HM Treasury

Digital currencies:

response to the call for information

March 2015

HM Treasury

Digital currencies:

response to the call for information

March 2015

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at public.enquiries@hmtreasury.gsi.gov.uk

ISBN 978-1-910337-91-2
PU1773

Contents

1 Introduction

Background to the call for information

1.1 In August 2014, the government announced a major programme of work looking into the benefits and risks associated with digital currencies and underlying technology, with a particular focus on the question of regulation. In November 2014, the government published a call for information to gather views and evidence on these questions. The call for information received over 120 responses. Submissions came from members of the public who use digital currencies, digital currency developers, businesses providing digital currency-related services, banks, payment scheme companies, academics, consultancies and other government departments and agencies.

1.2 This document summarises the submissions received in response to the call for information questions and, in light of the evidence gathered, outlines the government's views and proposed next steps. The government is grateful for all of the contributions made by respondents throughout the call for information process.

Key themes

1.3 As noted in the call for information, there are a number of diverging views on the benefits digital currencies can offer, and the risks they pose. Respondents to the call for information outlined a number of potential benefits that digital currencies could offer to consumers, businesses, charities and the wider economy as a method of payment. At the same time, respondents also noted that, as currently designed, digital currency systems have some inherent flaws which make them volatile and potentially unsuitable for mainstream usage. Other respondents focussed on the risk that digital currencies are an enabler of crime, a matter which is high on the government's agenda.

1.4 The government considers that while there are clear barriers to digital currencies achieving widespread use in their current form, the 'distributed ledger' technology that underpins digital currencies has significant future promise as an innovation in payments technology. The government wishes to foster a supportive environment for the development of legitimate businesses in the digital currency sector so that the UK can see some of the benefits of digital currencies, while also creating a hostile environment for illegal activity. At this early stage, the government's objectives for digital currency technology and the sector more widely are as follows:

- to provide clarity and certainty on the application of existing legislation and regulation for users, businesses and other parties dealing with digital currencies
- to limit any opportunities for criminals or terrorists to use digital currencies for illicit activities, and to support the effective identification and prosecution of illicit activity that does take place
- to create the right environment for legitimate digital currency entrepreneurs to flourish, including supporting the provision of banking and other financial and professional services to legitimate digital currency firms
- to support the research, development and application of new technology, to promote competition and innovation in payment systems, financial services and other relevant sectors
- to support monetary and financial stability in the UK, by monitoring the extent of usage of digital currencies in the UK and regularly assessing the risks posed

Next steps

1.5 The government intends to apply anti-money laundering regulation to digital currency exchanges in the UK, to support innovation and prevent criminal use. The government will formally consult on the proposed regulatory approach early in the next Parliament.

1.6 As part of this consultation on the proposed regulatory approach, the government will look at how to ensure that law enforcement bodies have effective skills, tools and legislation to identify and prosecute criminal activity relating to digital currencies, including the ability to seize and confiscate digital currency funds where transactions are for criminal purposes.

1.7 The government will work with BSI (British Standards Institution) and the digital currency industry to develop voluntary standards for consumer protection.

1.8 The government is launching a new research initiative which will bring together the Research Councils, Alan Turing Institute and Digital Catapult with industry in order to address the research opportunities and challenges for digital currency technology, and will increase research funding in this area by £10 million to support this.

Scope

1.9 The call for information document defined a digital currency scheme as one which incorporates both a decentralised payment system and a related currency. It was noted that digital currency systems can achieve consensus through a variety of means, including proof-of-work and trust-based consensus. The document focused in particular on decentralised digital currency schemes because of interest in the potential benefits of the distributed ledger technology.

1.10 However, the government recognises that other types of digital currency scheme may pose similar types of risks to those associated with decentralised schemes. For this reason, in principle, the scope of proposals on the regulation of digital currencies should be read as inclusive of convertible centralised currencies that are run and administrated by a central entity. The government will look to develop a suitable definition as it brings forward proposals for regulation of the digital currencies sector.

2 Benefits of digital currencies

2.1 This chapter looks at the benefits of digital currencies as a payment method, and the potential for innovative applications of the technology across financial services and beyond. This chapter also considers the barriers to digital currency firms setting up in the UK, and what steps the government could take to support the sector.

Benefits of digital currencies

2.2 Responses from all stakeholder groups identified potential benefits offered by digital currencies as a payment method, noting positive impacts for consumers, retailers, charities, the government and the wider economy. In particular, respondents commented on the potential for cheaper and faster payments. Respondents described how decentralised digital currencies can provide a more efficient infrastructure for the transfer of money, by removing the need for traditional intermediaries (such as banks or payment scheme companies) to oversee the process and verify that the transaction is genuine.

2.3 Stakeholders provided various data quantifying the cost benefits offered by digital currencies. Some responses noted that transactions can be zero-cost, because the payer can choose whether to offer a fee to incentivise miners to process their transaction more quickly.[1] Contributors also reported that fees are fixed, regardless of transaction size. On the amount of transaction fees, when applied, respondents suggested that these could offer some advantage over conventional payment methods, although a range of different figures was put forward.[2]

2.4 A number of submissions discussed the opportunities for new classes of payment which have not been economical with existing payment systems. Many responses explained that lower transaction fees could make it possible for businesses to monetise very low cost goods and services and accept micro-payments (e.g. downloading music or purchasing individual newspaper articles online). Respondents also outlined other forms of micro-transactions, such as internet tipping, charitable giving and micro-payrolls (e.g. employees receiving salaries on an hourly, daily or weekly, rather than monthly, basis).

