Terrorism Financing with Virtual Currencies – Can Regulatory Technology Solutions Combat this?

ABSTRACT

This article considers the terrorism financing risk associated with the growth of Financial Technology (FinTech) innovations and in particular, focuses on virtual currency (VC) products and services. The ease with which cross-border payments by virtual currencies are facilitated, the anonymity surrounding their usage and their potential to be converted into the fiat financial system, make them ideal for terrorism financing and therefore calls for a coordinated global regulatory response. This article considers the extent of the risk of terrorism financing through virtual currencies in 'high risk' States by focusing on countries that have been recently associated with terrorism activities. It assesses the robustness of their financial regulatory and law enforcement regimes in combating terrorism financing and considers the extent to which Regulatory Technology (RegTech) and its global standardisation, can mitigate this risk.

Keywords: FinTech, International Cooperation, Money Laundering, RegTech, Terrorism Financing, Virtual Currencies

INTRODUCTION

The growth in Financial Technology (FinTech) innovations and New Payment Products and Services (NPPS) is very welcomed as it brings numerous benefits both to businesses and

consumers. These products and services which include: prepaid cards, e-payments, mobile banking, mobile payment services, internet-based payment services and virtual currencies, are also associated with a myriad of challenges. The cross-border nature of the operation of these products and services call for international cooperation in the approach to be taken for their regulation. This article focuses on the potential risk of terrorism financing through virtual currencies which threatens the ground already gained in combating terrorism financing through the work of the Financial Action Task Force (FATF). Money laundering and terrorism financing have generally been associated with jurisdictions with weak financial regulatory and law enforcement regimes. However, with the introduction of speedy but much more technologically complex payment methods such as virtual currencies - operating across jurisdictions with varying approaches to regulating internet / cyber-based transactions - the risk of terrorism financing has become even greater. This article considers the extent to which Regulatory Technology (RegTech) and its global standardisation can mitigate this risk.

It is divided into five sections: section one provides a brief historical context of recent terrorism financing; section two considers the nature and operation of virtual currencies; section three assesses the limitations of the risk-based approach of the FATF Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) provisions and the effect of these on transactions involving virtual currencies and virtual currency exchanges; section four provides a case study of countries that have recently been linked with terrorism, assessing the extent to which their financial regulatory framework and law enforcement mechanisms are able to effectively mitigate potential risks of terrorism financing through virtual currencies. It also considers the extent to which the RegTech solutions can be applied in these states to enhance both financial regulation and law enforcements against terrorism financing using VC. Section five considers the need for international cooperation and the extent to which a possible

global standardisation of RegTech solutions to combat terrorism financing through virtual currencies, can succeed.

TERRORISM FINANCING – HISTORICAL CONTEXT

All terrorism acts require some form of financing. From large scale, coordinated terrorist attacks such as the 11 September 2001 attacks in US, to a one-man planned attack such as was carried out by Anders Behring Breivik in Oslo, in Norway in July 2011.

In the case of the 11 September attacks, the nineteen terrorist hijackers had opened bank accounts, established inter-connected drawing rights, and received several international money transfers. Their activities characterised their lack of concern for the ability of the authorities to trace their financial transactions. Fortunately, the scrutiny by the formal banking sector and the introduction of international standards on anti-money laundering and combating the financing of terrorism (AML/CFT) and the implementation of these regionally and nationally, have resulted in a curtailment in the financing these types of activities. Due to regulations around financial institutions' responsibility to know their customers, the organisation of a terrorist activity, financed through the formal banking sector is increasingly difficult and are more than likely to be flagged up by banks and financial institutions when suspicious activities are carried out.

With this increased scrutiny on the formal banking sector, the case of Anders Behring Breivik, who raised money largely through credit card borrowing[1], is an indication that terrorist attacks would seek more secretive mechanisms for financing their activities.

Despite the curtailment of terrorism financing in the formal financial sector, the rise and growth of New Payment Products and Services (NPPS) and, in particular, virtual currencies, presents a new challenge in this fight against the terrorism financing, thus challenging the progress that has been made thus far. This is so as the characteristics of virtual currencies and the degree of anonymity surrounding transactions settled through them, creates the possibility that the financing of terrorism through them can be widespread and go unnoticed by regulatory authorities.

The well-known case that drives this point home is the recent Liberty Reserve. This case illustrates the potential that virtual currencies have in facilitating money laundering and therefore, also, terrorism financing. Federal law enforcement charged Liberty Reserve, a digital currency provider, with running a $6 billion digital money-laundering scheme. Prosecutors called it possibly the biggest money-laundering case in US history. Liberty Reserve, a centralized digital currency service based in San José Costa Rica, was similar in function to PayPal, it allowed users to register and transfer money to other users with only a name, e-mail address, and birth date. No efforts were made by the site to verify identities of its users, which attracted much illegal activity. Users had a traditional bank from which they wire money to a third-party exchanger, which were usually unlicensed money-transmitting businesses without significant government oversight or regulation. The exchanger then converted the money to digital currency, untraceable from its original source. That digital currency was then deposited into a Liberty Reserve account. No limits were placed on transaction sizes. Liberty Reserve charged 1% service fee on each transfer and offered shopping cart functionality. All the transactions were 100% irrevocable.

Liberty Reserve was, in effect, a bank that issued its own digital currency. The key to Liberty's system was that it never actually received deposits, but instead used a series of middlemen, or money exchangers, who bought the currency in bulk and then sold smaller portions to people looking to convert money into the digital currency. Their website was shut-down by the US in May 2013.

Another well-known case is the Silk road case where payment for criminal activities, by virtual currencies (in this case bitcoin) facilitated through the 'dark web' was widespread and went unnoticed by the authorities. The cite which was launched in February 2011 was shut down in October 2011.

What further necessitates this article is the increasing need of terrorists to hide their identity from the formal financial sector and therefore their quest for payment mechanisms that facilitate anonymous transactions such as is characterised by New Payment Products and Services (NPPS). This explains why the Paris attacks of November 2015 were financed largely using prepaid cards, which are a class of NPPS. As such, if a coordinated global regime for regulating the use of VC is not instituted, there is a high likelihood of the widespread use of these currencies to finance terrorist activities.

THE NATURE AND OPERATION OF VIRTUAL CURRENCIES

Virtual currencies can be defined as a "digital representation 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… in any jurisdiction".[2] Virtual currencies can be explained as digital objects that hold economic value and are functionally similar to fiat

currencies (which are issued by governments), however they are not issued in the way that fiat currencies are but are instead created on the basis of private agreement among users and their operation is governed by this agreement.

There are two main characteristics of virtual currencies. They can be centralised or decentralised. Centralised virtual currencies have a central administering authority that controls the system. This administrating authority issues the currency; establishes the rules for its use; maintains a central payment ledger; and has authority to withdraw it from circulation. The exchange rate for a convertible virtual currency may be floating or fixed. It is floating when it is determined by market supply and demand for the virtual currency and it is fixed when it is pegged 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. Most virtual currency payments transactions involve centralised virtual currencies, such as the now defunct Liberty Reserve dollars/euros used by Liberty Reserve, discussed above. Others include: Second Life "Linden dollars" and World of Warcraft gold. [3]

Decentralised virtual currencies (meaning that they are issued without a central administering authority) are cryptography-based and are distributed, open source, and function on a peer-to-peer basis.[4] They are also known as crypto-currencies. Crypto-currencies are by definition convertible virtual currencies, meaning that they have an equivalent value in real fiat currency, and can be exchanged for such fiat currency.

