JOURNAL OF ANTI-CORRUPTION LAW

2019 Volume 3 Number 1 Pages 1 - 15

CRYPTOLAUNDERING: ANTI-MONEY LAUNDERING REGULATION OF VIRTUAL CURRENCY EXCHANGES*

Stefan Mbiyavanga**

ABSTRACT

Ten years on since their invention, virtual currencies are here to stay. However, virtual currencies come with money laundering risks. This paper discusses anti-money laundering regulation for virtual currency intermediaries, by showcasing and comparing regulatory models at the national and international levels.

It is found that the anti-money laundering regulation for virtual currencies — more than being merely "nice to have" — carries considerable potential in the fight economic crime. Where financial intermediaries engaged in virtual currencies are required to gather the full spectrum of information needed to identify their customers and the source of funds, virtual currencies become much less attractive to money launderers than traditional fiat money systems. Furthermore, anti-money laundering regulation means that supervisory and investigatory authorities can identify and act against money launderers and other delinquents.

1 INTRODUCTION

Virtual currencies, such as Bitcoin, as well as the technology that supports them, have created new options for the delivery of financial services. However, the rapid pace of innovations in virtual currency technology — as well as in the Fintech (Finance and Technology) sector in general — leaves regulators grappling to design adjusted legal frameworks. Notwithstanding all the excitement and hope, the risk of money launderers abusing these technologies on a large scale is serious. For instance, the United States Department of Justice reports that corrupt public

* This is a revised version of a paper read by the author at the *Economic Crime and Cybercrime Conference (ECCC)*, University of the Western Cape, 5 October 2018.

** MLaw, Doctoral Candidate (University of Basel, Switzerland).
Email: s.mbiyavanga@unibas.ch.

officials already have begun to launder proceeds of corruption through virtual currencies.[1]

In the light of the fast-moving nature of the above-mentioned issues, this paper seeks to understand the relationship between virtual currencies and the laundering of illicit assets, with special consideration being given to the laundering of proceeds of economic crimes such as corruption. To this end, the paper considers and compares which virtual currency operators are bound by anti-money laundering duties pursuant to the regulatory frameworks of South Africa, the United States and Switzerland.

A brief introduction to virtual currencies is presented in §2. Thereafter, §3 identifies a number of money laundering risks associated with virtual currencies and §4 discusses regulatory responses to them. On the international level, steps taken by the Financial Action Task Force (FATF) and the European Union (EU) are examined. Finally, the approaches taken by South Africa, the United States and Switzerland are contrasted.

2 VIRTUAL CURRENCIES

Virtual currencies have been described as a "digital representation of value".[2] Their legal classification remains controversial, however.[3] As of October 2018, roughly 2000 virtual currencies are in circulation.[4] Most of them resemble the well-known Bitcoin. Accordingly, §2.1 introduces the workings of Bitcoin to provide an idea of the way in which virtual currencies function. Thereafter, §2.2 explains virtual currency exchanges as the main entry and exit points to the virtual currency economy.

2.1 The Workings of Bitcoin

Bitcoin is a decentralised virtual currency. The distinctive feature of decentralised virtual currencies — also called cryptocurrencies — is that they are not issued by a

1 US Department of Justice Press Release (26 July 2017) *Russian National and Bitcoin Exchange Charged in 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds From Hack of Mt Gox*, available at https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged (visited 9 August 2018).

2 EU (30 May 2018) Fifth Anti-Money Laundering Directive 2018/843 (5AMLD) at 9. See also FATF Recommendations (2012: updated October 2018) "Glossary: Virtual Assets".

3 See, for example, Yermack D (2015) "Is Bitcoin a Real Currency? An Economic Appraisal" in Lee D (ed) *The Handbook of Ditigal Currency* New York: Elsevier at 31 *et seq*.

4 Coinmarketcap.com (undated) "List of All Cryptocurrencies", available at https://coinmarketcap.com/all/views/all/ (visited 21 September 2018).

central entity and do not depend on a single administrator.[5] Instead, Bitcoin is based on an online network. Within this network, users have one or any number of electronic wallets listing their Bitcoin balance and transaction history. The function of the wallets is similar to that of a bank account. However, their content is visible to the public.

