April 2019

Skadden

The Distributed Ledger

Blockchain, Digital Assets and Smart Contracts

SEC Releases Framework for Analyzing Initial Coin Offerings

On April 3, 2019, the Securities and Exchange Commission's (SEC) Strategic Hub for Innovation and Financial Technology (FinHub) released its much-anticipated guidance (the Framework) for analyzing whether U.S. federal securities laws apply to so-called initial coin offerings (ICOs) under the U.S. Supreme Court's decision in *SEC v. W.J. Howey Co*., 328 U.S. 293 (1946) (holding that an "investment contract" constitutes a regulated security when three factors are satisfied: (1) an investment of money (2) in a common enterprise (3) with the reasonable expectation of profits derived from the efforts of others). Although the Framework provides insight into how the commission views certain factors that may arise in an ICO analysis, it is evident that a *Howey* analysis of an ICO very much remains a case-by-case facts and circumstances analysis. It should also be noted that the primary focus of the Framework is on so-called utility tokens (*i.e*., tokens that are presold but that will eventually have use to procure goods or services on a platform). The Framework is less focused on cryptocurrencies and does not address tokens used to securitize a physical asset (such as real property), since such "security tokens" are typically not offered in an ICO.

The Framework focuses heavily on the third prong of *Howey* — reasonable expectation of profits derived from the efforts of others — noting briefly that with most digital assets, the first and second prongs (investment of money and common enterprise, respectively) were typically satisfied. However, it is noteworthy that when discussing the investment-of-money prong, FinHub states that "airdrops" — where a digital asset is distributed to holders of another digital asset or simply offered at no cost — can satisfy this *Howey* factor, providing some clarity in the debate as to whether using them automatically means an ICO would not meet the *Howey* factors. Additionally, FinHub's framework notes that while courts often analyze for horizontal or vertical commonality, the commission's position is that common enterprise is not "a distinct element" of the analysis, and rather, the fact that "the fortunes of digital asset purchasers have been linked" is typically enough to satisfy the test.

With respect to the third prong (reasonable expectation of profits derived from the efforts of others), the Framework breaks the analysis into three separate parts: reliance on the efforts of others, reasonable expectation of profits and other relevant considerations. After noting that this prong is an objective test, the Framework provides characteristics of each of the subparts to provide some guidance to individuals in determining whether an ICO is an investment contract.

Reliance on the Efforts of Others

FinHub notes that a determination of whether a purchaser is relying on the efforts of others requires a focus on two questions: (1) does the purchaser reasonably expect to rely on the efforts of a promoter, sponsor, or other third party or affiliated group of third parties — which, collectively, FinHub calls an "Active Participant," and (2) are those efforts the undeniably significant ones, those essential managerial efforts that affect the failure or success of the enterprise, as opposed to efforts that are more ministerial in nature? It should be noted that FinHub's definition of Active Participant is itself broadly construed and means that the actions of nonfounders and nonmanagement, and potentially large stakeholders and core developers, needs to be taken into account.

The Framework proceeds to list a number of characteristics to be considered, noting that no single factor is necessarily determinative but that the stronger its presence, the more likely a purchaser is relying on the "efforts of others." Considerations include:

- Is an Active Participant "responsible for the development, improvement, operation, or promotion of the network," which in part turns on whether the network is fully functional at the time of the offering;
- Are there "essential tasks or responsibilities" performed and expected to be performed by an Active Participant, rather than "a decentralized community of users";
- Will the Active Participant create or support a market for, or the price of, the digital asset;
- Does the Active Participant have a "lead or central role in the direction of the ongoing development of the network or the digital asset," in particular with respect to "governance issues, code updates ... or validation of transactions";
- Does an Active Participant have a "continuing managerial role in making decisions about or exercising judgment concerning the network or the characteristics or rights the digital asset represents" (this includes activities such as compensating service providers, setting trading parameters, distributing the digital assets or acting as a validator of transactions); and
- Does the Active Participant have the ability to profit from increases in value of the digital asset.