The characteristic of virtual currencies which include their convertibility to fiat currency and ability to be used as a medium of exchange, a unit of account and a store of value, all facilitate their usage as a currency and as a peer-to-peer payments mechanism for settling

commercial transactions. The acceptance of cryptocurrencies as payment method is becoming widespread in the advanced markets and Bitcoin - which was the first cryptocurrency to gain international reputation as a currency acceptable to settle transactions and which is the most widely used cryptocurrency - is now an acceptable form of payment by a good number of well-known merchants in exchange for goods and services. Examples of well-known merchants accepting this crypto currency include: Amazon, eBay, Expedia, Victoria Secrets and Subway.

Factors Making Virtual Currencies a Viable Approach for Terrorism Financing

The storing and mobilisation of finance raised by terrorists is also critical in determining their ability to carry out acts of terrorism. As these would necessarily involve people and transactions outside the terrorists' immediate network and be significantly conducted through the formal financial sector, they are therefore beyond their control.

Hence, as the financing of terrorism activities have become more visible in the formal financial sector and to law enforcement agencies, terrorists have increasingly had to look for alternative to methods of raising finance and have turned mainly to criminal activity. They have been known to raise finance through: kidnapping for ransom as done by al-Qaeda and Boko Haram in Nigeria; Boko Haram have also financed terrorism through robbing banks and hijacking cars. Al-Qaeda, in Iraq, also raises money through kidnapping and robbing of jewellery stores. Al-Shabaab, in Somalia, raises money, amongst other ways, through mounting 'tolls' on roads under its control.

As stated above, anti-money laundering regulation governing banks and the resulting clampdown on terrorism financing through the formal sector, have made it more difficult for

terrorists to raise money. They are thus, likely to see virtual currencies as an easier alternative for financing their activities if able to access this platform. Two characteristics that make virtual currencies attractive for use by terrorists is their convertibility to fiat money and the anonymity surrounding their usage.

In this vein, they are similar to 'hawala' transactions which is an ancient system of money transfer originating from South Asia and has also been used to finance terrorism. It works with a network of operators. An individual wishing to transfer funds would contact an operator at his location and pay a commission for money he wishes to transfer. The collector, at another location, contacts the local operator and collects the money less the commission. Its usage is now wide spread but purely based on trust. Like virtual currencies, it is an alternative remittance system, which works ideally outside the circle of banks and formal financial systems. However, unlike virtual currencies, transaction amounts are low and no-where near the scale moving through banks and potentially involving virtual currencies. In fact, when transaction amounts become large, operators eventually resort to banks to help them make transfers.[5] Also, virtual currencies transactions are financial technology products and are also described as new payment products and services, which as seen in the case of liberty reserve can mean that goods and services may be obtained without physical cash, whereas 'hawala' transactions involve the receipt of cash/legal tender.

INTERNATIONAL STANDARDS ON AML/CFT AND ITS LIMITATIONS WITH RESPECT TO VIRTUAL CURRENCIES

The FATF Risk-Based Approach to AML/CFT and Challenges

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 set out a framework of measures that countries should implement in order to combat money laundering and terrorism financing, as well as the financing of proliferation of weapons of mass destruction. The Recommendations constitutes international standards but are non-binding although countries are encouraged to implement them.

The FATF risk based approach (RBA) to AML/CFT means that countries, competent authorities and financial institutions, are expected to identify, assess and understand the money laundering and terrorism financing (ML/TF) risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively. The FATF states that when assessing ML/TF risk, countries, competent authorities and financial institutions should analyse and seek to understand how the ML/TF risks they identify affect them; the risk assessment therefore provides the basis for the risk-sensitive application of AML/CFT measures.[6]

The risk based approach was introduced in 2012, when the FATF updated its Recommendations to strengthen global safeguards and to further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crime.

One of the most important changes was the increased emphasis on the risk based approach to AML/CFT, especially in relation to preventive measures and supervision. The

2012 recommendations were to strengthen the 2003 coverage of risk-based approach. While the 2003 recommendations provided for the application of the risk based approach in some areas, the 2012 Recommendations consider the risk based approach to be an 'essential foundation' of a country's AML/CFT framework. This is a primary requirement applicable to all relevant FATF Recommendations.

The Introduction to the 40 Recommendations, the risk based approach 'allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way'.[7]

From the Guidance for a risk based approach document[8] itself, what is clear is that an effective risk based approach will depend on the soundness of financial institutions and the robustness of financial regulatory and law enforcement frameworks, since it is the financial institutions and regulatory and law enforcement authorities that are directly responsible for identifying, assessing and mitigating the AML/CFT risks identified. The main challenge, therefore to the risk based approach is the absence of robust legal and regulatory frameworks in countries, to support this approach which means that it is redundant to states both with weak banks and weak financial regulatory regimes, since these states are likely to be challenged with the inability of their banking sectors to effectively identify and assess their own ML/TF risks and therefore, will be unable to effectively mitigate them. The risk based approach is also redundant to these states as their legal systems would be unable to effectively enforce AML/CFT provisions, if at all discovered.

Challenges of the FATF RBA with Specific Reference to Virtual Currencies

This challenge of the absence of robust legal and financial regulatory regimes in a good number of countries is further exacerbated by the global nature of terrorism activities[9] and, particularly, by the likelihood that countries with weaker legal regimes can be used as potential breeding grounds for terrorism financing and thus present a global challenge. Hence, the precise challenges to the risk based approach to ML/FT is that it does not have a global reach. Setting a global standard would be challenging due to the varying degree of financial and legal systems development across the world ranging from advanced, emerging, developing to underdeveloped financial and legal systems which enabled criminal activity in cases like the Liberty Reserve, where jurisdictions with weak regimes - such as Nigeria - were used to launder money for illicit purposes. Also, the inconsistent commitment to fighting terrorism across the world, linked with the weakness of the rule of law and law enforcement mechanisms in most vulnerable jurisdictions, further promotes the platform for terrorism financing through these countries and, therefore, making the attainment of a global reach even more difficult.

The lack of a global reach of the risk-based approach to regulating money laundry and terrorism financing is further compounded by the possibility of the use of virtual currencies to finance terrorism activities. The technological complexities characterising the functionality of decentralised virtual currencies, as well as the anonymity underpinning both decentralised and centralised virtual currencies as payment mechanisms, in addition to ill-developed legal systems and financial regulatory regimes, all make the use of virtual currencies to finance terrorism activities challenging to control. The main problem here is that, whilst countries with sound legal and enforcement systems and robust financial regulatory regimes are more able to check the ML/FT risks of VC, countries with weaker institutions are less able to do so. As such,

global efforts to check ML/FT through VC would only be as strong as the weakest link of nations, with weak financial regulatory regimes and poor law enforcement mechanisms.

