Nigma REPORT

Are Cryptocurrencies an Efficient Way to Circumvent Sanctions?

September 2019

Table of Contents

SUMMARY

A wide range of circumvention strategies are being used in response to international sanctions against certain states, political actors or criminal and terrorist groups in a game of cats and mice. Among these, the use of cryptocurrencies has been pointed out or, on the contrary, nuanced. Can we reasonably suspect that Venezuela, Russia, Iran or even individuals or non-state actors such as Hamas or the Islamic State will develop impermeability to sanctions that affect them through this innovative technology?

To date, known or suspected attempts have not yielded convincing results, or only to a negligible extent. Some of them have more to do with an announcement effect than with a serious experiment. But let's be clear: neither the methods of financing illegitimate activities, nor technological innovation in the cryptocurrency sector are static, they are constantly evolving.

STATE-BACKED CRYPTOCURRENCIES

Venezuela and the Petro

Among these circumvention experiments, **Venezuela** has been the subject of satirical comments following the introduction of Petro, a national cryptocurrency supposedly supported by the country's oil reserves. Apart from the government's habits of manipulating exchange rates, which taint the credibility of this new virtual currency, it is actually neither technically functional nor used by the population. It is mainly a communication stunt that cannot hide the regime's economic disaster. Representatives of President Maduro admitted in November 2018 that the launch of Petro was intended to combat the "financial and economic blockade" operated by the United States by freeing itself from the international banking system.

Iran and the PayMon

Further east, **Iran** is also in the process of creating its own national cryptocurrency, openly declaring that this is an attempt to circumvent US sanctions on the country. The digital rial, or PayMon, backed by gold, would first be used for local real-estate transactions before expanding to the whole economy, and finally facilitate international transactions outside the SWIFT system. However, its launch has been announced since January 2019 and no details have emerged since then. The four banks and two private companies behind the project

have not clarified how it would work, excepted that it would be based on the Stellar open-source network. Such government-controlled virtual currencies indeed have the advantage of being based on softwares that are freely accessible on the Internet and impermeable to censorship by third parties, unlike transactions carried out on the international banking system, which can be blocked and subject to an asset freeze.

Russia and the CryptoRuble

Similarly, the imposition of new sanctions on **Russia** in August 2018 led Russian MP Vladimir Gutenev to threaten to allow Russian companies to accept payments in cryptocurrencies. He added that Russia should now consider measures to counter the effect of sanctions: "I'm sure other countries like China and India would be interested, too. In a boxing match, it's hard to fight properly if the rules are being broken and the referee does nothing to stop that." Gutenev then suggested creating a digital rouble backed by gold. This idea has been under consideration since 2017 with an announcement by President Vladimir Putin himself, but has not been implemented yet. According to NIGMA's information, representatives of the Russian-Syrian bilateral trade are discreetly trying to use cryptocurrencies to carry out commercial transactions between the two countries to the tune of several millions of dollars.

The US answer to these projects

These threats of circumvention led the United States to issue a presidential decree in March 2018 and a draft law codifying the decree in September. A statement on the US Treasury Department website warns that "any US citizen who uses the new Venezuelan digital currency is exposed to the risk of sanctions", as the purchase of Petro "can be considered as an extension of credit to the local government". In March 2019, Bill 1025 was introduced in the Senate to expand the ban on the Petro. Similarly, the US Treasury has clarified what obligations are imposed on virtual currency businesses with regards to sanctions against Iran. This demonstration of firmness indicates that it believes that the implementation of new sanctions will inevitably lead the Iranian regime to continue on its efforts to circumvent them).

Yet, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) noted that the Iran's circumvention of sanctions through virtual currencies is considered to be more of a potential concern in terms of laying the groundwork for the institution of a system able to make sanctions obsolete, than an actual immediate challenge to US interests. "Even if recent indictments show that Russia has used Bitcoin to avoid any external voting when purchasing equipment for political interference, it would be dangerous to generalize the use of a virtual currency to circumvent sanctions in general", the FinCEN added in its advisory. If

Iran were seeking to act in secret here, they would not have announced their intentions. On the contrary, they want their cryptocurrency projects to be public, FinCEN further elaborated. It also warned that if Iran were to launch a digital rial, the same sanctions that apply to the Iranian rial would also apply to its virtual version. Cryptocurrency trading platforms under US jurisdiction, and those abroad connected to them, would then not be able to accept the new digital rial, whose value would then be weakened, with the result of pushing away foreign investors.

