Monnaies virtuelles
Le cas Bitcoin : (2ème partie)

Risques et rapports à la cybercriminalité et au blanchiment

Après avoir évoqué le besoin de confiance dans les monnaies et vu leurs différentes formes ainsi que le statut juridique du Bitcoin, ses principes et son fonctionnement, puis ses paradoxes et sa portée dans un espace d'échanges ouverts à tous, l'auteur se propose maintenant d'en indiquer les rapports à la cybercriminalité et au crime organisé, y compris avec le blanchiment. En montrant les enjeux et les risques, en l'absence de régulation et de garanties, avec les besoins en matière de sécurité et d'encadrement, il sera tenté de conclure et notamment de répondre à la question : Pourquoi tant d'emballement ?

BITCOIN : ATTEINTES ET MOYEN DE BLANCHIMENT

Si le Bitcoin est une devise virtuelle populaire qui intéresse les négociants et les épargnants, comme le monde financier, il a surtout aiguisé l'intérêt de la cybercriminalité, compte tenu de son niveau de prix et de ses variations. Les créateurs de logiciels malveillants seront tentés d'exploiter tous les canaux, pour dérober les portefeuilles en menant des cyber-attaques ou pour extraire des Bitcoins par «*mining*» en utilisant les ressources informatiques des victimes. L'ingénierie sociale sera utilisée pour recueillir des informations sensibles sur les fonds. Les «*botnets*» contribueront à réaliser une extraction plus efficace en mettant de nombreuses machines victimes en pool et à permettre des cyber-attaques d'envergure par déni de service distribué (D-DoS) contre les principaux sites et services d'échanges, susceptibles de réduire le niveau de confiance et de causer une chute brutale de la valeur du Bitcoin. Ainsi initiés, les cybercriminels pourraient aisément spéculer par l'achat et la vente de volumes importants au bon moment et en tirer un grand profit. L'usage de Bitcoin apparaît aussi au niveau de boutiques du Web « *invisible* », qui servent de vitrines au crime organisé, pour la vente de marchandises : faux papiers, armes, contrefaçons, stupéfiants, données de cartes bancaires, etc., et de services : tueurs à gages (ex. Hitmann Network), prostitution, dons à des organisations terroristes, pornographie enfantine[1]. Des sites comme Silk Road et BlackMarket Reloaded, Sheep marketplace, CC.Planet.onion, etc., pour la plupart fermés, mais remplacés par d'autres, offraient une telle vitrine.

Typologie des risques

Les principales menaces proviennent notamment des développeurs, des traders et administrateurs de plateformes, et de la cybercriminalité[2], au regard du vol de données sensibles et de portefeuilles, et des manipulations de cours. Les vulnérabilités structurelles sont liées aux protocoles, aux algorithmes et à leur implantation sous forme de programmes informatiques, sans garantie par une certification à un niveau de confiance suffisant[3]. Les vulnérabilités conjoncturelles sont liées à la nouveauté et à l'apparente simplicité de Bitcoin autant qu'à la faible sensibilisation des utilisateurs qui ne prennent pas assez au sérieux la sécurité de leurs systèmes, en particulier mobiles. En outre, les attaques ne sont pas exclusives aux PCs sous Windows, par exemple, fin 2011, le code malveillant DevilRobber s'est répandu sous Mac OS X par le biais de sites Web compromis depuis un raccourci d'URL d'un spam ou depuis Facebook ou Twitter, pour infecter des machines Apple en nombre et constituer un «*botnet*».

Outre les risques d'atteinte des intérêts légitimes des usagers par des cybercriminels, le Bitcoin offre en plus des avantages à la cybercriminalité. Ceux-ci sont liés à l'instantanéité et à l'irréversibilité des opérations, mais également, à l'opacité et à un certain niveau d'anonymat, pour réaliser et masquer des transferts financiers relevant d'actes illicites par leur blanchiment.

