Digital Dollars, Virtual Payments, Real World Risk and Regulation.

The risks and regulation of Bitcoin and other digital currencies.

Nigel Morris-Cotterill

World Money Laundering Report

Volume 12 No. 3 July 2013

Vortex Centrum Limited, UK

www.vortexcentrum.com

World Money Laundering Report Volume 12, Number 3.

In this issue

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

THIS DOCUMENT WAS PRODUCED IN JULY 2013 AND MUST BE READ IN THAT LIGHT.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Digital Dollars, Virtual Payments, Real World Risk and Regulation.

The risks and regulation of Bitcoin and other digital currencies.

Nigel Morris-Cotterill,
Financial Crime Risk and Compliance Strategist.

ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Introduction.

Bitcoin is in the news but it is only the latest of a long line of alternative currencies. However, the surge of interest in Bitcoin over a very short period of time means that, at present, it does appear to be the most likely to succeed in gaining a critical mass. However, all e-currencies create a range of risks from systemic risk to economies to regulatory and financial crime risk. These affect populations at large, governments and banks and other financial institutions as well as all those subject to counter-money laundering law and regulation.

Nigel Morris-Cotterill, Financial Crime Risk and Compliance Strategist, first examined the question of e-currencies, private currencies and alternative payment methods in the mid 1990s and has tracked their development, use and failures since.

In this issue of World Money Laundering Report, he examines the regulation, financial and economic risk management issues issues that arise as Bitcoin gains wider acceptance. Inter alia, this paper draws out the distinction between "money" for currency purposes and "money" for counter-money laundering and anti-terrorist financing purposes (AML/CFT/CTF)

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Note: this paper is structured as a series of articles. It is not intended as a single piece to be read from beginning to end. The reason for this is that there are many individual topics which must be introduced and explained but which do not have starting points that fit easily into a logical structure. Readers may find it helpful to read the entire paper, then to return to individual articles once an overall picture has formed in their minds.

This issue of World Money Laundering Report was conceived as a multi-topic issue, as usual. A discussion of Bitcoin was expected to take up about six pages out of its usual 20 (approx). Instead, we are at over 170 pages, almost 30,000 words with many of references to additional reading accessible via the internet instead of copy/pasting substantial extracts.

The subject that initially appeared rather simple turned out to be extremely complex, taking in issues of psychology, economics, technology, law and regulation and, of course, the options of governments in relation to what they perceive as a new threat.

I hope that the explanations here will unravel some myths, create understanding and - most importantly - prepare the financial sector for the wide ranging risks and changes that such a disruptive concept creates.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Nigel Morris-Cotterill
Vortex Centrum – Financial Crime Risk and Compliance
www.countermoneylaundering.com July 2013.

CAVEAT and legal:

Nothing in this paper shall be considered legal or other advice. Where inferences are drawn and extrapolations made, these are the opinion of the author. All persons are cautioned to take specialist advice on their own specific circumstances.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Publisher: Vortex Centrum Ltd, UK.

ISSN: 1473-3439

World Money Laundering Report Volume 12, Number 3.

Overview

In late 2009 or perhaps early 2010, when I began to get quantities of spam about something called "Bitcoin," I kept some of them for a few weeks to see if it looked like it might turn into a risk for our financial sector clients, a headache for regulator and law enforcement clients or an out and out fraud. I tended towards the latter and, after a while when it all went quiet I deleted them.

But Bitcoin has not followed the patterns of many previous virtual currencies which have, like shooting stars, shone brightly and, mostly, burned out in a matter of months. And so when, at the beginning of June 2013, I was asked the simple question "is Bitcoin covered by the Hong Kong Counter-Money Laundering regulations?", I said that the answer was not immediately clear. But, by a process of analysis, I reached the answer:

I'm not at all certain where Bitcoin fits.

Let me put this comment into perspective: it's 17 years since I first analysed how electronic currencies and internet banking interfaced with each other and with the traditional banking sector.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

In doing so, I considered pre-paid cards and I've returned to that on several occasions.

I've looked at systems such as e-gold (which I don't think was as dodgy as it was painted) and a raft of copycats (which, generally, were worse).

I've looked at the use of on-line community building games, like Second Life, in the same light as the original analysis. And I've looked at various forms of e.g. gambling where deposits are made by one person and paid out to another.

I've looked at things like the Bank of Curaçao which was used as a mechanism for circulating fictitious funds arising out of fictitious transactions in a VAT carousel fraud - several thousand million pounds by the way, for those that are getting excited about a couple of recent US successes - and at banks such as the European Bank which wasn't in Europe and was told that its Russian owners weren't welcome on the Caribbean rock it was based on so they transferred ownership to a bunch of Russian émigrés in Florida who held US citizenship - again, remarkably similar to a current case that some people are getting excited about.

I've looked, over and over again, at pre-paid cards -

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

long before they were widely called that. And even longer before they became called "gift cards."

e-cash was the original (or at least the most likely to succeed of the original) electronic currencies. It fell apart, largely, because of lack of take-up. Then there was Mondex, a "wallet" that allowed on-line transfers before the internet was global by using terminals on a telephone line. It also allowed person to person transfers using a wallet into which two cards were placed and a transfer from one card to the other enabled.

Most fascinating of all, I've looked at "time banks" and concluded that this is the ultimate de-materialisation of money - literally, time becomes money.

When Bitcoin first came out, I looked at it, decided (for reasons unconnected with the product) that the whole thing was dodgy and regulators would jump on it and kill it as a fraud. I did not consider whether it was a fraud : for many reasons that would not define whether regulators found a way to close it down, only whether they used it as an excuse. I didn't get as far as looking at money laundering related issues.

So, the question is this: as it is working and regulators have not closed it down as a vehicle for fraud or, for that matter, money laundering or other illegal

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

payments, does it bear any similarity to those other things which have a very chequered past in terms of global approach to their regulation (as, incidentally, do ordinary, boring credit cards)?

So, what is Bitcoin?

That is actually the nub of the problem - and why I thought it would be stamped on.

It's a private currency, unrelated to any national currency. Therefore it operates outside the recognisable financial sector. In this way it is closest to time banking - which is (except for some tax authorities' interest) outside the scope of financial regulation. However, it does interface with national currencies, most obviously the US dollar.

Bitcoin not a national currency, it's not money in the usual sense, usual meaning of the word. But it is a medium of exchange: it's not a vehicle for barter (as, in effect, time banking is).

Box 1: What is Time Banking?

Imagine a simple system under which A performs a service for B and B owes A an equivalent

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

amount of time. So A might mow B's lawn which takes an hour in return for which A spends an hour proof reading documents for A. But what if B cannot deliver any service that A needs? Say, for example, B can cook but A has a maid. But C has no maid and comes home tired each day and would love to be able to pick up a hot meal or even find food waiting in his kitchen just needing a couple of minutes in the microwave. Wouldn't it be good if A could assign the hour he is owed by B to C, and in return C could give him a lift to work and back daily? All that is needed to make this work is some method recording "debits and credits" and cancelling them as the time is used up. So, what if B issued an IOU (promissory note) to A and A could assign it to C when he gets a lift then C assign it back to B when he gets a meal? Everyone gets an hour's service? Everyone gets an hour, no one makes a profit, no one makes a loss. Everyone is happy and they do it all again tomorrow....

That's fine in tiny user-groups, close neighbours, for example. Could it work in a larger, more distributed environment? Take the IOU example a step further, and link it to retail banking. A cheque (unless crossed to restrict its circulation)

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

is a combination of IOU and an instruction to a deposit holder to issue payment if the IOU is presented for payment. The deposit holder has three functions: record cheques presented for credit, keep a record of balances, record cheques presented for debit.

And so, the IOU can be used in two ways: as a direct person to person note - passing outside the record keeping system - in the example above, the IOU moves *qua* token i.e. in a manner similar to a banknote or coin until it reaches its issuer at which point it is cancelled.

But in a larger scheme, it can be passed to a record keeper who marks a debit in the account of the issuer and a credit in the account of the receiver and keeps a record of the new balances in the respective accounts. This is no different, in practical use, to retail banking for a current account.

In fact, it is also exactly the principle which applies to the record keeping functions of virtual currencies: the only difference is that, for virtual currencies, there is at some point an interface with a real-world national currency because,

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

> unlike time, a virtual currency cannot exist in a vacuum of its own making. Or to be more precise, it cannot do so unless and until it achieves widespread popular acceptance to the extent that it can operate alongside or in substitution for a national currency.

So far, bitcoins are not considered to be the equivalent of money in the way that, say, bonds are - if they were, they would be declarable at borders.

But even that argument is open to confusion: what if you store money on your phone as a pre-paid device? Different countries take a different view. The USA is tending towards the view that the question of cross-border currency movements is value-related not device dependent. Separately from that point, it is useful to note that, at the beginning of June 2013, the USA's ICE said that it could demand to examine data on a laptop at borders and did not need to specify e.g. child pornography to be able to do so. But a Court decision said that ICE could not insist that encrypted data be decrypted.

Bitcoins, or to be precise the records relating to them,

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

are encrypted. Further, it is the work of moments to encrypt data files on any device.

The fact that bitcoins are not considered "money" in this sense does not mean that they are not considered money under relevant counter-money laundering laws and regulation.

Trackability of bitcoins

Now another parallel: the USA says that all US dollars in bank accounts are technically held in Manhattan and that all inter-bank (or intra-bank for US banks) transactions anywhere in the world are in fact cleared there. But it makes no such claim for cash. In daily use, cash is a decentralised currency and (subject to certain practical limitations) untraceable in normal circulation. In fact, it's only when a bank note is returned to a bank and its serial number recorded that its whereabouts can be known to the government in what amounts to a spot-check.

This alludes to the fear with Mondex: once the cash was recorded on the card, there was no record of where it went or what it did until someone credited their account with money off the card. Even then, because there was no record of what cash was

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

deposited, it was even worse than cash from a traceability point of view - because cash has a serial number (or at least anything more than de minimis tokens do) and money on a Mondex card does not.

Bitcoins do have a serial number. And, because their movements are electronic rather than hand to hand, they have greater trackability and traceability than cash. Unlike person-to-person transfer outside any form of central recording, Bitcoin transfers take place through a server: in this way it is very similar to inter-account transfers at a bank.

Similarities between e-currencies and internet banking

From some perspectives, e-currencies are disturbingly similar to the mechanism used by the First Curaçao International Bank which was used in a fraud that has only one surprising feature: that it took carousel fraudsters more than a decade to realise that a VAT fraud is a document fraud and that physical goods are not necessary - indeed, physical goods present a trackable and traceable asset that a strictly document fraud does not present.

The First Curaçao International Bank was not, of itself,

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

a fraudulent institution. It was properly formed and subject to banking regulation (which it has to be said it largely ignored or did badly) in at least two jurisdictions. However, the bank was used by a substantial number (at least 2,000 in the UK) of European criminals who simply moved money between themselves, trading imaginary goods across borders, submitting VAT reclaims for goods that did not exist in respect of transactions that did not take place. Across the EU, national tax offices paid out the reclaims which, over a short time, ran to thousands of millions of euros and pounds. The salient point is that the money in the accounts was generated not by the criminals' trading activities nor by them injecting funds into the accounts but by their tax reclaims. As a fraud it was especially ingenious because it needed no, or insignificant, working capital.

Is Bitcoin covered by existing counter-money laundering laws? In many countries probably not: those are the countries that, despite the clear failure of the approach, insist on trying to codify everything. Therefore things falling outside the codified definitions are not subject to regulation. This has been found to be a problem in relation to, e.g. land banking where the UK considered it to be within the flexible definition of collective investments but other countries which list specific types of conduct found that it fell outside the scope of their lists resulting in a scramble to amend

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

the lists. Therefore in countries where a much more intelligent and flexible approach is taken to definitions, anything which can be or can be used as a medium of exchange is covered by the law and regulation relating to money laundering - even if, for the purposes of currency law and regulation it does not fall within the definition of money.

Using logical progression through law and regulation, I can prove, for example, that for money laundering purposes law and regulation purposes time is money, I can prove that lending someone a house for a family holiday - or using that house - can be money laundering. A jet-ski can be money and therefore is within the scope of the law.

Hong Kong has this enlightened approach.

Therefore, by the application of a ridiculously convoluted process of analysis, the answer to the question is "yes." Bitcoin does fall within the scope of the counter-money laundering regulations as set out by the Hong Kong Monetary Authority.

Nothing stands still for long.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

It is clear that a much more complex position had developed since the spam e-mails of 2009/2010.

In the few weeks since I wrote the note above, things have moved on apace. In fact, things had been moving quietly in the background for a short while before that. It is also clear that there are many more issues that need to be considered than simply money laundering regulation.

It may be that money laundering regulation is the hammer that governments take to crack the Bitcoin (etc.) nut. But that does not mean that money laundering is the only or, arguably, even the most important aspect of e-currencies from a risk management, legal or regulatory standpoint.

I am very surprised at the take-up of Bitcoin. It's geeky. And the vast majority of people don't like geeky, especially when it comes to their money. Over the years, several surveys have found that people are more likely to change their spouse than change their bank. If there is such loyalty to a financial institution, it would be surprising if there was disloyalty to an identifiable currency.

I find it very surprising that it has "escaped" into the wild, so to speak. It's anarchic and so logically those who adopt a safety first approach to financial matters

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

would stay away. That, to a degree, is why it is now of such concern to regulators from a money laundering perspective, in addition to the fact that they don't "have eyes on the money."

Is a psychological shift removing scepticism?

When trying to understand why Bitcoin is gaining acceptance where other schemes have failed, it seems to me that there is at least an argument that there is a culture change taking place. As society moved from cash to cheques to payment cards to internet payments, each with an initial resistance that, over time, has been overcome, the actual currency that underpins financial transactions has become both less identifiable and less important. Just as some credit card terminals can be set to choose whether to bill in the local currency or that in which a card is denominated, at the card-holder's option, so internet payments can be billed in a currency of choice, with the range of choice being set by the vendor but the final decision being made by the purchaser.

This appears to lead to a disassociation between the payment and the underlying account. While accepting that little to do with the way the human mind works is

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

logical, we can at least attempt to apply logical progression to this disassociation. If a card holder does not regard the currency in which his payment is made as a matter of importance *at the time of sale* then it is logical to assume that he has similarly little regard for the currency in which is card is denominated.

If we take a sidestep and consider the use of a pre-paid card, this is a means of storing a finite amount of value in a portable form and, in particular, one which might annoy the card holder if it is lost but will not, provided he has not loaded it with a substantial value, greatly disadvantage him. In practical terms, it is no different from losing his wallet containing the money he has taken out of an ATM for a dinner date.

Once the money is on that card, it does not matter if it is denominated in any recognisable currency or, for example, coffee beans. If he is going to a restaurant that is part of a network that accepts coffee beans, then he is happy using the card.

If we extend the analogy and replace the card with a near-field communications device then, provided the merchant accepts the coffee beans as a currency, payment can be made in a way that is functionally transparent to the paying party. Although NFC payments are theoretically possible for Bitcoin, at present there are no practical implementations, in part

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

because retailers do not have the necessary technology. But NFC receivers are cheap and if e.g. a major fast food chain adopted the scheme globally, then there is no doubt that the idea would take off. Why? If you have a smart-phone, you probably already have the necessary NFC technology in your pocket. Unless you have an iPhone, that is. Then you don't get it.

See http://www.techradar.com/news/phone-and-communications/what-is-nfc-and-why-is-it-in-your-phone-948410 for an explanation. Note, in that article, the discussion of PayPal's idea of a digital wallet "in the cloud." Remember that when you are reading "Where are bitcoins stored?", below.

Also related is the following http://www.techradar.com/news/phone-and-communications/mobile-phones/24-of-people-now-using-mobile-phone-to-pay-in-shops-1045288 published in December 2011, saying that globally 24% of people are using their phones to make payments in person, although adoption is not consistent. The data are open to question, though. Read the comments below it to see why. Ask yourself: do a quarter of the people you know use their phone for payments in person? It's highly unlikely to be so.

Taking one final step if, instead of coffee beans, what is

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

loaded onto the NFC device are Bitcoins, then the barriers to acceptability are all-but abolished.

Now if we turn back to considering internet payments, once more, with the growth of payments from funded accounts (such as PayPal, etc.) the user simply transfers an amount from his personal balance to the account of a third party. What is important to him is the amount his supplier requires and the balance in his account both before and after the transfer, especially if his account is denominated in one currency and his payment is made in another. The actual currency of denomination is largely irrelevant. He may, for example, have an account with a PayPal-style provider in the USA but hold a bank account in Australian dollars: if he funds his USA account with his debit card, then he has, for all practical purposes, bought US dollars with Aussie dollars using a payment method he is familiar with and he will make payments using an on-line account the features of which are fundamentally the same as other on-line payment systems. Functionally, this is identical to the purchase and use of e.g. Bitcoins.