The Framework also separates out factors to consider in evaluating whether a digital asset previously sold as a security should be re-evaluated at the time of later offers or sales. This is a reference to the concept that a token once sold as a security may no longer be a security at a point of decentralization. The Framework lays out the following factors for this analysis:

- Do the efforts of an Active Participant remain "important to the value of an investment in the digital asset";
- Does the underlying network operate in such a manner that purchasers would no longer reasonably expect an Active Participant to "carry out essential managerial or entrepreneurial efforts"; and
- Are the efforts of an Active Participant "no longer affecting the enterprise's success."

Reasonable Expectation of Profits

The characteristics FinHub lists to analyze the "reasonable expectation of profits analysis" factor include:

- Whether digital asset holders have the ability to share in profits or realize benefit from capital appreciation;
- Whether the digital asset is traded on a secondary market or offered broadly to potential purchasers rather than targeted to the expected users of the token (*i.e.*, those who will consume the products or services offered on the platform);
- The correlation between the values and quantities of the digital asset and the goods it can be used to acquire;
- Whether the funds raised are in excess of what is necessary to establish a functional network and whether proceeds are used to enhance the network;
- Whether marketing materials tout any of the following: the expertise of the Active Participants to build the network or digital asset, the digital asset as an investment, proceeds being used for development of the network, future (rather than present) functionality, ready transferability of the digital asset, profitability (rather than use) of the network and a market for trading the digital asset.

This section also concludes with characteristics for analyzing whether an ICO that was a security can be re-evaluated at a later date. Here, the Framework focuses on the following characteristics:

- Whether an Active Participant's efforts determine the value of the digital asset;
- Whether the value of the digital asset has shown a "direct and stable correlation" to the value of the goods or services for which it may be exchanged or redeemed;
- Whether the trading volume of the digital asset is correlated to the value and level of demand for the goods and services the digital asset can be used to buy;

- Whether the digital asset can be used for its intended functionality and whether any benefit from its increase in value is incidental to that functionality; and
- Whether any Active Participant has access to material, nonpublic information about the digital asset.

In some cases, it is not clear how these factors would be applied, since it might take some time after the launch of a decentralized platform to know whether the digital asset's value or trading volume has shown the requisite level of stability and correlation.

Other Relevant Considerations

The "other relevant considerations" section lists characteristics that federal courts have used to consider "the economic reality of the transaction," which look at "whether the instrument is offered and sold for use or consumption by purchasers." These characteristics include:

- Whether the distributed ledger and digital asset are "fully developed";
- Whether the digital asset is structured and designed to satisfy its intended functionality rather than to "feed speculation as to its value"; and whether it is marketed as such and has restrictions on transferability;
- Whether prospects for value appreciation are limited and "incidental" to obtaining the right to use the digital asset;
- Whether the digital asset can act as a substitute for fiat currency; and
- Where the Active Participant has facilitated a secondary market, can transfers occur only among users of the platform.

Key Takeaways

Since the Framework is not legally binding, it remains to be seen whether and how courts will rely on it in applying *Howey* to ICOs and other forms of token offerings. However, the Framework provides important insights into how the SEC is looking at these issues and reiterates the commission's view that digital assets can evolve to the point where they are so decentralized that they are no longer securities. This point of decentralization still remains an important issue, as the Framework does not definitively draw a line as to when it occurs. At the same time, the Framework makes clear that the true analysis for digital assets occurs under the third *Howey* prong and will hinge on the extent to which investors rely on the efforts of the developers and promoters of blockchain-linked digital assets. In particular, the Framework heavily emphasizes the importance of digital assets and their networks being fully functional at the time of the offering, and it focuses on whether the digital asset can be used for speculation or is limited to its main utility function.

SEC Releases 'No Action' Letter With Respect to Jet Charter Token

On April 3, 2019, the same day that the SEC released the Framework, Jonathan A. Ingram, chief legal adviser at FinHub, issued a "no action" letter with respect to a proposed digital asset token to be issued by TurnKey Jet, Inc. (TKJ), an air charter service.

