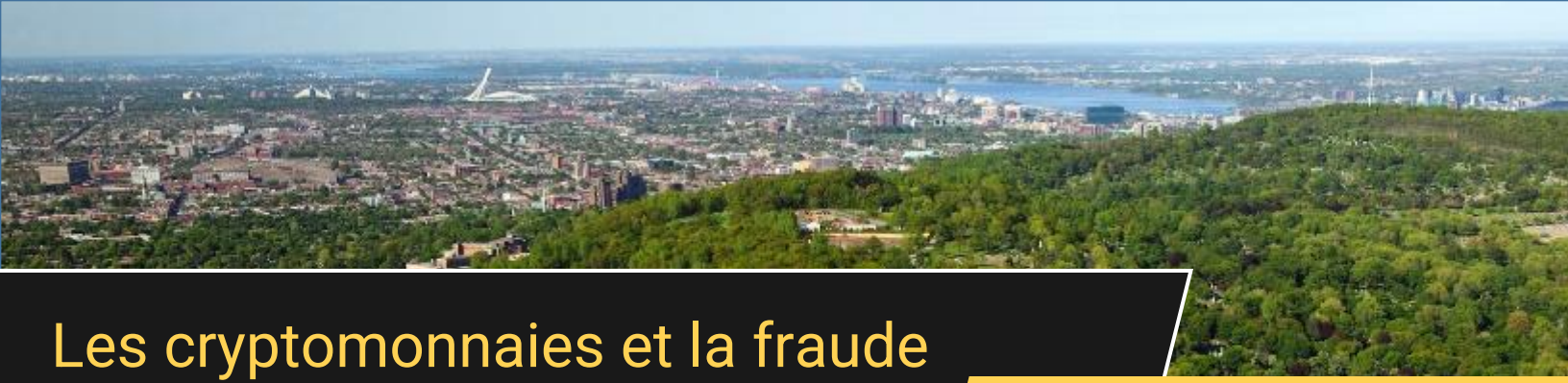
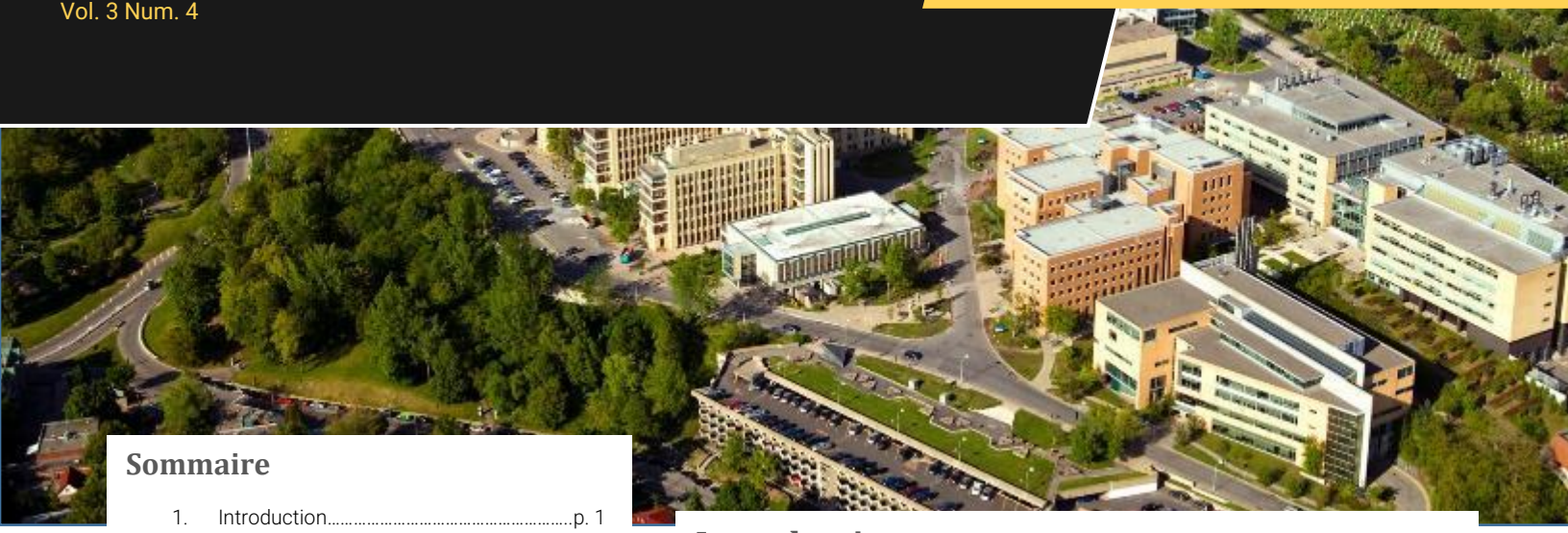


