Banking and
Finance Law Daily

Wolters Kluwer

February 23, 2018

Rise of Blockchain and ICOs Brings Regulatory Scrutiny

By Ryan J. Dzierniejko Gregory A. Fernicola Eytan J. Fisch Stuart D. Levi
Skadden, Arps, Slate, Meagher & Flom LLP

In 2017, the increased adoption of blockchain technology in various industries was partially obscured by the dramatic fluctuations in the price of bitcoins and the prevalence of so-called initial coin offerings (ICOs) to raise capital to build out blockchain applications and platforms. Adoption of blockchain technology is expected to continue to rise in 2018, and the growing popularity of both the technology and ICOs is likely to bring with it continued legislative and regulatory scrutiny, especially with respect to U.S. securities and anti-money laundering laws.

Blockchain Trends

Blockchain technology refers to a distributed ledger system in which all parties have access to a secure and immutable ledger, and can transact with unknown parties in a secure manner. The system used advanced cryptography and a consensus algorithm to achieve that end. Certain blockchains are public in that they are accessible to all, Bitcoin being the most popular example, while others are private or permissioned blockchains, which are accessible only to approved users, such as a consortium of banks. (For background on how the technology operates, see our *2017 Insights* article "Blockchains Offer Revolutionary Potential in Fintech and Beyond.")

In 2017, a number of organizations began to incorporate nascent blockchain technology in proof-of-concept projects such as tracking swaps contracts post-execution and managing supply chains. To date, most of these projects have run parallel to traditional transaction methods rather than replaced them. We anticipate this trend will continue in the near term; thereafter, companies may begin to fully adopt blockchain technology as a replacement for their current modes of conducting business. Two key factors will drive the pace and extent of increased adoption: the regulatory environment and the legal treatment of so-called smart contracts.

In any industry with established oversight, regulators will need to determine how they can adapt their current role to new blockchain-based environments. This will require them to dedicate resources to understand the technology and develop approaches that foster, not hamper, innovation. For example, in the U.S., a new Delaware law went into effect in 2017 that allows Delaware corporations to maintain shareholder lists, along with other corporate records, using blockchain technology. In the U.K., the Financial Conduct Authority's "sandbox," which allows approved companies to test new financial products and services in a live market environment, serves as a prime example of cooperation between regulators and innovators. Although many regulatory solutions are being

debated, one promising approach would be for regulators to act as a "node" on a private blockchain network in order to seamlessly execute their oversight role, thereby lowering compliance costs and increasing transparency.

Federal regulators also are grappling with the application of blockchain technology in securities financing/offerings, as described below, and derivatives, as described in "CFTC Updates on Virtual Currency Regulation, Alternatives to Libor and Fallout From Brexit." We expect that in 2018, regulators may make increased pronouncements and rulemaking in multiple arenas as they get up to speed on innovation in this area and industry players seek guidance on what is permissible.

Smart contracts to execute transactions on a blockchain are some of the most powerful tools used to enable this technology. Smart contracts are simply computer code that automatically execute agreed-upon transactions. For example, a piece of smart contract code might trigger an insurance payment to a farmer if the objectively verifiable temperature falls below freezing for a number of days. While smart contracts will not themselves replace most paper contracts, they are a necessary component of any blockchain-based transaction. An unresolved issue is how courts will treat this code in the event of a dispute, such as a case where the code and paper contract do not align. In 2017, Arizona partially addressed this issue when it enacted a law stating 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 other state laws in 2018, although some uncertainty will remain until courts begin to adjudicate the treatment of smart contracts.

ICOs

ICOs have become a significant source of funding for companies raising capital to build out blockchain applications and platforms. According to some sources, these offerings generated more than $3.7 billion of funding in 2017, more than 10 times the amount in 2016. As ICOs gained more prominence over the course of the year, many commentators and legal counsel began to highlight issues with the way these offerings were structured, including with respect to U.S. securities and anti-money laundering laws.