2.5 In addition to reducing the costs involved in moving money around the economy, respondents, on the whole, agreed that digital currencies can speed up transaction processing times.[3] Academics, consultancies, digital currency users and digital currency firms observed that existing inter-bank payment systems and debit and credit cards can take several hours, if not days, to move money between accounts. It was also noted that conventional payment services may only be available during banking hours, whereas digital currency transactions are processed 24 hours a day.

[1] 'Miners' are users in digital currency networks who gather together blocks of transactions and compete to verify them. In return for this service, miners that successfully verify a block of transactions receive both an allocation of newly created currency and any transaction fees offered by parties to the transactions under question. For more information, see the Bank of England's paper, *Innovations in payment technologies and the emergence of digital currencies* (September 2014).

[2] The following figures were put forward as to the typical cost of a digital currency transaction: for Bitcoin, 0.0005 of a Bitcoin; 0.0001 of a Bitcoin; 0.04 USD; 0.06 USD; 0.03 GBP; 0.002 GBP (i.e. a fifth of 1 penny); and for Ripple, 0.12 USD for Ripple. It was also suggested that fees in effect averaged between 1% and 3% of transaction values. By comparison, respondents noted that merchants taking card payment incur interchange fees and costs relating to fraud management and chargebacks. One submission indicated this may amount to between 2% and 4% of total payment received; another suggested accepting debit card payments on average costs 0.09 GBP, and credit card payments on average 0.37 GBP, with small merchants invariably paying more than larger retailers.

[3] Submissions reported that Bitcoin transactions take, on average, 10 minutes to complete, Litecoin approximately 2 and half minutes, Dogecoin approximately 1 minute, and Ripple, 3 to 6 seconds.

2.6 Many respondents agreed that the cost and time advantages of digital currencies are most notable in the context of cross-border transactions. It was noted that remitting money abroad can currently involve fees of around 8% of the total payment amount, and settlement can take several days. Responses from banks, consultancies, academics and the digital currency sector highlighted the opportunities for cross-border trade and exports, particularly for small businesses currently impeded by the costs and delays involved in taking payments from customers in other countries. It was also suggested that the global reach of digital currency networks could allow small and medium banks to provide international payments, without having to present large amounts of capital through the correspondent banking system. The government notes the European Central Bank's recent report, which states that the technology associated with digital currencies presents a potentially attractive option for both domestic and international remittances.[4]

2.7 While most submissions acknowledged the potential for cheaper and faster payments, some drew different conclusions about the overall significance of these advantages compared with existing payment options. A number of contributions from the banking and payments sector concluded that, on balance, the cost and time advantages are limited or negligible. For example, it was noted that many customers in the UK can already transfer money in near real-time using Faster Payments. Submissions also raised questions about the sustainability of low fees for digital currency payments. For example, respondents predicted that, if digital currency firms are brought into regulation, compliance costs may result in higher fees. Another issue raised was an anticipated rise in fees in the long-run, once currencies with a fixed supply reach the upper limit on the release of new units.[5]

2.8 Responses to the call for information referred to a number of other potential benefits of digital currency systems, including the features of privacy, security and transparency. On privacy, a range of submissions noted that digital currencies provide 'push' rather than 'pull' payments, meaning that a payer does not need to disclose any of their own personal information to the individual or organisation they wish to pay. Various respondents observed that this could have benefits for merchants, who currently incur costs and risks associated with securing sensitive customer payment data.

2.9 On the security of transactions made using digital currencies, submissions highlighted the use of cryptographic algorithms as a way of securely transferring funds over the internet and preventing the possibility of forged payments or double-spending of digital currency units. Respondents also set out the resilience advantages that come from having a decentralised, distributed network of miners verifying digital currency transactions. Responses said this would mitigate the risk of a single entity being able to manipulate transactions, and the risk of a single point of failure that could bring the system down. However, a number of responses highlighted the theoretical threat of a '51% attack',[6] and one payment scheme company anticipated mining pools will, in the long-run, consolidate to achieve economies of scale, creating a risk of system-wide fraud, and representing the re-centralisation of transaction processing.

2.10 Responses also explained that while digital currencies offer greater privacy in some respects, at the same time they also create greater transparency, because all transactions are published on the public ledger or 'blockchain', and this is maintained by the entire network and cannot be manipulated by any single entity. Some consultancies and digital currency firms also

[4] European Central Bank, *Virtual currency schemes: a further analysis* (February 2015).

[5] Low transaction fees for digital currency payments are largely driven by a subsidy that is paid to transaction verifiers (miners) in the form of new currency. The eventual supply of digital currencies is typically fixed, however, so that in the long run it will not be possible to sustain a subsidy to miners. For more information, see the Bank of England's paper, *The economics of digital currencies* (September 2014).

