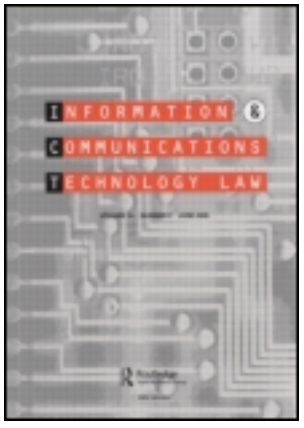

Information & Communications Technology Law
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/cict20

Virtual money laundering: the case of Bitcoin and the Linden dollar

Robert Stokes [a]
[a] The Liverpool Law School, University of Liverpool, Liverpool, UK
Published online: 11 Dec 2012.

To cite this article: Robert Stokes (2012) Virtual money laundering: the case of Bitcoin and the Linden dollar, Information & Communications Technology Law, 21:3, 221-236, DOI: 10.1080/13600834.2012.744225

To link to this article: http://dx.doi.org/10.1080/13600834.2012.744225

Information & Communications Technology Law
Vol. 21, No. 3, October 2012, 221–236

Routledge
Taylor & Francis Group

Virtual money laundering: the case of Bitcoin and the Linden dollar

Robert Stokes*

The Liverpool Law School, University of Liverpool, Liverpool, UK

This paper presents an analysis of the money laundering risks of two virtual currencies, the Linden dollar, the in-world currency of the interactive online environment Second Life, and Bitcoin, an experimental virtual currency that allows for the transfer of value through peer-to-peer software. The paper will demonstrate that although these virtual currencies have money laundering utility, they are currently unsuitable for laundering on a large scale. The paper also considers whether either of these virtual currencies fall under the scope of the Money Laundering Regulations 2007 and draws on similarities with online gambling to suggest a method of incorporating the Linden dollar and Bitcoin within the anti-money laundering framework.

Keywords: money laundering; virtual currency; virtual worlds

Introduction

The increasing scale and rigour of anti-money laundering regimes across the globe coupled with the vast extent of criminal proceeds has necessitated a certain creativity on the part of money launderers. Whilst, for obvious reasons, it is very difficult to ascertain the extent of laundering at either national or international level it has been estimated that figure is likely to be in the range of 1–3% of global GDP (Camdessus, 1998). Similar estimates for the amount laundered in the UK range from £19bn to £48bn (Harvey, 2005, p. 340). With the increasing depth and breadth of anti-money laundering measures, it is self-evident that a launderer cannot use only a handful of poorly regulated cash intensive businesses, such as casinos (Gallant, 2005, p. 11), or industries, such as the mainstream banking sector including for example the controversy surrounding the use of banks and financial institutions in London by General Abacha (Financial Services Authority (FSA), 2001), in order to surreptitiously integrate illicit funds into the mainstream financial world. This necessity has led to the diversification of money laundering methods or typologies so *anything* that has value is susceptible to money launders and any mechanism, technology or indeed profession, which facilitates the transfer of value, is equally vulnerable (Alldridge, 2003, pp. 2–3). The only limitation to the methods and techniques used to launder criminal funds is the imagination or creativity of would-be launderers themselves (Kennedy, 2005, p. 317). The co-evolution of currency and criminality has been noted: every new form or

*Email: R.Stokes@liverpool.ac.uk

ISSN 1360-0834 print/ISSN 1469-8404 online

http://dx.doi.org/10.1080/13600834.2012.744225
http://www.tandfonline.com

conception of money has served to provoke a 'new creativity in financial wrongdoing' (Mackenzie, 1998, p. 30). This article has three aims. First, it outlines and critically appraises the money laundering vulnerabilities of two novel virtual currencies, the Linden dollar and Bitcoin. This is important since the global (and many domestic) legal response to money laundering is determined by the specific risks identified. Thus, at a simplistic level, low-risk products have simplified anti-money laundering requirements whilst high-risk products have intensified regulation. Secondly, it considers whether the existing anti-money laundering regulation extends to virtual currencies such as Bitcoin and the Linden dollar. Thirdly, it critically considers how these virtual currencies might be regulated and integrated into the anti-money laundering regime of the United Kingdom. It will be contended that although virtual currencies could be useful for money launderers, their current operation is such that any large scale laundering would be very likely to garner unwanted attention and most probably detection. Nonetheless, regulatory attention is desirable if these emerging currencies gain economic momentum and wider uptake. However, notwithstanding the money laundering risks evident, it will be suggested that these virtual currencies could be relatively easily integrated into the anti-money laundering framework.

Money laundering and technology

It is useful to offer a brief introduction to the process of money laundering and the role played by technology in facilitating the evolution and diversification of money laundering typologies to place the discussion in context. Despite the multitude of discrete typologies money laundering itself is relatively easy to define. It is the process by which unlawful funds are bestowed with the appearance of legitimacy or lawfulness or, alternatively, the illicit nature of the funds is obscured (Hinterseer, 2002, p. 11). Most simply, it is the process by which criminals cleanse the fruits of their criminal labours. As Lilley (2006, p. 6) has noted:

> Laundering is the method by which all proceeds of crime are integrated into the banking systems and business environments of the world . . . [T]his is the process whereby the identity of dirty money that is the proceeds of crime and the real ownership of these assets is transformed so that the proceeds appear to originate from a legitimate source.