Les cryptomonnaies et la fraude

Marie-Pier Villeneuve-Dubuc, candidate à la maîtrise

Note de synthèse
Vol. 3 Num. 4

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.

Introduction

Les cryptomonnaies représentent un amalgame de technologies innovantes et de services financiers décentralisés attirant de plus en plus d'utilisateurs et d'attention médiatique. Cette hausse rapide et importante de l'offre de cryptomonnaies entraine bien évidemment des possibilités d'utilisation malveillantes. En effet, plusieurs types de crimes économiques, tels que la fraude ou bien encore le blanchiment d'argent peuvent s'effectuer via les cryptomonnaies[1]. Cette note de synthèse a pour objectif d'illustrer les principaux types de fraude faisant usage de cryptomonnaie et permettra aux lecteurs de se familiariser avec cette dernière et les caractéristiques pouvant être utilisées à des fins malveillantes ou illégales. Des recommandations pratiques, applicables par les décideurs gouvernementaux ou entrepreneuriaux seront également partagées.

Définition et principales caractéristiques des cryptomonnaies

La cryptomonnaie est une monnaie numérique, créée à l'aide d'algorithmes, qui n'est ni émise, ni administrée par un gouvernement ou une banque centrale[2]. Plus précisément, la cryptomonnaie est un actif numérique du secteur privé, qui s'appuie sur les technologies de la cryptographie, des registres distribués (par ex., les chaînes de blocs) et toutes autres technologies similaires[3]. Les différentes cryptomonnaies fonctionnent à l'aide d'un réseau décentralisé pair à pair (P2P) regroupant plusieurs acteurs[4]

et rejettent l'implication d'une tierce partie, comme un gouvernement ou une banque centrale à titre de gardien ou responsable de sa régulation[5, 6]. Le réseau de "pairs" réfère aux utilisateurs qui réalisent des transactions à l'aide de leurs ordinateurs et qui forment un réseau distribué[2]. Les détenteurs de cryptomonnaies peuvent dépenser leurs monnaies numériques à l'aide du système de chiffrement asymétrique impliquant une clé publique et clé privée. La clé publique leur permet d'envoyer leur argent et de créer des adresses qui représentent des identifiants afin d'envoyer ou recevoir des cryptomonnaies[1, 7]. La clé privée représente une série de chiffres aléatoires qui permettent à l'utilisateur de dépenser ses actifs de cryptomonnaies[8]. En résumé, les différentes cryptomonnaies partagent trois principales caractéristiques: elles sont décentralisées, pseudoanonymes, et transparentes[1]

En effet, la majorité des cryptomonnaies procurent un pseudoanonymat, car l'utilisation de la chaîne de blocs s'appuie sur un registre public permettant à tous les utilisateurs d'observer les transactions et de connaître des informations relatives à celles-ci telles que l'adresse de l'expéditeur et du destinataire ainsi que le montant envoyé[9, 10]. Plusieurs informations relatives à l'identité des parties impliquées dans une transaction peuvent ainsi mener leur identification. De plus, de nombreuses entreprises ont développé des outils permettant d'identifier des individus ou des regroupements à des numéros de portefeuille illicites ou légitimes. Il est aussi possible de trouver des informations sur l'identité de propriétaire de portefeuille de cryptomonnaie à l'aide d'outils en sources ouvertes. C'est principalement grâce aux sorties de transaction non dépensée (*Unspent Transaction Output* [UTXO] en anglais), représentant la balance du montant désirant être envoyé, qu'il est possible de retracer des portefeuilles ou des regroupements de portefeuilles[10].