[6] If an individual or pool of miners were to control a sustained majority of the computing power in a digital currency, that group would be able to control which payments were permitted or even to create fraudulent "double spend" payments: a '51% attack'. Some loosely co-ordinated pools of miners have, on occasion, represented a majority of computing power in the Bitcoin network.

commented on the open-source nature of digital currency protocols, which provides for continuous innovation and improvement, as the community of users can scrutinise the code for flaws and, if there is majority consensus, address problems over time.

2.11 A wide range of submissions commented on the accessibility of digital currency networks, and therefore the potential for the technology to provide payment and other financial services to the unbanked or under-banked in society. Most respondents determined that the opportunities to widen access would be greatest outside the UK, for example, in countries lacking an establishing banking infrastructure and with large proportions of the population unable to access a bank account. However, some respondents observed that there were also prospects for digital currencies to improve financial inclusion in the UK.

2.12 Respondents also discussed the potential positive implications for growth and the wider economy. Some calculated the aggregate benefits of transaction efficiencies.[7] One digital currency developer mentioned the cash-flow benefits for businesses of faster settlement, which would allow corporate capital to be put to more productive use than at present. A range of different types of stakeholder perceived that, as an innovation disrupting existing payments models, digital currency technology may increase competition in payments and banking services and incentivise incumbent players to improve their proposition for customers. Various digital currency users, businesses, banks, consultancies and academics also commented on the benefits for UK plc of the growth in the ecosystem around the technology, not least, of new types of business setting up operations here, creating jobs and generating tax revenues.

2.13 On balance, a broad range of respondents concluded that digital currencies represent an innovation in payments technology with future promise. Some respondents said its significance was analogous to that of the internet: the potential for digital currency technology to transform systems of value exchange was compared with the internet protocol and the way it has revolutionised the transfer of information. One bank drew parallels between potential advances using digital currency technology and previous steps to increase the functionality of money, such as the introduction of watermarks, holograms and plastic banknotes.

Benefits of the underlying technology

2.14 Digital currency developers and firms, banks, academics and consultancies provided the most thorough answers on the significance of the distributed ledger technology that underpins many digital currency systems. Respondents broadly characterised the importance of the technology as an innovation facilitating the fast, efficient, and secure transfer of ownership of a digital asset over the internet, providing a permanent record of what has taken place, and without the need for a third party to oversee the process.

2.15 Submissions suggested a variety of possible applications for this technology beyond retail payment services. Responses from a variety of stakeholder groups saw the potential for the technology to be used in financial services more widely, for example, for recording and transferring the ownership of bonds, shares, securities and other financial instruments. Digital currency users, firms, academics and consultancies proposed that the technology could be applied in many other contexts, where records need regularly updating and require authentication or proof of identity. Responses said that the function of digitally 'signing' and time-stamping digital assets could be used to efficiently and securely maintain records of digital

[7] One consultancy estimated card payments currently cost UK merchants between 2 and 3 billion pounds per annum; another consultancy cited hypothetical savings of $200 billion worldwide based on the adoption of Bitcoin.

documents, for both private and public record keeping, for example for passports, driving licences, criminal records, land registry and digital voting.

2.16 A further application, mentioned by a range of respondents, was the use of digital currency technology for 'smart contracts'.[8] Stakeholders characterised digital currencies as 'programmable money', or money with "in-built functionality", enabling users to encode requirements into a payment instruction in order to achieve autonomous, self-executing contracts. Contributors said the technology could be used for more efficient property transfers, or for loan repayments, where payment could automatically take place or be adjusted once specified conditions are met.

2.17 Respondents also described a number of other examples of use for the technology, including decentralised data storage solutions (using blockchain technology to store files securely and efficiently), encrypted peer-to-peer messaging networks and links with 'smart property' and the Internet of Things. For example, 1 respondent mentioned a major technology company's proposals to use blockchain technology to develop smart devices (such as internet-enabled domestic appliances) which can communicate with each other and maintain and update themselves semi-autonomously. Another respondent suggested the technology could have similar uses in the context of semi-autonomous driverless cars.

Barriers to digital currency firms

2.18 Two factors in particular were highlighted as the main challenges faced by digital currency businesses setting up in the UK, and many respondents saw these issues as inter-connected. Most stakeholders mentioned the lack of a regulatory framework for digital currencies, commenting that this has caused some uncertainty for businesses and has made it difficult for the industry to prove its credibility and legitimacy. The second theme that emerged in responses was that digital currency firms have encountered difficulties in opening bank accounts in the UK. Many businesses described how they have been forced to open bank accounts overseas, which results in day-to-day business being slower and drives up costs.

2.19 Submissions from the banking sector highlighted a lack of regulation as a key reason for hesitation amongst banks to take on digital currency firms as customers, and many digital currency firms also discussed the issue of access to banking as closely related to the question of regulation. However, some contributions also suggested that banks have made little effort to assess the real risks posed by firms on a case-by-case basis, and a small number observed that digital currency and other financial technology start-ups represent a potential competitive threat to incumbent financial institutions and to established business models for payment systems.

2.20 As to other challenges faced by the sector, respondents also commented on the general constraints to mainstream adoption of digital currencies, including the fact that the technology may be unfamiliar or complicated to use, price volatility, and the lack of consumer protection rights compared with conventional payment systems. These issues are covered in more detail in the discussion of risks to users in chapter 3.