Thus follows the generally accepted (though simplistic) tri-partite analysis of the money laundering process: placement, layering and integration (Gilmore, 1999, pp. 30–31). Within this broad framework, there are innumerable distinct money laundering methods and typologies ranging from the simple (yet ingenious) to the hugely complex. Indeed, Alldridge, relying on the observations of the Financial Action Task Force (2003, p. 3) suggests that there are 'an infinite number of mechanisms whereby money, commonly is laundered' (2003, p. 3). The US Department of State stated that the methods of laundering money are 'innumerable, diverse, complex, subtle and secret' (1988, p. 46). Furthermore, Ward (2004) cited a 2002 scheme to launder criminal funds through the Inland Revenue. The process worked through setting up front companies, overpaying tax liabilities using illicit funds in order to then claim the overpaid tax back. The Inland Revenue would then repay in the form of a cheque, thus changing the form of the funds, and also, crucially giving the complete appearance of legitimacy. The vulnerability of emerging

payment technologies to crime generally and money laundering specifically has long been recognised. Zagaris and MacDonald suggested:

> For those who conduct serious crimes, such as drug trafficking, arms smuggling, and terrorism, technological breakthroughs offer more sophisticated variations of the traditional means to launder ill-gotten proceeds. (1992, p. 63)

Moreover, it has been suggested that:

> Emerging technology, including the Internet's cyber-banking industry, will 'revolutionise' the money laundering process and make it significantly easier for launderers to insert dirty money into the stream of international commerce, to churn or wash it through legitimate businesses and hide its origin, and then to withdraw the money, ready to be spent. (Mills, 2001, pp. 365–366)

Certainly, with the evolution of electronic money and the internet came the potential for 'cyberlaundering', defined as the use of the 'Internet and stored value cards to turn illegally obtained money into clean, untraceable funds' (Welling and Rickman, 1998, p. 310). The continued development of payment (and other) technologies, it may be suggested, now allows for 'virtual laundering'; the use of virtual currencies and/or virtual environments to launder criminal funds and bestow them with the appearance of legitimacy whilst simultaneously obscuring their actual, illicit, origin. Virtual laundering typologies include the use of online casinos, virtual worlds (such as Second Life); massively multiplayer online role-playing games, abbreviated to MMORPG, (such as World of Warcraft); the use of digital precious metals (such as e-gold ltd.).

Laundering though Bitcoin and the Linden dollar

BitCoin

Bitcoin is an experimental virtual currency created, managed, and transferred ('spent') via a Peer-to-Peer (P2P) network, over the internet via users running the necessary software.[1] A BTC is a string of numbers generated by a computer, normally stored on a computer[2] (in a digital wallet) which can be used as payment at any retailer which accepts BTCs as payment (or transferred to any individual running the Bitcoin software). BTCs are not backed by any government or commercial organisation and as such there is no guarantor supporting each BTC. A BTC has value as a unit of currency only through confidence: individuals and organisations accord it value and accept it as payment for goods or services.[3] Though the number of businesses which accept BTCs is small, a market for the purchase and sale of BTCs has emerged through various Bitcoin exchanges. As of March 2012, one BTC is valued at around $4.5. The creation of BTCs is intriguing. In short, a BTC can be generated by anyone, anywhere, using the Bitcoin software, by what is referred to as 'mining' (Aron, 2011). In essence, BTCs are created as a computer solves a mathematical problem the difficulty of which is pre-determined by the software and adjusts over time in a pre-determined manner and at a stable rate. Thus, as more BTCs are generated, the computational effort required to create further BTCs increases.[4]

The process of spending this virtual currency is dependent on two further matters: A Bitcoin address and a private Bitcoin key. A Bitcoin address is a chain of

alphanumerical characters which signifies a possible recipient of a BTC. It can be thought of as an email address to which BTC payments can be sent. Every Bitcoin address has an associated private key which can be regarded as the 'ticket' which allows a user to spend the BTC. It is saved in the digital wallet of the holder. Without a key, transactions are not possible and as such if the key for a Bitcoin address is lost, any BTCs associated with that address are also lost (permanently).[5]

The Linden dollar

The Linden dollar is another example of a virtual currency, though it is distinct from the BTC in both purpose and design.[6] The Linden dollar is the in-world currency of Second Life,[7] an online interactive environment or virtual world designed and maintained by Linden Labs. It is accessed through the internet and created by its residents who are graphically represented in this virtual world by avatars. Residents have the ability to explore this virtual world and interact with other avatars for whatever purpose.[8]

The Linden dollar can be used to purchase virtual land, goods and services. Residents can receive Linden dollars through a variety of methods. First, certain residents can receive a weekly stipend of 300 Linden dollars, although this is dependent upon the subscription level of the resident concerned. There are two main levels of subscription, basic and premium. The basic account is free from (real-world) monthly fees but offers a more limited experience, and does not offer a stipend. The premium subscription requires a monthly fee but results in greater in-world service and a weekly stipend. Secondly, and irrespective of subscription level, residents can earn Linden dollars through in-world transactions (e.g. the sale of virtual goods) or, thirdly, residents can purchase Linden dollars through a virtual currency exchange, the LindeX.[9] Using the LindeX, residents purchase Linden dollars for United States dollars (or other real world currency local to the user). The value of the Linden dollar has proven to be stable (stability being maintained by Linden Labs) maintaining an exchange rate of around $1 to L$ 255.

Laundering risks of BTC and the Linden Dollar

It is crucial to identify the money laundering risks associated with any emerging payment or value transfer mechanism or product since it is only through understanding those risks that they can be effectively mitigated. It is for this reason that the Financial Action Task Force (FATF), for example, publishes typology reports which detail both particular money laundering processes identified over a given period and specific risk factors associated with those typologies.[10] The process of assessing money laundering risks now plays a fundamental role following the emergence of the risk-based approach to anti-money laundering regimes, led by, inter alia, the FATF and the European Union.[11] Under this proportionality-orientated approach, firms (and states) must ensure that they (i) recognise the laundering risks of their business; (ii) assess those risks and (iii) mitigate those risks as far as is possible. This section of the paper will therefore outline some of the core money laundering risks inherent to BTCs and the Linden dollar.

