Virtual currencies: the regulatory challenges

By Ross Leckow

1 Introduction

Technological innovation is transforming the financial services industry. The popular press is filled with stories about new technologies and startups that have the potential to fundamentally change the way in which financial services are provided. Many new technologies offer the hope of a financial system in which services are provided more quickly and cheaply and to a much wider range of consumers than was imaginable even a few years ago. The emergence of virtual currencies has been an important development in this field. Virtual currencies offer the promise of a global system of payments and transfers that would be far more efficient than that currently in existence. But they also pose risks. These risks range from the hypothetical to the immediate, and are attracting the attention of regulators around the world.

This paper examines the role that virtual currencies can play in the financial system, the challenges they pose for regulators, and the approaches that regulators are adopting in response. The paper begins with a brief description of virtual currencies and the manner in which they operate, and then examines four basic questions: (1) why national authorities should regulate virtual currencies; (2) the challenges that virtual currencies pose for regulators; (3) which aspects of virtual currencies should be the subject of regulation; and (4) how a regulatory regime could be most effectively designed. The paper ends with a discussion of the future of regulation in this field. In examining these questions, the paper focuses on decentralised virtual currencies (or “cryptocurrencies”), and pays particular attention to regulation in the field of anti-money laundering and combatting the financing of terrorism (AML/CFT).

As a starting point, it is important to note that the International Monetary Fund (IMF) is closely observing the development of virtual currencies. The IMF’s interest stems, in particular, from its purposes under its Articles of Agreement (the IMF’s constituent document), to “promote exchange stability, maintain orderly exchange arrangements” and to “assist in the establishment of a multilateral system of payments in respect of current transactions between members and in the elimination of foreign exchange restrictions which hamper the growth of world trade”. In January 2016, the IMF published a paper entitled “Virtual Currencies and Beyond:

1 Deputy General Counsel, International Monetary Fund. The views expressed in this article are those of the author and do not necessarily represent the views of the IMF, its Executive Board, or IMF management. The author gratefully acknowledges the advice and assistance of Ms Yasmin Almeida, Research Officer at the IMF in preparing this article.

2 Articles of Agreement of the International Monetary Fund, Article I(iii) and (iv).
Virtual currencies: the regulatory challenges

Initial Considerations’3 (hereinafter “Virtual Currencies and Beyond”). This paper represented the first effort by IMF staff to examine virtual currencies and their implications. IMF staff are continuing to study developments in the area of virtual currencies as well as in finance and technology (hereinafter “FinTech”) more broadly.

Virtual currencies are also attracting attention from other international organisations and national authorities. Important studies have been published, in particular, by the ECB, the European Commission, the Committee on Payments and Market Infrastructures and, at national level, the Bank of England and the Bank of Canada.4

2 What are virtual currencies?

Virtual currencies are digital representations of value issued by private developers and denominated in their own unit of account. They can be obtained, stored and transferred electronically and used for a variety of purposes by parties who agree to use them.

Virtual currencies fall within the broader concept of “digital currencies” but differ from other forms of digital currencies in at least one important respect: they are not denominated in a fiat currency.5

Virtual currency schemes comprise two important features: (1) the virtual currency itself or digital representation of value that parties hold and use; and (2) the underlying framework of rules and protocols that govern the operation of the system. It is this framework that governs the issuance and redeemability of virtual currencies, their use and circulation, and the payment and settlement process.

There are many different types of virtual currencies and virtual currency schemes. Some virtual currencies are non-convertible (i.e. they cannot be converted into fiat currency) and can only be used between participants inside the system for specified purposes. Other virtual currencies are convertible – that is, they can be converted into fiat currency and used for the purposes of making payments in the real economy.

