Apports et limites des données numériques pour l'analyse géopolitique de l'infrastructure Bitcoin

Hugo Estecahandy[1]

En Ukraine, dès les premiers jours de l'offensive russe, le gouvernement, des ONG et des groupes d'autodéfense ont accepté des dons en cryptomonnaies, afin de recevoir des finances rapidement mobilisables pour acheter des biens de première nécessité ou du matériel de guerre[2]. Certains Russes, quant à eux, les ont utilisées, dans des proportions limitées, à la fois comme valeur refuge face à la chute du rouble ou pour mobiliser leur épargne à l'étranger[3]. Si leur impact durant cette période est à relativiser, les cryptomonnaies ont permis de contourner des limites et restrictions (délais, coûts, interdits) des réseaux financiers traditionnels. Ces usages des cryptomonnaies sont à la fois dans la continuité de l'idéal sous-jacent à la première d'entre elles, bitcoin, et de nombreux usages similaires précédemment observés. Créé en 2009 par la ou les personnes réfugiées sous le pseudonyme de Satoshi Nakamoto, Bitcoin était justement présenté comme un réseau financier alternatif pair à pair, sur lequel les utilisateurs s'échangent

1. Doctorant à l'Institut français de géopolitique et membre du projet Geode-Géopolitique de la datasphère.

2. Christina Criddle, « How Ukraine embraced cryptocurrencies in response to war », *Financial Times*, 19 mars 2022, <https://www.ft.com/content/f3778d00-4c9b-40bb-b91c-84b60dd09698>.

3. Olivier Duplessix, « La Russie peut-elle utiliser des cryptomonnaies pour contourner les sanctions économiques ? », *Ouest France*, 2 mars 2022. <https://www.ouest-france.fr/leditiondusoir/2022-03-02/la-russie-peut-elle-utiliser-des-cryptomonnaies-pour-contourner-les-sanctions-economiques-f294dd52-1af4-42c9-8f02-d6a1bf4dff1e>.

directement de l'argent – des bitcoins – hors de la portée des gouvernements et des banques [Nakamoto, 2008]. L'enjeu était d'émanciper l'individu d'une centralisation de l'autorité sur l'argent. Ainsi, dès 2011, les dons en bitcoins ont été acceptés par le site WikiLeaks, déconnectés des principaux services de paiement[4] à la demande des autorités américaines. Le site avait auparavant fait fuiter des documents confidentiels de l'US Army. Plus récemment, en 2020, des dons en bitcoins ont été massivement envoyés aux meneurs de manifestations d'opposition au Nigeria, dont les comptes bancaires avaient été gelés par les autorités.

Les cryptomonnaies sont ainsi parfois utilisées comme alternatives à des réseaux sur lesquels certains gouvernements et banques disposent d'un pouvoir politique conséquent, comme le montre l'application des sanctions occidentales à l'encontre de la Russie. Elles participent ainsi à redessiner les réseaux de pouvoir traditionnels sur l'argent et, donc, certains rapports de force géopolitiques. Ce potentiel est désormais exploité par certains États, à l'image du Salvador qui a fait du bitcoin sa monnaie nationale en septembre 2021 aux côtés du dollar américain. Le gouvernement salvadorien souhaitait alors réduire sa dépendance aux États-Unis et à sa banque centrale (la Fed) qui émet et régule le dollar, monnaie unique du pays depuis 2001. À l'inverse, ce potentiel d'émancipation d'un contrôle étatique sur l'argent a poussé certaines autorités à prendre des mesures drastiques contre ces monnaies numériques, comme la Chine qui a banni les cryptomonnaies et leur industrie de création, le minage, également en septembre 2021. Ce faisant, les autorités chinoises souhaitent reprendre le contrôle sur les paiements électroniques de leur population[5] et se débarrasser d'une industrie jugée énergivore[6].

Avec ces évènements aux contextes très différents, les cryptomonnaies apparaissent désormais comme des outils, et même des enjeux géopolitiques de premier ordre. Ce travail est donc l'occasion de présenter des approches et méthodes désormais nécessaires pour appréhender et analyser les cryptomonnaies et leur place dans les enjeux contemporains. S'il existe désormais des milliers de cryptomonnaies[7], avec chacune des degrés de centralisation ou d'anonymat

4. Dont Mastercard, Visa, PayPal et Western Union.

5. En Chine, en 2018, 83 % des paiements ont été réalisés par smartphones (paiements mobiles). Voir Daxue Consulting, 4 juillet 2021, <https://daxueconsulting.com/payment-methods-in-china/>.

6. En 2021, la Chine a fait face à une crise de l'électricité, ne pouvant plus produire assez pour répondre à la demande énergétique du pays. Voir Philip Inman, « How bad is China's energy crisis ? », *The Guardian*, 29 septembre 2021, <https://www.theguardian.com/world/2021/sep/29/how-bad-is-chinas-energy-crisis>.

