Digital currencies: Call for information

Robert Stokes (Lecturer in Law) and Matthew Shillito (Doctoral Researcher)

The School of Law and Social Justice, University of Liverpool

Question 1: What are the benefits of digital currencies? How significant are these benefits? How do these benefits fall to different groups e.g. consumers, businesses, government, the wider economy? How do these benefits vary according to different digital currencies?

Digital currencies offer a number of advantages to business and consumers, many of which derive from the challenges they pose to some of the fundamental assumptions which underpin our conception of money e.g. decentralised issue, use of cryptography without a third-party to solve the 'double-payment' problem etc. In brief, we identify the key benefits of digital currencies for merchants and consumers to be:

(1) Global application

Digital currencies have the technical ability to act as a de facto global currency. Digital currencies are not limited by geographical area, whether country or region, and allow for payments to be made without regard to international borders. The only limitation on this would be those of end-user technology limitations and the current lack of general acceptance amongst retailers. As digital currencies become accepted more widely, something that would be thought likely with regulatory intervention, end-user adoption is likely to spread and in turn the commercial incentive to solve the technology problem increases. A similar pattern can be identified with regard to the development of M-PESA as a payment mechanism via mobile devices.

(2) Quick transaction times

Transaction times for digital currencies are swift. Clearance is usually received within 5 minutes. In relation to Bitcoin, for example, in 2014 the average transaction confirmation time has been between 6 to 9 minutes.[1] In contrast, transfers using the standard banking systems tend to receive confirmation over a longer time frame, e.g. BACS takes 3 working days to clear; CHAPS is same day for instructions made before 2pm; and the Faster Payments service, will take up to two hours. Moreover, digital currency is not restricted by banking hours. In essence, the user is in full control of their money.

(3) Low transaction costs

A key feature of digital currencies is their low transaction fees, for example, within Bitcoin the transaction fee, when applied, is charged at 0.0005 BTC irrespective of value. As at December 2, 2014, that equates to $0.19 (with a BTC valued at $382.59). Fees may also payable to merchant processor at the point of conversion into fiat currency. As this separate process (between merchant and merchant processor) also utilises the Bitcoin system, the associated transaction fees are lower than other payment systems like PayPal and Western Union.

In contrast it is worth noting that for users with access to the traditional financial systems, BACS is free but limited to under £10,000. CHAPS transfers cost around £20. Faster Payments are also free (but are subject to institution limits).

[1] Average transaction confirmation time: <https://blockchain.info/charts/avg-confirmation-time>

(4) Security in transactions

Security is a key feature of digital currencies, particularly those like Bitcoin which are based on the blockchain system. Bitcoin and many other similar digital currencies operate on the basis of a 'push' system. This means that the value is transferred to the merchant, but they have no further control.[2] There is no ability for the merchant to re-charge the account. Conversely, the merchant in turn has additional security over alternative payment mechanisms where 'charge-backs' (e.g. credit cards) are possible for a substantial period of time following the transaction. Bitcoin transactions are secure, irreversible, and do not contain customers' sensitive or personal information.

(5) Enhanced Information Security

Further, there is no identifiable material attached to a Bitcoin, meaning that the merchant has no database of customer information that can be targeted by hackers for the purposes of theft or identity theft.

(6) Security in Storage of Value

Whilst it may be acknowledged that there are a number of deficiencies in digital currencies with regard to security of stored value (for both businesses and consumers alike), e.g. volatility of exchange rates, cyber-risks around encryption keys being 'hacked' or otherwise compromised, it is clear that in comparison to other payment methods digital currencies have utility around the security they offer e.g. no large cash sums requiring special security procedures for business, security for consumers in avoiding the need to carry large sums of cash etc.

(7) Transparency

Perhaps counter-intuitively given the anonymity concerns surrounding the operation of some digital currencies, they offer unprecedented levels of transparency. All information concerning transactions is available on the public ledger for anybody to use and verify. As previously noted, for decentralised digital currencies, given they are not particularly susceptible to manipulation by a single entity. This level of trust within digital currencies is further enhanced by the use of cryptography to secure transactions and key information and it is likely in many cases, also by the fact that digital currencies are not part of the traditional financial 'establishment'.