Sanctions against Iranian cryptocurrency users are already being imposed as these users no longer have access to global digital currency trading platforms. As a collateral effect of sanctions targeting the government, these also prevent Iranians who wish to carry out legitimate transfers of cryptocurrencies for their families, for instance. Centralized platforms like Coinbase automatically reject transactions that are directly or indirectly related to prohibited bitcoins. The criminal activities of a few Iranians thus harm all those who unawarely transfer the "tainted" bitcoins, from transaction to transaction. American authorities suggest that individuals whose cryptoassets are derived from transactions that were previously flagged should notify the authorities of their situation. But how could ordinary individuals know if their Bitcoins are sanctioned if they do not have the necessary technical analysis skills and tools to conduct their own Bitcoin compliance investigation? US sanctions are hampering the development of a community of young Iranians seeking to free themselves from government yoke and economic crisis through technological innovation. The volatility of Bitcoin is negligible when compared to the hyperinflation of the Iranian currency.

Mining and Cryptocurrency Money-Laundering via OTC or P2P Networks

North Korean Mining and Hacks

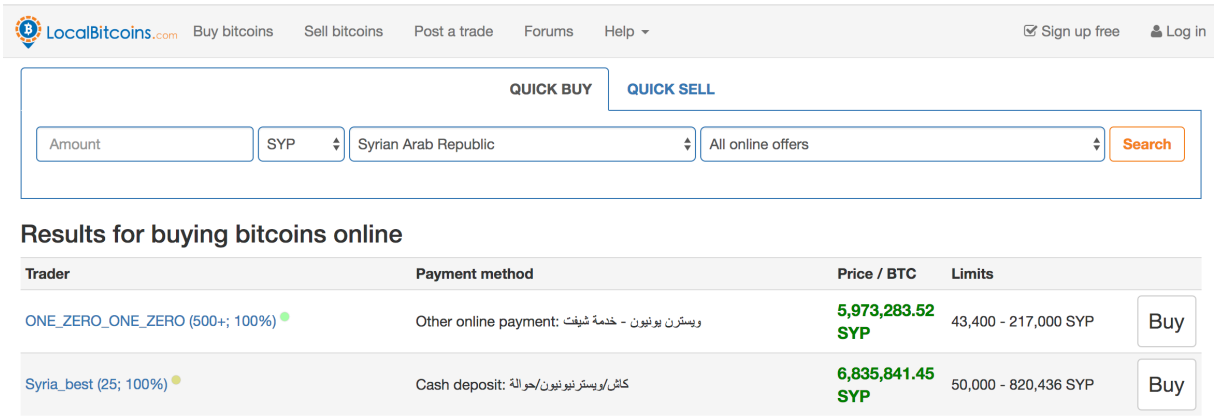
Other methods may be used to mitigate the impact of sanctions on Iranian liquidity. The example in this regard could be North Korea, another country heavily sanctioned by the international community, which has used mining and then cryptocurrency laundering to obtain supplies in dollars. By mining cryptocurrencies, i.e. by using computing power to validate transactions on a network of digital currencies such as Bitcoin in exchange for bitcoin fractions, North Korea or Iran could generate new and therefore non-suspect virtual assets that could be exchanged for real currencies. These real currencies, dollars or other, would then be laundered in bank accounts in countries not sanctioned by traditional money laundering methods. North Korea is also thought to be behind the hack of several Asian cryptocurrency exchange platforms for an amount exceeding 571 million dollars, according

to the US Treasury. In September 2019, the American Office of Foreign Assets Control added three cybercriminal groups responsible for cryptocurrency thefts on its sanctions list. After such hacks, North Korean actors are also believed to be laundering the funds through fiat and virtual transaction schemes. The disadvantage of this method is that it is highly unlikely that sanctioned and cash-strapped countries will be able to convert their virtual currencies for real ones. The conversion should take place on trading platforms which, for the most part, are prohibited in the sanctioned countries, or on local cryptocurrency trading platforms between private individuals, which are poorly frequented and have low liquidity.

The North Korean mining adventure has come to a halt and Iran too does not seem to be able to generate enough income from mining at the moment. Finally, any activity in cryptocurrency that is suspected of being linked to such sanctioned countries, individuals, or political parties, is likely to be identified by the competent authorities and hindered or even subject to countermeasures. This was the case in November 2018 when two Iranians responsible for a cyber attack, Ali Khorashadizadeh and Mohammad Ghorbaniyan, had their portfolios of bitcoins unmasked by the OFAC, the financial control body under the US Treasury, and placed on their sanctions list. In August 2019, the OFAC also added three Chinese drug smugglers and their Bitcoin and Litecoin addresses on their sanctions list.

