RIMÔN LAW
LawFirmEvolved.com

Blockchain Law: ICO Regulation and Other Legal Considerations in the Blockchain Ecosystem

This article has been published in The Current: The Journal of PLI Press, Vol. 2, No. 1, Winter 2018 - Page 21 - (© 2018 Practising Law Institute). http://www.pli.edu/THECURRENT

Dror Futter focuses his practice on startup companies and their investors, and has worked with a wide range of technology companies. His fifteen years' experience as in-house counsel includes positions with Vidyo, Inc., a venture-backed videoconferencing company, and New Venture Partners, a venture fund focused on corporate spinouts. Prior to that, Mr. Futter was Counsel to the CIO of Lucent Technologies, as well as supporting parts of its sourcing organization.

Dror Futter, **Partner**
dror.futter@rimonlaw.com
(201) 685-0007

The Current
The Journal of PLI Press
Vol. 2, No. 1, Winter 2018

Blockchain Law: ICO Regulation and Other Legal Considerations in the Blockchain Ecosystem

Dror Futter
Rimon PC

During 2017, blockchain and its progeny Bitcoin and initial coin offerings (ICOs) became "big news." By the end of the year, news of new record highs for Bitcoin and eight- and nine-figure ICOs became almost daily events. As blockchain has entered the mainstream and the dollars at stake have exploded, it has become clear that this exciting technology has raised and will continue to raise issues across a broad range of legal disciplines.

In many ways, the current state of blockchain technology and "blockchain law" brings to mind the Internet and "Internet law" circa 1993. Just like the Internet in 1993, the potential of blockchain is clear; but for blockchain to reach

its full potential, it needs to scale, become faster, more secure, and more reliable, and develop user-friendly interfaces and middleware. In 1993, some were boldly proclaiming that the Internet existed outside the jurisdiction of sovereign laws, and others proclaimed that content posted to the Internet was in the "public domain" and not subject to copyright protection. Still others argued that sui generis Internet laws were required. Similar legally unsupportable arguments are now heard within the blockchain community.

The evolution of Internet law has been far more incremental than revolutionary. While at the margins Internet-specific laws were introduced, in most instances, existing laws, precedents, and principles were applied to the Internet. Today, businesses built on the Internet operate with far more legal certainty. Government regulators, legislators, judges, and lawyers advising blockchain pioneers are in the early stages of the same process. The leading case defining what a security is is a 1946 Supreme Court decision involving orange groves. Applying this precedent to ICOs raises many questions, but history suggests that in most instances these questions can be answered by regulators and judges without the need for new laws and new legal categories.

The Technology

At its core, blockchain is a distributed digital ledger technology. In other words, the same data is stored on multiple servers or nodes. Additions to the database are replicated across all nodes. Data is stored in blocks, and each block is linked to the prior block, thereby creating a chain of blocks—and the name of the technology. As a result, modifying a block cannot be done after the fact without altering each block that had subsequently been added. In addition, modifying one copy of the database would place it out of sync with the other copies of the database stored in other nodes that are controlled by different entities. As a result, efforts to alter the chain are readily detectable.

Blockchains can be public or private. In a public blockchain such as Bitcoin or Ethereum, anyone can host a node, enter data, and in many instances become a miner of tokens on the chain (more below) and receive token compensation. Anyone can read the blockchain and, subject to certain rules, add blocks to the blockchain. With private or "permissioned" blockchains, the ability to read the chain, add new blocks, or host nodes can be restricted. An example is a company

that builds a blockchain using nodes it controls to track components through its supply chain. Suppliers might be granted limited read/write privileges to the chain by the company controlling it.

Using Blockchain to Record Transactions

If Jane wants to transfer a Bitcoin to Bob, the transaction would work as follows. Both Jane and Bob have public and private cryptographic keys. The keys are large alphanumeric strings. Jane and Bob can communicate their public keys to others, but only they know their respective private keys. To transfer a Bitcoin, Jane would use her private key to encrypt the transaction details and attach it to Bob's public key. The transaction data would then be time-stamped and added to a block that would be recorded on the blockchain. Future users of the chain would see that on date/time *X*, Jane transferred a Bitcoin to Bob and Jane and Bob's Bitcoin balances were adjusted upwards and downwards appropriately. Going forward, only Bob, using his private key, could authorize a subsequent transfer of the Bitcoin. This prevents a double spending of the same coin.