In some ways, services such as PayPal, etc. are no different to Bitcoin: a balance is paid into an account for later use. (There are legal differences - for example Bitcoin is a sale of assets while PayPal is a deposit of money). Therefore a user who is used to making

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

payments by PayPal type systems will not find it strange to be using using money that he has parted with but still has control over.

The result of this, it seems to me, is that Bitcoin and similar systems can capitalise on developments in currency and in payment mechanisms and benefit from the fact that other mechanisms have provided an environment where novel payment methods do not now seem so out of the ordinary. If the technology (at least insofar as the user sees it) is basically familiar, acceptance will prove much less difficult. In short, the psychological barrier to entry and acceptability will be lowered.

But the confidence in the system may be, at least in part, misplaced. Although its design is reassuringly secure, the mechanisms through which it operates are not. And there are some serious security issues. These are not secret and, again, the wary should be expected to adopt caution over novelty. And, again, to a degree that does not seem to be happening.

Bitcoin is a disruptive technology

In the current jargon of the tech industry, it is "a disruptive technology" - that means that it has the

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

capability to upset accepted behaviour and norms. Again, people like to play safe with their money. That is especially so during times of economic uncertainty - and yet Bitcoin has thrived during the most uncertain economic times since WWII.

Even though functionally Bitcoin is more or less familiar even to first time users (once they have set it up on their device), for everyone except users, it's a very different prospect for other players in the financial market and its regulators.

In fact, it is the speed of growth that demonstrates the disruption. The business area that is most at risk from a successful Bitcoin project is, obviously, the payments business. The major players that are likely to be under threat in this area are banks and money transfer businesses such as Western Union and MoneyGram.

For example, in recent months, the two ATMs nearest my Kuala Lumpur city centre apartment have been removed. Bank branches, too, have closed. The number of ATMs in convenience stores and in shopping centres has increased dramatically but they close out of shopping hours, leaving a busy residential and entertainment district very under-served at exactly the time visitors, in particular, are likely to want access to cash. But there has been an increase in the number of bureaux de change and agents for the big money

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

transmitters.

This creates the conditions where value stored on a near field device would be very attractive, especially if a user can re-charge the account on that device from his primary account which holds a larger balance, so avoiding a) the delays and costs associated with bank / money transmitter transactions and b) having to carry the wrong currency for no reason other than to be in a position to buy the right one if needed.

It is this that makes Bitcoin attractive and a disruptive technology. For all the talk about freeing people from currency, it is the ability to deliver near-instant payments, even to themselves anywhere in the world and to free them from the ties to banks and other payment providers. If Bitcoin becomes accepted as a means of payment in retail and entertainment premises, then it will provide the sort of convenience that is currently enjoyed only by users of payment cards but without the difficulties associated with lost, stolen or cloned cards and their replacement while away from home.

In short, it has the potential to undermine a significant business area for banks and other large players. It is not going to happen any time soon, but if acceptability and NFC technology continue to grow at current rates, it won't be a distant or theoretical prospect. It will be a

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

genuine alternative to the established order with, in some cases, significantly lower costs implications.

Bitcoins in your pocket: Mondex 20 years on?

While there are some rumours of proposed physical currency for bitcoins, that is fraught with technical, legal and other difficulties that make it unlikely, at least in any meaningful manner.

However, if we join up several aspects considered independently in this paper, we can see that a mobile wallet with NFC is an convenient and effective payment method. The only obstruction (other than widespread acceptance) is that of being able to load the account wherever and whenever it is required.

US company Lamassu has demonstrated a solution to this problem: a Bitcoin ATM - which is, in fact, exactly the opposite of the ATM we are used to. Functionally, it's very, very simple and the device consists of a device to read images on a smartphone (like automated check-in at airports), which identifies the relevant bitcoin account, a bank-note reader into which notes are fed and a screen containing instructions and a "transfer bitcoins" button. The whole

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

process, subject of course to comms line speed and the notoriously unreliable QR code reader technology, takes about three seconds - but the company says 15 seconds, presumably so as not to build expectations that will fall if the device becomes popular and the system busy. There is a demonstration of the device at http://www.youtube.com/watch?v=-zeMLcf66Y8. It has been demonstrated in both the USA and the UK. For more information, see www.lamassubtc.com/

This device creates a special headache for governments. It is clearly designed to be used in a retail environment for example a bar. But while the installation of an ATM in a bar is simply a location of an existing regulated entity, the installation of a bitcoin sales device is not, unless the devices are owned and operated by a locally regulated (or registered) business. But this may not be so: the device is said to be "compatible with leading exchanges" which means that users are buying bitcoins in the market rather than from a local seller.

The concept is not new: many banks offer ATMs which issue notes in a variety of currencies but this is against the background that there is a cardholder with an account held with a regulated institution and that the ATM is operated by or under the umbrella of a regulated or registered business.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Countries will have to find a way to manage devices of this nature: they will proliferate, even if not authorised for use.

On the face of it, this is a money launderer's dream: cash earned on the street can be paid into a machine and credited to an account that can be accessed from anywhere. All the upstream participants need to do is give the street dealer a graphic with the QR code to open on his phone.

But hold the phone - literally. Provided that the owner of the account holder has been properly identified and verified and provided that the monitoring systems are properly defined and set up (which is not rocket science) then in fact random deposits into a collection account are easier to spot than using a courier to carry cash upstream.

Again, the concepts are not worrying, only their execution and that is a matter for law, regulation and enforcement.

Have we seen something like this before? Yes, almost exactly like this: only the devices have changed. What we are looking at is Mondex almost two decades on: a portable wallet that can be charged from an ATM. In fact, the only difference is that the device is a money changer, not a disbursement machine and that's only

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

because there is no bank-like account holding service behind it.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Bitcoin: going mainstream for SMEs abandoned by Google Checkout?

There is another, more pragmatic reason for considering whether Bitcoin might "go mainstream." It's perfect for small businesses and for micropayments.

In November this year (2013), Google will close its Checkout service, orphaning an unknown number of small businesses which chose the service over rivals such as PayPal and credit card merchant accounts due to, respectively, a significantly better business ethic (many PayPal customers have had their accounts arbitrarily frozen and PayPal is, at best, dilatory over dealing with the problem with impenetrable customer service that is widely condemned as singularly unhelpful) and significantly lower charges with no monthly service fee. Google's attitude has been to recommend customers to companies with exactly the charging terms that they were seeking to escape.

Already there are computer programmers who accept payments only in bitcoins. It is unlikely that Bitcoin will reach a sufficient critical mass in time to save the SMEs who are being ditched by Google. However, many will simply abandon taking credit card payments.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

They may be tempted to offer a bitcoin option, which they can do at zero cost until a payment is made and then at very low cost, knowing the option will be used only rarely, but hoping that one day even corporate customers will follow them into its use.

Mt. Gox, based in Japan and the largest Bitcoin exchange (and the one that has drawn the most attention from regulators) has created a system that is functionally similar to Google Checkout. See https://mtgox.com/merchant for details. All it needs is for purchasers to use the system in sufficient numbers to make it viable.

There is a further issue: businesses quoting prices in Bitcoin may need to actively monitor their pricing. Because the price is volatile, a product priced at one bitcoin today is likely to require either a significantly higher or lower number of bitcoins at a future date. In short, currency risk will be a major factor in acceptance for online payments unless there is a mechanism for back-end pricing in, say, USD with an auto-update of prices as displayed to customers.

That feature is provided by the Mt.Gox service - which has no fees for receipt of payments (compared to substantial percentages for credit card payments). The company offers "Bitcoin prices are displayed in real-time relative to merchants' listed price in their local

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

currency " and "Never be forced to handle a single Bitcoin with our Instant Sell function and cash out into sixteen different currencies."

What is not clear from the marketing material is how those funds will be transferred to the user's real-world bank account and at what cost. Whatever the position, it seems as if Mt.Gox will, even if only for a short time, be holding customers' money.

Some participators in Bitcoin may be regarded as deposit taking.

Throughout this paper, those involved in the issue, sale and use of bitcoins are regarded as outside financial sector regulation as deposit taking institutions. But there is, on the face of it, one significant exception to that general principle.

Both MT.Gox and Tradehill hold bitcoins in accounts for account holders. These are not the same as bitcoins held in user's wallets.

For example, see https://support.mtgox.com/entries/21649594-Withdrawals-and-Deposits. That page includes the following: "By depositing funds into your Mt.Gox

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

account you agree to use this service only for the buying and selling of Bitcoins and associated activities." Tradehill has a similar clause.

The purpose of the account is similar to a stockbroker's clients' account - real world currency (I.e. fiat currencies) is accepted only from an account in the depositor's name and will be paid only to that account "in your country of origin." That relates to the identification documents which must include a national identity document although, on the face of the requirements it is possible to produce documents evidencing "origin" in more than one country. The account may be used only for trading. Tradehill says that it holds bitcoins "in cold storage" for users.

Mt.Gox also offers "user accounts" in which Bitcoins may be held and used to make payments to third parties.

If we return to Mt.Gox's merchant services, then it is clear that Mt.Gox holds bitcoins which are used in payment for goods and services sold by the account holder. As noted in "Bitcoin: going mainstream for SMEs abandoned by Google Checkout?" (above) Mt.Gox will receive bitcoins into the merchant's account and immediately convert them to any one of 16 real world currencies. However, it does not say that those funds are immediately transferred to a real world

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

bank account. Indeed, it would be unusual if that were to be so - most on-line payment providers allow the accumulation of balances in part to avoid bank charges on multiple transfers.

It follows that, unlike those who simply sell Bitcoins, including Bitcoin miners, the Mt.Gox (for example) service may be holding real world currency deposits for users for purposes other than their trading accounts.

In these circumstances, providers of such services appear to be liable to regulation as deposit takers with all the regulatory implications that such a designation creates.

Bitcoin Mining

Bitcoin mining is so-called because it involves data mining, of sorts. In summary, Bitcoin Miners install computer software dedicated to solving complex mathematical problems. This process is so computer intensive that miners can now purchase specially designed hardware although it requires, once set up, relatively little human intervention. In return for running the program, bitcoin miners are issued with bitcoins. This increases the supply of bitcoins.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Initially, miners used home or office PCs and the software ran as any other software, using the power of the computer's CPU. But the mining software was so demanding on the processor that computers became sluggish or, even, unusable for any other purpose. Later versions of the software sought out the spare processing capacity available on graphics cards (which, almost by definition, excludes most office PCs where graphics processing is performed on the motherboard. Therefore those who have specified their PCs for games and/or graphic design and as a result have high-performance graphics cards were the main beneficiaries of this design change. Some miners have built their own devices using motherboards that handle multiple (up to four) graphics cards to maximise performance. These generate huge amounts of heat - with two or three machines running, there are reports that the heat generated overwhelmed office air-conditioning. They also use a great deal of electricity.

Development continued with the use of "field programmable gate arrays" - a fancy name for an external processor running through a USB port - so reducing load on the host computer and returning it almost to its normal operating parameters.

More recently, dedicated hardware has been

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

developed. "Application Specific Integrated Circuit" (known as "ASIC") devices are very high speed, single purpose computers, a development that flies in the face of the general thrust of the computer industry's seemingly relentless convergence of devices and functions. The devices can be very expensive - and supply is at best uncertain.

So what is Bitcoin mining?

The technical details are beyond us. So here's the elementary school version. Bitcoins are created in blocks which sit in a "block chain." There are spaces in the chain. Bitcoin miners are looking for those spaces and when they find one, they are able to fill it up with a new block. For that, they are rewarded with credits of bitcoins. The size of the reward depends on the degree of difficulty in finding the space. There are technical limitations on the number of blocks that can be created - no matter how many miners are trying to create blocks, only one block can be created every ten minutes. The result is that there is intense competition amongst existing miners with more miners joining the fray daily, some making very significant investments - there are reports of some "addicts" spending tens of thousands of US dollars on equipment with no guarantee that they will ever be able to create a block and gain the reward.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

In short, while identifying the blocks might be relatively predictable creating them is not. It is said that, today, individual miners using a PC stand almost no chance of a win in the lottery that it has become.

For the technically minded, or curious, there is an excellent article explaining most of the relevant things about mining and its technology at http://www.tomshardware.com/reviews/bitcoin-mining-make-money,3514.html

Bitcoin miners also have a part to play in monitoring and maintaining transaction records, in part as a by-product of their mining activities. In short, in order to find spare blocks, they need to know exactly what blocks are in use. That means knowing the whereabouts of all bitcoins.

There is a complex formula as to how new issues are calculated but there are three things to know: first is that the ratio of new coins to transactions is scheduled to reduce in stages, with a reduction every four years. Secondly, the system is hard-set to prevent the creation of new Bitcoins when the limit reaches 21 million. Third within the first four years of operation, more than half that limit has already been produced and it is expected that three quarters will have been generated by the end of 2016. The planning for the

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

project expected that the 21 million limit would have been reached in 2040.

However, it is not clear how that "hard set" will be enforced. One of the strengths of Bitcoin is also potentially its biggest weakness. It is an open-source, peer-to-peer system. The open source part of that means that "the community" can modify the software at will. In fact, this is happening and the Bitcoin Foundation has, as one of its objects, to co-ordinate development to ensure that there are no "forks" that can compromise the integrity of the system as a whole.

However, there are no technical or legal safeguards in place which can be guaranteed to prevent that happening if someone decides to set off at a tangent. We cannot at this stage say what that tangent may be but it is not impossible that it might be to create coins operating in some way differently from the current system, in parallel to it or, even, expanding the supply more rapidly or to a greater number than planned. "Forking" is one of the core benefits of the open-source movement (indeed, when Windows Update caused some 64 Bit PCs running Windows 7 to reject the official 32 Bit Firefox browser, users were able to turn to a Firefox fork called PaleMoon which is designed specifically for 64 Bit processors and the versions of Windows designed for them.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

This uncertainty is a medium to long-term issue for the credibility and therefore viability of Bitcoin.

Interfacing virtual and real world currencies.

As noted elsewhere in this paper, Bitcoin cannot - until it gains a critical mass - exist in a vacuum. It functions only because it is a parallel currency that can be exchanged for real world (fiat) currencies.

On 29 May, 2013, payment services provider OKPAY (https://www.okpay.com) decided it would heavily restrict its users connectivity to Bitcoin. The company's statement issued on 27 May says "To reduce the risks and potential dangers, and in connection with anti-money laundering legislation, we decided to apply certain restrictions to bitcoin e-currency terms of use. Any financial transactions involving exchangers and stock exchanges trading bitcoin are now prohibited. We rely on receiving payments in bitcoin in favour of verified OKPAY merchants leading a legitimate business which passed appropriate legality and AML checks.
Bitcoin withdrawals from OKPAY account also remain available to all verified users.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Please note that OKPAY Card cannot be purchased or loaded with bitcoin."

In short, while there are very limited circumstances in which the company's verified merchants are able to do business in bitcoin, these are so constrained that there is little opportunity for use.

On 11 June, Mt.Gox tweeted "Dwolla has closed our account as of May 15, 2013.Please use alternative transfer methods such as an International Wire transfer. Pr..." (message truncated by twitter, remainder lost). The company recommended in other tweets various alternatives but users were critical of the cost of using alternatives.

As Mt.Gox came to grips with the fallout from the US government's action against Dwolla (about which see below) the company reviewed its existing accounts and certain accounts were flagged. One related to a Twitter user using the name Alexei Ovtcharov with the username Ikaruska who "flamed" the company and distributed his criticisms to the media. By 12 June he had been told that his account had been flagged for review in the absence of sufficient KYC documentation. The Twitter thread is at https://twitter.com/MtGox/status/344699970689052672 . His criticism began when he read the notice on the

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Mt.Gox website that identification would be required to exchange bitcoins for fiat currency, i.e. real-world currency.

The thread at http://www.reddit.com/r/Bitcoin/comments/1ebzru/dwolla_no_longer_allowed_to_do_business_with_mtgox/ lists one user's understanding of services that were, as at the (unspecified) posting date in the middle of May, useable for buying bitcoins on-line. That user goes on to say "Every single UK bank (yes all 5 of them) are blocking usage with bitcoin right now. I today had an account application declined for running a bitcoin related business. "

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

USA v Dwolla, Governments and banks v Bitcoin Exchanges.

On or about 14 May, 2013, US payment services provider Dwolla (www.dwolla.com) was served with a Court Order obtained by the Department of Homeland Security. That, Dwolla announced, meant that it was required to freeze the accounts of Mutum Sigillum, LLC the US entity which channels back to Bitcoin Exchange Mt.Gox, a company incorporated and operating from Japan. This information, incidentally, is publicly available: the structure is not in any way secret.

The USA frequently uses "in rem" orders which are orders against a thing rather than against a person. Perhaps, to help those outside the USA remember that this tool is quite widely used, the name of an old case might help in future recollection: "in re: Red Corvette."

A thread at reddit.com (a reposting and commenting platform) relating to the order against Dwolla is interesting for displaying levels of ignorance in the general population about financial crime laws and regulations and the background to them. One such comment is "DHS has a Financial Action Task Force on Money Laundering."
http://www.reddit.com/r/Bitcoin/comments/1ebzru/dwol

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

la_no_longer_allowed_to_do_business_with_mtgox/.