In order to open the wallet, users must know their private key. Besides giving access to the wallet, the private key can generate public addresses through cryptographic algorithms. The user may communicate public addresses to other users wishing to send Bitcoins. A transaction usually requires no more than a few seconds. Transactions are registered in the blockchain, which is a public online record of all previous transactions and the public addresses of the parties involved.[6] The manner in which blockchain technology has been put to use by the developers of Bitcoin is a major innovation. Information stored on the Bitcoin blockchain is permanent and immutable, which is vital for the creation and upholding of trust.[7]

The entries on the blockchain are pseudo-anonymous. The recorded public address is nothing more than a hashed code, that is, a string of numbers and letters which does not contain any indication of the user's identity or location. Also, users may repeat the process of generating new public addresses with their private key as many times as they like. Thereby, the task of linking transactions recorded on the blockchain to individual wallets is made more complicated for the outsider. It is possible, however, to associate the users' Internet Protocol (IP) addresses with Bitcoin transactions. In order to prevent this, a user may enter the Bitcoin network via the Onion Router (TOR).[8] TOR hides online activity by encapsulating the user's identity in layers of encryption, analogous to layers of an onion.[9]

5 However, centralised virtual currencies generally are issued, monitored and operated by a single entity. In this paper, the term virtual currency will be used to refer to both kinds, and cryptocurrencies will be used to indicate to decentralised virtual currencies.

6 Nakamoto S (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System", available at https://bitcoin.org/bitcoin.pdf (visited 9 August 2018).

7 Lumb R (9 September 2016) "Downside of Bitcoin: A Ledger That Can't Be Corrected" *New York Times*, available at https://www.nytimes.com/2016/09/10/business/dealbook/downside-of-virtual-currencies-a-ledger-that-cant-be-corrected.html (visited 9 August 2018).

8 Goldschlag D *et al* (1999) "Onion Routing for Anonymous and Private Internet Connections", available at https://www.onion-router.net/Publications/CACM-1999.pdf (visited 11 October 2018).

9 Khan I (2016) "The Virtual Future of Money Laundering" *Fraud Magazine*, available at http://www.fraud-magazine.com/article.aspx?id=4294993747 (visited 11 October 2018).

From the user's point of view, Bitcoin is generally a very safe payment network. It is virtually impossible to re-engineer a private key from a public address, as multiple, irreversible algorithms shield the private key. Also, due to the verification process inherent in the Bitcoin system (so-called "mining"), Bitcoins are almost impossible to forge.[10]

2.2 Virtual Currency Exchanges

In order to buy, sell and trade virtual currencies for fiat money, goods, services or other virtual currencies, many users turn to virtual currency exchanges. Commonly, virtual currency exchanges are centralised entities.[11] While the structure of operations of virtual currency exchanges can reach spectacular complexities,[12] there are fundamentally two types of virtual currency exchanges: custodial and non-custodial exchanges.

In a custodial exchange, the asset is transacted "through" the exchange, which acts as a custodial intermediary.[13] In other words, the exchange itself is party to the transaction, as it purchases virtual currency from the seller and sells it to the buyer. In many custodial exchanges, users first must deposit fiat or virtual currency in booking accounts to fund later transactions.

Non-custodial exchanges, by contrast, merely offer a platform for buyers and sellers to meet and match. The transactions in non-custodial exchanges operate exclusively on a peer-to-peer basis.

10 See KPMG (June 2018) "Clarity on Financial Crime in Banking", available at https://home.kpmg.com/ch/en/home/insights/2018/06/clarity-on-financial-crime-in-banking.html (visited 9 August 2018).

11 However, several reports indicate that decentralised exchanges are being developed. See, for instance, Young J (11 August 2018) "Decentralised Crypto Exchanges Can Solve Fake Volumes and Malpractices" *Forbes*, available at https://www.forbes.com/sites/youngjoseph/2018/08/11/waves-ceo-decentralized-crypto-exchanges-can-solve-fake-volumes-and-malpractices/#782b152277d0 (visited 7 August 2019).

