Skadden

As Interest in Blockchain Technology Grows, So Do Attempts at Guidance and Regulation

Contributing Partners

Alexander C. Drylewski / New York

Eytan J. Fisch / Washington, D.C.

Stuart D. Levi / New York

Of Counsel

Jonathan Marcus / Washington, D.C.

Counsel

Eve-Christie Vermynck / London

This article is from Skadden's *2019 Insights*.

Four Times Square
New York, NY 10036
212.735.3000

In 2018, the number of blockchain-enabled projects increased sharply as established companies sought to apply distributed ledger technology to their existing business models and startups developed new and disruptive models employing this technology. Projects have already been implemented in the financial services, insurance and supply chain fields, and important developments are taking place in blockchain-based identity services. As use of blockchain technology has expanded, regulators from a range of geographic and legal jurisdictions have struggled to apply laws and regulations that were drafted for business activities involving a clearly identifiable service "provider" to autonomous, decentralized platforms where the actual "provider" is not evident.

For example, regulators responsible for securities, commodities, anti-money laundering (AML) and privacy all wrestled with blockchain issues in 2018. Often, the cases brought and guidance offered raised more questions than they answered. Any company implementing or investing in blockchain technology will need to pay close attention to this evolving regulatory landscape.

Securities Law

A number of noteworthy legal developments relating to cryptocurrencies emerged in 2018, providing incremental clarity for participants in this emerging area of securities law.

- **Digital Tokens.** On June 14, 2018, William H. Hinman, director of the Securities and Exchange Commission's (SEC) Division of Corporation Finance, suggested that digital tokens like Ether might initially be defined as "investment contracts" (and thus as "securities" under the federal securities laws) but that their networks and decentralized structures could evolve to a point where the tokens no longer constituted securities.
- **FinHub.** On October 18, 2018, the SEC launched the Strategic Hub for Innovation and Financial Technology (FinHub), which was designed to provide a way for technologists and their advisers "to engage with SEC staff," according to Valerie A. Szczepanik, the SEC's senior adviser for digital assets and innovation. The creation of FinHub suggests that the SEC is willing to work with developers regarding compliance rather than approach the issue solely from an enforcement perspective.
- **SEC Settlements.** On November 16, 2018, the SEC announced that CarrierEQ Inc. (aka AirFox) and Paragon Coin Inc., which sold digital tokens in initial coin offerings (ICOs), agreed to pay penalties, register under Section 12(g) of the Securities Exchange Act and offer voluntary rescission rights to investors. These settlements may provide a road map to compliance for those who have already engaged in ICOs.

- ***SEC v. Blockvest, LLC.*** On November 27, 2018, Judge Gonzalo P. Curiel of the U.S. District Court for the Southern District of California denied the SEC's request for a preliminary injunction against a company that had engaged in an ICO. Judge Curiel concluded that the SEC had not established that the Blockvest tokens at issue were securities because there were disputed facts under the U.S. Supreme Court decision *SEC v. W.J. Howey Co.*'s "investment of money" and "expectation of profits" test prongs. This case may prove to be significant in that the court suggested the *Howey* test may not be met.
- **SEC Guidance.** On December 12, 2018, the SEC announced that it is developing guidance for cryptocurrencies that it hopes to publish in early 2019. The guidance is intended to help determine if a digital asset is a security. If it is, the guidance would detail what a business should do to comply with securities regulations. (See "SEC Continues Steady Progress With Regulatory, Enforcement Goals.")
- **Token Taxonomy Act.** On December 20, 2018, Reps. Warren Davidson, R-Ohio, and Darren Soto, D-Fla., introduced the Token Taxonomy Act, which seeks, in part, to clarify that securities laws would not apply to cryptocurrencies once they become a fully functioning network. Although we do not expect that this bill will be passed, it comes after a year of various congressional hearings on how current regulations apply to blockchain technology. We anticipate that Congress will remain focused on this issue in 2019.

FinCEN

Cryptocurrencies also have been the subject of increasing focus by the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), which exercises AML regulatory functions. Dating back to 2013, FinCEN has issued several rounds of guidance on the application of AML requirements to businesses performing certain functions or providing certain services related to cryptocurrencies. In 2018, FinCEN took additional steps toward answering outstanding questions, including in the context of ICOs. We expect FinCEN to issue further clarifying guidance in 2019.

In a February 2018 letter responding to questions from Sen. Ron Wyden, D-Ore., the Treasury Department took the position that "[g]enerally, under existing regulations and interpretations, a developer that sells convertible virtual currency, including in the form of ICO coins or tokens, in exchange for another type of value that substitutes for currency is a money transmitter" and is therefore subject to corresponding AML requirements for money services businesses. The Treasury Department, however, noted that ICOs vary in structure, and there could be circumstances in which AML requirements imposed by the SEC or Commodity Futures Trading Commission (CFTC) would apply.