Assessing the critical risk transmitted through virtual currency exchangers

One of the main risks associated with the use of virtual currencies is the possibility of their convertibility to fiat money (currency that is declared by a state's government to be legal tender such as US dollars and pound sterling) and through this, intersect with the regulated fiat currency financial system – as was the case in Liberty Reserve.[10] This can be done through convertible VC exchanges or exchangers. They can be a person or an 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.[11]

As nodes enabling the intersection of virtual currencies with the fiat currency financial system, a careful examination of their operation and the devising of an international mechanism / regime to regulate them is critical.

Regulatory aspects for virtual currency exchanges/exchangers

Virtual currency exchangers can also be referred to as providing Money or Value Transfer Services (MVTS) which "refers to financial services that involve the acceptance of cash,

cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods."[12]

Any persons or entities engaged in virtual currency exchange services can be used as a mechanism for money laundering and terrorism financing and as such, should be effectively regulated. For this, the FATF Recommendations are instructive.

Regulation should ensure that the regulatory authorities are able to assess money laundering and terrorism financing risks of the operation of such entities to ensure that sufficient resources are allocated to mitigate such risks. This also includes that such entities and institutions should be able to identify, assess and mitigate the ML/TF risks arising from their operations.[13]

Regulation should require that such entities fulfil customer due diligence (CDD) requirements and should know their customers and be able to verify their customer's identity using reliable, independent source documents, data or information. The entities should also be able to identify the beneficial owner, and taking reasonable measures to verify their identity, such that the entity is satisfied that it knows who the beneficial owner is, of the account holding the proceeds of the transaction. In fact, the FATF suggests that, in the light of the nature of Virtual Currency Payment Products and Services (VCPPS)[14], in which customer relationships are established and transactions conducted entirely through the internet – such as VC exchangers - institutions must necessarily rely on non-face-to-face identification and

verification. The FATF suggests that countries should consider requiring entities providing such services to follow the best practices suggested in the June 2013 New Payment Products and Services (NPPS) Guidance including: corroborating identity information received from the customer, such as a national identity number, with information in third party databases or other reliable sources; potentially tracing the customer's Internet Protocol (IP) address; and searching the Web for corroborating activity information consistent with the customer's transaction profile, provided that the data collection is in line with national privacy legislation.[15]

Regulation should require virtual currency exchangers/exchanges to maintain records on transactions and information obtained through the CDD measures. For instance, FATF recommends that they should keep, for at least five years, all necessary records on transactions, both domestic and international. The CDD information and the transaction records should be available to domestic competent authorities.[16]

Regulation should require VC exchange entities to be registered or licenced[17] as providers of Money and Value Transfer Services (MVTS). Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods (as in payment in virtual currency).[18] The registering of such entity should be done by a competent authority and subject to effective systems for monitoring and complying with AML/CFT provisions and domestic authorities should be able to identify such persons or entities carrying out virtual currency exchange services without a license or registration and apply appropriate sanctions. A typical example of an effective licensing and registration regime for such entities can be seen in the work of the US Financial Crimes Enforcement Network (FinCEN) which is a bureau of the United States Department of the Treasury that collects and analyses information about financial transactions in order to combat domestic and international money laundering, terrorist financing, and other financial crimes. In May 2015, in coordination with federal law enforcement partners, FinCEN assessed the first civil monetary penalty against a virtual currency exchanger, Ripple Labs Inc., for failure to register with FinCEN as a money services business as well as its failure to implement and maintain an adequate AML program designed to protect its products from use by money launderers or terrorist financiers. Nonetheless, the effectiveness of such regulation would

require the existence of a strong competent authority empowered both by the legal and regulatory framework within the state. As assessed below, this is a phenomenon lacking in most high-risk states.[19]

Regulation should also require that financial groups providing, amongst other services, MVTS including VC exchanges, should 'implement group-wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.'[20] These financial groups should be required to ensure that their foreign branches and majority- owned subsidiaries (which may include MVTS / VC exchange services) apply AML/CFT measures consistent with the home country requirements - thus home countries should have robust enough financial regulatory standards to be able to monitor the operations of the groups and their subsidiaries conducting VC exchange services.

Regulation should also require that virtual currency exchange services should maintain suspicious transaction reporting.[21] This will require that if VC exchangers providing exchange services suspect that or have reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligent unit. It is clear that the absence of such requirements greatly facilitated money laundering in the Liberty Reserve case.

Thus, the effective application of a risk based approach to AML/CFT provisions focused on the operation of VC exchanges and similar entities worldwide, would require the existence of a robust financial regulatory regime and able competent authorities. This would include law enforcement agencies and financial intelligence units.

Due to the cross-border nature of the operations of virtual currency exchanges, an effective global AML/CFT regime necessarily requires – as a first step - that all countries have robust financial regulatory and law enforcement regimes, so that money laundering and

terrorism financing activities do not gravitate to and concentrate on regions and countries with weak law and regulatory regimes.

Some of the current obstacles to applying some of the mitigating measures to VC exchange entities, as assessed above, is the weak financial regulatory regimes governing the global operation of VC exchanges in some jurisdictions, thus making such jurisdictions targets for money laundering and terrorism financing. As such, the application, for example, of FATF Recommendation 14 on registration or licensing requirements for Money and Value Transfer Services (MVTS) or VC exchange or exchangers is likely to be ineffective if the jurisdiction where the VC exchanger operates has a weak financial regulatory regime.

Thus, the success of the risk-based approach to AML/CFT with respect to virtual currency exchanges is very much dependent on the strength of the domestic financial regulatory framework in states and the strengthen of the law enforcement regime to criminalise illicit activities and transactions - all of which will require the requisite use of technology commensurate with the technology behind these financial technology (FinTech) innovations themselves, which is well-known now as Regulatory technology (RegTech). RegTech is described by the UK Financial Conducts Authority "as the adoption of new technologies to facilitate the delivery of regulatory requirements…"[22] to keep up with the increasingly dense data landscapes and the rapidly evolving FinTech sector, products and innovations.

RegTech solutions within this context involves, inter alia, the use of big data analytics[23] and artificial intelligence[24] where regulators will be able to use required technology to aid the identification and monitory of risks posed by these institutions. Typical example of how this will be useful to virtual currency exchanges will be through their compliance with KYC /CDD (Know Your Customer/Customer Due Diligence). As their services are characterised by the

provision of financial services over the internet, they hardly establish face to face contact with their customers, thus making compliance with KYC/CDD challenging. As such, to fulfil this arduous task would require the application of this type of technology – in other words RegTech.

It also would necessitate that regulators are able to integrate RegTech solutions into their supervision and examination functions. A *"RegTech for regulators"* approach could help provide a multi-faceted solution to tackle regulatory complexity inherent in recent development of financial technology. By digitising the regulatory architecture, RegTech could also support a less burdensome approach to financial regulation as technology encourages transparency, addresses asymmetries and empowers consumers, market participants and regulators to better manage risk.

Regulators have to be comfortable with the technological changes introduced by FinTech products. In the UK, actions already taken by the government to achieve its vision include the introduction of Project Innovate within the FCA and the resultant Innovation Hub and Regulatory Sandbox initiatives. This was achieved by the FCA inviting Innovate Finance[25], which is an independent not-for-profit membership association representing the UK's global FinTech community. The Sandbox is an initiative to provide FinTech innovators with support to navigate the regulatory system and promote competition in the interest of consumers. It aims to create a 'safe space' in which businesses can test innovative products, services, business models and delivery mechanisms in a live environment while ensuring that consumers are appropriately protected.