Les cryptomonnaies et les possibles utilisations malveillantes

Néanmoins, certaines cryptomonnaies, communément nommées « cryptomonnaies à anonymat augmenté » (*anonymity-enhanced cryptocurrencies* [AECs] en anglais), déjouent la nature transparente et pseudonyme des cryptomonnaies. Monero (XMR) est la plus populaire en termes de quantité de transactions, mais aussi en termes de valeur unitaire, mais il en existe d'autres telles que ZCash (ZEC), Oasis Network (ROSE), Secret (SCR) et Decred (DCR)[11]. Développée en 2014, Monero a fait de la protection de la vie privée de ces utilisateurs son argumentaire de vente et s'appuie sur la technologie de la chaîne de bloc en y ajoutant un algorithme ayant une fonction spéciale permettant d'exercer de la cryptographie avancée[12]. En effet, c'est grâce à la technologie cryptographique de la signature de cercle (*Ring Confidential Transactions* en anglais) que le camouflage des identifiants des deux parties dans une transaction est rendu possible[13, 14]. Cette technologie représente un système de signatures chiffrées multicouches qui permet de masquer les montants des transactions, les origines et les destinations à l'intérieur du groupe d'utilisateurs[13]. Cette technologie d'anonymat amène plusieurs chercheurs et agences gouvernementales à soulever des préoccupations face à l'utilisation des AECs et la signature de cercle par les groupes criminels[1, 14, 15].

Il existe aussi des services de mixage de cryptomonnaies qui appliquent des techniques permettant de réduire la traçabilité des transactions des utilisateurs[16]. Ces services permettent d'obscurcir la relation entre les entités de la transaction, rendant difficile l'identification de l'origine fonds[17]. Il existe trois types de service de mixage des cryptomonnaies, tous ayant leur lot d'avantages et d'inconvénients : le service centralisé (par ex., Bitcoin Fog), le service décentralisé (par ex., CoinJoin) et le *cross-blockchain mixing service / Decentralized Finance* (finance décentralisée) (DeFi) (par ex., ShapeShift). Les services de mixage centralisés s'appuient sur des serveurs centralisés permettant d'effectuer le mélange, mais aucune garantie d'envoi aux destinateurs ou d'un réel mélange n'est assurée[17].

Les deux autres services apparaissent moins risqués pour les utilisateurs puisque les fonds ne sont pas détenus par un tiers et/ou les transactions se font sans intermédiaire. Ainsi, les services de mixage décentralisés s'appuient plutôt sur la signature conjointe d'un contrat intelligent

numérique afin de camoufler les entrants et sortants des transactions[18]. Finalement le *cross-blockchain mixing service* / DeFi fournit un service de convertisseurs de cryptomonnaies[17]. Il est donc possible pour les utilisateurs d'échanger leur bitcoin avec d'autres cryptomonnaies rendant le suivi des transactions difficiles[17]. Ces services sont un facilitateur pour les activités criminelles telles que le blanchiment d'argent[17]. Toutefois, bien que ces services rendent plus difficile le suivi des transactions, le traçage n'est pas impossible. Une équipe de chercheurs[17] ont d'ailleurs proposé un algorithme étant en mesure d'identifier 92% des transactions provenant de services de mixage.

Criminalité économique et cryptomonnaie : qu'en est-il?