Both BTCs and the Linden dollar share a number of key features which make them attractive to money launderers. In short, the risks posed are largely the same as for electronic money (pre-paid, stored value products)[12] and digital currencies (such

as digital precious metal dealers) in that they offer an accessible facility for the transfer of value across international borders without reliance on the (heavily regulated) traditional financial and credit institutions. This is particularly significant and is one of the key money laundering risks posed by both the Linden dollar and BTCs. A similar assessment of digital currencies led to the conclusion that such currencies were an 'ideal money laundering instrument' (United States Department of Justice, 2008, p. 1). Thus, two users of either Bitcoin or Second Life could transfer value to one another in the form of BTCs or Linden dollars without any bank or financial institution being involved at any stage. In fact, with peer-to-peer movements of value such as these, the transfer could be made without any professional acting as intermediary. This is problematic since the general approach of anti-money laundering regulation (whether at a global or national level) has focused upon the use of key professions as de facto policemen, guarding entry points into the financial system and limiting the ability of criminals to transfer value without scrutiny (Wadsley, 1994). Transfers through Bitcoin and Second Life could circumvent the plethora of anti-money laundering regulation developed over the past twenty-five years (Weimer, 2000–2001, pp. 225–226).

This circumvention of the established financial infrastructure is exacerbated by the fact that both BTCs and the Linden dollar allow for the transfer of value without any face-to-face contact and without regard for international borders. The FATF has stated that it renders such products particularly vulnerable to identify-fraud enabled laundering operations (Financial Action Task Force, 2010, pp. 40–41). The risk-based approach of the Third EU Directive makes it clear that enhanced due diligence is required where the customer is not physically present for identification purposes (Article 13(2)).[13]

A further core money laundering risk of the Linden dollar and BTC is anonymity in transferring value. The vulnerability of any financial (or other) product which masks ownership and identity whether intentionally through product design, operationally through product use (such as the ability to use pseudonyms, obviously false names or multiple accounts, etc.) has long been recognised. See, for example, the Austrian Sparbuch accounts discussed in Lilley (2006, pp. 10–11). Unsurprisingly, reflecting the risk anonymity poses to constructing a viable audit trail, both the EU and the FATF (together with most individual states) prohibit anonymous accounts with financial and credit institutions.[14]

In the case of Bitcoin, although each BTC transfer is published within the software itself, anonymity is essentially preserved since the only data which is available is the amount of the transfer and the public addresses involved in the transfer[15] and there are no records linking any public address to an individual or organisation. Public addresses within Bitcoin are not static in the sense that an address may well be used for only one BTC transfer (indeed, that is the advice of the Bitcoin developers). This, coupled with the easy availability of new addresses would suggest that knowledge of the public address and transaction history of a BTC is, independent from further evidence, of little use to any law enforcement investigation. Even where IP addresses are recorded and retained, it is questionable how effective this would be in offering useful intelligence on a professional, organised launderer. See for example, the discussion of architectural anonymity by Hollis (2011, pp. 397–400).

Finally, the speed and ease of the transactions is an advantage over, for example, cash, which is both awkward and cumbersome to move physically and in respect of

which careful thought must be given to how best to layer the transactions so as to avoid any reporting requirements, whether as a result of moving currency across international borders or suspicious activity-based reporting. Bitcoin and the Linden dollar avoid these limitations of physical currency and allow for the speedy transmission of substantial sums of value (whether in a single transaction or more likely, through the cumulative process of multiple transactions). They also allow for considerably easier payment structuring or 'smurfing' so as to avoid suspicion generally and any reporting provisions specifically.[16] The increased ability to structure payments, or smurf, has been recognised as being a particular risk of electronic money generally: 'technology can help split large amounts through standardised and scarcely risky procedures, that can escape controls on financial transactions and minimise the use of (human and IT) resources devoted to these activities' (Merlonghi, 2010, p. 208). In the case of BTCs, since each transfer would likely be made to a separate Bitcoin address, as noted above, it would be very difficult without any further evidence to link structured transfers to each other.

Virtual laundering: Virtual threat?

It may be thought, given the preceding discussion of the money laundering risks inherent to these virtual currencies, that they present an ideal opportunity for would-be launders, however, this is not the case. Although both forms of virtual currency are likely to avoid the existing anti-money laundering framework in the UK (and EU), there are practical considerations which limit the utility of either as a laundering mechanism at the present time.

One of the significant limitations on the ability to detect money laundering is sheer volume of licit transactions which provide ample cover for launderers to hide behind. This is amplified through modern technologies, such as the wire transfer where it is very much a case of 'not being able to see the wood for the trees'. However, uptake, particularly of BTCs, is almost trivial from a money laundering perspective with 8,673,750 BTCs currently in existence as of March 2012. At the current exchange rate, the totality of BTCs created to date is $39,031,875. If criminals were to suddenly employ BTCs as a core money laundering mechanism, it would be readily revealed through exchange rate fluctuations since this market is volatile. This volatility is well demonstrated by the crash of BTC value following the theft and subsequent fraudulent sale of a significant volume of BTCs (Wallace, 2011). Although it would not be possible to link such movement with money laundering, it would incur attention both within the Bitcoin community and, ultimately at a law enforcement level. It is unlikely that the attention such market events would garner would be in the interests of a money launderer.

The same limitation applies to the Linden dollar where although the financial figures are significant, it may be argued that it is not suited to any large-scale laundering operation. User-to-user transactions in 2009 totalled US$567 million and the US dollar value of Linden dollars in circulation totaled US$26.5 million in December 2009 and $29.3 in 2011.[17] Thus, whilst the volume of Linden dollars in virtual circulation is significant (ibid), it is not sufficient, in real world currency value, to surreptitiously integrate large volumes of illicit currency. Moreover, since the Linden dollar is an in-world currency only, i.e. it cannot be used for payment outside of the Second Life environment, the launderer would have to both place the illicit funds into Linden dollars and convert into real-world funds without detection.