Significance of the benefits

Where a currency is not backed by an asset e.g. gold, nor underpinned by guarantee (e.g. by a central state issuer) the adoption of that currency is in a very significant way driven by the benefits it offers users, whether businesses or individuals. Using Bitcoin as an example, the benefits are clearly significant enough to warrant 100,786 unique transactions[3] of 8,116.67 Bitcoins (hereafter BTCs) on the 2nd of December 2014.[4] At the current exchange rate that equates to over $3,000,000 transferred in the last 24 hours. The significance of this

[2] Credit cards for instance are the inverse. They operate on the basis of a 'pull' system. Customers agree to merchants taking money from their account by providing them with the necessary data to access the account.

[3] <https://blockchain.info/charts/n-transactions?timespan=30days&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=>

[4] <http://www.bitcoinwatch.com/>

cannot be understated, and whilst the future of Bitcoin specifically is unknowable, points to substantial interest in the use of digital currency as an alternative to other currencies or payment mechanisms, albeit not, perhaps in the UK at present (e.g. a recent YouGov survey indicated that 71% of respondents were not interested in digital currencies).

Question 2: Should the government intervene to support the development and usage of digital currencies and related businesses and technologies in the UK, or maintain the status quo? If the government were to intervene, what action should it take?

In the UK specifically, it is unclear to us what the imperative would be for the Government to directly support the *development* of digital currencies. Certainly, digital currencies have the potential to fulfil a social good, e.g. around the unbanked, however, with regard to the relatively small percentage of unbanked persons within the UK, it is by no means clear that digital currencies are the solution in our case. This may be contrasted with populations where the causes (and extent) of individuals not having access to banking services is more amenable to useful intervention through the development of digital currencies. The potential, for example, for a digital currency such as Bitcoin to develop so as to facilitate financial inclusion where more formal financial systems have struggled is potent e.g., in Africa where 80% of the adult population are unbanked.[5] The Bitcoin structure would be easier to implement; fundamentally requiring only improved access to the internet and compatible devices.

One matter which should form a key part of the Government's response here is to invest in education. This can be done in two main ways: first, investment in skills; and second investment in educating the public as to the use of digital currencies and risks thereof. Digital currencies and the blockchain technology which underpins them, represent a significant opportunity to further the technology and information based economies within the UK. This point will be addressed further below but in short, the technology has implications far beyond digital currencies, e.g. self-executing contracts using blockchain technology. The key is not to stifle innovation by over regulation/intervention whilst also ensuring that where consumers (in particular) utilise digital currencies, they do so fully aware of the advantages and risks, just as is the case for currency (or payment mechanisms) generally. Regulatory intervention is necessary here, but the nature of the intervention must be appropriate to the specific risks it is intended to mitigate. In the case of digital currencies, we would identify the core drivers for intervention by Government to be limited to (i) consumer protection and (ii) financial (and other) crime risks.

It should also be recognised that whilst there may be 'unintended' consequences of regulatory intervention, e.g. costs, which will ultimately reduce current advantages of digital currencies, i.e. transaction costs will rise particularly with regard to third-party services, this may be a necessary step in the development of digital currencies. With regulation comes legitimacy and increased uptake and usage ought to follow where regulatory measures increase consumer (and business) confidence in digital currencies. This may be thought of as a crucial step in the evolution of digital currencies, albeit one which has potential negative impacts and may be thought of by some users as contrary to the principles on which some digital currencies were developed (e.g. Bitcoin).

[5] < http://www.mckinsey.com/insights/financial_services/counting_the_worlds_unbanked>

Question 3: If the government were to regulate digital currencies, which types of digital currency should be covered? Should it create a bespoke regulatory regime, or regulate through an existing national, European or international regime? For each option: what are the advantages and disadvantages? What are the possible unintended consequences (for instance, creating a barrier to entry due to compliance costs)?