Atteinte aux portefeuilles Bitcoin

Le vol de Bitcoins s'est développé avec la popularité de Bitcoin[4]. Les attaques exploitent le manque de sécurité des systèmes et des portefeuilles, notamment par la découverte du mot ou de la phrase de passe, qui reste malgré tout vulnérable à la présence d'un cheval de Troie de type «*keylogger*» ou à une attaque par rejeu si le serveur a été compromis par un code malveillant, ce qui permet aux pirates d'accéder au portefeuille de l'utilisateur, chiffré ou non.

L'auteur d'un logiciel dénommé «*Bitcoin Jacker*» encourage autrui à utiliser son code malveillant pour la recherche systématique de portefeuilles en Bitcoins et ensuite les copier sur un serveur FTP public afin de permettre à un maximum de

personnes de tenter d'en déchiffrer le contenu par des essais en force brute de mots de passe faibles, dans le but d'en voler les Bitcoins[5]. Le couplage de ce dernier à un logiciel «*keylogger*», (ex. Private Keylogger), sera naturellement plus efficient, pour pouvoir saisir à la volée les mots de passe des portefeuilles introduits au clavier par l'utilisateur légitime, et ainsi les rendre immédiatement utilisables sans passer par la seconde phase. D'autres logiciels comme «*Bitcoin Infostealer.Coinbit*» ont été créés dans l'intention similaire de découvrir des portefeuilles non chiffrés pour les transmettre par l'intermédiaire d'un serveur de messagerie.

Le marché noir participe en continu à l'amélioration apportée par des groupes criminels qui louent ou vendent leurs services sur le Web «*invisible*».

Atteinte aux ressources du «mining»

Concernant le «*mining*» pratiqué en nuage ou au travers d'un pool centralisé ou non, il existe une menace d'attaque par déni de service distribué (D-DoS) ou de pratiques malhonnêtes internes. Dans tous les cas, y compris avec un logiciel fourni et installé localement, le risque lié à un code malveillant est une constante qui dépend du niveau de sécurité de l'ensemble utilisé, même si le système Bitcoin vérifie la validité de chaque transaction et peut se protéger de plusieurs formes d'attaques. En effet, en 2011 il a été vu le détournement de temps CPU de machines distantes par des codes JavaScript pouvant fonctionner comme outils de «*mining*» à l'insu des visiteurs de sites Web. En 2013, il a été découvert de façon croissante plus de 5000 codes binaires exécutables permettant un tel détournement sur une longue période.
Vu les propositions du marché noir sur le Web caché, il ne serait pas extraordinaire de découvrir que des microordinateurs sont ou ont été compromis par milliers pour constituant un «*botnet*» pour en détourner les ressources vers à une activité de «*mining*», non sans avoir repéré et dérobé les portefeuilles Bitcoin contenus[6]...

Atteinte liée à la malléabilité d'une transaction Bitcoin

Les transactions de Bitcoins exigent les données critiques usuelles à toute transaction. Il s'agit des adresses des portefeuilles de Bitcoins identifiant respectivement l'expéditeur et la destinataire, de la signature de l'expéditeur réalisée à l'aide de sa clé privée pour vérifier son consentement, de la clé publique du destinataire et du montant de la transaction. L'ensemble est combiné avec des données subsidiaires[7] puis haché pour produire un condensé unique, lequel est employé comme identifiant pour pister la transaction. Une variation, même infime, dans les données de transaction produirait un condensé totalement différent. Ces données et cet identifiant sont alors inclus dans la blockchain pour vérification par les mineurs. Les fonds seront transférés à condition que ces données soient intégralement présentes et que les identifiants reçus et calculés soient identiques. Dans le cas contraire, la transaction serait rejetée.
Il en découle une vulnérabilité dénommée «*malléabilité de transaction*» qui peut être exploitée. Il est en effet possible de procéder à des changements dans les données qui produiront un condensé différent de celui d'origine, sans infirmer la transaction mutée. Pour cela, cette dernière devra être relayée pour être annoncée avant la transaction d'origine aux nœuds les plus importants, pour augmenter la réussite de se voir inclure dans la blockchain. Ces transactions seront traitées en tant que double au niveau de cette dernière et la transaction mutée sera confirmée au détriment de celle d'origine et les fonds seront transférés vers le destinataire indiqué.
L'emploi d'une telle vulnérabilité permettrait aux attaquants de réaliser des milliers de transactions pour transférer des Bitcoins sur des comptes intermédiaires puis de les transférer vers d'autres, avec des difficultés de traçabilité[8].

