Digital Currencies – Call for information
Banking and Credit Team
Floor 1, Red
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

3 December 2014

Dear Sir/Madam

Digital Currencies: Call for Information

PwC welcomes the opportunity to respond to HM Treasury's call for information, which invites views and evidence on the benefits and risks of digital currencies.

Our responses to the questions posed by HM Treasury primarily refer to Bitcoin and bitcoins. Where appropriate we have made comments relating to digital currencies as a whole, but given the timeframe we do not feel it appropriate to provide specific comments on any other individual digital currency.

With regard to Bitcoin, there are characteristics that give rise to both benefits and risks for different groups of stakeholders. We have outlined these benefits and risks in our detailed responses, which are included in the appendix to this letter. It is important to recognise that Bitcoin has existed for less than a decade and as such the significance of the stated benefits and risks is difficult to ascertain and further benefits and/or risks may emerge over time or become less relevant as usage rates and user types change.

Appropriate regulation will help to legitimise business models, provide the basis for sound operational procedures, stimulate growth and attract investment in the wider infrastructure required to allow digital currencies and the blockchain technology to thrive. Regulation that stifles innovation or which comes with prohibitively high compliance costs must be carefully considered given the nascent state of the industry and infrastructure being built around Bitcoin and other digital currencies.

We believe any regulatory regime (new or existing) should primarily focus on anti-money laundering, consumer protection and data security and will be most effective if coordinated at a global level.

Blockchain technology is also potentially a very significant creation with wide ranging implications across sectors. The true potential of this technology is not yet fully understood but it could extend far beyond digital currencies. The technology has proved remarkably resilient and robust since its inception but, as with all technologies, could be susceptible to issues that we are not currently aware of.

PricewaterhouseCoopers LLP, 1 Embankment Place, London, WC2N 6RH
T: +44 (0) 20 7583 5000, F: +44 (0) 20 7212 4652, www.pwc.co.uk

We hope that our response will be helpful to you and we would be pleased to discuss our comments further either in person or on a call. Please direct all enquiries to Richard Porter and Fergus Lemon.

Yours faithfully

Richard J Porter
Partner
PricewaterhouseCoopers LLP

Appendix 1: HM Treasury questions and detailed responses

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?*

There are a number of benefits associated with Bitcoin, a non-exhaustive list of which has been compiled in the table below along with an indication of how significant we believe each benefit to be and which groups of stakeholders they affect. Some of these benefits may also pose risks, please see our responses to questions 6 and 9 for further detail.

It is important to recognise that Bitcoin has existed for less than a decade and as such the significance of the benefits is difficult to ascertain and further benefits may emerge over time or become less relevant as usage rates and user types change.

Ref.	Characteristic	Benefit	Significance	Group
1	Decentralised – there is no central authority with control over the currency	(a) The currency cannot be manipulated by a central body. Changes to the Bitcoin protocol are made by majority consensus amongst the nodes in the network (b) Individuals cannot be blocked from joining the Bitcoin network (c) Bitcoin wallets cannot be frozen	High	Consumers
2	Peer-to-Peer and divisible up to eight decimal places	(a) Eliminates a number of intermediaries in financial transactions (b) Lowers the cost of transactions by eliminating fees associated with traditional payments (c) Increases privacy for the parties involved in a transaction (d) Makes micro-payments possible / economical	High	Consumers / Businesses / Wider Economy
3	Cryptographically secured	(a) Transactions in bitcoin are individually encrypted using industry standard methods similar to those used for secure banking	High	Consumers / Businesses
4	Digital	(a) Bitcoins can be carried and stored digitally	Medium	Consumers / Businesses /

		(b) Bitcoin wallets can be backed up, reducing the risk of loss, damage and theft of devices upon which wallets are stored (c) No associated costs of dealing with physical currency		Government / Wider Economy
5	Scarce – the algorithm that governs Bitcoin stipulates that only 21 million bitcoins will ever exist	(a) Predictable supply of currency (b) Unaffected by artificial stimuli	High	Consumers / Businesses / Government / Wider Economy
6	Publically recorded – all transactions in bitcoin are recorded on a public ledger known as the blockchain	(a) Transparency – any transaction in bitcoin can be seen by any person at any time (b) Security – transaction information can only be manipulated by majority consensus amongst the network (c) Privacy – whilst all transactions are publically recorded, the personal information of parties to the transaction is not recorded or associated with the transaction	High	Consumers / Businesses / Government / Wider Economy
7	Global	(a) Bitcoin, as a currency, is not bound by geographical limitations (b) It provides a quick and cheap means for cross-border money transfers	High	Consumers / Businesses / Governments / Wider economy
8	Pseudo-anonymous	(a) Privacy - whilst all transactions are publically recorded the personal information of parties to the transaction is not recorded or associated with the transaction (b) Lowers the risk of financial fraud related to transactions in bitcoin (c) Lowers the risk of identity theft for consumers (d) Removes the risk of handling customers' personal information locally and globally	Medium	Consumers / Businesses / Wider economy
9	Non-repudiation - once a	(a) Lowers costs for businesses in that there can be no 'chargeback'	Medium	Businesses

