Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

REGULATING VIRTUAL CURRENCIES

Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering

Virtual Currencies Working Group - June 2014

MINISTÈRE DES FINANCES
ET DES COMPTES PUBLICS

Background

In 2011–2012, Tracfin (the French Financial Intelligence Unit) chaired a working group on new means of payment. Among other topics, the group discussed the risks and threats associated with virtual currencies[1]. Since that time, virtual currencies have stayed in the headlines, as much for their legitimate use as their misuse[2]. There are an increasing number of ways to spend virtual currencies, the currencies themselves are proliferating, and national and international responses are on the rise.

With this in mind, and as an extension to work that began in 2011, Tracfin initiated a working group on virtual currencies in December 2013. The group included members from the Directorate General of the Treasury (DGT), the Directorate General of Customs and Excise (DGDDI), the Public Finances Directorate General (DGFiP), the Directorate General for Competition Policy, Consumer Affairs and Fraud Control (DGCCRF), the Directorate for Criminal Affairs and Pardons (DACG), the National Criminal Police Directorate (DCPJ), the Gendarmerie General Directorate (DGGN), the Autorité des Marchés Financiers (AMF), the Prudential Supervisory and Resolution Authority (ACPR), the Banque de France and representatives from the Ministry of Defence and Ministry of the Interior. The group produced an overview of the risks and threats associated with virtual currencies, and drew up a set of recommendations with an eye to lessening their impact. Since the virtual currency sector is growing by leaps and bounds, it is worth pointing out that the recommendations are based on an analysis of the situation as of June 2014.

Acknowledgements

Our thanks to French Banking Federation (FBF), which organised a working session on virtual currencies that brought together banking sector specialists. We would also like to thank Philippe Rodriguez, president of the association Bitcoin France; Gonzague Grandval, CEO of Paymium; Laurent Nizri, deputy director of Altéir Consulting and chair of the Means of Payment Commission of the Digital Economy Association (ACSEL); and Jean-Michel Cornu, scientific director of the Next Generation Internet Foundation (FING), all of whom agreed to be interviewed by the working group.

[1] Tracfin's Annual Report for 2011 lists the results of the group's work.

[2] The best example of this is the FBI's shutdown of the darknet website Silk Road on 2 October 2013. Silk Road specialised in the sale of illegal goods, particularly drugs, and accepted payment only in bitcoins.

Virtual currencies were designed as an alternative to legal tender, initially for use in virtual communities, and online gaming sites in particular. The number of such currencies grew as uses for them expanded and extended to include the real world. There are now a great many virtual currencies in circulation. They can be acquired either directly (through mining, bilateral transactions with other investors, from a firm selling virtual currencies, the purchase of options, etc.) or indirectly via a virtual currency exchange. They may also be borrowed.

The term "virtual currency" is traditionally defined as a unit of account stored on an electronic medium. It is created, not by a State or monetary union, but by a group of individuals or legal entities, and is used for multilateral exchanges of goods or services between the group's members. A virtual currency scheme may be "open" or "closed" (depending on whether or not it is convertible into a currency that is legal tender. The exchange rate may be fixed or variable. Open virtual currency schemes may have bidirectional or unidirectional flows (in the latter case, only a conversion from legal tender to virtual currency is possible).

Since a virtual currency does not represent a claim on the issuer and is not issued on receipt of funds within the meaning of the second Electronic Money Directive (2EMD), the term "electronic money" cannot be retained given the current state of the legislation. Nor are virtual currencies payment instruments as defined by Article L. 133-4 c) of the French Monetary and Financial Code. Nevertheless, they may fulfil an economic function on a private, contractual basis. Virtual currencies are not included in any of the categories of financial instruments defined in Article L. 211-1 of the Monetary and Financial Code.

Issue No. 10 of the Banque de France's online newsletter *Focus* (5 December 2013) warned users of virtual currencies about the risks they face. On 29 January 2014, the Prudential Supervisory and Resolution Authority (ACPR) issued its position concerning transactions involving bitcoins in France, and emphasised that the act of intermediation with respect to the purchase or sale of virtual currencies in exchange for a currency with legal tender is that of a financial intermediary who receives funds on a third party's behalf. On the other hand, there are persistent doubts in France as to the legal characterisation of virtual currencies.