12 See, for example, the case of *Liberty Reserve* as described in Mabunda S (2018) "Cryptocurrency: The New Face of Cyber Money Laundering" *International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)* at 4.

13 Van Valkenburgh P (2017) *The Bank Secrecy Act, Cryptocurrencies, and New Tokens* Coin Center Report at 11, available at https://coincenter.org/entry/aml-kyc-tokens (visited 9 August 2018).

Crack Down on Exchanges

Several virtual currency exchanges have optimised their structures to allow users to transact virtual currencies undetected and grant them the highest degree of anonymity possible. Law enforcement actions against such virtual currency exchanges have at times led to huge fines and drastic penalties.

A recent investigation against the BTC-e exchange, for example, has resulted in a fine of over US$ 110 million for failure to comply with US anti-money laundering (AML) regulation. BTC-e was one of the world's most widely used virtual currency exchanges. From 2011 to 2017, it exchanged virtual currencies for a range of fiat currencies as well as other virtual currencies for about 700 000 users.[14] BTC-e lacked any sort of internal control, customer identification or other AML programme.[15] Cybercriminals — and also corrupt public officials — quickly started using BTC-e to store, distribute and launder their proceeds.[16]

At the time of writing, the suspected operator of the exchange faces a 21-count criminal indictment in the United States.[17]

3 MONEY LAUNDERING RISKS

Many commentators have rained down harsh criticism upon cryptocurrencies and predicted an aggravation of money laundering activities through cyberspace.[18] This section will look at the above-mentioned aspects of virtual currencies from a money laundering perspective and seek to identify the benefits and drawbacks which virtual currencies offer to those seeking to launder money.

Money laundering is understood generally as a three-step process of giving assets tainted by crime a lawful appearance. The three steps are: the placement of illegal assets in the legal financial system; the layering of the assets, or the obfuscation of their illicit origin; and the re-integration of the laundered assets into the legal economy.[19]

14 FinCEN (26 July 2017) *Assessment of Civil Money Penalty in BTC-E a/k/a Canton Business Corporation and Alexander Vinnik* No 2017-03 at 2.

15 FinCEN (26 July 2017) at 4.

16 FinCEN (26 July 2017) at 8; Department of Justice (2017).

17 Department of Justice (2017). See §4.2.2 below for an explanation of what a money service business is.

18 The head of the US Central Bank, for instance, stated that "cryptocurrencies are great if you're trying to hide or launder money". See Shi M (18 July 2018) "Fed Chair: Cryptocurrencies Are 'Great' For Money Laundering" *Coindesk*, available at https://www.coindesk.com/fed-chair-cryptocurrencies-are-great-for-money-laundering/ (visited 20 July 2017).

19 Pieth M (2016) *Wirtschaftsstrafrecht* Basel: Helbing Lichtenhahn Verlag at 190.

In the context of cryptocurrencies, the three-step scheme may play out as follows. The exchange of a tainted asset for cryptocurrency at a virtual currency exchange constitutes the first step (placement).[20] In recent times, the large and regulated custodial exchanges have begun to require detailed personal information for account verification. However, launderers may make use of "straw men" or intermediaries with clean records to shield their identities.[21] There is also an online market for fully verified accounts.[22]

Once a suitable exchange is found, the tainted assets may be transferred in the form of bank transfers or in kind.[23] However, where a launderer seeks to place large amounts of dirty proceeds, scalability issues may emerge. The cryptocurrency market still is rather small and a massive purchase is likely to trigger suspicions. If the trading volume of Bitcoin or another cryptocurrency increases significantly, however, economic criminals soon may find it easier to make extensive purchases without being noticed.

Having converted the tainted asset into virtual currency, the possibilities for the layering of the illicit virtual currency are plenty. Such layering may take place in form of a series of transactions between different wallets controlled by the launderer or affiliated persons. Transactions on the Bitcoin network easily cross national borders and clear at a much higher speed than, for instance, via the correspondent banking network. The creation of new wallets takes mere seconds and each wallet can generate new public addresses for every transaction.