Virtual currency schemes can be centralised, decentralised or a hybrid between the two. In a centralised system, the system is administered by a central private party. In a decentralised system, the central administrator is replaced by the protocols that govern the operation of the system, and many administrative functions are performed by the system’s participants themselves.6 As payments and transfers are

---

5 “Virtual Currencies and Beyond”, p. 7.
6 Ibid., p. 9.
made, the participants in a decentralised scheme verify whether the transferor has the necessary funds and, if so, record the transaction as having been completed. Participants who perform this verification function (known as "miners") are then rewarded through the issuance of newly-minted units of the virtual currency. This verification process has the dual function of ensuring the validity of the transaction without the involvement of a central trusted intermediary (e.g. a bank), and introducing new units of the cryptocurrency into the system.

The virtual currencies that form part of these decentralised systems are known as "cryptocurrencies". While there are a number of cryptocurrencies whose model may vary, Bitcoin is the most well-known example. A key feature of a cryptocurrency scheme is the "distributed ledger technology" underlying the system. In contrast to the traditional financial system where trusted intermediaries (e.g. banks) maintain the ledgers and accounts and verify the validity of particular transactions, the ledgers in a cryptocurrency scheme are distributed to each participant. In the Bitcoin model, as transactions are executed and verified by participants, the ledgers are periodically updated with new transactions recorded in the distributed ledger. As such, the distributed ledger, or "blockchain", provides a complete and immutable record of all transactions that have ever taken place within the system. For each unit of virtual currency, the distributed ledger provides a complete history of every transaction that has ever taken place involving that particular unit.

Three other important features of cryptocurrencies should be noted. First, most cryptocurrency schemes (including Bitcoin) only allow for the issuance of a finite number of cryptocurrency units. Second, cryptocurrencies are "pseudo-anonymous": while all cryptocurrency transactions are recorded in the distributed ledger available to all participants, the users behind these transactions are known only by their cryptocurrency "addresses" and not by their real identity. As such, cryptocurrencies are more transparent than cash but less transparent than other forms of online payment. Finally, cryptocurrencies challenge the fundamental principles underlying fiat currencies: while fiat currencies are backed by the credibility of the issuing central bank and government, cryptocurrencies are not backed by any source and their value is determined entirely by the willingness of users to accept them.

There are several different ways in which cryptocurrencies can be acquired. In addition to the acquisition of cryptocurrencies through the "mining" process described above, they can be purchased in a virtual currency exchange (an online service provider that buys and sells cryptocurrencies against fiat currencies and other cryptocurrencies), a trade platform, or directly from another holder of cryptocurrencies. Cryptocurrencies can be held in a "wallet", typically maintained with a wallet provider or exchange.

---

7 ibid.
3 Why regulate virtual currencies?

There is no doubt that virtual currencies have the potential to provide substantial benefits to the financial system, market participants, and consumers. They enable direct “peer-to-peer” transactions and eliminate the need for an intermediary or central clearinghouse. As such, they have the potential to enhance the efficiency of the financial system by enabling the making of payments – including cross-border payments – more quickly and cheaply than ever before. They could deepen financial inclusion, in particular, in the developing world by significantly improving the opportunities for fast low-cost cross-border remittances, and by bringing the “unbanked” of many developing countries into the financial system.

At the same time, cryptocurrencies pose risks. In “Virtual Currencies and Beyond”, IMF staff identified six potential risks.8 These risks can be placed on a continuum, some of which are more remote and others which are more immediate.

In the longer term and at the more remote end of the spectrum, there are two risks. First, the widespread use of virtual currencies could complicate the conduct of monetary policy – for example, where the use of a cryptocurrency in a jurisdiction becomes so widespread that it undermines the conduct of the authorities’ monetary policy which relies on the use of a fiat currency. Second, there is a risk that the use of cryptocurrencies in a country could become such an important part of the financial system that it would pose risks to financial stability – for example, through the failure of an important part of a cryptocurrency infrastructure or a key participant within the system. Both of these risks may be viewed as remote at this stage as the total amount of cryptocurrencies in circulation is still very small. For example, as of October 2016, there were somewhat more than 15 million bitcoins in circulation worth approximately USD 9.7 billion according to blockchain.info,9 while US dollars of a value of approximately USD 1.48 trillion were in circulation according to the U.S. Federal Reserve System.10

Beyond these more remote risks, the IMF paper identified four risks that are more immediate in nature. These are outlined below.