The goal of this report is not to address the issue of the legal status of virtual currencies, which has been the focus of a number of working groups at both European and international levels. Rather, based on a finding from June 2014, and following a brief overview of the characteristics, uses and risks associated with virtual currencies, it proposes a series of recommendations. These are put forth with an eye to **encouraging the establishment of a framework to prevent and deter the use of virtual currencies for fraudulent purposes and money laundering**.

I – THREE ASPECTS OF VIRTUAL CURRENCIES THAT ARE SOURCES OF RISKS

Assessing the risks associated with virtual currencies must factor in how these currencies are issued, how they are used and in particular transparency of flows, issues of liquidity and their convertibility to legal tender. There are various types of virtual currencies, and they operate in different ways. However, they share a certain number of characteristics, three of which we would like to focus on, as they can be the source of risks:

- **The presence of unregulated participants**: examination of a sampling of virtual currencies shows that they are produced by a variety of stakeholders. These include natural persons, activists and private-sector companies. In some cases, a virtual currency was designed to meet the needs of individuals engaged in illegal activities. Issuance of a virtual currency is not covered by current banking and financial legislation. A virtual currency is not a payment instrument as defined by Article L. 133-4 c) of the French Monetary and Financial Code, nor is it electronic money, or one of the financial instruments defined in Article L. 211-1 of the Monetary and Financial Code. Thus, a virtual currency may be issued either by a community of "miners" (decentralised cryptocurrency) or by a single entity (centralised virtual currency). Given the lack of a legal status and a regulatory framework, virtual currencies provide no certainty with respect to either price or liquidity. With respect to volatility and liquidity risks, it

should be emphasised that the value of a virtual currency is not guaranteed and that the value of cryptocurrencies is generated solely by the interaction of supply and demand. For Bitcoin and other cryptocurrencies, limiting the number of units issued without indexing the currencies' value introduces the risk of speculation that in turn leads to excessive price volatility. Finally, the operational risks of virtual currencies must be reckoned with.

- **Lack of transparency**: currently, there are no special requirements for setting up a virtual currency wallet[3], particularly where this is accomplished by downloading a software application. A virtual currency wallet can also be opened by a service provider who may, although under no legal obligation to do so, carry out an identity check. One of the primary advantages of virtual currencies is that they provide total anonymity for transactions. For many cryptocurrencies, although the identities of principals and beneficiaries are encrypted, transactions are recorded in a public register, thus ensuring their traceability. Nevertheless, traceability of cryptocurrency flows does not address the issue of the identities of the principal and effective beneficiary. On the one hand, this traceability is neither assured nor systematically possible – some cryptocurrencies offer anonymity and non-traceability, and there are tools and applications that can be used to combine payments from multiple users – and on the other hand, the usability of transactions is uncertain, from both a technical and legal standpoint.
- **Extraterritoriality**: thanks to the Internet, the use of virtual currencies can dematerialise, anonymise and expand money laundering and fraud techniques. The difficulties created by virtual currencies stem as much from the elusiveness of the various stakeholders as from the international (and extraterritorial) nature of both transactions and participants. This is particularly the case when the servers and the individuals and legal entities that use them are located in non-cooperative countries and territories.

Bitcoin ATMs

Several companies have begun to design Bitcoin ATMs that allow users to withdraw cash (resulting from the sale of Bitcoins) from a Bitcoin account, and to make deposits into a Bitcoin account (i.e. to purchase Bitcoins). This is the case with kiosks manufactured by Robocoin Technologies.

The first Robocoin ATM was installed in Vancouver in October 2013. In its first month of operation, transactions at the Robocoin kiosk totalled one million Canadian dollars (USD 942,000). Since then, Robocoin ATMs have appeared in other North American cities (Alberta, Seattle, Austin, New York, etc.), in Asia (Hong Kong) and also in Europe (Prague, London, etc.). The Robocoin kiosks identify users via biometrics (palm scans) and by scanning an identity card and comparing the user's face with the identity photo.