Furthermore, technically able launderers are able to design software that automatically obscures the electronic paper trail. For instance, anonymising services, called mixers or tumblers, can execute immense volumes of transactions in irregular intervals and between large numbers of wallets. They re-route transactions through complex, semi-random series of dummy transactions and commingle incoming transactions with many others. Of course, these mixing services are a highly useful feature for launderers. Fanusie & Robinson have found

20 See Swiss Federal Council (25 June 2014) *Report on Virtual Currencies in Response to the Schwaab (13.3687) and Weibel (13.4070) Postulates* at 19, available at https://www.news.admin.ch/NSBSubscriber/message/attachments/35355.pdf (visited 9 August 2018).

21 Fruth J (13 February 2018), "Crypto-Cleansing: Strategies to Fight Digital Currency Money Laundering and Sanctions Evasion" *Reuters*, available at https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I (visited 11 October 2018).

22 Fruth (13 February 2018).

23 See KPMG (June 2018) at 28.

evidence that these services are receiving disproportionately high numbers of illicit transactions.[24]

In addition, the launderer might acquire so-called privacy coins. Privacy coins are a type of cryptocurrency specifically designed to provide the user especially far-reaching anonymity. They do not provide a public record of previous transactions. *Monero*, for example, operates a blockchain that encrypts the recipient's public address and automatically creates false addresses to obscure the particulars of the real sender.[25] At this juncture, these privacy coins must be considered niche products which are used mostly by people engaged in online trade in illegal drugs or other petty crimes. For anyone looking to layer the proceeds of large-scale (economic) crime, however, they are not very suitable yet.

In the third and final step of the money laundering cycle (re-integration), the now unsuspicious virtual currency is converted into fiat money again.[26] What is more, considering that the number of businesses accepting virtual currencies is rising, re-conversion to fiat may not be required and launderers soon may be able to purchase real estate, cars or luxury assets with cryptocurrency directly.[27]

4 REGULATION

Regulators at the national and international levels started to address virtual currencies in the early 2010s already. Below, §4.1 provides an overview of regulatory responses to virtual currencies at the international level. Thereafter, §4.2 examines the South African, the US and the Swiss approaches to the regulation of virtual currencies.

4.1 International Regulation

In 2015, the Financial Action Task Force (FATF) — an inter-governmental anti-money laundering — established an important blueprint by identifying and discussing recommendations for national regulators wishing to address virtual

24 Fanusie Y & Robinson T (2018) "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services" at 10, available at https://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf (visited 9 August 2018).

25 Kharif O (2 January 2018) "The Criminal Underworld Is Dropping Bitcoin for Another Currency" *Bloomberg*, available at: https://www.bloomberg.com/news/articles/2018-01-02/criminal-underworld-is-dropping-bitcoin-for-another-currency (visited 24 July 2018).

26 See Swiss Federal Council (25 June 2014) at 19.

27 See Swiss Federal Council (25 June 2014) at 20.

currencies.[28] In a report, the FATF identified convertible virtual currencies, that is, virtual currencies that can move value into and out of fiat currencies and thereby the regulated financial system, to be the main money laundering risks.[29] Hence, it recommended focusing AML measures on virtual currency exchanges and other gatekeepers between fiat and virtual currencies.[30] It reasoned that criminals would want to convert virtual currencies to fiat currencies at some point — an assumption that may no longer hold true in the medium to long run since, as noted above, the number of merchants accepting virtual currencies as payment continues to increase.

In October 2018, the FATF updated its guidance to include "virtual assets" and "virtual asset service providers".[31] It saw an "urgent need" for member states to introduce AML policies proportional to risks posed by virtual currencies.[32] The term "virtual asset service provider" is given a very broad scope of application and encompasses virtual currency exchanges. The definition includes natural and legal persons who professionally conduct one or more of a number of activities,

28 FATF (2015) *Guidance for a Risk-Based Approach to Virtual Currencies*, available at http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html (visited 11 July 2018).
In March 2018, the FATF announced that it was considering reviewing its guidance, due to the speed with which cryptocurrencies had evolved over the past three years. See FATF (March 2018) *FATF Report to the G20 Finance Ministers and Central Bank Governors* at 7, available at www.fatf-gafi.org/media/fatf/documents/FATF-G20-FM-CBG-March-2018.pdf (visited 23 July 2017). See also European Parliament (2018) *Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses* at 46, available at http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf (visited 23 July 2018).

