Le crime international organisé et les cryptomonnaies

Jacques Fontanel

Le crime international organisé et les crypto monnaies

Jacques Fontanel

Conférences
Géopolitiques de Brest
4 Mars 2022

Document disponible

Le développement de l'économie digitale permet de nombreuses actions malveillantes sont nombreuses comme le sabotage des programmes, l'espionnage, le phisting (hameçonnage), le vol de données, l'usurpation d'identité, la perte de confiance dans un service public ou privé et les fameux rançongiciels. Les cryptomonnaies sont les bienvenues pour opérer dans ce milieu crimine. Ils sont aussi bien accueillis par les délinquants financiers chercheurs d'évasion fiscale. Les fournisseurs de services sur le Dark Net mettent à disposition des groupes criminels les infrastructures nécessaires. Les actions de rançongiciels coûtent très cher à la société et les Etats commencent à intervenir afin de limiter les effets néfastes sur la confiance des agents économiques et financiers d'opérations légales. Le gouvernement chinois a interdit l'utilisation du bitcoin et la question est posée pour l'Union européenne.

The development of the digital economy allows many malicious actions such as sabotage of programs, espionage, phishing, data theft, identity theft, loss of trust in a public or private service and the famous ransomware. Cryptocurrencies are welcome to operate in this criminal environment. They are also welcomed by financial criminals looking for tax evasion. Service providers on the Dark Net provide criminal groups with the necessary infrastructure. Ransomware actions are very costly to society and governments are starting to intervene in order to limit the negative effects on the confidence of economic and financial agents of legal operations. The Chinese government has banned the use of bitcoin and the question is being asked in the European Union.

Bitcoin, crypto monnaie, économie digitale, crime organisé, évasion fiscale, rancongiciel

Bitcoin, crypto currency, digital economy, organized crime, tax evasion, ransomware

Le **crime organisé** est une structure humaine respectant les ordres d'un chef pour conduire des opérations illicites en vue de faire des profits. La question est alors de savoir si les règles sont justifiées (prohibition de l'alcool aux Etats-Unis ou celle de la drogue aujourd'hui). Plus un bien ou service est interdit, et plus il est rare, risqué et donc cher. Le domaine de l'économie digitale intéresse le crime organisé car des actions illégales mais économiquement très fructueuses peuvent être engagées.

Le développement de l'économie digitale, organisé autour des GAFAM (Fontanel, 2019), permet de nombreuses actions malveillantes comme le sabotage des programmes, l'espionnage, le phisting (hameçonnage), le vol de données, l'usurpation d'identité, la décrédibilisation d'un service et les fameux rançongiciels. Avec le processus de la mondialisation (Fontanel, 2005), elles deviennent de plus en plus coûteuses car ces opérations pénètrent, parfois de manière aléatoire, dans de nombreux systèmes digitaux connectés.

Le Distributed Denial of Service a pour objet de bloquer un compte internet en le saturant de connexions, grâce à la mise en place d'un botnet, un réseau de milliers d'ordinateurs infectés par un malware inconnu des utilisateurs, qui vient à la même seconde sur ce compte internet. Un service complet peut lui être proposé sur le Dark Net.

De nombreuses cyberattaques ont retenu l'attention des acteurs politiques et économiques.

- En 1999, un virus créé par un hacker a causé des dégâts de l'ordre de 400 millions de dollars à Microsoft.
- En 2010 Stunet le site d'enrichissement d'uranium de Natanz en Iran a été attaqué, sans doute par les services secrets israéliens.

- En 2013 le vol de 3 milliards de comptes sur Yahoo n'a été révélé 3 années plus tard,
- en 2017, WannaCry a concerné 300.000 ordinateurs sur une faille de sécurité de Windows, par un opérateur venu probablement de Chine.
- Toujours en 2017, le célèbre NotPetya s'est engouffré dans la faille dévoilée par Wannacry et il a paralysé de nombreuses entreprises dans le monde entier, notamment la SNCF, Saint-Gobain ou déjà la gare de Kiev. Cette attaque a sans doute coûté plus de 10 milliards de dollars à l'économie mondiale.