Cryptocurrencies present opportunities for fraud. Because the cryptocurrency market is still opaque and the regulatory framework still in the process of development, cryptocurrencies present opportunities for scams including the theft of units of cryptocurrency through fraud or hacking. In 2013, for example, the U.S. Securities Exchange Commission filed a complaint against a company engaging in a bitcoin-denominated “Ponzi” scheme pursuant to federal securities legislation that prohibits fraudulent offers and sales of securities.11 In 2014, what was then then the largest Bitcoin exchange in the world, Mt Gox, filed for bankruptcy in Japan after announcing that nearly half a billion dollars’ worth of bitcoins held for customers had gone

---

8 At pp. 27-35.
10 Source: https://www.federalreserve.gov/faqcurrency_12773.htm
missing. The CEO of Mt Gox was subsequently charged with embezzlement by the Japanese authorities.  

Cryptocurrencies also facilitate tax evasion. As participants in a cryptocurrency scheme do not have to fully disclose their identity and can engage in peer-to-peer transactions without an intermediary, cryptocurrencies make it easier for market participants to hold and use funds without disclosing them to the authorities.

Cryptocurrencies can be used to circumvent exchange and capital controls. By facilitating the making of cross-border payments and transfers outside of the banking system, users can avoid the application of exchange or capital controls that banks, in some countries, are required to observe. Rather than purchasing foreign currency and transferring it abroad through an authorised bank, market participants can purchase cryptocurrency and transfer it abroad on a peer-to-peer basis. Such practices have already been reported in countries such as Venezuela and China where exchange and capital control regimes remain in place.

Furthermore, cryptocurrencies may be used to facilitate money laundering and terrorist financing. The pseudo-anonymous and peer-to-peer nature of cryptocurrency schemes make them an ideal mechanism through which to disguise the illicit origin or destination of funds. There have already been a number of serious and well-publicised cases of money-laundering involving cryptocurrency schemes. For example, Bitcoin was used as the currency of choice in “Silk Road”, a “dark web” market place for illegal goods that was shut down by US law enforcement authorities in 2013.

If regulation is unnecessary for more remote risks, it is necessary to prevent the types of abuses described above, even if cryptocurrencies are not yet widely used. The question therefore arises: if cryptocurrencies are to be the subject of regulation, what are the challenges that national authorities will have to confront in regulating them?

4 What are the challenges of regulation?

In designing a regulatory framework, it is important to note four challenges that cryptocurrencies pose. Specifically these are as described below.

They pose a definitional challenge. Cryptocurrencies (and virtual currencies more generally) combine the properties of currencies, commodities, and payments systems. Their classification as one or the other will have implications for their regulatory treatment. Different regulatory agencies within a jurisdiction may classify

---

13 Virtual Currencies and Beyond”, p. 31.
14 Anonymising service providers known as “tumblers” assist in obfuscating a transaction chain and more effectively concealing the identity of a user.
them in different ways, depending on their own policy priorities. In the United States, for example, the Financial Crimes Enforcement Network (FinCEN), the national financial intelligence unit, treats virtual currencies as “value” for the purposes of AML/CFT regulation, while the Internal Revenue Service treats them as “property” for the purposes of federal taxation, and the Commodities Futures Trading Commission defines them as “commodities” for its own regulatory purposes.

The use of cryptocurrency within a cryptocurrency scheme is difficult to monitor. Their pseudo-anonymity and potential for peer-to-peer transactions make it difficult, in some cases, to determine the identity of a user, or that person’s use of the currency within the system.