When considering regulatory responses to any phenomenon, Government must consider two potentially conflicting interests: on the one hand, Government should encourage an environment suitable for innovation to flourish whilst, on the other, it should ensure that firms performing similar functions are regulated in similar ways. All of this must be done in such a way as to protect the consumer and, potentially in the case of digital currencies, the financial system more broadly. The challenge to be overcome here is that of how to effectively regulate digital currencies when one considers the key features, e.g. decentralised architecture, no inherent value or guarantee of value, pseudo-anonymity etc.

Should the Government decide to regulate digital currency then a uniform approach needs to be developed with regard to the regulatory environment active on firms fulfilling similar functions, e.g. third-party exchanges should face the same level of regulatory intervention where their risk factors are broadly similar (e.g. distribution channels, geographical coverage, self-imposed monetary limits etc). However, the different drivers for intervention should be reflected within the nature of the intervention itself. Thus, with regard to the financial crime imperative, a risk-based model could be of use similar to that which underpins much of the domestic, European and global anti-money laundering framework. In contrast a risk-based approach would not seem appropriate to ensure consumer protection risks are properly mitigated and so a different approach is required there, perhaps using licensing/registration mechanisms.

This approach will mean that the regulation is multi-faceted, reflecting the different aspects warranting regulatory intervention yet fair to all commercial actors within the emerging digital currency sector by creating a level playing field. Whichever driver, however, regulatory measures should apply to all digital currencies (though not virtual currencies as defined in the consultation). This has the effect of future-proofing, as far as possible in a field as fast-paced as this, the regulatory coverage and enhancing consumer protection and reducing criminal utility of digital currencies. It also prevents the framework from becoming reactive and dependent on understanding new products and technologies before it is able to include them within its scope.

The FCA's policy unit responsible for 'project innovate' could be further empowered to cover digital currencies. It currently works with firms who have developed innovative approaches in the financial sector; which is not explicitly covered by regulation, or for which application of regulation is ambiguous. It is very much a supportive role and could be of use here, notwithstanding the decentralised nature of digital currencies by supporting associated businesses e.g. exchange services; secure online wallet services etc.

Question 4: Are there currently any barriers to digital currency businesses setting up in the UK? If so, what are they?

No particular view.

Question 5: What are the potential benefits of this distributed ledger technology? How significant are these benefits?

The distributed ledger technology solves issues relating transaction security, i.e. preventing a unit of digital currency from being spent more than once without any third-party intervention or observation. Further, it also enhances customer information, privacy and data security protection. Most significantly however, is the potential utility of the blockchain technology coupled with the decentralised architecture of digital currencies, to broader applications rather than digital currencies, i.e. next-generation or Bitcoin 2.0 platforms. As an example of such platforms, for social media there is Twister (decentralised, effectively anonymous version of Twitter) and Ethereum which is geared towards autonomous contracts. Smart, self-executing, contracts are likely to be a significant development over the coming years with numerous possibilities, e.g. smart loans with automated interest rate adjustment according to set parameters e.g. repayment history over the course of the loan. Similarly, decentralised cloud storage services are in development.

This is an area where, with Government support, the UK could become a leader in this emergent area of technology, particularly given the potential cross over between smart contracts and smart property, e.g. driver-less cars with the UK's investment in such technology continuing through the Autumn Statement.[6] Further, developments such as Ripple have the potential to take the application and usefulness of the blockchain further. Ripple allows for lower-cost avenues for worldwide money access due to giving servers the ability to establish transaction veracity without crunching number intensive calculation as is the case, for example with Bitcoin.

Question 6: What risks do digital currencies pose to users? How significant are these risks? How do these risks vary according to different digital currencies?