Transactions recorded on the blockchain have several advantages over a centralized database:

- *Immutability.* Once a transaction is recorded, it cannot be altered. If a correction is required, a new transaction reversing the incorrect transaction must be recorded, and both entries are accessible to individuals accessing the blockchain.
- *Provenance*. If an asset is recorded on the blockchain, its entire chain of ownership is recorded on the blockchain.
- *Validation*. For a transaction to be valid, all participants must agree on its validity (different blockchains deploy different consensus mechanisms).
- *Finality.* The identical database stored on multiple nodes provides a single source for verifying the ownership of an asset or the completion of a transaction.

Smart Contracts

Blockchains can be passive stores of data or actively engage in transactions through the use of smart contracts. Smart contracts are basically agreements converted into code. Certain blockchains such as Ethereum allow tokens to include

smart contracts that can execute transactions. For example, a smart contract could be an option agreement. If the option condition is met, the smart contract would detect the occurrence of the option condition and automatically make the resulting transfer of payment, which would be recorded on the blockchain.

Use Cases for Blockchain Technology

Blockchain technology can support a seemingly limitless number of use cases. For example, Walmart is using a blockchain to track mangos through its supply chain. This will allow Walmart to dramatically reduce the time required to undertake a product recall if there is a food safety issue. In another example, the diamond industry has started using blockchain to record the cut, quality, and sourcing of individual gems. Among other things, this will help the industry prevent the distribution of "blood diamonds" from war zones. Currently, however, two use cases have achieved the most widespread adoption: cryptocurrencies and ICOs.

Cryptocurrencies and Initial Coin Offerings (ICOs)

Cryptocurrencies are digital currencies in which, in lieu of a central bank, encryption techniques are used to control the generation of units of currency and verify the transfer of funds. Blockchain is used to record ownership and transfers of these currencies. In a process called "mining," individuals and entities seeking tokens (miners) use special software to solve math problems; in return, these miners are issued tokens. In the case of Bitcoin, this mining process secures the Bitcoin network by approving the transactions that are recorded on the Bitcoin blockchain. There are well over 1,000 such digital currencies, and as of the end of 2017, the largest by market capitalization were Bitcoin, Ripple, Ethereum, Bitcoin Cash, and Litecoin. While Bitcoin is essentially a digital currency, Ethereum includes a coin (Ether) and the ability to run smart contracts.

Blockchain technology can also be used to facilitate corporate fundraising. Like an IPO, the ICO marks the first time an issuer releases a new cryptocurrency to buyers. The tokens sold in such an offering may be purchased on exchanges with legal tender or through the use of another cryptocurrency such as Bitcoin or Ethereum. ICOs are typically marketed through the issuance of a white paper describing a current or future use for the tokens to be issued. In many cases, funds

raised through ICOs replace conventional early-stage funding. ICOs are seemingly subject to fewer restrictions and conditions than angel and venture funding. Nearly $4 billion was raised in over 225 ICOs in 2017 alone.

SEC Regulation of ICOs

Given the large sums of money raised through ICOs, the question of the legal status of the tokens issued in ICOs has drawn outsized attention. Under applicable law, all securities offered and sold in the United States must be registered with the SEC or qualify for an exemption from the registration requirements. The majority of ICO issuers have positioned their offering as "utility tokens"—providing purchasers with future access to the issuer's product or service. As a result, they have been offered without the benefit of a registration or qualification for one of a handful of potential exemptions from registration.

The SEC began studying blockchain in 2013, when it formed the Digital Currency Working Group (since renamed the Distributed Ledger Technology Working Group). It was not until the summer of 2017, however, that the SEC began to directly assert its authority to regulate ICOs. In a July 2017 report,[1] the SEC declared that the DAO tokens issued by Slock.it were securities within the meaning of the Securities Act of 1933 and the Securities Exchange Act of 1934. However, this announcement was widely viewed as a "shot across the bow" by the SEC, establishing that ICOs could be within the regulatory scope of the SEC:

> Accordingly, the Commission deems it appropriate and in the public interest to issue this Report in order to stress that the U.S. federal securities law may apply to various activities, including distributed ledger technology, depending on the particular facts and circumstances, without regard to the form of the organization or technology used to effectuate a particular offer or sale.[2]

The SEC also made it clear that in analyzing whether a token was a security, it would apply its traditional analysis based on a four-part test delineated by the Supreme Court in the 1946 *SEC v. Howey*[3] decision. On the question of whether a transaction is an "investment contract" and therefore included within the statutory definition of a security, *Howey* held that a transaction was an "investment contract" if:

(1) it is an investment of money,
(2) in a common enterprise,
(3) with an expectation of profits from the investment,
(4) where those profits are derived solely from the efforts of the promoters or third parties.