Bitcoin en faveur du blanchiment

Il est recherché une anonymisation renforcée, le masquage des origines et l'obscurcissement de l'historique des Bitcoins, en particulier s'ils sont issus ou participent à des activités illégales, tout en permettant des dépôts et retraits immédiats et automatiques, avec de surcroît des adresses multiples pour être au service de la logistique financière et un instrument de blanchiment. BitLaunder.com annonce clairement ce service en passant par l'application BitLaunder. De plus, le support de la carte BitPlastic permet la conversion des Bitcoins en argent comptant de façon anonyme à partir de distributeurs ATM ou des transferts variés, notamment par Western Union. Les offres ne manquent pas sur l'Internet : bitlaundry, coinchimp, etc., autant prometteuses que risquées et sans garanties toutefois de ne pas voir les Bitcoins disparaître...

Bitcoin étendu à la vente de secrets

DarkLeaks[9] apparaît comme une nouvelle plateforme de marché noir décentralisé pour l'achat et la vente anonymes de données sensibles ou de secrets, fondée sur la technologie blockchain de Bitcoin[10].
Les développeurs présente Darkleaks comme le meilleur outil actuel d'échanges de tout type de données secrètes, illégales ou confidentielles : secrets industriels et commerciaux, vulnérabilités «*O-day*», bases de données volées, etc. Les fichiers mis en vente sur le site DarkLeaks sont chiffrés, divisés en parties, puis ajoutés à la blockchain Bitcoin. Ceci permet à l'acheteur de vérifier une partie en clair comme aperçu, avant la décision d'achat pour le paiement, à l'issue duquel une clé de décryptage est fournie à l'acheteur pour déchiffrer le document en entier.

BITCOIN : SÉCURITE ET ANONYMAT

Mesures inhérentes à la sécurité attendues

Bitcoin étant un système de crypto-monnaie informatique décentralisé, sa maîtrise repose sur la sécurité cryptologique et informatique et celle des réseaux pour contrer les menaces.

Compte tenu des enjeux, le niveau d'assurance des fonctionnalités de sécurité est essentiel et devrait être démontré par une certification, dès la conception jusqu'au paramétrage et à l'utilisation. En outre, l'apport permanent de correctifs est indispensable pour réduire les vulnérabilités.

Au niveau de l'utilisateur, la sécurité dépend de plusieurs éléments. Il s'agit de l'objet numérique employé et du système d'exploitation installé, de l'application Bitcoin de génération et de gestion du portefeuille électronique, et du portefeuille lui-même. La sécurité du navigateur et des serveurs distants et de la transmission est également concernée.

Concernant les portefeuilles Bitcoin, les mesures de prévention visent à éviter la compromission et le détournement des clés et des fichiers sensibles (ex. wallet.dat). Il s'agit de disposer d'un mot de passe de qualité pour le stockage et la mise en ligne, d'envisager le chiffrement des données sensibles et de s'assurer d'un couple de clés unique à chaque transaction pour améliorer l'anonymat. Les mesures de protection sont nécessaires en cas de vol ou de pertes matérielles et pour maintenir l'intégrité des portefeuilles. Il s'agit de disposer de sauvegardes sûres et régulières et sur un autre support des fichiers vitaux, en particulier des portefeuilles, sans lesquels les Bitcoins de ces derniers seraient perdus. Un portefeuille sur support papier représenterait l'enregistrement de données privées employées pour stocker des Bitcoins dans un format autre, restant toutefois sensible au vol comme un billet de banque. Un portefeuille sur support microélectronique augmenterait la sécurité et la facilité d'usage, au mieux comme substitut d'une carte bancaire, mais avec une moindre à garantie et des frais supplémentaires.

