FATF REPORT

Virtual Currencies

Key Definitions and Potential AML/CFT Risks

June 2014

FATF

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

Photocredits coverphoto: ©Thinkstock

CONTENTS

ACRONYMS

AML/CFT	Anti-money laundering / countering the financing of terrorism
ECB	European Central Bank
FATF	Financial Action Task Force
NPPS Guidance	Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services

VIRTUAL CURRENCIES - KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS[1]

INTRODUCTION

As decentralised, math-based virtual currencies—particularly Bitcoin[2]—have garnered increasing attention, two popular narratives have emerged: (1) virtual currencies are the wave of the future for payment systems; and (2) virtual currencies provide a powerful new tool for criminals, terrorist financiers and other sanctions evaders to move and store illicit funds, out of the reach of law enforcement and other authorities.[3] Against this backdrop, this paper builds on the 2013 New Payment Products and Services (NPPS) Guidance (FATF, 2013) by suggesting a conceptual framework for understanding and addressing the anti-money laundering / countering the financing of terrorism (AML/CFT) risks associated with one kind of internet-based payment system: virtual currencies. Specifically, the paper proposes a common definitional vocabulary that clarifies what virtual currency is and classifies the various types of virtual currency, based on their different business models and methods of operation,[4] and identifies the participants in typical virtual currency systems. It also applies risk factors set forth in Section IV (A) of the 2013 NPPS Guidance to specific types of virtual currencies to identify potential risks; describes some recent investigations and enforcement efforts involving virtual currency; and presents a sample of jurisdictions' current regulatory approaches to virtual currency.

While the 2013 NPPS Guidance broadly addressed internet-based payment services, it did not define "digital currency," "virtual currency," or "electronic money." Nor did it focus on virtual currencies, as distinct from internet-based payment systems that facilitate transactions denominated in real money (fiat or national currency) (e.g., Pay-Pal, Alipay, or Google Checkout). It also did not address decentralised convertible virtual currencies, such as Bitcoin. The 2013 Guidance also notes that, "[g]iven the developing nature of alternate online currencies, the FATF may consider further work in this area in the future" (2013 NPPS Guidance, p. 11, para. 29). A short-term typologies project on this basis was initiated with the following objectives:

- develop a risk-matrix for virtual currencies (or perhaps, more broadly, for both virtual currencies and e-money);
- promote fuller understanding of the parties involved in convertible virtual currency systems and the way virtual currency can be used to operate payment systems; and
- stimulate a discussion on implementing risk-based AML/CFT regulations in this area.

This typologies project may lead to policy work by the FATF, e.g. the issuance of supplemental guidance for applying a risk-based approach to virtual currencies that would incorporate the proposed vocabulary and risk-matrix developed by the typologies project and explain how specific FATF Recommendations apply in the context of virtual currency.

KEY DEFINITIONS:

A common set of terms reflecting how virtual currencies operate is a crucial first step to enable government officials, law enforcement, and private sector entities to analyse the potential AML/CFT risks of virtual currency as a new payment method. As regulators and law enforcement officials around the world begin to grapple with the challenges presented by virtual currencies, it has become apparent that we lack a common vocabulary that accurately reflects the different forms virtual currency may take. The following set of terms is intended to aid discussion between FATF members. It is important to note that this vocabulary may change as virtual currency evolves and as regulators and law enforcement/government officials continue to consider the challenges virtual currencies present. Nevertheless, the proposed vocabulary aims to provide a common language for developing conceptual tools to help us better understand how virtual currencies operate and the risks and potential benefits they offer.

VIRTUAL CURRENCY

Virtual currency is a digital representation[5] of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment)[6] in any jurisdiction.[7] It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from **fiat currency** (a.k.a. **"real currency," "real money,"** or **"national currency"**), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-**money**, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status.

Digital currency can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat) and thus is often used interchangeably with the term "virtual currency". In this paper to avoid confusion, only the terms "virtual currency" or "e-money" are used.

