Security or not security? Scrutiny of blockchain and ICOs mounts

Angela Bilbow - 29 January, 2018

A report published by Skadden, Arps, Slate, Meagher & Flom on the increasing use of blockchain technology and initial coin offerings has highlighted a rise in regulatory scrutiny and potential areas for commercial disputes.

In its report, *Rise of Blockchain and ICOs Brings Regulatory Scrutiny*, New York-headquartered **Skadden, Arps, Slate, Meagher & Flom** has highlighted mounting regulatory scrutiny as various industry sectors embrace blockchain technology.

Indeed, the United States **Securities and Exchange Commission** (SEC) has recently ramped up its message to market professionals and main street investors, with its chair **Jay Clayton** issuing a warning in December that, as it stands, there is "substantially less consumer protection" under current cryptocurrency and initial coin offering (ICO) market operations than there is in traditional securities markets, and a by-product of that is "greater opportunities for fraud and manipulation".

Clayton urged lawyers, accountants and consultants to be aware of the disclosure requirements, processes and investor protections that current US securities laws mandate, and pointed to enforcement action already taken by the SEC, including that against California-based **Munchee** which was forced in December 2017 to halt its USD 15 million ICO after consenting to an SEC cease-and-desist order that found the blockchain-based food review service had conducted unregistered securities offerings and sales.

Because Munchee and other promoters had emphasised that investors could expect that certain efforts made by the company would lead to an increase in the value of the digital tokens they purchased – the tokens can be a considered a 'security' based on the 'long-standing facts and circumstances test' which assesses whether investors' profits are to be derived as a result of the managerial and entrepreneurial efforts of others.

With ICOs generating an estimated USD 3.7 billion in funding during 2017, around 10 times the amount generated in 2016, the SEC has devoted specific resources to oversee the practice, with its new cyber unit specifically focused on misconduct involving distributed ledger technology (such as blockchain) and ICOs.

In its statement, **Stephanie Avakian**, co-director of the SEC's enforcement division said: "We will continue to scrutinise the market vigilantly for improper offerings that seek to sell securities to the general public without the required registration or exemption. In deciding not to impose a penalty [on Munchee], the Commission recognised that the company stopped the ICO quickly, immediately returned the proceeds before issuing tokens, and cooperated with the investigation."

Responding to such enforcement activity, Skadden questioned whether the SEC would develop a new regulatory framework

for ICOs and added: “In the absence of additional guidance and in the face of the SEC’s recent actions and a rising tide of private class action law suits, issuers and counsel are struggling to find consensus regarding an approach to ICOs that complies with securities laws while retaining the unique opportunities that ICOs offer to both token sellers and purchasers.”

INCREASED RULEMAKING, SMART CONTRACTS AND AML

Highlighting an expectation that federal regulators may make increased pronouncements and rulemaking in multiple arenas, as they get to grips with innovation in the blockchain space, Skadden referenced another regulator attuned to the risks; namely, the US **Commodity Futures Trading Commission**’s enforcement division, which has been active on issues surrounding virtual currencies – such as retail fraud and failure to register – since 2015.

Skadden then turned the focus on smart contracts – blocks of computer code that automatically execute pre-agreed transactions on a blockchain. Here, the firm warned that, “while smart contracts will not themselves replace most paper contracts, they are a necessary component of any blockchain-based transaction”; what remains unclear is how a court will approach the code in the event of a dispute, “such as a case where the code and paper contract do not align”.

This had been partially addressed last year in Arizona, the report explained, when the state enacted a law which provided that a contract “may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term”.

“We expect similar amendments to state laws in 2018, although some uncertainty will remain until courts begin to adjudicate the treatment of smart contracts,” the firm added.

On the anti-money laundering (AML) side, the report said that focus has been on whether the structure of an ICO, the nature and intended use of a token or coin being issued, or the company’s operations after the ICO, could mean that the company is considered to be a ‘money transmitter’.

If so, it is a money service business and therefore subject to US federal AML regulations, and required to register with the US Treasury’s Financial Crimes Enforcement Network and implement an AML compliance programme to that effect.

FURTHER PRACTICAL ISSUES

At a recent event hosted by **Brown Rudnick** in London, **Michael Booth QC** of **New Square Chambers** spoke on the emergence of technological developments, such as cryptocurrencies, and how they impact the way lawyers must address issues, such as disclosure.

Speaking to *CDR*, Brown Rudnick partner **Jane Colston**, an expert in commercial fraud, outlines another area that is currently under question – whether freezing orders should be amended to require the disclosure of cryptocurrencies, like bitcoin, specifically.

Owners can access their bitcoin via a private key assigned to them, and a collection of keys can be kept in a digital wallet. If an owner loses the key/s, their bitcoin is lost forever because there is no recognition of ownership. Owners of bitcoin, or other virtual currencies, cannot be explicitly identified.

As such, Colston says that freezing, disclosure and search orders can be used to identify if a defendant has any bitcoins assets and/or has received stolen monies in the form of bitcoins.

“It is important that such orders specifically seek disclosure of bitcoin so these are firmly on the radar of the disclosure required by the defendant. Although disclosure orders may say that the individual subject to the order should comply with the order, the question is whether they will comply.”

She asks: “If disclosure is not made, then how do you then find out about any bitcoins [or other virtual currencies]?”

While on one hand, Bitcoin or crypto records will be permanent and publically available to view on the blockchain, “the real issue is linking that transaction to a specific person”, Colston adds.

Here, she suggests that Norwich Pharmacal orders are unlikely to assist, as the whole point of virtual currencies is that there is no intermediary.

Colston's advice is to compel disclosure from the defendant, "such as bank account statements in order to see if bitcoin-related purchases have been made from online merchants, brokers or an exchange".

Further, the imaging and analysis of data obtained a search order may show if the defendant has accessed a bitcoin wallet so you may be able to view the user's transactions on the blockchain if, for example, the private key and/or wallet are stored on the defendant's computer, she explains, adding that if the defendant fails to disclose its ownership of virtual currencies, especially if these have been expressly identified in the order, it may be in contempt of court.

"In recent times the court has been willing to imprison defendants who have failed to give full asset disclosure," Colston concludes.

Skadden's report also highlighted positive areas of collaboration between regulators and innovators, citing the United Kingdom **Financial Conduct Authority**'s 'sandbox' – a project allowing approved users to live test new financial products and services in a live market environment.