In its letter to the SEC, TKJ explained that it faced "significant transactional costs and inefficiencies" regarding payment settlement and accepting wire transfer payments for those looking to procure charter jet services. TKJ's business plan is to create a private, permissioned blockchain platform where charter jet users pay for a membership in the platform and then procure TKJ tokens that could be used to purchase charter jet services from carriers. The platform would also support brokers who act to connect consumers and carriers. The TKJ tokens could only be used on the platform and would not be transferable to nonmembers, and there is no assurance they could be redeemed for cash. Only TKJ would have the authority and capability to issue TKJ tokens into circulation (which it would do at a fixed price of $1 per token) or remove them from circulation upon redemption. The development of the platform and tokens would be funded by TKJ through its own capital resources and not through any token sale. The platform is to be fully developed and operational at the time any tokens are sold.

Ingram's letter stated the SEC Division of Corporation Finance would not recommend enforcement action to the commission if TKJ sold the tokens without registration, based on the opinion of it counsel. Among the factors Ingram cited were no token sale would be used to finance development; the platform would be "fully developed and operational" when the tokens were sold; and the tokens would be immediately available for purchasing air charter services, would have a fixed price and could only be used within the platform, and would be marketed solely for their functionality.

Key Takeaways

While the Ingram letter provides some insight into FinHub's thinking in this area, most would agree that the proposed TKJ system — a closed, permissioned system where tokens cannot be used externally — is not an optimal use case for decentralized blockchain projects. Developers of such projects, particularly permissionless systems, may find little useful guidance in the Ingram letter.

Other Legal Developments

Blockvest Reconsideration Decision

On February 14, 2019, Judge Gonzalo P. Curiel of the U.S. District Court for the Southern District of California granted the SEC's motion for reconsideration in its enforcement action against Blockvest, LLC and its chairman and founder, Reginald Buddy Ringgold, III, arising out of the defendants' offer and sale of digital tokens. Judge Curiel had previously denied the SEC's motion for a preliminary injunction. (See our *2019 Insights* article "As Interest in Blockchain Technology Grows, So Do Attempts at Guidance and Regulation.") Upon further review, however, the court considered marketing materials on the Blockvest website and concluded that the SEC's evidence was sufficient to give rise to a *prima facie* showing that defendants engaged in an unregistered securities offering under *Howey*. In light of this conclusion, as well as the likelihood of future violations, the court granted the SEC's reconsideration motion and imposed a preliminary injunction from violating the Securities Act. Judge Curiel's decision highlights the care those in the cryptocurrency and blockchain space must take in advertising. It also serves to highlight the difficulties cryptocurrency defendants have in overcoming SEC enforcement actions.

Gladius SEC Order

On February 20, 2019, the SEC and Gladius Network LLC (Gladius) entered into a consent order and settlement relating to Gladius' unregistered digital coin offering in late 2017. Gladius, a Washington, D.C.-based company, raised $12.7 million to develop a network for cybersecurity and efficiency, allowing users to rent spare bandwidth, enhance delivery speed and defend against cyberattacks. Gladius agreed to return funds to those investors who purchased tokens and requested their funds back, and to register its tokens as securities pursuant to the Securities Exchange Act. Gladius will also be required to file required periodic reports with the SEC.

While the SEC issued a cease-and-desist order, it did not impose a fine on Gladius. The lack of penalty was due in part to the fact that Gladius self-reported the ICO to the SEC, took prompt remedial steps and cooperated with the investigation.

The order is significant for the fact that it did not impose a fine, suggesting that active self-reporting and cooperation with the SEC can lead to more lenient results.

Vircurex Jurisdiction Decision

On February 21, 2019, Judge Philip A. Brimmer of the U.S. District Court for the District of Colorado denied the plaintiff's motions for default judgment and class certification. The case stemmed from the collapse of an online currency exchange, Vircurex, that resulted in some $50 million of Vircurex's customers' funds being frozen since March 2014. One customer filed suit on behalf of a putative class in the District of Colorado on January 10, 2018. Vircurex (and other defendants) did not appear in the lawsuit, and on March 19, 2018, Judge Brimmer entered an initial default under Federal Rule of Civil Procedure (FRCP) 55(a) against Vircurex. However, when the plaintiff sought to effectuate the default order by moving for default judgment under FRCP 55(b), Judge Brimmer determined that the court lacked personal jurisdiction over Vircurex, as none of the U.S. Court of Appeals for the Tenth Circuit's specific jurisdiction frameworks indicated that Vircurex had purposefully directed its activity at Colorado. As a result, the court dismissed the case in its entirety. While obviously limited to the factual aspects of the case at hand, Judge Brimmer's *sua sponte* dismissal of the case emphasizes the importance litigants must place on technical aspects of lawsuits, particularly with respect to issues like venue and jurisdiction when, as is common in many cryptocurrency companies, the companies and individuals involved are located in foreign jurisdictions.