CONVERTIBLE VERSUS NON-CONVERTIBLE VIRTUAL CURRENCY

This paper proposes dividing virtual currency into two basic types: convertible and non-convertible virtual currency.[8] Although the paper uses "non-convertible" and "closed", and "convertible" and "open" as synonyms, it should be emphasised that the notion of "convertible currency" does not in any way imply an ex officio convertibility (e.g. in the case of gold standard), but rather a de facto convertibility (e.g. because a market exists). Thus, a virtual currency is "convertible" only as long as some private participants make offers and others accept them, since the "convertibility" is not guaranteed at all by law.

Convertible (or open) virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency.[9] Examples include: Bitcoin; e-Gold (defunct); Liberty Reserve (defunct); Second Life Linden Dollars; and WebMoney.[10]

Non-convertible (or closed) virtual currency is intended to be specific to a particular virtual domain or world, such as a Massively Multiplayer Online Role-Playing Game (MMORPG) or Amazon.com, and under the rules governing its use, cannot be exchanged for fiat currency. Examples include**:** Project Entropia Dollars; Q Coins; and World of Warcraft Gold.

It should be noted that even where, under the terms set by the administrator, a non-convertible currency is officially transferrable only within a specific virtual environment and is not convertible, it is possible that an unofficial, secondary black market may arise that provides an opportunity to exchange the "non-convertible" virtual currency for fiat currency or another virtual currency. Generally, the administrator will apply sanctions (including termination of membership and/or forfeiture of remaining virtual currency) to those seeking to create or use a secondary market, contrary to the rules of the currency.[11] Development of a robust secondary black market in a particular "non-convertible" virtual currency may, as a practical matter, effectively transform it into a convertible virtual currency. A non-convertible characterisation is thus not necessarily static.

CENTRALISED VERSUS NON-CENTRALISED VIRTUAL CURRENCIES

All non-convertible virtual currencies are centralised: by definition, they are issued by a central authority that establishes rules making them non-convertible. In contrast, convertible virtual currencies may be either of two sub-types: centralised or decentralised.

Centralised Virtual Currencies have a single administrating authority (**administrator)**—i.e., a third party[12] that controls the system. An administrator issues the currency; establishes the rules for its use; maintains a central payment ledger; and has authority to redeem the currency (withdraw it from circulation). The exchange rate for a convertible virtual currency may be either **floating**—i.e., determined by market supply and demand for the virtual currency--or **pegged**—i.e., fixed by the administrator at a set value measured in fiat currency or another real-world store of value, such as gold or a basket of currencies. Currently, the vast majority of virtual currency payments transactions involve centralised virtual currencies. Examples: E-gold (defunct); Liberty Reserve dollars/euros (defunct); Second Life "Linden dollars"; PerfectMoney; WebMoney "WM units"; and World of Warcraft gold.

Decentralised Virtual Currencies (a.k.a. crypto-currencies) are distributed[13], open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight. Examples: Bitcoin; LiteCoin; and Ripple.[14]

Cryptocurrency refers to a math-based, decentralised convertible virtual currency that is protected by cryptography.—i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred. The safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties (in Bitcoin, referred to as miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee (in Bitcoin, a small number of newly created bitcoins, called the "block reward" and in some cases, also transaction fees paid by users as a incentive for miners to include their transactions in the next block). Hundreds of cryptocurrency specifications have been defined, mostly derived from Bitcoin, which uses a proof-of-work system to validate transactions and maintain the block chain. While Bitcoin provided the first fully implemented cryptocurrency protocol, there is growing interest in developing alternative, potentially more efficient proof methods, such as systems based on proof-of-stake.

Bitcoin, launched in 2009, was the first decentralised convertible virtual currency, and the first cryptocurrency. Bitcoins are units of account composed of unique strings of numbers and letters that constitute units of the currency and have value only because individual users are willing to pay for them. Bitcoins are digitally traded between users with a high degree of anonymity and can be exchanged (purchased or cashed out) into US dollars, Euros, and other fiat or virtual currencies. Anyone can download the free, open-source software from a website to send, receive, and store bitcoins and monitor Bitcoin transactions. Users can also obtain Bitcoin addresses, which function like accounts, at a Bitcoin exchanger or online wallet service. Transactions (fund flows) are publicly available in a shared transaction register and identified by the Bitcoin address, a string of letters and numbers that is not systematically linked to an individual.. Therefore, Bitcoin is said to be "pseudo-anonymous". Bitcoin is capped at 21 million bitcoins (but each unit could be divided in smaller parts), projected to be reached by 2140.[15] As of April 2, 2014, there were over 12-and-a-half million bitcoins, with total value of slightly more than USD 5.5 billion, based on the average exchange rate on that date.