Accessing Laundered Funds in Complex Environments

In countries like Lebanon or Syria, the main global cryptocurrency exchange platforms (Coinbase, Binance, Kraken...) are inaccessible, and local prospects for exchange between individuals remain extremely limited. An over-the-counter (OTC) trading platform like LocalBitcoins could help find buyers and sellers locally to arrange for face-to-face transactions, but users are scarce. There are only four individuals in Lebanon willing to buy or sell bitcoins on LocalBitcoins and they are limited to a maximum of a few millions Lebanese pounds (the equivalent of a few thousand dollars). In Syria, only two individuals offer to sell bitcoin up to 820,000 Syrian pounds — about 1600 dollars; no one wants to buy any. The platform also offers to buy or sell bitcoin in dollars to individuals around the world



with far larger volumes, but the proposed payment methods — interbank transfer, Western Union, PayPal … — are not sanctions-proof. In such countries, individuals subject to international sanctions would therefore have difficulty accessing significant quantities of cryptocurrencies through this method. However, one could imagine that an individual who owns large quantities of cryptocurrencies acquired abroad could negotiate an OTC transaction for cash or through a legitimate bank transfer. The hypothesis of buying cryptocurrencies via networks of partners abroad, although complex, could lead to the creation of strategies to circumvent sanctions or money laundering, in countries where some actors are considered as terrorists. The main issue of exchanging cryptocurrencies against cash to fund activities would then remain.

As for authoritarian states, they probably have no interest in promoting the use of payment networks that they cannot control.

Cryptocurrency AML-CTF and Sanctions

The Limited Use of Cryptocurrency by Terror Organizations

Terrorist organizations have been found to be barely using cryptocurrencies to fund their activities though. After a few failed attempts to collect crypto donations, more sophisticated methods have also not proved efficient, though they had a massive impact in the mainstream media. In January 2019, the Palestinian Hamas Ezzedeen Al Qassam Brigades attempted to raise cryptocurrency via a Bitcoin address on its Telegram channel, but only received about 2500 dollars in cryptocurrency that mainly came from the Gaza Strip. In spite of a successful communication operation, the funds were tracked easily to the Coinbase exchange platform and frozen. In April 2019, the Brigades shifted tactics and managed to organize a crypto fundraising campaign generating a new Bitcoin wallet for each donor, thus making tracking of transactions harder. The network can however still be uncovered by sending a fraction of bitcoin using the new system and analyzing where it is sent on the blockchain — an infrastructure for storage and transparent transmission of encrypted data and value such as Bitcoin, thus identifying addresses involved. Moreover, research firm Elliptic estimated the four months campaign raised around 7400 dollars only. All in all, a 2019 report by the RAND Corporation on the Terrorist Use of Cryptocurrencies concluded that the main cryptocurrencies like Bitcoin are not satisfying terrorist technical and operational needs and challenges due to their traceability and regulation, while more anonymous ones are not widespread enough. David Carlisle, a former agent of the U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence, had also argued

in a 2017 report by the British think tank RUSI that terrorism use of cryptocurrencies was not a serious threat.

Blockchain Forensics

Indeed, due to the fundamental nature of the main decentralized blockchain-based digital currencies such as Bitcoin or Ethereum, these are not anonymous as claimed by the mainstream media but pseudonymous and easily traceable for anyone using advanced blockchain forensics tools, such as the American Chainalysis or the French-Lebanese e-NIGMA. Such transaction monitoring softwares allow for a clear visualisation of complex or unstructured data on Bitcoin wallets, the real-life entities behind them, display a risk-score, analyze suspicious transaction behaviors and patterns, display custom alerts for new activities by monitored wallets and so on. Some of them even integrate data on wallets from the dark and clear web using advanced open-source intelligence techniques and scraping tools, including email or IP addresses. Law enforcement agencies, virtual assets service providers and banks can thus detect and prevent illicit cryptocurrency activities.

Since the main cryptocurrency exchange platforms have a know-your-customer (KYC) process when onboarding clients and perform due diligence on certain clients, it is possible for law enforcement agencies to subpoena these platforms to uncover personal information on users suspected of illicit activities. Platforms can also freeze assets that are flagged as illicit. That is why the Financial Action Task Force and some national financial regulators have taken steps to expand compliance of states and cryptocurrency businesses with strict anti money-laundering & terrorism financing (AML-CTF) standards. As for transactions in peer-to-peer networks, these are less widespread and showcase low volumes: they can be considered as a niche for limited potential illicit activities but may still be investigated by law enforcement agencies using analytics tools.

For all these reasons, traditional methods of circumventing sanctions, such as transit of cash and persons through allied countries, use of the euro, binational joint ventures, opening bank accounts abroad, sophisticated barter systems (Special Purpose Vehicle), remain predominant.

