Une analyse sociotechnique d'un type d'usage du bitcoin : le crypto-marché SilkRoad

Alan Ouakrat

Ouakrat Alan (2015), « Une analyse sociotechnique d'un type d'usage du *bitcoin* : le crypto-marché *SilkRoad* », *Revue Banque & Droit*, n°159, janvier-février, pp.14-17.

Résumé : Ce papier s'intéresse à l'économie souterraine du Bitcoin, et non au commerce légal de biens et services qui y sont liés[1]. Les usages illicites participent à alimenter l'intérêt pour la monnaie virtuelle qu'est le Bitcoin. Nous proposons une analyse socio-économique du fonctionnement de la place de marché SilkRoad (SR). Lancée en février 2011, la plateforme opère sur le web invisible (*deep web, darknet*), accessible uniquement depuis le navigateur anonyme Tor. L'activité de SR est illégale puisque spécialisée dans la vente de substances contrôlées (drogues essentiellement). Le site est saisi par le FBI le 2 octobre 2013, mais une nouvelle version apparaît en ligne quatre semaines plus tard, le 6 novembre 2013. Ce phénomène peut surprendre en raison de ce que cette plateforme rend possible : le commerce de substances illicites sur Internet de façon relativement anonyme. Le site a ainsi joué un rôle pionnier dans la popularisation d'usages sociotechniques jusqu'ici relativement marginaux et confidentiels, en mettant à la portée du grand public – notamment par la couverture médiatique dont a bénéficié le site et le procès de son fondateur Ross Ulbricht – les connaissances nécessaires à un anonymat relatif en ligne dans un univers numérique caractérisé au contraire par sa traçabilité.

Mots-clés : bitcoin, économie souterraine, marché noir, crypto-anarchisme, Silk Road.

Le Bitcoin est aussi un moyen de paiement utilisé pour le commerce de produits et services illégaux. Ses avantages sont en certains points similaires à ceux de l'argent en espèces : l'anonymat[2] et l'irréversibilité des transactions. Les marchés noirs en ligne participent à l'engouement autour du Bitcoin. Les barrières à l'entrée de ces marchés se sont abaissées pour les acheteurs avec les plateformes d'échanges légales de Bitcoin (ex. bitcoin.de, mais aussi les marchés entre particuliers[3]). Il n'est ainsi plus nécessaire de « miner » les bitcoins[4]. La communauté Bitcoin aide à valider les transactions, assure qu'elles sont conformes. Le rapport du Sénat (2014, p.10) considère le Bitcoin comme « une aubaine pour la cybercriminalité et le blanchiment » du fait de l'anonymat attaché à ses transactions. Des chercheurs décrivent les marchés noirs, et en particulier SR, comme une « innovation criminelle radicale » (Aldrige and Decary-Hetu, 2014). Après deux ans et demi d'activité, SR est saisi par le FBI le 2 octobre 2013 et son fondateur Ross Ulbricht est inculpé. Une version en reprenant la charte graphique, SR2, est mise en ligne quatre semaines plus tard, le 6

[1] La présente version est révisée et enrichie par rapport à l'article original publié dans le numéro 159 de la revue *Banque & Droit*. Cette publication fait suite à une communication réalisée dans le cadre de la matinée d'études organisée par l'Association des Doctorants et des Docteurs d'Assas (ADDA) « Le Bitcoin, une monnaie ? », qui s'est tenue le vendredi 27 juin 2014 en Salle des Conseils de l'Université Panthéon-Assas, Paris 2, sous la présidence du Professeur Thierry Bonneau. Précisons que cet article ne s'appuie pas sur une enquête scientifique, mais propose simplement des pistes d'analyse socioéconomique d'un phénomène dont il tente d'identifier les dimensions structurantes en termes de confiance et d'organisation économique des échanges, à partir d'un corpus composé par la collecte de ressources en ligne (essentiellement, articles de presse en ligne et posts de forums, mais également d'observations réalisés sur la plateforme SR).