The risk that digital currencies pose to users, is in many ways the threat that users pose to themselves when using digital currencies. Users need to be educated about using digital currency in a safe, secure manner. Users should be clear that without their cryptographic key, they have, effectively, lost their BTCs. Information technology literacy around back-ups, malware protection etc is crucial as is ensuring that each user controls access to their key in the same way that PINs are not to be circulated. One of the obvious risks that digital currencies pose to users is the fact that they are easy to lose, similar in many respects to cash. By way of illustration, an individual lost 7,500 Bitcoins when he discarded the hard-drive that he had them stored on.[7] The hard-drive contained the crypto-graphic "private key" without which there is no way to access and spend the BTCs. A solution of sorts was created when third party deep storage websites like Elliptic Vault began providing 'deep cold' storage systems for these keys. The issue with this is that access to a consumer's BTCs is being placed in the hands of start-up third-party companies with little or no track record. These third-party service providers are a potential area of regulation.

Another risk with digital currencies is that they tend to be extremely volatile in terms of their exchange rate into fiat currency. Bitcoin prices fluctuate wildly. This again, is an area which could prove to be a significant blocker to large scale uptake amongst consumers (certainly, businesses can use contract terms to protect themselves against price fluctuations, however, such volatile movements will do little to inspire confidence within consumers, and ultimately (digital currency as with fiat) confidence is everything.

[6] http://www.bbc.co.uk/news/technology-30316458
[7] < http://www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site >

Question 7: Should the government intervene to address these risks, or maintain the status quo? What are the outcomes of taking no action? Would the market be able to address these risks itself?

Yes, intervention to protect consumers should be welcomed. Education as to the risks (and advantages to consumers) of digital currencies is crucial. The growth of BTCs as a speculative investment is one which will be hard to prevent (as a market response) but it is a matter which requires further thought and research since the volatility created by speculative investment in digital currencies is a significant bar to wider adoption as a token of value by consumers. The advantages of digital currencies are in its use as a means of transferring value, and not as an investment opportunity.

Question 8: One of the ways in which the government could take action to protect users is to regulate. Should the government regulate digital currencies to protect users? If so, should it create a bespoke regime, or regulate through an existing national, European or international regime?

For each option: what are the advantages and disadvantages? What are possible unintended consequences (for instance, creating a barrier to entry due to compliance costs)? What other means could the government use to mitigate user detriment apart from regulation?

As noted elsewhere in this response, we would support regulatory intervention to protect users from the risks identified in the manner suggested in the different responses to other questions.

Question 9: What are the crime risks associated with digital currencies? How significant are these risks? How do these risks vary according to different digital currencies?

Money is the lifeblood of crime. Thus, with the uptake of digital currencies comes the risk of criminal operations responding, adapting, and utilising such currencies. Every currency or indeed store of value and payment mechanism has criminal utility whether cash, plastic cards, wire transfer or other. One of the most obvious crimes that can be committed on digital currencies is theft and with increased uptake and acceptance of a digital currency comes a corresponding increase in the risk of theft. There are three key ways in which theft of digital currencies has occurred:

1. Attack on a third-party website
2. Malware programmes
3. Third party companies exploiting consumers

As an example of the first category, the third-party website, BIPS (Bitcoin Internet Payment System) suffered a denial-of-service attack, however, that was merely a smokescreen for a digital heist that quickly drained numerous wallets, netting the criminals a reported 1,295 BTCs (worth nearly $1 million). As a technology-based development, digital currencies are vulnerable to malware specifically designed to infect a user's computer and cede control to the criminal.

The final way is third part companies exploiting consumers. One such example is Mt.Gox. Mt.Gox which lost $600m in BTCs in uncertain circumstances. Another example is a China based Bitcoin exchange called GBL launched in May. Almost 1,000 people used the service to deposit BTCs worth about $4.1 million. The exchange was revealed to be an elaborate scam after the perpetrator closed the site later that year and absconded with the funds. Where businesses create a centralized body to operate as an adjunct to a decentralized structure, but with no corresponding oversight for the centralized body, fraud is both possible and, in general terms, predictable.