2.21 While responses identified a number of issues affecting the sector at present, submissions also commented on the conditions that make the UK an attractive and supportive environment for digital currency start-ups. Digital currency firms viewed the UK to be favourable location as a result of its existing position as a global hub for financial services. Submissions also drew contrasts with other countries that have, in their view, taken overly-restrictive action in relation

[8] 'Smart contracts' involve greater automation of the processes of creating, monitoring and enforcing contracts. This may be intended to increase efficiency and reduce the risk of human error.

to digital currencies, or even sought to prohibit use altogether. In addition, many responses welcomed the steps taken by the government in 2014 to clarify the tax treatment of digital currencies,[9] and urged the UK to use its influence to ensure that the same treatment is applied across the rest of the EU.

Options for intervention to support the digital currencies sector

2.22 On the question of what steps the government could take to support the industry, many responses focused on the question of bringing the sector into regulation. The different possible rationales and options for regulation are discussed in more detail in the next chapter. Nearly 80 responses considered the question of whether the government should introduce regulation of any kind; over 80% of these contributions said that the sector should be brought into some form of regulation, with the other answers arguing the government should not regulate, or not at this time.

2.23 Aside from regulation, several other actions were suggested to support the development and usage of digital currencies and related businesses. Over 20 responses mentioned that guidance and education would help to improve awareness and understanding and develop skills relevant to the technology. In addition, a consultancy, several banks and payment scheme companies, digital currency businesses and another government department suggested that a positive step would be for the government to make direct use of digital currency technology, and raised the possibility of banks or the Bank of England integrating digital currency technology into existing payment systems and state-issued currencies, including the option of the Bank of England issuing 'digital sterling'.

Government response

2.24 The government considers that digital currencies represent an interesting development in payments technology, with distributed, peer-to-peer networks and the use of cryptographic techniques making possible the efficient and secure transfer of digital currency funds between users. The government notes that the potential advantages are clearest for purposes such as micro-payments and cross-border transactions.

2.25 Beyond retail payment services, the government considers there are opportunities to explore a number of different applications for the distributed ledger technology that underpins digital currency systems, in retail payments, financial services and beyond.

2.26 However, while the technology offers considerable potential, digital currencies have so far been adopted by a relatively small number of consumers and retailers around the world, and both the technology, and the industry that has grown up around it, are still in a nascent state. The evidence suggests that market in which digital currency firms are operating is not functioning as well as it could, and there is a good case for proportionate regulation at this time, to provide a supportive environment for legitimate digital currency users and businesses. The government's proposed next steps are set out in chapter 4.

[9] In March 2014, HM Revenue & Customs published its position on the tax treatment of income received from, and charges made in connection with, activities involving digital currencies, specifically for VAT, Corporation Tax, Income Tax and Capital Gains Tax. The full brief can be found here: www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies.

3 Risks of digital currencies

3.1 This chapter summarises the potential risks presented by digital currencies in relation to crime, consumer detriment and monetary and financial stability. This chapter also discusses the options for regulatory and non-regulatory steps the government could take to mitigate these risks.

Crime risks

3.2 In October 2014, the National Crime Agency (NCA) assessed the nature and scale of the threat posed by digital currencies, and concluded that the predominant criminal use of such currencies was on online marketplaces for the sale and purchase of illicit goods and services. The NCA commented that digital currencies had not been widely adopted as a means of payment for goods and services in the broader criminal community. It noted that the scale of the threat was difficult to assess, but said that there was little evidence to indicate use by established money laundering specialists or that digital currencies played a role in terrorist financing. The NCA also judged that the majority of illicit digital currency spends were for low-value transactions.

3.3 Almost all respondents to the call for information commented that digital currencies can offer a degree of anonymity to users, and that this factor could be a driver of criminal activity. Contributions also noted that the use of specific digital currencies, and anonymising services can increase the degree of user anonymity. However, stakeholders diverged in their assessment of the overall significance of the risks here. Some banks and payment scheme companies characterised digital currencies as anonymous and untraceable, but many of the submissions from users, digital currency firms and consultancies challenged this view and termed the technology 'pseudonymous' rather than anonymous. They noted that the publically visible ledger (or blockchain) of historical transactions makes digital currency payments less opaque than traditional payment methods, especially cash. Stakeholders saw that this ledger of historical transactions could potentially prove helpful for regulators and law enforcement.

3.4 Other risks drivers identified were features that may attract illegitimate and legitimate users alike, including lower costs, faster settlement times, and the ease of transferring funds across borders. Beyond the intrinsic properties of digital currency networks that might encourage illicit actors, responses also discussed relevant external conditions. In particular, submissions noted the unregulated status of third party intermediaries dealing with digital currencies and the challenge of global co-ordination on a future regulatory approach.

3.5 Stakeholders also outlined a number of potential criminal activities that could take place involving digital currencies. Contributions referred to specific examples where digital currencies have been in evidence as a payment vehicle, such as the buying and selling of illicit goods and services via online marketplaces (e.g. the Silk Road), and cases where computers have been infected with 'ransomware' and criminals have demanded payment in digital currency.[1] In addition, there were a number of other illicit activities mentioned where respondents considered there to be potential for digital currencies to be used, although they did not provide evidence on whether, or to what extent, this might be taking place. Submissions mentioned money laundering, terrorist financing, tax evasion and sanctions evasion as possible or likely activities facilitated by the distinctive features of digital currencies.