[2] Notons que ce point fait débat dans la mesure où il serait possible pour les services de renseignements de « dés-anonymiser » certaines transactions, jusqu'à remonter à l'individu qui en est l'auteur ou le bénéficiaire, en s'appuyant sur une analyse de la *blockchain*. L'anonymat du Bitcoin doit donc être considéré comme relatif.

[3] Du type localbitcoins.com. L'autorité de supervision financière allemande, la BaFin, qualifie les monnaies virtuelles « d'unités de compte », de fait ces dernières entrent dans la catégorie des instruments financiers, au même titre que les devises. L'Allemagne a donc choisi un point de vue pragmatique vis-à-vis du Bitcoin : réguler pour contrôler et taxer.

[4] On peut lire dans le rapport du Sénat au sujet du Bitcoin, p.8-9 : « *Ingénieux mécanisme de « création monétaire » qui rémunère les utilisateurs du système : les transactions sont validées par les ordinateurs connectés au réseau ; en échange de la mise à disposition de leur puissance de calcul, les « mineurs » se voient rétribués en bitcoins générés automatiquement par l'algorithme du système. On estime à environ 100 000 le nombre de processeurs participant aux opérations, parfois regroupés en véritable « fermes de minage », consommant d'importantes ressources mais pouvant engendrer d'importants profits*. »

novembre 2013[5]. La relative réussite de la place de marché SR, une expérience de crypto-marché fondée sur le principe de la « contre-économie » libertarienne, interroge le socio-économiste. Dans quelle mesure la confiance, nécessaire aux transactions, peut-elle s'établir sur un marché anonyme et sous quelles formes se matérialise-t-elle ?

1. De SR1 à SR2, un crypto-marché peut en cacher un autre

SR1 aurait représenté, selon la fourchette haute des estimations de certains, près de 10 % des transactions liées au Bitcoin[6] (Christin, 2013). Sur la plateforme, un système de couverture du risque (*hedging*) existe. Il prémunit acheteurs et vendeurs contre la volatilité du cours du Bitcoin à court terme. Les prix de vente restent relativement stables (plus ou moins 10%), malgré les fortes fluctuations du cours du Bitcoin. La plateforme assure ainsi un rôle de tiers de confiance. Le chiffre d'affaires de SR1 a été estimé à 1,2 milliards de dollars pour deux ans et demi d'activités. Les revenus collectés par la plateforme furent évalués à 80 millions de dollars, perçus en commissions d'intermédiations (10%) prélevées sur les revenus des vendeurs. Le nombre d'utilisateurs actifs était, au moment où la plateforme a été saisie par le FBI, de 150 000, dont 146946 acheteurs contre 3877 vendeurs (2,5%). 144 000 BTC, l'équivalent de 28,5 millions de dollars ont alors été saisis. D'après les documents du FBI, sur une période de près de six mois (du 6 février au 23 juillet 2013), plus de 1,2 millions de transactions ont été enregistrées. Selon les données renseignées par les utilisateurs, 30 % venaient des Etats-Unis, 27 % n'avaient rien déclaré, puis par ordre de grandeur l'Angleterre, l'Australie, l'Allemagne, le Canada, la Suède, la France, la Russie, l'Italie et les Pays-Bas. D'après Christin (2013) qui s'est appuyé sur une aspiration quotidienne de SR1 pendant six mois au cours de l'année 2012, 24 400 produits différents étaient vendus sur le site, bien que la plupart ne soient plus disponibles après trois semaines. La plupart des vendeurs disparaissent dans les trois mois, alors que seuls 112 vendeurs ont été présents tout au long de la période observée. L'apparition de SR2 fut une sorte de pied de nez à la justice américaine. La tonalité donnée à ce projet par ses protagonistes fut celle d'une lutte pour l'existence d'une « contre-économie » chère aux libertariens (Konkin, 1980), dont SR était l'incarnation. SR2 disait vouloir se montrer à la hauteur de la confiance que lui accordaient ses utilisateurs. En remboursant les utilisateurs suite à une attaque informatique, les administrateurs de la plateforme ont montré leur détermination à traduire leur parole en actes : la plateforme offrant ainsi un gage de la crédibilité de son discours[7]. Le site dû arbitrer entre les exigences des utilisateurs et les impératifs de sécurité afin de maintenir un rapport de force équilibré entre offre et demande. La tension autour du système *Escrow* est emblématique de ce difficile équilibre. Autrefois, en faveur des acheteurs, la fonctionnalité intégrée au système de paiement sur la plateforme leur permettait de relâcher le paiement au vendeur une fois le produit reçu et confirmé conforme. Supprimée par la suite pour des raisons de sécurité liées à l'attaque informatique de février 2014, son retour a fait débat au sein de la communauté sur les forums du site SR2.

