins reçus en Francs Suisses. Certaines le font directement après la transaction et d'autres le font à la fin du mois, en effectuant leur comptabilité mensuelle. Aucune des entreprises ne dispose de renseignements sur les aspects fiscaux

et légaux de cet échange, qui ne présentent par ailleurs pas de particularités par rapport aux conversions usuelles des monnaies officielles.

- Au niveau de l'implémentation du Bitcoin, nous avons obtenu un résultat divergeant, puisque des pratiques différentes sont possibles. Une partie des entreprises ont effectué les installations nécessaires elles – même, sans des interventions externes. D'autres ont été assisté par des clients, qui ont non seulement soulevé l'idée d'utilisation du Bitcoin, mais ont préparé tout le système et matériel nécessaire pour l'entreprise, puisqu'ils disposaient de fortes connaissances dans le domaine de l'informatique. Seulement dans une des entreprises une société externe a participé dans les installations, en octroyant de l'aide et des conseils pratiques. Cette société souhaite ne pas être nommée dans le cadre de cette recherche. De cela, nous pouvons tirer la conclusion que l'implémentation du Bitcoin peut être faite par toute entreprise, sans nécessité d'intervention externe (société tierce) ou des savoir-faire spécifiques.
- Quant aux résultats de cet usage, seulement une des entreprises a connu une augmentation de clientèle, suite à l'introduction du Bitcoin (environ 4-5 clients par mois de plus).

En conclusion de ces entretiens, l'implémentation du Bitcoin dans l'entreprise présente un coût très faible et ne produit pas par la suite de frais de maintenance au niveau matériel, ce qui est un avantage considérable. En revanche, l'usage de la monnaie virtuelle n'entraîne pas une augmentation de la clientèle, vu le nombre bas d'utilisateurs en Suisse. Pourtant, une telle introduction crée un coup de publicité non-négligeable puisque cela est perçu par la société comme une innovation, modernisation des moyens de paiement, voire une entrée dans le futur.

Conclusion

Est-ce que le Bitcoin est vraiment la monnaie du futur ?

Le Bitcoin est encore aujourd'hui un sujet intéressant qui passionne des personnes de tous les domaines de la société. Il est adaptable et facile à utiliser, sans que des connaissances techniques spécifiques soient nécessaires. Le marché économique d'aujourd'hui démontre qu'il peut être implémenté dans toutes les sphères et servir à des buts différents. L'anonymat, le coût très bas et la sécurité qu'il présente au moment de la dépense sont des avantages attirants et non-négligeables.

Au niveau technique, le Bitcoin présente aussi des nouveautés et a créé un véritable progrès technique dans ce domaine. On peut dire que le blockchain, la base du réseau, est une innovation, un pas dans le futur des technologies informatiques. Le nombre élevé d'articles scientifiques et de divers matériaux sur le sujet du Bitcoin démontre que la tendance n'est pas encore complètement dépassée et qu'un développement et un saut inattendu ne sont pas exclus. Le Bitcoin a réussi à changer notre vision sur la monnaie et les possibilités technologiques qui sont devant nous.

En conclusion, le Bitcoin reste une invention étrange, mais passionnante. Son grand coup de publicité en 2013/2014 a fait beaucoup de personnes s'intéresser et se lancer dans le « minage », mais voici l'aspect de l'utilisation commerciale du Bitcoin dans notre vie de tous les jours, non pas comme un moyen de faire de l'argent, mais comme un moyen d'en dépenser.

Bibliographie

Satochi Nakamoto, 24 Mai 2009, *Bitcoin: A Peer-to-Peer Electronic Cash System* - https://bitcoin.org/bitcoin.pdf

FINMA. Bitcoins. *FACT SHEET* 25.06.2014 - Swiss Financial Market Supervisory Authority, 2014.

O'REILLY RADAR SUMMIT, 2015, Bitcoin & the Blockchain: Realities, Risks, Rewards - http://conferences.oreilly.com/bitcoin-blockchain-2015

Confédération Suisse, décembre 2014, *Documentation pour la conférence de presse concernant le cas des commissions domestiques d'interchange pour les cartes de crédit II (KKDMIF II)*
http://www.news.admin.ch/NSBSubscriber/message/attachments/37692.pdf

Confédération Suisse, 25 juin 2014, *Rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070)* https://www.news.admin.ch/NSBSubscriber/message/attachments/35353.pdf

Confédération Suisse, 2015, Impôt fédéral direct 2014 - https://www.ictax.admin.ch/extern/fr.html#!/ratelist/2015

PayPal, 2014, *Modern Spice Routes: The Cultural Impact and Economic Opportunity of Cross-Border Shopping.*
https://www.paypalobjects.com/webstatic/mktg/2014design/paypalcorporate/PayPal_ModernSpiceRoutes_Report_Final.pdf

Ecurex & Deutsche Bundesbank, Paolo Tasca, 2015, *Digital Currencies: Principles, Trends, Opportunities, and Risks.*

REUBEN GRINBERG, 2011, Bitcoin: An Innovative Alternative Digital Currency

Félix BREZO and Pablo G. BRINGAS, 2012, *Issues and Risks Associated with Cryptocurrencies such as Bitcoin*

PEDRO, Franco, 2015, *Understanding Bitcoin: Cryptography, Engineering and Economics.* ISBN 9781119019152

Conrad BARSKI & Chris WILMER, 2014, The *Blockchain Lottery: How Miners Are Rewarded* - http://www.coindesk.com/blockchain-lottery-miners-rewarded/