29 FATF (2015) at 6.

30 FATF (2015) at 4 & 6.
In 2014 the European Banking Authority recommended obligating exchangers to collect and verify information allowing for the identification of clients. See European Banking Authority (4 July 2014) *EBA Opinion on 'Virtual Currencies'*, available at https://www.eba.europa.eu/.../EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (visited 23 July 2018).
The US regulator adopted the same principle in 2013 already. See §4.2.2 below.

31 Recommendation 15 of the FATF Recommendations (2012: updated October 2018).

32 FATF (19 October 2018) "Regulation of Virtual Assets", available at http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html (visited 17 February 2019). See also Cliffe Dekker Hofmeyr (5 December 2018) "Towards the Regulation of Virtual Currencies?" *Corporate & Commercial Alert*, available at https://www.cliffedekkerhofmeyr.com/en/news/publications/2018/Corporate/corporate-and-commercial-alert-5-december-towards-the-regulation-of-virtual-currencies.html (visited 17 February 2018).

including exchanges between virtual and fiat currencies, inter-virtual currency exchanges or safekeeping of virtual currencies.[33]

Earlier in 2018, the European Union (EU) had introduced regulation of virtual currencies in its Fifth Anti-Money Laundering Directive (5AMLD).[34] Pursuant to 5AMLD, Member States must introduce legislation subjecting "providers engaged in exchange services between virtual currencies and fiat currencies" to AML duties.[35] However, contrary to the approach taken by the FATF, inter-virtual currency transactions are not covered, which omission has been criticised.[36]

5AMLD obligates Member States to license or register virtual currency exchanges.[37] In order to facilitate the work of Financial Intelligence Units (FIUs), the EU suggests granting them access to information to associate virtual currency addresses to the identity of the owner of virtual currency.[38]

4.2 National Regulation

In response to the oft-discussed money laundering risks that virtual currencies pose, a number of countries around the world have regulated them.[39] However, several countries, including South Africa, have excluded virtual currencies explicitly from the purview of regulation. The ensuing sections will compare the approaches taken by South Africa, the USA and Switzerland.

4.2.1 South Africa

In South Africa, the South African Reserve Bank (SARB) is responsible for regulating virtual currencies.[40] However, in 2014 it stated that it does not intend to "oversee, supervise or regulate" virtual currencies and that all activities related to them would be performed at the user's own risk.[41] While the SARB noted that virtual

33 FATF Recommendations (2012: updated October 2018) "Glossary: Virtual Asset Service Provider".
34 EU 5AMLD at 9.
35 EU 5AMLD at 36.
36 Fanusie & Robinson (2018) at 11; European Parliament (2018) at 46.
37 EU 5AMLD at 82.
38 EU 5AMLD at 7.
39 See European Parliament (2018) at 47.
40 Cliffe Dekker Hofmeyr (5 December 2018) at 3.
41 SARB (12 March 2014) *Position Paper on Virtual Currencies* No: 18/5/2-2014, available at https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf (visited 9 August 2018); See also National Treasury (18 September 2014) "User Alert: Monitoring of Virtual Currencies" at 1, available at *www.treasury.gov.za* (visited 9 August 2018).

currencies need to be monitored further, it was of the opinion that they do not pose systemic threats and therefore do not require regulation.[42]

With the introduction of the positive obligation to regulate exchanges by the FATF in October 2018, the SARB could no longer persist with its "study and monitor" approach.[43] Furthermore, Fintech industry entities active in South Africa have called for regulation and fraud scandals have harmed investors.[44] The SARB since has recognised that risks regarding virtual currencies and other blockchain-based technologies are increasing. At the time of writing, different regulatory models are being discussed.[45]

It is submitted that regulation of virtual currency exchanges is more than merely "nice to have" or a tool to facilitate competition or create clearer market conditions. From the criminal law perspective, AML regulation also means that there is a preventive framework in place enabling supervisory authorities to identify and act against money launderers and other delinquents.