Lamassu Bitcoin Ventures has rolled out Bitcoin ATMs in the US, Canada and Australia, as well as in Europe in Helsinki, Berlin and Bratislava. Lamassu's machines offer only unidirectional flows: users can only deposit cash in order to purchase Bitcoins.

In France, two Bitcoin ATMs are currently in operation, and other installations are planned.

Paradoxically, therefore, we are witnessing an increase in means for materialising virtual currencies.

II – RISKS CONNECTED TO THE THREE MAIN USES FOR VIRTUAL CURRENCIES

- **Settling a transaction in a virtual currency**

Virtual currencies can be used to settle Internet-based transactions, but they may also be used in the wider economy with merchants that accept them. Supporters of virtual currencies often emphasise the low cost, speed[4] and irreversibility of transactions, as well as the ability to

[3] The term "virtual currency wallet" can be used interchangeably with "virtual currency account".

[4] Validating a Bitcoin transaction takes about ten minutes, although many cryptocurrencies have sharply reduced this waiting time.

protect oneself against data theft. They also enable micro-payments and purchases abroad free from currency exchange fees. **It should be emphasised that any analysis of payment method costs needs to take into account security and the guarantees offered**.

Examples of risks connected to this use:

- There are no guarantees as to whether a virtual currency is reimbursable or convertible into a currency with legal tender. There are also serious risks with respect to price volatility.
- Since virtual currencies are not legal tender, settlements with such currencies do not have a discharging effect. Consumers should be alerted that it is extremely risky to pay with virtual currency on websites about which they have doubts. This is equivalent to giving cash to an unknown person in the street in payment for a product that he promises to deliver to you later.
- There are no consumer protection measures applicable to virtual currencies
- Virtual currencies do not fall within the scope of the EU Directive on Payment Services (PSD), and thus, unlike traditional payment methods, offer no protection against fraud. The operational security of these new methods of payment is also not guaranteed.

- **Transferring money**

The technical and functional infrastructures that ensure the circulation of virtual currency units are not regulated, and may be used to transfer money at lower rates than those charged by the banking network and international money transfer services. A recent study by Goldman Sachs[5] estimates that, as things currently stand, using Bitcoin would cut transfer fees by 90%. Nevertheless, **any analysis of cost needs to take into account the level of security provided**. Finally, it remains to be seen whether these competitive fees can be maintained in the face of increasing regulation of virtual currencies.

Examples of risks connected to this use:

- The exchange risk is an obstacle to more widespread adoption of this use
- The operational risks of these transfers continue to pose a problem

- **Virtual-currency-linked investments**

In addition to speculative purchase and sale of virtual currencies by individuals, there is a move (outside France) to **develop investment products indexed to the price of Bitcoins**. It is thus possible to invest in virtual-currency-linked products. Funds develop investment strategies based on virtual currencies and their ecosystem. Funds or financial products could be exposed to the risks inherent in virtual currencies – contracts for differences (CFDs) have already been offered to the general public.

Examples of risks connected to this use:

- Virtual currency exchanges present problems for users due to, among other things, a lack of transparency with respect to executing payment orders and price formation (information asymmetry) and to the risk of market abuse. There is no compensation for these anonymous, Internet-based over-the-counter transactions, and the market lacks depth.
- There is also a risk of regulatory arbitrage as certain stakeholders can carry out their activities in offshore financial centres.

- **Other possible uses:**

Virtual currency loans are just beginning to emerge, based largely on trust, particularly via social networks.

On crowdfunding sites, the use of virtual currencies could allow payment in return for fulfilment of certain conditions.

[5] Goldman Sachs, 2014: "All About Bitcoin", Global Macro Research, *Top of Mind*, no. 21, March 2011

III - RISKS OF USING VIRTUAL CURRENCIES FOR FRAUDULENT PURPOSES

Given their nature (specifically their extraterritoriality and the lack of a regulatory body) and how they operate, virtual currencies are inherently risky, and can be used to finance criminal activities and facilitate the laundering of proceeds from those activities.