Given the measures put into place by Linden Labs which suspend the LindeX where the value of the Linden dollar moves (in either direction) by more than a predefined percentage, the launderer would need to ensure that the exchange of Linden dollars into real world currency was organised in such a way so as to avoid this eventuality.

Second Life has also designed in various financial limits on its users in accordance with their previous financial activity and length of time as a user of Second Life. These limits serve to reduce the utility of the Linden dollar to launderers. Hence, if a launderer had accumulated 10 million Linden dollars as of March 2012, this would have a dollar value of $39,000. Since the highest resident level only permits the sale of $5000 per 30 days, even such a small sum of money would take a significant length of time to convert into US dollars.[18]

Regulating virtual currency?

Having identified that both the BTC and Linden dollar possess money laundering utility, the question becomes one of how the regulatory framework can deal with these novel payment processes. This section will use the United Kingdom's anti-money laundering framework to consider two fundamental questions.[19] First, could virtual currencies such as BTCs or Linden dollars fall under the Money Laundering Regulations as currently drafted? Secondly, if not, how could they be regulated?

It might be presumed that the Linden dollar and BTCs are archetypal examples of electronic money. Electronic money has long been recognised as presenting various money laundering threats, and consequently electronic money products are regulated at a pan-European level via the Third Money Laundering Directive, implemented in the United Kingdom by the Money Laundering Regulations 2007 (SI 2007/2157). If either of the virtual currencies under consideration were deemed to be 'electronic money', any issuer (miner) or exchange service provider in the United Kingdom would fall under the scope of the Money Laundering Regulations.

It would seem clear, however, that neither the Linden dollar nor BTC would fall within the legal conception of electronic money in the Second E-Money Directive (2009/110/EC). Notwithstanding the fact that the Directive makes it clear that the definition of electronic money should be technically neutral, thus capable of applying both software- or card-based products[20] the definition is not sufficiently broad so as to include products such as the BTC or Linden dollar. Article 2(2) states that 'electronic money' is:

> electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions . . . and which is accepted by a natural or legal person other than the electronic money issuer.

A BTC does not involve a claim on the issuer, rather the BTC itself is the unit of currency. It is not a pre-paid access product (i.e. issued on receipt of funds) as a BTC is issued as computers solve mathematical problems. It is not the representation of value transferred from the acquirer to the issuer. The Linden dollar is more straightforward since it is, fundamentally, not money. It cannot be regarded as money any more than 'play' money could be deemed real-world currency. This is reinforced by the Second Life Terms of Service itself where it is stated that a Linden dollar is 'not real currency or any type of financial instrument' but rather a 'virtual

token representing contractual permission from Linden Lab to access features of the Service' (para 5.1).

It is possible that businesses offering Bitcoin exchange services within the UK are already covered by virtue of the inclusion of money service businesses within the scope of the Money Laundering Regulations 2007. A money service business is defined under these regulations as, inter alia, dealing in currency exchange, transmitting money *or representations of monetary value* by any means. This is significant since where a business falls under this definition, it is included within the broad scope of a 'financial institution' within the regulations. This would be significant for Bitcoin exchanges based in the United Kingdom (and the EU generally) since if they are included within this definition then their money laundering obligations would be that same as those imposed on every other financial institution. 'Financial institution' is defined by reg.3(3) as an undertaking, including a money service business, when it carries out one or more of some of the activities listed in Annex 1 of the Banking Consolidation (Directive 2006/48/EC). Those activities cover a substantial range of financial services, however, the most pertinent for our analysis of Bitcoin is point 4 of Annex 1, payment services within the Payment Services Directive 2007 (64/EC).[21]

This Directive covers a wide range of payment services, however, the most relevant activities are those found at points 5 and 6 of the Annex: Issuing and acquiring payment instruments and money remittance. A payment instruction is defined in Art.4(23) as being 'any personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used by the payment service user in order to initiate a payment order'. Bitcoin would not fall under the former since the BTC is not the payment instruction, but rather the object of a payment instruction. Neither will Bitcoin fall under the definition of 'money remittance' and thereby be included within the ambit of the Payment Services Directive (and thereby also the Money Laundering Regulations). Article 4(13) defines 'money remittance' as:

> a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.

This would include a number payment process (including for example, hawala) but does not appear to describe the conception or application of Bitcoin since Bitcoin is not a payment service in this sense. A 'corresponding amount' of money is not made available to the payee from the payer, rather, currency is exchanged for what is in effect a bearer payment instrument, a BTC.

If correct, this analysis would preclude Bitcoin exchanges from the ambit of the Money Laundering Regulations and consequently the only remaining option for their inclusion within the domestic anti-money laundering framework as a money service business is through the catch all provision of point 5 of the Annex to the Banking Consolidation Directive: Issuing and administering other means of payment which are not covered by the Payment Services Directive. This is intended to include payment products such as paper-based vouchers, however, it is unlikely that the scope of this provision could be extended so as to include BTCs, which are conceptually not a payment service but rather a form of currency.

In spite of contrary indicators, in principle, virtual currencies, such as the Linden dollar and BTCs are entirely amenable to regulation within the established anti-money laundering framework notwithstanding the fact that it would appear that both currently escape the domestic anti-money laundering framework. The central tenets of any anti-money laundering regime seek to deter laundering by ensuring that vulnerable businesses understand the laundering risks of their product or services and, crucially, that they understand their customer. This is achieved through customer due diligence (CDD) provisions which allow for both an understanding of suspicious transactions and the collation and retention of identification. This is crucial to ensure a sound audit trail in the event of any subsequent investigation. The third tenet to the preventative framework relies on private sector reporting, whether of suspicious activity and or of activity above a particular threshold.