---

[5] *lemonde.fr*, « Le site illégal Silk Road recréé un mois après sa fermeture par le FBI », article publié le 07 novembre 2013 : http://www.lemonde.fr/technologies/article/2013/11/07/le-site-illegal-silk-road-recree-un-mois-apres-sa-fermeture-par-le-fbi_3510291_651865.html. Le site a été à nouveau saisi un an jour pour jour après sa mise en ligne, le 6 novembre 2014. Cf. *Business Insider UK*, "FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0", article publié le 6 novembre 2014 par James Cook : http://uk.businessinsider.com/fbi-silk-road-seized-arrests-2014-11?r=US, voir également l'article d'*Ars Technica*, "Silk Road 2.0, infiltrated from the start, sold $8M per month in drugs" : http://arstechnica.com/tech-policy/2014/11/silk-road-2-0-infiltrated-from-the-start-sold-8m-per-month-in-drugs/

[6] Il n'existe, à notre connaissance, aucune quantification fiable de la part des transactions de SR dans l'économie totale du Bitcoin. Selon Christin (2013, p.8), les transactions liées à SR pourraient, de façon plausible, correspondre à entre 4,5% et 9% de l'ensemble des transactions.

[7] Après une attaque informatique en février 2014 d'une valeur de 2,7 millions de dollars, SR2 a remboursé la quasi-intégralité des utilisateurs lésés. Voir l'article d'Ars Technica précédemment cité, note de bas de page 5.

Schéma 1. Le fonctionnement du système Escrow[8]

D'un côté, les vendeurs étaient favorables à la disparition du système Escrow car être payé avant la confirmation de la réception des marchandises ou services par les acheteurs les assure contre la dévaluation du cours du Bitcoin, un délai de paiement jugé trop long ou le risque de mauvaise foi des acheteurs (qui pouvaient prétendre n'avoir rien reçu et exiger un remboursement partiel ou une nouvelle livraison). D'un autre côté, avec la disparition du système Escrow, les acheteurs sur SR2 se sentaient démunis face aux vendeurs en cas de non-livraison ou de tromperie sur la marchandise[9].

En raison de la méfiance qui préside à l'engagement de transactions sur un marché noir, des gages de crédibilité, notamment dans les développements de la sécurité de la plateforme doivent être régulièrement apportés. Dans le cas contraire, la confiance des utilisateurs s'étiole et ils peuvent être tentés de migrer vers d'autres plateformes. Exerçant une activité criminelle relative au commerce de produits stupéfiants, la plateforme est constamment menacée par plusieurs adversaires : l'Etat, les individus et groupes criminels rivaux, qui peuvent l'attaquer à tout moment. Il s'agit donc d'une course-contre-la-montre pour adapter l'interface et les fonctionnalités aux besoins des acheteurs et des vendeurs, ainsi qu'arbitrer sur la priorité de ces développements, sachant que le site peut être saisi à tout moment. SR est passé d'une situation quasi-monopolistique à un marché fragmenté. Plus le marché est fragmenté, plus les risques de conduites opportunistes des vendeurs comme des acheteurs sont grands, en particulier pour les acheteurs ponctuels non connus des vendeurs. Les utilisateurs agissent en fonction du niveau de risque perçu à échanger sur une plateforme et se protège de façon similaire.