The transnational reach of cryptocurrencies may complicate regulation. Asserting jurisdiction over a particular virtual currency transaction, market participant or scheme may prove challenging in some cases.

Finally, the decentralised nature of cryptocurrencies challenges conventional regulatory models. Cryptocurrency schemes eliminate the role of traditional intermediaries that are normally the focal point of regulation. For example, in the field of exchange control, it is the banks and other financial intermediaries that play a critical role in ensuring that particular payments and transfers of currency are made in a manner that complies with applicable exchange control regulations. Within a cryptocurrency scheme, these traditional intermediaries are generally not present.

5 What should be the subject of regulation?

Against this background, in the design of a regulatory framework for cryptocurrencies, what should be the subject of regulation? Conceptually, there are three broad features of a cryptocurrency system that may be subject to regulation.

First, regulation could apply to the cryptocurrency scheme itself – that is, the protocol, procedures and rules governing the operation of the system to which all participants in the system must adhere. Second, regulation could apply to the uses which market participants make of a cryptocurrency, including the making of payments, or the exchange of cryptocurrency for fiat currency. Third, regulation could apply to the users of the system, including service providers within the system.

For now, regulation has focused on the uses that can be made of cryptocurrencies and the service providers in the virtual currency sphere. Less focus has been placed on regulating a cryptocurrency system itself. Regulation of a decentralised virtual

---

16 “Application of FinCEN’s regulations to persons administering, exchanging or using virtual currencies”, Guidance, Department of the Treasury Financial Crimes Enforcement Network, FIN-2013-G001, 18 March 2013.


currency system may prove extremely difficult as there is no central authority that controls the system and that could be made the subject of regulation.19

6 How should a regulatory framework be designed?

Against this background, how should a regulatory framework for cryptocurrencies be designed? In these early days, countries have taken a broad range of approaches. National responses have ranged from a completely laissez-faire approach, to issuing advisories warning of the risks associated with cryptocurrencies (e.g. fraud and theft), to restricting or banning their use20. In addition to enforcing existing laws, in particular criminal laws prohibiting fraud and money laundering, some jurisdictions have taken a step further and extended the application of selected financial and consumer protection legislation and regulations to virtual currency-related uses and/or intermediaries. This has notably been done by issuing interpretative guidance on their applicability.

Enforcement presents a major challenge for regulators. As the business model for cryptocurrency schemes differs fundamentally from traditional payment models, regulators are adopting new approaches to ensure that certain types of regulation are observed. An important example of this development is in the field of AML/CFT. In many countries, it is the banks and conventional providers of money or value transfer services that typically play a key role in ensuring that AML/CFT regulations are observed in the payment sphere.21 These entities are required to take the necessary “preventive measures” (e.g. customer due diligence, record keeping, suspicious activity reporting) to ensure that they know the identity of their customers and that they understand the purpose and intended nature of the business relationship. Without traditional financial institutions to play this role in the virtual currency sphere, regulators have had to look at new types of service providers on whom responsibility for AML/CFT compliance should fall.

The Financial Action Task Force (FATF) has provided guidance on the application of the global AML/CFT standards (the FATF standards) to virtual currencies. Its guidance focuses on how the risk-based approach inherent in the FATF standards can be applied in the context of virtual currencies. One particularly important issue it has addressed concerns who, in the absence of traditional regulated entities like

19 In the United States, “administrators” of virtual currency schemes are considered to be “money transmitters” and, therefore “money services businesses” that, under the Bank Secrecy Act, are required to register with the Department of the Treasury and to develop AML/CFT programmes. See FIN-2013-G001, “Application of FinCEN’s Regulations to Persons Administering, Exchanging or Using Virtual Currencies”, 18 March 2013. Administrators are more common in centralised virtual currency schemes. Identifying an “administrator” in a hybrid or decentralised scheme may be more challenging.