Des failles de la sécurité étant régulièrement découvertes dans les systèmes d'exploitation comme dans les applications, il est indispensable d'appliquer au plus vite les corrections authentifiées. En raison de la fréquence des compromissions, il est conseillé de chiffrer les portefeuilles, ainsi que les mots de passe, les clés privées et d'autres données sensibles employées, sinon de les maintenir sur une image chiffrée de disque dur créée par un logiciel tiers digne de confiance[11]. En effet, un fichier comme wallet.dat étant en texte clair, n'importe qui pourrait accéder à un portefeuille non chiffré et récupérer les Bitcoins contenus.

Si les portefeuilles sont en ligne, il est possible d'accéder, légitimement ou non, aux portefeuilles depuis n'importe quel ordinateur dans le monde. Si le niveau de sécurité est insuffisant, le service peut être compromis et les Bitcoins seraient perdus. Un dispositif matériel[12] s'avèrerait utile pour contenir les données sensibles : clés privées, mots de passe, adresse électronique, tandis que ce mode d'accès en ligne se résumerait à annoncer au blockchain des transactions signées à l'aide de ce dispositif matériel.
Par ailleurs, des applications mobiles Bitcoin sont disponibles pour envoyer des Bitcoins depuis un portefeuille par un code QR ou sans contact (NFC), ce qui ouvre à la possibilité de perte en cas de compromission du périphérique mobile. Les portefeuilles mobiles peuvent peut-être se révéler utiles pour réaliser de petites dépenses, mais pas pour stocker l'épargne en Bitcoins.

Défi lié à l'anonymat des uns et des autres

D'ordinaire, le secret et l'anonymat ont toujours joué un rôle central dans les échanges de monnaies et des transferts de fonds, le plus souvent pour la protection contre les voleurs et à l'opposé, parfois pour couvrir l'identité de personnes liées à des crimes et délits ou cherchant à échapper à la fiscalité.

Le nombre considérable d'utilisateurs d'Internet et des réseaux sociaux, la complexité et la diversité des systèmes : fixes, mobiles, ATM, etc., et des services, changent les transactions financières à un niveau jamais atteint en nombre et en variété, avec des déploiements rapides au niveau mondial.

Il s'agit de pouvoir tracer les transactions financières numériques liées au terrorisme et à la criminalité. Pour être en mesure de surmonter les défis techniques et organisationnels liés à la détection et à la surveillance de ces transactions, ceux-ci exigeront néanmoins une part de régulation et la collaboration des pouvoirs publics avec l'industrie, en appréhendant les changements culturels et technologiques au sein des organismes gouvernementaux. Avec Bitcoin, l'anonymat n'est pas une question simple alors que les utilisateurs sont déjà identifiés par des clés publiques.

Brèche dans l'anonymat utile à l'inforensique

Pour instaurer la confiance nécessaire à son développement et permettre la disponibilité des données par distribution, en l'absence d'autorité centrale, Bitcoin dispose de la blockchain qui contient en totalité l'historique des transactions accessibles à tous. Ceci permet la collecte de données qui y sont représentées et constitue une brèche dans l'anonymat qui ne peut donc être réel et complet, et donc une opportunité à exploiter lors d'investigations judiciaires.

L'analyse de ce registre permettrait de tracer un ensemble de transactions frauduleuses relevant d'un compte ou d'un pseudonyme, en rapport avec des paiements pour des services en ligne, des produits illicites, des demandes de rançon, des escroqueries, des opérations de blanchiment. Il serait ainsi possible de faire le rapprochement entre différents acteurs de réseaux illicites ou criminels : pirates, escrocs, activistes, etc., et de déterminer les groupes et acteurs les plus déterminants par l'analyse criminelle. Elle permettrait aussi de détecter des schémas frauduleux ou des anomalies lors des transactions, telles que la dispersion de montants, la création de plusieurs adresses Bitcoin pour des opérations de blanchiment, etc.