	transaction has been verified and recorded in the blockchain it cannot be reversed	requests or fees / fines associated with such requests		
10	Open-source	(a) Allows visibility of the code that underlies Bitcoin (b) Alterations can be made to improve upon the functionality as a method of payment	Medium	Consumers / Businesses / Government / Wider Economy

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?*

Please refer to our responses to questions 3, 10 and 11.

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)?*

We recognise that regulation will play an important role and we believe any regulatory regime (new or existing) should primarily focus on anti-money laundering, consumer protection and data security.

Appropriate regulation will help to legitimise business models, provide the basis for sound operational procedures and stimulate growth and attract investment in the wider infrastructure required to allow digital currencies and the blockchain technology to thrive. Regulation that stifles innovation or which comes with prohibitively high compliance costs must be carefully considered given the nascent state of the industry and infrastructure being built around Bitcoin and other digital currencies.

We consider there to be three fundamental points of consideration before any regulation is implemented:

(1) Classification of digital currencies is required. The content of any regulatory regime will depend on whether digital currencies are classified as currencies, financial instruments, digital commodities or something bespoke. It may be that different types of digital currencies need to be classified differently.

(2) Bitcoin itself should not be regulated. Bitcoin operates across a decentralised peer-to-peer network across geographies; as such regulation of that network would be extremely difficult if not impossible. Furthermore, decentralisation is one of the main tenets of Bitcoin, and other digital currencies based on its software, to attempt to regulate it at this level would likely result in negative sentiment towards HM Treasury from the global Bitcoin community.

(3) Certain digital currency entities should be regulated. A non-exhaustive list of the different categories of entity and the potential for regulation is outlined below:

a. ***Creator***: an individual or entity that creates a digital currency. The Bitcoin software is open-source making it easy and cheap for others to create their own digital currency.

Regulation: given the open-source nature it may be difficult, if not impossible, to implement effective regulation at this level. However, given the potential for fraudulent digital currencies to be created (see response to question 10) some safeguards should be considered to protect consumers. At this point it is unclear what form those safeguards should take.

b. ***Miner***: an individual or entity that participates in a decentralised digital currency network by running special software to execute computationally expensive algorithms in a distributed network used to validate transactions in the digital currency system. At present, significant hardware is required to make mining profitable and as such the majority is now carried out by entities or mining pools.

Regulation: at the individual level we see no need for regulation, at the entity or 'mining pool' level the situation is less clear. These entities and pools play a significant role and other users of digital currencies and digital currency businesses should be afforded some safeguard against potentially malevolent actors. At this point it is unclear what form those safeguards should take.

c. ***Exchange***: an individual or entity engaged in the exchange of digital currency for fiat currency, other digital currency, funds and / or precious metals and vice versa.

Regulation: we believe it is important to bring exchanges under a regulatory regime. These entities could be treated as Money Service Businesses (MSBs), in the UK this would require them to be registered with HMRC or supervised by the Financial Conduct Authority (FCA) and be subject to money laundering regulations.

d. ***Service provider***: an individual or entity that provides services related to digital currencies such as payment processing or cold storage.

Regulation: certain businesses providing digital currency services should be brought under existing regulatory regimes and it may be advisable to create bespoke regulation or guidelines for specific types of entity given some of the unique characteristics and risks associated with digital currencies. Some may be considered MSBs, see the discussion above with regard to regulation for these types of entities. Payment Services Regulations 2009 may also be appropriate. New services and products being developed specifically for digital currencies may require bespoke regulation, an example of such a product / service is 'cold storage' of digital currencies.

e. ***Retailer***: an individual or entity that accepts digital currencies as payment for goods or services, there are more than 200 such businesses in the UK at the date of this response.

   Regulation: we do not believe any action is required beyond what is required for ordinary cash transactions.

Useful lessons may be drawn from experiences in other countries, for example in July 2014 the New York Department of Financial Services (DFS) released a draft of its BitLicense regulatory framework for companies buying, selling or processing bitcoins. It is recommended that HM Treasury review the proposed framework and take note of the feedback it received from industry.