4.2.2 United States

US anti-money laundering law is found primarily in the Bank Secrecy Act (BSA) of 1970. The main addressees of the BSA are financial institutions. These include banks, securities dealers and brokers, as well as so-called money service businesses.[46] Money service businesses are entities doing business "wholly or in substantial part" in the United States and falling within one of the designated subcategories.[47] One such subcategory comprises money transmitters. A money transmitter is a person or company providing money transmission services, which is defined as:

> the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.[48]

42 SARB (12 March 2014) at 12.
43 See Cliffe Dekker Hofmeyr (5 December 2018) at 3.
44 See Toyana M (25 May 2018) "South Africa Investigates $80 Million Bitcoin Scam" *Reuters,* available at https://www.reuters.com/article/us-safrica-crime-bitcoin-idUSKCN1IQ162 (visited 1 September 2019); Intergovernmental Fintech Working Group (April 2018) *Fintech Workshop* at 9, available at https://www.cnandco.com/wp-content/uploads/2018/07/IFWG-Report-2018.pdf (visited 1 September 2019).
45 Intergovernmental Fintech Working Group (April 2018) at 8 & 39.
46 31 CFR §1010.100 para (t)(3).
47 FinCEN (26 July 2017) at 2.
48 31 CFR §1010.100 para (t)(5)(i)(A).

Money transmitters are obligated to register with the Financial Crimes Enforcement Network (FinCEN), the US Treasury Department's division in charge of AML law. Furthermore, money transmitters must evaluate money laundering risks in their business operations and implement a compliance programme to mitigate those risks. In addition, they must adhere to recordkeeping, reporting and transaction monitoring requirements.[49]

FinCEN issued a Guidance on virtual currencies in 2013 in which it sought to clarify whether virtual currency exchanges are to be considered money transmitters.[50] The Guidance distinguished "real currency" from "virtual currency".[51] While real currency is all money that has the status of legal tender in the country of issue, virtual currency does not have legal tender status.[52] Virtual currencies which have an equivalent in real currency and those that may be used as a "substitute" are deemed convertible virtual currencies.[53]

A virtual currency exchange is defined in the Guidance as any "person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency".[54] Unfortunately, the Guidance does not state what it means by "engaged as a business". Accordingly, it is not clear at what volume or size an entity becomes subject to BSA obligations.

When subsuming the definition of a virtual currency exchange under the definition of a money transmission service, FinCEN found that any exchange who "(1) accepts and transmits convertible virtual currency or (2) buys or sells convertible virtual currency for any reason *is* a money transmitter" and, therefore, is subject to all relevant BSA obligations.[55] However, FinCEN then adds several exceptions to this rule. One such exception is the case in which a *bona fide* service provider — much like a *bureau de change* — exchanges virtual currency for another (virtual) currency in a transaction involving only one counterparty (hereafter

49 FinCEN (27 October 2014) *Administrative Ruling FIN 2014-R012* at 7, available at: https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R012.pdf (visited 18 August 2019).

50 FinCEN (2013) *Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies* (FIN-2013-G001). In May 2019, FinCEN issued a new guidance, available at https://www.fincen.gov/news/news-releases/new-fincen-guidance-affirms-its-longstanding-regulatory-framework-virtual (visited 18 August 2019).

51 FinCEN (2013) at 1.

52 FinCEN (2013) at 1.

53 FinCEN (2013) at 1.

54 FinCEN (2013) at 2.

55 In its definition of money transmission, FinCEN does not differentiate between real currencies and virtual currencies. See FinCEN (2013) at 3.

referred to as virtual exchange offices).[56] Here, FinCEN does not consider that the BSA's AML regulations apply.[57] This view is in conformity with the BSA's definition of "money transmission service", as cited above, which only extends to entities which transmit assets to "another location or person".[58]

4.2.3 Switzerland

In Switzerland, the key AML duties are to be found in the Anti-Money Laundering Act (AMLA) of 1997. AMLA contains AML obligations such as the duty to identify the beneficial owner in terms of a risk-based approach, the duty to file suspicious transaction reports where necessary, and the duty to become a member of a self-regulatory organisation or to submit to supervision by the Swiss Financial Market Supervisory Authority (FINMA).[59]

AMLA applies to financial intermediaries. Financial intermediaries include natural and legal persons "who on a professional basis … provide services related to payment transactions".[60] The Anti-Money Laundering Ordinance (AMLO) of 2015 defines "payment transactions" as including:

> the transfer of assets through the acceptance of cash, precious metals, virtual currencies … and the payout of a corresponding sum in cash, precious metals or virtual currencies.[61]

Accordingly, virtual currency exchanges may fall within the sphere of AMLA where they operate on a professional basis.