7. Le site Coinmarketcap.com référence 10 080 cryptomonnaies différentes en circulation au 17 mai 2022.

différents, cet article se concentre exclusivement sur Bitcoin, le premier de ces réseaux numériques. L'objectif de cette démarche est de pouvoir analyser plus précisément la place et l'impact de Bitcoin dans l'espace physique, les réseaux de pouvoir qui se dessinent avec et au sein du réseau, initialement pensé autour du concept de décentralisation. Cette décentralisation théorique du pouvoir est censée être garantie par plusieurs facteurs, dont la distribution du pouvoir de validation des nouvelles transactions entre les membres du réseau ou encore la transparence de l'information avec des transactions consultables par tout un chacun. Ainsi, l'utilisation même du réseau produit des données numériques, dont certaines sont en libre accès. Les chercheurs peuvent s'approprier ces sources ouvertes pour mieux cerner les dynamiques et logiques de ce réseau. Car un bitcoin est immatériel. Il n'« existe » que par l'inscription, sur un registre numérique dénommé blockchain (pour « chaîne de blocs »), de son émission d'une adresse à une autre. La blockchain fonctionne comme un livre de comptes, libre de consultation, sur lequel ces transactions composent autant de « preuves de propriété » d'un ou d'une subdivision de bitcoin. Aussi virtuel que puisse paraître ce processus, il présente néanmoins une forte matérialité, que ce soit par les infrastructures physiques impliquées dans le fonctionnement du réseau (puissance de calcul, stockage) ou par les potentielles répercussions de cette transaction au sein de l'espace physique (achat de biens ou de services). Afin de distinguer les différents espaces et dimensions dans lesquels évolue Bitcoin, il est nécessaire d'en définir les contours et composantes. En cela, Bitcoin doit être étudié comme un tout, un ensemble d'entités, physiques et immatérielles, dont l'ensemble des relations créent des enjeux et relations de pouvoir au sein et autour de ce réseau. L'enjeu de cet article est alors double. Tout d'abord, l'idée est de définir Bitcoin comme une infrastructure numérique intégrée dans l'espace et ses multiples dimensions, physiques ou immatérielles. Ensuite, l'objectif est de présenter les apports et les limites de différents types de données numériques qui permettent d'analyser et de visualiser cette infrastructure ainsi que ses logiques et dynamiques internes.

Bitcoin, un objet géopolitique

Par son fort ancrage dans l'espace physique et les enjeux qui émergent avec l'augmentation de son utilisation et de son adoption, Bitcoin est un objet géopolitique qui se doit d'être analysé comme tel. Pour ce faire, il est nécessaire de bien cerner les différentes entités qui composent cette infrastructure numérique, elle-même insérée dans le réseau Internet. Cela afin de pouvoir analyser Bitcoin comme un espace où apparaissent des enjeux de pouvoir et des conflits.

Une infrastructure numérique construite autour de la décentralisation

Bitcoin possède une architecture particulière, qui est à mettre en relation avec les objectifs et les idées envisagés par son, sa ou ses créateurs. Pour garantir un niveau d'autorité équivalent à tous les membres du réseau Bitcoin, ainsi délesté de « tiers de confiance » (gouvernements, banques), plusieurs éléments ont été mis en œuvre par Nakamoto. Ils s'appuient à la fois sur l'algorithme qui soutient Bitcoin et sur les modes d'organisation des acteurs impliqués dans le fonctionnement du réseau. Par exemple, chaque membre peut héberger une copie, entière ou partielle, du registre numérique (la blockchain), sur lequel sont inscrites les transactions, ce qui diminue le risque de corruption et/ou de destruction des informations. La totalité de ces milliers de copies est mise à jour de manière synchronisée, et les transactions sont librement consultables. En plus d'offrir tout un panel de données numériques qui permettent d'étudier le fonctionnement de Bitcoin, ce à quoi la deuxième partie de cet article est dédiée, ce principe de transparence de l'information permet à chaque membre de participer à la sécurisation du réseau.

Effectivement, le processus de vérification et de validation des nouvelles transactions de bitcoins, le « minage », est théoriquement réalisable par n'importe lequel des membres. Les nouvelles transactions, en attente de validation, sont insérées dans un bloc, l'équivalent d'une nouvelle page de ce registre numérique. Les vérificateurs utilisent alors de la puissance de calcul informatique pour vérifier l'intégrité des données de transactions inscrites sur la blockchain Bitcoin et le nouveau bloc, notamment le fait qu'un même bitcoin n'est pas été dépensé deux fois par la même personne par exemple, puis entrent ensuite en concurrence pour résoudre un calcul. Le premier à trouver la solution voit sa vérification validée par le réseau et est automatiquement rémunéré en bitcoins en « récompense » du temps et de la puissance de calcul mobilisés. C'est également *via* cette récompense que les bitcoins sont émis dans le réseau et donc directement envoyés à certains vérificateurs, également dénommés mineurs. Le nouveau bloc validé est alors ajouté au registre, qui n'est autre qu'une suite de blocs d'informations où sont inscrites des transactions, liés entre eux par des procédés cryptographiques permettant de garantir l'inaltérabilité des données. Théoriquement, pour modifier une information dans cette chaîne de blocs, il faudrait disposer de la majorité de la puissance de calcul de Bitcoin, pour revalider tous les blocs entre le plus récent et celui où se trouve l'information modifiée.

Avec l'augmentation de l'utilisation et de la valeur du bitcoin, d'autres services ont été développés et greffés à la blockchain Bitcoin et à son logiciel client originel, Bitcoin Core, développé par Nakamoto et qui permet d'interagir avec le registre (pour miner, effectuer des transactions). Ainsi, des plateformes d'échange de cryptomonnaies contre des monnaies fiduciaires et des solutions

Hérodote, n° 186, La Découverte, 3e trimestre 2022.

de portefeuilles numériques, proposant un hébergement sécurisé des clés permettant à l'utilisateur d'accéder à ses unités de cryptomonnaies, sont par exemple apparues. Le minage est devenu une activité très rentable, tant la valeur de la récompense a pu augmenter depuis 2009 et la hausse de la valeur de la cryptomonnaie, et a été développé à une échelle parfois industrielle, impliquant des besoins croissants en énergie électrique. Certains bâtiments, des « fermes de minage », peuvent renfermer jusqu'à plusieurs milliers de processeurs. Bitcoin ne se limite pas alors à la seule blockchain sur laquelle sont inscrites les transactions, mais est composé d'une multitude d'acteurs (mineurs de cryptomonnaies, utilisateurs, développeurs...), d'interfaces et de services (plateformes d'échange, portefeuilles numériques), de processeurs et de serveurs informatiques en interaction. Bitcoin doit alors être pensé et analysé comme une infrastructure. Si cette notion d'infrastructure « se réfère typiquement à des systèmes physiques et matériels à large échelle nécessaires pour l'organisation et l'activité humaine » [Musiani, 2018] comme les routes et autres canalisations, le réseau Bitcoin est également un concept « fondamentalement relationnel, devenant une vraie infrastructure en relation avec des usages organisés » [Star et Ruhleder, 1996]. Cette démarche permet de visualiser les différentes entités qui composent Bitcoin, de se pencher sur leurs interactions et de prendre conscience de la relation dialectique qu'entretiennent espaces physique et virtuel.