One user published what he says was Dwolla's notice to him. It says

"DWOLLA

As of 12:13 PM on 5/14/2013:

You're receiving this notice because our systems have indicated that you've processed and completed a real-time Dwolla-to-Dwolla payment to Mutum Sigillum LLC ("Mt. Gox") within the last 24 hours.

Due to recent court orders received from the Department of Homeland Security and U.S. District Court for the District of Maryland, Dwolla is no longer legally able to service Mutum Sigillum LLC's account.

This is a courtesy email encouraging you to follow up on any uncompleted orders with Mutum Sigillum LLC as Dwolla is now unable to move money to and from Mutum Sigillum LLC's Dwolla account.

Dwolla is not party to this matter nor does it have any information or further insight into the situation. We strongly encourages those with questions to contact Mutum Sigillum LLC

Note: Dwolla requires a court order before honoring requests such as seizing funds or revoking access to an account.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

On behalf of Dwolla, we apologize for this inconvenience."

Note: what was frozen was an account or accounts holding US Dollars, not accounts holding bitcoins. Although at the time of writing we have not found out exactly what authority the DHS claimed for the freezing of the accounts, because the action was taken by DHS and the Immigration and Customs Enforcement divisions of government, it is reasonable to assume that it was action relating to undeclared expatriation of funds.

Dwolla is closely affiliated with a US regulated financial services company.

But it was not only in the USA that MT.Gox found its access to banking blocked. Although the details are sketchy, various internet bulletin boards contain postings that Mt.Gox's UK accounts were "closed" - which is not the same as "frozen."

Can Bitcoins be considered an investment product?

Can Bitcoins be considered, in any sense of the word, an investment? There is (at least in principle) a limited

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

number of bitcoins in circulation. They can be - and are - traded not as a medium of exchange but as a commodity. It is here that the fears of a bubble arise - and the volatility is seen. Because the supply is, in economics terms, scarce (the rest of us would call the supply "limited" or "finite") the value is determined by the market. In addition to providing record keeping services (similar to a current account at a bank) Bitcoin exchanges (about which see below) also provide a platform for the trading of bitcoins: in short a person can buy or sell products or services denominated in bitcoins - or buy or sell bitcoins themselves.

Starting with the premise that bitcoin is a currency: ignore for a moment, any legal or technical definitions of "currency," and look at the reality. Regardless of any formal definitions, Bitcoin works in exactly the same way as any other currency, except it has no physical form. Yet, that, readers may remember, is precisely how the euro was introduced: first as an e-currency held only in banks. Notes and coin were issued three years later.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Box 2: The word's biggest e-currency - the euro.

"When the euro was launched on 1 January 1999, it became the new official currency of 11 Member States, replacing the old national currencies – such as the Deutschmark and the French franc – in two stages. First the euro was introduced as an accounting currency for cash-less payments and accounting purposes, while the old currencies continued to be used for cash payments. Since 1 January 2002 the euro has been circulating in physical form, as banknotes and coins. "

Source:
http://ec.europa.eu/economy_finance/euro/

Like any currency, the value (and therefore the investment potential) of Bitcoin depends on one thing: the confidence people have in it. It is that confidence that defines its purchasing power and that confidence that defines its convertibility: that is to say, the number of bitcoins a seller will accept for his goods or

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

services (purchasing power) and the amount of another currency that a Bitcoin can be sold for (convertibility).

In a regulatory environment "investment" does not mean "good investment." Whether a country regulates a specific type of investment depends on whether

a) it follows the "principles" approach or the codified approach and

b) whether the subject matter is, probably by accident, excluded from definitions. That happens more often than we might like to imagine. See Box 3.

Box 3. A "private" currency is not "foreign" currency.

For example: the USA's Commodity Futures Trading Commission refers to "foreign currency trading." It talks of "foreign exchange." It's the word "foreign" that causes interpretation problems. We looked at dozens of legal reference sources and although they differed in precise wording, they all meant the same - regardless of

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

the area of law to which they referred "foreign" related to another country or jurisdiction. In short, a private currency is not "foreign" currency for the purposes of US regulation. If the wording were "in any currency other than US currency" then private currencies would be included.

It follows then that trading in Bitcoin v the US dollar within the USA is, on the face of it, outside the currency trading regime - and outwith the supervision of the CFTC.

Writing in the Harvard International Law Journal (http://www.harvardilj.org/ - Winter 2010) Julian Mortenson, a lecturer at the University of Michigan, published an article "The meaning of "investment" : ICSID's Travaux and the domain of international investment law. " The paper refers to "international investment law's keystone treaty." The ICSID of the title is the International Centre for Settlement of Investment Disputes" which is a part of the World Bank. So, working on the assumption that the definition it adopts was settled by some of the best government lawyers in the world working in committee and with the inevitable representations from pressure groups and lobbyists, it's as close to a global definition

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

as we are likely to get. Or so one would hope.

Mortenson says "The Convention's *travaux* [we can interpret this, broadly, as "working papers"] demonstrate that the drafters adopted a clear — and extremely broad — meaning of "investment." It is not that all parties agreed on this broad understanding from the start. Rather, the broad definition was part of a compromise reached after long and contentious negotiations over what that definition should be. The other element of the compromise was a series of opt-out provisions by which states could narrow the Convention's capacious baseline definition on an individual basis."

The paper is an interesting treatise on the use of the term "investment" across many international treaties, not the least of which is the Vienna Convention of the Law of Treaties. Basically, everywhere Mortenson looked, he found, as one citation says "the term *investment* is a quintessentially *ambiguous* term ..." Which means, of course that, despite his earlier statement, he did not find a "clear" meaning.

The Centre's website at https://icsid.worldbank.org .

Before the Centre can accept a dispute for arbitration, the parties have to both consent and to make certain statements confirming jurisdiction. The application

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

may include the following clause:

"It is hereby stipulated that the transaction to which this agreement relates is an investment. "

On the face of it, that's clear. But there is a guidance note which says

"While the Convention requires that the dispute arise "directly out of an investment," it deliberately does not define the latter term. The Report of the World Bank Executive Directors on the Convention explains that such definition was not attempted "given the essential requirement of consent by the parties." Parties thus have much, though not unlimited, discretion to determine whether their transaction constitutes an investment. The fact that the parties consent to submit a dispute to the Centre of course implies that they consider it to arise out of an investment. If the parties wish to strengthen the presumption, they may include an explicit statement to this effect in the consent agreement. "

The "explicit statement" is as set out above.

So that ends up being both circular and conclusive: the Convention does *not* define "investment."

Indeed, while treaty itself says "The jurisdiction of the Centre shall extend to any legal dispute arising directly out of an investment, ..." and various parts of the provision

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

from which that is extracted are defined, "investment" is not. Therefore while Mortenson's studies of the working papers leading up to the Convention tells him what the negotiators intended, no definition found its way into the Convention itself.

What the best legal minds available to governments actually concluded this: an investment is an investment if the parties agree that it is.

Mortenson's paper is at http://www.harvardilj.org/articles/257-318.pdf.

Still hoping to find clarity, we turned to the UK''s regulators. The Bank of England and the Financial Services Authority published a joint paper in December 2012 on the policy that would apply after the creation of the Prudential Regulation Authority. It's called "Designation of investment firms for prudential supervision by the PRA: consultation on a draft policy statement."

In that document it refers to companies that "deal in investments as principal.' "Investments" is not defined. But in the Financial Conduct Authority and Prudential Regulation Authority websites, we found a cross-reference to The Financial Services and Markets Act 2000. The definitions section does not include a definition of "investments" but it does refer to

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

"investment services and activities" which it says is defined in Article 4.2.1 of the Markets in Financial Instruments Directive (MiFID) (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0039:EN:HTML)

Investment firm is defined as "any legal person whose regular occupation or business is the provision of one or more investment services to third parties and/or the performance of one or more investment activities on a professional basis; (and, subject to certain conditions, a natural person) . "Investment services and activities" is defined as relating to scheduled activities carried out in relation to scheduled instruments" and "investment advice" is defined as "provision of personal recommendations to a client, either upon its request or at the initiative of the investment firm, in respect of one or more transactions relating to financial instruments."

The list is found at Annex 1, Section C and includes:

(1) Transferable securities;

(2) Money-market instruments;

(3) Units in collective investment undertakings;

(4) Options, futures, swaps, forward rate agreements and any other derivative contracts relating to

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

securities, currencies, interest rates or yields, or other derivatives instruments, financial indices or financial measures which may be settled physically or in cash;

(5) Options, futures, swaps, forward rate agreements and any other derivative contracts relating to commodities that must be settled in cash or may be settled in cash at the option of one of the parties (otherwise than by reason of a default or other termination event);

(6) Options, futures, swaps, and any other derivative contract relating to commodities that can be physically settled provided that they are traded on a regulated market and/or an MTF;

(7) Options, futures, swaps, forwards and any other derivative contracts relating to commodities, that can be physically settled not otherwise mentioned in C.6 and not being for commercial purposes, which have the characteristics of other derivative financial instruments, having regard to whether, inter alia, they are cleared and settled through recognised clearing houses or are subject to regular margin calls;

(8) Derivative instruments for the transfer of credit risk;

(9) Financial contracts for differences.

(10) Options, futures, swaps, forward rate agreements and any other derivative contracts relating to climatic

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

variables, freight rates, emission allowances or inflation rates or other official economic statistics that must be settled in cash or may be settled in cash at the option of one of the parties (otherwise than by reason of a default or other termination event), as well as any other derivative contracts relating to assets, rights, obligations, indices and measures not otherwise mentioned in this Section, which have the characteristics of other derivative financial instruments, having regard to whether, inter alia, they are traded on a regulated market or an MTF, are cleared and settled through recognised clearing houses or are subject to regular margin calls.

Note, especially, subsection (4). The term "currencies" is not limited to "foreign currencies." That overcomes the difficulty posed in the USA.

So, within Europe, there is at least some definition of "investment" and, at least insofar as it relates to derivatives, a clear indication that private currencies are - for that purpose - considered to be included.

Is dealing in Bitcoin futures a regulated activity?

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

It follows from the EU definition of investment that, within the EU, dealing in futures in Bitcoin is, at least on the face of the legislation, a regulated activity.

However, within the USA, because of the word "foreign" and the manner in which the USA defines that to relate to currencies by a foreign country or jurisdiction, dealing in futures in Bitcoin appears to be outside the scope of the CFTC's regulatory regime.

To answer the question as to whether Bitcoins themselves are considered an investment, we were unable to find any compelling argument to say that they are - although speculators clearly regard them as such, in exactly the same way as they do any other currency. Accordingly, the term "investment" for regulatory purposes is different to the use by the public at large.

Therefore, our conclusion is that a dealer in Bitcoins is in the same position as a dealer in any other currency: he is not a dealer in investments, merely a dealer in currencies and, therefore, while required to register with the appropriate authorities under consumer protection and counter-money laws and regulations, he is not by reason of that activity subject to financial sector regulation *qua* bank, investment adviser, etc.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Bitcoin bubbles - fact or fantasy?

A bubble is where there is mass hysteria that results in spectacularly high prices for assets which do not have the necessary underlying value.

A more formal definition of "bubble" is from the FT's Lexicon which says "When the prices of securities or other assets rise so sharply and at such a sustained rate that they exceed valuations justified by fundamentals, making a sudden collapse likely - at which point the bubble "bursts". "

Any currency speculation is therefore open to creating a bubble. The reason for this is simple - no currency is backed by sufficient gold or other asset holdings to cover the money in circulation (although Singapore comes close with its sovereign wealth funds holding assets exceeding GDP - unless there is another global economic collapse). There are persistent rumours across the internet that China is taking steps to hoover up gold on the world's markets with a view to converting the yuan to a gold-backed currency but it is difficult to imagine this to be a realistic objective. The stories seem to have a common theme: a conspiracy theory that China is planning to take such a step because, if it did so, the US Dollar would immediately lose its safe haven status and in one fell swoop, the

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

yuan would become a reserve currency of choice.

Applying the above reasoning, all currencies are in a permanent state of bubbledom because - like Bitcoin - they have no value except that which the parties to a transaction put on them.

The question then is whether Bitcoin is more susceptible to a bubble than a national currency? Based on a sample of one event, it has to be accepted that there is the potential for a Bitcoin bubble. In early 2011, Bitcoins were priced at less than one US dollar - not long before they had been less than ten cents. By the middle of the year, they were being priced at in excess of USD33. The price collapsed to somewhere around USD2.50 in a matter of days. Then just days later it was back up to USD18, approx. In April 2013, the price reached USD155, then climbed to USD260. . As this section was being written in the first week of July 2013, it had fallen back to approx USD69. An up to date price is published at www.coindesk.com.

Can Bitcoins be pumped and dumped?

In June 2011, immediately before the collapse in

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Bitcoin prices from more than USD30 to around USD2.50, The New York Observer carried an article which interviewed one Bruce Wagner, a self-appointed Bitcoin expert who was producing his own cable TV programme called "The Bitcoin Show." He had other Bitcoin related media interests. The article contains the following statement "He doesn't give investment advice, he's careful to say. But he's bullish. "It's a bubble, but it's an unbreakable bubble, one that is just going to keep growing and growing and growing," he said. He had predicted Bitcoins would be going for USD10 each by the end of May; the price hit USD9.999 on June 1. He now says it will hit USD100 by the end of the month and USD10,000 within one year."

It didn't, it collapsed. The bubble was not "unbreakable."

While there is no suggestion intended or implied that Wagner was talking up an asset in which he had a position with a view to selling while others were still buying to support the price, the potential for harm is obvious.

The "hype" - which is of course the essence of a pump phase of a pump and dump scheme - is palpable. See this corporate promo by WeUseCoins.Com : http://www.youtube.com/watch?v=Um63OQz3bjo&feature=youtu.be

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Non-bank issuers of electronic money.

From a money laundering, market conduct and prudential perspective, banks are regulated for all relevant activities including the issue of e-money. Therefore, the group we are concerned with in this paper are the non-bank issuers of electronic money.

The UK's Financial Conduct Authority says "Electronic money (e-money) is money 'stored' electronically to spend later. This includes pre-paid cards, such as travel money cards and some gift cards, and online accounts used instead of credit or debit cards. Find out whether you should search this area of the Financial Services Register for an e-money issuer and what to look for. "

Therefore, having established that e-currencies are "money," it follows that they fall within this definition. The definition is based in EU law and therefore applies across the EU. Examples of Electronic Money Institutions (EMIs), and the regulated activities, can be found at http://www.fsa.gov.uk/register/2EMD/2EMD_MasterRegister.html .

Examples of regulated activities that EMIs are

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

authorised for are:

a) Services enabling cash placement on a payment account
b) Services enabling cash withdrawals from a payment account
c) Execution of payment transactions (not covered by a credit line)
d) Execution of payment transactions (covered by a credit line)
e) Issuing payment instruments or acquiring payment transactions
f) Money remittance
g) Execution of payment transactions via telecoms IT system or network operator
h) Issuing electronic money

It is clear then that those operating Bitcoin servers in the UK are covered by these activities: the Financial Conduct Authority lists, in the master register countries for which "passport" approval applies, showing the common approach across the EU.

However, in December 2012, the European Banking Authority published two reports that made it clear that there were clear inconsistencies across the EU.

1. Report on the AML/CTF obligations to, and the AML/CTF supervision of e-money issuers, agents and

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

distributors in Europe.

http://www.eba.europa.eu/documents/10180/16148/JC-2012-086--E-Money-Report----December-2012.pdf

The report says "

The 3rd Money Laundering Directive applies to e-money issuers as it does to other credit and financial institutions, alongside certain non-financial persons.

The EU's e-money regime provides for two exemptions that are relevant in the AML/CTF context:

- The first exemption covers pre-paid instruments that may be used to purchase goods and services within a limited network of service providers or for a limited range of goods or services.

- The second, optional, exemption covers situations where an e-money product's features meet the conditions for simplified due diligence.

Note, the first exemption would apply to the case of Square and its pre-paid cards (see elsewhere in this paper) .

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Bitcoin wallets do not qualify under the simplified due diligence exemption which requires, the Report says "either:

- Non-reloadable and whose total purse limit does not exceed €250 (or €500 for domestic transactions); or

- Reloadable, cannot transact more than €2500 in a calendar year and be used to redeem more than €1000 in that same calendar year.

No such restrictions apply to bitcoin wallets. Again, then, it appears that Bitcoin wallets fall within an aspect of a regulatory regime.

There is an additional complication. Especially important is the obligation as follows:

Regulation (EC) 1781/2006 defines 'complete information on the payer' as comprising the payer's name, address and account number or their name, account number and either their date and place of birth, customer identification number or national identity number. This requirement applies where the destination payment service provider is located in a jurisdiction outside the European Union. "

"The term "payer" means "paying party" or "the

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

person making payment." The use of the term "payer" coupled with the use of the term "issuance" in various documents strongly implies US involvement in the drafting: these are not usual terms found in documents drafted by English law draftsmen. This is relevant because it implies an aim to adopt as close to standardised terms as possible across the global financial spectrum. But this is not the complication.