A further criminal risk associated with digital currencies is money laundering. Digital currencies provide opportunities for criminals to exploit its interconnectedness, accessibility and anonymity to achieve their illicit objectives without detection or sanction. The ongoing revolution around payment technology and specifically, peer-to-peer transfer of money using the internet, has heightened regulatory concern around what is being termed "cyberlaundering". Essentially, Bitcoin and analogous digital currencies *could* enable money launderers to move illicit funds more quickly, with little expense, and even less scrutiny, than technology has allowed in the past.

The general approach of AML regulation (whether at a global or national level) has focussed upon the use of key professions as de facto policemen, guarding entry points into the financial (and other) systems and limiting the ability of criminals to transfer value without scrutiny. Digital currencies, such as Bitcoin, evade these key professions for as long as the user is content to keep the value as digital currency, i.e. unless and until the digital currency is exchanged for fiat currency (or goods or services) where the business, whether merchant or exchange service, is amenable to anti-money laundering regulation.

It should be pointed out, however, that the extent of these risks is by no means fully understood. There are, for example, significant limitations on digital currencies as currently operative from the perspective of a serious organised launderer. The volatility of the exchange rates e.g. BTC to US dollar would represent a significant risk to criminal organisations. This is true in two distinct ways. First, the value of the BTCs will be unpredictable and second, where a criminal organisation buys/sells significant sums of BTCs, that could in itself trigger a response within the exchange rate markets, thus fuelling the volatility. Most fundamentally, the scale of money laundering globally is such that the relatively limited uptake of digital currencies in effect hampers the laundering utility of that currency – one can only fail to see the wood for the trees where there are sufficient trees to obscure the wood.

Question 10: Should the government intervene to address these risks, or maintain the status quo? What are the outcomes of taking no action?

We would support regulatory intervention to address the criminal risks associated with digital currencies. As noted previously, together with consumer protection, these are the most pressing imperatives for regulating digital currencies. Given the difficulties of attempting to regulate digital currencies as currency (no central issuer; no control over supply/demand; no central organisation to impose regulatory requirements upon) it would seem futile to attempt such an approach. On the other hand, the commercial element of digital currencies, i.e. where they are accepted as payment for goods and/or services, would seem amenable to certain anti-financial crime regulatory measures, e.g. customer due diligence measures when high-value goods are purchased using digital currency. In this sense, digital currencies can be regulated in the same way as cash (e.g. the high-value dealers regime within the MLR 2007). The other avenue to mitigate crime risks associated with digital currencies would be to focus regulatory attention on the exchange services i.e. use the need for digital

currencies to be converted into fiat currency as a regulatory choke point.[8] Two key AML initiatives noted elsewhere in this report, CDD and SARs could be of some utility at that stage. There are also arguments to support controlling, perhaps through a positive licensing scheme, access to that form of business venture, from the criminal risk perspective.

In our view, with decentralised, pseudo-anonymous currencies such as Bitcoin, it is only that commercial side of the network which could or should be regulated to mitigate criminal risks. To attempt to regulate peer-to-peer transfers of BTCs would seem to be an exercise in futility.

Question 11: If the government were to take action to address the risks of financial crime, should it introduce regulation, or use other powers? If the government were to introduce regulation, should it create a bespoke regime, or regulate through an existing national, European or international regime? For each option: what are the advantages and disadvantages? What are possible unintended consequences (for instance, creating a barrier to entry due to compliance costs)?