This section of the article will consider the regulatory approach to online casinos, which represents an analogous method of transferring value sharing similar risk factors as virtual currencies. It must be emphasised at this point that the question of effective regulation of any product which allows for the transfer of value across borders is ultimately one of international co-operation. One country alone cannot hope to effectively regulate such activity. However, the article seeks to demonstrate that existing legal frameworks, such as that in the United Kingdom, can deal with the challenges posed by virtual currencies.

In an online casino, a customer transfers real money in order to gamble with virtual chips. In effect, this is an online interactive environment similar to that of Second Life, where instead of Linden dollars as a store or token of value virtual chips are used instead. The chips may be used in regular casino games where the customer bets against the 'house' i.e. the casino, or from peer-to-peer in online games such as poker. The chips are therefore easily transferable to another user. Thus, if User A in country 1 wanted to transfer value to User B in country 2, User A could quite easily do so by transferring casino chips to User B through arranging a $1-1$ game of poker in which User A 'loses' (i.e. transfers) all of their chips to his 'opponent', User B. Consequently, the risks of online casinos are analogous to those of both BTC and the Linden dollar. Online casinos offer a means of transferring value across national boundaries in an easy and fast manner without any face-to-face contact. The virtual chips only have real world value when the user 'cashes out', that is, exchanges the chips acquired online for real world currency as is the case with the Linden dollar and Bitcoin. The anti-money laundering regulations imposed on online casinos are likely to offer a useful starting point in considering whether BTCs and the Linden dollar can be regulated so as to effectively mitigate their laundering utility.[22]

The Money Laundering Regulations 2007 impose a comprehensive regime of anti-money laundering requirements on online casinos. They are specifically included within the gateway concept of 'relevant persons' (reg. 3(1)(h)) and have a tailored CDD regime to comply with under reg.10. This requires the casino to establish and verify the identity of all customers before access is given to any remote gaming facility (Reg.10(1)(a)(ii)) or where the customer purchases or exchanges casino chips totaling €2000 or more. Under reg.14, since the customer will not be physically present for identification checks, the provision of remote gaming services are required to take additional measure when verifying the customer identity such as requesting additional documentation or most likely, by requiring that the first

payment is carried out through an account in the customer's name with a credit institution (reg. 14(2)).

Under reg.20, the casino is required to establish policies and procedures in respect to all of the following matters: CDD and monitoring; reporting; record-keeping; internal control; risk assessment and management; and monitoring of compliance with anti-money laundering policies and procedures. Furthermore, these policies must provide for the scrutiny of (i) complex or unusually large transactions (ii) unusual patterns of transactions which appear to have no economic purpose and (iii) any other activity which the casino deems is particularly likely to be related to money laundering.[23]

The third tenet of the anti-money laundering regime is that is that of reporting which is dealt with under s.330 of the Proceeds of Crime Act 2002. Casinos are included within the reporting framework of this Act by virtue of schedule 9(1)(1)(r). Under s.330, a person must disclose (as soon as is practicable) where they either know or suspect that another person is engaged in money laundering where the information which gave rise to the knowledge or suspicion came to him through the course of a business in the regulated sector.

Online casinos operating under the necessary license in the United Kingdom must comply with CDD, record keeping, and reporting requirements. The same framework could be applied to virtual currencies. In the case of the Linden dollar, it would seem that a two-pronged approach could be adopted which places the regulatory focus both on Linden Labs to monitor the transfer of Linden dollars from user-to-user and also on any operator of an exchange facility which affords virtual currency real world value. The latter point is crucial since the laundering potential of both Linden dollars and BTCs stems from the fact that they can be exchanged for real world currency. Regulatory efforts, must then, focus on the stage where stored value moves from the virtual world into the real world. This process of exchange is readily susceptible to money laundering control. Businesses offering such services should, it may be argued, be required to comply with the same money laundering regime as applicable to those offering remote gaming facilities. Thus, at the point where the virtual currency is exchanged for real world currency, customers should be subject to standard CDD measures and businesses ought to take steps to verify the customers' identity and maintain records of transactions made. This can be done at both stages of the exchange process – where real world currency is used to purchase virtual currency and vice versa.

There is one fundamental difficulty in the application of such a system of regulation in respect to Bitcoin, and that stems from the fact that Bitcoin is decentralised, both in the issuance of new BTCs but also, crucially, in terms of the software which acts as the payment system. Whether or not Bitcoin is conceptualised as a currency or not, there is no central organisation upon which these money laundering controls could be imposed. It may be thought that the software developers could introduce changes to the software itself allowing for the monitoring of transactions and the process of de-anonymising transfers. However, since the Bitcoin software is open source and developed by the Bitcoin community generally, Bitcoin is not centrally controlled by one organisation or business. This is difficult from a regulatory perspective since the entirety of our current anti-money laundering framework is predicated on the assumption that there are central organisations or businesses which can impose obligations.

This difficulty is mitigated to an extent by the requirement to exchange BTCs for real-world currency. If a virtual currency has no real world value, i.e. it cannot be exchanged for real world currency or spent outside of the virtual environment, then the money laundering risks associated with the product are mitigated. This is true even for Bitcoin even though it is designed to be form of money in its own right since and is accredited with value by those who accept it as payment.[24] In principle, a BTC could remain in circulation indefinitely without being converted into real-world currency. This would allow BTC transfers to avoid money laundering controls if those controls were solely focused on the exchange mechanism. However, given the limited acceptance of BTCs as payment, businesses, it can be suggested, will only accept BTCs due to their ability to be exchanged for real-world currency. This allows a system of anti-money laundering regulation to focus upon the BTC exchange businesses, although the situation would be different if the BTC ever becomes universally accepted.