However, individual regimes at a national level may not be the most effective option given the characteristics of Bitcoin, as outlined in our response to question 1. A coordinated global response to classification and regulation, of Bitcoin, other digital currencies and associated entities, is likely to be the most effective. There are several international fora, such as the OECD (tax), the Financial Stability Board (regulation) and the Basel Committee (central banking), which can facilitate the development of international standards.

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

Lack of regulation may inhibit certain businesses – both looking to set up in the UK for the first time and established UK businesses looking to create a new service or product based on digital currencies.

The limitations arise from an uncertain environment and reluctance of established businesses to offer their services to digital currency businesses in the UK, namely banking and assurance services, due to risk management. Appropriate regulation and guidance from the government would have a positive signalling effect.

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

The benefits of the blockchain technology are potentially very significant and could bring about a step change in the way that individuals and organisations interact with each other both online and offline across a range of sectors.

The main benefits appear to be (1) the ability to transfer ownership of a digital asset, in a secure manner, and to prove transfer of that ownership between two parties, without the need for a trusted intermediary and (2) the ability to reach a consensus amongst a decentralised network of individuals.

The opportunity to build on top of this technology may also be one of the major benefits in that it presents a wide range of possibilities across a number of different sectors of the economy. These possibilities have not been fully explored yet but, for example, the ability to build a programming

language on top of the blockchain means it could be used as the basis for much more than digital currencies.

A number of the benefits outlined in our response to question 1 are also directly related to the technology.

It is important to note that these benefits only hold true in a scenario where there are no fatal flaws in the technology, including the cryptography that underlies it. To date, the technology has remained resilient, but that may not always be the case.

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?*

There are a number of risks associated with digital currencies, a non-exhaustive list of which has been compiled in the table below along with an indication of how significant we believe each risk to be and which groups of stakeholders they affect. Some of these risks may also be benefits, please see our response to question 1 for further detail.

It is important to recognise that Bitcoin has existed for less than a decade and as such the significance of the risks is difficult to ascertain and further risks may emerge over time or become less relevant as usage rates and user types change.

Ref.	Characteristic	Risk	Significance & Mitigation
1	Decentralised	(a) No party is liable for any system errors, payment failures or contractual failures of involved parties (b) The risk of loss or theft, by whatever means, lies with the owner (c) Operates outside the traditional financial system, making the network attractive for illegal transactions	Medium Self-policing: it is in the interest of the core developers, miners and users to maintain the network and cooperate to fix known problems in order to protect the value in / derived from the network. Companies can be established and contracted to act as a trusted counterparty to assume transaction or security risk. Demand in the market for such counterparties will be the primary driver, an appropriate regulatory environment for these counterparties will also be important. Regulation and law enforcement (see responses to questions 3 and 10) can reduce these risks.
2	Unregulated	(a) Lack of regulation exposes the network to facilitating illegal	High

		activities such as money-laundering and illegal transactions (b) Restricts growth – without regulation financial institutions and professional service providers are reluctant to offer services to 'digital currency businesses' (c) Increases the risk of adverse impacts on consumers and businesses from poorly run 'bitcoin service providers' (d) Risk of market manipulation on conversion to fiat currencies	Appropriate regulation can mitigate and / or reduce these risks.
3	Cryptographically secured	(a) If the cryptography fails or a flaw exposed the network becomes unsecure and the impact on price will be severe and rapid	We do not have the expertise to comment on the significance or likelihood of this taking place.
4	Non-repudiation	(a) There is no method for reversing or cancelling transactions if they are made in error or are fraudulent	Medium Innovation in the market by third party providers can offer consumers protection by acting as intermediaries.
5	No upper limit to the value of a single transaction	(a) An incorrect and large value could be sent in one transaction accidentally	Low Decreases as users become more accustomed to transacting in bitcoin. Innovation in the market by third party providers can offer consumers protection.
6	Scarce	(a) The limited supply of bitcoins currently programmed in the algorithm means that miners will eventually not be rewarded by the creation of new bitcoins	Low Transaction fees (potentially in bitcoin) will replace bitcoins as the reward / incentive for miners.
7	Pseudo-anonymous	(a) Reduces the potential to trace illegal activity back to an individual (b) Is at odds with the current anti-money laundering (AML) regime of 'Know Your Customer'	Medium Regulation and innovation may reduce or mitigate this risk.
8	Peer-to-peer network with majority consensus	(a) If 51% of the computing power in the bitcoin network is controlled by an individual or a group then fraudulent transactions could occur and ultimately the entire bitcoin network could collapse	High Regulation at the mining level may reduce or mitigate this risk.