Zerocoin and Darkcoin: two anonymous, untraceable virtual currencies

Zerocoin was proposed as an extension to the Bitcoin protocol that adds anonymity to Bitcoin transactions. Darkcoin (DRK), another cryptocurrency, made its appearance in 2014. It combines fully encrypted transactions and anonymous block transactions. Given their anonymity and non-traceability, these two virtual currencies appear to be the medium of choice for transactions involving the underground economy. Two months after it was launched, there were DRK 3,828,495 in circulation (the equivalent of USD 3,161,707, at an exchange rate of 1 DRK to USD 0.83 as of 27 March 2014[6]). On this same date, Darkcoin was in 22nd position[7] among virtual currencies in terms of the value of the volume of units issued. As of 15 May 2014, Darkcoin was in 7th place, and had reached 4th place by 8 July 2014[8].

Dark Wallet: a virtual wallet that scrambles the traceability of Bitcoin transactions

This application is a Bitcoin wallet that was released in early 2014. It is still in a beta version, and was financed through crowdfunding. Dark Wallet combines users' transactions in such a way as to make it impossible to determine who sent what to whom. This procedure makes it easy to launder one's own Bitcoins. Dark Wallet also allows users to generate a Bitcoin address using a secret key, associated with another address in Dark Wallet, thus masking the address of the end Bitcoin account to which funds were transferred.

A virtual currency presents a twofold risk in terms of committing criminal offenses, as it facilitates the commission of the underlying crime and serves as a tool for laundering the proceeds of such a crime.

Finally, there is a significant risk with respect to the very nature of cryptocurrencies[9] whose money supply has been capped, as there is concern that the money supply itself could be the target of fraud.

Virtual currencies – a vector for facilitating fraud and money-laundering

When it comes to perpetrating fraud, the anonymity provided by virtual currencies allows fraudsters to collect money without leaving a footprint of the transaction. This is similar to a cash-based transaction, but one conducted on the Internet without the criminal and the victim ever meeting face-to-face. Here we are dealing with standard criminal activities tailored to new technologies and the possibilities they open up.

For example, fraudsters might set up a fake e-commerce site that accepts payment in virtual currency, then shut down the site and have access to the funds collected in any country whatsoever, without leaving behind the slightest trace of any transaction. The risk of money laundering is all the higher

[6] Source : https://coinmarketcap.com/all.html

[7] Among cryptocurrencies.

[8] *Ibid*.

[9] In this it resembles a Ponzi scheme, an investment fraud that involves the payment of purported returns to existing investors from funds contributed by new investors. If the fraud is not discovered, it is revealed when the scheme collapses. This is to say that individuals who set up and launch a cryptocurrency with a speculative component based on windfall profits when the currency is resold increase the number of injured parties when the currency collapses. They will no longer be able to exchange the virtual currency for legal tender, as the virtual currency offers no guarantee and has zero intrinsic value.

since the operation is divided into three stages – purchasing virtual currency with cash, setting up an e-commerce site from which fictitious purchases of goods are made from a number of computers using virtual currency, and collecting often large sums of money, which can then be exchanged for legal tender.

The use of a virtual currency can render Internet-based money laundering techniques even more opaque. Examples of this include online gaming, fraudulent e-commerce transactions, online auctions or fake projects listed on foreign crowdfunding sites.

Although virtual currencies satisfy money launderers' needs for speed, discretion and global reach, funds converted into virtual currencies are vulnerable to operational risks and to volatility. In light of these limitations, the use of virtual currencies for money laundering appears more suitable for small-scale money laundering or the laundering of the proceeds of cybercrime. This said, the creation of gold-backed virtual currencies, such as Gold Backed Coin (GBC), lessens the financial risk connected to virtual currency price volatility.