Regulation through the existing anti-financial crime mechanisms would seem the most beneficial approach. However, certain core aspects of that regime e.g. Suspicious Activity Reporting obligations on third-party exchanges would require further consideration. Most fundamentally the limited knowledge and understanding as to legitimate usage of digital currencies e.g. Bitcoin is such that it would be very difficult for an exchange service provider to identify an abnormal i.e. suspicious Bitcoin transaction (as opposed to say, wire transfers where we have an understanding of laundering behaviour). Government should support multi-agency, cross-disciplinary research into this area so that the aspects of digital currencies which are more amenable to regulation under the existing financial crime measures are fully utilised, whilst accepting that certain aspects of digital currencies, e.g. P2P transfers are simply not susceptible to or indeed, suitable for, regulatory intervention. Moreover, in general terms, the role of the third-party exchange service is vital to serious organised crime (unless and until digital currencies are accepted as a de facto global currency in their own right, in which case, third-party exchanges will be defunct in any event.) At that point, effective regulation of digital currency will be challenging to say the least.

What has been the impact of FinCEN's decision in the USA on digital currencies?

The impact of FinCEN's decision to issue guidance on 'Virtual Currencies and Regulatory Responsibilities' is still relatively new, but its impact is already reasonably clear. The guidance provides that "administrators" or "exchangers" of virtual currency are considered MSB's for the purposes of the Bank Secrecy Act. Therefore, a virtual currency transmitter must be licensed whether starting or continuing relevant business activities. The guidance has provided a certain level of certainty in the market place, classification as an MSB is made based upon clear factual criteria, and all businesses which fall within that definition are subject to the rules.

What is significant is the choice of money transmitters as the first target for regulation of virtual currencies. They are the 'players' that are on the surface, visible to the outside world. As third parties to transactions they present a lot of the risks discussed above in the crime

[8] See further, 'Anti-Money Laundering Regulation and Emerging Payment Technologies' (2013) 32(5) *Banking & Financial Services Policy Report* 1; 'Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar' (2012) 21(3) *Information and Communications Technology Law* 221.

section. By classifying them as MSBs it brings these Bitcoin exchanges and payment processors into the regulatory framework, where previously they were unregulated. As a result of the US approach businesses may simply choose to locate overseas to evade regulation, digital currencies are not restricted by borders and in that sense it is not important where they are operating from. To register in all of the states could take a significant amount of time; such a requirement would not be as burdensome for virtual currency transmitters in the UK.

In terms of impact, the Department of Homeland Security ("DHS") issued a seizure warrant for a bank account held by a US subsidiary of Mt.Gox, because it failed to register as a money transmitter. This highlights that the guidance has had an almost immediate impact.

Question 12: What difficulties could occur with digital currencies and financial sanctions?

In terms of the key characteristics of financial sanctions, they must be: capable of application; and either restrictive or coercive in nature. If they are not capable of application then they offer little deterrent to financial crime. Digital currencies provide a barrier to the effective implementation of financial sanctions.

The 'Consolidated List of Financial Sanctions Targets in the UK' is a good illustration of the difficulties here. It provides a list of individuals and entities, by country, which should have their assets frozen. Key to it functioning is that those individuals or entities can be identified. The problem is that digital currencies mean that the transaction could be taking place anywhere in the world with originator information masked. Further, unlike other non-traditional payment methods (such as wire transfers) there is no need for a third-party intermediary, due to the decentralised structure and the technology used; therefore there is no one that can freeze the funds. Quasi-anonymity is another issue, even though every transaction is recorded on the blockchain (and freely available) as mentioned in response to Question One there is no personally identifiable information on it. This means that there would be a need to link wallets with real people, which can be difficult when the transactions are simple, but is particularly tough when users operate numerous wallets. This problem is further compounded by "dark" wallets which have been termed 'super-anonymous'; it encrypts and mixes users' payments so as to make flows of money online untraceable. The effort required to source an individual or entity, if possible, would not justify the resources it would undoubtedly take.

So, it seems that sanctions are only of use where there is some other kind of information which facilitates sanctions, e.g. as was the case where the CIA was able to confiscate BTCs as part of the closure of Silk Road. Consideration is needed as to how confiscation and asset freezing systems within the UK could operate in the realm of digital currency.

Question 13: What risks do digital currencies pose to monetary and financial stability? How significant are these risks?

The risks here are potential not actual, and given the scale of use and rate of growth, unlikely to be relevant at a systemic level for a significant period of time.