Building an Alternative to the SWIFT System

Private Blockchains for Local or Intergovernmental Transfers

The real threat could in fact arise in the long term. Since the use of existing cryptocurrencies is unlikely to limit the effects of sanctions, the most successful experiments in the field of blockchain technology are not those that rely on a public network. Unlike open Bitcoin-type blockchains, there are private blockchains that have been developed for commercial uses such as Hyperledger Fabric, the result of the work of a consortium of companies led by the NGO Linux Foundation supporting open-source technology projects in San Francisco.

By building a functional value transfer system that is hermetically sealed from the US dollar and Western sanctions, some countries would find an alternative to the Western SWIFT payment system from which they are squeezed out or which they wish to bypass. In May 2018, the Chairman of the Economic Affairs Committee of the Iranian Parliament Mohammad Reza Pour Ebrahimi announced that he had discussed a project to find an alternative to the SWIFT with his Russian counterpart, which was already based on concrete technological advances. He added that the Iranian Central Bank would issue proposals for a state cryptocurrency to free national financial institutions "from the dollar as well as the SWIFT system".

It was precisely on the basis of the aforementioned Hyperledger private blockchain that the Iranian Central Bank announced in August that it planned to launch a national cryptocurrency. Sberbank, Russia's leading bank, sanctioned by the United States, conducted transactions in May for $12 million using the same technology. As this platform is built on an open source program, the Linux Foundation cannot oppose Iranian projects. It would be counterproductive to ban initiatives such as Hyperledger, which contribute to the modernisation of banking systems worldwide through transparency and therefore to the best auditability possible under the blockchain.

Russia, China and… the EU

On the Russian side, the Central Bank has already set up its Financial Message Transfer System (SPFS), an alternative to SWIFT initiated in 2014 following American threats to exclude Russia from SWIFT. The first SPFS transaction took place in December 2017 and Moscow is reportedly in discussion with China, Turkey, Iran and some Eastern European countries to further integrate it. The idea of an international payment system that would bypass US sanctions on Iran has even been discussed between Russia and China on the one hand, and France, Germany and the United Kingdom led by the European Union on the other. The French agency for the financing and development of companies, Bpifrance, which in 2017 was studying various channels for financing French companies for exports to Iran and for the repatriation of their capital to France, has however abandoned this overly cumbersome project.

It is clear that the advent of a consortium of dissident states basing their international transactions on a private blockchain alternative to the SWIFT will not see the light before several years or even decades. But some states such as China and Russia are directing their efforts towards long-term goals. China has invested more than three billion dollars in Blockchain projects in 2018, partly in cooperation with Russia. A $100 million investment pool for the sector was created in 2017 by companies from both countries.

CONCLUSION

Cryptocurrencies have often been depicted as a key vector for criminals and terrorist organizations to fund their activities in the face of government oversight or sanctions, be it through fundraising campaigns on Telegram, darknet marketplaces, or money-laundering schemes. One of the major reasons for this is that Bitcoin is widely believed to be an innovation that allows anonymous transactions. A myth that has the dangerous side-effect of belittling the real channels for crime and terror financing: traditional ones. Attempts by State and non-State actors to avoid international sanctions against them through the use of cryptocurrencies have all had poor results, except for pure communication ones. They can thus be viewed as internal and/or political strategies to give the impression that a government or a militia has adopted a strong and tech-savvy attitude against Western sanctions.

However, it is not because cryptocurrency financial crime and terrorism financing is marginal — about one or two percent of Bitcoin transactions are estimated to be illicit — that it shouldn't be firmly addressed. Law enforcement agencies have a duty to fight financial crime in all its forms, and regulators to protect consumers against scams. Emerging regulation at the international level with the Financial Action Task Force, at the European level with the 5th EU Anti-Money-Laundering Directive and within national jurisdictions tends to compel cryptocurrency businesses to implement strong AML-CTF processes and tools. The new standards will make it even harder for sanctioned entities to circumvent sanctions by requiring all virtual assets service providers to:

- be registered and/or licensed by the national regulator;
- collect KYC data on their customers and share it with beneficiary VASPs for any transaction over 1000 dollars or euros;
- conduct due diligence when onboarding special clients or for large transactions;
- set AML-CTF tools to monitor suspicious wallets and transactions;

- issue suspicious activity reports to be shared with the national regulator or used for audits or legal procedures;
- freeze assets and uncover personal data associated with illicit and sanctioned activities and actors; etc.

In the end, the most serious and large-scale perspectives in terms of sanctions circumvention could be found, not in decentralized cryptocurrencies, but rather in private blockchain-based transfer infrastructures at the government or intergovernmental level. Development and full implementation for these faces major technical challenges and costs, notwithstanding political constraints.