Thus, two main areas of concern with respect to the risk based approach to money laundering and terrorism financing, especially with respect to the operation of VC exchanges

are: (1) financial regulatory quality and the robustness of law enforcement regimes in countries and (2) the extent to which the regulators can speedily adopt RegTech solutions to monitor compliance with AML/CFT provisions and their ability to effectively standardise those RegTech solutions across the industry.

Thus, although the risk-based approach to payments using virtual currencies examines how convertible virtual currency exchangers should, amongst other things, be subject to international AML/CFT standards[26], efforts should also be channelled towards strengthening the regulatory framework in countries (along the lines of the UK FCA) and making their authorities more aware of the potential risk of VC exchangers. This would involve the adoption of the requisite RegTech, standardised to be able to address new financial regulatory issues arising from FinTech products and services, such as virtual currencies and virtual currency exchanges.

Applying RegTech solutions to virtual currency exchanges and challenges

It should be mentioned that with specific reference to decentralised virtual currencies, it is only recently that decentralised convertible VC technology allows certain risk mitigants to be built into decentralised Virtual Currency Payment Product and Services (VCPPS) in order to restrict functionality and reduce risk. For instance, multisignature (multi-sig) technology now enables VCPPS to effectively build in loading total wallet value, and value/velocity transaction limits into decentralised VCPPS. However, current decentralised VC technology does not make it possible to effectively build in geographic limits; limit use to the purchase of certain goods and services; or prevent person-to-person transfers.

While technology may be able to build this in future, the concern for regulators should be the fact that these decentralised convertible VC technology / operators may decide not to build in these mitigants in order to maintain the anonymity functionalities of these platforms.[27] It would thus appear that, for now, the most practical way of inhibiting their ability to be converted to real asset is by restricting their entry into the fiat monetary system and this would be done primarily through the regulation of virtual currency exchangers.

Suffice to mention that the adoption of RegTech by regulated financial institutions is also vital especially as they have been criticised of both the cost and time wasted on analysing data for the purposes of AML/CFT compliance. Most of their effort result in time and money spent chasing false-positive alerts of criminal or terrorist financing. These financial institutions therefore need to strengthen their own anti-money laundering (AML) and know-your-customer (KYC) systems or renting in better ones by adopting RegTech solutions. Thus, by using the latest artificial intelligence and machine-learning tools, they can manage their compliance burdens with sharper focus and at lower cost. This can be used to build a comprehensive global data set of individuals and companies that represent a potential money laundering and terrorism financing threat.[28]

CASE STUDIES ON FINANCIAL REGULATORY QUALITY AND LAW ENFORCEMENT MECHANISMS

This section examines the extent to which banks and financial institutions in 'high-risk' countries with weak legal and financial regulatory regimes are able to identify and mitigate risks associated with convertible VC exchanges operating within their jurisdiction or providing services to customers in their jurisdiction.

As institutions offering VC exchange services would typically be providing cross-border financial services, mechanisms for monitoring their operation would be through effective financial regulation. The section also then considers the extent to which legal systems are or would be able to effectively prosecute acts of terrorism financing through the operation of VC exchanges or other MVTS, when discovered. The assessment of both financial regulatory quality and the quality of the legal system uses the World Governance Indicators (WGI), developed by the World Bank, which rank countries according to quality of governance by aggregating data from many available sources.[29]

The two main WGI indicators relevant for assessing the countries' financial regulatory quality and strengthen of their law enforcement mechanisms are: Regulatory quality (RQ) and Rule of law (RL).[30]

The countries that would be assessed in this case study are a select list of countries that have been associated with terrorism activities in recent times. Although they are not the only countries associated with terrorism activities internationally, they are referred to as 'high-risk' countries for the purposes of this article and include: Afghanistan, Kenya, Iraq, Nigeria, Somalia, Sudan and Syria.

Going by the analysis above, the adoption of RegTech solutions in these countries is unlikely to be at the same pace as their counterparts in advanced markets. Of these seven 'high-risk' countries, three of them (Afghanistan, Iraq and Syria) have been identified by FATF as high-risk and non-cooperative jurisdictions.[31] Even though Kenya, Nigeria, Somalia and Sudan

are not deemed as high-risk and non-cooperative jurisdictions, their financial regulatory quality all need strengthening.

As of writing, the WGI[32] are based on 340 variables produced by 32 different sources, including commercial information providers, surveys of firms and households, non-governmental organizations and public sector organizations.[33] These indicators have been used to assess the governance status of countries across the world.

The composite measures of governance generated by the Model used by the WGI team are in units of a standard normal distribution, with mean zero, standard deviation of one, and running from approximately -2.5 to 2.5, with higher values corresponding to better governance. WGI also report the data in percentile rank term, ranging from 0 (lowest rank) to 100 (highest rank). As such, the two aggregate indicators are reported in two ways: (1) in their standard normal units, ranging from approximately -2.5 to 2.5, and (2) in percentile rank terms from 0 to 100, with higher values corresponding to better outcomes.[34]

Regulatory Quality

Regulatory quality (RQ) measures perceptions of the ability of the government to formulate and implement sound policies and regulations that permit and promote private sector development. In the context under review, it would mean the ability of regulatory authorities to strike the ideal balance between ensuring that robust AML/CFT standards are in place, without stifling the developments of FinTech products and services - such as virtual currency and the operation of virtual currency exchanges - through overregulation.

This would require, among other things, that the regulatory framework is robust enough to effectively implement CDD through KYC policies. Due to the critical role played by financial regulatory authorities in ensuring sound AML/CFT through financial institutions, the focus of the measurement of regulatory quality in these high-risk states, is significant. Strong regulatory quality indicates that terrorism financing activities through the operation of virtual currency exchanges and other MVTS in these jurisdictions, are likely to be spotted and acted upon.

The rankings of these 'high risk' states and the estimate of governance for this indicator (regulatory quality) is an indication, among other things, of the extent of the robustness of states' financial system to check money laundering and terrorism financing through the operation of virtual currency exchanges within their territory.

In 2015 the country that ranked the highest for regulatory quality was Singapore at 100,[35] whilst its estimate of governance for the observance of this indicator on a scale of -2.5 to 2.5 was 2.26,[36] which indicates very strong governance performance for the quality of regulation in the country in general including financial regulation and indeed, the regulation and monitoring of ML/FT. Thus the IMF describes Singapore's financial regulation and supervision as "...among the best globally."[37] Suffice to mention also that in 2015, Singapore ranked fourth place globally of the world's leading FinTech hubs.[38] As the country appears to have embraced FinTech, it is not surprising therefore that, much like the case in the UK, the regulatory framework for the development of this sector would be keen to adopt RegTech solutions to ensure safe operation of FinTech product and services including virtual currencies and virtual currency exchanges.

Afghanistan

Far from the ranking in Singapore, Afghanistan, of the 'high-risk' countries under review in this article, for regulatory quality ranked 13.46[39] in 2015, placing it as one of the poorest performing countries for regulatory quality in the world. Its estimate of governance for the observance of this indicator, on a scale of -2.5 to 2.5, was -1.00.[40] This is an indication of a significantly weak governance performance for this indicator and highlights, also, a weak framework for financial regulation and, therefore, a potential enabler of money laundering and terrorism financing through virtual currency exchange operations within the country.