Un espace dans le cyberespace

Cette définition d'infrastructure numérique permet alors de penser et analyser Bitcoin comme étant lui-même inséré dans une infrastructure encore plus large et complexe : Internet. D'ailleurs, sans faire de parallèle hasardeux entre les réseaux Internet et Bitcoin, les différentes analyses et définitions du premier peuvent permettre de mieux appréhender le second. L'interconnexion des entités, objets ou individus grâce au développement d'Internet, et la massification importante et rapide des données numériques produites et échangées qu'il induit [Cattaruzza, 2019] ont amené à appréhender un nouveau type d'espace créé par la place croissante prise par Internet au sein des sociétés. Ainsi, le terme de cyberespace a commencé à être utilisé pour tenter de définir « à la fois ce "monde" virtuel, dématérialisé, sans frontières [...], mais également un espace "dangereux" et nébuleux » [Desforges, 2014]. Au-delà de l'Internet lui-même en tant qu'infrastructure, c'est tout un nouvel espace que les chercheurs, politiques ou autres stratégistes conceptualisent. Ainsi, une approche souvent utilisée du cyberespace est son découpage en différentes couches (ou strates), allant des infrastructures physiques (serveurs, câbles) aux couches dites sémantiques, c'est-à-dire virtuelles [Ventre, 2012 ; Douzet, 2014].

Cette conceptualisation théorique « très opérationnelle » du cyberespace permet de « fournir une dimension géopolitique plus concrète d'Internet [...] une matérialisation plus concrète du pouvoir sur Internet » [Cattaruzza, 2019]. Ce découpage du cyberespace par couches permet de visualiser la mégastructure qu'est Internet, et plus largement les autres objets ou sous-réseaux numériques qui y sont connectés. Il permet également de prendre conscience des différents types d'enjeux, économiques ou encore sécuritaires, induits par le cyberespace.

TABLEAU 1. – LE CONCEPT DE CYBERESPACE COMME CLÉ DE LECTURE GÉOPOLITIQUE DE BITCOIN

Couche du cyberespace	Définitions [Ventre, 2012 ; Douzet, 2014 ; Cattaruzza, 2019]	Équivalent infrastructure Bitcoin
Matérielle	Périphériques d'accès et infrastructures physiques nécessaires au fonctionnement d'Internet (serveurs, câbles, datacenters).	Fermes de minage, processeurs, serveurs stockant les copies de la blockchain Bitcoin.
Logique	Langage machine et protocole qui permettent aux ordinateurs de communiquer les uns avec les autres, et d'échanger un volume important de données. Repose sur un langage commun (protocole TCP/IP) et sur des services comme le routage, le nommage, ou l'adressage.	Protocole Bitcoin, algorithme de hachage SHA-256, restriction de la taille des blocs, etc.
Des applications	Permet « à tout un chacun d'utiliser l'Internet sans rien connaître à la programmation informatique (Web, e-mail, réseaux sociaux, moteurs de recherche, etc.) » [Douzet, 2014].	Bitcoin Core, portefeuilles numériques, logiciels de minage, plateformes d'échange.
Sémantique	En rapport avec le contenu informationnel. En clair, l'ensemble des messages qui passent par Internet. Cette couche est donc le lieu des interactions sociales et des échanges d'informations.	L'ensemble des transactions effectuées et consultables par tout internaute *via* des services tiers (explorateurs de blockchain).

Comprendre dans quels réseaux et structures, et par extension dans quels espaces et dimensions évolue Bitcoin est une étape clé pour mieux le cerner.

Hérodote, n° 186, La Découverte, 3e trimestre 2022.

Ce concept de cyberespace offre des grilles de lecture intéressantes pour visualiser et conceptualiser l'infrastructure Bitcoin. Elle est composée d'éléments extrêmement divers, dont l'interconnexion crée le réseau et les normes d'interaction au sein de ce dernier.

Bien qu'une cosmographie complète des entités composant Bitcoin soit impossible, les différents concepts d'infrastructure numérique et de cyberespace permettent d'appréhender les différentes dimensions et « couches » dans lesquelles chacune de ces entités évolue. Ainsi peuvent commencer à être pensés et appliqués des outils et méthodes pour étudier la distribution et la circulation des pouvoirs au sein de l'infrastructure Bitcoin et de ses différentes couches.

Une infrastructure décentralisée où se dessinent des réseaux de pouvoir

Cette approche de Bitcoin en tant qu'infrastructure et espace permet de mieux visualiser les différentes circulations et centralisations des pouvoirs au sein du réseau. Le modèle de gouvernance théorique de Bitcoin est originellement basé sur la transparence et le consensus, et est caractérisé par une forte décentralisation de l'autorité et une distribution du pouvoir entre tous les membres du réseau. Mais, au-delà des lignes de codes initiales sur lesquelles Bitcoin a commencé à fonctionner, et ses mises à jour ultérieures, l'infrastructure prend forme *via* les usages et comportements des acteurs qui interagissent avec elle, ainsi qu'avec les normes et contraintes de fonctionnement des services permettant d'interagir avec le réseau (services de portefeuilles numériques, plateformes d'échange). Des formes de centralisation, de différentes échelles et dimensions, sont ainsi apparues au fil de l'évolution de Bitcoin.