En 2018, le ministre britannique des Affaires étrangères, Jeremy Hunt, a accusé les services de renseignement militaire russes (GRU) d'avoir mené des cyberattaques, en toute impunité et en contradiction avec le droit international, contre des institutions politiques et sportives, des entreprises et des médias à travers le monde, notamment contre le Parti libéral en 2016, contre les infrastructures de la Georgie et de l'Ukraine et contre l'Agence mondiale de l'antidopage. Le Service de renseignement russe soutiendrait officieusement plusieurs groupes pirates dont les fameux Fancy Bear, Strontium ou Black Energy Actors.

C'est dans ce contexte que le bitcoin a rapidement intéressé tous les systèmes de profit. Les cryptomonnaies sont les bienvenues pour opérer dans ce milieu criminel mais aussi en faveur des délinquants financiers chercheurs d'évasion fiscale.

Il y a actuellement plus de 1.300 cryptomonnaies sur le marché. Le bitcoin est la toute première monnaie virtuelle, créée en 2009. Cette monnaie électronique repose sur un réseau informatique décentralisé dans lequel chaque utilisateur exerce à la fois le rôle de serveur et de client. Il s'agit donc d'un bien dématérialisé, résultat de codes informatiques et de clés de chiffrement. Les bitcoins sont créés par le minage, avec un plafond de 21 millions d'unités, dont 10% seulement restent à dégager. Toutes les transactions des utilisateurs du bitcoin sont répertoriées dans un grand registre informatique qu'on appelle la « blockchain », laquelle utilise des blocs de transaction chiffrés, infalsifiables et anonymes, ajoutés les uns aux autres. C'est pour cette raison que l'on parle de crypto monnaie. L'anonymat du

bitcoin est assuré par un code, qui ne requiert ni le nom, ni e-mail, ni l'adresse de son propriétaire.

Son prix de départ était de **0.001 dollar**, et l'année dernière il a atteint 66.000 dollars. Il se présente alors comme une valeur refuge, notamment dans toutes les périodes de crises économiques ou de conflits politico-militaires. Avec les événements d'Ukraine, il a repris au moins 25% de sa valeur en une semaine. Pourtant, le bitcoin n'est adossé à **aucune activité réelle**, il connaît une forte **volatilité**, il implique des délais de transactions importants et il n'a évidemment aucune garantie légale. Enfin, l'anonymat est relatif aujourd'hui, car s'il est difficile aux services de l'Etat de vérifier les déclarations ou plutôt les non-déclarations des ressources et des plus-values des bitcoins, ils peuvent le faire, même si le coût du contrôle très élevé s'avère décourageant. **Enfin, les** porteurs n'ont donc aucun recours en cas de vol. En 2014, La plate-forme japonaise d'échange de crypto monnaies a été piraté et a subi une perte de 850.000 bitcoins, propriété de 127.000 porteurs. Les usurpations d'identité par hameçonnage et des courriels commerciaux, visant directement les détenteurs de crypto monnaies sont de plus en plus fréquents, mais difficilement vérifiables..

Les ransomwares, ou rançongiciels restent cependant la plus grande menace informatique pesant sur les entreprises. C'est l'un des secteurs les plus lucratifs de la cybercriminalité. Pour rappel, les ransomwares sont des logiciels malveillants déployés sur des réseaux informatiques d'institutions et d'entreprises, en vue de paralyser parfois des centaines ou des milliers d'ordinateurs, et d'imposer le paiement d'une rançon à leurs victimes. Ils procèdent par le cryptage de tous les fichiers d'une entreprise, les rendant impossibles à déchiffrer par son utilisateur normal. Les hackers se manifestent ensuite en demandant une rançon en échange de la clé de déchiffrement.

Bien avant les cryptomonnaies, il y avait déjà des rançongiciels. Le virus Archiveus demandait à ses victimes, en guise de rançon, d'effectuer des achats sur des sites pharmaceutiques. Avec l'arrivée du bitcoin en 2009, les menaces qui pèsent sur les entreprises, les administrations et même les citoyens, sont à la fois plus fréquentes et

moins faciles à combattre. Le montant total des transactions suspectes liées aux rançongiciels s'élevait à 700 millions de dollars US par an. Selon un rapport du Département du Trésor des États-Unis, des transactions Bitcoin sortantes, d'une valeur de 5,2 milliards de dollars US, sont dues en grande partie aux paiements de rançongiciel, connues ou non. Le bitcoin est le moyen de paiement exigé à plus de 95% même si aujourd'hui noté le paiement de la rançon en Monero, une crypto-monnaie à l'anonymat améliorée, est demandée pour plus de sécurité dans les affaires importantes. Le coût de ces opérations se chiffrent en dizaines de milliards de dollars, protection informatique comprise.