Kenya

Kenya in 2015, ranked 43.26[41] for regulatory quality of all the countries assessed which shows that by global ranking standards it ranked at the low end of average for regulatory quality but the highest ranking of the 'high-risk' countries under review in this article. Its estimate of governance for the observance of this indicator, on a scale of -2.5 to 2.5, was -0.29.[42] This is also closer to average and indicates a stronger regime for licensing virtual currency exchanges/exchangers and a stronger CDD/KYC framework and therefore a robust AML/CFT regime, in comparison to all the other countries under review in this article. This also indicates that regulators may be able to identify money laundering and terrorism financing activities through the operation of virtual currency exchange operations within Kenya. Nonetheless, quite a bit still needs to be done in strengthening the financial regulatory quality in this country.

Nigeria

Nigeria, of the 'high-risk' countries under review for regulatory quality ranked 21.63,[43] ranking it as one of the countries in the last 30 ranking for regulatory quality across the world. Its

estimate of governance for the observance of this indicator on a scale of -2.5 to 2.5 was -0.84,[44] which indicates a weak governance performance for this indicator and thus indicating that the quality of regulation in Nigeria is weak including the quality of the regulation of financial markets. This suggests the existence of weak policy formulation, implementation and enforcement of financial regulation. It is also not surprising that the third-party exchangers in the Liberty Reserve case who took and made payments and then credited and debited the Liberty Reserve account (thus allowing LR to avoid collecting any banking information on its clients and as such leaving no paper trail) tended to be unlicensed money-transmitting businesses without significant government oversight or regulation and whose services, amongst other jurisdictions, were concentrated in Nigeria. Nigeria, of course, was a conducive environment since its financial regulatory framework was weak to ensure that parties providing financial services through the third-party exchangers in the Liberty Reserve case, were effectively licensed to perform such activities. This, of course, would have ensured they were checked for effectively complying with CDD/KYC rules.

Iraq

Iraq, of the 'high-risk' countries under review, for regulatory quality ranked 8.65,[45] placing it as one of the worst 10 performers world-wide for regulatory quality. Its estimate of governance for the observance of this indicator, on a scale of -2.5 to 2.5, was -1.23.[46] This is an indication of a quite weak governance performance for this indicator and again highlighting the potential for harboring unlicensed virtual currency exchangers or even if licensed, is likely to have a weak CDD/KYC framework.

Sudan

Sudan of the 'high-risk' countries under review for regulatory quality ranked 4.80,[47] placing it as one of the worst 10 performers world-wide for regulatory quality. Its estimate of governance for the observance of this indicator, on a scale of -2.5 to 2.5, was -1.50[48] and is an indication of a quite weak governance performance for this indicator. This like the case of Iraq, again highlights a potential weakness in licensing the operation of virtual currency exchangers and would indicate a weak CDD/KYC framework even if such entities/persons providing such services were licensed.

Syria

Syria of the 'high-risk' countries under review for regulatory quality ranked 4.32,[49] placing it as one of the worst 10 performers world-wide for regulatory quality. Its estimate of governance for the observance of this indicator on a scale of -2.5 to 2.5 is -1.63.[50] This is an indication of a quite weak governance performance for this indicator and again highlights the potential weakness in licensing the operation of virtual currency exchangers and a weak CDD/KYC framework even if such entities/persons were licensed.

Somalia

Somalia of the 'high-risk' countries under review for regulatory quality ranked 0.96,[51] placing it as one of the lowest ranking countries in the world for regulatory quality. Its estimate of governance for the observance of this indicator on a scale of -2.5 to 2.5 was -2.14[52] and is an indication of a very weak governance performance for this indicator, again highlighting the potential for a weak framework for licensing the operation of virtual currency exchangers and CDD/KYC.

Strength of Legal Enforcement / Rule of Law Regime

Rule of law (RL) measures perceptions of the extent to which agents have confidence in and abide by the rules of society, and in particular the quality of contract enforcement, the police and the courts, as well as the likelihood of crime and violence.

Thus, in the context under review, it would refer to the robustness of the criminal justice system in investigating and prosecuting acts of terrorism financing when identified. Such a system would be capable of investigating and adjudicating criminal offenses speedily and effectively, while ensuring that the rights of both victims and the accused are effectively protected. The delivery of criminal justice should take into consideration the entire system, including the police, the lawyers, prosecutors, judges, and prison officers.

Suffice to mention that applying traditional law enforcement to cases involving virtual currency payment products and services present numerous challenges due to the anonymity inherent in their operation. The anonymity of most transactions makes it difficult to determine the identities of the persons involved thus making the process of investigation and prosecutions challenging. The situation is particularly worst with respect to decentralised VC transactions, where no central administering authority can be consulted and the underlying protocols on which most decentralised VCPPS are currently based, do not require or provide identification and verification of participants. Moreover, the historical transactions records generated on the blockchain by the underlying protocols are not necessarily associated with real world identity.[53] This level of anonymity limits the blockchain's usefulness for monitoring transactions and identifying suspicious activity, and presents a significant challenge to law enforcement's ability to trace illicit proceeds that are laundered using decentralised convertible VC. Furthermore,

law enforcement cannot target one central location or entity for investigative purposes. These challenges, therefore, undermine countries' ability to utilise effective, dissuasive sanctions.

Nonetheless within this current state of affairs two approaches can be adopted to facilitate investigation of illicit conduct such as money laundering and terrorism financing. First, it is possible for financial institutions (and virtual currency exchangers) to be required to maintain transaction records that include: information to identify the parties; the public keys, addresses or accounts involved; the nature and date of the transaction, and the amount transferred. The public information available on the blockchain provides a foundation for record keeping, provided institutions can adequately identify their customers. Countries should require institutions to be attentive to the type of suspicious activity they are in a position to detect.

Secondly, since these virtual currencies are likely to be converted to fiat money, to have any real usable value, investigations can be focused around the operation of VC exchangers to check any unusual activities. Thus, the regulation of virtual currency exchanges, particularly regulation around their licensing or registration requirements; their application of customer identification/verification (at the point of exchange) and recordkeeping requirements, could provide a pathway enabling countries to better apply effective and dissuasive sanctions in the virtual currency context.

Whichever approach is adopted, it is clear – as revealed in the Liberty Reserve case – that the strength of a country's criminal justice system (a critical part being its law enforcement mechanism) places it in the right position to be able to, through investigations around the work of VC exchangers, discover, investigate and prosecute, where necessary, individuals using

virtual currencies as a platform for money laundering and terrorism financing. It is not likely that countries with weak legal systems and enforcement regimes would be able take such actions. This explains why, of all the jurisdictions where Liberty Reserve operated across the globe, only a few where able to cooperate with the US in the investigation against Liberty Reserve.

The strength of countries' criminal justice system[54] including, critically, the strength of its enforcement regimes, is therefore pivotal to this process. The ensuing paragraphs, as such considers the extent to which the rule of law, as manifested in the strength both of the criminal justice system and the strength of the law enforcement, exists in the 'high-risk' states. The score on the Rule of Law indicator of these high-risk states is an indication of the extent to which their enforcement regime would be able to effectively prosecute terrorism financing through virtual currencies.