[8] Cette illustration est issue du site https://www.escrowindia.com/

[9] Les acheteurs conservent toutefois la possibilité de laisser une évaluation (note+avis) sur la transaction, ce qui est un moyen de contrôle de la stabilité de la qualité du service assuré par les vendeurs et leur donne le pouvoir de signaler publiquement une transaction qui n'aurait pas aboutie ou ne se serait pas déroulée dans de bonnes conditions. D'autres sites de marché noirs ont intégré par défaut cette fonction Escrow afin de se différencier.

2. SR, un marché illégal fondé sur la confiance interpersonnelle

Le partage d'expériences entre utilisateurs par le biais du forum et le système de notes et avis sur les transactions sert à créer de la confiance. L'information ainsi produite permet aux acheteurs de réaliser des choix informés. Les forums permettent la ré-assurance des nouveaux utilisateurs, cantonnés au rôle de lecteurs jusqu'à ce qu'ils atteignent un certain nombre de posts[10]. Les liens entre les membres de la communauté se bâtissent au fil des échanges interpersonnels (transactions ou messages privés[11]) et semi-publics (forums). C'est avant tout le système de notes et avis sur les transactions qui concoure à établir et maintenir (ou non) la réputation d'un vendeur. Un autre élément à prendre en compte en analysant ce qu'est ce marché anonyme est le forum où les utilisateurs échangent par le biais de pseudonymes, attachés à une réputation et à un profil sur le site. L'information autour des produits (notes, avis de consommateurs, échanges d'opinions, d'informations en tout genre ou concernant la sécurité de la plateforme par exemple) contribue à créer la confiance entre les utilisateurs, nécessaire aux transactions effectuées sur la plateforme (Gensollen, 1999). Sur un marché illégal, l'appariement entre l'offre et la demande repose sur un niveau de risque plus élevé. Un minimum de confiance est nécessaire à la réalisation de ces transactions, qui n'impliquent pas la rencontre physique. La confiance entre les parties est établie par un système de notes et d'avis qui peuvent faire l'objet de manipulations (comme dans l'internet « en clair », Beauvisage *et al.*, 2014). S'agissant d'une économie informelle reposant sur l'échange de substances contrôlées, l'identité réelle des partenaires est inconnue[12]. Les vendeurs ont une réputation à construire ou à défendre. La plateforme doit réduire le risque de « passager clandestin » en appariant offre et demande grâce à un système de réputation (notes et avis sur les transactions, ainsi que commentaires sur les forums), tout en assurant la confidentialité des transactions, la protection des fonds et de l'identité des acheteurs et des vendeurs. La confiance des utilisateurs est ainsi l'actif essentiel de ces plateformes. Cette dernière est objectivée par l'historique des évaluations sur les transactions pour une annonce (un produit proposé par un vendeur) ou de façon agrégée sur l'ensemble des produits proposés par un vendeur. Le nombre et la qualité continue des évaluations (note + avis) témoignent de la fiabilité d'un vendeur. Ainsi équipés, les acheteurs peuvent réaliser des choix informés et se prémunir, dans une certaine mesure, contre le risque d'aléa moral.

3. Crypto-anarchisme

SR s'appuie explicitement sur une utopie libérale-libertaire portée par ses fondateurs qui associent un geste politique libertarien au commerce de produits et services illicites en ligne. Pour la plateforme, il s'agit de protéger la communauté des poursuites judiciaires, des cyber-attaques, des utilisateurs-fraudeurs et des autres menaces. Cependant, la sécurité des utilisateurs ne peut leur être garantie que par le cryptage de leur communication, des mesures individuelles qu'ils ne peuvent prendre qu'eux-mêmes pour protéger leur identité réelle. Certes, sur les forums de SR, on peut lire de multiples recommandations et avertissements de sécurité visant à inciter les utilisateurs à pratiquer le chiffrement asymétrique des messages échangés lors des transactions, mais est-ce

[10] Un seuil de 50 posts a été défini pour pouvoir poster dans tous les sujets. Avant cela, les nouveaux utilisateurs ont seulement la possibilité de poster dans un sujet dédié. Ils se livrent alors à des pratiques de « *flood* », visant à poster le plus rapidement possible ces 50 messages, qui sont, généralement, des suites de caractères sans signification.