Les fournisseurs de services sur le Dark Net mettent à disposition des groupes criminels des infrastructures, qui aident à l'exfiltration de données ou permettent la mise en place de clouds illicites où l'on peut placer des données volées. Ils développent une chaîne d'approvisionnement du rançongiciel, de la mise en place du hardware et de l'infrastructure à la conception et au développement des codes malveillants. Ils appliquant les techniques d'opacité des transactions et de blanchiments des fonds. Dans ce contexte, les cryptomonnaies constituent des services importants de rapidité, de sécurité et d'anonymat des transactions illicites.

En 2013, les officiers du service de police de Swansea sont informés que leur système informatique était touché par un virus, du nom de Cryptolocker et rendait dorénavant illisibles des documents d'enquête et documents administratifs. Une rançon de 2 bitcoins (750 dollars de l'époque) à verser rapidement, avec compte à rebours, était réclamée, ce qui fut fait. Les analystes de la police y ont vu un génie du mal utilisant un procédé criminel révolutionnaire et une rançon en bitcoins, un moyen de paiement encore mal connu. L'auteur, un russe dirigeant d'une organisation criminelle le Business Club, a continué plusieurs autres opérations, malgré une prime une prime de 3 millions $ proposée pour son arrestation. Mais les autorités russes n'ont pas réagi.

Au début de 2022, le groupe Lockbit 2.0 semble avoir piraté le Ministère de la Justice et déclare vouloir publier les documents à leur

disposition si la rançon n'était pas payée. Ce logiciel malveillant, déjà été utilisé aux Etats-Unis, en Inde, en Ukraine ou en Chine, bloque le système informatique des utilisateurs. La question est alors de savoir quelles sont les informations susceptibles d'être divulguées. Le secret de l'instruction suppose un paiement rapide.

Les collectivités et services publics locaux sont eux-mêmes fortement attaquées dans le monde entier. Les systèmes informatiques de la Mairie de Saint-Cloud ont été paralysées tout comme l'hôpital de Dax.

L'intérêt fondamental du bitcoin, au-delà de sa valeur spéculative, porte sur une méthode de paiement a priori intraçable. Cependant, le bitcoin n'est pas un vrai instrument de compte ou d'échange caractéristiques d'une monnaie. D'abord parce que sa valeur fluctue d'heure en heure et d'autre part parce que le bitcoin s'invite peu dans les affaires commerciales. Egon Musk a bien émis l'idée que ses Tesla pourraient être achetées en bitcoins, mais il a vite renoncé du fait du facteur spéculatif dans lequel il entraînait la vente des Tesla et de l'empreinte numérique colossale du bitcoin.

Lorsque les bitcoins ont été recueillis par les criminels, il s'agit pour eux soit de les remplacer sur le marché en dollars, soit de les conserver comme épargne spéculative. Il est alors possible d'échanger les bitcoins en d'autres crypto monnaies (saut de chaîne), de délocaliser les adresses, d'utiliser des plates-formes pour cacher ou obscurcir l'origine ou le propriétaire du bitcoin. Des « mixers », des outils servant à brouiller les transactions en cryptomonnaies pour compliquer le travail des enquêteurs judiciaires sont alors organisés. La rançon est immédiatement répartie dans d'autres portefeuilles et mélangées à d'autres bitcoins. Dans ce cas, la traçabilité est très complexe à réaliser.

La cryptodevise existe en quantité limitée, l'achat de bitcoin en fait augmenter la valeur. Plus les investisseurs sont paniqués, plus ils achètent des crypto devises dont la valeur augmente. Les criminels sont obligés de les conserver et le bitcoin joue alors un rôle comparable à celui de l'or placé dans des coffres-forts dans les paradis

fiscaux, notamment en Suisse (Fontanel, 2016). Dans ce cas, une thésaurisation s'installe à terme qui ne s'investit plus dans l'économie réelle.

Réglementation

Les paiements en bitcoins ou autres crypto monnaies sont peu réglementés, anonymes, et décentralisés. C'est pourquoi il est ensuite difficile à la Justice de déterminer les coupables des rançongiciels. Il faut alors chercher à améliorer la sécurité des systèmes informatiques des unités productives et des services publics afin de combattre les cyberattaques des crypto monnaies.