In 2015 the country that ranked the highest for rule of law was Norway at 98.55,[55] whilst its estimate of governance for the observance of this indicator on a scale of -2.5 to 2.5 was 2.02.[56] This shows very strong governance performance for rule of law in the country in general and is indicative of an effective criminal justice system that has a robust basis for effectively supporting the investigation and prosecution of criminal offenses such as terrorism financing through virtual currencies and virtual currency exchanges.

Afghanistan

In 2015, Afghanistan ranked 2.40[57] for rule of law of all the countries assessed, which shows that by global ranking standards, it ranks as one of the lowest for rule of law. Its estimate of

governance for the observance of this indicator on a scale of -2.5 to 2.5 was -1.59.[58] This is significantly less than the average, which is 0 and even bearing towards the higher end of worst performing, which is -2.5. This is a huge indication that the law enforcement system is quite weak, in comparison to the rest of the world and significantly lacks the fundamentals for an effective criminal justice system that would be able to effectively investigate and prosecute terrorism financing through virtual currencies and virtual currency exchanges.

Kenya

In 2015, Kenya ranked 36.53[59] for rule of law of all the countries assessed, which showed that, by global ranking standards it ranked quite low for the rule of law, although the highest ranking of the high-risk countries reviewed in this article. Its estimate of governance for the observance of this indicator on a scale of -2.5 to 2.5 was -0.49.[60] This is less than the average and indicates that the criminal justice system has inherent weaknesses, although in comparison to the high-risk countries assessed in this article, this score is higher, thus indicating an inclination towards better criminal justice system that may be able to effectively investigate and prosecute terrorism financing by individuals using virtual currencies through the operation of virtual currency exchanges.

Iraq

In 2015, Iraq ranked 3.84[61] for rule of law of all the countries assessed, which shows that by global ranking standards it ranks as one of the lowest for rule of law. Its estimate of governance for the observance of this indicator on a scale of -2.5 to 2.5 was -1.45.[62] This is significantly less than the average, which is 0 and even bearing towards the higher end of worst performing which is -2.5 and is a huge indication that the criminal justice system is quite weak in comparison to the rest of the world and significantly lacks the fundamentals for an effective

criminal justice system that would, someday, be able to effectively investigate and prosecute terrorism financing of individuals using virtual currencies through the operation of virtual currency exchanges.

Nigeria

In 2015, Nigeria ranked 12.98[63] for rule of law of all the countries assessed, which shows that by global ranking standards it is one of the lowest performing 15 countries for rule of law in the world. Its estimate of governance for the observance of this indicator on a scale of -2.5 to 2.5 was -1.04.[64] This is significantly less than the average, which is 0 and a big indication that the criminal justice system is quite weak in comparison to the rest of the world and also lacks the fundamentals that form the basis for an effective criminal justice system that would be able to effectively investigate and prosecute terrorism financing by individuals using virtual currencies through the operation of virtual currency exchanges.

Somalia

In 2015, Somalia ranked 0[65] for rule of law, of all the countries assessed, which shows that by global ranking standards it is was the worst performing country for rule of law in the world. It is not surprising that its estimate of governance for the observance of this indicator on a scale of -2.5 to 2.5 is -2.33,[66] almost hitting the -2.5 worst performance limit. This is indicative that it lacks a criminal justice system and therefore lacks the fundamentals to effectively investigate any form of crime, how much more, investigating and prosecuting terrorism financing by virtual currencies someday. It would first need to build a criminal justice system before it can think of prosecuting the criminal activities that utilize such advanced technologies as virtual currencies, whose operation - as seen above - is heavily based on disguised identities and anonymity.

Sudan

In 2015, Sudan ranked 8.17[67] for rule of law of all the countries assessed, which places it as one of the worst 10 performers world-wide for rule of law. Its estimate of governance for the observance of this indicator on a scale of -2.5 to 2.5 was -1.18.[68] This is significantly less than the average, which is 0 and an indication that the criminal justice system is quite weak in comparison to the rest of the world and significantly lacks the fundamentals for an effective criminal justice system that would be able to, someday, effectively investigate and prosecute terrorism financing through virtual currencies and virtual currency exchanges.

Syria

In 2015, Syria ranked 4.32[69] for rule of law of all the countries assessed, which places it as one of the lowest ranking countries for rule of law world-wide. Its estimate of governance for the observance of this indicator on a scale of -2.5 to 2.5 was -1.43.[70] This is significantly less than the average, which is 0 and even bearing towards the higher end of worst performing which is -2.5, and is a huge indication that the criminal justice system is quite weak in comparison to the rest of the world and like the stats for Iraq, significantly lacks the basis for an effective criminal justice system that would be able to effectively investigate and prosecute terrorism financing by virtual currencies and through currency exchanges, someday.

On the basis of the analysis of the strength of the financial regulatory regimes and law enforcement regimes through the assessments of perceptions of regulatory quality and the rule of law, it appears all the countries are quite weak. Apart from Kenya, they all significantly lack the rudiments for building regimes both for effectively regulating financial institutions (such as virtual currency exchanges) transacting in virtual currencies, as well as investigating and

prosecuting terrorism financing by virtual currencies (through virtual currency exchanges). The countries could, as such, continue to be breeding grounds / hideouts for terrorism financing in their current state of affairs.

THE NEED FOR INTERNATIONAL COOPERATION AND GLOBAL STANDARDISATION OF REGTECH SOLUTIONS

The ease with which FinTech innovations - as is seen in the operation of virtual currencies – can be used to facilitate cross-border payment and therefore used to facilitate the financing of illicit activities such as acts of terrorism, calls for international cooperation. Due to the cross-border nature of transactions involving virtual currencies, no single jurisdiction can boast of a robust regulatory / law enforcement regime for virtual currency transactions and virtual currency exchanges on its own. The strength of criminal justice and law enforcement systems varies across jurisdictions and where virtual currencies are used to facilitate crime, criminal activity in one territory can go without detection or punishment because they cannot be effectively investigated or enforced by persons outside the jurisdiction. This thus calls for coordination and cooperation among regulators and law enforcement authorities to address these issues. The importance of such cooperation is underscored by the case of the Liberty Reserve (and Silk road) where illegal transactions were conducted cross-border and went undetected by authorities and law enforcement agencies. The operation, therefore, of virtual currencies necessitates that the regulatory space should have, among other things, an extra-territorial reach.

The main challenge of having an extra-territorial reach for the operation of virtual currencies or indeed any internet-related transaction, is that international cooperation on such

issues can be complicated due to the different perspectives and approaches taken by countries which are then transposed in their national law and policy stance on the issue. In some countries, the regulation of the internet and cyber-related transactions is significant for national security and these countries have legal mechanisms in place allowing extensive governmental intrusion into the sender and recipient details of every single transmission, and the contents of such transmissions. Other countries approach the regulation of the internet and internet-based transactions with caution, noting the requirement for balancing security concerns against certain constitutionally protected freedoms, and there embrace the preservation of privacy and data protection laws.