Altcoin refers to math-based decentralised convertible virtual currency other than bitcoins, the original such currency. Current examples include Ripple; PeerCoin, Lite-coin; zerocoin; anoncoin and dogecoin. One popular exchanger, Cryptsy, would reportedly exchange over 100 different virtual currencies (as of 2 April 2014). (Popper, N., 2013)

Anonymiser (anonymising tool) refers to tools and services, such as darknets and mixers, designed to obscure the source of a Bitcoin transaction and facilitate anonymity. (Examples: Tor (darknet); Dark Wallet (darknet); Bitcoin Laundry (mixer)).

Mixer (laundry service, tumbler) is a type of anonymiser that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address. A mixer or tumbler sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address. The mixing service then "comingles" this transaction with other user transactions, such that it becomes unclear to whom the user intended the funds to be directed. (Examples: Bitmixer.io; SharedCoin; Blockchain.info; Bitcoin Laundry; Bitlaunder; Easycoin).

Tor (originally, The Onion Router) is an underground distributed network of computers on the Internet that conceals the true IP addresses, and therefore the identities of the network's users, by routing communications/transactions through multiple computers around the world and wrapping them in numerous layers of encryption. Tor makes it very difficult to physically locate computers hosting or accessing websites on the network. This difficulty can be exacerbated by use of additional tumblers or anonymisers on the Tor network. Tor is one of several underground distributed computer networks, often referred to as darknets, cypherspace, the Deep web, or anonymous networks, which individuals use to access content in a manner designed to obscure their identity and associated Internet activity.

Dark Wallet is a browser-based extension wallet, currently available on Chrome (and potentially on Firefox), that seeks to ensure the anonymity of Bitcoin transactions by incorporating the following features: auto-anonymiser (mixer); decentralised trading; uncensorable crowd funding platforms; stock platforms and information black markets; and decentralised market places similar to Silk Road.

Cold Storage refers to an offline Bitcoin wallet—i.e., a Bitcoin wallet that is not connected to the Internet. Cold storage is intended to help protect the stored virtual currency against hacking and theft.

Hot Storage refers to an online bitcoin wallet. Because it is connected to the Internet, hot storage is more vulnerable to hacking/theft than cold storage.

Local Exchange Trading System (LETS) is a locally organised economic organisation that allows members to exchange goods and services with others in the group. LETS use a locally created currency to denominate units of value that can be traded or bartered in exchange for goods or services. Theoretically, bitcoins could be adopted as the local currency used within a LETS. (Examples: Ithica Dollars; Mazacoin).

VIRTUAL CURRENCY SYSTEM PARTICIPANTS

An **exchanger (also sometimes called a virtual currency exchange)** is a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wires, credit cards, and other virtual currencies, and can be administrator-affiliated, non-affiliated, or a third party provider. Exchangers can act as a bourse or as an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts.

An **administrator** is a person or entity engaged as a business in **issuing** (putting into circulation) a centralised virtual currency, establishing the rules for its use; maintaining a central payment ledger; and who has the authority to **redeem** (withdraw from circulation) the virtual currency.

A **user** is a person/entity who obtains virtual currency and uses it to purchase real or virtual goods or services or send transfers in a personal capacity to another person (for personal use), or who holds the virtual currency as a (personal) investment. Users can obtain virtual currency in several ways. For example, they can (1) purchase virtual currency, using real money (from an exchanger or, for certain centralised virtual currencies, directly from the administrator/issuer); (2) engage in specific activities that earn virtual currency payments (e.g., respond to a promotion, complete an online survey, provide a real or virtual good or service); (3) with some decentralised virtual currencies (e.g., Bitcoin), self-generate units of the currency by "mining" them (see definition of miner, below),and receive them as gifts, rewards, or as part of a free initial distribution.