La blockchain s'avérera très utile à l'analyse inforensique pour la recherche de preuves numériques liées à Bitcoin. Des outils comme CryptoCrumb sont déjà dédiés à l'analyse de la blockchain, et d'autres, à la visualisation du réseau d'utilisateurs.

De façon annexe, la blockchain pourrait servir à véhiculer d'autres informations que les transactions financières. De façon ciblée ou non, il est en effet possible de diffuser des messages, des annonces et des images avec des fichiers variés : TXT, PDF, JPG, etc., associés à de fausses adresses Bitcoin. Cet usage parallèle serait alors en mesure de discréditer Bitcoin ou de lancer des «*spams*».

Des mesures et services anti-inforensiques apparaissent déjà, au prétexte du respect de la vie privée, en s'appuyant sur des monnaies voisines, mais plus anonymes et cryptées (ex. BitcoinDark), sur des protocoles spéciaux (ex. CoinJoint, Darksend+), sur un tiers de confiance intermédiaire.

CONCLUSION

Alors que les États-nations ont cherché à disposer de systèmes monétaires régulés par des accords internationaux longuement négociés pour assurer d'une certaine stabilité, les crises financières ont altéré la confiance. Dans ce temps, différentes technologies permettent d'imaginer d'autres systèmes et d'autres monnaies sur lesquels il faut s'interroger.

Bitcoin est un système décentralisé fondé sur un protocole technique implémentant des algorithmes sous forme informatique pour assurer des transactions. C'est aussi une unité de compte fractionnable qui circule sur son réseau pair-à-pair par Internet pour exercer un pouvoir de transformation et de gestion de sa propre masse monétaire. Sa maîtrise comme sa faiblesse reposent à la fois sur la sécurité cryptologique et informatique et sur la confiance au fur et à mesure de son histoire, depuis sa création en 2009.
La forte volatilité du taux de change du Bitcoin se traduit par des variations importantes promptes à des activités financières spéculatives ordinaires de toutes sortes et d'autres, associées à des actions visant à induire une perte de confiance. Malgré ces variations, les tout premiers adeptes de Bitcoin, et en particulier les créateurs, ont amassé des fortunes virtuelles quand la création de Bitcoins était facile, d'où leur incitation à maintenir le développement du système.
Un premier paradoxe est lié à la présence de Bitcoins dans des produits financiers qui sont des répliques de ceux classiquement rencontrés et que la communauté Bitcoin, après avoir cherché à s'écarter du système traditionnel, a maintenant besoin des banques et d'une certaine régulation, pour que Bitcoin puisse être largement admis. Un second paradoxe relève de son caractère inégalitaire du fait de la détention de sa masse monétaire par peu de personnes, à l'opposé d'une monnaie virtuelle circulante qui contribuerait à l'économie. Bitcoin se présentait comme une alternative au monopole bancaire, le voilà empreint d'une mainmise par ses créateurs !
Avec 12,5 millions de Bitcoins à la mi-2014 créés par «*mining*», soit l'équivalent de 6 milliards d'euros, et une limite de 21 millions qui devrait être atteinte aux environs de 2140, l'unité Bitcoin ne paraît pas avoir un poids suffisant pour pouvoir concurrencer les monnaies de référence. Il s'agit davantage d'une commodité générée par ordinateur plus qu'une monnaie. Outre le fait que le Bitcoin peut être considéré par certains comme une valeur de refuge ou un moyen anonyme, même si c'est un leurre, il n'est ni régulé ni garanti par les États. En outre, il est utilisé pour la vente de biens et de services interdits, le financement illicite et le blanchiment, facilitant les opérations du crime organisé et le développement des fraudes et trafics en tous genres. Les distributeurs automatiques de Bitcoins (BTM) et surtout les plateformes explicites dédiées au blanchiment y participent déjà, mais avec des frais et des risques importants. Avec les produits financiers complexes qui se développent en Bitcoins, l'origine des fonds restera difficile à déterminer du fait de flux engendrés et de l'opacité des mouvements sans réel contrôle. Bitcoin nécessite à l'évidence une régulation équilibrée dans le respect de la vie privée et des intérêts des personnes comme des États.
Compte tenu des risques informatiques généraux, que ce soit au niveau de l'utilisateur ou des plateformes, et d'autres inhérents aux principes de Bitcoin et en particulier aux portefeuilles, il n'est pas certain que le consommateur moyen sera tenté d'adopter le Bitcoin, en dehors des micro-paiements. En cela, Bitcoin s'inscrit dans un dilemme lié à l'acceptation ou non par les vendeurs et à la possession ou non par un nombre suffisant de consommateurs, pour pouvoir atteindre une masse critique.
Il faut ajouter que les mesures à mettre en œuvre pour durcir la sécurité des Bitcoins pourraient se traduire par plus de complexité et par des frais pas moins élevés que ceux des cartes bancaires, à niveau de sécurité comparable. Par ailleurs, si d'autres gouvernements que la Chine et la Russie déclaraient les paiements illégaux ou imposaient des gains de la vente des Bitcoins, comme les États-Unis, l'usage des Bitcoins pourrait être sérieusement compromis.