[11] Sur la période du 24 mai au 23 juillet (deux mois), plus de 1,2 millions de messages ont été envoyés par le système de messagerie privé de SR (Christin, 2013).

[12] C'est par le biais de pseudonymes que les vendeurs et les acheteurs échangent sur la plateforme. Les pseudos des acheteurs sont même parfois partiellement masqués afin de rassurer ces derniers sur l'anonymat de leurs commentaires liés aux transactions. L'identité réelle des acheteurs peut être révélée aux vendeurs lorsqu'ils fournissent leur adresse de livraison qui peut-être (ou non) liée à une identité réelle. Les vendeurs s'engagent à détruire ces informations sitôt l'envoi effectué. De plus, ces informations peuvent transiter de façon cryptée (PGP) pour que seuls les vendeurs aient accès à cette information.

suffisant ? La majeure partie des acheteurs semblent ne pas être inquiété par le risque collectif qu'ils font subir à la plateforme et aux vendeurs en ne cryptant pas leurs communications par l'usage du chiffrement asymétrique[13]. Les petites transactions concourent à faire penser à l'individu qu'il prend des risques limités et ne l'incite par conséquent pas à supporter les coûts d'apprentissage nécessaires à la montée en compétences en cryptographie destinée à l'usage du logiciel de communication cryptée PGP. Moins les individus utilisent PGP, plus la surveillance de la plateforme aura un intérêt pour les autorités qui capteront ainsi les informations échangées « en clair » diffusées par les utilisateurs. Les coordonnées envoyées par les acheteurs sont des informations particulièrement sensibles, dans la mesure où elles fournissent aux autorités une raison supplémentaire pour saisir les serveurs contenant nom et adresse postale d'un grand nombre de petits acheteurs. Pour la plupart, ces derniers estiment qu'ils n'ont pas besoin de se protéger étant donné les petites transactions effectuées. Toutefois, là réside un point de tension entre les utilisateurs de la communauté et les développements de la plateforme. Pour que le cryptage des messages soit efficient, il ne peut être intégré d'emblée par la plateforme à partir d'une clé unique de chiffrement. Les utilisateurs sont donc contraints de prendre eux même en main leur propre sécurité, en adéquation avec la philosophie libertarienne, bien qu'ils fassent souvent preuve de négligence en ce domaine faute de temps ou de conviction de l'utilité de ces mesures de protection individuelle et collective.

Conclusion

Au terme de cet éclairage, deux points retiennent notre attention : premièrement, la capacité à créer de la confiance sur un marché anonyme grâce à un système de notes et avis (comme dans le web « en clair ») mais également la fragilité d'un tel système en cas de disparition de la plateforme (les risques d'usurpation de l'identité d'un vendeur par un autre vendeur ou les autorités de ne sont pas nuls) ; deuxièmement, la revendication d'une utopie politique comme ciment de la confiance de la communauté d'utilisateurs par le site SR (incarnée notamment par le remboursement des fonds détournés lors de l'attaque informatique de février 2014). Ainsi, au-delà des échanges de marchandises et de services, nous avons pointé la dimension sociale des échanges commerciaux qui s'effectuent sur la plateforme.

Laboratoire d'expérimentation d'une économie informelle en ligne, SR a montré qu'une combinaison de techniques de cryptographie (Tor pour la navigation, PGP pour les messages et Bitcoin pour le moyen de paiement) permettait un relatif anonymat et rendait les échanges possibles, même en dehors d'un cadre légal, et ce, à un niveau international. Alors même que le web « en clair » faisait l'objet de scandales concernant la surveillance généralisée des usages du grand public suites aux révélations d'Edward Snowden, révélant la circulation des données des utilisateurs et leur vulnérabilité à la surveillance commerciale et étatique, la petite communauté d'utilisateurs de SR a fait la démonstration d'une capacité d'échange de ressources informationnelles et de substances contrôlées de façon relativement autonome par rapport à cette surveillance. La couverture médiatique de l'arrestation de Ross Ulbricht a contribué à populariser cette place de marché, mais aussi plus largement, les technologies utilisées pour anonymiser la navigation sur l'Internet. Cette préoccupation dépassant désormais le simple cadre des dissidents politiques et des journalistes pour devenir, dans une certaine mesure, plus générale. Cependant, la capacité à se protéger des utilisateurs du web invisible demeure liée à la plus ou moins grande facilité d'accès à ces technologies et aux compétences requises pour les utiliser, qui sont elles-mêmes inégalement distribuées dans la population. La couverture médiatique de l'affaire SR a donc concouru à une forme d'éducation à la traçabilité et à la sécurité informatique en ligne concernant le cryptage informatique. L'élargissement du public de la plateforme dû à l'attention médiatique qu'elle a suscité se révèle finalement contre-productif pour faire cesser ses activités criminelles, de