Given the challenge of international cooperation in this space, a possible approach that could be adopted is a regional approach to regulating virtual currency transactions and exchanges. For instance, recently in South East Asia - Singapore, Japan and South Korea - regulators have engaged in partnerships on the cyber-security front, including through the signing of information sharing and collaborative agreements. It is believed that international cooperation will continue to deepen with the opening of the INTERPOL Global Complex for Innovation in Singapore in 2014.[71]

Effective virtual currency regulation (both for convertible decentralised and centralised virtual currencies) will require more detailed cooperation arrangements with foreign regulators. RegTech, as such will play a key role here and its international standardisation will be needed. Suffice to mention that in some jurisdictions, virtual currency regulation takes on an extra-territorial approach. In countries, such as the US or Canada, such regulations are expressed as having extraterritorial effect, however due to absence of an international regulatory approach to virtual currency exchanges, firms are subject to multiple layers of regulation with potentially

conflicting and irreconcilable rules at the same time. For instance, Canada's recently released virtual currency regulations, issued by the Financial Transactions and Reports Analysis Centre of Canada ("Fintrac"), are stated to have extraterritorial effect and captures foreign firms that either have a place of business in Canada, or are offering services to Canadians. Thus, a virtual currency firm or exchange operating in any other jurisdiction, may have to comply both with the regulation in their jurisdiction and regulations in jurisdictions whose regulation have extra-territorial effect, such as Canada, to the extent that such firms has a Canadian office or markets to Canadian customers. In a case of conflict, the firm may have no choice but to comply with the stricter standard, even though its competitors may not be similarly constrained; worse still, in cases of more fundamental conflict, complying with either standard may put a firm in breach of the other standard it is subject to. This thus calls for coordinated international approach for the regulation of virtual currencies.

A robust international regulatory regime should focus, as a matter of urgency, on the cross-border harmonisation of regulations of virtual currencies / virtual currency exchanges transactions, in order to minimise, amongst other things, terrorism financing through money laundered by the operation of these VC firms. An international regime can take on the US approach to regulating these entities through the US Financial Crimes Enforcement Network (FinCEN). This approach could lead to civil monetary penalties against virtual currency exchangers, for violating regulatory standards, such as licensing and registration requirements, as seen in the US case of Ripple Labs Inc, cited above.

Suffice to mention that the FATF Recommendations also offers suggestions as to areas where cross-border harmonisation of regulation of VC/VC exchanges can be concentrated. For instance, Recommendation 2[72] requires national cooperation and coordination with respect to

AML/CFT policies. According to the FATF, countries may consider putting in place mechanisms, such as inter-agency working groups, to enable policy-makers, regulators, supervisors, the financial intelligence unit (FIU), and law enforcement authorities to cooperate with each other and any other relevant competent authorities to develop and implement effective policies, regulations and other measures to address VC ML/TF risks.[73]

With specific reference to virtual currency exchangers – who are the nodes through which such transactions are linked to the fiat financial system – as they transfer value digitally, via the internet, and are not subject to territorial boundaries and generally offer VCPPS to persons in countries in which they are not physically present, it is very important that all home countries apply domestic licensing or registration requirements on such entities or institutions providing such services. As such, the need for proper oversight by the home jurisdiction and adequate cooperation and information exchange between competent authorities between jurisdictions where the entity provides services is of high importance.[74] This of course, as considered earlier, is a problem given that some jurisdictions have quite weak financial regulatory regimes and countries are at different degrees of financial systems and financial regulatory developments.

While there are gaps in regulating this sector and while nations have diverse financial regulatory strengths and robustness of law enforcement/criminal justice systems, terrorism financing through virtual currencies remains a real threat.

The introduction of global RegTech standards, which is the fast pace direction which the FinTech industry is heading, would make significant contributions to the regulation of virtual currencies. Critical to these developments would be: countries' acceptance of the

regulation of this space; the speed to agree robust global standards and the extent of the global application /adoption of these RegTech standards and, in particular, within 'high-risk' states.

CONCLUSION

While the growth of the Financial Technology (FinTech) industry world-wide signals huge opportunities for businesses and consumers, it also introduces a myriad of challenges to the global financial industry. The challenge considered in this article is the potential of virtual currencies, a key FinTech innovation, to be used to finance terrorism activities.

This article has argued that, while financial regulatory regimes world-wide are at different stages of development and the robustness of law enforcement regimes worldwide vary, the threat of terrorism financing remains real - more so as terrorism financing is likely to shift to jurisdictions with weaker regimes.

This calls for global action that, itself, is not without challenges due to the different approaches taken by countries in regulating internet/cyber-based transactions – the main channel for virtual currencies transactions. The development of Regulatory Technology (RegTech) to enable the regulation and monitoring of FinTech products and services, like virtual currencies, offers some solutions. Critical to its effectiveness in regulating virtual currency transactions are: the speed of the adoption of global RegTech standards for virtual currency transactions; the strength of such standards - since countries take different approaches to regulating internet-based transactions - and the national adoption of those standards, especially in 'high-risk' states with weak financial regulatory and law enforcement regimes.

[1] *See* Erica Alini, 'The Meticulous Planning of the Oslo Massacre' (Macleans, 28 July 2011). Available at <http://www.macleans.ca/news/world/the-meticulous-planning-of-the-oslo-massacre/> (accessed 24 November 2016). This article captures Breivik's personal manifesto, noting among other things his detailed financial preparation for the attack.
[2] Financial Action Task Force Report, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' (FATF, June 2014), 4. Available at <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> (accessed 26 November 2016).
[3] n 2 above, 5.
[4] ibid.
[5] Economist, 'Terrorists and Hawala Banking: Cheap and Trusted Homing in on Networks of Informal Money Transfers', (Economist 22 November 2001). Available at http://www.economist.com/node/877145 (accessed 1 June 2017).
[6] For more on this see: FATF, 'Guidance for a Risk-Based Approach - The Banking Sector' (FATF, October 2014), 6-7. Available at <http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf> (accessed 24 November 2016).
[7] ibid, 6.
[8] ibid.
[9] ibid, 4.
[10] FATF, 'Virtual Currencies: Guidance for a Risk-Based Approach' (FATF, June 2015). Available at <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> (accessed 24 November 2016).
[11] For more on this see FATF (n 2) 7.
[12] See FATF, 'Glossary' (FATF, 15 April 2017). Available at <http://www.fatf-gafi.org/glossary/j-m/> (accessed 15 April 2017).
[13] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation' (FATF February 2012, amended in 2016), (FATF Recommendations), FATF Recommendation 1. Available at <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> (accessed 24 November 2016).
[14] Such as virtual currencies and virtual currency exchanges.
[15] FATF, 'Prepaid Cards, Mobile Payments and Internet- Based Payment Services Guidance' (FATF June 2013). Available at < *http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf*> (accessed 29 November 2016).
[16] FATF (n 10) 6.
[17] FATF Recommendation 14.
[18] FATF (n 10).
[19] Jennifer Calvary, FinCen, 'Stopping Terror Finance: A Coordinat2ed Government Effort,' Testimony to the United States House of Representatives Committee on Financial Services Task Force to Investigate Terrorism Financing (FinCEN, 24 May 2016). Available at <https://www.fincen.gov/news/ testimony/testimony-jennifer-shasky-calvery-director- financial-crimes-enforcement- network> (accessed 1 June 2017).
[20] FATF (n 13) Recommendation 18.
[21] FATF (n 13) Recommendation 20.
[22] UK Financial Conducts Authority, 'Call for Input: Supporting the development and adoption of RegTech' (FCA, 23 November 2015). Available at <https://www.fca.org.uk/news/news-stories/call-input-supporting-development-and-adoption-regtech> (accessed 2 February 2017).
[23] Big data analytics is the process of examining large and varied data sets - i.e., big data - to uncover hidden patterns, unknown correlations, market trends, customer preferences and other useful information that can help organizations make more-informed business decisions. Driven by specialized analytics systems and software, big data analytics can point the way to various business benefits, including new revenue opportunities, more effective marketing, better customer service, improved operational efficiency and competitive advantages over rivals. Big data analytics applications enable data scientists, predictive modellers, statisticians and other analytics professionals to analyse growing volumes of structured transaction data, plus other forms of data that are often left untapped by conventional business intelligence and analytics programs. That encompasses a mix of semi-structured and unstructured data-- for example, internet clickstream data, web server logs, social media