20 See “Virtual Currencies and Beyond”, pp. 25 and 42.

21 Under the international standards, financial institutions as well as designated non-financial businesses and professions are required to implement AML/CFT preventive measures (see the 2012 FATF 40 Recommendations).
banks, would be responsible for ensuring the rules are observed. The guidance also points out which recommendations are relevant in relation to virtual currencies.22

In the world of cryptocurrencies, there are two possible points of intersection at which AML/CFT obligations may be imposed. The first stage may be called the gateway. This exists at the point where a user purchases or sells units of cryptocurrency in exchange for fiat currency. The purchase or sale of cryptocurrency is the principal point of entry into and exit from the cryptocurrency sphere. The second point may be found within the cryptocurrency system – that is, when units of cryptocurrency are being held or transferred between participants.

In identifying intermediaries upon whom to impose AML/CFT obligations, FATF has looked to the “gateways” between the virtual currency world and the traditional financial sector. It has called for the obligation to apply preventive measures to be imposed on the “gatekeepers” – in particular, the virtual currency exchanges through which market participants purchase virtual currency to enter the system or to sell it for fiat currency to leave the system. The FATF guidance links virtual currencies and virtual currency exchanges to the definition of a “financial institution”, meaning that virtual currency exchanges are considered “covered entities” under the FATF standard.23 As is the case with traditional financial institutions, virtual currency exchanges would then be required by national authorities to perform customer due diligence, keep records and report suspicious transactions to the AML/CFT authority in the relevant country in the event that the FATF guidance were to be followed in that jurisdiction.

A number of countries (e.g. Germany, the United Kingdom, the United States, and Canada) have taken similar approaches in practice.24 In the United States, FinCEN has issued guidance clarifying that virtual currency exchanges are “money services businesses” for the purposes of US AML/CFT legislation and, as such, are required to apply AML/CFT preventive measures.25

The effectiveness of the approach set out in the FATF guidance will depend on how the virtual currency market evolves. Requiring gatekeepers to take preventive measures is certainly an important step forward in combatting money laundering and terrorist financing. However, as the virtual currency market evolves and new money laundering and terrorist financing typologies emerge, the effectiveness of this approach will need to be reassessed. More generally, the cryptocurrency world is still small, and most users will likely have to convert their holdings into fiat currency at some point. However, the volume of cryptocurrency in circulation may grow to the point that “cashing out” will no longer be necessary. In these circumstances, it may become necessary to extend regulation to other virtual currency network participants

22 “Virtual Currencies: Key Definitions and Potential AML/CFT Risks” (FATF, 2014); “Guidance for a Risk-Based Approach to Virtual Currencies” (FATF, 2015).
23 Within a centralised virtual currency scheme, the concept of a “covered entity” would also include the central administrator of the system.
24 “Virtual Currencies and Beyond”, p. 28.
25 See FIN-2013-G001 (FinCEN, 2013).
such as wallet service providers and payment processors that operate entirely within the system.

Some regulators have already begun to move towards this approach. A proposal was adopted by the European Commission in July 2016 to amend Directive (EU) 2015/849, which concerns the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. In particular, this proposal provides for an expanded definition of “obliged entities” to include both virtual currency exchanges and providers of certain types of digital wallets in which users may hold units of cryptocurrency that are referred to as “custodian wallet providers”. These are identified as “wallet providers offering custodial services of credentials necessary to access virtual currencies”. While this definition may not include all types of digital wallet providers currently operating in the virtual currency sphere (e.g. non-custodian wallet providers), it does go beyond the gateways that have so far been the target of regulation. The imposition of such obligations with respect to other types of wallets with more complex rules of access (e.g. multi-signature wallets) may prove to be more difficult.

