Digital, virtual and crypto currencies: issues and accounting risks

Almost on a daily basis there are reports in the media regarding digital currencies; ‘FCA considers approving blockchain businesses’, ‘WEF: Blockchain will become the ‘beating heart’ of finance’, ‘Bank and tech firms apply blockchain to trade finance’, to name but a few.

This article seeks to demystify the terminology by providing an overview of digital currencies, and highlight the key accounting challenges, namely; valuation, existence and regulatory risk, facing companies entering this ever developing area.

What are digital, virtual and crypto currencies?
Digital currency is a broad medium of monetary exchange in which the value is both stored and transferred electronically. Virtual currencies and crypto currencies are both types of digital currencies. Digital currencies can include a multitude of common products; gift cards, product rebate cards, airline reward points, credit card cash-back rewards. These share a similar trait in that they have a value in the real world, and can be used to purchase goods and services.

Virtual currencies are centralised, internet based currencies, which are used as medium of exchange in the framework of a virtual world. Often these are associated with online games or social media platforms and used by ‘members of a specific virtual community’.

Crypto currencies are a form of digital currency but differ in that they are not denominated in an official currency and are not controlled by a centralised authority.

This paper has focussed on crypto currencies, specifically convertible digital currencies, being those with an equivalent value to a recognised legal tender, and the technology underpinning them, as this is the area which is most likely to have accounting implications, and potential impact on established stores of value in the future.
Crypto currencies
A crypto currency, of which there were more than 669 available for trade in online markets as of 24 August 2015¹, uses cryptography for security (with the intention of making it difficult to counterfeit) and is not backed by a central bank, government or commodity, but can still be used as a currency of exchange and store of value. There are a number of common crypto currencies in use today but the most recognisable of these is bitcoin.
Unlike traditionally recognised legal tender, digital currencies do not have to be issued by a central authority; bitcoin was the first decentralised ledger² currency when it was released in 2009. To record bitcoin transactions without the use of a trusted central authority, a public ledger, known as the blockchain, is used and is maintained by a network of communicating nodes which run the bitcoin software. The bitcoin system is designed so that there will never be more than 21 million bitcoins and it is currently estimated that there are around 13 million in existence³.

The advantages of a crypto currency
The benefits and potential competitive advantages that crypto currencies offer are very compelling; transactions are fully processed and verified quickly, there are no banking or currency exchange fees, privacy and the system is potentially more secure than those for credit cards given the encryption.

Issues
On the downside there are currently some real challenges facing the fledgling industry. The three most prominent being volatility, regulatory and technological complexity.

Volatility
The value of a bitcoin has fluctuated significantly since it was released (see left), reaching its highest value in 2013. It is possible that this is due to the infancy of the currency and that this will stabilise over time, but it could also be indicative of inherent weaknesses.

(Un)regulatory environment
Given the currency is not controlled by a centralised entity it raises a number of concerns with law enforcement agencies and tax authorities because of its anonymity, and hence the ease at which it can be used for money laundering and other illicit activities. This is demonstrated by Liberty Reserve, which essentially offered a precursor product to common crypto currencies of today. Liberty Reserve was shut down by United States federal prosecutors in May 2013 who charged its founder, Arthur Budovsky, and six others with money laundering. It is alleged to have been used to launder more than $6 billion in criminal proceeds during its brief seven year history.