SEC Chairman Clayton Public Comments

On March 12, 2019, SEC Chairman Jay Clayton confirmed in a letter to U.S. House of Representatives member Ted Budd that he agreed with Division of Corporation Finance Director William Hinman's previous comments in his June 2018 "When *Howey* Met Gary (Plastic)" speech, which included an assessment that Ethereum (ETH) is not a security under *Howey*. The letter was sent at the behest of Coin Center, a nonprofit research and cryptocurrency advocacy group, which then published the letter. Clayton wrote, "I agree that the analysis of whether a digital asset is offered or sold as a security is not static and does not strictly inhere to the instrument. ... I agree with Director Hinman's explanation of how a digital asset transaction may no longer represent an investment contract." While still not the level of clarity that many in the cryptocurrency world are looking for, Clayton's comments reinforce the notion that sufficient decentralization removes digital assets from SEC scrutiny, providing a goalpost for those involved with ICOs.

AriseBank/AriseCoin Plea Agreement

After being indicted in November 2018, the CEO of AriseBank, Jared Rice Sr., pleaded guilty to fraud in connection with raising $4.25 million through an unregistered ICO for AriseBank's digital currency, AriseCoin. On March 11, 2019, as part of the plea agreement, prosecutors agreed to seek a five-year prison sentence for Rice. Rice had previously settled SEC civil charges against him without admitting guilt for allegedly falsely claiming that AriseBank offered Federal Deposit Insurance Corp.-insured accounts and traditional banking services beyond those associated with AriseCoin. As part of the settlement, Rice and his co-founder agreed to pay back approximately $2.7 million. In the latest agreement, Rice admitted to converting investors' funds to his own use and benefit. He is scheduled to be sentenced on July 17, 2019. The fact that prosecutors sought prison time for Rice after he had settled his civil case without admitting guilt serves to show the potential consequences individuals face when engaging in ICOs that violate securities laws.

ATBCoin LLC Decision

On March 31, 2019, Judge Vernon S. Broderick of the U.S. District Court for the Southern District of New York denied a motion to dismiss a putative class action lawsuit filed against ATBCoin LLC and others. ATBCoin LLC offered ATB Coins to the public through an ICO in 2017. The plaintiff, a purchaser of ATB Coins, alleged that the ICO constituted an unregistered securities offering in violation of federal securities laws. In denying the defendants' motion to dismiss, the court held that the plaintiff had adequately alleged personal jurisdiction because, among other things, the defendants had conducted business in New York and promoted the project both in the state and across the United States. The court further held that the plaintiff adequately alleged that ATB Coins constituted an "investment contract" (and was thus a security) under the *Howey* test because, among other things, the ICO funds were pooled together and used to launch the advertised blockchain platform, and investors expected to share in any gain in value of ATB Coins as a result of the success of the project. In his decision, Judge Broderick emphasized ATBCoin's marketing materials, which claimed that the success of the blockchain platform would lead to the success of the ATB Coins. The ruling once again underscores the risk that ICOs will be deemed "securities" by courts and highlights the importance of blockchain developers' marketing and promotional materials, which can play a critical role in such determinations.