[13] Le logiciel le plus répandu pour pratiquer le chiffrement asymétrique est *Pretty-Good-Privacy* (PGP), GPG dans sa version libre.

la même manière que l'arsenal juridique déployé contre le piratage de musique en ligne n'a pas contribué à faire disparaître ces pratiques dans la population.

Le marché comporte aujourd'hui plusieurs acteurs en situation de concurrence, les utilisateurs voguant au gré des opportunités de migration et des garanties de sécurité offertes par ces plateformes. Mais nulle part ailleurs que sur SR, le discours idéologique en faveur du libertarisme n'a été aussi fort, ainsi que les appels à la communauté à soutenir « le combat », « les efforts entrepris », « la lutte ». La mesure dans laquelle les utilisateurs adhérent à cette idéologie libertarienne, qui rejoint leurs intérêts personnels, reste cependant à évaluer.

Références

Aldrige J. and D. Decary-Hetu (2014), "Not an 'eBay for Drugs': The Cryptomarket 'Silk Road' As a Paradigm Shifting Criminal Innovation", Working-paper, 29 p.
http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2436643

Beauvisage T., J.S. Beuscart, V. Cardon, K. Mellet et M. Trespeuch (2013), « Notes et avis de consommateurs sur le web. Les marchés à l'épreuve de l'évaluation profane », *Réseaux*, Vol.1, N°177, pp.131-161.

Biryukov A., I. Pustogarov, R.-P. Weinmann (2013), "Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization", *IEEE Symposium on Security and Privacy,* pp.80-94
http://cryptome.org/2013/08/trawling-tor-hidden.pdf

Christin N. (2013), « Traveling the Silk Road : A Measurement Analysis of a Large Anonymous Online Marketplace », *International World Wide Web Conference Committee (IW3C2), WWW2013*, May 13-17, Rio de Janeiro, Brazil.
https://www.andrew.cmu.edu/user/nicolasc/publications/Christin-WWW13.pdf

Gensollen Michel (1999), « La création de valeur sur Internet », *Réseaux*, 17 (97), 15-76.
http://www.persee.fr/web/revues/home/prescript/article/reso_0751-7971_1999_num_17_97_2167

Turner F. (2012), *Aux sources de l'utopie numérique. De la contre-culture à la cyberculture : Steward Brand, un homme d'influence*, C&F Editions, 427 pages.

Konkin III S.E. (1980), *New Liberarian Manifesto*,
http://www.agorism.info/docs/NewLibertarianManifesto.pdf

Liens

Le Monde.fr, « Le site illégal Silk Road recréé un mois après sa fermeture par le FBI », le 7 novembre 2013 : http://www.lemonde.fr/technologies/article/2013/11/07/le-site-illegal-silk-road-recree-un-mois-apres-sa-fermeture-par-le-fbi_3510291_651865.html

Ross Ulbricht Criminal Complaint :
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0CDIQFjAC&url=https%3A%2F%2Fwww.cs.columbia.edu%2F~smb%2FUlbrichtCriminalComplaint.pdf&ei=xoasU9vTMtDP0AWt-4HIBA&usg=AFQjCNGorVwfS0rJWcr1oZKNaf5ieRqqwQ

Rapport N°767 rectifié, enregistré à la présidence du Sénat le 23 juillet 2014, 143p., MM. Philippe MARINI et François MARC : http://www.senat.fr/rap/r13-767/r13-7671.pdf