One fundamental regulatory advantage stemming from the need to exchange BTCs into real world currency is that it mitigates the anonymity of each BTC user since it will allow for the CDD and other anti-money laundering provisions to take effect at this point. The exchange process acts as a regulatory choke point. Thus, a system of registration or licensing of BTC exchange business could be introduced and those businesses could easily be incorporated into the existing anti-money laundering framework. Although this will not, of its own accord, allow for the tracking of transfers from one Bitcoin user to another, it will allow for the value of the BTCs, once converted, to be traced into the real-world financial systems. This of course is dependent upon the format of the value once converted out of the Bitcoin system. If, for example, a Bitcoin user can elect to take the value of his BTCs as cash, then this will cease to be traceable in any meaningful sense, although, it should be pointed out that it is unlikely that any serious laundering operation would want to exchange BTCs for cash (since it is likely that converting cash is likely to be one of their greatest operational difficulties in any event) and furthermore it would at least ensure that the identity of the individual who is exchanging BTCs for real world currency is documented, verified and stored thus allowing for both an audit trail and CDD at that point.[25]

Conclusions

It hardly needs to be restated that the emergence of new and alternative payment technologies and products pose a genuine money laundering risk. Whilst those risks may be only potential at present, it is clear that the current legal framework is unable to deal with these novel means of transferring value, particularly where, as is the case with Bitcoin, the traditional financial infrastructure is circumvented through a peer-to-peer model of both value creation and value transfer. That the current framework is ill-equipped to deal with such mechanisms is not surprising given the historical development of both laundering typologies and the development of the legal response to them. Nonetheless, it may be suggested that the legal treatment of analogous typologies such as online casinos is useful in demonstrating how these emerging value transfer products could be incorporated into the anti-money laundering framework. It must also be emphasised that although these new payment products are challenging from a regulatory perspective in many instances they can, if properly designed, be intrinsically less subject to criminal misuse than existing

typologies and payment products, such as, cash. One of the greatest difficulties to solve is how to define and conceptualise virtual currencies. Are they for example 'money' and thereby a 'money service business'. The Linden dollar is unlikely to be considered 'money' being more suitably defined as a digital commodity. This issue in respect of Bitcoin is more uncertain and requires further analysis so as to allow for an effective regulatory framework to be constructed.

As the definition of electronic money demonstrates, it is difficult to define emerging products with sufficient clarity so as to apply to all possible formulations whilst simultaneously avoiding unintentional inclusions and also future-proofing the concept. Once that definition has been established, however, it would be possible to require, for example, the various virtual currency exchange businesses to establish general anti-money laundering policies as laid down by the Money Laundering Regulations 2007 (reg. 20) and the creation of a supervisory body with responsibility for monitoring the application of such policies mirroring the current regulatory system dealing with, for example, money service business.

There are, however, risks inherent to incorporating virtual currencies into the anti-money laundering regime. First, and foremost, there is a danger that creativity and technological development will be stifled under the weight of intensive money laundering requirements. This is not insurmountable. It could easily be the case that particular payment products or services are integrated into the regulatory regime using a progressive stepped-approach. Thus, for example, one could include the virtual currency exchange businesses within the customer due diligence and record keeping requirements, but absent those businesses from the reporting regime for a set period of time. A similar approach was adopted by the United States in the 1990s in order to protect the then fledging pre-paid card and electronic money industry.[26]

This objection could also be met in part through the use of specific exemptions where the level of exchange is below certain levels. The use of such provisions is well established, as noted above in the context of online casino due diligence measures. Similarly, de minimis provisions within the framework employed for electronic money could be adapted in order to limit obligations of smaller businesses offering virtual currency exchange mechanisms.[27]

The second danger in regulating virtual currencies is that it could be thought of as an over-zealous approach to something which would appear to be of little practical use to a prospective launderer. Birch (2007, p. 7) has suggested that:

> Imposing stringent tracking and monitoring requirements on low-value epayment schemes when no such strictures apply to banknotes is, in effect, another hidden subsidy to cash and getting obsessed with smurfing wizards when they account for a tiny, tiny fraction of criminal transactions, is a distraction.

It has been noted that the laundering potential of virtual currencies is, at present, minimal. However, virtual currencies do constitute a genuine money laundering risk and as such, attention ought to be given as how best to manage those risks.

Two further observations can be made. First, if these virtual currencies become more popular, the ability to launder criminal funds using Bitcoin or Linden dollars will increase accordingly. It would be preferable from an anti-money laundering perspective that pre-emptive attention is given to these facilities before their use becomes widespread. Secondly, it must be recognised that virtual currencies do presently allow for small-scale laundering operations, notwithstanding any of the money laundering limitations whether by design or volume.[28] Whilst this is a

significant issue, it is also true of every other payment technology whether emerging or established.[29] The likelihood of current anti-money laundering regulation detecting, for example, an illicit £5000 wire transfer is very slender indeed without any other factors to arouse suspicion. It should also be remembered that this is not a zero tolerance area of regulation. Since *anything* of value can be misused to launder criminal proceeds, there is a balance which must be struck. As Bosworth-Davies notes:

> It would require a counsel of perfection to require banks and financial institutions to institute a regulatory regime which would ensure that the phenomenon of money laundering was extinguished forever from commercial life. (1994, p. 56)

Instead, the task must be to identify the particular risks posed by the product and mitigating them as far as is possible whilst protecting the social or financial utility of the product itself. The aim of the anti-money laundering regulation is not to prevent every instance of laundering from occurring, but rather, to create an environment where it is increasingly difficult to launder criminal funds without detection and to force the launderers to employ increasingly risky methods of laundering as the intensity of regulation on known laundering products and services increases.