A **miner** is an individual or entity that participates in a decentralised virtual currency network by running special software to solve complex algorithms in a distributed proof-of-work or other distributed proof system used to validate transactions in the virtual currency system. Miners may be users, if they self-generate a convertible virtual currency solely for their own purposes, e.g., to hold for investment or to use to pay an existing obligation or to purchase goods and services. Miners may also participate in a virtual currency system as exchangers, creating the virtual currency as a business in order to sell it for fiat currency or other virtual currency.

Virtual currency wallet is a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency.

A wallet provider is an entity that provides a virtual currency wallet (i.e., a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency). A wallet holds the user's private keys, which allow the user to spend virtual currency allocated to the virtual currency address in the block chain. A wallet provider facilitates participation in a virtual currency system by allowing users, exchangers, and merchants to more easily conduct the virtual currency transactions. The wallet provider maintains the customer's virtual currency balance and generally also provides storage and transaction security. For example, beyond providing bitcoin addresses, the wallet may offer encryption; multiple key (multi-key) signature protection, backup/cold storage; and mixers. All Bitcoin wallets can interoperate with each other. Wallets can be stored both online ("hot storage") or offline ("cold storage"). (Examples: Coinbase; Multibit; Bitcoin Wallet).

In addition, various **other entities** may participate in a virtual currency system and may be affiliated with or independent of exchangers and/or administrators. These include web **administration service providers (a.k.a. web administrators)**; **third party payments senders** facilitating merchant acceptance; **software developers**; and **application providers** (some of the "other entities" listed in this paragraph may already fall into one of the categories above.). Applications and software development can be for legitimate purposes—e.g., to increase ease of merchant acceptance and customer payments or to respond to legitimate privacy concerns—or for illicit purposes—e.g., a mixer developer/operator can target illicit users with products designed to avoid regulatory and law enforcement scrutiny.

It must be emphasised that this list of participants is not exhaustive. Moreover, given the rapid development of virtual currency technologies and business models, additional participants could arise within virtual currency systems and pose potential AML/CFT risks.

Taxonomy of Virtual Currencies

	Centralised	**Decentralised**
Convertible	Administrator, exchangers, users; third-party ledger; can be exchanged for fiat currency. Example: WebMoney	Exchangers, users (no administrator); no Trusted Third-Party ledger; can be exchanged for fiat currency. Example: Bitcoin
Non-convertible	Administrator, exchangers, users; third-party ledger; cannot be exchanged for fiat currency. Example: World of Warcraft Gold	Does not exist

LEGITIMATE USES

Like other new payment methods, virtual currency has legitimate uses, with prominent venture capital firms investing in virtual currency start-ups. Virtual currency has the potential to improve payment efficiency and reduce transaction costs for payments and fund transfers. For example, Bitcoin functions as a global currency that can avoid exchange fees, is currently processed with lower fees/charges than traditional credit and debit cards, and may potentially provide benefit to existing online payment systems, like Paypal.[16] Virtual currency may also facilitate micro-payments, allowing businesses to monetise very low-cost goods or services sold on the Internet, such as one-time game or music downloads. At present, as a practical matter, such items cannot be sold at an appropriately low per/unit cost because of the higher transaction costs associated with e.g., traditional credit and debit. Virtual currency may also facilitate international remittances and support financial inclusion in other ways, as new virtual currency-based products and services are developed that may potentially serve the under- and un-banked. Virtual currency - notably, Bitcoin-may also be held for investment. These potential benefits need to be carefully analysed, including whether claimed cost advantages will remain if virtual currency becomes subject to regulatory requirements similar to those that apply to other payments methods, and/or if exchange fees for cashing out into fiat currency are factored in, and whether volatility, consumer protection and other factors[17] limit their potential for financial inclusion.

POTENTIAL RISKS

Convertible virtual currencies that can be exchanged for real money or other virtual currencies are potentially vulnerable to money laundering and terrorist financing abuse for many of the reasons identified in the 2013 NPPS Guidance. First, they may allow greater anonymity than traditional non-cash payment methods. Virtual currency systems can be traded on the Internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified.