The complication relates to the "destination payment service provider." Who are "service providers" in any bitcoin transaction? The transactions are conducted between the paying party and the receiving party. Unlike a bank which has its own servers and therefore both because of its corporate structures and (more controversially) the location of its servers, a location can be identified. However, Bitcoin operates on a peer-to-peer basis (see below) and, although there are command and control servers, they do not take active part in the transfer of funds. There is no central controlling authority and once bitcoins have been issued, they are like cash, and not attached to any specific issuer. Indeed, when a P2P "client (that is the user's device) connects, there is no predetermined point of connection.

Countries are - rightly - saying that bitcoin falls within counter-money laundering law and regulation. There is, in my view, no argument that issuers (and through

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

them their agents and distributors) must undertake due diligence as part of full set of compliance and risk management measures. But as the technology stands, this can only happen at the point where bitcoins are exchanged for another currency, a subject covered elsewhere in this paper.

However, there is no e-currency equivalent of SWIFT's data collection (which, in the case of Bitcoin, is actually quite technically simple to do because coins are identifiable and trackable so, provided all users are properly registered, then the data could be collected and retained with simple database operations). The above provision is an attempt to ensure that record keeping provides similar data to that collected by Swift - and any other money transmitter. In short, it is placing all players in the funds transfer market on a similar footing.

Box 4: European Banking Authority: defining e-money issuer, agent, distributor

The difficulty that faces compliance and risk management officers in banks is set out in the

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

report as follows:

E-money issuers distribute their products in different ways, for example by establishing a direct business relationship with the customer, or through distance selling means (such as the internet). E-money can also be distributed and redeemed by persons other than the issuer. In addition, agents can provide payment services on an e-money institution's behalf. But although agents and distributors play a central role in many e-money business models, the concepts of 'agents' and 'distributors' and the role they play in the e-money distribution chain are not clearly defined.

As a result, Member States (MS)' recognition and, where applicable, use of both terms varies significantly.

E-money issuers

The large majority of MS define e-money issuers as legal entities or persons authorised or licensed to issue e-money under relevant legislation, in accordance with the 2nd EMD. One MS does not define e-money issuers, only e-money

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

institutions, which are financial institutions authorised to issue and redeem e-money and to settle transactions involving e-money.

Agents

Most MS broadly define agents as natural or legal persons who can provide payment services and act on behalf of an e-money issuer but cannot issue e-money. One MS's regulation states that a payment institution can commission another legal person to execute parts of the activity, but does not specify which ones. Three MS specified that agents cannot distribute and/or redeem e-money unless they are also a distributor. In two MS, the legislation does not define agents.

Distributors

Fifteen MS do not define distributors; of these, two consider agents and distributors to be the same and therefore do not provide a definition of distributor. A further three provide that distribution and redemption of e-money may be done by – unnamed - natural or legal persons acting on the Electronic Money

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Institution's (EMI) behalf.

Eleven MS define distributors as natural or legal persons who can distribute and/or redeem e-money on behalf of an EMI, but who cannot provide payment services. One MS defines distributors as persons authorised to distribute and/or redeem e-money acting on behalf of an EMI

Incidentally, slightly off topic - the report says in a footnote "Another exemption, in Art 1(5) 2nd e-money directive, concerns the use of telecommunication, digital or IT devices to pay for some goods or services that are delivered to and are to be used through a telecommunication, digital or IT device. This exemption is of limited relevance in the AML/CTF context." This is regrettably a grave under-statement of the risks of money laundering in the pre-paid telephone call market, a subject I worked on extensively in the 1990s and can personally attest to money laundering schemes in that market.

E-money directive:

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0110:EN:NOT

- The EU e-money directive says "It is appropriate to introduce a clear definition of electronic money in order to make it technically neutral. That definition should cover all situations where the payment service provider issues a pre-paid stored value in exchange for funds, which can be used for payment purposes because it is accepted by third persons as a payment.

- The definition of electronic money should cover electronic money whether it is held on a payment device in the electronic money holder's possession or stored remotely at a server and managed by the electronic money holder through a specific account for electronic money. That definition should be wide enough to avoid hampering technological innovation and to cover not only all the electronic money products available today in the market but also those products which could be developed in the future.

2. European Banking Authority: Joint Committee published a report on the implementation of anti-money laundering and counter-terrorist financing requirements for e-money in the EU.

http://www.eba.europa.eu/-/joint-committee-publishes-

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

report-on-the-implementation-of-anti-money-laundering-and-counter-terrorist-financing-requirements-for-e-money-in-the-eu

Are Bitcoin miners (and their equivalents in the similar systems which are inevitable) "issuers" of electronic currency?

It seems to be very difficult to argue that they are not, given that they increase the supply and sell bitcoins.

Could there be a "run" on Bitcoin?

A run on a bank happens when account holders turn up and demand that they withdraw from their accounts moneys that, in aggregate, exceed the bank's cash-on-hand. The account holders, both in relation to current and savings accounts, are depositors and deposits are repayable on demand or on a fixed date, although in the latter case it is usual for on-demand withdrawals upon payment of a penalty, usually in for form of a back-dated reduction in interest paid.

It follows, then, that in relation to a run, we are talking about a deposit-taking institution.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Bitcoin is not a deposit taking institution. Bitcoins are sold to the account holder who is himself responsible for their security because they are stored in his wallet or a web wallet. There is no central storage as there would be with a bank, only an electronic record of what coins are held by whom. That record is distributed across the internet through the peer-to-peer network.

A holder of bitcoins may go back to the person he bought them from and make a deal to sell them back but that is a discrete transaction which, like all contracts, requires consent. There is no buy-back provision and, it follows, no right to a refund. Even if there were, this would not be a withdrawal.

Therefore there cannot be a run on Bitcoin.

However, this is not to say that there cannot be a crisis of confidence which undermines, perhaps destroys the system.

A further consequence of the fact that there is no right of redemption or withdrawal of bitcoins is that a holder of bitcoins is stuck with them unless he can find a counter-party willing to accept them in return for goods, services or a real-world currency.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

What is a Bitcoin exchange?

A Bitcoin exchange is, simply, a market place for willing buyers and willing sellers of Bitcoins to trade.

The biggest is Mt.Gox. A company called "Tradehill" launched in early 2011 with offices in Chile (according to the New York Observer). Tradehill says "Tradehill initially launched in June 2011 and functioned as the second largest Bitcoin exchange in the world until temporarily shutting down in January 2012. .. The business recently underwent a major re-organization, received USD400,000 in seed-funding, hired a new team of top legal and engineering talent, and re-launched in March 2013, with a new focus on the accredited investor and institutions market. " It now quotes an address of 1 Market Street, San Francisco. The entry level account with Tradehill requires users to exchange at least USD10,000 in order to create a "prime" account.

MT.Gox has no minimum requirement.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Bank secrecy / confidentiality

Despite the assault on bank secrecy and customer confidentiality, it does still have its strongholds, albeit with special powers to go behind the veil where a court or other authorised person is satisfied on the evidence before it that there is a reasonable suspicion of money laundering or terrorist financing.

But to avail themselves of such secrecy or confidentiality, customers must be dealing with a regulated bank.

As shown above, Bitcoin is emphatically not a financial institution, therefore it is not a bank and therefore the secrecy and confidentiality provisions do not apply.

Further, there is no professional privilege applicable to any data held by the server operator.

Data Security

It is self-evident that data security is of paramount importance in relation to the control of both "current" and "trading" accounts.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

There have been several serious security breaches at Bitcoin miners: for example, Mt.Gox (about which more later) was reportedly hacked in June 2011. It was reported that a hacker had obtained credentials from a professional adviser to Mt.Gox and transferred about half-a-million Bitcoins to himself, then dumped them through Mt.Gox's own trading platform. In essence, he put out an order saying that he would sell the coins he had stolen at any price. The price of Bitcoins on the Mt.Gox exchange dropped sharply and for a few minutes, it fell to USD0.01 from a previous price of USD17.50, approx). The price re-adjusted very quickly but substantial losses had been incurred. What was most interesting about the theft was that it was not a theft from a single account - but used the almost mythical method of taking tiny amounts from many accounts - salami slicing, in the argot of the industry. Several people had complained that their balances were incorrect and alleged that their accounts had been accessed without authority. But it was on 13 June 2011 in the late afternoon that one Bitcoin was taken from each of 25,000 accounts. The stories began to become even more bizarre with Mt.Gox issuing a statement saying the the dumper had tried to buy back the coins he had stolen once the price had dropped - clearly indicating what might be the first ever market manipulation in a private, electronic currency.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Mt.Gox initially argued that they were not responsible for the losses because the access was made by a person using the correct login credentials and accessed on the first attempt. But they soon backed down from that position. Moreover, the following Sunday, 19 June, Mt.Gox closed while "*we rollback all trades that have happened after the huge Bitcoin sale that happened on June 20th near 3:00am (JST).*

"*Service should be back by June 20th 11:00am (JST, 02:00am GMT) with all the trades reversed and accounts available.*

"*One account with a lot of coins was compromised and whoever stole it (using a HK based IP to login) first sold all the coins in there, to buy those again just after, and then tried to withdraw the coins. The $1000/day withdraw limit was active for this account and the hacker could only get out with $1000 worth of coins.*

"*Apart from this no account was compromised, and nothing was lost. Due to the large impact this had on the Bitcoin market, we will rollback every trade which happened since the big sale, and ensure this account is secure before opening access again.* "

What actually happened, according to the most common version of events, was that MT.Gox's database was compromised and stolen - in fact, within

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

a few days of the theft, it was available on-line (the link we found to the data is now blocked). But the account into which the Bitcoins were transferred was identified, frozen (it is a private system after all so no court order is required) and eventually re-credited to the various accounts. It was said that only accounts with a USD equivalent value of more than 8,750 were affected, presumably because only one missing coin would be less likely to be noticed from larger balances.

Having said all of that, there is another version of events: there is a claim that the security breach related not to MT.Gox's servers at all but to a file called wallet.dat owned by a user "allinvain" and that the addresses of the 25,000 bitcoins related to accounts (not 25,000 accounts) referred to in that file. There was also a suggestion that "hacktivist" group LulzSec released the Bitcoin database - this would seem to be a bizarre thing for that group to do as it strikes at the heart of exactly the kind of anti-establishment concept that the group seems to support. But that version does not say how the allinvain file was obtained or by who.

MT.Gox's actions demonstrate the fallacy of one of the myths of Bitcoin - that of being anonymous and therefore suitable for use in criminal activities. In fact, the records show the full history of each bitcoin, which account it was held in and where it came from and went to. There is just one snag with that: there is no

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

obligation on a Bitcoin exchange to identify and verify from independent sources those who use its accounts nor the provenance of the funds.

So, while the bitcoins themselves are fully traceable, the people using them are not, unless they have paid for them with credit cards. But in a private exchange situation, that is unlikely.

The biggest problem facing any parallel currency is that, unless it is received in return for labour at a fixed rate, it will have to interface with real currency and that means there must be an exchange rate. Either that exchange rate has to be fixed by a central authority (and one of Bitcoin's selling points is that it is peer-to-peer and no one is in control) or left to market forces.

We have no data on what happens in very low volume trading of a new currency in the open market but we do know what happens in relation to very thinly traded shares on, for example, the USA's over the counter market. They either sit at a very low value or they are very, very volatile with relatively small transactions having a disproportionate effect on value.

There have been fears of a Bitcoin bubble and a Bubble bursting - and the volatility might indicate that - prices v USD have, over the past three years, ranged

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

from USD2 to USD165 and all points between with massive swings within hours. But the general trajectory has been steadily upwards.

Like almost all currencies, bitcoins have no intrinsic value, only that which people agree to assign to them. But unless there is a sufficient critical mass of businesses and workers willing to conduct their activities outside the regime defined by national currencies, then it is always going to be subject to constant pressures - and the risk of massive inflation. That translates into the bald statement that Bitcoin has value only if people have confidence in it; lack of confidence turns into inflation and, ultimately, a financial crisis. How much that crisis is contained within the Bitcoin network is the big question for regulators.

That and how to tax it for while the G7 etc. is getting its knickers in a twist over the question of expatriation of profits made by international companies, on the face of it, Bitcoin sidesteps the payment mechanisms.

Actually it doesn't: that’s another point to return to.

The exchange rate v USD is not the primary concern if Bitcoin is going to become a major player as a currency.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

After my advice that Bitcoin is covered by the HKMA's Money Laundering Regulations, it became apparent that various US authorities were looking for ways to declare Bitcoin within their regulatory regime.

It has recently come to light that California decided, on 30 May, 2013, that Bitcoin is a money transmission system. It wrote to the Bitcoin Foundation which has a drop-box in Seattle, Washington and declared that "Bitcoin Foundation may be engaged in the business of money transmission without having obtained the license (sic) or proper authorisation required by the California Financial Code."

A copy of that "cease and desist" letter is at http://www.scribd.com/doc/149335233.

The letter refers to Federal law under s.5330 of the Title 31 of the US Code and defines "money transmitter" as "a business which provides cheque cashing, currency exchange or money tramsmitting or remittance services or issues or redeems money orders, travellers' cheques and other similar instruments or any other person who engages as a business in the transmission of funds including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

conventional financial institutions system" and says that any such person "must register with the US Treasury Department. "

Reference is made to other US Code provisions.

As noted above, I have no difficulty in establishing that Bitcoin is "money" within the broad definitions applicable to money laundering regulations. The US provisions relate to counter-money laundering provisions and therefore I am satisfied that Bitcoins fall within the definition of money for those purposes.

Where I do have more difficulty is in finding who to regulate.

Is "The Bitcoin Foundation" the appropriate target? The answer to that question is , on current law and regulation, a very clear "no" and California should have been aware of that before issuing its letter.

The reason for that is simple: while The Bitcoin Foundation is the public face of Bitcoin it does not, itself, control, own or operate a Bitcoin exchange in California or elsewhere. It is therefore, by definition, not a "money transmitter." Nor, we should add for the sake of completion although California did not make reference to it, is The Bitcoin Foundation itself an issuer of electronic currency.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

However, that doesn't mean that US (in particular) authorities won't stretch the law to make it fit.

The Bitcoin Foundation instructed lawyers to reply to California's letter and, on 1 July 2013, they did so. The letter is at http://www.scribd.com/doc/151346841/Bitcoin-Foundation-Response-to-California-DFI . However, there are a number of matters in that letter which are inconsistent with my interpretation as noted above, not the least of which is the assertion that Bitcoin does not fall within the definition of "money."

However, the lawyers do make an fascinating point: California's own Department of Financial Institutions, which issued the letter, wrote an "opinion letter" on 6 December 2011. That letter was at http://www.dfi.ca.gov/Laws/orders_files/Opinion-Foreign_Currency_Exchange_Services.pdf. Yet, on 1 July 2013, the Department of Corporations and the Department of Financial Institutions became the stupidly named (anything that equates "oversight" with "supervision" is stupid) "The California Department of Business Oversight" and the page is now missing.

The lawyers argue "In that opinion, the DFI determined that the receipt of dollars and the delivery of pesos for

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

a fee did not constitute money transmission. The company did not hold customer funds for future transmission and was not financially liable to the consumer. Under these facts, the DFI determined that the company was not subject to the Money Transmitter Act. The sale of a bitcoin functions the same way: legal tender is received and bitcoin is delivered. Further, the customer's legal tender is not held for future transmission, it is merely tendered to the seller, and upon delivery of bitcoin, the seller is not financially liable to the purchaser. The same rationale that applied to the sale of a pesos should prevail under the California statute with regard to the sale of a bitcoin."

That argument, on its very narrow point, appears to hold water - not because it says that Bitcoin is not a currency (a position with which I strongly disagree) but because it says that California accepts that currency exchange is not a money transmission business. That, in relation to that simple one-to-one, instant transaction, is true.

Even so, excuse me while I have a belly laugh: the only major success that FinCEN repeatedly points to is the Black Market Peso Exchange a significant part of which related to currency exchanges along the Mexico/US border. Cambios (the Spanish for Bureaux de Change) are, under Federal law, regulated as money services businesses. They are not money transmitters per se

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

(although they may, and often do, provide that service, too). If California is really declaring that currency exchange is outside the money laundering regulatory regime, that's a significant undermining of the US federal strategy. The fact is that, even if California takes it out of its state provision, currency exchange remains subject to Federal law. It's not difficult to make that determination: it's listed at http://www.fincen.gov/financial_institutions/msb/amimsb.html.

California is an important state for tech-based money transmitters and other payment service providers (see Regulating Silicon (Valley) Money). It is also a Mexican border state.

FinCEN was clear: it would treat bitcoins as money and therefore those who were involved with it would be treated in the same way as those involved with money.