IV - RECOMMENDATIONS FOR REGULATING VIRTUAL CURRENCIES TO PREVENT THEM FROM BEING USED FOR FRAUDULENT PURPOSES AND MONEY LAUNDERING

The nature and multifunctionality of virtual currencies means that there is a risk of them being used for fraudulent purposes. Due to the upswing in new criminal activities in connection with virtual currencies, legislative and regulatory frameworks need to be updated and adapted in response to these new challenges, particularly with respect to the fight against money laundering and terrorist financing. One possible strategy would include three complementary components:

- Limiting the use of virtual currencies
- Regulation and cooperation
- Knowledge and investigation

Limiting the use of virtual currencies – Key points

Without prejudice to the conclusions drawn from national and international discussions of the legal characterisation of virtual currencies, proposals could be put forth to limit:

- **The anonymity of users of virtual currencies**, particularly by introducing mandatory proof of identity when opening a virtual currency account[10] as well as an obligation to declare such accounts. In addition, it is important to have the tools for identifying and monitoring these accounts, at least when they exceed a certain amount.
- **The possibilities for using a virtual currency as an anonymous payment method**, particularly by strictly capping the sums that can be paid in this way.
- **Cash/virtual currency flows**, particularly when it comes to using Bitcoin ATMs, by setting caps and by ensuring that the identity of a party to a transaction is checked using reliable means.

Regulation and cooperation – Key points

Proposals should also be put forth **to ensure that the AML/CFT system is capable of addressing the risks posed by virtual currencies and the upswing in new criminal activities in connection with these currencies**. To this end, we recommend:

- **Harmonising regulations concerning virtual currency exchanges at EU and international level and prevent virtual exchanges located abroad and who have French users from circumventing French law**: subjecting virtual exchanges to the AML/CFT regime will, among other benefits, lift users' anonymity prior to converting virtual currencies into legal tender.

[10] A minimum requirement when the account is opened by a service provider.

- **Requesting that professionals subject to AML/CFT reporting requirements exercise heightened vigilance with respect to flows in connection with individuals using virtual currencies.**
- **Reminding individuals offering virtual currencies for sale or operating Bitcoin ATMs[11] of the provisions of Article L. 561-1 of the French Monetary and Financial Code[12]**.

Knowledge and investigation – Key points

Given the rapid expansion of the virtual currency sector, explosive technological progress and the need to **bolster international cooperation**, we also propose that **the risks and opportunities associated with virtual currencies be monitored**:

- **Adapt the legal framework and investigative methods**
- **Improve sector knowledge and risk monitoring**

These recommendations do not address the issue of the legal characterisation of virtual currencies, nor issues of preventing risks in terms of protecting and informing users[13]. As the virtual currency sector is changing rapidly, it is worth pointing out that the recommendations are based on an analysis of the situation as of June 2014. We should also point out that these recommendations should be rolled out slowly and in stages, based on appropriate circumstances for implementing them.

Summary table of the three components of the proposed strategy

Limiting the use of virtual currencies	Regulation and cooperation	Knowledge and investigation
Limit and cap the use of virtual currencies as a payment method Limit and monitor cash/virtual currency flows Limit the anonymity of virtual currency users	Ensure that the AML/CFT system is capable of addressing the risks posed by virtual currencies and the activities in connection with these currencies Harmonise regulations at EU and international level	Introduce special-purpose resources and analytical tools Monitor risks and opportunities, particularly through exchanges with sector professionals

[11] Or exchange kiosks.

[12] Article L. 561-1 stipulates, among other provisions, that "Individuals and legal entities other than those referred to in Article L. 561-2 [i.e. those subject to the obligations relating to the prevention of money laundering and of terrorist financing] who, in the normal course of their business, execute, supervise or recommend transactions giving rise to capital movements, shall be required to declare to the Public Prosecutor any transactions they have knowledge of that involve sums which they know to be the proceeds of an offence referred to in Article L. 562-15. Source : www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000020196700&cidTexte=LEGITEXT000006072026&dateTexte=20090201

[13] See *Focus* no. 10, Banque de France, 5 December 2013 : www.banque-france.fr/fileadmin/user_upload/banque_de_france/publications/Focus-10-stabilite-financiere.pdf

Working group chaired by Tracfin

Members:

- Prudential Supervisory and Resolution Authority
- Autorité des marchés financiers
- Banque de France
- Directorate for Criminal Affairs and Pardons
- National Criminal Police Directorate
- Gendarmerie General Directorate
- Directorate General of the Treasury
- Directorate General of Customs and Excise
- Public Finances Directorate General
- Directorate General for Competition Policy, Consumer Affairs and Fraud Control
- Ministry of Defence
- Ministry of the Interior

www.economie.gouv.fr/tracfin