1 'Ransomware' is a type of malware which restricts access to the computer system that it infects, and demands a ransom be paid in order for the restriction to be removed.

3.6 Some responses also identified factors that may, at present, deter the use of digital currencies by illicit actors. As well as the transparency and visibility of transactions discussed in chapter 2, submissions highlighted conditions such as price volatility, the need for some technical familiarity or expertise, the relatively small number of individuals and businesses accepting digital currencies as payment for goods and services, low numbers of total transactions and low levels of liquidity in digital currency systems. For such reasons it was suggested that, for example, serious organised money launderers may favour conventional payment methods instead.

Financial sanctions

3.7 Most respondents saw that digital currencies could create a considerable challenge for the enforcement of financial sanctions, highlighting the degree of anonymity, the ability to make payments across borders without going through intermediaries, and the fact that there may be no third party authorities with the ability to freeze or reverse digital currency payments. Several submissions suggested practical ways of addressing these issues (for example, if, through regulation, digital currency wallets were matched with real-world identities), but it was also acknowledged that users could easily create multiple new addresses, transfer funds without going through third party wallet providers, and use anonymising services to further disguise transaction flows.

Options for intervention to mitigate crime risks

3.8 There was strong support across stakeholders for government intervention to address the risk of criminal use and to help legitimate users and businesses. Three quarters of those who answered this question favoured regulation to address the issue of anonymous use, and most focused on the need for 'know your customer' requirements be applied to digital currency intermediaries. The majority of digital currency firms, consultancies and academics called for such regulation, and they also emphasised that regulatory requirements must be proportionate to the risk posed, to avoid unnecessarily stifling competition and innovation in a nascent industry. Most banks and payment scheme companies also recommended regulation, and highlighted the need for clear guidance on their obligations under anti-money laundering and counter terrorist financing rules.

3.9 On the question of how regulation could be implemented, respondents on the whole favoured acting using existing frameworks in the short-term, for reasons of timeliness and also as some expected that creating a bespoke regime would result in higher compliance costs for firms. Some of these answers indicated existing rules should be leveraged, but might need to be tailored to fit the digital currency sector. Several responses noted that, in principle, an ideal solution would be a new regime, designed to address the distinctive nature of digital currencies, but most concluded that the government should leverage existing regulation to address the most pressing risks in the short-term. One contribution also commented that it would be premature to draw up a bespoke regime given digital currencies are still in a very early stage of development and it is difficult to predict what direction the technology might go in.

3.10 Many responses commented on the desirability of European or global co-ordination and a consistent international regulatory framework. Responses thought that this would increase the effectiveness of law enforcement efforts, given the internet-based, borderless nature of digital currency networks. In addition, for digital currency firms that seek to expand and operate in multiple jurisdictions, consistency in requirements would reduce the cost and complexity of compliance. A variety of ideas were put forward as to how to achieve a coherent international framework, including using existing EU institutions and legislation (e.g. the Anti-Money

Laundering Directive), the Organisation for Economic Co-operation and Development (OECD) and the international Financial Action Task Force (FATF).

3.11 Some submissions discussed the scope of the regulatory perimeter, mentioning specific market participants who they thought should be subject to regulatory requirements. The most common response was that exchange businesses should be the focus of regulation, as 'gateways' or the 'entry' and 'exit' points to and from a digital currency system. A small number of responses discussed the regulation of digital currency ATMs specifically.[2] Some responses also suggested including wallet providers within the scope of regulation, which would provide greater visibility of transactions inside digital currency systems. The remaining submissions were even broader in their replies, suggesting all institutions handling or dealing with digital currencies should be captured by regulation.

3.12 Of the responses opposed to regulation to address crime risks, a small number of users and digital currency firms emphasised the libertarian origins of private digital currencies, which were first created to avoid central authorities, and therefore argued that governments should not interfere in any way. Other submissions objected on the basis of timing rather than principle, regarding it as premature to regulate at this time and raising concerns about the risk of heavy-handed regulation creating barriers to entry and inhibiting innovation.

3.13 As to non-regulatory interventions to mitigate crime risks, the main recommendation was that the government should train law enforcement personnel and develop existing law enforcement techniques. Several users and digital currency firms suggested using trade bodies or other sources of expertise to improve understanding and awareness amongst police and intelligence agencies. Other recommendations included setting up a designated task force and monitoring and analysing the blockchain to identify and trace suspicious transactions. There was 1 proposal, from a payments infrastructure provider, that the government consider banning digital currencies, should it decide the risks outweigh the benefits. All other stakeholders addressing this option concluded it would drive market participants underground, reduce visibility of transactions and encourage the appropriation of the technology by criminals instead of legitimate users.

3.14 The call for information also asked for views on the impact of the Financial Crimes Enforcement Network (FinCEN) in the USA, where anti-money laundering regulations have been applied to administrators and exchangers of digital currencies. On the whole, responses from digital currency firms (including a number which operate and are regulated in the US) were positive, reporting that regulation has increased the legitimacy of digital currency firms, helped firms establish banking partnerships and investment, and deterred criminals. Despite this, however, various stakeholders also commented that there is a lack of clarity about which categories of business activity are captured by the FinCEN requirements, and some said that the process of registering in multiple American states has been burdensome and has forced smaller firms to exit the market.