But it was not the first time FinCEN had considered e-currencies. In July 2011, FinCEN redefined "money transmission services" as "the acceptance of any currency, funds or other value that substitutes for currency from one person and the transmission of currency, funds or other value to another location or person by any means." What is most surprising is that it took ten years after the USA finally woke up to money transmission services in the wake of the events

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

of 11 September 2001 for this sensible definition to be imagined and adopted. It's not rocket science: it's common sense.

It was in March 2013 that FinCEN first made plain that it was looking at Bitcoin per se. On 18th March it issued Guidance (http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html) "to clarify the applicability of the regulations implementing the Bank Secrecy Act ("BSA") to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies."

So users, per se, are not regulated.

"However, an administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. An administrator or exchanger is not a provider or seller of prepaid access, or a dealer in foreign exchange, under FinCEN's regulations," says FinCEN.

That, it seems to me, is exactly the correct view. And demonstrates a sensible attitude of applying existing flexibility within laws to new situations instead of codifying detail and creating a rigid framework which criminals can readily circumvent.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Regulating Silicon (Valley) Money

California is struggling to come to terms with three conflicting goals: first, it is the USA's most consumer orientated state in terms of legislation and it regularly produces laws that constrain the IT industry for reasons of consumer and data protection. Secondly, music, film and IT have turned California into the USA's biggest domestic economy - bigger, in fact, than many entire countries outside the USA. Third, the IT sector is, by definition, always developing ahead of law and regulation (or, at least, law and regulation which is defined in codified terms which is what the USA in general and California in particular usually do).

In early March 2013, the Department of Financial Institutions (which would along with the Department of Corporations on 1 July, be subsumed into a new Department of Business Oversight) held a hearing to decide what to do about The Money Transmission Act. The 2010 Act was far removed from the law as it had previously been but it had unexpected (not unintended) consequences. The biggest of them was that the nascent interest in providing e-payment systems was about to explode - and California, with its highly developed tech and tech-funding sectors would

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

be at the heart of what would grow not only in size but also in several different directions.

From PayPal and its near-clones, suddenly there were a raft of alternatives.

While the USA is a country, it is also a federation of surprisingly independent states. Indeed, Texas is often seen as considering itself as a country within a federation, rather than a state in a larger country.

States are responsible for laws that apply to conduct that occurs entirely within their own borders; cross-border (inter-state or international) activity falls under federal jurisdiction. It is for this reason that, for many years, several US states did not have state counter-money laundering laws and it is also the reason that the FBI and Department of Justice tag "wire fraud" charges onto their cases - it creates the jurisdiction that an otherwise single-state act would not give them.

But California's interpretation of its own laws is at best open to question.

As noted elsewhere in this paper, California has decided that currency exchange does not fall within its definition of money transmitter. On the face of it, that's fine. Further, Teveia Barnes, in March the head of the California Department of Financial Institutions,

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

admitted in her statement to the state legislature on the current law that the DFI takes the "eyes on the money" approach which FinCEN espoused when decided to abort its plans to require "hedge funds" to comply with counter-money laundering regulations. Basically, if the money is in a bank, then the DFI doesn't consider the business collecting and paying it out as a money transmitter.

That, it has to be said, is a deeply naïve and flawed view, even if all funds are paid in and paid out electronically and therefore the bank has at least some records. The reason is simple: risk assessment information (if there is any) is held by the money transmitter but the money laundering risk is held by the bank: the arrangement is an archetypal pass-through or payable through account, even though the bank has the information as to the paying party and the beneficiary with some information as to the purpose of the transfer.

There is a fundamental issue with states being responsible for authorising payment systems that operate their own businesses across borders. Of course, a simple one-shop money transmitter has one place of business and his customers come into his shop to hand over the money that he sends as instructed.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

But e-payments and e-currencies do not operate according to that model. PayPal, for example, found that it has had to obtain state licences and not all states wanted to issue them or if they did wanted to impose a variety of conditions. The result is that new payments businesses - even if they want to operate only in the USA, face considerable barriers to entry. A far more sensible solution is for multi-state businesses, or international businesses, to be licensed and regulated nationally. This is the model that is available to banks: they can choose state or federal regulation.

Part of the problem is that payment companies in fact operate bank-like services, they accept payments in and make payments out to order. As a result, they are required to provide bank-like security for the amounts they hold. That, one might think, would be a simple matter to regulate: it could be required that all moneys held on behalf of clients and all clients' in/out transactions must take place in a single hypothecated account - a trust or clients' account for want of a better expression. The law could, simply, require such a business to hold one and only one account in one bank for client purposes and that the only funds that the business is allowed to debit against that account - and transfer to its own operating accounts - are its own agreed fees. The account must be sacrosanct and no payment of operating expenses including salaries must be allowed. Translating that to payment

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

processors, they are, by definition, not lenders. They offer a service that is tantamount to a current account that must be kept, at all times, in credit. Therefore the risks are business failure (mitigated by the requirement for a trust account) and fraud not bad investment decisions which is what have left so many traditional banks reeling.

Of the payment systems that have cropped up recently, the two with the biggest buzz are Square and Stripe. One wonders if regulatory issues are behind Google's decision to abandon its (very popular with Small and Medium Sized Enterprises or SMEs) Checkout system as from the end of October this year, dumping customers onto a highly fragmented market filled with exactly the kind of companies that Google's users were trying to escape from.

Square applied for and was awarded a California licence, in part so that it could offer pre-paid debit cards (the USA calls them "gift cards"). But at the end of June, it announced that its "gift card" service would be scrapped. But in truth, it wasn't a properly formulated plan: the cards were, in effect, vouchers for use at a small number of participating outlets, far away from the Visa/Mastercard versions with their ATM and millions of outlets profile. Square's core business is to supply a device that plugs into a phone and allows on-line payments between participating customers and

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

merchants. There is also Square Wallet" which turns a mobile phone into a portable payment terminal: at first sight, conceptually weird, it actually makes some sense. The phone automatically logs into a shop's internal system when you walk in. When you want to pay, you tell the cashier your name, he finds it on the list of logged-in phones and checks an on-line photo against the person standing in front of him. Satisfied, he clicks and the system debits the credit card registered to your wallet account. Some will love it, others will find it disturbing.

There was another problem - and once more it was California that caused it: one of the aspects of "gift card" use that exercises the minds of US federal regulators is that of "breakage" - this is where a card is bought with a face value of x but only a certain percentage of x is spent. The companies therefore are left with orphaned money which they cannot send anywhere and which either sits as a balance, is lost to the consumer after an expiry date specified on the card (similar to a pre-paid telephone card) or eroded away by charges. So California decided that participating merchants must be required to pay any balance on a card of less than USD10 in cash. The difficulty is that merchants have to program their POS systems to provide an item that does not involve a sale of product - and it seems this is beyond the wit of their providers.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Square is available only in the USA, Canada and Japan. Another near-start up is Stripe - which is available only in the USA and Canada but is presently being tested in the UK. The interesting development at Stripe is that it was, previously, a one-way payment system but recently it added a service of allowing payments to third party bank accounts, putting it in direct competition with e.g. PayPal.

California's Money Transmission Act defines a money transmitter as "a person who receives money for transmission." That, opponents say, is so wide that it takes in businesses that are not in the money transmission business per se. It includes, it seems, booking agents who market e.g. concert tickets, collect payment and pay it to the promoter, etc.

Whatever the niceties of the wording, it seems clear that anyone who, as a business, receives money in California and sends it to any third party anywhere in the world, is subject to California law. That would include, for example, the payment services offered by Bitcoin exchanges.

e-money issuers: capital adequacy issues

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

The EU e-money directive says"

-There is a need for a regime for initial capital combined with one for ongoing capital to ensure an appropriate level of consumer protection and the sound and prudent operation of electronic money institutions. Given the specificity of electronic money, an additional method for calculating ongoing capital should be provided for. Full supervisory discretion to ensure that the same risks are treated in the same way for all payment service providers and that the method of calculation encompasses the specific business situation of a given electronic money institution should be preserved. "

- The issuing of electronic money does not constitute a deposit-taking activity pursuant to Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions , in view of its specific character as an electronic surrogate for coins and banknotes, which is to be used for making payments, usually of limited amount and not as means of saving. Electronic money institutions should not be allowed to grant credit from the funds received or held for the purpose of issuing electronic money. Electronic money issuers should not, moreover, be allowed to grant interest or any other benefit unless those benefits are not related to the length of time during

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

which the electronic money holder holds electronic money. The conditions for granting and maintaining authorisation as electronic money institutions should include prudential requirements that are proportionate to the operational and financial risks faced by such bodies in the course of their business related to the issuance of electronic money, independently of any other commercial activities carried out by the electronic money institution.

- The rules governing branches of electronic money institutions which have their head office outside the Community should be analogous in all Member States. It is important to provide that such rules not be more favourable than those for branches of electronic money institutions which have their head office in another Member State."

Having regard to that, it is instructive to note the EU's definition of "electronic money."

Article 2.2: "electronic money" means 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 as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issue

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

The fact that the EU is not a single currency zone means that the EU needed to prepare wording that would allow flexibility across the eurozone. Moreover, for much of the time during which the EU was negotiating the Directive, and since, there have been questions over the future of the Eurozone and whether some countries might be barred entry, thrown out or voluntarily leave.

Unfortunately, the Directive does not define "monetary value." This is a surprise because the EU has already struggled with terminology for value transfer systems such as hawala or the chop.

However, Article 10 gives an indication of the direction of thought. It says "Member States shall ensure that, upon request by the electronic money holder, electronic money issuers redeem, at any moment and at par value, the monetary value of the electronic money held. " This clearly implies that a person holding value on e.g. a card may - subject to the payment of permitted fees - receive their full value on demand. That is only possible with a national currency, including, for ease of definition, the Euro because to do it with a physical alternate currency would raise the spectre of the Liberty Dollar case, below.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Who owns Bitcoin?

What might be regarded as the official Bitcoin website declares that it is not actually an "official" site. See www.Bitcoin.org

It also makes it plain that no one "owns" Bitcoin, except as to its brand.

It's called what?

There are many variants of the name so we've stuck with the one chosen by its creators and used in their website: Bitcoin. Not BitCoin, not bitcoin (except in a web address) and not BTC.

But when used as a unit, there is no capital (i.e. I have three bitcoins in my account).

So it's correct to talk about "Bitcoin" and "a bitcoin."

Where are bitcoins stored?

This is by far the most difficult to understand thing about Bitcoin - and from a personal user's point of view, the thing that makes one ask questions.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

First, a bit about the tech. Peer-to-Peer (P2P) systems have been around a long time. The first hugely successful P2P system was developed by the people who had invented file sharing service Kazaa, although they did not design the underlying protocols. When the music industry decided to combat music file sharing, Kazaa the developers realised that they could use much of the Kazaa platform for internet communications. That led to the birth of Skype which now mixes P2P and server-based communications.

But P2P systems are very common. One would have had to have been living under a rock not to have heard of BitTorrent, PirateBay and other services but there are hundreds more. The USA's FBI warns of the dangers of P2P use: "Peer-to-Peer networks allow users connected to the Internet to link their computers with other computers around the world. These networks are established for the purpose of sharing files. Typically, users of Peer-to-Peer networks install free software on their computers which allows them (1) to find and download files located on another Peer-to-Peer user's hard drive,[to collect and collate those files to make up e.g. a full length film,] and (2) to share with those other users files located on their own computer. Unfortunately sometimes these information-sharing systems have been used to engage in illegal activity."

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

It warns of the dangers of becoming involved in the distribution of illegal copies of files but, equally importantly, warns that P2P networks can be used to gain access to user's computers. It says "Peer-to-Peer networks also have been abused by hackers. Because these systems potentially expose your computer and files to millions of other users on the network, they also expose your computer to worms and viruses. In fact, some worms have been specifically written to spread by popular Peer-to-Peer networks. Also, if Peer-to-Peer software is not properly configured, you may be unknowingly opening up the contents of your entire hard drive for others to see and download your private information."

Source: http://www.fbi.gov/scams-safety/peertopeer . Text in square brackets is ours.

Translation: P2P software, in order to work at all, has to have access through your firewall. Once you've granted it that access to the network, there are no controls on what can pass through it. Therefore you are entirely dependent on the effectiveness of your anti-virus software which is only as good as the database it is connected to. P2P, therefore, creates an inherent risk to data security.

That latter warning is potentially the most important for Bitcoin: people who would not dream of

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

downloading and installing e.g. BitTorrent will, if Bitcoin becomes popular amongst a wide cross-section of society, install the Bitcoin software. Failures in configuration are a risk area that is largely outside the control of the system designers and maintainers.

Therefore, even the installation of a Bitcoin wallet on a PC in an office environment or on a company-use mobile device creates a material risk to the company's data security.

There are three ways that users can store their Bitcoin Wallet:

1. Software Wallet - Bitcoin.org says "Software wallets are installed on your computer. They give you complete control over your wallet. You are responsible for doing backups and protecting your money. "

2. Mobile Wallet of which Bitcoin.org says "Mobile wallets allow you to bring Bitcoin with you in your pocket. You can exchange coins easily and pay in physical stores by scanning a QR code or using NFC "tap to pay". (QR codes are and NFC means "Near Field " and is functionally similar to e.g. Visa Wave.

3. Web Wallets are basically a place to store your bitcoins on a server somewhere. "Web wallets allow you to use Bitcoin anywhere with less effort to protect

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

your wallet. " But they come with caveats. The Bitcoin Foundation issued the following warning: "you must choose your web wallet service with care as they host your bitcoins. " It also says "**Be careful.** Web wallets host your bitcoins. That means it is possible for them to lose your bitcoins following any incident on their side. As of today, no web wallet service provide enough insurance to be used to store value like a bank."

The term "insurance" is perhaps misleading: what it means is security and data integrity and this is at the heart of the issue as to whether confidence in the system will extend to the general population.

See http://bitcoin.org/en/choose-your-wallet for information on each of the approved Wallets which are not, because of the Open Source nature of the project, necessarily designed or maintained by the original developers of BitCoin.

However, there are examples of where Bitcoins are stored by a third party in an account in the user's name. See about Bitcoin exchanges, below

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Box 5: The Liberty Dollar case: a red herring?

There has been some talk that Bitcoin miners may be held liable under US law preventing the production of money. To make that claim, those supporting it cite a 2011 federal case against Bernard Von NotHaus. The 67 year old man was convicted of producing "Liberty Dollars" which were, in fact, minted coins. They were not counterfeit - but they were accepted to be a currency. He produced coins said to be worth approximately USD7 million. He was convicted of of making coins resembling and similar to United States coins; of issuing, passing, selling, and possessing Liberty Dollar coins; of issuing and passing Liberty Dollar coins intended for use as current money; and a somewhat strange charge of conspiracy against the United States.

Conspiring to do what is not known but an FBI statement at the time said ""“Attempts to undermine the legitimate currency of this country are simply a unique form of domestic terrorism,” U.S. Attorney Tompkins said in announcing the verdict. “While these forms of anti-government

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

activities do not involve violence, they are every bit as insidious and represent a clear and present danger to the economic stability of this country," she added. "We are determined to meet these threats through infiltration, disruption, and dismantling of organizations which seek to challenge the legitimacy of our democratic form of government."

In coordination with the Department of Justice, on September 14, 2006, the United States Mint issued a press release and warning to American citizens that the Liberty Dollar was "not legal tender." The U.S. Mint press release and public service announcement stated that the Department of Justice had determined that the use of Liberty Dollars as circulating money was a federal crime.

Saying that the alternative is "not legal tender" is fine. But it is a stretch to say that circulating tokens which do not purport to be what the British would term "currency of the Realm" is illegal per se, and an even bigger stretch to argue that the use of tokens that persons accept is a form of terrorism.

ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

The reason that the von Nothaus case was of such importance to the authorities was because of his intention: the FBI says "According to the evidence introduced during the trial, von NotHaus was the founder of an organization called the National Organization for the Repeal of the Federal Reserve and Internal Revenue Code, commonly known as NORFED and also known as Liberty Services. Von NotHaus was the president of NORFED and the executive director of Liberty Dollar Services, Inc. until on or about September 30, 2008. Von NotHaus designed the Liberty Dollar currency in 1998 and the Liberty coins were marked with the dollar sign ($); the words dollar, USA, Liberty, Trust in God (instead of In God We Trust); and other features associated with legitimate U.S. coinage. Since 1998, NORFED has been issuing, disseminating, and placing into circulation the Liberty Dollar in all its forms throughout the United States and Puerto Rico. NORFED's purpose was to mix Liberty Dollars into the current money of the United States. NORFED intended for the Liberty Dollar to be used as current money in order to limit reliance on, and to compete with, United States currency."

ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

It is therefore arguable that the Liberty Dollar case was decided on its own facts and does not apply to electronic currencies.

But it is equally possible that a court might be persuaded that the leap from physical to e-currency may present the same threats that the Liberty Dollar case was designed to counter.

See http://www.fbi.gov/charlotte/press-releases/2011/defendant-convicted-of-minting-his-own-currency

ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Is Bitcoin developing in a responsible manner?