Swiss law contains a two-fold approach to the determination of whether a person operates "on a professional basis". To begin with, it must be assessed whether the person is engaged in money transmitting or currency exchange.[62] Money transmitting is understood as the practice by which the sender's money is transferred to a new owner. In Switzerland, money transmitting virtually always is considered to be conducted on a professional basis, which is explained by the

---

56 FinCEN (2013) at 6; See also Middlebrook S & Hughes S (2014) "Regulating Cryptocurrencies in the United States: Current Issues and Future Directions" 40(2) *William Mitchell Law Review* 814-848 at 829.

57 FinCEN (2013) at 6.

58 See also FinCEN (27 October 2014) at 3.

59 Article 3 *et seq* of AMLA.

60 Article 2(3)(b) of AMLA.

61 Article 4(2)(a) of AMLO. AMLO is published only in German, French and Italian. The unofficial English translation used here was found in KPMG (2016) "Ordinance on Combating Money Laundering and Terrorist Financing, Version as of 1 January 2016", available at https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/ch-ordinance-combating-money-laundering-terrorist-financing-en.pdf (visited 13 August 2018).

62 Swiss Federal Council (25 June 2014) at 15.

higher exposure to the risk of money laundering inherent in this type of service.[63] Further, the issue of currency exchange, which refers to the activity of a virtual exchange office, has to be considered.[64] Currency exchange is deemed to be carried out on a professional basis only where the service provider:

- achieves a gross revenue in excess of 50 000 Swiss francs;
- takes up business relationships with more than 20 parties more than once a year;
- has unlimited control of third-party funds in excess of five million Swiss francs; or
- transacts in more than two million Swiss francs per year.[65]

In practice, virtual exchange offices automatically are considered money transmitters, and thus financial intermediaries, unless they can ensure beyond a doubt that their transactions involve only one counterparty.[66] A banking licence generally is not required, as long as the virtual currency exchange does not re-invest or pay interest on public deposits.

Deregulation Race
Switzerland, along with a number of other small jurisdictions,[67] is competing to attract Fintech companies to its territory. The Swiss Canton of Zug, for instance, has branded itself as the *Crypto Valley* (following the Californian *Silicon Valley*) and currently hosts approximately 530 Fintech entities.[68] However, larger Swiss banks — thus far — mostly have refused to open bank accounts for these companies, as the provenance of their funding often is unclear[69] and many of the "startups" have turned out to be scams.[70]

63 Article 9 of AMLO.
64 See §4.2.2 above.
65 Article 7(1) of AMLO.
66 Swiss Federal Council (25 June 2014) at 15.
67 Shaxton mentions Switzerland, Malta, Jersey, the Isle of Man, Kaliningrad, Gibraltar and the Cayman Islands. See Shaxton N (29 August 2018) "Fintech, Hotbed of Offshore Deregulation and Crime" *Tax Justice Network*, available at https://www.taxjustice.net/2018/08/29/fintech-hotbed-of-offshore-deregulation-and-crime/ (visited 21 September 2018).
68 Berman A (21 September 2018) "Swiss Bankers Ease Access for Crypto Startups to Prevent Mass Exodus" *Cointelegraph*, available at https://cointelegraph.com/news/swiss-bankers-ease-access-for-crypto-startups-to-prevent-mass-exodus (visited 23 September 2018).
69 Neghaiwi B (21 September 2018) "Switzerland Tries to Stem Blockchain Exodus by Improving Access to Banks" *Reuters*, available at https://www.reuters.com/article/us-crypto-currencies-switzerland/switzerland-tries-to-stem-blockchain-exodus-by-improving-access-to-banks-idUSKCN1M11H3 (visited 23 September 2018).
70 Allen M (9 April 2018) "ICO Start-Up Funding Craze Starts to Show Cracks" *swissinfo.ch*, available at https://www.swissinfo.ch/eng/business/failing-firms_ico-start-up-funding-craze-starts-to-show-cracks/44026942 (visited 24 September 2018).