Depuis l'apparition et le développement rapide des monnaies numériques, les fraudes liées aux cryptomonnaies sont devenues un enjeu mondial[1]. À titre d'illustration, une revue systématique, s'appuyant sur de la littérature scientifique, des rapports du secteur privé et public a identifié 47 stratagèmes de fraudes et arnaques de cryptomonnaies regroupées en 29 catégories[1]. Malgré la quantité de stratagèmes de fraude possible, selon Chainanalysis[19], les transactions de cryptomonnaies associées à des activités illicites ne représenteraient que 0,34% de l'ensemble des transactions en 2020. Parmi ce faible pourcentage, les crimes liés à l'utilisation de cryptomonnaies sont très diversifiés : rançongiciels, vente de produits illégaux sur les sur le darkweb, vente de matériels montrant l'exploitation sexuelle d'enfants, échange de fonds volés ou bien encore fraude en ligne, alors que les fraudes et arnaques représentent une portion significative de l'ensemble des crimes rapportés dans ce rapport[19]. De plus, plus de 33 milliards de dollars de cryptomonnaies auraient été blanchis, et ce, depuis 2017[19]. En 2021, le blanchiment d'argent représentait seulement 0,05% du volume total des transactions en cryptomonnaies[19]. Le Centre Anti-Fraude du Canada (CAFC) rapporte quant à lui une augmentation de 5 600% des signalements de fraudes impliquant l'utilisation de cryptomonnaies depuis 2015. Le CAFC affirme d'ailleurs les cryptomonnaies peuvent être utilisées afin de faciliter la fraude, et qu'elles représentent une menace pour l'intégrité financière du Canada[20].

Il importe de mentionner que les transactions en cryptomonnaies impliquant des adresses illicites semblent à la baisse depuis 2017[21]. En effet, alors que la criminalité appert prendre une place de plus en plus petite dans l'écosystème de la cryptomonnaie, la capacité des forces de l'ordre à lutter contre cette criminalité évolue grandement[21]. Les outils de traçage, combinés à la technologie de la chaîne de bloc, permettent aux forces de l'ordre de suivre des transactions plus facilement contrairement à la monnaie fiduciaire[21]. Les enquêtes policières concernant la monnaie fiduciaire peuvent être longues et difficiles en raison des possibilités de dissimulation et de dispersion des avoirs dans différentes banques étrangères, contrairement aux cryptomonnaies où l'ensemble des transactions sont enregistrées dans la chaîne de blocs[21]. Les analyses des données de masse et des sources ouvertes permettent d'identifier les entités criminelles[22] et de connecter les adresses des utilisateurs entre elles en utilisant des analyses de réseau ou des heuristiques de co-dépenses afin de regrouper des clés publiques entre elles[23]. Cependant, le traçage peut être plus difficile lorsque le crime n'est pas commis par l'entremise d'un réseau internet et lorsqu'une adresse de portefeuille illicite n'est pas préalablement identifiée[22] ce qui nécessite davantage d'indices et de preuves pour le traçage. De plus, comme nous l'avons vu plus haut, certaines mesures peuvent compliquer le traçage. Ainsi, une intervention ciblée peut nuire grandement au réseau criminel et empêcher les individus d'avoir accès à leur actif[21]. Selon Chainalysis, il est toutefois possible de voir un déplacement du blanchiment d'argent vers les plateformes de cryptomonnaie dans les prochaines années en raison de la hausse de leur popularité[21].

Conclusion

Cette note de synthèse nous permet d'émettre quatre catégories de recommandations concernant l'utilisation des cryptomonnaies à des fins criminelles: 1) le renforcement des régulations, 2) les innovations techniques, 3) l'amélioration des formations et 4) l'augmentation des ressources en prévention. Ces recommandations représentent davantage des propositions pour diriger les actions des gouvernements et législateurs vers une adaptation adéquate de la société face à la hausse de l'offre des cryptomonnaies et des produits numériques susceptibles d'être utilisés à des fins criminelles dans les prochaines années.

En conclusion, malgré leur potentiel malveillant, les cryptomonnaies et les technologies sous-jacentes représentent des innovations inéluctables qui attirent un grand nombre d'individus. En termes d'étude du phénomène, il importe de se questionner sur une augmentation réelle de la criminalité liée aux cryptomonnaies ou bien s'il s'agit d'un déplacement et de l'adaptation des criminels aux innovations technologiques.