From both a society viewpoint ("do we want this in our society?") to a regulatory or even criminal law viewpoint ("how do we manage it and integrate it?"), one of the baseline questions is whether Bitcoin (insofar as it is an entity) behaves responsibly. This also, of course, underpins the question of viability of the project and its public acceptance.

Given that the Bitcoin Foundation does not "own" Bitcoin but merely guides its development and that open source development may - arguably maliciously - militate against stated policy any statement it makes is, in general, no stronger than a recommendation to the industry and users.

Even so, the Bitcoin Foundation makes a series of statements that are designed to at least encourage the proper and prudent use of Bitcoin.

For example,

- bitcoin transactions are not reversible and

- instant transactions are less secure because the

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

system takes about ten minutes to verify the coins and accounts and to update both the distributed databases and individual wallets. Until that happens, a transaction is, in fact, reversible. Confirmations come from multiple servers: Bitcoin recommends that users wait until they have received at least six individual confirmations before considering a transaction final.

- Bitcoin is not anonymous. Some critics read The Bitcoin Foundation's comment on this as demonstrating how users may create artificial anonymity. But that is not what the statement does, if it is read carefully. In fact, it relates to on-line privacy and security. It does not create ways of hiding relevant information from e.g. enforcement agencies nor, with appropriate court orders, civil suits. It says

"Some effort is required in order to protect your privacy with Bitcoin. All Bitcoin transactions are stored publicly and permanently on the network, which means anyone can see the balance and transactions of any Bitcoin address. However, the identity of the owner cannot be associated with their Bitcoin address until personal information is revealed by the owner during an exchange. This is why it is recommended for Bitcoin owners to use many different Bitcoin addresses; in fact, you should create a new one each time you receive money. This is especially important for public uses such as websites. You might also want

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

to consider hiding your computer's IP address with a tool like Tor so that it cannot be logged. "

Bitcoin warns "Bitcoin is still experimental... a new invention that is exploring ideas that have never been attempted before. As such, its future cannot be predicted by anyone. " Clearly this is designed to discourage large holdings and the trading of futures.

The fact that prices fluctuate widely is the subject of another caveat: "The price of a bitcoin can unpredictably increase or decrease over a short period of time due to its young economy, novel nature, and sometimes illiquid markets. Consequently, keeping your savings in bitcoin is not recommended at this point. Bitcoin should be considered as a high risk asset, and you should never store money that you cannot afford to lose with Bitcoin. If you receive payments with Bitcoin, many service providers allow you to convert them instantly to your local currency. "

There is also a warning that "Bitcoin is not an official currency. That said, most jurisdictions still require you to pay income, sales, payroll, and capital gains taxes on anything that has value, including Bitcoin. "

For a full list of the "You need to know" statements see http://bitcoin.org/en/you-need-to-know

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

It is also useful to read the "Innovation" page at http://bitcoin.org/en/innovation.

Can regulators shut down the service?

There are three discrete avenues of approach: legislation/ regulation, direct action and indirect action.

Bitcoin says "Bitcoin allows people to securely store and exchange value on a network that cannot be seized, manipulated or stopped by any organisation or individual. It gives many powerful tools to the people so that it is easier to protect individual rights against various levels of corruption. "

Legislation / Regulation

It is possible for countries to simply ban the use of currencies other than fiat currencies. However, while possible, it is unlikely to be practical. For example, to do so would, unless an express exemption is made, prevent the use of e.g. gold and silver which are widely used as a medium of exchange.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

If this option were to be considered, the legislation would need to be modelled on e.g. Hong Kong's gambling laws which make it an offence for any person in Hong Kong to gamble anywhere in the world (except using the very limited authorised schemes in Hong Kong itself.)

It would also be necessary to create an offence under which means of funding purchases were illegal. Again, there is a precedent e.g. in the USA where credit card companies are not supposed to permit payments for gambling by those in the USA anywhere in the world. However, experience has shown that such measures are easily circumvented by persons determined to gamble offshore.

Again, then, while possible, this option is not practical.

A third option would be to make it an offence to deal in bitcoins or to make or receive payments in them. In theory, this would be relatively simple to police - businesses soliciting payments in bitcoin would be readily identified by setting up a Google alert - however, while simple, it would be costly and arduous because of the amount of data that would be generated for analysis and would require a specific ban on each similar currency as it appears.

Once more, then, this is possible but not practical.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

On balance, then, to ban the currency by legislation is probably both too costly and complex to enforce.

However, it is much simpler to deal with it by regulation.

First, given that all those who deal in bitcoin by way of a business are subject to registration and regulation as bureau de change, e-money issuers, money transmitters or a combination of two or all three, the cost of compliance may be sufficient to drive small operators out of the market entirely. And if it does not, then inspections by registering authorities or regulators will ultimately prove so costly that they give up. Simply, the volume of e-currency related business is highly unlikely to cover the costs of the required measures and management time.

However, where dealing in bitcoin, etc. is done alongside an existing bureau de change, etc. then the cost is no different to that relating to other currency transactions.

But there are also pressures that may be brought to bear in other parts of the financial sector. See "Indirect action," below.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Direct action

Direct action against file-sharing networks is notoriously difficult because they are, by definition, distributed i.e. there is no single point at which any enforcement agency or regulator can take aim.

To understand this difficulty, it is helpful to look at exactly the opposite side of the coin: criminals use a variety of methods to turn the computers of innocent users into "zombies" - a very unhelpful name because the computers are nothing of the sort. The criminals install - either by voluntary download or by "drive-by-download" which happens when a user opens an e-mail that loads a web page or when a user visits a webpage that automatically installs software on the user's computer. This allows the criminals access to that computer. Depending on the criminals' intent, they may steal data or even take control of the computer so that it sends out millions of spam messages. This all happens in the background and the user is unaware that it is happening. Some programs wait until the machine has been idle for a predetermined time, presuming that the load the program places on the machine will never be seen because the user is away. In this way, PCs left on overnight can originate vast numbers of e-mails or, as is increasingly common, attempts to access websites

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

for a variety of purposes. Such attacks are designed to create accounts on website and to post comments or, depending on how the system is set up, to create or edit documents within the website. The criminals operate a network of "command and control" servers which, although distributed, are the heart of the criminal's networks.

It is because the criminals are able to place their software on millions of machines around the world that they are able to obtain data and place spam or deface websites. Attempts to combat this are led by the software industry which, through its own update systems, is able to identify machines that have been infected (ironically, using technology similar to that used by criminals) and to do three things: remotely kill offending programs, inform users through a secure channel that their machine appears to have been compromised and to trace the dataflows back, even indirectly, to the command and control servers. Having identified the controlling servers, depending on where they are (and despite the common perception, the top level is more often than not in the USA) it is possible to shut them down or block access to them in a kind of national firewall.

There are legal and technical difficulties with a remote kill: it is modifying the user's PC without his express consent. Under most laws, implied consent is not

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

viable and there are questions about the validity of consent to such modification as part of a bundle of consents, on take-it-or-leave it basis. A typical clause might say "you agree to download updates to your system to improve or add features or for security."

There has been much debate over Apple's use of a "kill switch" for software that the company has not authorised for installation on devices using its iOS (phones, tablets, etc.), even for phones that - in iPhone terms - have been "jailbroken" i.e. freed up for use of third party software or - even more controversially, "unlocked" from a particular provider's network. This is not new: the killswitch has been embedded in iPhones since 2008 and possibly earlier. Yet in June 2010, Apple applied for a patent for a kill-switch that would enable the company to wipe any phone that it detected had been modified. http://www.techdigest.tv/2010/08/poll_-_is_apple.html

Apple's justification was that evidence that a phone had been tampered with was evidence that it had been stolen, a dubious proposition given the number of users who simply wish to take control of the device they have paid for.

The company said ""An activity that can detect an unauthorized user can be any action that may indicate the electronic device is being tampered with by being,

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

for example, hacked, jailbroken, or unlocked. Jailbreaking' of an electronic device can generally refer to tampering with the device to allow a user to gain access to digital resources that are normally hidden and protected from users. "'Unlocking' of a cellular phone can generally refer to removing a restriction that 'locks' a cellular phone so it may only be used in specific countries or with specific network providers. Thus, in some embodiments, an unauthorised user can be detected if it is determined that the electronic device is being jailbroken or unlocked."

The patent also provided for remote control of the device - taking photographs and sending them and location information before killing the phone.

Apple is not alone: also in 2008, when Apple admitted to its kill-switch, Android admitted to having something similar - but in the case of Android, it is (reportedly) limited to killing malicious applications, or "apps." And Google has used it: in June 2010 it controversially used it to remotely kill two apps that the company said were harmless but "practically useless" - it turned out that the apps “misrepresented their purpose in order to encourage user downloads” according to Google which said the removal was for "security purposes." Reading between the lines, it seems that the apps did little or nothing except overtly (i.e. not secretly) collect data from users, the purpose of which was never fully

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

explained.

But Android, itself, does not prevent unlocking or hacking the device (indeed, it actively encourages it - if users are brave enough to dig around in an unfamiliar operating system) and there are a host of free and paid for applications to locate lost and stolen phones, to monitor their whereabouts (some of which are buried and invisible to thieves) and to which a SIM independent code can be sent to wipe the phone as soon as it is logged onto a wifi or other internet connection. The difference between this and Apple's idea is that it's user-instigated. Google also provides a remote-wipe at the user's behest within versions of Android after 2.2. This is managed through the user's own Google account.

In June 2013, Apple announced that its kill-switch was to be enhanced in the iOS7 due to be released later this year. Apple says that it's in response to requests from US prosecutors and in April 2013 a "top prosecutor" in California San Francisco District Attorney George Gascon said he "pressed an Apple representative to design a 'kill switch' for iPhones so that it would render devices useless after they are stolen and diminish its value on the black market." (Huffington Post)

There are Bitcoin apps for both iPhone and Android.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

However, Apple refuses to allow Bitcoin wallet apps into the AppStore. That means that, under Apple's stated policy, it can use its kill-switch to wipe a wallet installed using an App that Apple has not approved. In June 2013, Forbes (http://www.forbes.com/sites/jonmatonis/2012/06/13/why-apple-is-afraid-of-bitcoin/) said that Apple is afraid of Bitcoin because it hopes that its own mobile payments app, Passbook, will become the standard for iPayments. The article is useful: it deals with how Apple removed Bitcoin apps from the AppStore and the company's reasoning. Two Bitcoin apps to make it onto an iPhone are available from third party sites - if user have a jailbroken phone.

So, the technology is there to perform search-and-destroy actions against all manner of data on mobile devices. Is it also there for e.g. Windows or Linux PCs?

Yes. Most Linux distributions include near-constant updating which searches for files and replaces them as required, adds new files and removes obsolete files and, even, registry entries. So does Microsoft's Windows (although it leaves behind all manner of litter in, for example, the "Registry" - as do many other programmes.

Windows, in particular, has the built-in capacity to command a remote search and destroy : by updating

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

its Firewall and other security programs it can locate any wallet and delete or rename it. It is such an action that would raise the question of consent: by agreeing to the installation and running of a Firewall update, which never gives specific information as to what it is looking for, is the user consenting to the removal or hiding of his Bitcoin data? On the face of it, no. But the user might, in the USA in particular, have difficulty convincing a Court of his rights. Few would argue that to remove or kill of a criminal's remote control program is a bad thing - but it is the definition of "security" that raises questions. See "Bitcoin and the USA PATRIOT Act 2011, s311."

The overall picture, then, is that the technology is present for a wide range of parties to effect a remote search and destroy for a wide range of purposes.

So, if the software industry, of its own volition, can kill programs is it feasible that a government might require a software company to kill a program? It's a very small leap to be able to say "yes."

Indirect action

The simplest form of indirect action is to inform banks, in particular, that they are to carry a greater degree of

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

responsibility in relation to accounts relating to high-risk sectors. This may include requiring the banks to regard the owners and the businesses in the sector as high-risk and therefore subject to higher levels of due diligence and monitoring, the result of which would be to increase the costs of operating the accounts, perhaps to the point where they become uneconomic.

Already, in the UK, both HSBC and Barclays have informed those operating a range of money services businesses that their accounts are to be closed and requiring them to find alternative banking services. This feeds through into both a simplified counter-money laundering regime and lower costs for the bank, even where there is no suspicion of untoward conduct. The scale of this is shown in a Complinet article by staff writer Martin Coyle who says that, until recently, Barclays "around 75 percent of the market for payment services firms." See http://www.complinet.com/global/news/news/article.html?ref=165014&high=aml+risk+aversion

It is not, here, suggested that these decisions have been taken as a result of pressure from regulators but given that both banks have been undertaking a root and branch review of their business as a result of regulatory and criminal actions around the world, it is not surprising that an area which is inherently high-risk would be regarded as unwelcome, particularly if that

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

review shows that the costs of maintaining the accounts is disproportionate to the income derived.

Other forms of indirect action are, simply, governments either by ministries or by regulators briefing against new forms of currency and transactions. Some of this may be truthful, some may be misleading. One area which is especially important is the question of guarantees and capital adequacy. If a company holding bitcoins for account holders, or holding fiat currency on their behalf, were to go into liquidation, the legal position of the holdings is uncertain. Only if the company has put those funds into a segregated trust account will they be safe. There are no capital adequacy requirements and no insurance in the event of failure. This is why the Bitcoin Foundation warns users not to hold substantial balances in bitcoins.

As always, the greatest threat to the acceptance of any new currency is consumer confidence. Regulators are uniquely placed to destroy this.

Bitcoin as a vehicle for financial crime

In April 2012, the FBI published a report called "*Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*"

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

(http://cryptome.org/2012/05/fbi-bitcoin.pdf). The report is marked "unclassified" (which means it is not a "classified" as confidential or secret document) but for "official use only." However, it was distribute by the FBI to a number of enforcement and intelligence agencies around the world. The Observer reported that the FBI had confirmed to them that the release into the wider world was unauthorised but that the document is genuine.

The FBI concluded that "since Bitcoin does not have a centralised authority, law enforcement faces difficulties detecting suspicious activity, identifying users and obtaining transaction records - problems that might attract malicious actors to Bitcoin."

On the face of it, that sounds damning but the same criticism could be levelled at, say, the US Fed - it issues currency and it watches it down as far as the banks to which it is delivered but then, once withdrawn in cash, it disappears from view. Identifying users and obtaining transaction records is not difficult - that information is available in exactly the same way as it would be for any money services business. And if it is not, it is due to inadequacies in the legal and regulatory framework, not due to any inherently obstructive design of Bitcoin.

Is it difficult to detect suspicious transactions? Yes,

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

more so than within the banking system. This is because the money does not pass through the banking system when transfers are made. However, there are already laws in place to deal with e.g. hawala and if they have not been made to apply to e-currencies then, again, that is due to a shortcomings in the legal and regulatory framework.

E-currencies have not appeared out of the blue, unexpectedly: as noted at the top of this paper, I first considered them in 1996 - and Mondex pre-dated that consideration. If legislatures and those defining regulations and risk have failed to plan for e-currencies, then that is due to a failure of policy making and a lack of understanding of the direction that risks will take.

The FBI report is couched in terms that are designed to be prejudicial, literally to make readers pre-judge the service and to consider it undesirable. That, I would argue, is not the job of an enforcement or intelligence agency, especially one which intends to influence the decision making processes of similar agencies around the world.

For example, it says on page 1: "Bitcoin... provides a venue for individuals to generate, transfer, launder and steal illicit funds with some anonymity... Bitcoin will likely continue to attract cyber criminals who view

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

it as a means to move or steal funds as well as a means of making donations to illicit groups. If Bitcoin stabilises and grows in popularity, it will become an increasingly useful tool for various illegal activities beyond the cyber realm. "

In fact there are two items of real value on that page:

1 "unique complexities for investigators because of its decentralised nature." But, as noted above, even this risk is not quite what it first appears.

2. "Although Bitcoin does not have a centralised authority, the FBI assesses with medium confidence that law enforcement can identify or discover more information about malicious actors if the actors convert their bitcoins into fiat currency. Third-party bitcoin services may require customers to submit valid identification to complete transactions. Furthermore , any third party service that qualifies as a money transmitter must register with FinCEN and implement an anti-money laundering" scheme.

Therefore, once the boot was well and truly in, the FBI did in fact produce the true position - that it is those who operate a money transmitting business that are subject to regulation and must comply with, inter alia, due diligence requirements. And it doesn't matter if the transmission is of bitcoins, US dollars or Smarties.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

If value moves, no matter how it is represented, it counts as a money transmitter for money laundering regulation purposes.

For all the criticisms of its partisan terms, the FBI report is a very useful explanation of Bitcoin and some of the risks attached.

However, it is important that when reading the report a sense of proportion is maintained. While it is true that there are features that combine to make Bitcoin something different, none of those features are themselves new and, in particular, unique to Bitcoin.

The FBI frequently refers to "unique features" but in fact this is not so except insofar that it is, at present, the widely adopted only peer-to-peer private currency. But the underlying technology is, as noted elsewhere, commonplace.