Les autorités publiques cherchent à identifier des points faibles dans ces nœuds de réseau et de perturber les chaînes d'approvisionnement. Aujourd'hui encore, il est rare que les rançons versées par des entreprises soient récupérées. Certaines entreprises préfèrent payer sans porter officiellement plainte, car elles ne veulent pas inquiéter leurs fournisseurs, clients ou actionnaires.

Quelques résultats commencent à apparaître :
- Dans le rançongiciel de Colonial Pipeline, 45 % des carburants consommés sur la côte Est, le bitcoin a été au cœur de la proposition des criminels. La police américaine a accusé le réseau DarkSide en lien avec la Russie, d'être à l'origine de l'attaque. Colonial Pipeline a été contraint de suspendre toutes ses opérations. En mai 2021, la Justice américaine a pu récupérer 64 bitcoins sur les 75 payés par Colonial au groupe de hackers DarkSide. La question maintenant est de savoir comment le FBI a-t-il pu obtenir des informations ? Le FBI explique avoir suivi à la trace toutes les transactions bitcoins, qui ont été transférés à de multiples reprises. Il « possédait » la clé privée du portefeuille en bout de chaîne. A l'époque, le versement de 75 bitcoins étaient estimés à 4,4 millions de dollars. Entre-temps, le cours de la monnaie virtuelle a chuté, 2,3 millions de dollars ont été effectivement récoltés.

- En 2018, deux Iraniens ont été accusés d'avoir causé 30 millions de dollars de pertes pour un butin personnel de 6 millions de dollars en concevant et en propageant le rançongiciel SamSam. Ces cybercriminels sont encore recherchés par le FBI.

- Début 2021, le réseau Netwalker utilisant un rançongiciel du même nom a paralysé le réseau informatique de nombreuses entreprises et d'administrations, en chiffrant toutes les données présentées sur les ordinateurs ciblés. Le coupable a été arrêté, il n'avait pas développé lui-même le logiciel qu'il s'était procuré sur le Dark Net. Près de 720 bitcoins ont été saisis, 1 200 bitcoins avaient transité sur son porte-monnaie numérique.

- Décembre 2021, un jeune homme, vivant chez ses parents, a été interpellé à Sault dans le Vaucluse, avec des comptes en banque d'une dizaine de monnaies virtuelles valorisées à près de 20 millions d'euros (dont 28 bitcoins), un lingot d'or et une Rolex, sur la base d'informations fournies par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), chargé de l'enquête. Il avait utilisé le système des rançongiciels.

Les interpellations restent rares. Les responsables du rançongiciel ont généralement échappé jusqu'ici aux autorités, protégés par leur habileté technique, avec des paiements en cryptomonnaies – difficiles à tracer – et des serveurs informatiques hébergés par des entreprises imperméables aux réquisitions judiciaires.

- Les cryptomonnaies ne sont pas intraçables, car la blockchain est visible et publique en permanence. Il faut du temps et de la technique pour relier ces transactions les unes aux autres et retrouver la place d'échange. Les mouvements des rançons représentent une mine d'informations que les autorités judiciaires peuvent sans doute exploiter, malgré la complexité de l'opération.

- Beaucoup d'opérateurs de rançongiciels louent leurs outils à d'autres groupes affiliés, spécialisés dans l'intrusion, qui mènent eux-mêmes

les attaques contre leurs victimes. Une fois la rançon payée, elle doit être divisée entre les affiliés et le « vaisseau mère ». Là encore, ces mouvements financiers, s'ils sont retracés par les enquêteurs, peuvent apporter des informations sur les suspects.

Pour lutter contre ces opérations, les autorités exercent leur pouvoir sur les plateformes de conversion. Comme les crypto monnaies ne sont pas réellement des monnaies, il faut s'engager dans l'utilisation du fiduciaire. Utiliser cet argent pour des achats reste très difficile. Toute une infrastructure de blanchiment du bitcoin existe avec une commission de 10%, sans impôts. Le transfert en bitcoins prend quelques secondes, sans coûts de transaction pour les opérateurs, les deux parties étant identifiables uniquement par un numéro de compte ou une adresse.

Faut-il interdire le bitcoin ?