Decentralised systems are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. There is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns. Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger may collect). It thus offers a level of potential anonymity impossible with traditional credit and debit cards or older online payment systems, such as PayPal.

Virtual currency's global reach likewise increases its potential AML/CFT risks. Virtual currency systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and funds transfers. In addition, virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them. This problem is exacerbated by the rapidly evolving nature of decentralised virtual currency technology and business models, including the changing number and types/roles of participants providing services in virtual currency payments systems. And importantly, components of a virtual currency system may be located in jurisdictions that do not have adequate AML/CFT controls. Centralised virtual currency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes. Decentralised convertible virtual currencies allowing anonymous person-to-person transactions may seem to exist in a digital universe entirely outside the reach of any particular country.

LAW ENFORCEMENT ACTIONS INVOLVING VIRTUAL CURRENCY

Law enforcement is already seeing cases that involve the abuse of virtual currency for money laundering purposes. Examples include:

LIBERTY RESERVE

In what is to date the largest online money-laundering case in history, in May 2013, the US Department of Justice charged Liberty Reserve, a Costa Rica-based money transmitter, and seven of its principals and employees with operating an unregistered money transmitter business and money laundering for facilitating the movement of more than 6 billion USD in illicit proceeds. In a coordinated action, the Department of the Treasury identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the US financial system.

Established in 2006, Liberty Reserve was designed to avoid regulatory and law enforcement scrutiny and help criminals distribute, store, and launder the proceeds of credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography by enabling them to conduct anonymous and untraceable financial transactions. Operating on an enormous scale, it had more than a million users worldwide, including more than 200 000 in the United States, and handled approximately 55 million transactions, almost all of which were illegal. It had its own virtual currency, Liberty Dollars (LR), but at each end, transfers were denominated and stored in fiat currency (US dollars).

To use LR currency, a user opened an account through the Liberty Reserve website. While Liberty Reserve ostensibly required basic identifying information, it did not validate identities. Users routinely established accounts under false names, including blatantly criminal names ("Russia Hackers," "Hacker Account," "Joe Bogus") and blatantly false addresses ("123 Fake Main Street, Completely Made Up City, New York"). To add a further layer of anonymity, Liberty Reserve required users to make deposits and withdrawals through recommended third-party exchangers—generally, unlicensed money transmitting businesses operating in Russia, and in several countries without significant governmental money laundering oversight or regulation at that time, such as Malaysia, Nigeria, and Vietnam. By avoiding direct deposits and withdrawals from users, Liberty Reserve evaded collecting information about them through banking transactions or other activity that would create a central paper trail. Once an account was established, a user could conduct transactions with other Liberty Reserve users by transferring LR from his or her account to other users, including front company "merchants" that accepted LR as payment. For an extra "privacy fee" (75 US cents per transaction), users could hide their Liberty Reserve account numbers when transferring funds, making the transfers completely untraceable. After learning it was being investigated by US law enforcement, Liberty Reserve pretended to shut down in Costa Rica but continued to operate through a set of shell companies, moving millions through their accounts in Australia, Cyprus, China, Hong Kong, Morocco, Russia, Spain and elsewhere.[18]

SILK ROAD

In September 2013, the US Department of Justice unsealed a criminal complaint charging the alleged owner and operator of Silk Road, a hidden website designed to enable its users to buy and sell illegal drugs, weapons, stolen identity information and other unlawful goods and services anonymously and beyond the reach of law enforcement, with narcotics trafficking, computer hacking, and money laundering conspiracies. The Justice Department also seized the website and approximately 173 991 bitcoins, worth more than USD 33.6 million at the time of the seizure, from seized computer hardware. The individual was arrested in San Francisco in October and indicted in February 2014; the investigation is ongoing.

Launched in January 2011, Silk Road operated as a global black-market cyber bazaar that brokered anonymous criminal transactions and was used by several thousand drug dealers and other unlawful vendors to distribute unlawful goods and services to over a hundred thousand buyers, a third of whom are believed to have been in the United States. It allegedly generated total sales revenue of approximately USD 1.2 billion (more than 9.5 million bitcoins) and approximately USD 80 million (more than 600 000 bitcoins) in commissions for Silk Road. Hundreds of millions of dollars were laundered from these illegal transactions (based on bitcoin value as of dates of seizure). Commissions ranged from 8 to 15 percent of total sales price.