Note, too, on page 4, in the breakout box research at University College Dublin describes the limits on the anonymity that the FBI was so anxious to trumpet in the first paragraph of the report.

The break-out box on page 5 says ""no historical records of transactions associated with real-world identity." This is so only because, at the time, FinCEN had not notified Bitcoin server operators that they

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

were included within the MSB requirements. Mt.Gox, the largest server, has made an application which, at the time of writing, is understood to be pending.

Note: when reading the FBI report, do not be misled by the expression "open source reporting." It's nothing to do with open source in the software sense: it means they found the information on the internet. Their view (see the explanatory box on page 2) is that if it's on the 'web it must be true because if it wasn't, someone would have written a contrary view. Obviously they have never tried to correct mistakes in Wikipedia (sic).

It is notable that the examples used - for example uncorroborated stories that someone has said that Lulzsec, a hacking group, has used BitCoin as a mechanism for fundraising. From the "yeah, right" department: elsewhere in this issue, we report on similarly unsubstantiated reports - in that case alleging that Lulzsec hacked bitcoin.

"The FBI assesses … that malicious actors will exploit bitcoin to launder money." They say that they have based this assessment on other virtual currencies such as e-Gold and WebMoney. But the examples used are not specific to virtual currencies, much less exclusive to Bitcoin.

I am not, here, underplaying the risk of Bitcoin and

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

other virtual currencies being used for money laundering. There is no doubt that since I began looking at the area of e-currency and virtual currency in 1996, each one presents opportunities for laundering. But while they present those opportunities (and the corresponding risks for financial institutions) the simple truth is that the risks they present are, in principle, not new. The vehicle - as we saw with so many fraudsters aping e-Gold's service - is not the problem: the problem is lax, slow or otherwise inadequate responses when criminals move into the field. It is significant that the FBI report sets out the case of 16,000 bank accounts with a US regulated bank being used to create 3,000 online "membership" accounts at an online auction site, offered for sale non-existent goods and collected the money.

That had nothing to do with virtual currency or e-currency. It was a clear and obvious failure by the traditional bank. But the FBI has then tried to use the case for further "smearing" of the e-money sector by saying "these funds were then used to purchase gold from gold farmers. The subjects then sold this gold for real money [to persons entirely unconnected to the scheme] using a dedicated third party scheme."

The laundering scheme (i.e. taking the money from the bank, buying and selling assets with it so as to collect apparently unconnected cash) has nothing material to

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

do with the e-money / virtual currency sector except insofar as the gold dealer did not undertake due diligence, which, again, is a failure of old fashioned legal and regulatory systems and their enforcement.

So, again, it is important to realise that Bitcoin, because of its distributed nature, does make investigations more challenging but, contrary to the FBI's paper, the traceability of the coins makes it more accountable than cash issued by the USA. Secondly, provided that those who operate servers properly conduct due diligence, then there is real world information, at least insofar as that specific operator is concerned.

Is there a financial crime risk that the FBI missed? Yes. What they missed was money laundering *within the system* by a person using multiple identities registered at multiple providers in multiple countries, or by connected persons who, as in the case of the International Bank of Curaçao simply moved money around within their own network.

Bitcoin and the USA PATRIOT Act 2011, s311

Without wanting to pour petrol on the conspiracy theory fires that are raging out of control since Edward

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Snowden told that part of the world that had been asleep since at least the 1970s that the US government is watching them, it is important to realise just how deep into the everyday use of computers the US government in particular can reach.

Simply, it does not need to monitor individuals' use of Bitcoin if it can find what passes in the US Treasury for "evidence" that Bitcoin can be classed as being "of primary money laundering concern under s312, USA PATRIOT Act 2011.

How strong need that "evidence" be? Not strong at all, as the 2007 listing of Banco Delta Asia demonstrated. In fact, several independent reviews showed that the USA had nothing that would pass as evidence in a court for the simple reason that there was none: there was no evidence of converting counterfeit notes for North Korea and no evidence of laundering the proceeds of an alleged drugs trade conducted by North Korea, both the central planks of the US Treasury action.

It had been long known that the bank had dealings with North Korea which means dealings with the government per se and the leaders in their personal capacity But none of those dealings were illegal, not even under US sanctions at the time.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

The decision to list Banco Delta Asia was, it seems, a political decision to create pressure on North Korea and its leadership. The quality of the intelligence that led to the decision to list the bank was seemingly on a par with the quality of the intelligence that stated that Saddam Hussein had weapons of mass destruction.

We know that the US Treasury is prepared to act, in a similar way, against the operators of on-line payment systems: in May 2013, the US Treasury designated Liberty Reserve S.A. as being of Primary Money Laundering Concern under s311 USA PATRIOT Act.

Liberty Reserve had been identified as a money laundering risk by World Money Laundering Report several months earlier.

The decision (the "finding" and "proposed rulemaking" are linked via http://www.fincen.gov/statutes_regs/patriot/section311.html) says that Liberty Reserve "is a financial institution operating outside the United States that is of primary money laundering concern." The finding says "Liberty Reserve is a web-based money transfer system or "virtual currency." That, I have no difficulty finding, is a description that can accurately be applied to Bitcoin.

The finding goes on "[Liberty Reserve] is a financial

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

institution currently registered in Costa Rica and has been operating since 2001. Liberty Reserve's system is structured so as to facilitate money laundering and other criminal activity while making any legitimate use economically unreasonable." Were these criteria to be applied to Bitcoin, the tests would, mostly fail: there is no Bitcoin "financial institution" therefore therefore there is no place of registration. Also, Bitcoin does not "make any legitimate use economically unreasonable." However, Bitcoin, along with every retail bank and payment services provider would fall within the broad terms of "structured so as to facilitate money laundering and other criminal activity." That sentence encompasses all retail banking functions, money transmitters and - frankly - almost any business activity whether in financial services or otherwise. However, fortunately, the document sets out the specifics which it says are grounds for concern. Readers are recommended to obtain a copy from the above link.

The US Treasury's specific concerns over Liberty Reserve were that it "uses a system of internal accounts and a network of virtual currency exchanges to move funds... users [add credit] to their accounts buy ordering a bank wire or money services business (MSB) transfer to the bank of a Liberty Reserve exchanger. Users can also [add credit to] Liberty Reserve accounts by depositing cash, postal money

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

orders or cheques directly into the exchanger's bank account. The exchanger then credits a corresponding value to the user's Liberty Reserve account denominated in "Liberty Reserve Dollars" or "Liberty Reserve Euros."

So, the Liberty Reserve scheme was, in principle, similar to e.g. e-gold and a host of other schemes under which agents for the promoters sold something (in this case a nebulous concept of LR dollars or LR euros) in return for a currency. A centrally held record then permits transfers between users which, again, is in principle no different to internet banking.

It is perhaps not surprising that Liberty Reserve operates in a functionally similar way to e-gold: it grew out of GoldAge, a New York e-gold exchanger. The US Treasury's document is less than precise in its description of the action against e-gold and its results. E-gold and its affiliate Gold and Silver Reserve, and E-gold's founder pleaded guilty to "conspiracy to launder money" but were not charged with money laundering per se. The facts as presented related to failure to adhere to e.g. customer identification and record keeping. The directors of the company pleaded guilty to operating an unlicensed money transfer business.

It was the statement of the Washington DC district attorney Jeffery Taylor that relates specifically to

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

similar systems: he said ""Because of the successful prosecution of these defendants, digital currency providers everywhere are now on notice that they must comply with federal banking laws or they will be subject to prosecution." However, Taylor was wrong in one significant respect: e-gold was no more a digital currency than the US dollar and, indeed, arguably less so. In fact, e-gold operated on a gold standard - a fact that US prosecutors did not at first believe and tried to allege that the claims that the company's issued e-gold currency was fraudulent - until they actually saw the gold.

E-gold put in place a full customer identification scheme, customer due diligence and, where appropriate, enhanced due diligence for all existing accounts which were, to all intents and purposes, frozen at the behest of the US government until it was satisfied as to the company's measures. That resulted in what amounted to a form of administration and, co-incidentally in June 2013, the receivers announced that those who have proved their bona fides would be entitled to recover their money under a "Value Access Program."

But the way the US Government dealt with the scheme raises serious questions: in a media release dated June 2011, the company said "EGL originally contacted the government in 2009 and offered to assist it in

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

recovering proceeds from criminal activity believed to be engaged in by certain third-party account holders while at the same time ensuring the return of value to qualified account holders. This dialogue culminated in the development of a Value Access Plan ("VAP") acceptable to EGL and the government.

"Pursuant to the terms of the VAP, the government filed papers today to initiate the forfeiture of the value of all e-metal accounts, an important first step in the process of returning value to the e-metal account holders who satisfy certain specified requirements. The VAP provides a process to facilitate the forfeiture of proceeds of criminal activity in which certain third-party account holders are alleged to have been engaged. The VAP also sets forth a process to enable the return of value to e-metal account holders not alleged to have been involved in any illicit activity if they comply with EGL's Customer Identification Program ("CIP") requirements. The filing of today's civil action marks an essential step in winding down the current e-metal system." (http://blog.e-gold.com/press_releases/)

It also said "In compliance with the terms of a plea agreement between the Department of Justice and EGL, account holder activity has been restricted since October 2008. " It would not be difficult to see that the management of e-gold was put into a position where

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

they faced serious criminal penalties if they did not freeze the assets of all of its customers - worldwide - with immediate effect, such assets to be released only if the USA did not "allege" involvement in criminal activity.

This, it has to be said, is not very different to the treatment of John Mathewson who entered into a US plea agreement that was accepted only if he agreed to (and did in fact) commit a criminal offence in the Cayman Islands - that of revealing confidential banking information in relation to the bank he controlled, Guardian Bank & Trust.

NB: e-gold.com, which we are talking about, and egold.com, which we are not, are entirely unrelated. Don't confuse them.

The US Treasury's case against Liberty Reserve quotes another US government department - the US Department of State which, in its 2012 International Narcotics Control Strategy Report said that Costa Rica's 2002 laws "create an invitation to launder funds by eliminating the government's licensing and supervision of casinos, jewellers, [real estate agents, lawyers] and other non-bank financial institutions. The US Treasury goes on to say that Liberty Reserve's own website said that "registering in Costa Rica allowed the company to avoid US authorities because Costa Rica does not have a mutual legal assistance treaty with

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

the USA." Combined, the US Treasury opined "suggests that Liberty Reserve has specifically sought out jurisdictions with weak anti-money laundering controls and apparent immunity from US prosecution.

The US Treasury's case against Liberty Reserve sets out why it says that it is "designed to facilitate money laundering and illicit finance."

In short (for the full detail, please see the US Treasury note) "to open an account through the Liberty Reserve website, a user is asked to enter basic identifying information such as name, e-mail address and date of birth. Liberty Reserve does not require users to validate any of that information.... Liberty Reserve requires only a working, even if anonymous, e-mail address. Once a user has an account with Liberty Reserve, its anti-money laundering policy does not suggest that it either requires or verifies any information associated with any transaction."

This of course means that, once within the system, inter-partes transactions are conducted between persons who have not been verified and who are able to operate on an information-only basis outside the banking sector. As the US Treasury says "accounts can be entirely anonymous and.. account holders can transfer funds to or from anywhere with anyone with anonymity. Indeed, Liberty Reserve advertises this fact

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

as a virtue of the service."

For the full view as explained by the US Treasury, see the document referred to above.

So, if Bitcoin is not a financial institution and it has no place of registration, can it be said to have a central place where records are kept?

No. There is a network of servers but these are not operated by Bitcoin, per se. They are operated by Bitcoin miners and they do have a place of business - both where they do actual business and where their servers are located.

How does Bitcoin work?

The following is based, mainly, on information from arimaa.com, a Bitcoin provider which has published possibly the clearest guide to how Bitcoin works in practice.

1. All users need "a place to store your bitcoins" and this is the "bitcoin address." This is a long alpha-numeric string (it's not technically a series or a sequence). It has both a "public" and "private" key - just like most encryption programs. The private key is

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

also a long alpha-numeric string. The keys are stored in a file called a bitcoin wallet. That wallet file is also encrypted and password protected. The user has that password and the private key. The public key - the address - is the way the system syncs to recognise where bitcoins are stored.

2. The Bitcoin wallet is downloaded from bitcoin.org - a website that says that is was registered and is owned by the Bitcoin core developers and community members. Although there is a link to the Foundation, the .org site says "Bitcoin.org is not an official website. Just like nobody owns the email technology, nobody owns the Bitcoin network. As such, nobody can speak with authority in the name of Bitcoin."

3. There are wallets for computers/laptops, wallets for phones/tablets and web wallets.

4. Users create one or more bitcoin addresses. In fact, Bitcoin recommends using multiple addresses for privacy and security reasons (while reminding users that use is not anonymous). Addresses are, in effect, a front-line which guards the privacy of the Wallet holder - similar to the way that anyone can know a street address but only those with permission know exactly who is in the house (not a good example, as any due diligence practitioner will know).

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

5. A user logs onto his account, issues a payment instruction in a system similar to an on-line banking system, marks the payee as a bitcoin address and sends the money. Because of the time taken to sync the system, it takes about 15 minutes for the entire system to know where that money has left and where it went. Once that is confirmed, the transactions is concluded and cannot be reversed.

Non-legislative / law enforcement threats to Bitcoin

In Bitcoin mining (above) it was noted that Bitcoin mining is becoming a very uncertain way of creating blocks and, in particular, the lottery of gaining a block, creating it and securing the reward.

A very clear explanation of the reasons why mining is becoming difficult to earn more than pocket money at (ignoring the cost of technology and running it) is at http://www.youtube.com/watch?v=4fwAseQoUCs. Note that things are moving very quickly in this area and this video, produced only in March this year, is in parts obsolete.

This is, practically, one of the biggest threats to

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Bitcoin.

First, without the miners, the supply will decrease and the price will increase. If miners are not making enough money to cover the costs of equipment and running it, then even hobbyists are going to stop doing it.

Second, miners are an integral part of the transaction and record keeping functions that keep Bitcoin working. If miners' machines are turned off and volumes increase, there is a danger that the system will simply overload itself. It is possible that the system protects at least some part of this by the overall peer-to-peer function but inevitably as the number of machines operating that function falls, leaving a greater proportion operating as wallets only, the remaining machines will have to work harder.

The Bitcoin Foundation already requests users who run computers 24 hours a day to adopt the P2P version of the wallet even though they are not engaged in mining.

Also a realistic threat to Bitcoin is a whispering campaign designed to undermine confidence in it. Basically, planted stories about the risks of losing money if the value of Bitcoins falls, of the unpredictability of pricing goods and services as well

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

as stories about data security will reduce public confidence and therefore the viability of Bitcoin.

There are valid concerns: in April 2013 it was reported that IT security specialists Kaspersky had identified a virus, spread via Skype, that turned user's PCs into zombies operating a massive virtual network for Bitcoin mining purposes. As noted elsewhere in this paper, that the P2P system can come under attack in this way is nothing unforeseen. But the virus was being accessed, at its peak, some 2,000 times per hour. Most disturbing that it was done from within the Skype network - quite probably the most trusted P2P network (if only because most people don't realise how it works - although these days it is a hybrid of P2P and server-based). Source: http://www.bbc.co.uk/news/technology-22064534 . The Skype distribution was done by the sending of messages with an attachment containing the virus or a link to it. The message was seemingly sent from within a Skype account to the contacts in that account, with a message similar to "this is my favourite photo of you." Given the widespread hijacking of both yahoo.com and hotmail.com accounts, which are then used for phishing attacks on those in the contact book of the original account holder using a very similar message, the prospect for similar distribution from apparently trusted sources is extraordinarily high. However, it is important to notice that this distribution method has

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

been in use for some time, long pre-dating the use to deliver the Bitcoin related virus. However, those who wish to brief against Bitcoin are likely to focus on that one instance, ignoring the fact that the risk is applicable to any illicit activity the criminals wish to perform under guise of that message.

Thirdly, several financial regulators have a policy of holding private meetings with senior officers of financial institutions and instructing them to take action which the current law might not cover. It falls short of a formal, public instruction. It would not be outside the bounds of reasonable assumption that some banking regulators will use arguments similar to those in the FBI report referred to elsewhere in this document to say to banks that they consider that dealings with bitcoins or those in business related to Bitcoin are of such an elevated risk relating to e.g. money laundering that if they are found to have been involved in transactions relating to Bitcoin that late turn out to be related to money laundering, the regulator will adopt stern measures.

Keeping eyes on the money

When the USA's FinCEN decided, in December 2007, to abandon its proposed rules relating to "hedge funds"

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

(alternative investment schemes or private investment funds) it was because, as their spokesman said "we have eyes on the money through the banks." Although there are rumours that this policy may be reviewed, there are as yet no firm indications that this is so.

The policy was and remains deeply flawed. To assume that an intelligence agency (for that is what FinCEN is, in its FIU role), has a monitoring function in relation to accounts which are portmanteau accounts operated by the bank's customer - in banking parlance a payable-through or pass-through account - is naïve in the extreme.