Nevertheless, the Swiss parliament have sought to increase Switzerland's attractiveness to the Fintech sector and relaxed AML duties for entities generating an annual gross revenue of less than 1.5 million Swiss francs.[71]
However, it remains doubtful whether lighter regulation leads to better market conditions. As Kaminska writes, the deregulation race exposes an unhealthy "security/access paradox".[72] Jurisdictions abolishing AML and other regulation to make their domestic markets more accessible run the risk of jeopardising the security of their financial markets. Furthermore, under-regulated competition pushes market participants to lower profit margins, meaning that their economic viability relies heavily on large transaction volumes and efficacy — all of which favours the money launderers.

4.3 Analysis

This section will compare the approaches taken by the United States and Switzerland. The analysis focuses on the question of whether the two legal frameworks adequately engage virtual currency exchanges in the detection of illicit clients and assets.

Two key differences between the US and the Swiss approaches have been identified. Firstly, nominally the United States and Switzerland both subject professional money transmitters to their AML provisions. However, while Switzerland's definition of money transmission encompasses custodial and non-custodial virtual currency exchanges, the United States's definition arguably extends only to custodial exchanges.[73] This conclusion was reached because the BSA requires that a money transmitter be engaged in the "acceptance" or "transmission" of assets.[74] For non-custodial exchanges, this is not the case. Non-custodial exchanges merely serve as matching platforms for direct, peer-to-peer transactions. FinCEN indirectly confirmed this view in a 2014 ruling, when it found that an exchange engages in money transmission where the buyer and seller transact only with the exchange.[75]

Secondly, the AML law of the United States contains an exemption for *bona fide* virtual exchange offices.[76] Switzerland, by contrast, does subject virtual exchange offices to its AML regulations, unless their activity does not exceed a

71 See FINMA (10 December 2018) *Fintech-Bewilligung: FINMA konkretisiert Geldwäscherei-Sorgfaltspflichten*.
72 Kaminska I (3 October 2016) "Fintech's Security/Access Paradox Problem" *Financial Times*, available at https://ftalphaville.ft.com/2016/10/03/2176471/fintechs-securityaccess-paradox-problem/ (visited 23 September 2018).
73 See §4.2.2 above for the US and §4.2.3 above for Switzerland. See also Van Valkenburgh (2017) at 14.
74 See also: Van Valkenburgh (2017) at 13 *et seq*.
75 FinCEN (2014) at 3 *et seq*.
76 See §4.2.2 above.

minimum standard[77] — an approach which is more likely to be compliant with the latest version of the FATF Recommendations.[78]

An explanation for why these two exclusions exist in FinCEN's Guidance could not be found. Be that as it may, they may prove to be critical weaknesses in the fight against money laundering in the United States. The Swiss approach appears to be more comprehensive. However, further developments in the current roll-back of AML regulation in Switzerland should be scrutinised closely.

5 CONCLUSION

Virtual currencies are a rapidly evolving field which is difficult to assess. They contain considerable potential as tools in the fight against money laundering: opportunities relate to the more transparent record of transactions stored on the blockchain. Where virtual currency exchanges gather the full spectrum of information needed to identify their customers and the source of funds, virtual currencies become much less attractive to money launderers than the traditional fiat money system.

In the light of these considerations, an adequate regulatory framework providing guidance to innovators — also in South Africa — seems desirable. In the interests of keeping dirty money out of a promising but vulnerable industry, virtual currency exchanges and other Fintech entities should be obligated to check the origin of funds diligently. This paper has identified the regulation of exchange offices and decentralised exchanges as areas for further regulatory activity.

77 See §4.2.3 above.
78 See §4.1 above.