The SEC concluded that the DAO token met all four of these criteria and, as a result, was a security. The SEC declined to take action against the DAO issuers. Most observers were not surprised at the SEC's determination—in many ways, the DAO tokens resembled equity shares in a company. However, because the DAO's was a relatively clear-cut case, it did little to resolve the security-versus-utility debate in the legal community.

Since then, several SEC actions have focused on fraudulent ICOs. In September, the SEC charged Maksim Zaslavskiy and his companies (REcoin Group Foundation and DRC World) with fraud in ICOs that were purportedly backed by investments in real estate and diamonds. In December 2017, the SEC froze the assets of PlexCrops. The SEC maintained that the company had promised unlikely returns, advertised a non-existent team of experts, and did not disclose the financial crimes of its founder. The complaint also alleged that the company violated the Securities Act of 1933 by undertaking an unregistered offering. The filing was the first by the SEC's Cyber Unit, which was formed in September 2017 to "focus the Enforcement Division's cyber-related expertise on misconduct involving distributed ledger technology and initial coin offerings, the spread of false information through electronic and social media, hacking and threats to trading platforms."[4] While these cases sent a clear message to the market that the SEC would not tolerate fraud, again they did little to clarify the security-versus-utility divide.

In December 2017, the SEC stepped in to stop the ICO of Munchee, Inc.[5] Funds raised by Munchee would be used to improve its existing app and recruit users to eventually buy advertisements, write reviews, sell food, and conduct other transactions using Munchee's MUN token. The Munchee white paper described how the MUN tokens would increase in value and highlighted the ability of MUN token holders to trade the tokens on the secondary market. The document even claimed that "as currently designed, the sale of MUN utility tokens does not pose a significant risk of implicating federal securities laws."

Applying *Howey*, the SEC found that:

> [a]mong other characteristics of an "investment contract," a purchaser of MUN tokens would have had a reasonable expectation of obtaining a future profit based upon Munchee's efforts, including Munchee revising its app and creating the MUN "ecosystem" using the proceeds from the sale of MUN tokens.[6]

Based on Munchee's marketing, the SEC found that token purchasers could reasonably believe they could profit by holding or trading the tokens, whether or not they used the tokens or participated in the MUN ecosystem. The SEC highlighted that Munchee's marketing did not target existing users of its app and that the offering was promoted "in forums aimed at people interested in investing in Bitcoin and other digital assets."

The Munchee announcement was noteworthy because it made it clear that even if a token has a utility function, it may still be a security. The SEC also zeroed in on the hype machinery that often accompanies ICOs—the "manner of sale," which in the case of MUN created the expectation of profit. Further, the SEC indicated that creating a robust secondary market for a token could lead the SEC to classify as a security a token that would otherwise be considered a "utility token."

In the months since the DAO announcement, SEC Chairman Jay Clayton made several statements in his personal capacity in which he articulated his belief that most ICO tokens were securities. On the same day as the Munchee announcement, Clayton released a "Statement on Cryptocurrencies and Initial Coin Offerings."[7] His statement was directed at two audiences—"Main Street" investors and market professionals (broker-dealers, investment advisers, exchanges, lawyers, and accountants). For Main Street investors, Clayton's statement contained a strongly worded warning to be wary of fraud and manipulation. He wrote: "As with any other type of potential investment, if a promoter guarantees returns, if an opportunity sounds too good to be true, or if you are pressured to act quickly, please exercise extreme caution and be aware of the risk that your investment may be lost." He highlighted a string of warnings that the SEC had issued to Main Street investors.[8]

In his comments on market professionals, Clayton was even blunter:

> A change in the structure of a securities offering does not change the fundamental point that when a security is being offered, our securities laws must be followed. Said another way, replacing a traditional corporate interest recorded in a central ledger with an enterprise interest recorded through a Blockchain entry on a distributed ledger may change the form of the transaction, but it does not change the substance.[9]

Chairman Clayton continued with his critique of market professionals:

> [C]ertain market professionals have attempted to highlight utility characteristics of their proposed initial coin offerings in an effort to claim that their proposed tokens or coins are not securities. Many of these assertions appear to elevate form over substance. Merely calling a token a "utility" token or structuring it to provide some utility does not prevent the token from being a security. Tokens and offerings that incorporate features and marketing efforts that emphasize the potential for profits based on the entrepreneurial or managerial efforts of others continue to contain the hallmarks of a security under U.S. law. *On this and other points where the application of expertise and judgment is expected, I believe that gatekeepers and others, including securities lawyers, accountants and consultants, need to focus on their responsibilities.* I urge you to be guided by the principal motivation for our registration, offering process and disclosure requirements: investor protection and, in particular, the protection of our Main Street investors.[10]

Evidently the chairman felt that even this blunt statement was insufficient. Speaking before the Securities Regulation Institute on January 22, 2018,[11] he continued his critique of market professionals generally, but focused almost exclusively on lawyers. Clayton zeroed in on the role of attorneys in this market and highlighted two areas where he felt they were falling short.