content, text from customer emails and survey responses, mobile-phone call-detail records and machine data captured by sensors connected to the internet of things. For more on this see TechTarget, 'Big Data Analytics' (2017). Available at <http://searchbusinessanalytics.techtarget.com/definition/big-data-analytics> (accessed 2 April 2017.

[24] For more on this see Martin Arnold, 'Market grows for 'regtech', or AI for regulation' (Financial Times, 14 October 2016). Available at <https://www.ft.com/content/fd80ac50-7383-11e6-bf48-b372cdb1043a> (accessed 3 April 2017). Also see Deloitte, 'RegTech Is The New FinTech: How Agile Regulatory Technology Is Helping Firms Better Understand and Manage Their Risks' (Deloitte, 2015). Available at <https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/ie-regtech-pdf.pdf> (accessed 3 April 2017).

[25] Innovate Finance was founded in 2014 with the support of the City of London and Canary Wharf Group, Innovate Finance aims to accelerate the UK's leading position in the global financial services sector by directly supporting the next era of technology-led financial services innovators, from start-ups to institutions. With over 250+ members, Innovate Finance seeks to address the key barriers and opportunities in the FinTech ecosystem: attracting greater investment, supporting the development of proportionate and effective regulation, engaging in community collaboration, and promoting innovation in financial services, whilst championing an open, inclusive and secular FinTech community. Members range from start-ups to the world's leading global corporations. Through Innovate Finance membership they have a single point of access to innovators, investors, regulators, policy makers and commercial partners. For more on this see Innovate Finance, 'About' (2017) Available at <http://new.innovatefinance.com> (accessed 3 April 2017).

[26] FATF (n 10) 6.

[27] This is regardless of the public nature of transaction information available on the blockchain which theoretically facilitates transaction monitoring, but as noted in the June 2014 VC Report (Appendix A), the lack of real world identity associated with many decentralised VC transactions limits the blockchain's usefulness for monitoring transactions and identifying suspicious activity, presenting serious challenges to effective AML/CFT compliance and supervision.

[28] Peter Lee, 'Banking: Regtech promises better and cheaper AML and KYC compliance,' (Euromoney, 20 February 2017). Available at <http://www.euromoney.com/Article/3663095/Banking-Regtech-promises-better-and-cheaper-AML-and-KYC-compliance.html?p=2> (accessed 3 April 2017).

[29] As of this writing, the WGI are based on 340 variables produced by 32 different sources, including commercial information providers, surveys of firms and households, non-governmental organizations and public sector organizations. See also Daniel Kaufmann, Aart Kraay, Massimo Mastruzzi, 'Governance matters VII: Aggregate and individual governance indicators 1996–2007' (World Bank, Washington DC, 2008). Available at <http://info.worldbank.org/governance/wgi/index.aspx#home> (accessed 19 April 2017).

[30] The definitions of the indicators have changed over time since the indicators were first introduced 10 years ago. The indicators are defined to correspond to what the authors consider to be fundamental governance concepts. For more on this see Daniel Kaufmann, Aart Kraay and Pablo Zoido-Lobaton, 'Governance matters' (World Bank, Washington DC, 1999).

[31] See FATF, 'High risk and non-cooperative jurisdictions' (2017). Available at <http://www.fatf-gafi.org/countries/#high-risk> (accessed 15 February 2017).

[32] See World Bank, World Governance Indicators Index (2016). Available at http://info.worldbank.org/governance/wgi/index.aspx#home (accessed 20 April 2017).

[33] See Kaufmann, Kraay and Zoido-Lobaton (n 30). The indicators are defined to correspond to what the authors consider to be fundamental governance concepts.

[34] See World Bank, 'Worldwide Governance Indicators methodology' (World Bank, Washington DC, 2016). Available at <http://info.worldbank.org/governance/wgi/#doc-methodology> (accessed 20 April 2017).

[35] World Bank, 'World Governance Indicators 2016: Aggregate and individual governance indicators for 215 countries and territories over the period 1996–2015, for six dimensions of governance (World Bank, Washington DC, 2016). Available at <http://data.worldbank.org/data-catalog/worldwide-governance-indicators> (accessed 20 April 2017).

[36] ibid.

[37] See IMF Country Report, 'Financial System Stability Assessment' (IMF Report No. 13/325 November 2013), 6. Available at http://www.imf.org/external/pubs/ft/scr/2013/cr13325.pdf (accessed 21 April 2017).

[38] Huw Jones, 'These are the world's fintech Hubs' (World Economic Forum, 9 August 2016). Available at <https://www.weforum.org/agenda/2016/08/these-are-the-worlds-fintech-hubs/> (accessed 22 April 2017).

[39] n 32 above, country: Afghanistan.

[40] ibid.

[41] n 32 above, country: Kenya.

[42] ibid.

[43] n 32 above, country: Nigeria.

[44] ibid.
[45] n 32 above, country: Iraq.
[46] ibid.
[47] n 32 above, country: Sudan.
[48] ibid.
[49] n 32 above, country: Syria.
[50] ibid.
[51] n 32 above, country: Somalia.
[52] ibid.
[53] Stuart Hoegner (ed), *The Law of Bitcoin* (iuniverse, 2015), 7 - 10. Explaining the blockchain in the context of Bitcoin, the decentralised virtual currency, which introduced the concept of blockchain technology.
[54] The delivery of criminal justice should take into consideration the entire system, including the police, the lawyers, prosecutors, judges, and prison officers.
[55] n 32 above, country: Norway.
[56] ibid.
[57] n 32 above, country: Afghanistan.
[58] ibid.
[59] n 32 above, country: Kenya.
[60] ibid.
[61] n 32 above, country: Iraq.
[62] ibid.
[63] n 32 above, country: Nigeria.
[64] ibid.
[65] n 32 above, country: Somalia.
[66] ibid.
[67] n 32 above, country: Sudan.
[68] ibid.
[69] n 32 above, country: Syria.
[70] ibid.
[71] Jonathan Lim, 'A Facilitative Model for Cryptocurrency Regulation in Singapore' in David Chuen (ed), *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments and Big Data* (Elsevier, San Diego USA, 2015) 379.
[72] FATF (n 13) 11.
[73] FATF (n 10) 8.
[74] ibid, 9-10.