Securities Laws

Although other jurisdictions have taken drastic steps to curb the pace of ICOs — including China's flat ban on the sale of blockchain tokens — the U.S. Securities and Exchange Commission (SEC) has yet to develop an ICO-specific regulatory framework. Instead, in September 2017, the SEC announced the creation of the Cyber Unit within the Enforcement Division, which focuses on targeting cyber-related misconduct, including violations involving distributed ledger technology and ICOs. In the months since its formation, the Cyber Unit has filed complaints in court and brought administrative proceedings against a number of issuers, alleging that their ICOs are either fraudulent or otherwise do not comply with U.S. federal securities laws. In one such action, the Cyber Unit issued a cease-and-desist order to halt Munchee Inc.'s sale of MUN tokens. Munchee marketed MUN tokens as "utility tokens," which it said removed the offer and sale of the tokens from the purview of

U.S. federal securities laws. The Cyber Unit, in its cease-and-desist order, disagreed with Munchee's position, finding that the company was offering securities in a manner that did not comply with applicable laws.

On December 11, 2017, SEC Chairman Jay Clayton issued a "Statement on Cryptocurrencies and Initial Coin Offerings," in which he drew a distinction between true cryptocurrencies that have inherent value (similar to cash or gold) and those blockchain tokens that resemble securities. Chairman Clayton emphasized that simply calling a token a "utility" token or structuring it to provide some consumptive value does not prevent it from being a security. He noted that "[b]y and large, the structures of initial coin offerings that I have seen promoted involve the offer and sale of securities and directly implicate the securities registration requirements and other investor protection provisions of our federal securities laws."

It remains to be seen whether the SEC will develop a new regulatory framework for ICOs or continue applying traditional principles to determine whether a cryptocurrency or blockchain token is a security under federal securities laws. In the absence of additional guidance and in the face of the SEC's recent actions and a rising tide of private class action lawsuits, 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.

Anti-Money Laundering Laws

In the anti-money laundering (AML) arena, a key area of focus has been on whether the structure of an ICO, the nature and intended use of the token or coin being issued, or the company's operations after the ICO may qualify a company as a "money transmitter" and, consequently, as a money service business (MSB) under U.S. federal AML regulations. MSBs are required to register with the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and implement an AML compliance program that includes policies, procedures and internal controls to ensure compliance with applicable laws.

While FinCEN has issued certain interpretive guidance at the federal level to clarify the applicability of the regulations implementing the Bank Secrecy Act (BSA) to persons creating, exchanging and transmitting virtual currencies, it has not yet issued ICO-specific regulatory guidance. Congress has begun to seek greater clarity regarding FinCEN's approach to ICOs. For example, in December 2017, Sen. Ron Wyden, D-Ore., sent FinCEN a request for answers to a series of questions on ICOs, including how FinCEN will apply the BSA framework to participants in the ICO market, like token developers, and when FinCEN will issue guidance regarding its enforcement intentions regarding digital token exchanges and ICOs.

Although FinCEN has yet to take an enforcement action in connection with the issuance of tokens in the ICO context, it has made clear that it will not hesitate to take action against companies dealing in the virtual currency realm. (See our article in the November 2017 issue of *Cross-Border Investigations Update*, "ICOs and Cryptocurrencies: How Regulation and Enforcement Activity Are Reshaping These Markets.")

Nearly all U.S. states enforce their own state laws related to money transmission, which may be relevant to certain ICOs or to a company's subsequent operations. State money transmitter laws are varied and do not take a uniform approach to virtual currency-related businesses.

New York has added to the complexity of the regulatory landscape by adopting a "BitLicense" regulation in addition to its own state money transmitter regulatory laws. Companies engaged in a "Virtual Currency Business Activity" involving the state or a New York resident must receive a BitLicense from the New York State Department of Financial Services (NYDFS). Regulated virtual currency business activities include controlling, administering or issuing virtual currency — which the regulation defines broadly — and receiving virtual currency for transmission or transmitting virtual currency for a financial purpose. Licensees must meet AML program standards similar to those imposed by FinCEN as well as certain capitalization, consumer protection and cybersecurity standards, and must comply with applicable U.S. sanctions laws. To date, there have been no ICO-related NYDFS AML enforcement actions. However, NYDFS is a regulator known for its aggressive enforcement posture, and its approach to ICOs will be closely watched.

Certain other states, including California, also are considering regulatory frameworks specific to virtual currency business activities. To help harmonize the patchwork of state laws regarding virtual currencies, in 2017, the National Conference of Commissioners on Uniform State Laws issued the model Uniform Regulation of Virtual Currency Businesses Act (VCBA), which would create a licensing and registration framework for engaging in virtual currency business activities. The VCBA has yet to be adopted by any state, but its existence may drive states toward a more synchronized approach to the world of virtual currency-related businesses.

Associates Valian A. Afshar, Pamela Nwaoko, James E. Perry and Ashton M. Simmons contributed to this article.