- There are ICOs where lawyers appear to be assisting issuers on structuring offerings "that have many of the key features of a securities offering, but call it an 'ICO,' which sounds pretty close to an 'IPO.'" At the same time, these lawyers claim the offerings are not securities, and the tokens are issued without securities law compliance.
- In other ICOs, "lawyers appear to provide the 'it depends' equivocal advice, rather than counseling their clients that the product they are pro-

> moting likely is a security. Their clients then proceed with the ICO without complying with the securities laws because those clients are willing to take the risk."

He also criticized public companies that are trying to take advantage of the blockchain hype by announcing blockchain projects or "[changing] its name to something like 'Blockchain-R-Us.'" Leaving little doubt that stepped-up enforcement was coming, Clayton added, "With respect to these two scenarios, I have instructed the SEC staff to be on high alert for approaches to ICOs that may be contrary to the spirit of our securities laws and the professional obligations of the U.S. securities bar."

Threading the Securities Needle

ICOs that are securities can still go to market without registration. Several private-placement exemptions could be utilized to sell the securities, such as Regulation A+, Regulation CF (crowdfunding), and Regulation D exemptions such as sections 506(b) and 506(c). Often these are not appealing to ICO issuers because they either restrict the amounts that can be raised, have significant and ongoing disclosure obligations, have limitations on transfer, and/or limit the identity of the buyers (*i.e.*, accredited investors). An attempt has been made to create a hybrid instrument that addresses some of these shortcomings—the Simple Agreement for Future Tokens (SAFT).[12]

Simple Agreement for Future Tokens (SAFT)

The SAFT begins its life as a security, and in most instances it will be sold only to accredited investors.[13] However, when the issuer has completed the project for which the SAFTs were issued, the SAFTs convert into tokens. Proponents of the SAFT argue that once there is a use for the tokens, the fourth *Howey* criterion (profits are derived solely from the efforts of the promoters or third parties) is not met and the tokens are considered "utility tokens." Utility tokens are not subject to registration requirements and would not have restrictions on resale or the identity of the purchasers.

While the SAFT represents a novel approach to threading the securities needle, it is important to keep in mind that the SEC has not weighed in on the validity of the SAFT. In addition, in the Munchee Order, the SEC stated: "Even if MUN

tokens had a practical use at the time of the offering, it would not preclude the token from being a security."[14] Clearly, just getting the utility "up and running" is not enough to ensure that a token issued upon the conversion of a SAFT will be a utility.

For those ICOs that are launched as utility tokens or through SAFTs, the lack of regulatory certainty leaves issuers and their advisers with significant risks. For example, if a token should have been offered as a security, intermediaries such as promoters and token exchanges may have needed to comply with broker-dealer registration requirements under the Exchange Act. Investors may be entitled to rescission (a refund of the initial investment) resulting from the participation of unregistered broker-dealers in the offering. Section 20(e) of the Exchange Act imposes "aiding-and-abetting liability" on those that knowingly provide substantial assistance to a violation of that act. In addition, such sales may violate state "blue sky" laws.[15] Many white papers flag the regulatory uncertainty around ICOs and attempt to limit or disclaim liability. The enforceability of such provisions in the face of securities law violations is questionable.

Global Focus

Blockchain is on the radar of regulators all over the globe. In the wake of the DAO announcement, regulators in Canada, the United Kingdom, Hong Kong, Thailand, Switzerland, Australia, Gibraltar, and Singapore have issued similar announcements. Although the details varied by jurisdiction, in each case regulators made it clear that ICOs were subject to the security regulations of their country, but also stressed that not all ICO tokens were necessarily securities. In the most extreme cases, South Korea and China banned ICOs—although in the case of China there is a strong belief that the ban will be somewhat rolled back.

In November, the Monetary Authority of Singapore (MAS) issued additional guidance:

> Offers or issues of digital tokens may be regulated by MAS if the digital tokens are capital markets products under the SFA (the Securities and Futures Act). Capital markets products include any securities, futures contracts and contracts or arrangements for purposes of leveraged foreign exchange trading.[16]

MAS then provided six case studies that illustrated some of the parameters for what constitutes a security. The first case study illustrates that global regulators vary in their view of what constitutes a security.