FinCEN Director Kenneth A. Blanco echoed this view in an August 2018 speech at the Chicago-Kent Block (Legal) Tech Conference, stating that "[w]hile ICO arrangements vary and, depending on their structure, may be subject to different authorities, one fact remains absolute: FinCEN, and our partners at the SEC and CFTC, expect businesses involved in ICOs to meet all of their AML/CFT obligations." It is notable that Blanco did not specifically reassert the view in the Wyden letter that companies conducting ICOs generally are money transmitters. The failure to do so raises some questions as to whether FinCEN viewed the reaffirmation as unnecessary or was backtracking on the more categorical position.

FinCEN also is working with foreign governments to address risks related to virtual currencies, including through the Egmont Group of Financial Intelligence Units and through the Financial Action Task Force. Treasury Under Secretary Sigal P. Mandelker has stated that, as part of this effort, the Treasury Department is "encouraging our international partners to take urgent action to strengthen their AML/CFT frameworks for virtual currency and other related digital asset activities." We expect that efforts to align global approaches to cryptocurrencies will increase in 2019.

Applying GDPR to Blockchain Platforms

Blockchain technology has the potential to revolutionize how personal information is stored and processed. However, many of its fundamental concepts clash with the requirements of the European Union's General Data Protection Regulation (GDPR) requirements. (See "European Data Protection and Cybersecurity in 2019.")

In 2018, EU regulators began to focus on this issue, with the French supervisory authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), and the EU Blockchain Observatory and Forum (the Observatory) publishing initial reflections on this matter but offering little definitive guidance. For example, the reports acknowledged that with a blockchain platform, it is difficult to determine the identity of the data controller (which determines the purpose and means of processing personal data) and the data processor, since in many blockchain platforms, multiple nodes hold the data without any single controller or processor. The reports acknowledge this issue but simply conclude it must be resolved on a case-by-case basis.

Similarly, a cornerstone of blockchain technology is the use of hashing to cloak and represent specific data sets. While many see these hashes as anonymous and therefore not subject to privacy regulations, the GDPR narrowly limits anonymization to cases where it is impossible to reverse the encryption process or link the encrypted data to an individual by studying usage patterns. Hashes may not meet this definition. Here, too, the reports acknowledge the issue but leave it to case-by-case analysis.

The GDPR also provides individuals with a series of rights, including a right in certain cases to have their data deleted (known as the right to be forgotten). This principle conflicts with the immutability of a blockchain, where once data is stored, it cannot be erased or modified. Furthermore, it is not clear who enforces this right if a data controller cannot readily be identified. The CNIL's preliminary suggestion is that encryption coupled with the destruction of the encryption key might satisfy this requirement.

Although the reports signal that regulators are beginning to focus on this issue, they may not issue any meaningful guidance for some time. Developers of blockchain platforms will need to glean what they can from these initial reports and keep compliance with the GDPR and other privacy laws in mind during the development process.

CFTC/Derivatives Law

While the CFTC has actively used its enforcement authority to police fraud and protect retail customers in the cryptocurrency markets, its formal guidance on how the Commodity Exchange Act (CEA) applies to the blockchain and cryptocurrency space has been fairly sparse. Aside from a few short releases, the CFTC's primary guidance in this area is its December 2017 proposed interpretation of what constitutes "actual delivery" in retail cryptocurrency transactions. (The CFTC regulates leveraged or margined cryptocurrency transactions involving retail customers where the cryptocurrency is not "actually delivered" within 28 days.)

Near the end of 2018, the CFTC demonstrated its continuing interest in cryptocurrencies and their relationship to derivatives markets by requesting public input (RFI) on Ether and the Ethereum network. The RFI illustrates that the CFTC is relying on market participants and the public to help inform its understanding of, among other areas, how cryptocurrencies and their networks operate, the technology they depend on, their governance structures, the purposes for which they are used, and their liquidity and susceptibility to manipulation. This information is relevant to the CFTC in deciding how to police cryptocurrency fraud and regulate derivatives contracts based on cryptocurrencies. It is evident that the CFTC also is looking beyond cryptocurrencies and closely monitoring the development of decentralized systems generally. For example, LabCFTC, the agency's initiative to engage with the fintech innovation community, recently issued a primer on smart contracts to explain the technology and related risks and challenges.

Given the CFTC's interest in blockchain applications, one area to watch in 2019 will be the CFTC's regulatory approach to emerging smart contracts. On October 16, 2018, Commissioner Brian D. Quintenz stated at the 38th Annual GITEX Technology Week Conference that the CFTC's existing regulatory authority may apply to smart contracts, encouraging innovators to engage with the commission but also focusing on potential liability for coders whose smart contracts facilitate trading in products subject to CFTC jurisdiction, such as options entered into with retail customers. The SEC recently settled an enforcement action against Zachary Coburn, the founder of EtherDelta — a smart contract-based market platform for trading digital tokens — for causing it to operate as an unregistered securities exchange. The CFTC may not be far behind in pursuing smart contract applications that may not comply with the CEA or CFTC regulations.

Associates Andrew R. Beatty, Jeongu Gim and Trevor A. Levine contributed to this article.

Click here for a full list of fintech-related articles authored by Skadden attorneys in the last year.