Des travaux analysent déjà ces phénomènes, notamment les crises de gouvernance traversées par le réseau Bitcoin. Que ce soit lors de résolution d'un problème technique qui nécessitait que certains nœuds du réseau reviennent à une version logicielle antérieure [Musiani *et al*., 2018] ou l'impossible consensus entre partisans et opposants d'une augmentation de la taille des blocs [De Filippi et Loveluck, 2016], certaines formes de centralisation des pouvoirs apparaissent durant ces crises. Ces travaux mettent en évidence non seulement la difficulté d'atteindre un consensus entre les différents acteurs du réseau, mais aussi que les membres qui ont une réelle influence sur le réseau, que ce soit par le poids politique de leurs décisions ou leur capacité à intervenir techniquement, ne sont qu'extrêmement minoritaires. En étudiant des incidents techniques et le processus de leur résolution, l'approche des chercheurs révèle ainsi une hiérarchie du pouvoir dans un système à l'autorité théoriquement hautement distribuée. Ces travaux rappellent aussi que la « qualité normalement invisible de l'infrastructure devient visible lorsqu'elle

se brise » [Star, 1999], puisqu'ils mettent en lumière certains processus technico-politiques, comme des prises de décision pour modifier Bitcoin, et des hiérarchies de pouvoir au sein de Bitcoin en étudiant des résolutions de problèmes techniques.

Mais l'une des plus importantes formes de centralisation qui est apparue dans Bitcoin est celle entraînée par les plateformes d'échange de cryptomonnaies. Elles représentent près de 75 % des transactions de bitcoins [Makarov et Schoar, 2021]. Ces plateformes détiennent réellement les bitcoins de leurs utilisateurs. Cela entraîne alors une forte concentration de richesse et de pouvoir politique entre les mains d'entreprises commerciales, avec qui les autorités et forces de l'ordre étatiques collaborent pour réguler et surveiller les transactions. Le succès de Bitcoin est alors venu fragiliser l'idéal politique qu'il devait soutenir, en entraînant l'apparition de certains nœuds du réseau qui se sont arrogé un pouvoir sur certaines fonctionnalités de l'infrastructure, en facilitant notamment un traçage et une surveillance étatiques des transactions. En plus de cela, l'augmentation de la valeur du bitcoin entraînée par des logiques de spéculations a rendu le minage très lucratif. L'activité a alors été développée à l'échelle industrielle, en laissant apparaître une concentration des moyens de production (de la puissance de calcul) entre les mains de certains groupes d'acteurs, qui mettent cette ressource en commun afin de maximiser leurs chances de toucher la récompense en bitcoins [Romiti *et al*., 2019]. Ces groupes de mineurs à la puissance de calcul mutualisée sont appelés des « pools ». Une concentration géographique de l'activité au sein de territoires physiques disposant des ressources nécessaires est également apparue [Maurer *et al*., 2013], comme cela a déjà été étudié en Sibérie orientale où se trouvent une électricité très bon marché, un climat froid et sec permettant une bonne efficience des processeurs et une connexion Internet rapide et fiable [Estecahandy et Limonier, 2021].

Que ce soit dans les dimensions physiques ou virtuelles de Bitcoin, des phénomènes de concentration (du pouvoir, des moyens de production, des richesses) apparaissent. Cela permet alors de penser ce réseau non plus seulement comme une infrastructure numérique ou un espace, mais comme un objet géopolitique à part entière. Car, dès lors que l'espace est envisagé en tant qu'enjeu, car étant disputé par des acteurs, il devient l'objet de la géopolitique [Rosière, 2001]. Les acteurs de ces luttes de pouvoir, continues ou occasionnelles, sont internes à Bitcoin (plateformes d'échange, pools de minage, développeurs) ou externes (régulateurs étatiques, forces de l'ordre). Mais ils font tous de cet espace l'enjeu de leur pouvoir, et permettent ici d'adopter une approche de Bitcoin par la géopolitique.

Quelles données numériques pour naviguer dans le réseau Bitcoin ?

De plus, d'autres formes de centralisation apparaissent aussi bien dans l'espace physique que dans la couche des applications. Et plusieurs types de données numériques sont mobilisables pour les étudier, avec certaines limites parfois importantes.

Des données de localisation très limitées

Pour nourrir les réflexions de géographe, très expérimentales, présentées ici, les données numériques, pouvant apporter des informations de localisation des composantes matérielles du réseau, présentent un intérêt tout particulier. Elles permettent d'étudier la géographie de l'infrastructure numérique au sein de l'espace physique, notamment la localisation des milliers de disques durs et serveurs hébergeant des copies de la blockchain, et des fermes de minage conférant à Bitcoin une importante matérialité. Localiser les nœuds qui hébergent des copies complètes de la blockchain Bitcoin permet théoriquement de localiser avec précision des mineurs, puisqu'il leur est nécessaire de bénéficier de la copie de toutes les transactions précédemment enregistrées pour valider les nouvelles. Ainsi, plusieurs projets ont vu le jour, avec pour objectif de dresser une cartographie de la répartition des entités qui composent Bitcoin dans l'espace physique.

Le site Bitnodes.io propose une carte mise à jour en direct avec les localisations des nœuds du réseau atteint par un crawler, un programme informatique automatisé envoyé vers les nœuds du réseau pour récupérer leur adresse IP. La première limite est que près de 55 % de ces connexions, observées le 18 avril 2022, passent par le réseau Tor, qui change l'adresse IP de l'utilisateur au même titre qu'un service de VPN (Virtual Proxy Network), ce qui rend leur localisation précise impossible. Environ 12 % des nœuds crawlés apparaissent aux États-Unis et 9 % en Allemagne. Mais ici intervient la deuxième grande limite de cette technique, liée à une utilisation supposément massive de VPN et autres proxys au sein de la communauté Bitcoin, tant la question de l'anonymisation de données personnelles est ancrée dans le projet. Cette tendance rend alors impossible une cartographie précise de la répartition physique des nœuds de Bitcoin.