> Company A plans to set up a platform to enable sharing and rental of computing power amongst the users of the platform. Company A intends to offer digital tokens ("Token A") in Singapore to raise funds to develop the platform. Token A will give token holders access rights to use Company A's platform. The token can be used to pay for renting computing power provided by other platform users. Token A will not have any other rights or functions attached to it. Company A intends to offer Token A to any person globally, including in Singapore.[17]

MAS found:

> A holder of Token A will only have rights to access and use Company A's platform, and the right to use Token A to pay for rental of computing power provided by other users. Token A will not provide its holder any other rights or functions attached to it. Hence, Token A will not constitute securities under the SFA.[18]

This guidance does not seem consistent with SEC guidance to date and highlights another ICO risk. In the absence of guidance from the SEC, many ICO issuers prohibited U.S. purchasers. However, issuers often overlooked the fact that their global sales were still subject to inconsistent regulation globally. Further, when U.S. investors are impacted, the SEC has often worked with foreign regulators to bring actions against foreign defendants—often extraditing and prosecuting defendants and in some cases obtaining freezes of perpetrators' assets, even without knowing their identity.[19]

Accounting Concerns

Even if a company successfully escapes securities scrutiny for its ICO, other uncertainties remain. There are currently no accounting standards specific for blockchain or cryptocurrencies under U.S. generally accepted accounting principles (GAAP). In September 2017, the chief accountant of the SEC raised a list of

accounting concerns triggered by an ICO and noted that many SEC registration requirements include the requirement for filing audited financial statements.[20] This will be very difficult in the absence of applicable GAAP standards.

Other Regulatory Concerns

The SEC is not the only government agency with regulatory oversight in the blockchain ecosystem and the demarcation of regulatory authority is evolving. For example, the Commodity Futures Trading Commission (CFTC) regulates Bitcoin and has designated Bitcoin as a commodity. However, in his recent comments, the SEC Chair noted:

> Fraud and manipulation involving bitcoin traded in interstate commerce are appropriately within the purview of the CFTC, as is the regulation of commodity futures tied directly to bitcoin. That said, products linked to the value of underlying digital assets, including bitcoin and other cryptocurrencies, may be structured as securities products subject to registration under the Securities Act of 1933 or the Investment Company Act of 1940.[21]

Class Action Lawsuits

Regulatory action is not the only risk faced by participants in the blockchain ecosystem. Attorneys have begun filing private actions on behalf of investors. In February 2016, a class action lawsuit was filed against the Project Investors, Inc. cryptocurrency exchange (d/b/a Cryptsy) alleging that the defendant had stolen investors' money and fled to China. In August 2017, the court ruled that the defendant had to return 11,000 Bitcoins to investors, worth $30 million at the time.[22]

The *Cryptsy* case underscored one of the challenges in enforcing legal decisions in this space. The judgment listed the alphanumeric public keys of twelve cryptocurrency wallets[23] where the stolen Bitcoins were stored. However, the corresponding private keys are needed to transfer the Bitcoins to plaintiffs. Due to the decentralized nature of blockchain, there is no central authority for the court to order to produce these keys.

Autumn 2017 saw the first of what is likely to be many class action lawsuits related to ICOs. In early November, the first of at least four class action lawsuits

was filed in connection with the $232 million Tezos ICO. The defendants in the cases are project co-founders Arthur and Kathleen Breitman, Dynamic Ledger Solutions, which owns the rights to the underlying code, and the Tezos Foundation, a Swiss entity that was set up to carry out the raise. In the original Tezos complaint,[24] only one of the claims is for the sale of unregistered securities. The remaining claims include two accusations of fraud and claims of false advertising and unfair competition under California state law. In December 2017, there were at least three additional ICO-related class action lawsuits filed.[25] All alleged that the defendants had engaged in the issuance of unregistered securities.

Other Legal Issues

Although much of the legal attention paid to blockchain has been focused on the regulatory status of ICOs, the growth of the blockchain ecosystem raises issues across a broad range of legal specialties. What follows is a select overview of some of these issues.

Blockchain-Based Evidence

Despite the immutable nature of blockchain records, their admissibility as evidence is still governed by rules of evidence at the state and federal levels. Today in most jurisdictions, admitting blockchain evidence would require expert testimony. However, some states have passed legislation recognizing the admissibility or validity of blockchain-based records in specific contexts.