Silk Road achieved anonymity by operating on the hidden Tor network and accepting only bitcoins for payment. Using bitcoins as the exclusive currency on Silk Road allowed purchasers and sellers to further conceal their identity, since senders and recipients of peer-to-peer (P2P) bitcoin transactions are identified only by the anonymous bitcoin address/account. Moreover, users can obtain an unlimited number of bitcoin addresses and use a different one for each transaction, further obscuring the trail of illicit proceeds. Users can also employ additional "anonymisers," beyond the tumbler service built into Silk Road transactions (see discussion below).

Silk Road's payment system functioned as an internal Bitcoin bank, where every Silk Road user had to hold an account in order to conduct transactions on the site. Every Silk Road user had at least one Silk Road Bitcoin address (and potentially thousands) associated with the user's Silk Road account, stored on wallets maintained on servers controlled by Silk Road. To make a purchase, a user obtained bitcoins (typically through a Bitcoin exchanger) and sent them to a Bitcoin address associated with his or her Silk Road account to fund the account. When a purchase was made, Silk Road transferred the user's bitcoins to an escrow account it maintained, pending completion of the transaction, and then transferred the user's / buyer's bitcoins from the escrow account to the vendor's Silk Road Bitcoin address. As a further step, Silk Road employed a "tumbler" for every purchase, which, as the site explained, "sen[t] all payments through a complex, semi-random series of dummy transactions ... --making it nearly impossible to link your payment with any [bit]coins leaving the site."[19]

WESTERN EXPRESS INTERNATIONAL

An eight-year investigation of a multinational, Internet-based cybercrime group, the Western Express Cybercrime Group, resulted in convictions or guilty pleas of 16 of its members for their role in a global identity theft/cyberfraud scheme. Members of the cybercrime group interacted and communicated primarily through Internet "carding" web sites devoted to trafficking in stolen credit card and personal identifying information and used false identities, anonymous instant messenger accounts, anonymous email accounts, and anonymous virtual currency accounts to conceal the existence and purpose of the criminal enterprise; avoid detection by law enforcement and regulatory agencies; and maintain their anonymity.

The criminal enterprise was composed of vendors, buyers, cybercrime services providers, and money movers located in numerous countries, ranging from Ukraine and throughout Eastern Europe to the United States. The vendors sold nearly 100 000 stolen credit card numbers and other personal identification information through the Internet, taking payment mostly in e-Gold and WebMoney. The buyers used the stolen identities to forge credit cards and purchase expensive merchandise, which they fenced (including via reshipping schemes), committing additional crimes, such as larceny, criminal possession of stolen property, and fraud, and generating about USD 5 million in credit card fraud proceeds. The cybercrime services providers promoted, facilitated, and aided in the purchase, sale and fraudulent use of stolen credit card numbers and other personal identifying information by providing computer services to the vendors and the buyers. The money mover laundered the cybercrime group's illicit proceeds in a variety of high-tech ways, moving more than USD 35 million through various accounts.

The hub of the entire operation was Western Express International, Inc., a New York corporation based in Manhattan that operated as a virtual currency exchanger and unregistered money transmitter to coordinate and facilitate the Internet payment methods used by the criminal enterprise, and to launder the group's proceeds. One of the largest virtual currency exchangers in the United States, Western Express International exchanged a total of USD 15 million in WebMoney and USD 20 million in e-Gold for the cybercrime group and used banks and traditional money transmitters to move large sums of money. It also provided information and assistance through its websites (including Dengiforum.com and Paycard2000.com) on ways to move money anonymously and to insulate oneself from reporting requirements.

Western Express International and its owner/operator, a Ukrainian national, plead guilty in February 2013 in New York State to money laundering, fraud, and conspiracy offenses. (In February 2006, Western Express was also indicted for running an illegal check cashing/wire transfer service.) Three other defendants were convicted after trial in June 2013; several more plead guilty in August 2009. Two indicted defendants remain fugitives. The investigation was conducted jointly by the US Secret Service and the Manhattan (New York County) District Attorney's Office and was successfully prosecuted by the Manhattan District Attorney's Office.