One of the main current challenges facing crypto currencies like bitcoin is around transparency. Whilst the transactions are completely transparent, the individuals connected to any one transaction, as with cash transactions, cannot be easily identified. A paper released in 2011 in the United States⁴ sought to address this and determine whether the anonymity of users can be eroded. It was argued that public keys can be attached to users by transacting with them and logging the related address. Whilst this may be possible for established services within the bitcoin economy, it is not clear if this could be used to deter criminal activity. One simple circumnavigation of the control would be for a user to create multiple addresses and prevent transactions being linked together. There has been significant discussion at a governmental level on the use of crypto currencies. In specific response to the transparency concerns, the Financial Crime Enforcement Network (FinCEN) issued

---

¹ https://en.wikipedia.org/wiki/List_of_crypto_currencies
² A decentralised ledger or marketplace is one that allows users to conduct transactions peer-to-peer without a central administrator/exchange
⁴ IMF Staff Discussion Note: Virtual Currencies and Beyond: Initial Considerations. January 2016. Source: CoinDesk.com, Datastream and IMF staff calculations
⁵ Mieklejohn et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names
guidance on the use of virtual currencies in March 20134 and HM Treasury issued a call for information in respect of digital currencies in March 20155. These publications outlined the potential risks of virtual currencies and highlighted that there is currently no clear consensus on regulation.

More recently, authorities have begun to incorporate digital currencies into their anti-money laundering policies. In February 2016, the European Commission set out proposals to make amendments to the Fourth Anti-Money Laundering Directive and, in July 2016, announced that virtual currencies would be covered by the changes. The amendments are yet to be approved by the EU Parliament and member states, however the European Banking Authority (EBA) understands that member states have committed to implementing the directive by December 20166. The EBA, whilst it welcomes the changes, has requested that the legal framework is not implemented until 26 June 2017, at the earliest, to allow businesses time to adapt to the new regulatory requirements. In July 2016, the UK Gambling Commission also issued an update to its code of practice to cover cash equivalents, including digital currencies, for the purpose of protecting consumers and mitigating financial crime7.

**Technological complexity**

The complex technology and operating mechanism supporting a crypto currency like bitcoin means many people are inevitably wary of this new monetary concept that they don’t fully understand.

This has been borne out by bitcoin experiencing some glitches in the technology underpinning it which has resulted in transactions being halted and improper transactions being allowed to occur, for example using the same bitcoins to make two separate payments.

Similarly, the legal landscape around applying this complex technology is unclear. To obtain bitcoins a user must mine for them using specific software which requires them to have sufficient computing resources; it is not uncommon for users to join mining pools to combine their resources for this purpose. It is possible, in an organisation without adequate security measures, that an individual could gain access to multiple company computers and use them to mine for bitcoins whilst they are idle (similar to the strategy used in the Search for Extra-terrestrial Intelligence (SETI) at home project). This falls within a grey area with regard to whether any inappropriate action has been undertaken and would often depend on the organisation’s information systems policy. It is unclear whether such action could be considered as theft, however it could be considered an offence under the Computer Misuse Act 1990 if unauthorised access has been obtained.

**Developments**

Whilst Bitcoin grabbed the headlines initially, it is the underlying technology of crypto currencies that is the main area of development. The blockchain, or distributed digital ledger approach, that has been used for these currencies offers development potential in many other areas of provenance, or value exchange. Grant Thornton recently published an article on blockchain which describes it in greater detail8.

The most obvious future development and application of the technology underpinning bitcoin is the use by banks to automate their payment systems. Several banks, including BNP, Barclays, UBS and Deutsche Bank, are experimenting with their own technologies based on the blockchain model and have filed patents9. Others, such as JP Morgan, are backing fintech start-ups, such as Digital Asset Holdings, which has recently announced an agreement with the Depository Trust and Clearing Corporation to develop a distributed ledger solution to drive improvement in repo clearing.

However, at this stage there appear to be few working models and a lack of joint adoption across the industry. The Linux Foundation announced an open source project to advance the blockchain digital technology for recording and verifying transactions, the Hyperledger Project, in December 2015 and has received proposed code and technology contributions from several companies, including Blockstream, Digital Asset, IBM and Ripple.

In principle, a distributed ledger is shared by many parties amongst a network of computers and consequently is near-on impossible to tamper with. Each participant needs to approve the transaction before it is recorded on the ledger, with cryptography used to secure the details of the transaction. Further development of the technology is needed to ensure near-instantaneous execution.