- Vermont passed legislation creating a presumption of admissibility for blockchain evidence subject to certain conditions;[26]
- Delaware passed legislation allowing Delaware corporations to issue and trade shares on a blockchain platform;[27]
- Arizona[28] and Nevada[29] passed legislation recognizing blockchain signatures and smart contracts. The Nevada legislation also blocks local government entities from taxing and licensing blockchain use.[30]

Anti–Money Laundering (AML), Know-Your-Customer (KYC), and Privacy Regulations

Blockchain-based transactions are a potential double-edged sword for anti–money laundering and know-your-customer compliance. In 2013, FinCEN, the

Financial Crimes Enforcement Network, issued a statement clarifying the applicability of the regulations implementing the Bank Secrecy Act to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies.[31] As noted above, in a public chain, participants in blockchain transactions are publicly identified by their public keys. While the identity of public key holders may be known to counterparties, they are not generally known, although there are ways to deduce identity in some instances. At the same time, blockchains can centralize user data used to verify customers and transaction data in ways that support AML and KYC compliance. For example, in February 2017, the chief of the Danish cyber crime unit revealed authorities had cracked a drug trafficking ring utilizing a tracking system that analyzes Bitcoin transactions.

Mindful of the global web of KYC and AML regulations, many token issuers and exchanges have implemented AML and KYC screening as a condition of transacting with them. The regulatory impact is clearly having an impact, as noted in the white paper of the $42 million ICON ICO in September 2017:

> There are two main reasons why ICON is adding KYC. Firstly, the SEC (U.S. Securities and Exchange Commission) is preparing to prosecute Token Sales without KYC procedures. Secondly, cryptocurrency exchanges are beginning to exclude cryptocurrencies that did not implement KYC.[32]

Complying with global data privacy regulations could pose a unique problem. Blockchain nodes can be located in many jurisdictions, and updating the chain could involve moving personal information between nodes located in different countries. It is unclear whether pseudonymizing data will be enough or how the "right to be forgotten" will be addressed.

Jurisdiction

As lawsuits emerge in the blockchain space, many jurisdictional issues need to be addressed—questions such as:

- Which courts will have subject matter and personal jurisdiction over disputes?
- Which national laws will apply?

- Where are smart contracts deemed to be transacted?
- Who has jurisdiction over DAOs (decentralized autonomous organizations—organizations that are run through rules encoded in smart contracts)?

Many ICO terms and conditions attempt to designate both choice of law and jurisdiction. Courts will have to address whether such provisions are enforceable.

Intellectual Property

Given the relatively recent growth of the blockchain ecosystem and the length of time it takes to obtain patents, it is not surprising that the number of blockchain patents is still relatively low. However, the picture is rapidly changing. By the end of 2017, James Bessen, an economist and Executive Director of the Technology & Policy Research Initiative at Boston University School of Law, had identified 265 patents related to Bitcoin and fifty-three patents related to blockchain, the earliest blockchain patent having been issued in April 2015.[33] Another study highlighted the dramatic climb in applications for blockchain patents, noting that in 2011 there were six applications, and by 2015 the number had risen to 294.[34]

Several factors will make obtaining blockchain patents challenging. First, most blockchain innovations are based on software or involve business methods. Since the 2014 Supreme Court decision in *Alice Corp. v. CLS Bank International*,[35] these innovations have become very difficult to patent. In addition, much of the basic blockchain functionality was published in the 2008 "Blockchain White Paper" under the pseudonym Satoshi Nakamato.[36] This leaves blockchain patents open to challenge on the grounds of lack of novelty. As a result, while patents for emerging technologies tend to be quite broad, patents in the blockchain space are likely to be more limited. Despite the challenges, the growing size of the blockchain ecosystem makes future patent wars seem inevitable. One early warning sign: CNBC has reported that a well-known patent troll has begun amassing blockchain patents and set up a company to develop such intellectual property.[37]

Taxes

In 2014, the IRS issued initial guidance on cryptocurrencies.[38] In this "IRS Virtual Currency Guidance," the IRS held that virtual currencies such as Bitcoin and Ether are property. In addition, the IRS offered the following as part of its answers to frequently asked questions:

- A taxpayer who receives virtual currency as payment for goods or services must include in gross income the fair market value of the virtual currency, measured in U.S. dollars, as of the date that the virtual currency was received.
- Transactions using virtual currency must be reported in U.S. dollars based on the fair market value of the virtual currency in U.S. dollars as of the date of payment or receipt.
- Gains and losses can be capital or ordinary depending on whether the virtual currency is a capital asset in the hands of the taxpayer.
- When a taxpayer successfully "mines" virtual currency, the fair market value of the virtual currency as of the date of receipt is includible in gross income.[39]

Notably, funds raised in an ICO will in most instances be taxed. The only exception might be ICOs that represent tokenized equity issuances—although the criteria to qualify for this treatment are unclear.