REFERENCES

Government and International Organisations

www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

https://www.whitehouse.gov/presidential-actions/executive-order-taking-additional-steps-address-situation-venezuela/

https://legiscan.com/US/text/SB3486/2017

https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#551

https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190821.aspx

https://home.treasury.gov/index.php/news/press-releases/sm774

https://www.fincen.gov/news/news-releases/fincen-issues-advisory-iranian-regimes-illicit-and-malign-activities-and

https://www.congress.gov/bill/116th-congress/senate-bill/1025

www.minci.gob.ve/anc-aprobo-ley-de-criptoactivos/

Think Tanks and Private Research

https://rusi.org/commentary/cryptocurrencies-and-terrorist-financing-risk-hold-panic

https://www.rand.org/pubs/research_reports/RR3026.html

https://www.kaggle.com/ellipticco/elliptic-data-set

http://www.fletcherforum.org/the-rostrum/2018/10/1/sanctions-vs-strategy-how-us-sanctions-are-fostering-innovative-strategies-for-resiliency-in-russia

https://www.linkedin.com/posts/loryfeuvrier_m%C3%A9moire-master-ii-droit-bancaire-et-financier-activity-6577870124093587456-6QOy/

https://www.recordedfuture.com/north-korea-internet-behavior/

https://www.virtualcurrencyreport.com/2018/10/fincen-advisory-emphasizes-importance-of-u-s-iran-sanctions-and-aml-cft-compliance-for-virtual-currency-businesses/

Businesses

https://www.sberbank.ru/en/press_center/all/article?newsID=bfbc4479-6a04-46f2-9d52-0b81093590aa&blockID=1539&regionID=77&lang=en

https://localbitcoins.com

Media and News Agencies

https://www.rt.com/business/406960-russia-issue-blockchain-cryptoruble-putin/

https://www.bloomberg.com/news/articles/2018-11-28/u-s-exposes-bitcoin-users-addresses-in-iran-cyber-sanctions

https://www.interfax.ru/business/612729

https://www.la-croix.com/Monde/bourse-dechange-commercer-librement-entre-lEurope-lIran-2018-09-25-1200971439

https://www.lorientlejour.com/article/1147332/le-bitcoin-va-t-il-vraiment-mourir-.html

https://en.mehrnews.com/news/147584/1st-Iranian-cryptocurrency-under-CBI-permission-to-be-unveiled

https://www.latribune.fr/actualites/economie/international/20120403trib000691766/comment-l-iran-contourne-les-sanctions-internationales.html

https://www.ccn.com/can-china-pursue-blockchain-innovation-amid-cryptocurrency-ban/

https://www.finextra.com/pressarticle/70566/china-and-russia-collaborate-on-cryptocurrency-fund-and-blockchain-projects

https://cryptonews.com/news/russia-politician-seeks-crypto-counter-to-us-sanctions-2523.htm

https://www.coindesk.com/iran-bitcoin-sanctions-wallets-ofac-crypto

https://bitcoinmagazine.com/articles/report-just-1-percent-bitcoin-transactions-involve-illicit-dark-web-activity

Les cryptomonnaies sont-elles un moyen pour contourner les sanctions imposées à des pays, des groupes politiques ou des individus ?

Aux sanctions internationales frappant certains Etats, acteurs politiques ou groupes criminels et terroristes, répondent dans un jeu du chat et de la souris tout un éventail de stratégies de contournement. Au nombre de celles-ci, l'utilisation des cryptomonnaies a pu être pointée du doigt ou au contraire nuancée. Peut-on raisonnablement imaginer que le Venezuela, la Russie, l'Iran ou même encore des individus ou groupes politiques comme le Hamas développent une imperméabilité aux sanctions qui les touchent grâce à cette innovation technologie ?

Jusqu'à maintenant, les tentatives connues ou suspectées n'ont pas donné lieu à des résultats probants, ou bien dans des proportions négligeables. Certaines relèvent d'ailleurs plus de l'effet d'annonce que d'une expérimentation sérieuse. Mais qu'à cela ne tienne : ni les méthodes de financement d'activités illégitimes ou considérées comme telles, ni par ailleurs l'innovation technologique dans le secteur des cryptomonnaies ne sont statiques.

Au titre de ces expériences, le Venezuela a fait l'objet de commentaires satiriques suite à la mise en place du Petro, une cryptomonnaie nationale soi-disant appuyée aux réserves de pétrole du pays. Outre les habitudes de manipulation des taux de change par le gouvernement qui entachent la crédibilité de cette nouvelle monnaie virtuelle, cette dernière n'est en réalité ni fonctionnelle sur le plan technique, ni utilisée par la population. Il s'agit principalement d'un coup de communication en dépit duquel le régime ne saurait masquer le désastre économique de son pays. Des représentants du Président Maduro ont admis le 21 novembre que le lancement du Petro devait permettre de combattre le "blocus financier et économique" opéré par les Etats-Unis en s'affranchissant du système bancaire international.