Notes

1. The software, freely available, is also called Bitcoin. Therefore, to avoid confusion, this paper uses the abbreviation BTC to refer to the currency specifically.
2. Physical BTCs have been developed to facilitate the use of BTCs in a face-to-face transaction. A physical BTC can take a variety of physical forms (in fact, it could take *any* physical form) but the underlying principle is the same as that with the virtual counterpart: The code is physically transcribed, for example on a piece of paper which is then enclosed, by a physical surround, such as a card or coin type and then protected by a tamper proffer seal such as a hologram. The bearer can then use this in a face-to-face transaction with anyone who accepts BTCs as payment. Once used, the physical BTC ceases to have any value and is worthless.
3. Though unusual, this is not unique as demonstrated by the ability of the 'Swiss' dinar to retain its use and value in Iraq after it ceased to be legal tender in Iraq following the Gulf War.
4. See https://en.bitcoin.it/wiki/FAQ#How_are_new_Bitcoins_created.3F
5. Similarly, if the data is overwritten, the BTC's are lost forever, a fate which befell Bitomat (at the time the third largest BTC exchange business). See further, http://siliconangle.com/blog/2011/08/01/third-largest-bitcoin-exchange-bitomat-lost-their-wallet-over-17000-bitcoins-missing
6. Much of the discussion which follows in the context of Second Life is also relevant to other online interactive environments including MMORPG's where conversion of in-game currency into real-world currency is possible.
7. Second Life raises a number of interesting legal issues surrounding online environments and the criminal law which are beyond the scope of this paper. Interested readers may be directed to Kerr (2008) and Landman (2008–2009 at 5171–5176).
8. For an account of activities undertaken in Second Life, see Bond (2009, pp. 122–123).
9. Numerous third-party exchanges are also available, see for example, CrossWorlds xchange based in Gibraltar http://www.crossworldsxchange.com and VirWox, based in Austria https://www.virwox.com. Interestingly, VirWoX accepts BTCs as payment. Thus, you could buy L$ with BTCs.
10. Of particular relevance for this article are the two key Reports dealing with emerging payment methods: FATF (2006) FATF (2010).
11. The risk-based approach was adopted at the EU level by the Third EU Money Laundering Directive (Directive 2005/60/EC) and has recently received greater

prominence at the global level under the revised FATF 40 Recommendations, in particular note the new Recommendation 1. Furthermore, Recommendation 15 requires both states and *financial institutions* identify and assess money laundering risks surrounding 'the development of new products and new business practices, including new delivery mechanisms'. See further, Ross and Hannan (2007) and FATF (2007).

12. For a more detailed account of the laundering risks of these products see, Sienkiewicz (2007).
13. This echoes the recognition of the greater risk of non face-to-face in the Second Money Laundering Directive, Directive 2001/97/EC. See, in particular, Art.3(11).
14. Art.6 and Recommendation 10. Note also that the interpretative notes to the Recommendations expressly deem anonymous transactions as a specific risk factor (at p.64)
15. By way of illustration, an example address is: 37muSN5ZrukVTvyVh3mT5Zc5ew 9L9CBare.
16. The increased ability to structure payments, or smurf, has been recognised as being a particular risk of electronic money generally: 'technology can help split large amounts through standardised and scarcely risky procedures, that can escape controls on financial transactions and minimise the use of (human and IT) resources devoted to these activities' (Merlonghi, 2010, p. 208).
17. https://blogs.secondlife.com/community/features/blog/2010/01/19/2009-end-of-year-second-life-economy-wrap-up-including-q4-economy-in-detail (account needed to view) and http://community.secondlife.com/t5/Featured-News/The-Second-Life-Economy-in-Q3-2011/ba-p/1166705
18. For details of the trading limits imposed by Linden Labs, see https://secondlife.com/my/lindex/describe-limits.php (account needed to view). Note also that the criminal could elect to maintain a presence on Second Life as a business owner rather than resident in which case the limit would be $320,000 per 30 days. They could, if feeling adventurous, join Second Life as a currency trader in which case the limit would be $128,000 per 30 days. Whether the criminal would want the increased scrutiny that would come with setting up anything other than a resident account is doubtful. Conversely, it ought to be noted, that there are examples of electronic money products with restricted value limits which have been employed by launderers. See, for example, the discussion by He (2010, p. 29).
19. Ultimately, payment products such as virtual currencies can only be dealt with effectively through internationally co-ordinated measures, however, as an illustration of how such typologies could be regulated, the UK is a useful case study.
20. See in particular, Recitals 7 and 8 to the Directive. The closing words of recital 8 indicate the intention to 'future proof' the definition but it would seem clear that the design of BTC in particular has escaped this catch-all.
21. Directive 2007/64/EC. Art. 4(3) defines payment service as one of the activities listed in the Annex.
22. Or in any event, at least, offer law enforcement the opportunity to trace the flows of value from source to destination and investigate further where relevant.
23. Reg.20(2)(a).
24. It would seem that BTCs do act as a means of exchange which is core to the concept of money, however, the question is one of how widely the BTC is accepted as payment without question as to the character of the holder, *Moss* v. *Hancock* [1899] 2 Q.B. 111 at 116. At what stage will it become a *universal* means of exchange?
25. If, for example, BTCs were exchangeable for stored value cards pre-loaded by the exchange business this would obviously increase the money laundering risk. These services do currently exist.
26. Providers or issuers of stored value (pre-paid access) products were exempted from registration as a money service business and had only limited anti-money laundering obligations under the Bank Secrecy Act. This more relaxed approach has recently been revoked, see further, http://www.fincen.gov/statutes_regs/frn/pdf/Prepaid_Final_7-22-201.pdf
27. Under the Regulations for example where the sum of transactions on a rechargeable electronic money device is less than €2500 in one calendar year, the provider need not

apply CDD unless money laundering (or terrorist financing) is suspected (this being the combined effect of reg.13(7)(d) and reg.7(1)).