Les gouvernements et institutions financières seraient avisés de prendre la mesure et la portée de ce phénomène en apprenant des bienfaits comme des erreurs de Bitcoin pour faire mieux. Il y va de l'intérêt de l'économie et des citoyens et de la lutte contre le crime organisé, la cybercriminalité, le blanchiment et la finance criminelle. Ceci permettrait que Bitcoin ne soit pas vu seulement comme une aubaine pour certains et pour d'autres, un moyen d'évasion fiscale ou au service de délinquants et d'organisations criminelles, mais comme une alternative au service de l'économie. C'est pourquoi la question : « *Pourquoi tant d'emballement ?* » reste entière et se pose même de façon plus aigüe après cet exposé qui s'accorde toutefois avec cette maxime ancienne[13] mais clairvoyante : «*Ne mettez pas votre confiance dans l'argent, mais mettez votre argent en confiance*».

Daniel GUINIER
Docteur ès Sciences
Certifications CISSP, ISSMP, ISSAP en sécurité des SI et MBCI en gestion des crises
Expert en cybercriminalité et crimes financiers près la Cour Pénale Internationale de La Haye

Notes

(1) The Hidden Wiki Uncensored - Hard_candy - The child pornography network Copywrong (C)

(2) Le 04/01/15, Bitstamp, une des trois principales plateformes d'échanges a dû interrompre ses services pendant 48 heures après avoir été victime d'un piratage qui a conduit au vol de 19 000 Bitcoins, soit 5,2 millions de Dollars correspondant à 10% de ses réserves, entraînant une chute de 12% du cours du Bitcoin.

(3) Par exemple, selon la norme ISO 15408, fondée sur le schéma des critères communs de la sécurité des technologies de l'information, en termes de fonctionnalités et d'assurance, concernant la faiblesse de la sécurité des échanges.

(4) Ex. En mars 2012, une vulnérabilité a d'abord permis la compromission des comptes administrateur de Linode, un fournisseur de services cloud, permettant ensuite l'accès aux portefeuilles stockés sur ses serveurs. Les pirates auraient ainsi pu dérober environ 47 000 Bitcoins. Le montant maximum par vol de 2011 à 2012 a été de 78 739 Bitcoins, soit l'équivalent de plus d'un million de Dollars, pour MyBitcoin. D'autres événements concernaient MyBitcoin, Bitcoinica, Allinvin, Bitfloor, Tony Silk Road, Bitomat.pl, Bitcoin7, BTC-E, etc., selon Amoros R. (2013).

(5) Selon la devise : « Voler les riches et donner aux pauvres en vidant leur portefeuille par un serveur ftp public», suivi de : «... Envoyez-moi l'argent s'il vous rend riche».