Plus à l'Est, l'Iran est également en cours de création de sa propre cryptomonnaie nationale, en déclarant ouvertement qu'il s'agit là d'une démarche visant à contourner les sanctions américaines sur le pays. Le rial digital, adossé à l'or, aurait pour but de faciliter les transactions internationales en marge du système SWIFT. De telles monnaies virtuelles gouvernementales ont en outre l'avantage d'être développées sur la base de logiciels et programmes informatiques librement accessibles sur internet et imperméables à la censure par des tiers, contrairement aux transactions réalisées sur le système bancaire international qui peuvent être bloquées et faire l'objet d'un gel des actifs.

De même, l'institution de nouvelles sanctions sur la Russie en aout dernier a conduit le député russe Vladimir Gutenev à menacer d'autoriser les entreprises russes à accepter des paiements en cryptomonnaies. Il avait alors ajouté que la Russie devait désormais considérer des mesures visant à contrer l'effet des sanctions: "je suis certain que d'autres pays comme la Chine et l'Inde seraient intéressés aussi. Dans un match de boxe, il est difficile de se battre dans le respect des règles quand ces dernières sont violées et quand l'arbitre n'intervient pas." Gutenev suggérait alors de créer une rouble digitale adossée à l'or. Selon nos informations, des représentants du commerce bilatéral russo-syrien cherchent discrètement à utiliser les cryptomonnaies pour effectuer des transactions commerciales entre les deux pays à hauteur de plusieurs millions de dollars.

Ces menaces de contournement ont conduit les Etats-Unis à publier un décret présidentiel en mars et une proposition de loi codifiant ce décret en septembre. Une déclaration sur le site du Département du Trésor américain avertit que "tout citoyen américain qui utiliserait la nouvelle monnaie digitale vénézuélienne s'expose au risque de sanctions", l'achat de Petro "pouvant être considéré comme une extension de crédit au gouvernement local". De même, le Trésor américain a explicité quelles obligations pèsent sur les intermédiaires d'échanges de cryptomonnaies au regard des sanctions contre l'Iran. Cette démonstration de fermeté s'explique par la prédiction qu'à la suite de l'imposition de nouvelles sanctions le 5 novembre 2018, les institutions financières iraniennes déploient de nouveaux efforts pour les contourner.

Pourtant, dans son communiqué du 11 octobre, le Financial Crimes Enforcement Network (FinCEN) du Département du Trésor note que le contournement des sanctions contre l'Iran par le biais des monnaies virtuelles est plus une préoccupation potentielle qu'un phénomène effectivement observé. "Même si de récents actes d'accusation montrent que la Russie a utilisé le bitcoin pour éviter tout scrutin extérieur lors de l'achat de matériel à finalité d'ingérence politique, il serait hasardeux de généraliser l'utilisation d'une monnaie virtuelle pour le contournement des sanctions en général". Si l'Iran cherchait ici à agir en secret, ils n'auraient pas annoncé leurs intentions. Ils souhaitent au contraire que leurs projets de crypto-monnaie soient publics. Le FinCEN prévient par ailleurs que si l'Iran lançait un rial digital, les mêmes sanctions qui s'appliquent au rial iranien toucheraient sa version virtuelle. Les plateformes d'échanges de cryptomonnaies sous juridiction américaine et celles à l'étranger qui leur sont connectées ne pourraient alors pas accepter le nouveau rial digital, dont la valeur serait alors affaiblie, et qui n'attirerait donc plus les investisseurs étrangers.

Les sanctions contre les utilisateurs iraniens de cryptomonnaies se feraient déjà sentir selon le media spécialisé CoinDesk, ceux-ci n'ayant plus accès aux plateformes d'échanges de

monnaies digitales. On voit ici les effets collatéraux des sanctions qui empêchent des Iraniens désireux de réaliser des transferts légitimes de cryptomonnaies pour leurs familles par exemple. Des plateformes comme Coinbase rejettent automatiquement les transactions liées de plus ou moins loin à des bitcoins interdits. Les activités criminelles de quelques Iraniens nuisent ainsi à tous ceux par qui passeront ensuite les bitcoins "salis", de transaction en transaction. Les autorités américaines suggèrent aux particuliers dont les cryptoactifs seraient issus de transactions interdites dans le passé à leur notifier leur situation. Mais comment de simples individus pourraient-ils savoir que leurs bitcoins sont potentiellement sanctionnés s'ils n'ont pas les compétences nécessaires en matière d'analyse de la blockchain pour faire leur propre enquête de *compliance* ? Les sanctions américaines entravent le développement d'une communauté de jeunes Iraniens cherchant à se libérer du joug gouvernemental grâce à l'innovation technologique. La volatilité du bitcoin leur est d'ailleurs négligeable par comparaison avec l'hyperinflation de la monnaie iranienne. C'est pourquoi les Iraniens ont tendance à s'intéresser à d'autres types de cryptomonnaies tels que Monero ou zCash qui font la part belle à la discrétion et demeurent intraçables.