28. Note for example that the daily volume of Linden dollars traded presently ranges from 70,000,000 to 110,000,000 which equates to US dollar values of $280,000 to $445,000.
29. The ability to launder smaller sums of illicit money through virtual currencies would also suggest that such currencies are also suitable for the financing of terrorist cells. The operational funding requirements of such groups are notoriously small and as such these virtual currencies could offer a particularly useful typology for their funding. However, the need for novel mechanisms to transfer operational funds is, it may be suggested negligible since the existing mechanisms, e.g. wire transfers allow for the transfer of operation funds with the risk of detection being very low.

References

Alldridge, P. (2003). *Money laundering law*. Oxford: Hart Publishing.

Aron, J. (2011). Virtual money gets real. *New Scientist*, *210*, 23–25.

Birch, D. (2007). Virtual money: Money laundering in virtual worlds: Risks and reality. *E-Finance & Payments Law and Policy*, *1*, 6–7.

Bond, R. (2009). Business trends in virtual worlds and social networks: An overview of the legal and regulatory issues relating to intellectual property and money transactions. *Entertainment Law Review*, *20*, 121–128.

Bosworth-Davies, R. (1994). CJA 1993: Money laundering. *Company Lawyer*, *15*, 56–58.

Camdessus, M. (1998). Money laundering: The importance of international countermeasures. An address to the FATF at the plenary meeting of the financial action task force on money laundering. Retrieved from http://www.imf.org/external/np/speeches/1998/021098.htm

FATF. (2000). *Report on money laundering typologies*. Paris: OECD.

FATF. (2006). *Report on new payment methods*. Paris: FATF/OECD.

FATF. (2007). *Guidance on the risk-based approach to combating money laundering and terrorist financing*. Paris: FATF/OECD.

FATF. (2010). *Money laundering using new payment methods*. Paris: FATF/OECD.

Financial Services Authority (FSA). (2001). FSA publishes results of money laundering investigation. Retrieved from http://www.fsa.gov.uk/pages/library/communication/pr/2001/029.shtml

Gallant, M. (2005). *Money laundering and the proceeds of crime*. Cheltenham: Edward Elgar.

Gilmore, W. (1999). *Dirty money: The evolution of money laundering countermeasures*. Strasbourg, France: Council of Europe Publishing.

Harvey, J. (2005). An evaluation of money laundering policies. *Journal of Money Laundering Control*, *8*, 339–345.

He, P. (2010). A typological study on money laundering. *Journal of Money Laundering Control*, *13*(1), 15–32.

Hinterseer, K. (2002). *Criminal finance: The political economy of money laundering in a comparative legal context*. The Hague: Kluwer.

Hollis, D. (2011). An e-SOS for cyberspace. *Harvard International Law Journal*, *52*, 373–432.

Kennedy, A. (2005). Dead fish across the trail: Illustrations of money laundering methods. *Journal of Money Laundering Control*, *8* 305–319.

Kerr, O. (2008). Criminal law in virtual worlds. *University of Chicago Legal Forum*, 415–429.

Landman, S. (2008–2009). Funding Bin Laden's avatar: A proposal for the regulation of virtual hawalas. *William Mitchell Law Review*, *35*, 5159–5184.

Lilley, P. (2006). *Dirty dealing: The untold truth about global money laundering*. London: Kogan Page.

Mackenzie, R. (1998). Virtual money laundering, vanishing law: Dematerialisation in electronic funds transfer, financial wrongs and doctrinal makeshifts in English legal structures. *Journal of Money Laundering control*, *2*(1), 22–32.

Merlonghi, G. (2010). Fighting financial crime in the age of electronic money: Opportunities and limitations. *Journal of Money Laundering Control*, *13*, 202–214.

Mills, J. (2001). Internet casinos: A sure bet for money laundering. *Journal of Money Laundering Control*, *8*, 365–383.

Ross, S., & Hannan, M. (2007). Money laundering regulation and risk-based decision-making. *Journal of Money Laundering Control*, *10*(1), 106–115.
Sienkiewicz, S. (2007). Prepaid cards: Vulnerable to money laundering? Federal Reserve Bank of Philadelphia Discussion Paper. Retrieved from http://www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2007/D2007FebPrepaidCardsandMoneyLaundering.pdf
United States Department of Justice (NDIC) Report. (2008). *Money laundering in digital currencies*. Washington, DC: US Department of Justice.
US Department of State. (1988). *International narcotics control strategy report*. Washington, DC: US Department of State.
Wadsley, J. (1994). Professionals as policemen. *Conveyancer and Property Lawyer*, 275–288.
Wallace, B. (2011). The rise and fall of Bitcoin. *Wired*, p. 19.
Ward, C. (2004 February 21). Bulwarks in the fight against crime. *Estates Gazette*, pp. 130–131.
Weimer, W. (2000–2001). Cyberlaundering: An international cache for microchip money. *De Paul Business Law Journal*, *13*, 199–235.
Welling, S., & Rickman, A. (1998). Cyberlaundering: The Risks, the Responses. *Florida Law Review*, *50*, 295–327.
Zagaris, B., & MacDonald, S. (1992–1993). Money laundering, financial fraud, and technology: The perils of an instantaneous economy. *George Washington Journal of Law and Economics*, *26*, 61–107.