Recommandations pratiques

Renforcer les régulations vis-à-vis la cryptomonnaie

- **Favoriser la collaboration internationale** afin de collecter et partager l'information pour avoir un portrait complet de l'évolution des marchés et minimiser l'arbitrage réglementaire[3].
- **Concentrer les réglementations sur les interfaces entre les cryptomonnaies, les banques et les services de paiement**[6]. Les régulations visant directement les codeurs, programmeurs ou mineurs impliqués dans la création et le fonctionnement des cryptomonnaies sont difficilement applicables en raison des législations et des restrictions issues des différentes juridictions. La régulation des plateformes d'échanges et des services de conversion de cryptomonnaie en monnaie fiduciaire a démontré de meilleurs résultats[6].
- **Encourager la création de partenariat entre les policiers, les équipes à l'origine des protocoles DeFi et les institutions bancaires**. Une réglementation devrait être mise sur pied afin de nuire à l'abus des plateformes DeFI par les criminels.

Innover dans les techniques d'exploration de données

- **Utiliser la technologie d'intelligence artificielle** telle que l'apprentissage automatique et l'analyse des données de masse afin d'identifier et classer les adresses illicites.

Formations et ressources

- **Mettre en commun les ressources humaines et matérielles des différentes agences policières** chargées de répondre aux crimes économiques[23]. Il existe une disparité entre les ressources disponibles au sein des différentes organisations policières dans le monde causant des lacunes importantes dans la réponse policière face aux crimes internationaux, dont les fraudes et le blanchiment d'argent usant de cryptomonnaie[1].
- **Formation poussée sur l'importance de la preuve** notamment quant à la collecte, au stockage et au traitement des preuves numériques lors de la perquisition[24].
- **Développer des équipes spécialisées d'individus dynamiques et confortables** avec les innovations technologiques afin d'éviter les biais cognitifs de la fatigue professionnelle qui nuisent à la réponse policière face à ces types de crimes.
- **Former des équipes spécialisées dans la réponse policière et l'enquête sur le cas de fraudes liées aux cryptomonnaies** pour contrer le manque de connaissances, de formation et d'expériences sur les technologies et les nouvelles méthodes criminelles[25, 26].

Prévention

- Considérant la hausse de la popularité des cryptomonnaies, il serait pertinent de favoriser un **discours public nuancé sur les cryptomonnaies** afin que la population puisse faire un choix éclairé de son utilisation. Ainsi, il serait pertinent de renseigner la population sur les risques, mais aussi son fonctionnement et des mesures de sécurité.
- **Mettre sur pied un registre d'adresses identifiées comme illicites** accessible au public afin qu'il puisse se renseigner sur la légitimité de l'adresse avant de faire affaire avec celle-ci.
- **Mettre sur pied un registre public des plateformes d'échange de cryptomonnaies légitimes** afin de permettre aux utilisateurs de s'assurer de la légitimité de la plateforme avant de faire affaire avec celle-ci. Tout comme le registre d'entreprise du Gouvernement du Québec, la population aurait accès à l'ensemble des informations qu'une plateforme d'échange déclare.

Références

[1] Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T. et Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*(1), 1-35.

[2]Gouvernement du Canada (2021). *Monnaie numérique*. https://www.canada.ca/fr/agence-consommation-matiere-financiere/services/paiment/monnaie-numerique.html

[3] Financial Stability Board (2022). *Assessment of Risks to Financial Stability from Crypto-assets*. https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/

[4] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, 88, 173-190. https://doi.org/10.1016/j.future.2018.05.046

[5] Payne, J. (2015). The Role of Gatekeepers. Dans Niamh Moloney, Eil´s Ferran et Jennifer Payne (dir.), *The Oxford Handbook of Financial Regulation*.

[6] Nabilou, H. (2019). How to regulate bitcoin? Decentralized regulation for a decentralized cryptocurrency. *International Journal of Law and Information Technology*, *27*(3), 266–291.