(6) DevilRobber OS X/Miner-D utilisait l'unité GPU des microordinateurs Macs compromis pour procéder au «mining» en transférant les Bitcoins extraits et en cas de découverte de portefeuilles l'ensemble des données les concernant à un serveur C&C du «botnet».

(7) Les données subsidiaires sont la représentation de la taille en octets de la transaction (ex. 04), laquelle peut être changée sans altérer l'intégrité des données (ex. 004), mais en produisant un autre résultat de hachage aboutissant à un identifiant différent de celui d'origine.

(8) Mt. GOX a vécu une attaque liée à cette vulnérabilité de «malléabilité de transaction», avec une disparition définitive de 650 000 Bitcoins, soit 355 millions de Dollars.

(9) Le site dont le nom évoque clairement «Wikileaks» est totalement illégal apparemment orchestré par les membres d'un système collectif crypto-anarchiste, dans le but d'aider à «stopper la corruption et à défier le pouvoir».

(10) Disponible en open source sur Internet sur le site de partage de code Github.

(11) Si le chiffrement réalisé à l'aide d'un fichier keyfile et d'un mot de passe fort de bonne qualité, il est peu probable qu'un dossier chiffré puisse être déchiffré par une méthode en force brute.

(12) Le dispositif stocke les clés dans une zone protégée d'un microcontrôleur. Ainsi, elles ne peuvent pas être transférées hors du dispositif et ne sont pas sensibles aux codes malveillants.

(12) O.W. Holmes (1809-1881), L'autocrate à la table d'hôte.

Bibliographie

Allais M. (1999) : La crise mondiale d'aujourd'hui. Pour de profondes réformes des institutions financières et monétaires, Ed. Clément Juglar.

Amoros R. (2013) : Digital virtual currency and Bitcoins : The dark web financial markets - Exchanges & secrets. CreateSpace Independent Publishing Platform, 308 p.

Andresen G. (2012) : BIP16 : Pay to script hash, Bitcoin improvement proposal.

https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki.

Back A., et al. (2014) : Enabling blockchain innovations with pegged sidechains, 22 oct.

BdF (1999) : Bulletin de la Banque de France, n° 70, oct.

BdF (2013) : Focus de la Banque de France, n° 10, 5 déc.

de Boissieu C., Lorenzi J.-H. (2008) : Un nouveau Bretton Woods, Le Monde, 7 octobre.

Bronk C., Monk C., Villasenor J. (2011) : Shadowy figures: Tracking illicit financial transactions in the murky world of digital currencies, peer-to-peer networks, and mobile device payments. The Brookings Institution

Carbonnier J (1988) : Conclusion générale du colloque «Droit et monnaie», in Droit et Monnaie, Ed. Litec

CE (2012) : Criminal money flows on the Internet : methods, trends and multi-stakeholder counteraction, Typology research, MONEYVAL 38th Plenary meeting, 5-9 mars, www.coe.int/moneyval

Chavagneux C. (2004) : Ce qui s'est vraiment passé à Bretton Woods, Alternatives économiques, no 227, juil.

Cusumano M. A. (2014) : Technology strategy and management — The Bitcoin ecosystem. Communications ACM, Oct., Vol.57, n° 10, pp. 22-24

Danchev D. (2013) : Cybercriminals sell access to tens of thousands of malware-infected russian hosts. Webroot Threat Blog, 23 Sept.

ECB (2012) : Virtual currency schemes. European Central Bank, Eurosystem, oct., Case study - Bitcoin, pp. 21-33

Even M., Gery A., Louis-Sidney B. (2014) : Monnaies virtuelles et cybercriminalité – Etat des lieux et perspectives, Les notes stratégiques, CEIS

Galston E. (2014) : The Bitcoin paradox that undid Mt. Gox. The Wall Street Journal , 27 février.