Le constat est le même pour le projet du chercheur Pablo Velasco. Il a réalisé une carte qui représente les nœuds complets, c'est-à-dire de ceux qui hébergent une copie complète de la blockchain Bitcoin, atteints par son crawler entre mars et juin 2015 [Velasco, 2016]. Il opère pourtant une classification intéressante des nœuds complets. Il qualifie de nœuds « forts » ceux qui sont restés connectés durant la totalité des quatre mois de son analyse. *A contrario*, il qualifie les nœuds

connectés moins de 10 % de ce temps de « fantômes ». Il en déduit que les nœuds forts sont ceux qui sécurisent vraiment le réseau, puisqu'ils sont connectés sans discontinuité et ont une copie du registre sans cesse mise à jour. Ces tentatives ont permis de faire ressortir d'autres éléments intéressants, notamment une hiérarchie des nœuds du réseau dans leur rôle dans la sécurisation de l'infrastructure.

Le bitcoin, une cryptomonnaie très traçable

Le fait que les données de transactions en bitcoins soient en accès libre offre des possibilités intéressantes pour la recherche. La consultation du registre est plutôt aisée, grâce à des explorateurs de blockchain (BlockchainExplorer, WalletExplorer) qui permettent de récupérer des informations sur les transactions et les adresses impliquées (nombres, adresses d'expédition ou de destination, montant, horodatage). L'un des principes originels de Bitcoin était d'offrir l'anonymat aux utilisateurs. Ainsi, les utilisateurs de bitcoins n'apparaissent sur le registre que *via* une adresse publique, c'est-à-dire une suite de vingt-quatre à trente-six caractères alphanumériques, commençant par « 1 », « 3 » ou « bc1 ».

Afin d'observer certaines possibilités offertes par l'exploitation de données de transactions en bitcoins, une étude de cas semble appropriée. L'objectif est, à partir d'un exemple concret, de présenter comment lire, analyser et visualiser certaines de ces données. Ici, l'analyse débute à partir d'une adresse trouvée sur la page d'un site français d'extrême droite et affichée comme une solution pour recevoir des dons. Le choix est fait d'anonymiser le site en question et de ne pas faire figurer les adresses, car ce n'est pas sur cela que se porte l'intérêt de l'étude. L'idée est de présenter une étude de cas générique afin de mettre davantage en avant les méthodes, et leur reproductibilité, que le résultat de la recherche. Un tel choix permet également de déceler les comportements spécifiques sur Bitcoin d'un individu aux idées politiques bien précises, mais ne sous-entend à aucun moment que cette cryptomonnaie sert d'abord au financement de certains projets ou courants politiques.

Une recherche de cette adresse Bitcoin sur un explorateur de blockchain permet de voir qu'une demi-douzaine de transactions ont été effectuées vers cette adresse, pour un total de plus de 30 000 euros (au 18 avril 2022), et qu'aucun envoi n'a été effectué depuis. Cette dernière donnée permet de comprendre que les bitcoins reçus n'ont pas été retirés, et donc pas échangés. L'objectif est ici de sélectionner l'une de ces adresses d'expédition, appartenant à l'une ou l'un des donateurs, et d'essayer de récupérer des informations sur des transactions précédentes, afin de voir s'il a déjà pu avoir recours au bitcoin pour des dons similaires. Ainsi, l'un d'eux, ici le « donateur », a envoyé 0,0008 bitcoin (environ 30 euros, au 19 avril 2022) le 19 juin 2021, à 16 h 46. L'identifiant unique de la transaction est

Hérodote, n° 186, La Découverte, 3e trimestre 2022.

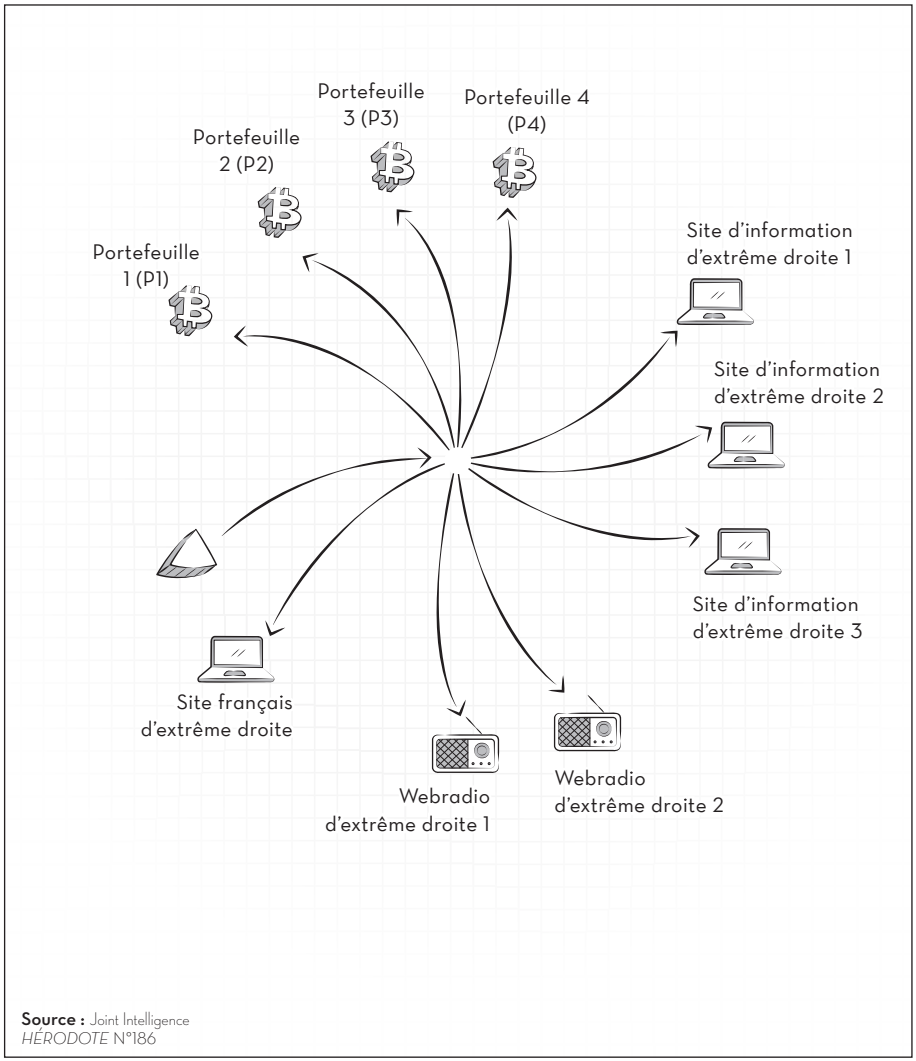
également visible, ainsi que ceux de trois adresses, une adresse d'émission et deux adresses de réception. La présence de deux adresses de réception est très courante dans des transactions de bitcoins, et comprendre la logique derrière ces dernières est une étape incontournable pour pouvoir lire ces échanges.