[7] CoinMarketCap (2022a). *Top 100 Crypto-monnaies par capitalisation de marché*. https://coinmarketcap.com/fr/

[8] Loshin, P. et Cobb, M. (2022). *Definition Private Key. TechTarget Security*. https://www.techtarget.com/searchsecurity/definition/private-key

[9] Bunjaku, F., Gjorgieva-Trajkovska, O. et Miteva-Kacarski, E. (2017). Cryptocurrencies–advantages and disadvantages. *Journal of Economics*, *2*(1), 31-39.

[10] Akcora, C. G., Gel, Y. R. et Kantarcioglu, M. (2022). Blockchain networks: Data structures of Bitcoin, Monero, Zcash, Ethereum, Ripple, and Iota. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *12*(1), e1436. https://doi.org/10.1002/widm.1436

[11] Culafi, A. (2022, 24 janvier). *Monero and the complicated world of privacy coins*. TechTarget: SearchSecurity.

[12] CoinMarketCap (2022c). *Monero*. https://coinmarketcap.com/fr/currencies/monero/

[13] Noether, S. (2015). *Ring signature confidential transactions for Monero*. IACR Cryptology ePrint Archive, 2015, 1098.

[14] Alexandria (2022). Ring Signature. *CoinMarketCap: Glossary*. https://coinmarketcap.com/alexandria/glossary/ring-signature

[15] Keller, P., Florian, M., & Böhme, R. (2021). Collaborative deanonymization. *In Financial Cryptography and Data Security. FC 2021 International Workshops: CoDecFin, DeFi, VOTING, and WTSC*, Virtual Event, March 5, 2021, Revised Selected Papers 25 (pp. 39-46). Springer Berlin Heidelberg.

[16] Sun Yin, H. et Vatrapu, R. (2017). A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning. *2017 IEEE International Conference on Big Data (Big Data)*, 3690 3699.

[17] Wu, L., Hu, Y., Zhou, Y., Wang, H., Luo, X., Wang, Z., Zhang, F. et Ren, K. (2021). Towards Understanding and Demystifying Bitcoin Mixing Services. *Proceedings of the Web Conference 2021*, 33 44.

[18] Hayes, A. (2021). World monies or money-worlds: a new perspective on cryptocurrencies and their moneyness. *Finance and society*, *7*(2), 130-39. https://doi.org/10.2218/finsoc.v7i2.6629

[19] Chainanalysis (2021). *The 2021 Crypto Crime Report: Everything you need to know about ransomware, darknet markets, and more*. Chainanalysis.

[20] Centre Anti-Fraude du Canada (CAFC) (2021, septembre). T*he Use of Crypto Currencies in Fraud* (publication no CAFC AL- 2021-3421).

[21] Grauer, K., Kueshner, W. et Updegrave, H. (2022). The 2022 Crytpo Crime Report - Original data and research into cryptocurrency-based crime. *Chainalysis*. https://go.chainalysis.com/2022-Crypto-Crime-Report.html

[22] Hassani, H., Huang, X., et Silva, E. (2018). Big-Crypto: Big Data, Blockchain and Cryptocurrency. *Big Data and Cognitive Computing*, *2*(4), 34.

[23] Lemieux, F. (2018). Police Cooperation Across Jurisdictions. *Oxford Research Encyclopedia of Criminology*.

[24] Dodge, C. et Burruss, G. W. (2019). Policing cybercrime: Responding to the growing problem and considering future solutions. Dans R. Leukfeldt et T. J. Holt (dir.), *The Human Factor of Cybercrime (Chapter 15*). Abingdon, UK: Routledge.

[25] Boes, S. et Leukfeldt, R. (2017). Fighting cybercrime: A joint efforts. Dans R. M. Clark et S. Hakim (dir.), *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level* (pp. 185-203). Springer.

[26] Dolliver, D. S. (2019). Emerging technologies, law enforcement responses, and national security. *Journal of Law and Policy for the Information Society*, *15*, 123-150.