3.15 A number of submissions also commented on the proposed 'BitLicense' framework that has been put forward by the New York Department of Financial Services. Digital currency firms answering on this agreed that the proposed BitLicense regime, at least as initially drafted, would be too wide in scope and would impose very high compliance costs on digital currency firms and risk damaging the sector.

[2] Digital currency ATMs allow users to deposit fiat currency (e.g. sterling) and receive digital currencies to their digital currency wallet, or to deposit digital currencies to the ATM operator's wallet (via the ATM) and receive fiat currency (e.g. sterling).

Government response

3.16 The evidence available indicates that digital currencies have been used by illicit actors, but the information does not suggest that digital currencies have, at present, been widely adopted as a payment vehicle in the wider criminal community. The government notes that the degree of anonymity and the ease of making payment are key drivers of potential criminal use; and that anonymous use of digital currencies is closely linked to the absence of an effective 'know your customer' regime being in place.

3.17 The government recognises the broad support for proportionate, but robust, anti-money laundering regulation in order to limit the abuse of digital currencies by criminals or terrorists, and to support development and innovation in the sector. The government's proposed next steps to mitigate the risk of criminal use are set out in chapter 4.

Risks to users

3.18 As discussed in chapter 2, respondents explained that digital currencies draw on cryptographic techniques to offer a secure way of transferring value between users across the digital currency network. However, contributors also saw that there could be security issues for users at various points where they are obtaining, holding or transferring digital currency funds.

3.19 Nearly every response to this question highlighted the risk of price fluctuations users have experienced with digital currencies that are not backed by any authority or pegged to any other currency or commodity. However, many respondents noted that digital currencies have only been in existence since 2009, and predicted that exchange rates will stabilise as digital currencies mature and adoption increases.

3.20 In the case of decentralised digital currencies, stakeholders commented on the absence of an overarching authority with control over transactions (e.g. with the power to reverse erroneous or fraudulent payments) and therefore the irrevocable nature of digital currency payments. Some submissions speculated about the chances of an unknown future system glitch or collapse, or the theoretical possibility of a 51% attack if a pool of miners gained sufficient computing power. It was noted that such risks may be reduced in the case of centralised schemes.

3.21 Respondents observed that digital currencies can empower users with greater freedom and personal control over their own money, but this can in turn place greater responsibility on individuals to protect their funds, and there may not be recourse to a bank, payment scheme company or regulator if something goes wrong. Submissions cited examples where users have forgotten or misplaced their payment credentials, or hackers have compromised their device and gained access to their digital currency funds.

3.22 Respondents also described cases of detriment in situations where third party digital currency firms have been entrusted with users' funds. Stakeholders reported that exchanges and wallet providers have been hacked, have carried out deliberate fraud against customers, or have become insolvent, with no recourse for users who have lost funds as a result (e.g. Mt. Gox). Respondents also mentioned 'pump and dump' scams relating to new digital currencies. Contributing factors mentioned included the non-face-to-face nature of transactions, the anonymity of actors in such situations, the fact that firms are not registered with any authority, and lack of clarity over the application of existing consumer or buyer protection rights.

3.23 A number of responses from the digital currency sector, as well as consultancies, academics, banks and payment schemes, said that the market has been able to address some of

the risks to users. They mentioned creative new technological solutions, such as multi-signature authentication, escrow accounting and 'cold storage' used digital currency firms.[3]

Options for intervention to mitigate risks to users

3.24 Where there was strong backing for the government to regulate to address crime risks, responses on policy interventions for consumer protection were more mixed. Just over half of those who answered this question called for some form of government intervention, such as regulation or consumer rights to apply to the digital currency sector. Just under half of those who answered this question did not think the government should regulate specifically for consumer protection; but many of these respondents called for a framework for consumer protection to be developed, with voluntary rather than compulsory compliance with best practice standards.

3.25 Of the responses opting for a regulatory response to user risks (comprising digital currency firms, banks, payment companies and some academics and consultancies), not all necessarily advocated a full consumer protection regime equivalent to the regulation that currently covers financial or payment institutions. Several responses simply stated that existing consumer protection rights should apply (e.g. the Consumer Protection Act 1987). Others said merchants accepting payment in digital currency, and service providers such as wallet providers, should be required to provide clear policies up-front on what protections and dispute resolution procedures are available.

3.26 However, some of these submissions did suggest importing or adapting a full regime for consumer protection regulation. Contributors mentioned a number of possible requirements that could be applied to registered or licensed digital currency firms, including the following:

- technical standards for safe storage of digital currency funds (such as multi-signature authentication and cold storage)
- cyber security or IT standards
- prudential requirements
- conduct requirements
- a deposit guarantee scheme, along the lines of the government's Financial Services Compensation Scheme (FSCS)

3.27 As to how the government could regulate for consumer protection, many respondents proposed regulating using an existing framework, and mentioned the following options for doing so: the Payment Services Directive; the E-Money Directive; the Market in Financial Instruments Directive. These regulations are currently enforced by the Financial Conduct Authority; in addition, a small number of submissions suggested the Payment Systems Regulator and the Financial Ombudsman Service could have a role.