Reverse ICOs

"Reverse ICOs" is a term that some have used to describe situations where venture-backed companies undertake an ICO. Not surprisingly, the standard documents used in the venture industry—SAFEs, convertible notes, series seed, and NVCA Model Series A—never contemplated ICOs. This raises a host of unanticipated issues. For example, none of these documents gives shareholders/note holders the right to approve ICOs. Convertible notes and SAFEs are both intended to convert upon a "qualified financing," but an ICO would generally not fit into the definition of such a financing. Further, if an ICO is deemed an offering of a utility token, the funds raised are essentially an unsecured obligation of the issuer. If the company were to liquidate, there is an argument that token holders should receive liquidation proceeds ahead of even preferred shareholders.

Conclusion

"Uncertain" is probably the best word to describe practitioners in the nascent field of blockchain law. With questions multiplying faster than answers, definitive answers are in short supply. Compounding the difficulty is the rapid evolution of the underlying technology and the use cases to which it can be applied. Practi-

tioners in this space also must be cognizant of the "Gold Rush" mentality that has developed in the blockchain ecosystem, which unfortunately seems to have attracted a significant percentage of "bad actors." Legal advisers in this space will have to help their clients identify these bad actors, while also helping clients understand the legal risks faced by the blockchain-based businesses they are developing.

Dror Futter was a speaker at PLI's October 2017 One-Hour Briefing Blockchain, Cryptocurrencies and Smart Contracts–What Lawyers Need to Know.

NOTES

1. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81,207 (July 25, 2017), www.sec.gov/litigation/investreport/34-81207.pdf.
2. *Id*. at 10.
3. SEC v. W.J. Howey Co., 328 U.S. 293 (1946).
4. Press Release 2017-219, U.S. Sec. & Exch. Comm'n, SEC Emergency Action Halts ICO Scam (Dec. 4, 2017), www.sec.gov/news/press-release/2017-219.
5. Press Release 2017-227, U.S. Sec. & Exch. Comm'n, Company Halts ICO After SEC Raises Registration Concerns (Dec. 11, 2017), www.sec.gov/news/press-release/2017-227.
6. Order Instituting Cease-and-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933, Making Findings, and Imposing a Cease-and-Desist Order, *In re* Munchee, Inc., Securities Act Release No. 10,445 (Dec. 11, 2017) [hereinafter Munchee Order], www.sec.gov/litigation/admin/2017/33-10445.pdf.
7. Public Statement, U.S. Sec. & Exch. Comm'n, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017) [hereinafter Clayton ICO Statement], www.sec.gov/news/public-statement/statement-clayton-2017-12-11.
8. Public Statement, U.S. Sec. & Exch. Comm'n, Statement on Potentially Unlawful Promotion of Initial Coin Offerings and Other Investments by Celebrities and Others (Nov. 1, 2017), www.sec.gov/news/public-statement/statement-potentially-unlawful-promotion-icos; U.S. Sec. & Exch. Comm'n, Investor Alert: Public Companies Making ICO-Related Claims (Aug. 28, 2017), www.sec.gov/oiea/investor-alerts-and-bulletins/ia_icorelatedclaims; U.S. Sec. & Exch. Comm'n, Investor Bulletin: Initial Coin Offerings (July 25, 2017), www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings; U.S. Sec. & Exch. Comm'n, Investor Alert: Bitcoin and Other Virtual Currency-Related Investments (May 7, 2014), www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-alert-bitcoin-other-virtual-currency; U.S. Sec. & Exch. Comm'n, Investor Alert: Ponzi Schemes Using Virtual Currencies (July 23, 2013), www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf.
9. Clayton ICO Statement, *supra* note 7.
10. *Id*.
11. *Opening Remarks at the Securities Regulation Institute*, U.S. Sec. & Exch. Comm'n (Jan. 22, 2018) (text of speech by Chairman Jay Clayton), www.sec.gov/news/speech/speech-clayton-012218.
12. The SAFT Project, https://saftproject.com/ (last visited Jan. 18, 2018).
13. A search of the EDGAR database reveals at least fifteen Reg D filings for SAFTs.
14. Munchee Order, *supra* note 6.
15. In early 2018, the Massachusetts Securities Division charged a Massachusetts resident with violating securities and other laws through an initial coin offering of the "Caviar" token. Although the offering was formally not open to U.S. investors, state regulators identified at

least two U.S.-based purchasers. *See* Administrative Complaint, *In re* Caviar & Bensonoff, No. E-2017-0120 (Mass. Sec. Div. Jan. 17, 2018), http://bit.ly/2mWrBnb.