En coulisses toutefois, il se pourrait que d'autres méthodes soient employées pour atténuer l'effet des sanctions sur les liquidités iraniennes. L'exemple en la matière pourrait être la Corée du Nord, autre pays lourdement sanctionné par la communauté internationale, qui aurait utilisé le minage puis le blanchiment de cryptomonnaies pour s'approvisionner en dollars. En minant des cryptomonnaies, c'est-à-dire en utilisant de la puissance de calcul informatique pour valider des transactions sur un réseau de monnaies digitales tel que Bitcoin en échange de fractions de bitcoins, la Corée du Nord ou l'Iran pourraient générer des actifs virtuels neufs et donc non suspects, échangeables contre des monnaies réelles. Ces monnaies réelles, dollars ou autres, seraient alors blanchies sur des comptes bancaires dans des pays non sanctionnés selon les méthodes traditionnelles du blanchiment d'argent. L'inconvénient de cette méthode réside dans la forte improbabilité que ces pays sanctionnés et en manque de liquidités puissent convertir leurs cryptomonnaies pour procéder à des transactions réelles. Cette conversion doit en effet avoir lieu sur des plateformes d'échanges qui, pour la plupart, sont interdites d'accès dans les pays sanctionnés, ou sur des plateformes locales d'échange de cryptomonnaies entre particuliers, trop peu fréquentées.

Ainsi en est-il au Liban et en Syrie, où les principales plateformes internationales d'échange de cryptomonnaies (Coinbase, Binance, Kraken…) sont inaccessibles et où les perspectives locales d'échange entre particulier restent extrêmement limitées. Sur le plus connu de ces derniers vecteurs, LocalBitcoins, seule une personne propose de vendre ou d'acheter des bitcoins mais dans la limite de quelques centaines de milliers de livres libanaises. En Syrie,

un seul individu également propose de vendre du bitcoin dans la limite de 217,000 livres syriennes — environ 420 dollars, aucun ne souhaite en acheter. Syriens comme Libanais pourraient toutefois via cette plateforme acheter ou vendre du bitcoin en dollars à des particuliers dans le monde entier, si les moyens de paiement proposés ne rendaient pas leurs transactions complexes du fait des sanctions: transfert interbancaire, Western Union, PayPal etc. Dans de tels pays, des individus faisant l'objet de sanctions internationales ne sauraient donc que difficilement accéder à des quantités significatives de cryptomonnaies par ce biais. On pourrait toutefois imaginer qu'un individu propriétaire d'une grande quantité de cryptomonnaies acquises à l'étranger puisse négocier une transaction de gré à gré — *over-the-counter* — contre du cash ou un virement bancaire légitime. L'hypothèse de l'achat de cryptomonnaies via des réseaux de partenaires à l'étranger, certes complexe, pourrait mener à la constitution de strategies de contournement de sanctions ou de blanchiment d'argent dans des pays comme le Liban ou la Syrie.

Quant aux États autoritaires, ils n'ont d'ailleurs probablement pas intérêt à favoriser l'utilisation de réseaux de paiement qu'ils ne peuvent pas contrôler.

En outre, l'aventure minière nord-coréenne a tourné court et l'Iran également ne semble pas être actuellement en mesure de produire suffisamment de revenus par le *mining*. Enfin, toute activité sur la blockchain qui serait suspectée d'être liée à de tels pays, individus ou partis politiques sanctionnés est susceptible d'être repérée par les services compétents et entravée, voire faire l'objet de contre-mesures. Ainsi en a-t-il été fin novembre quand deux Iraniens responsables d'une cyber-attaque, Ali Khorashadizadeh et Mohammad Ghorbaniyan, ont vu leurs portefeuilles de bitcoins démasqués par l'OFAC, organisme de contrôle financier dépendant du Trésor américain, et placés sur leur liste de sanctions. C'est en particulier grâce au recours à des technologies d'investigations blockchain telle que celle développée par la firme libanaise CSI que des mouvements de fonds suspects ou illicites — blanchiment d'argent, financement du terrorisme et de réseaux criminelles, fraude — peuvent être détectés et entravés.