BitcoinArmory, 2015, *FAQ* - www.bitcoinarmory.com/faq/

Bitcoin.org, 2015, *Securing your wallet* - https://bitcoin.org/en/secure-your-wallet

Bitcoin.org, 2015, *Bitcoin Developer Guide* - https://bitcoin.org/en/developer-guide

Coindesk.org, Octobre 2015, How to Store Your bitcoins –

http://www.coindesk.com/information/how-to-store-your-bitcoins/

BitcoinIntro, 2015, An Introduction to Bitcoin: Wallets - http://bitcoinintro.com/wallets/

BitcoinWiki, 2015, Block chain - https://en.bitcoin.it/wiki/Block_chain

BitcoinWiki, 2015, Private Key - https://en.bitcoin.it/wiki/Private_key

BitcoinWiki, 2015, Address - https://en.bitcoin.it/wiki/Address

BitcoinWiki, 2015, Minning, https://en.bitcoin.it/wiki/Mining

Wikipedia, 2015, Bitcoin Network, - https://en.wikipedia.org/wiki/Bitcoin_network

DORIT Ron & ADI Shamir, 2012, *Quantitative Analysis of the Full Bitcoin Transaction Graph* - http://eprint.iacr.org/2012/584.pdf

Annexe 1 :
Questionnaire: Le Bitcoin dans la réalité économique

(Questionnaire destiné à la réalisation du Travail de Bachelor, dans le cadre de la formation « Informatique de gestion » de la Haute Ecole de Gestion, Genève).

1. Depuis quand acceptez-vous le Bitcoin comme moyen de paiement dans votre entreprise ?
2. Pourquoi avez-vous décidé d'intégrer la monnaie virtuelle à votre entreprise ?
3. Combien de personnes par mois en moyenne utilisent le Bitcoin pour le paiement de vos prestations ? Combien le font par jour ?
4. Est-ce que vous pensez que le Bitcoin attire des nouveaux clients ?
5. Indiquez quelle méthode a été utilisée pour implémenter le Bitcoin (entreprise tierce/ par vous-mêmes). Indiquez la marche à suivre pour demander le Bitcoin, ainsi que les machines physiques qui sont installées dans l'entreprise pour permettre l'utilisation.
6. Selon la marche de l'entreprise et le coût de l'installation, diriez-vous que le Bitcoin présente des avantages financiers ?
7. Quels sont, à votre avis, ses inconvénients ?
8. Quel moyen de stockage utilisé vous pour les bitcoins reçus par les clients ? Préférez-vous les garder en état de monnaie virtuel ou transférez-les vous sur un compte bancaire, moyennant leur échange en francs suisses ?
9. Au moment de la transaction, le client doit en principe scanner votre QR Code pour transférer les Bitcoin. Sur quel type de support physique ou virtuel se trouve le Code (par exemple, sur une tablette, un smartphone à disposition ou un papier) ?
10. Comment vérifiez-vous que les Bitcoin sont bien arrivés sur votre compte ? Y-a-t-il un moyen d'en être informé instantanément ?
11. Conseillerez-vous ce moyen de paiement à d'autres entreprises ? Estimez-vous que cela présente un avenir pour le marché économique, et plus spécifiquement dans votre domaine particulier ?

Annexe 2 : Echange email – Roland Godel

Mon email 20/11/2015 :

Cher Monsieur Godel,

Je me permets de vous contacter suite à notre bref entretien téléphonique de la semaine dernière.

Je m'appelle William Bisol et je suis actuellement étudiant en dernière année à la HEG Genève, filière Informatique de gestion.

J'effectue mon projet de Bachelor sur le sujet du Bitcoin et son utilisation économique en Suisse. Pour pouvoir présenter un profil complet sur cette monnaie virtuelle, je m'intéresse vivement à l'aspect fiscal que l'utilisation du Bitcoin implique pour une entreprise. Suite à votre conseil, je vous adresse donc mes questions:

- Si une entreprise ayant son siège en Suisse procède à une activité de vente de biens et/ou de services et accepte des paiements avec des bitcoins, a-t-elle une obligation de convertir le Bitcoin en CHF après chaque transaction ou à la fin de chaque mois? Le cas échéant, comment indiquer cela dans la comptabilité?
- Est-ce qu'un taux de conversion existe actuellement pour le Bitcoin? Après consultation du site de l'Administration fiscale fédérale, j'ai pris connaissance avec les taux concernant les autres monnaies étrangers (comme l'Euro), mais il n'y a aucune indication concernant les monnaies virtuelles. Source : https://www.ictax.admin.ch/extern/fr.html#!/ratelist/2014

Dans l'attente de votre réponse, je vous prie d'agréer, cher Monsieur, mes salutations distinguées.

William Bisol

La réponse 10/12/2015:

Bonjour,

Voici les réponses que m'a données l'administration fiscale : les règles générales s'appliquent, à savoir que les comptes d'une entreprise, qui pratique ses échanges dans une monnaie autre que le franc suisse, doivent être présentés en francs suisses à la fin de l'année. Le taux applicable est celui au 31 décembre et c'est l'administration fédérale qui édite la liste des cours.

Vous trouverez des renseignements dans le document annexé, qui vient de la Confédération (en allemand, malheureusement).

Cordialement,

Roland Godel
Secrétaire général adjoint chargé de la communication

Note : Le document annexe mentionné par Monsieur Goland est cité dans la bibliographie.