Ironically, it is because FinCEN takes exactly the opposite view in relation to virtual currencies, that operators of such businesses are required to register as money services businesses.

To simplify: where "hedge funds" are concerned, FinCEN says that inter-bank data is sufficient to assess and manage money laundering risk and that the managers of such funds are not required to undertake due diligence on their clients; where providers of payment services are concerned, even though the banks have exactly the same data as in the case of hedge funds, managers of payment services companies are required to undertake due diligence.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

This is an anomaly - and one which makes no sense. There is no justification for suggesting that a wealthy client of a hedge fund is any less likely to be a money launderer than a foreign worker sending money home to his family through a virtual currency system.

A client of a hedge fund should be put to rigorous due diligence as to the source of the funds he is depositing: "I'm rich, look me up in Google" is not an acceptable response to KYC enquiries. Those clients are likely to be, also, clients of private banking services - which are required to undertake due diligence.

This is not to argue that providers of virtual currency should be exempt: they should not. But where credits are made through a recognised and trusted bank or through a credit / debit card issued by such a bank, then some proportionality should be applied. This may be in relation to small accounts for some systems.

However, it it is not feasible to apply, in the case of Bitcoin, a small account exemption. This is because of the highly volatile value. If a small exemption limit of, say, USD5,000 were applied when the value was 1 bitcoin = USD5 and a balance held of equivalent to USD2,000 but then the price increased to 1 bitcoin = USD165 (as has happened) the limit would be breached without any action by the account holder.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Yet there is one important feature of Bitcoin which means that - provided there is proper identification of customers - it provides less not more risk of money laundering. That is that, at all times, the Bitcoin system knows where each coin is and its history. Ironically, then, there is more prospect of a regulator having "eyes on the money" than in many existing payment or even investment systems.

This ties back to the earlier question of whether Bitcoin sidesteps payment mechanisms. The answer is not a simple yes or no. For payments made within the Bitcoin network, the coins do not touch the banking sector. This, on the face of it, is a worrying prospect. But of itself, it is not: it is no different to banknotes and coins in circulation. In Ghana in the mid 2000s, the government struggled to increase the use of banks: the reason was that more than 70% of issued currency was in circulation. Some 90% of the population did not have a bank account. There was a widespread mistrust of banking procedures - from what I could see from my work with banks there entirely unjustified.

But even large payments were made not with cards, cheques or even drafts but with - literally - suitcases full of cash. This was made worse when, in 2001, banks refused to clear cheques drawn on other banks. As the purchasing power of the Cedi diminished, amount equivalent to as little as USD30 required a

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

bundle of notes literally the size of a housebrick.

In 2007, the New Cedi was introduced with 1 New Cedi = 10,000 Cedi. But the reasons for preferring cash did not relate only to the banking sector: cash became king when, in the 1960s, extensive price control mechanisms were introduced: this had the effect of taking significant slices of commerce, especially that in imported goods, into what amounted to a black market which was conducted exclusively in cash, a cultural change that has been difficult to unwind.

A final factor was due to the government's attempt to control the black market by removing from circulation the largest bank notes, the 50 Cedi. Although Ghanaians were able to deposit these notes and/or to exchange them for smaller denomination notes, an unknown but reportedly substantial proportion were never returned to banks. Interestingly, it has been suggested that this was because those who had profited from the black market and had hoarded their profits in 50 cedi notes realised that if they did so, they may be identified as black marketeers. In 1982, this may be seen as in some way prefacing the effects of counter-money laundering laws. Following this, faith in the currency continued to decline, leading to commerce resorting to the use of hard currency and the widespread use of barter.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

ATMs were rare: incredibly, in 2005, there were a total of 84 ATMs from five banks all using the VISA network (http://www.balancingact-africa.com/news/en/issue-no-274/computing/visa-international-i/en)

There is one other material aspect of Ghana's banking system: in the mid 1990s, a now defunct bank introduced an electronic wallet similar to Mondex but its take-up was poor. In 2000, Ghana Commercial Bank and Agricultural Development Bank formed Mondex Ghana which was "expected to form the bedrock of an e-cash banking project in West Africa. Orders were placed with Hitachi to deliver the required technology. In March 2003, it was announced that Mondex would be launched in March that year. In May, there was some roll-out (see http://www.bankinginsurancesecurities.com/banking/payment_systems/payment_systems_news/ghana_tries_out_mondex) . However, all references to Mondex have disappeared from the websites of both banks.

Do Bitcoin and other e-currencies have the potential to undermine economies?

It is important to differentiate between the legitimate

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

concerns of revenue authorities (which drive the views of governments in relation to currency) in large economies and the realities that may result from the use of private currencies.

However, there are also social concerns: the risk of social instability resulting from a collapse in a financial system were demonstrated by the actions of the "Occupy" movement during the Financial Crisis that began in the USA in 2006 and spread around the world, the effects of which are, even seven years later, still causing considerable uncertainty and upheaval around the world.

The initial hurdle that must be overcome if an e-currency is to make significant inroads into an economy are confidence and acceptability. For the e-currency to become acceptable as a medium of exchange within a country, the question of convertibility is of diminishing importance as the use becomes both greater and more widespread. In short, will the e-currency gain such a critical mass that it becomes the basis of a parallel economy?

Size, surprisingly, may not matter. In "How not to be a money launderer" (1996) I quoted the then Finance Minister of Russia who, interviewed by The New Yorker magazine, had said that the USA's plan to replace the USD100 banknote may cause deep instability in

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Russia. Confidence in the rouble was so low that on many levels, the Russian economy ran on US dollars, he said. The fact that this was illegal was no bar to the parallel economy. But, even more worrying - and even more pertinently for our present purposes, what worried him most was not that Russia was dependent on the US dollar but that he was aware that a very significant proportion of the notes circulating in Russia at that time were counterfeit. In short, there was greater confidence in fake US notes than in legitimate roubles. He was concerned at the very real risk of economic collapse if the USA issued new notes and ordered the withdrawal of the old notes because, at that point, the counterfeits would become worthless.

At the other end of the scale, there are many small jurisdictions around the world which have a domestic currency but which are "dollarised" - that is they are functionally dependent on the use of the US dollar.

An extreme example is the island of Yap in the South Pacific where the local currency is stones. The history of these is well documented but be careful - a lot of that which appears on the internet is both lightweight and derivative. Their currency worked, there was an effective banking system (which many laugh at, failing to realise that it is, in principle, exactly the same as other banking systems) but it was a bit impractical. And so the US Dollar became the de facto currency.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

However, the stones remain legal tender and are, in fact, used.

Somewhere in the middle is the example of Ghana, discussed above. What happens when a population loses faith in its currency was demonstrated in Germany in the 1930s and in Zimbabwe less than a decade ago: hyper-inflation resulted in widespread dissent which was subjected to (to be polite) outrageous responses from those able to capitalise on it.

More recently, the (legally questionable) use of the US dollar in Iraq was viewed as a stabilising influence in a country where there were multiple domestic currencies - each of which needed to have convertibility for, even, domestic transactions. The plan was to replace the USD with a national, universally accepted currency.

In each of the above cases, the US dollar was the invader. In the cases of both Russia and Yap, its acceptance was by popular adoption, not as a result of any official policy. That can be compared to Guam in which the USD is the official currency, replacing the former national currency. Guam is, in effect, an overseas territory of the USA and its banks are regulated in the USA. The Bank of Guam is a member of the USA's FDIC.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

Other jurisdictions which are often regarded as "dollarised" include Vietnam, Cambodia, The Bahamas, Afghanistan and several UK Overseas territories including the BVI and the Cayman Islands - even though the East Caribbean Dollar (bearing the image of HM Queen Elizabeth II) is, in eight of the nine members of the Organisation of Eastern Caribbean States, the official currency.

It follows,then, that public acceptance of a private currency is the key factor.

In France , the cost of wars, settlement in the Americas and general bad economic management led to the then king being unable to issue sufficient gold coins. The solution, as created by Englishman John Law, was for the King to issue, what amounted to freely transferable IOUs and to keep the gold in his vaults. The assumption was made that there would not be a simultaneous demand for the return of all deposits and therefore he could expand the money supply by issuing more notes for more than the total gold held.

We can view the issue of those paper notes as, in some ways, similar to the issue of a private currency, albeit one backed with the reputation of the monarch.

Although France no longer makes such a promise, the Bank of England still perpetuates the myth that

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

anyone can turn up with a note and demand gold to the face value of the note with the words "I promise to pay the bearer.." on its banknotes.

I recommend readers get a copy of "The History Of Money" by Glyn Davies. It's not a new book but it gives a very clear indication of how currencies develop, the factors affecting acceptability, etc. Also recommended is "The Money Maker" by Janet Gleeson which explains, amongst other things, how France moved from the gold standard to paper money and how the paper became accepted.

Using these examples, we can demonstrate the following:

1. if conditions are right, populations will accept a medium of exchange operating in parallel to the official currency

2. that the conditions are that there be faith in and (within an economy) substantial acceptance of the currency.

We have demonstrated that populations can and do elect to operate in a parallel currency or even to use a supplemental currency.

Therefore, provided that an e-currency gains the

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

confidence of a sufficient proportion of the population, and that that proportion actively uses it either as a supplemental currency or, in extreme cases, as a replacement for national currency, it is clear that the potential exists for a private currency, including e-currencies, to undermine a national currency.

However, Bitcoin goes further: it is a truly global currency. Bitcoin itself says "Not often in our history has money been disconnected from any political influence or national economy. Could Bitcoin be the first global currency to cross all barriers between nations, politics, and cultures for the benefit of the common good?" Therefore, its popularity may be defined with reference to a national population but it may also be defined with reference to other populations. It is already being adopted by a noticeable number of software developers as a means of payment in preference to e.g. credit cards or PayPal type systems.

Threats to confidence include widespread ignorance and rumour. See **USA v Dwolla ex parte Mt.Gox** , above, for an example of how the action against Mt.Gox's account at Dwolla spurred, on one website alone, a slew of comments that tended to undermine confidence not in Bitcoin itself but in users' ability to both conduct transactions in bitcoins and to trade in Bitcoin, including "cashing out."

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

What are the risks for banks?

If it is accepted that bitcoin, etc. issuers are operating what amount to pass through accounts, then their bankers are taking the money laundering risk but do not have the information necessary to assess that risk.

But that risk is no different in principle to to the risk posed by any money transmitter.

Where the risk does differ is that the persons engaged in e.g. bitcoin mining and exchange have no history in the regulated financial sector and are therefore having to learn their money laundering / financing of future crime (including terrorism) risks from scratch.

While they may employ outside assistance to create systems, they will almost certainly have no compliance culture which is at the heart of any risk management system, in particular that involving the identification of suspicion.

Therefore, banks may be best advised to look at customers who are trading, as a business, in bitcoins and bitcoin miners not only in relation to their financial profile (itself difficult) but also as to the relevant

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

experience of their management team and compliance / risk management systems.

There is an irony: by insisting the Bitcoin exchanges register for counter-money laundering purposes and create and maintain counter-money laundering systems, governments and regulators are potentially increasing the risks for banks. The reason for this is the frequently argued position (with which I have always been diametrically opposed) that if a business is regulated within a jurisdiction that is a member of the FATF or an FATF Style Regional Body, then it becomes a business in respect of which a lower standard of risk assessment and management may be applied.

I take the view that mere membership of the FATF does not mean that all businesses within a country are safe to deal with nor, on a larger scale, does it mean that the country itself is safe to deal with. To prove my argument, I have to say only two words: "Russia" and "India." I could also say Germany (corruption), the UK (VAT fraud), France (corruption), Spain (drugs trafficking) , Italy (people trafficking), USA (Ponzi and securities fraud schemes) ...

The argument that a company is somehow automatically a good citizen because it is subject to a regulatory regime is facile. Those who rely on that

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

false presumption in relation to the conduct of accounts trading in private currencies will find that out for themselves.

This is not to say that banks should refuse to open and operate accounts for such businesses - if they allow other money transmitters or currency dealers to hold accounts, then there is no reason in principle to refuse to deal with those dealing in or mining bitcoins nor with bitcoin exchanges. But they should be assessed on a case by case basis.

Conclusions

1. If A transfers bitcoins to B who pays A in real-world currency in cash, provided A is not selling the coins in the course of a business, there is no record of the cash transaction and no obligation on A to comply with any money laundering regulations. As noted above, even if A sells bitcoins in the course of a business he is outside the regulatory regime relating to currency trading (he may nevertheless be subject to e.g. consumer protection legislation. It is only it A is an issuer that he falls within e-money laws and regulations, as a simple trader, he does not fall within that net.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

2. There are services provided by e.g. Bitcoin Exchanges which on the face of it bring those providing such services into the scope of financial regulation as deposit takers. The precise extent to which this is so depends on applicable jurisdictional laws and regulation. What is clear is that having any footprint in a jurisdiction will expose the providers of such services to applicable laws in that jurisdiction.

3. Bitcoin is vulnerable to market manipulation. While investment in Bitcoin itself is not subject to regulation, it is at least arguable that markets and dealers in Bitcoin futures are subject to regulation, depending on the definition of "currency" adopted in applicable law and regulation.

4. Bitcoin has the potential to undermine national economies. It also has the potential to be a disruptive technology in relation to payments which may have significant implications for banks and money transfer businesses.

4. Bitcoin has the potential to become a valid and valuable payment vehicle for micropayments and on-line traders, opening up the use of internet sales to SMEs and those who make few credit card sales and for whom existing systems are uneconomic.

5. Bitcoin has the potential to be used as a vehicle for

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

money laundering but, provided accounts are subject to due diligence of a standard applicable to other money transfer business, etc., the risk is similar to that for any money transfer business. No good reason has been established for holding it to a higher standard than, say, Western Union.

6. The volatility of Bitcoin prices means that it is has the potential to result in considerable social pressure if users see the value of the bitcoins they hold plummet. Recent history shows that the media is prepared to make extended and harsh criticism if they are echoing public sentiment, even when that sentiment is based on ignorance (to whit much of the criticism of the world's bankers in respect of the global financial crisis when those at fault were a very small percentage of the banking industry).

7. Those providing funds transfer services are subject to counter-money laundering law and regulation in jurisdictions where they operate.

8. Individual users, including those operating as miners, are not subject to any form of regulation as financial services providers. However, those selling Bitcoins will be subject to e.g. consumer protection measures in the same way as Bureau de Change and will be liable to registration under counter-money laundering laws as a money services business (or local

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

applicable terminology).

9. Banks face the same risks as they do in relation to e.g. bureaux de change or stockbrokers, for example. They bear the money laundering risk but they do not have the information to assess that risk.

10. The success of Bitcoin (and its inevitable clones to come) depends on public confidence, the extent to which it can be used, in practice, as a currency e.g. at point of sale and the extent to which it can operate in parallel with (i.e. without exchange with fiat currencies).

11. In the event that governments decide that there are insurmountable problems, including potentially matters of national security, it is possible that steps may be taken to block or close down the service. Direct action may be complex and difficult. Legal measures will also be complex. However, regulatory measures, influencing financial institutions and briefing against virtual currencies may be low cost, high impact ways of making such currencies unattractive if not actually undermining them to the point of near-destruction.

July 2013.

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

About World Money Laundering Report

World Money Laundering Report is published by Vortex Centrum Limited, which can legitimately claim to be one of the world's first "new media" companies. Vortex Centrum Limited's first publication, in 1999, World Money Laundering Report was unique in being the first e-publication to cover money laundering. It has a reputation for blunt speaking.

World Money Laundering Report is edited (and mostly written) by Nigel Morris-Cotterill, Head, The Anti Money Laundering Network. With a quarter of a century of practise in law in a wide range of areas including criminal defence,financial services compliance, litigation, Morris-Cotterill formed Silkscreen Limited, a consulting firm, in 1994 to deliver advice and consultancy on money laundering risk management and compliance, and in doing so became one of the first specialist advisers to financial institutions on this area.

Morris-Cotterill wrote "How not to be a money launderer" in 1996, a non-legalistic guide to counter-money laundering laws, regulations and money laundering risk management (long before the term gained general currency) which predicted the course of development of money laundering techniques and the laws to combat them. Although long out of stock and out of print, the second edition (1998) has recently been released for the Kindle platform and reprinted in paperback. Morris-Cotterill is also author of Sun Tzu and the Art of Litigation (July 2012).

The Anti Money Laundering Network delivers training (face to face and e-learning) all over the world including high-level training for directors of financial institutions, regulators and legislators and organises high level conferences; publishes a wide range of information services including a library of white collar case studies.

For further information please see:
World Money Laundering Report:
www.worldmoneylaunderingreport.com
Vortex Centrum Limited:
www.vortexcentrum.com
Nigel Morris-Cotterill
www.countermoneylaundering.com

 ISSN 1473-3439

World Money Laundering Report Volume 12, Number 3.

ISSN 1473-3439