3.28 Various stakeholders recommended introducing consumer protection regulation domestically, rather than internationally, mainly because this would allow for action in the near-term. Others favoured taking action at an EU or international level, noting that the borderless

[3] A 'multi-signature' address needs two (or more) different keys on different machines for the transaction to work, and therefore means no one person can authorise the transfer of funds, making it more difficult for someone to steal units of digital currency from that address. It may also be useful for organisations or groups that would like a majority vote to confirm the transaction, meaning all shareholders can have a key and the funds are only used when there is an agreed majority. An 'escrow' service can allow for safer payments between individuals, using a neutral third party that holds the units of digital currency until the buyer confirms they have successfully receive the good/service; the third party will then release the units to the intended recipient on authority of the buyer. 'Cold storage' entails storing units of digital currency in an offline mode rather than online ('hot storage'), to reduce the risk of remote hacking.

nature of digital currencies makes an international framework more appropriate and would give greater consistency for firms operating in more than 1 country.

3.29 Where respondents referred to specific market participants that should be within the scope of consumer protection regulation, most focused on businesses that have custody and control of users' funds, which could include wallets and exchanges. One consultancy put forward the idea of regulating miners, given their key role in the issuing of new units of currency and to address the risk of a 51% attack on the network.

3.30 Just under half of those responding to this question (comprising digital currency users, firms, academics and consultancies) did not think there was a case for consumer protection regulation at this time. Some noted that the total scale of use of digital currencies is still very small, and several commented that the market has been able to address some of the risks to users, for example, with creative new technological solutions such as those outlined in paragraph 3.23. Contributors thought that prescriptive regulation could inhibit the market from responding flexibly with new technology and products to solve security problems.

3.31 It was also acknowledged that it may be too early for the government to intervene in an effective way to protect consumers, given the need to fully understand the new types of potential detriment posed to consumers, and the risk that these would not be comprehensively addressed by existing regulatory frameworks. However, respondents also commented that the risk of taking no action at all would be that consumers are unable to trust digital currency firms and this could be more damaging to the sector's growth than any other factor.

3.32 Various digital currency businesses, including a trade body for the sector, as well as users, a university and a payments trade body, suggested that the best way of addressing the risks to users and improving the reputation of the sector would be a middle-way, of self-regulation. These submissions supported a model where the industry could develop best practice and apply these standards with a formal accreditation scheme. Respondents suggested this would allow the market to signal clearly to users which businesses offer greater security, without imposing expensive compliance costs on small start-ups trying to enter the market.

3.33 As with responses on the question of interventions to address crime risks, stakeholders urged the government to take a risk-based approach and act in a proportionate manner, to avoid unnecessarily stifling innovation or driving the technology underground. In addition, a wide range of responses noted that more education or guidance for users is need, either instead of or in addition to regulation.

Government response

3.34 The government notes that there are a number of potentially significant risks for those using digital currencies at present, and recognises the need for action to improve standards and offer greater clarity to users about which services are safe to use, but without unnecessarily stifling innovation and development. The government's proposed next steps to mitigate the risk of consumer detriment are set out in chapter 4.

3.35 Steps that make digital currencies safer to use may, as a result of greater stability and increased transaction volumes, make those currencies more attractive to criminals as well as to legitimate users. The government therefore notes that implementing effective anti-money laundering regulation, and ensuring that law enforcement bodies have effective skills, tools and legislation to identify and prosecute criminal activity relating to digital currencies, will help mitigate changing crime risks.

Monetary and financial stability

3.36 On balance, respondents concluded that digital currencies currently pose very low risks to monetary and financial stability. Stakeholders considered the very low volumes of digital currencies circulating at present, with even the most popular currencies representing a very small proportion of total transaction volumes in the UK and globally. Some also discussed the obstacles to digital currencies (at least in their present form) reaching mainstream acceptance and becoming a serious rival to stable national currencies. These conclusions were generally in line with the Bank of England's assessment in September 2014, which stated that digital currencies do not pose a material risk to stability in the UK.

3.37 A small number of digital currency users and businesses took the view that digital currencies could offer greater stability than the current monetary system. For example, on the basis that some digital currencies have a pre-determined growth path for supply, submissions said this could offer an element of predictability that would also prevent inflation. (This was despite other comments on the price volatility and deflationary tendencies of such digital currencies.) Some of these responses made these comments as part of a broader critique of the current position and activities of central banks, for example, in relation to quantitative easing.

3.38 A number of respondents recommended that the government should monitor the sector closely and reassess at regular intervals whether the risk has changed. In the event that digital currencies did become sufficiently widespread, respondents noted that the risks could be highly significant in impact. If digital currency usage grew considerably this could limit the effectiveness of monetary policy tools, for example, central bank policies and objectives relating to money supply and inflation in the economy. Respondents also argued that the fixed supply of digital currencies would also likely result in deflation, and as a consequence, economic depression. If used on a wide enough scale, digital currencies could also limit the ability of governments to respond to financial crises. For example, in the event that capital controls were needed, these could potentially be circumvented. Responses also said that, if an unforeseen flaw in a digital currency network emerged, there could be significant fluctuation in values and instability across markets.

3.39 As set out in the previous chapter, a number of responses raised the possibility of the government or the Bank of England integrating digital currency technology into fiat payment systems, including the option of the Bank of England issuing a fiat digital currency or 'digital sterling'.