NOTES

[1] The first draft of this paper was prepared jointly by Australia, Canada, Russia, the United Kingdom and the United States for the FATF meetings in February 2014. After that all delegations were invited to provide comments on the draft with a view to adopting a final paper at the next meeting. Comments were received from 10 delegations, and these have been taken into account in preparing this revision.

[2] "Bitcoin" (capitalised) refers to both the open source software used to create the virtual currency and the peer-to-peer (P2P) network formed as a result; "bitcoin" (lowercase) refers to the individual units of the virtual currency.

[3] It should also be noted that some observers, including former US Federal Reserve Chairman Alan Greenspan, Nout Wellink, a former President of the Dutch Central Bank, and Nobel Laureate economist Robert Shiller, maintain that virtual currency is a passing fad or bubble, akin to Tulipmania in 17th Century Netherlands.

[4] Virtual currency is a complex subject that implicates not only AML/CFT issues, but also other regulatory matters, including consumer protection, prudential safety, tax and soundness regulation, and network IT security standards. The proposed vocabulary is thus relevant across a number of complementary regulatory jurisdictions. Adoption of consistent terms and a common conceptual understanding of virtual currency by all relevant government entities is important to avoid duplicating efforts and/or working at unintended cross purposes, and facilitates the capacity of governmental authorities to leverage their various perspectives and areas of expertise in order to most effectively identify and address relating to virtual currencies.

[5] **Digital representation** is a representation of something in the form of digital data—i.e., computerised data that is represented using discrete (discontinuous) values to embody information, as contrasted with continuous, or analog signals that behave in a continuous manner or represent information using a continuous function. A physical object, such as a flash drive or a bitcoin, may contain a digital representation of virtual currency, but ultimately, the currency only functions as such if it is linked digitally, via the Internet, to the virtual currency system,

[6] Legal tender status does not necessarily require an entity or individual to accept payment in a particular type of legal tender. For example, in many jurisdictions, a private business, person, or organisation is free to develop internal policies on whether or not to accept the jurisdiction's physical currency or coins (cash) as payment for goods and/or services.

[7] This definition differs from that offered in 2012 by the European Central Bank (ECB), which defined virtual currency "as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community" ECB, *Virtual Currency Schemes* (October 2012), p. 6. The ECB recognised on p.13 of its report that its "definition may need to be adapted in future if fundamental characteristics change." Its definition now appears too limited, since math-based, decentralised virtual currencies like Bitcoin are not issued and controlled by a central developer, and some jurisdictions (e.g., the United States, Sweden, and Thailand) now regulate virtual currencies.

[8] This categorisation differs from the ECB's three-part classification, which divides virtual currencies into three types: "Type 1 . . . refer[s] to closed virtual currency schemes . . . used in an online game. Type 2 . . . [refers to] schemes [that] have a unidirectional flow (usually an inflow), i.e. there is a conversion rate for purchasing the virtual currency, which can … be used to buy virtual goods and services . . . (and exceptionally also … real goods and services) . . . Type 3 [refers to] schemes . . .[with] bidirectional flows, i.e. the virtual currency . . . acts like any . . . convertible [real] currency, with . . . [buy and sell] exchange rates . . . [and] can . . . be used to buy [both] virtual . . . [and] real goods and services." ECB *Virtual Currency Schemes,* p. 6. This discussion paper adopts a simpler, bifurcated classification because at present, only (fully) convertible virtual currencies that can be used to move value into and out of the formal financial sector present significant AML/CFT risks. This is because money laundering requires: Conversion or transfer (of illicit funds); concealment or disguise of the source/origin (of illicit funds); or acquisition/possession/use (of illicit funds).

[9] Some convertible virtual currencies can be exchanged directly through the issuing administrator (directly exchanged); others must be exchanged through a virtual currency exchanger (third-party exchanged).