Pour toutes ces raisons, les méthodes traditionnelles de contournement des sanctions — transit de cash et de personnes par des pays alliés, utilisation de l'euro, co-entreprises binationales, ouvertures de comptes bancaires à l'étranger, systèmes de troc sophistiqués (*Special Purpose Vehicle*) — restent donc prédominantes.

La véritable menace pourrait en fait s'inscrire dans le plus long terme. Puisque l'utilisation des cryptomonnaies existantes se révèle à peine susceptible de limiter les effets des sanctions, les expérimentations les plus probantes dans le domaine de la technologie blockchain — infrastructure de stockage et de transmission transparente et cryptographiée

de données — ne sont pas celles qui s'appuient sur un réseau public. Au contraire des blockchains ouvertes de type Bitcoin, il existe des blockchains privées qui ont été développées pour des usages commerciaux telles que Hyperledger Fabric, fruit du travail d'un consortium d'entreprises menées par l'ONG de soutien aux projets technologiques open-source Linux Foundation à San Francisco.

En construisant un système de transfert de valeur fonctionnel hermétique au dollar américain et aux sanctions occidentales, certains pays trouveraient une alternative au système de paiement occidental SWIFT dont ils sont évincés ou qu'ils souhaitent contourner. L'Iran et la Russie au moins seraient en discussions pour l'établissement d'une telle infrastructure dédiée au commerce bilatéral en cryptomonnaies. En mai 2018, le président de la Commission des affaires économiques au Parlement iranien Mohammad Reza Pour Ebrahimi a annoncé avoir discuté avec son homologue russe d'un tel projet, déjà appuyé sur des avancées concrètes sur le plan technologique. Il ajoutait alors que la Banque centrale iranienne allait émettre des propositions relatives a une cryptomonnaie d'Etat en vue de libérer les institutions financières nationales "du dollar comme du système SWIFT". Côté russe, la Banque centrale a déjà mis en place son Système pour le Transfert de Messages Financiers (SPFS), alternative au SWIFT initiée en 2014 suite aux menaces américaines d'exclure la Russie du SWIFT. La première transaction SPFS a eu lieu en décembre 2017 et Moscou serait en discussion avec la Chine, la Turquie, l'Iran et quelques pays d'Europe de l'Est pour en développer l'intégration. L'idée d'un système international de paiements qui contournerait les sanctions américaines sur l'Iran a même été discutée entre la Russie et la Chine d'une part, la France, l'Allemagne et le Royaume-Uni emmenés par l'Union européenne d'autre part. L'agence française de financement et de développement des entreprises Bpifrance, qui étudiait en 2017 divers canaux de financement d'entreprises françaises à l'export en Iran ainsi que pour le rapatriement en France de leurs capitaux, a toutefois pour sa part abandonné ses projets trop contraignants.

Il est certain que l'avènement d'un consortium d'Etats dissidents appuyant leurs transactions internationales sur une version blockchain privée alternative à SWIFT ne saurait voir le jour avant plusieurs années voire décennies. Mais de fait, certains Etats comme la Chine et la Russie jouent sur le temps long. Ce sont plus de trois milliards de dollars qui ont été investis par la Chine dans les projets blockchain en 2018, parfois en coopération avec la Russie. Un fonds commun d'investissement dans le secteur doté de l'équivalent de 100 millions de dollars a été créé en 2017 par des entreprises des deux pays.

C'est bien sur la base de la blockchain privée Hyperledger susmentionnée que la Banque centrale iranienne avait annoncé en août prévoir de lancer une cryptomonnaie nationale. La Sberbank, principale banque de Russie, sanctionnée par les Etats-Unis, a procédé en mai a

des transactions pour 12 millions de dollars en utilisant la même technologie. Cette plateforme étant construite sur un programme en accès libre de droits et gratuit, la Linux Foundation qui en est l'auteur ne saurait s'opposer aux projets iraniens. Il serait contre-productif d'interdire des initiatives telles que Hyperledger, qui concourent à la modernisation de systèmes bancaires dans le monde entier grâce à la transparence et donc à la meilleure auditabilité permise par la blockchain. Quant à la Banque centrale libanaise, l'infrastructure et la réalité de ses projets annoncés de version digitale de la livre libanaise demeurent trop floues pour pouvoir analyser ses intentions ou anticiper quels garde-fous pourraient entraver son utilisation a des fins criminelles. Son gouverneur, Riad Salame, a pourtant confirmé lors de la Conférence Euromoney Lebanon de juin 2019 que ses équipes travaillaient encore sur le projet.