Government response

3.40 The government agrees with the majority of respondents, and the assessment of the Bank of England, that the risks to monetary and financial stability are currently low in the UK. The Bank of England continues to monitor developments in this area.

4 Conclusion and next steps

4.1 The government is committed to increasing banking competition in the interests of all customers. Encouraging greater innovation in payments, which provide the plumbing for the banking sector, is central to this. The government intends to create a world-leading environment for the development of innovative payments and financial technology. At Budget 2015, the government is announcing a package of measures to address key crime and consumer protection risks associated with digital currencies. These measures are intended create the right environment for legitimate actors to flourish, and to create a hostile environment for illicit users of digital currencies.

4.2 The government notes that the distinctive features of digital currencies can be attractive to illegal users as well as people and businesses who like to use digital currencies for legitimate purposes. **In response, the government intends to apply anti-money laundering regulation to digital currency exchanges, to support innovation and prevent criminal use.** The government is committing to a full consultation on the proposed regulatory approach early in the next Parliament. The consultation will seek views and evidence on key questions including how anti-money laundering regulation should be applied to the digital currencies sector, the scope of the regulatory perimeter and the identity of the regulator.

4.3 **As part of the consultation on the proposed regulatory approach, the government will look at how to ensure that law enforcement bodies have effective skills, tools and legislation to identify and prosecute criminal activity relating to digital currencies, including the ability to seize and confiscate digital currency funds where transactions are for criminal purposes.**

4.4 The Financial Action Task Force (FATF) has noted the legitimate uses of digital currencies, and identified characteristics of digital currencies that present potential anti-money laundering and counter-terrorist financing risks. **The FATF has said that it wants to progress on its initial report for a decision at the June 2015 Plenary. The UK will continue to feed into the FATF process.**

4.5 The government notes the nascent state of the technology and the surrounding industry, and recognises that users of digital currencies are potentially exposed to a number of risks. **In response, the government considers that a framework for best practice standards for consumer protection is the right step to take at this stage, in order to address the risks identified but without imposing a disproportionate regulatory burden on the industry. The government intends to work with BSI (British Standards Institution) and the digital currency industry to develop pioneering voluntary standards for consumer protection.**

4.6 The government considers that digital currencies, when used legitimately, offer an innovative, alternative payment option, which competes with existing payment models and has particularly clear short-term advantages for micro-payments, overseas remittances and cross-border trade.

4.7 The government recognises that the technology associated with digital currencies offers considerable promise, making it possible for users to transfer value (or other information) quickly, efficiently and securely, providing a permanent record of what has taken place, and without the need for a trusted third party to oversee the process. **In response, the government is launching a new research initiative which will bring together the Research Councils, Alan Turing Institute and Digital Catapult with industry in order to address the research opportunities and challenges for digital currency technology, and will increase research funding in this area by £10 million to support this.**

4.8 In addition, in February 2015, the Bank of England announced it will undertake research on central bank-issued digital currencies as part of its new research agenda. This work covers the potential costs and benefits of doing so as well as the economic impact, technological requirements and necessary regulations for a central bank-run system.

A List of respondents

A.1 The following organisations submitted responses to the call for information:

Accenture

Altana Wealth

ATM Industry Association

Azteco

Bitcoin Magazine

Bitcoin Manchester

Bitcoin Technology Ltd

Bitnet

BitPay

BitReserve

Bristol Pound

British Bankers' Association/Payments Council (joint submission)

Calibrated Markets LLC

CFA Institute

Children's Charities' Coalition on Internet Safety

Chiralkine

Circle

Citi

COEPTIS

The Coin Company/Future Finance Group

Coinbase

CoinCut

Coinduit

Coinerz

Coinfloor

CoinJar

Coinoshi

Coinstructors

CryptoCoinComparison

Deloitte

Digital Currencies Working Group/Electronic Money Association (joint submission)

Dogecoin

Dogecoin Foundation

Elliptic

Epiphyte

eToro

Financial Supervision Commission, Isle of Man

FirstHand

GreenCoin

Home Office

HSBC

IBOS Association

IBWT

Imperial College Bitcoin Forum

Information Commissioner's Office

Innovate Finance

LEOcoin

Lockspin/BitBargain

London School of Economics, Economic History Department

Maclay Murray & Spens LLP

MasterCard

MatrixVision

MetaLair

Micro Code Cambridge

Mimex

MultiSigX

National Crime Agency

Netagio

Orwell Group

Payments Advisory Group

Project Azura

PwC

Ripple Labs

Ripula

Royal Bank of Scotland

SatoshiPoint

Selachii LLP

Silicon Valley Bank

UK Cards Association

UK Digital Currency Association

University of Birmingham, Birmingham Law School

University of Liverpool, School of Law and Social Justice

University of Southampton, Web Science and Cyber Security Academic Centre of Excellence

Vendorcom

VocaLink

Where to Spend Bitcoins UK

Yacuna

HM Treasury contacts

This document can be downloaded from www.gov.uk

If you require this information in an alternative format or have general enquiries about HM Treasury and its work, contact:

Correspondence Team
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel: 020 7270 5000

Email: public.enquiries@hmtreasury.gsi.gov.uk