[10] For example, WebMoney is a virtual currency because “valuables” (assets) are transferred and stored in the form of a non-fiat currency, The units of measurement of the valuables' property rights stored by the guarantor are WebMoney Title Units (WM) of the corresponding type. http://wmtransfer.com/eng/about/

[11] For example, despite such deterrence measures, several exchanges allow blackmarket conversion of World of Warcraft Gold.

[12] A third-party is an individual or entity that is involved in a transaction but is not one of the principals and is not affiliated with the other two participants in the transaction—i.e., a third party functions as a neutral entity between the principals (e.g., sender and receiver, buyer and seller) in a business or financial transaction. The third party's involvement varies with the type of business or financial transaction. For example, an online payment portal, such as PayPal, acts as a third party in a retail transaction. A seller offers a good or service; a buyer uses a credit or debit card entered through the PayPal payment service; and the trusted third party completes the financial transfer. Similarly, in a real estate transaction, a third-party escrow company acts as a neutral agent between the buyer and seller, collecting the documents from the seller and money from the buyer that the two principals need to exchange to complete the transaction.

[13] Distributed is a term of art that refers to an essential feature of decentralised math-based virtual currencies: transactions are validated by a *distributed* proof-of-work system. Each transaction is *distributed* among a network of participants who run the algorithm to validate the transaction.

[14] Apart from the initial creation and issuance of ripple coins (RXP), Ripple operates as a decentralised virtual currency. Ripple’s founders created all 100 billion ripple coins and retained 20 billion of them, with the remainder to be distributed by a separate entity, Ripple Labs. However, all transactions are verified by a decentralised computer network, using Ripple’s open source protocol, and recorded in a shared ledger that is a constantly updated database of Ripple accounts and transactions.

[15] In 2140, the block award will cease to be available and miners will be rewarded only by transaction fees.

[16] For example, PayPal is actively looking at accepting and clearing bitcoins on the PayPal platform, and JP Morgan Chase has filed a US patent application for an online electronic payments system using a math-based virtual currency protocol that would enable users to make anonymous payments without providing an account number or name, with the virtual currency to be stored on JPMC computers and verified through a shared log, much like the ‘block chain’ in the bitcoin system.

[17] For instance, it remains to be seen whether virtual currency systems can provide a pathway to other financial services, like credit and insurance.

[18] The Liberty Reserve investigation and takedown involved law enforcement action in 18 countries and jurisdictions, including Costa Rica; the Netherlands; Spain; Morocco; Sweden; Switzerland; Cyprus; Australia; China; Hong Kong, China; Norway; Latvia; Luxembourg; the United Kingdom; Russia; Canada; and the United States to restrain criminal proceeds, forfeit domain names, and seize servers.

[19] The Silk Road investigation involved multiple US law enforcement agencies, led the Federal Bureau of Investigation’s (FBI’)s New York Special Operations and Cyber Division, and the Drug Enforcement Administration’s (DEA’s) New York Organized Crime Drug Enforcement Strike Force (comprised of agents and officers of DEA, the Internal Revenue Service (IRS), the New York City Police Department, US Immigration and Customs Enforcement’s (ICE) Homeland Security Investigations (HSI), the New York State Police, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the US Secret Service, the US Marshals Service, Office of Foreign Assets Control (OFAC), and NY Department of Taxation), with assistance and support of the ICE-HIS Chicago field office, the Department of Justice’s Computer Crime and Intellectual Property and Asset Forfeiture and Money Laundering Sections, the United States Attorney’s Office for the Southern District of New York, and foreign law enforcement partners, particularly the Reykjavik Metropolitan Police of the Republic of Iceland and the French Republic’s Central Office for the Fight Against Crime Linked to Information Technology and Communication.

BIBLIOGRAPHY AND SOURCES

FATF (2013), FATF *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services,* FATF, Paris
www.fatf-gafi.org/topics/fatfrecommendations/documents/rba-npps-2013.html

Popper, N. (2013), "In Bitcoin's Orbit: Rival Virtual Currencies vie for Acceptance", in *New York Times, Dealb%k,* (Nov. 24, 2013) http://dealbook.nytimes.com/2013/11/24/in-bitcoins-orbit-rival-virtual-currencies-vie-for-acceptance/?_r=0, accessed June 2014.