Les défenseurs du bitcoin mettent en avant la liberté des personnes, le rejet des politiques monétaires officielles et la protection contre l'autoritarisme de l'Etat. Le Bitcoin est utilisé sur des sites commerciaux de biens et services illicites. Le marché actuel des cryptomonnaies, en plus d'être insuffisamment régulé, apporte peu à l'économie réelle, et il nourrit essentiellement la spéculation ou la criminalité. Les rançongiciels ne sont qu'un symptôme du manque d'investissements en cybersécurité au cours des dernières décennies.

Il faut réguler plus fermement l'écosystème qui entoure le bitcoin pour plus de transparence, et notamment le secteur des plates-formes d'échange qui ne vérifient pas toujours l'identité des utilisateurs, comme si elles souhaitaient faciliter les activités illicites. Il convient de réintroduire des valeurs éthiques (Fontanel, 2007) pour empêcher que les crypto monnaies ne soient que des instruments destinés à un enrichissement frauduleux.

Le gouvernement des Etats-Unis s'est engagé fermement contre la menace cybercriminelles et il appelle à une harmonisation des réglementations internationales concernant les cryptomonnaies. Les mafias ou le terrorisme utilisent le bitcoin à des fins de blanchissement de l'argent du crime ou de transfert vers des paradis fiscaux.

Le Salvador a décidé de faire du bitcoin sa monnaie nationale, au même titre que le dollar. Il est vrai que le taux d'inflation dans ce pays est très élevé et que d'une certaine manière les évolutions du bitcoin sont moins violents. Cependant, le Salvador s'inscrit dans les mouvances des paradis fiscaux et de la protection des grandes fortunes pas nécessairement gagnées de manière légales.

Aujourd'hui, le gouvernement chinois interdit aux banques nationales les transactions avec les bitcoins et toutes autres cryptomonnaies. Les Etats-Unis commencent aussi à exiger des contribuables (mais pas des banques) une information sur les mouvements de plus de 10.000 dollars. Les Etats cherchent à empêcher la création d'un système fermé de crypto monnaies qui pourraient remplacer le marché en monnaie nationale. Ils s'organisent pour créer des e-monnaie dans les mois à venir. L'Union européenne s'engage juridiquement vers un contrôle, voire une interdiction, de ces crypto monnaies, ou de l'anonymat.

Le bitcoin est une œuvre d'art mathématique. Ce n'est pas une monnaie, tout juste une sculpture artificielle artistique qui ne vaut que par la loi de l'offre et de la demande, sans avoir pour autant un intérêt positif pour l'économie réelle. Sauf pour les spéculateurs, le crime organisé et l'évasion fiscale. « Nous pouvons vivre dans un monde avec des cryptomonnaies ou un monde sans rançongiciel, mais on ne peut pas avoir les deux ».

Pour prolonger cette analyse, vous pouvez vous référer à la bibliographie fournie dans le document que vous pouvez vous procurer auprès des organisateurs.

Merci pour votre attention.

Bibliographie sommaire

Davidson, S., De Filippi, P., Potts, J. (2018), Blockchains and the economic institutions of capitalism, *Journal of Institutional Economics*.

De Filippi, P.(2020), *Blockchain et crytomonnaies*, Que Sais-Je ? Presses Universitaires de France.

Dupont, Q. (2018), *Blockchain and Cryptosurrencies*, Polity.

Fontanel, J. (2005). *La globalisation en analyse: géoéconomie et stratégie des acteurs*. Editions L'Harmattan.

Fakunmoju, S. K., Banmore, O., Gbadamosi, A., & Okunbanjo, O. I. (2022). Effect of Cryptocurrency Trading and Monetary Corrupt Practices on Nigerian Economic Performance. *Binus Business Review*, *13*(1)

Fontanel, J. (2007), *Questions d'éthique : guerre, démocratie, économie, éducation, marketing, sport, genre.* », L'Harmattan, Paris.

Fontanel, J. (2016), Paradis fiscaux, pays filous. La fuite organisée des impôts vers les pays complices fiscaux, L'Harmattan, Paris,

Fontanel, J., Sushcheva, N. (2019), La puissance des GAFAM : réalités, apports et dangers, *AFRI, Annuaire Français des Relations Internationales*, Paris.

Leloup, L. (2017), *Blockchain. La révolution de la confiance*, Editions Eyrolles.

Redon, M., Lebeau, M. (2020), Les flux de capitaux, légaux et plus obscurs : les tripots de la globalisation, in *Géopolitique des jeux d'argent, les enjeux d'une mondialisation silencieuse*. Le Cavalier Bleu.