Guinier D. (2000a) : Exigences d'une signature digne de confiance et d'un droit adaptés aux documents et transactions électroniques. Revue A. Bensoussan — Droit des technologies avancées, HERMES Sciences, vol. 7, n° 3, pp.218-232

Guinier D. (2000b) : Cryptographie : Des algorithmes et des clés de taille raisonnable, mais encore... Revue A. Bensoussan — Droit des technologies avancées, HERMES Sciences, vol. 7, n° 5, pp.399-409

Guinier D. (2006) : Incertitude technologique sur la preuve électronique liée à certaines fonctions cryptographiques.

Expertises, n° 301, Mars, pp. 96-100

Guinier D. (2014) : «Hackers» en devenir et en repentir — Quand les talents s'orientent différemment... et sont recrutés La Revue du GRASCO, Doctrine Sciences criminelles, n° 8, février, pp. 36-48

Lamport L (1979) : Constructing digital signatures from a one-way function, Tech. Report SRI-CSL-98, SRI

International Computer Science Laboratory

Libchaber R. (1998) : Recherche sur la monnaie en droit privé. Bibliothèque de droit privé, T. 225, LGDJ

Liu A. (2013) : Beyond Bitcoin : A Guide to the most promising crypto-currencies

Moulin A.-M. (1992) : Le droit monétaire français et les paiements en écus. Bull. trim.de la Banque de France, déc.

Nakamoto S. (2008) : Bitcoin : A peer-to-peer electronic cash system. Cryptography Mailing List, Nov.

Ossowski Y. (2013) : Alternative monétaire et législation de Bitcoin, L'AGEFI, Genève, 17 nov.

Percival C., Josefsson S. (2012) : The Scrypt password-based key derivation function , IETF, 24 sept.

Quéméner M. (2013) : Cybersociété — Entre espoirs et risques. Ed. L'Harmattan, 241 p.

Quéméner M. (2015) : La territorialité à l'épreuve de la cybercriminalité. Expertises, n° 398, Jan., pp. 17-18, 23-24

Rahn R. W. (1999) : The end of money and the struggle for financial privacy, Seattle, Discovery Inst. Press

Reid F., Harrigan M. (2012) : An Analysis of Anonymity in the Bitcoin System. Cornell University Lib., mai

Ron D., Shamir A. (2013a) : Quantitative analysis of the full Bitcoin transaction graph. Proc. 17th Intern. Conf. on

Financial Cryptography and Data Security, Okinawa

Ron D., Shamir A. (2013b) : How did Dread Pirate Roberts acquire and protect his Bitcoin wealth?

Servet J.M. (1988) : La monnaie contre l'État ou la fable du troc, in Droit et monnaie, Ed. Litec

SGDN (2007) : Algorithmes cryptographiques pour l'interopérabilité du format V1 de signature électronique XAdES de l'Administration, V 0.4, n° 193/SGDN/DCSSI/SDS, 31 jan.

Strohm C. (2014) : Cybercrime remains growth Industry with $445 billion lost. Bloomberg, 9 Juin

Wallace B. (2011) : The Rise and Fall of Bitcoin, Wired Mag., nov, www.wired.com/magazine/2011/11/mf_bitcoin/all/

Sitographie

http://coinatmradar.com/bitcoin_atm/169/bitcoin-atm-btc-o-matic-hilversum-antminer-distribution-eu/

http://csrc.nist. gov/publications/fips/fips186-3/fips_186-3.pdf

http://www.alloscomp.com/bitcoin/calculator

http://www.bitcoin.fr/post/Les-confessions-d-un-mineur-de-bitcoin#main

http://www.coindesk.com/7-charts-show-year-growth-bitcoin-atms/

http://resources.infosecinstitute.com/diving-in-the-deep-web/

https://blockchain.info/fr

https://en.bitcoin.it/wiki/Comparison_of_mining_pools

https://en.bitcoin.it/wiki/Protocol_specification

https://en.bitcoin.it/wiki/Research

https://en.bitcoin.it/wiki/Securing_your_wallet