9	Bitcoin and related infrastructure are both immature	(a) Services can be attacked, often using well-known hacking methods (b) Adverse financial impact on consumers and businesses due to loss or theft of bitcoin held with external service providers (c) Fraudulent schemes – lack of clarity and guidance around trusted service providers increases the risk of consumers and businesses being defrauded (d) The price, at which bitcoins can be converted into fiat currencies, is extremely volatile	High Regulation and third party providers may reduce or mitigate these risks.

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?*

Our response to question 6 briefly outlines potential mitigating factors for each risk. Mitigation can largely be carried out by the Bitcoin network and entities in the industry. Regulation and law enforcement, as outlined in our responses to 3 and 10, are both areas where the government can intervene effectively.

Question 8: *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?*

Please refer to our responses to question 3, 6, 10 and 11, where a number of these points have been covered.

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?*

In our response to question 6 we noted the risks around money-laundering, illegal transactions and the risk of fraud. These are the three most prominent crime risks at the date of this response but do not represent an exhaustive list of crime risks associated with digital currencies. Furthermore, the significance of these risks will vary across different digital currencies.

Ref.	Crime risk	Significance
1	Money laundering Bitcoin operates outside the regulated financial system making it attractive for those who want to launder money.	Medium / High The risk can be mitigated in most instances via regulation of the service providers operating alongside the

	Transactions in bitcoin are pseudo-anonymous – every transaction is recorded in a public ledger along with the public wallet addresses of the parties to the transaction but no personal information is attached to the transaction. Whilst offering the benefit of privacy it hinders the ability to monitor for, and detect, money laundering and is at odds with current AML regime requirements to identify customers. Bitcoin is also a global digital currency with no restrictions on who can use it.	Bitcoin network.
2	Use in illegal transactions The pseudo-anonymous nature means that it is attractive to those looking to purchase illegal items via online marketplaces. Online market places exist where illegal goods are sold in return for digital currencies (mainly bitcoin). Bitcoin may also be used to finance terrorism.	Medium Regulation and innovation may reduce or mitigate this risk.
3	Fraud Wallets can be hacked and fraudulent transactions made with the purpose of stealing bitcoins. The open-source nature of the majority of digital currencies also means that it is relatively easy to create a new digital currency. Some are created for the purpose of defrauding consumers in a similar manner to a Ponzi scheme.	High Risk of theft is high for those that are uneducated in how to protect themselves adequately. Risk of entirely fraudulent digital currencies being created is also high due to ease of creation, lack of regulation and poor consumer understanding of digital currencies.

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

Please refer to our responses to questions 3 and 6. Furthermore, the role of law enforcement agencies (LEAs) should be considered. Ensuring LEAs have the ability to intervene and recover the mechanism through which value passes is important and recent examples of confiscations / seizures by the Federal Bureau of Investigations (FBI) highlight how intervention is possible.

However, classification of digital currencies will have a substantial impact on the role of LEAs. For example, under the Proceeds of Crime Act 2002 (POCA), it is unlikely that bitcoins can be defined as cash which may impact the ability of police officers to seize bitcoins under the current definitions (see S289 and S316 POCA 2002).

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

The money laundering offences in POCA 2002 (S327, 328 and 329) can be applied, i.e. if the proceeds of a crime were placed into a bitcoin account that account would be the vehicle through which the individual has laundered and would allow LEAs to enforce a confiscation order.

A new regime, if introduced, could be bolted onto the existing money laundering regulations and the money laundering offences in POCA, but specifically dealing with the use and application of digital currencies. Any new regime should be coordinated through the OECD/Council of Europe so that a consistent approach to the regulation and use of digital currencies can be developed. There will remain a possibility of 'treaty shopping' to evade detection if the digital currency systems are not coordinated and regulated through coordinated legislation /directives.

We are not in a position to give an informed response on the impact of FinCEN's decision in the USA on digital currencies.

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

The application of sanctions could drive the use of digital currencies further away from the mainstream and indirectly promote the use of offshore entities and weak jurisdictions. LEAs would in turn find it difficult, if not impossible, to target individuals that are using digital currencies for nefarious purposes.

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

As at the date of this response, risks posed to monetary and financial stability are low. Digital currencies are still in their infancy, the value (in fiat currency) of all digital currencies that have been created to date is still very small on a national or global basis and adoption rates are also still low. At the point where the value and usage of digital currencies become relevant for monetary and financial stability the risks outlined in our response to question 6 will need to be mitigated or reduced to an acceptable level.