16. Monetary Authority of Singapore, A Guide to Digital Token Offerings 2 (Nov. 14, 2017), http://bit.ly/2zBaAaI.
17. *Id*. at 8.
18. *Id*.
19. *See, e.g.*, Ericka Chickowski, *SEC Freezes Assets of Unknown Eastern European Scammers in Pump-and-Dump Scheme*, Med. Mktg. & Media (Mar. 12, 2007), http://bit.ly/2GcVvfP.
20. Wesley R. Bricker, Chief Accountant, U.S. Sec. & Exch. Comm'n, Remarks Before the AICPA National Conference on Banks & Savings Institutions: Advancing High-Quality Financial Reporting in Our Financial and Capital Markets, Washington, D.C. (Sept. 11, 2017), http://bit.ly/2h2f2DX.
21. Clayton ICO Statement, *supra* note 7, at n.2.
22. The same law firm that brought the Cryptsy lawsuit also brought a class action lawsuit against the operator of the Kraken cryptocurrency exchange alleging that plaintiffs lost 3,414 ETH tokens in connection with a market flash crash.
23. A secure digital "wallet" used to store, send, and receive a digital currency.
24. Class Action Complaint, Baker v. Dynamic Ledger Sols., Inc., No. CGC-17-562144 (S.F. Cty. Super. Ct. Oct. 25, 2017), www.almcms.com/contrib/content/uploads/documents/403/4319/tezos-sfo-complaint.pdf.
25. Class Action Complaint, Rensel v. Centra Tech, Inc. et al., No. 1:17-cv-24500-JLK (S.D. Fla. Dec. 13, 2017) (alleging, inter alia, false statements made by defendants related to paid endorsements from celebrities including boxer Floyd Mayweather), www.scribd.com/document/367278725/367102541-Rensel-v-Centra-Tech-Inc-Etal-1-17-Cv-24500-JLK-S-D-Fla-Dec-13-2017-Class-Action-Complaint#from_embed; Class Action Complaint, Balestra v. ATBCOIN LLC et al., No. 1:17-cv-10001 (S.D.N.Y. Dec. 21, 2017), www.dandodiary.com/wp-content/uploads/sites/265/2017/12/ATB-Coin-Complaint-2.pdf; Class Action Complaint, StormsMedia LLC v. Giga Watt, Inc. et al., No. 2:17-cv-00438-SMJ (E.D. Wash. Dec. 28, 2017), www.dandodiary.com/wp-content/uploads/sites/265/2017/12/Giga-Watt-complaint.pdf.
26. Vt. Stat. Ann. tit. 12, § 1913.
27. Multiple amendments to Del. Code Ann. tit. 8.
28. Ariz. Rev. Stat. Ann. § 44-7061.
29. Nev. Rev. Stat. ch. 719, *amended by* 2017 Nev. Laws ch. 391 (S.B. 398).
30. Nev. Rev. Stat. chs. 244, 268, *amended by* 2017 Nev. Laws ch. 391 (S.B. 398).
31. U.S. Dep't of Treasury, Guidance FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013), http://bit.ly/2D33N7W.
32. *See ICON Adds KYC to Token Sale (Refund Policy Updated)*, Hello ICON World (Sept. 18, 2017), https://medium.com/helloiconworld/icon-adds-kyc-to-token-sale-e66085dc7a55.
33. *See* Eric Rosenbaum, *The Price of the Bitcoin Bubble: Patent Trolls Are Digging into the Blockchain*, CNBC (Dec. 19, 2017), www.cnbc.com/2017/12/19/a-new-form-of-bitcoin-mining-patent-trolls-coming-for-the-Blockchain.html.

34. *The Emerging Blockchain Patent Landscape*, Law360 (Mar. 10, 2017), www.law360.com/articles/899815/the-emerging-Blockchain-patent-landscape (registration required).
35. Alice Corp. v. CLS Bank Int'l, 134 S. Ct. 2347 (2014).
36. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (Oct. 31, 2008), https://bitcoin.org/bitcoin.pdf.
37. *See* Rosenbaum, *supra* note 33.
38. I.R.S. Notice 2014-21, 2014-16 I.R.B. 938 (Apr. 14, 2014), www.irs.gov/irb/2014-16_IRB#NOT-2014-21.
39. *See id*. at Q5–Q8.