En effet, lors de l'envoi de bitcoins, c'est la totalité des unités stockées sur l'adresse d'émission qui est mobilisée dans la transaction. Ensuite, une fois la transaction validée, le montant prévu pour le don est envoyé vers l'adresse du destinataire (ici le site d'extrême droite) et le reste de la somme, le « change », est renvoyé à l'émetteur (ici le donateur) sur une autre adresse, activée pour l'occasion au sein de son portefeuille numérique. Ainsi, la transaction étudiée ici implique une adresse d'émission, qui envoie la totalité des bitcoins qu'elle contient, soit 0,01 BTC, au sein de la transaction. Une partie de cette somme, 0,0008 BTC, est envoyée vers l'adresse du site d'extrême droite et le reste, 0,0092 BTC, est envoyé vers une adresse de change appartenant au donateur. Cette logique s'applique à la plupart des transactions en bitcoins : il faut alors bien comprendre que, parmi les deux adresses de réception, l'une d'elles appartient également à l'expéditeur. Dans certains cas, l'adresse de change est la même que l'adresse d'émission, ce qui rend la lecture des échanges plus simple. En comprenant comment fonctionne cette transaction, il va alors être possible de remonter les autres transactions du donateur, puisque son adresse d'émission du don était également l'adresse de change d'une transaction précédente.

Afin de simplifier à la fois la récupération de données de transaction, et la visualisation des différents paiements réalisés par le donateur, le logiciel Maltego est ici utilisé. Maltego permet d'interroger la base de données de l'explorateur de blockchain Blockchain.com, et de produire des graphes en croisant les données récupérées. Et en différenciant les adresses de paiement des adresses de change du donateur, il est possible de créer un premier graphe de ses transactions.

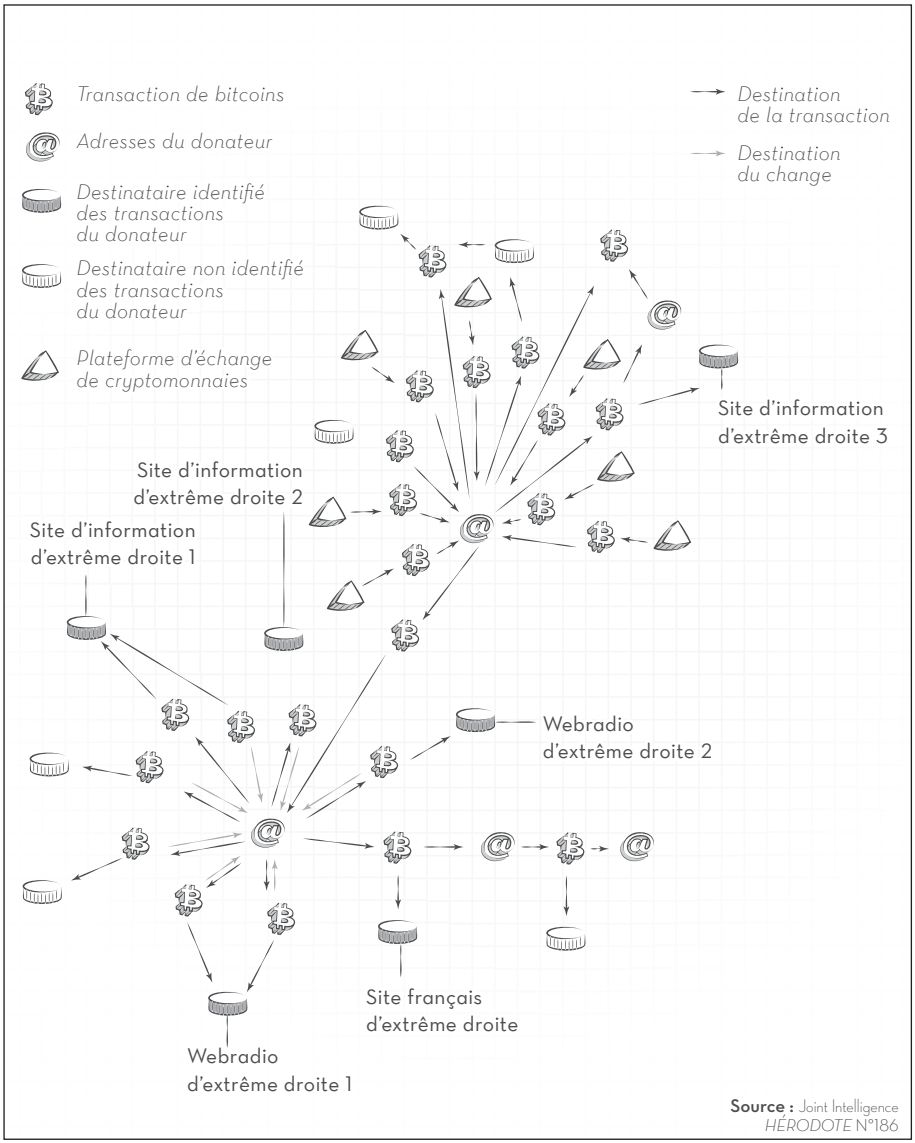
Apparaissent alors les adresses appartenant au donateur, dont certaines reçoivent pendant un temps le change des transactions effectuées. Il apparaît également que le donateur utilise principalement une seule de ses adresses pour recevoir des bitcoins sur son portefeuille, depuis ce qui semble être des plateformes d'échange. Ces services sont facilement visibles sur ces analyses, car ils engendrent des transactions contenant une ou plusieurs adresses émettrices qui envoient d'importants montants en bitcoins, vers plusieurs dizaines, voire centaines, d'adresses de destination. Afin de gérer plus rapidement de grandes quantités d'envois de bitcoins demandés par leurs clients, les plateformes les rassemblent au sein d'une seule transaction. Pour plus de lisibilité, sur le graphe 1, les adresses des plateformes sont représentées avec un figuré spécifique et seules les adresses de réception du donateur figurent. Pour la même raison, les dates et montants n'ont pas été affichés. Ainsi, en récoltant les données de

