Modular FX Services Limited
86-90 Paul Street
London EC2A 4NE
Tel: +44 (0)20 3727 5131

16 July 2015

ESMA
European Securities and Markets Authority
CS 60747
103 rue de Grenelle
75345 Paris Cedex 07
France

Submitted via esma.europa.eu

Sub: Feedback to ESMA/2015/532:
Investment using virtual currency or distributed ledger technology

Dear Sir or Madam,

Modular FX Services Limited[1] appreciates the opportunity to provide information in response to the above paper.

As part of our advisory work with regulated entities and providers of services to investors, we have engaged in conversations around the application of distributed ledger technology, as one potential means to reduce costs and to improve the speed and resilience of digital systems. Our responses to the paper relate to the research and findings from our work.

Yours faithfully,

Howard Grubb
Director
Modular FX Services Limited

Stephan von Massenbach
Director
Modular FX Services Limited

[1] Modular FX Services Limited is an independent provider of Analytics and Advisory Services for FX market participants.

Modular FX Services Limited
86-90 Paul Street
London EC2A 4NE
Tel: +44 (0)20 3727 5131

Responses to ESMA/2015/532

Q3: Do you have anything to add or suggest a change to the description (paragraphs 15-18) of how virtual currency distributed ledgers work? Please clearly state to which virtual currency you are referring in your answer or whether your answer refers to virtual currencies in general

- Not all distributed ledger implementations rely upon an embedded VC "token" to form part of the verification protocol (e.g. Hyperledger, Eris Industries[2] [3] [4]). However, despite lacking a VC as a component for investment, these implementations may still form part of a transaction or settlement system (e.g. Hyperledger by Digital Asset Holdings).
- A VC token, as part of distributed ledger technology, can be subject to speculative activity, which may add higher volatility than otherwise to an investment product.

Q8: Do you agree with the assessment of benefits and risks of VC based financial assets/securities or are there other benefits/risks for investors, for other market participants, and for the financial system as a whole?

We group our responses under general headings for each area of potential benefit/risk, which can help evaluate the potential applications of these innovative technologies, as they are undergoing rapid evolution and widening deployment.

Note that many points below refer to the "Bitcoin" implementation of distributed ledger technology ("Bitcoin" is commonly used to refer to both the VC token, or asset, and the network protocol for transmission and verification). This is the most mature implementation of such technology, so it has been extensively exercised in a range of applications. Many of the points may also be relevant to other distributed ledger implementations.

Speed/capacity

- The potential speed benefits of distributed ledger technologies remain to be evidenced and compared with alternatives for the various stages of investment transactions, where these technologies may be applied. Some consensus verification mechanisms (as used for example by the Bitcoin protocol) can take several minutes[5] before confirmation that the transactions are part of a verified block. Other verification mechanisms are closer to real-time[6].
- The "block size" (of each set of transactions) in some implementations imposes a limitation on transaction volume that the network can process and consequently also on minimum viable transaction sizes.

[2] http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf
[3] http://hyperledger.com/posts/2015-04-27-how-to-explain-the-value-of-replicated-shared-ledgers-from-first-principles.html
[4] http://gendal.me/2015/06/08/towards-a-unified-model-for-replicated-shared-ledgers/
[5] https://blockchain.info/charts/avg-confirmation-time
[6] https://ripple.com/integrate/executive-summary-for-financial-institutions/

Modular FX Services Limited
86-90 Paul Street
London EC2A 4NE
Tel: +44 (0)20 3727 5131

- Partly to offset some of the limitations ("block size", verification speed) some gateways to VCs use "off-chain" transactions, which circumvent the security benefits of a blockchain ledger.

Cost

- The (total) cost of transactions on distributed ledgers needs further consideration and validation against alternatives (including traditional).
- In "mining" based protocols, the reward for miners is usually in units of VC, the value of which should cover the real resource cost of mining[7] [8].
- Further, once all VC "tokens" have been "mined", the future transaction costs of such a network are unknown (indeed, the existence of miners is not guaranteed at this stage in the evolution) – to be determined by miners, but presumably at a minimum to cover their fixed real resource cost of verifying transactions.

Gateways

- In order to access a VC, or other distributed ledger implementation, investors must make use of one of a range of "gateways", which themselves represent both a real cost per transaction (into and out of the VC instrument[9]) and a counterparty risk between the gateway and investor.
- Further, bringing funds into and out of the VC instrument is subject to the relatively high price volatility exhibited by many of the existing VCs (paragraph 37 refers to the exchange rate risk when investing in VC based assets).

Regulation/supervision

- Decentralised and/or "permissionless" blockchain implementations are not amenable to conventional regulatory oversight.
- Permissioned implementations, relying on known "validators", may however fit within current regulatory regimes.
- Where verification is permissionless, it is possible for a single entity with sufficient resources to control the consensus. Indeed with specialisation in "mining" technology, this is considered to be relatively likely[10].

Technology stability

- The technologies are rapidly evolving, which can lead to risks (e.g. around stress-testing and resilience). Some implementations rely upon consensus-driven code development,

[7] http://www.allied-control.com/publications/Analysis_of_Large-Scale_Bitcoin_Mining_Operations.pdf reported at: http://motherboard.vice.com/read/bitcoin-is-unsustainable
[8] https://blockchain.info/charts/cost-per-transaction-percent, https://blockchain.info/charts/cost-per-transaction
[9] Anecdotally, most VC gateways currently seem to be charging around 1%.
[10] https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/bitcoin%20%20final.pdf

Modular FX Services Limited
86-90 Paul Street
London EC2A 4NE
Tel: +44 (0)20 3727 5131

which brings operational risks (e.g. Bitcoin)[10]. Not all distributed ledger implementations have this consensus dependency.

- This development approach can lead to transactions on a non-consensus "fork" of the protocol code to be invalidated, which has significant implications for investors[11]. Such an issue has recently occurred on Bitcoin[12] [13] [14], resulting in an inability to verify transactions until resolved. This also brought to light the partial validation of blocks being applied by many miners.

Q9: How is distributed ledger technology being used or likely to be used in relation to the issuance, distribution, trading, recording of transactions and ownership of 'traditional' securities or investment products and why?

- One emerging application of blockchain technology in investments is for so-called "smart contracts", where several stages of a transaction or product can be encoded at the start and triggered by external inputs (e.g. Digital Asset Holdings, Eris Industries).
- This application has potential for considerable improvements in speed for some currently slow stages of certain financial transactions' lifecycle (e.g. corporate actions, credit events) and can ensure deterministic behaviour to "triggers" in the existing standardised legal framework.
- However, the immutable nature of the blockchain requires careful consideration in this complex application area.
- A key risk to consider in these applications is the verification of input triggers to the stages of the contracts, since only the set of rules is encoded in the blockchain.

[11] https://www.mail-archive.com/bitcoin-development@lists.sourceforge.net/msg08305.html
[12] http://ftalphaville.ft.com/2015/07/06/2133719/bitcoin-being-forked/
[13] https://bitcoin.org/en/alert/2015-07-04-spv-mining
[14] http://www.coindesk.com/double-spending-risk-bitcoin-network-fork/