Approval of the transactions prior to being recorded on the blockchain results in a more regulated platform and reduces the potential for money laundering, which makes it more appealing to banks. Such technology is being developed by Symbiont and is being piloted in two US top 10 banks10. By recording every action and transfer of ownership, which can each be easily verified by the counterparties, on the blockchain, every transaction could be accessed by the regulators using privileged cryptographic keys.

There are however many practical challenges facing the implementation of a distributed ledger system: any blockchain system used would need to be linked to allow the transacting parties to work together (in all likelihood, it would be operated by a third party); the ledger would need to be compatible with the existing Information Technology systems in place at each of the various banks; and the system would need to meet the requirements of the market regulators (including anti-money laundering and trade reporting laws).

---

5 https://www.gov.uk/government/consultations/digital-currencies-call-for-information
6 https://www.gov.uk/government/consultations/digital-currencies-call-for-information
9 https://www.coindesk.com/uk-gambling-digital-currency-rules/
10 http://www.grantthornton.co.uk/insights/a-beginners-guide-to-the-blockchain/
11 http://www.fintimes.com/2015/02/05/what-is-a-blockchain-and-how-does-it-work/
Accounting issues arising from the use of digital currencies

Revenue recognition and taxation
If digital currencies become more widely used it will be necessary to consider the revenue recognition in relation to any transactions undertaken using them, the associated measurement criteria and any tax implications. How they are treated (cash, non–cash assets), and accordingly which accounting policies apply (depreciation)?

If a holding of a digital currency is an asset, how is this accounted for in the books and records, for example what happens when an accounts receivable entry is paid via a bitcoin? Currently in the UK there is no specific accounting guidance in relation to transactions undertaken in a digital currency.

Valuation
As noted previously, the values of digital currencies are volatile. This could represent challenges when determining the valuation of an entity which holds any significant quantity of digital currency as an off–balance sheet asset or liability, as well as considering how such holdings should accounted for when producing financial statements.

Verifying existence
Bitcoins are susceptible to being lost or stolen either due to the device on which they are stored being lost, for example a laptop or mobile phone, or by the device being hacked. To prevent them being lost in this way, users can print out the code associated with their bitcoins. At present, there is no legislation in place to protect those who have had their bitcoins stolen or their digital wallets hacked.

Regulation
As there is no verification of the users, this opens up the digital economy to the possibility of money laundering and fraud. If the technology was to be used within banks, it is currently not clear what systems would be put in place to comply with anti-money laundering regulations. This is an area for further consideration and is expected to develop in the future should banks proceed with the technology.

Summary
Digital and specifically crypto currencies developed by the banking community represent a real opportunity for commerce and economic development, but this is not without sizeable challenges.

At Grant Thornton we have industry specialists who are familiar with ensuring the correct accounting treatment is applied, whether that be valuing complex financial products, confirming the revenue recognition or providing assurance that assets or liabilities are appropriately substantiated. On the regulatory side, many of our 500 financial service professionals deal with national and international regulatory matters. Our forensic team, supported by dedicated digital disclosure and digital forensic specialists, conduct investigations into the provenance, third party validation and quantum on a range of subjects.

Therefore whilst it is currently unclear as to how this area will ultimately develop we consider we are well placed to advise on myriad aspects.

For further information please contact:

James Helme
Associate Director
T 020 7865 2487
E james.helme@uk.gt.com

Emma Wilkinson
Executive
T 020 7865 2385
E emma.l.wilkinson@uk.gt.com

Grant Thornton
An instinct for growth

© 2016 Grant Thornton UK LLP. All rights reserved. ‘Grant Thornton’ refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and ‘or its partners’ refers to one or more member firms, as the context requires. Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another’s acts or omissions. This publication has been prepared only as a guide. No responsibility can be accepted by us for loss occasioned to any person acting or refraining from acting as a result of any material in this publication.

grant-thornton.co.uk