Even within such a framework, the enforcement of AML/CFT regulations in the cryptocurrency sphere may prove challenging. While a growing segment of transfers and transactions are being conducted with the involvement of exchanges or wallet service providers, it is still possible for a user to make a transfer without using an intermediary. It remains to be seen whether the portion of the market that exists outside the reach of intermediaries will shrink to the point where money launderers will be unable to perform transactions in the volumes they need. Moreover, even where virtual currency exchanges are subject to regulation, the effectiveness of imposing freezing and seizing orders with respect to funds held in cryptocurrencies is not clear.27

Beyond the area of AML/CFT regulation, some jurisdictions are subjecting the new virtual currency service providers to more comprehensive licensing regimes. Many of these requirements are motivated more by concerns over consumer protection rather than over financial stability. Many such jurisdictions are clarifying that some types of virtual currency service providers – in particular, exchanges – fall within the licensing requirements for money transmitters within the jurisdiction. As a result, these entities are subject to licensing regimes that impose fit and proper requirements on their management and owners (for instance by examining the experience and backgrounds of the chief officers and significant shareholders) and also impose requirements in respect of the entity’s financial soundness including minimum capital levels and the reserves they are required to maintain.

A few jurisdictions are establishing licensing regimes that apply specifically to virtual currency service providers. An example of this is the New York BitLicense adopted


27 “Virtual Currencies and Beyond”, p. 28.
by the New York Department of Financial Services in 2015. This framework sets out a comprehensive regime for the licensing of a broad range of virtual currency service providers, including exchanges, wallet service providers, and dealers.\(^{28}\) The licensing process examines the appropriateness of the owners and principal officers of the business, the capital position and reserves of the business, its programmes and arrangements for AML/CFT compliance and the maintenance of cyber-security, and its procedures for the disclosure of potential risks to customers. The regulator’s assessment of the financial position and reserves of the business takes a risk-based approach that examines the nature of the business being conducted.

While recognising the need to impose AML/CFT obligations on certain service providers, some jurisdictions have in parallel put in place “regulatory sandboxes” to foster responsible innovation. In an effort to ensure that regulation does not stifle innovation, a few countries (e.g. the United Kingdom, Singapore) have put in place regulatory sandboxes that allow FinTech startups of many different types (including virtual currency companies) to test new products with a small number of actual users in a simulated environment.\(^{29}\) These sandboxes provide a safe space for innovation to happen without potentially adverse effects for financial markets or consumers. Within the sandbox, certain regulatory requirements may be relaxed for a specified period of time. However, some jurisdictions (e.g. Singapore) specify that regulatory requirements will be fully enforced even within the sandbox.

7 Conclusions

As we are at an early stage of market development for cryptocurrencies, it is not surprising that we are also at an early stage in the design of a regulatory environment for their use. While a great deal of progress has been achieved in thinking through the issues in some areas, more work will need to be done or redone as cryptocurrencies continue to evolve.

Moving forward, what principles should guide the development of regulatory frameworks for cryptocurrencies? The key guiding principle should recognise the need to draw an appropriate balance between regulation and innovation. While cryptocurrencies do present risks, they also offer the potential to significantly enhance the efficiency and inclusiveness of the global financial system. Regulators therefore need to put in place frameworks that guard against risk but in a manner that does not stifle innovation. Regulatory approaches will also need to be flexible, and able to adapt to potentially significant changes as the virtual currency landscape continues to evolve. Regulators will need to take into account the novel business models inherent in cryptocurrency schemes and decide on the appropriate degree of integration (if any) between the conventional financial system and the cryptocurrency world. Finally, more will need to be done to develop an effective regulatory framework.


framework at international level. International bodies have an important role to play in this respect, in studying cryptocurrencies and in discussing potential regulatory approaches. In the longer term, consideration could be given to the development of international standards and best practices, as some standard-setting bodies like FATF have already clarified the application of their standards to virtual currencies. But these are still early days in the development of cryptocurrencies and the regulatory frameworks that apply to them. While much more work remains to be done, it is work that calls for a cooperative effort on the part of the entire international community.

Bibliography


ECB,”Virtual currency schemes” (2012).


IMF, “Virtual Currencies and Beyond: Initial Considerations” (January 2016).