GRAPHIQUE 1. – SCHÉMATISATION DES TRANSACTIONS EN BITCOINS DU DONATEUR



Source : Joint Intelligence
HÉRODOTE N°186

GRAPHIQUE 2. – LES TRANSACTIONS DU DONATEUR



transactions liées à une adresse Bitcoin, il a été possible de produire une cartographie de certains de ses paiements.

Que peuvent nous apprendre les données de transactions ?

Il convient alors de s'intéresser aux autres adresses recevant des transactions émanant du donateur. Afin de récupérer des informations sur les adresses qui apparaissent, il est possible de les rentrer individuellement dans des explorateurs de blockchain pouvant donner des informations supplémentaires, à l'instar du portefeuille numérique ou de la plateforme auquel elle appartient. L'adresse peut également être rentrée dans un moteur de recherche classique afin de découvrir si elle n'apparaît pas sur certaines pages de sites Internet. Dans ce cas précis, il n'est pas possible d'obtenir le nom des plateformes d'échange. Mais plusieurs des adresses ayant reçu des transactions du donateur apparaissent sur des sites anglophones d'extrême droite, sur des pages appelant aux dons. En plus du site français figurent deux webradios et trois sites d'information centrés sur les dangers de l'immigration et de l'homosexualité pour les sociétés occidentales, soutenant un retour des nationalismes forts ou encore l'invasion russe en Ukraine (voir graphes 1 et 2). Nous pouvons désormais simplifier la visualisation de ces différentes transactions (graphe 2).

Il n'est pas possible de connaître l'identité réelle du donateur aux idées politiques très identifiées, et ce n'est pas l'objectif de la démarche. Ce qui est intéressant avec cette méthode de visualisation, c'est qu'elle permet d'observer une circulation de flux de cryptomonnaies entre des acteurs aux idées politiques cohérentes.

Cette analyse a également permis de faire ressortir, au sein de ces transactions, la place centrale des plateformes d'échange qui permettent au donateur d'alimenter son ou ses portefeuilles en bitcoins. Le recours à ces plateformes fragilise le degré d'anonymat originellement proposé par Bitcoin. En effet, la plupart de ces services sont assujettis à la législation du territoire sur lequel ils sont enregistrés ou autorisés à opérer, et doivent le plus souvent appliquer des politiques dites KYC (pour « *know your customer* »). Afin d'ouvrir un compte sur ces plateformes pour acheter ou échanger des bitcoins et d'autres cryptomonnaies, l'utilisateur doit prouver son identité. Ainsi, certains services de police et de sécurité travaillent de pair avec ces plateformes, en leur demandant de leur transmettre l'identité réelle derrière une transaction jugée illégale ou d'intérêt. Désormais, le terme de « pseudonymat » est souvent préféré à celui d'anonymat en ce qui concerne Bitcoin. Ainsi, le principe de transparence de l'infrastructure, soutenant une décentralisation des pouvoirs, couplé à des phénomènes de centralisation au sein du réseau avec l'apparition des

plateformes d'échange, a commencé à mettre à mal l'un des principes fondateurs de Bitcoin. En plus de fragiliser l'anonymat supposément apporté par Bitcoin, le recours aux plateformes présente d'autres risques pour le consommateur : il n'est pas vraiment propriétaire des cryptomonnaies associées à ses transactions, et peut voir ses fonds disparaître en cas de fermeture du service ou d'un piratage. En 2014, 200 millions de dollars de bitcoins ont ainsi été dérobés de la plateforme Mt. Gox par un pirate informatique. Cet acte fut le premier d'une liste qui s'allonge toujours aujourd'hui. Ainsi, les plateformes, si elles participent à la sécurisation et la stabilisation des réseaux de cryptomonnaies du point de vue des régulateurs et forces de l'ordre, participent également, dans une certaine mesure, à une fragilisation des libertés et de la sécurité financière des utilisateurs. Et si ces données en accès libre et le traçage des transactions en bitcoins facilitent aujourd'hui une surveillance et une régulation accrues de ce réseau, elles permettent aussi d'en étudier le fonctionnement. Cette analyse permet à la fois de visualiser clairement les logiques de fonctionnement de Bitcoin en tant que réseau d'échange, en plus de permettre d'éclairer sur les intentions de certains utilisateurs.

Conclusion

Bitcoin est une infrastructure complexe qui, bien que numérique, dispose d'un fort ancrage spatial et d'un important potentiel de contournement et de restructuration de réseaux de pouvoir préexistants. En ce sens, Bitcoin peut être appréhendé et analysé comme un objet géopolitique à part entière. Mais son architecture particulière et les multiples dimensions dans lesquelles il s'inscrit nécessitent une vision globale de ce qu'est Bitcoin, ce que permet l'approche par l'infrastructure et l'analyse de ses différentes entités et couches. Ainsi, il devient plus aisé d'analyser les différentes circulations et concentrations des pouvoirs au sein du réseau et d'observer les acteurs qui disposent d'une autorité supérieure à d'autres (développeurs, plateformes d'échange). Cette approche devient même opératoire dès lors qu'elle permet, *via* la récolte et le traitement de certaines données numériques, de naviguer au sein de ces différentes couches du réseau et d'y observer des dynamiques spécifiques. Malgré le caractère expérimental de l'étude de cas de cet article, cet exercice de visualisation de flux de cryptomonnaies a permis de clairement faire apparaître des logiques cohérentes dans le comportement d'acteurs. Les possibilités d'applications de ce type d'approche pour les sciences sociales semblent alors prometteuses**.**

Ces recherches deviennent de plus en plus nécessaires tant Bitcoin prend une importance croissante au sein de nos sociétés et de leurs enjeux, avec la multiplication des usages et usagers du réseau et les évolutions de ce dernier. La perception

de Bitcoin comme espace d'enjeux et objet géopolitique ne cesse de croître. En avril 2022, alors que l'Union européenne consolide son projet de loi pour un encadrement plus strict de l'usage des cryptomonnaies[8], le bitcoin a pris un cours légal en République centrafricaine (RCA)[9]. Le gouvernement centrafricain s'offre ainsi une alternative au franc CFA, dont la valeur est garantie par la France, l'ancien colonisateur dont la RCA souhaite s'émanciper, notamment en consolidant ses relations avec la Russie.

Bibliographie

CATTARUZZA A. (2019), *Géopolitique des données numériques*, Paris, Le Cavalier Bleu.

DE FILIPPI P. et LOVELUCK B. (2016), « The invisible politics of bitcoin : governance crisis of a decentralised infrastructure », *Internet Policy Review*, vol. 5, n° 3.

DESFORGES A. (2014), « Les représentations du cyberespace : un outil géopolitique », *Hérodote*, vol. 152-153, n° 1, p. 67-81.

DOUZET F. (2014), « La géopolitique pour comprendre le cyberespace », *Hérodote*, vol. 152-153, n° 1, p. 3-21.

ESTECAHANDY H. et LIMONIER K (2021), « Cryptocurrencies and processing power in Russia : a new strategic territory in eastern Siberia ? », *Journal of Cyber Policy*, vol. 6, n° 1, p. 68-80.

MAKAROV I. et SCHOAR A. (2021), « Blockchain analysis of the bitcoin market », National Bureau of Economic Research, octobre.

MAURER T. B., NELMS T. C. et SWARTZ L. (2013), « "When perhaps the real problem is money itself !" : the practical materiality of Bitcoin », *Social Semiotics*, vol. 23, n° 2, p. 261-277.

MUSIANI F. (2018), « L'invisible qui façonne. Études d'infrastructure et gouvernance d'Internet », *Tracés*, n° 35, p. 161-176.

MUSIANI F., MALLARD A. et MEADEL C. (2018), « Governing what wasn't meant to be governed. A controversy-based approach to the study of Bitcoin governance », *in* CAMPBELL-VERDUYN M. (dir.), *Bitcoin and Beyond. Cryptocurrencies, Blockchains and Global Governance*, Londres/New York, Routledge/Taylor & Francis Group.

NAKAMOTO S. (2008), « Bitcoin : a peer-to-peer electronic cash system », bitcoin.orghttps://bitcoin.org/en/bitcoin-paper

ROMITI M., JUDMAYER A., ZAMYATIN A. et HASLHOFER B. (2019), « A deep dive into bitcoin mining pools : an empirical analysis of mining shares », Boston, WEIS 2019, 3-4 juin.

8. « Les dangers des crypto-monnaies et les avantages de la législation européenne », Site du Parlement européen, 1er avril 2022. <https://www.europarl.europa.eu/news/fr/headlines/economy/20220324STO26154/les-dangers-des-crypto-monnaies-et-les-avantages-de-la-legislation-europeenne>.

9. « La Centrafrique adopte le bitcoin comme monnaie officielle », *La Croix*, 27 avril 2022.

ROSIÈRE S. (2001), « Géographie politique, géopolitique et géostratégie : distinctions opératoires », *L'Information géographique*, vol. 1, n° 65, p. 33-42.
STAR S. L. (1999), « The ethnography of infrastructure », *American Behavioral Scientist*, vol. 43, n° 3.
STAR S. L. et RUHLEDER K. (1996), « Steps toward an ecology of infrastructure : design and access for large information spaces », *Information Systems Research*, vol. 7, n° 1, p. 25.
VELASCO P. R. (2016), « Sketching bitcoin : empirical research of digital affordances », *in* KUBITSCHKO S. et KAUN A. (dir.), *Innovative Methods in Media and Communication Research*, Cham, Springer International Publishing, p. 99-122.
VENTRE D. (2012), « Le cyberespace : définitions, représentations », *Revue Défense Nationale*, p. 33-38.