New York Rejects Bittrex

On April 10, 2019, the New York State Department of Financial Services (NYSDFS) ordered Bittrex Inc., a cryptocurrency exchange, to stop operating in New York. Bittrex applied for a license to engage in a virtual currency business in 2015 and another license to engage in money transmission activities in 2018, and had been operating under New York's "safe harbor" rule, which allows companies with pending applications to conduct business. While operating, Bittrex had previously received multiple deficiency letters from the NYSDFS, which led to a month-long, on-site audit in February 2019. For the first time ever, the NYSDFS publicly announced the results of the audit in a letter to Bittrex's CEO, Bill Shihara. The letter denied Bittrex's pending applications and ordered Bittrex to stop operating in New York as of April 11, 2019. The NYSDFS also gave Bittrex 60 days to fully wind down and provide for the safe custody of New York residents' assets. The NYSDFS explained, "Bittrex has failed to demonstrate responsibility, financial and business experience, or the character and fitness to warrant the belief that its business will be conducted honestly, fairly, equitably and carefully," citing "nonexistent or inadequate" internal controls to prevent money laundering, poor corporate governance, and lack of employee training as reasons for the rejection. While all license denial letters are publicly available, the fact that the NYSDFS chose to publish this one proactively suggests that they are taking regulation of virtual currencies and exchanges seriously.

Blockchain Development and the California Consumer Privacy Act

When the European Union's General Data Protection Regulation (GDPR) went into effect in May 2018, there was considerable discussion within the blockchain community as to whether blockchain technology, and specifically open, permissionless systems, could be compatible with certain GDPR requirements, such as the right to have one's data rectified and whether data on a blockchain meets the GDPR definition of "anonymous." The reality was that the GDPR was drafted and debated at a time when blockchain technology was at its earliest stages of development and was therefore not a focus of data privacy regulators. Since the GDPR became effective, the French Data Protection Supervisory Authority (the CNIL)[1] and the EU Blockchain Observatory and Forum (the Observatory Report), which is run under the aegis of the European Commission's Directorate-General for Communication, published reports with preliminary thoughts on how blockchain developers should approach GDPR issues.[2] And, in its Blockchain Resolution, the EU Parliament acknowledged that it is of the "utmost importance" that compliance with the GDPR is ensured, calling on the European Data Protection Board to provide further guidance.[3]

As blockchain developers contemplate their GDPR obligations, they will also need to take into account the new California Consumer Privacy Act (CCPA), which goes into effect on January 1, 2020, with certain enforcement provisions taking

[1] Commission Nationale de L'informatique et des Libertés Report, "Blockchain: Premiers éléments d'analyse de la CNIL: 2018."

[2] The European Union Blockchain Observatory and Forum Thematic Report, "Blockchain and the GDPR: 2018."

[3] Resolution of the European Parliament of October 3, 2018, on distributed ledger technologies and blockchains: Building trust with disintermediation (2017/2772(RSP)).

effect a few months after that. The CCPA applies to every individual who is domiciled in California and every individual who is domiciled in California while outside of California for a temporary or transitory purpose. (See our CCPA Compliance Guide.) While the CCPA is less complex than the GDPR in many respects, it presents many of the same issues from a blockchain development perspective. We discuss some of those issues below:

Defining Personal Information. The CCPA's definition of personal information is very broad and does not overlap in all respects with that used by the GDPR. Of particular note is the fact that the CCPA's definition includes "unique personal identifiers," which are persistent identifiers that can be used to recognize a consumer. There is a reasonable argument that information stored on a blockchain would satisfy this requirement.

Deidentified Data. The CCPA requirements do not apply to "deidentified information," which is defined as "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer." In order to rely on this exception, a company must have (1) implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain; (2) implemented business processes that specifically prohibit reidentification of the information; (3) implemented business processes to prevent inadvertent release of deidentified information; and (4) made no attempt to reidentify the information. The question for blockchain developers is whether, given the transparency of certain transactions, there are sufficient safeguards to prevent reidentification. The GDPR presents similar issues. While that regulation does not apply to personal data that has been anonymized, the GDPR defines anonymization narrowly, stating that it is not possible to reverse the encryption process and recreate the original data (a "reversal risk"), nor link the encrypted data to an individual by studying usage patterns or combining it with other data (a "linkability risk").

The Consumer's Right to Deletion. Similar to the GDPR, the CCPA provides California consumers with the right to have their data deleted in certain cases. A central benefit of blockchain technology , however, is "immutability" (*i.e.*, once data is stored on a blockchain, it cannot be erased). While there are techniques that might satisfy the deletion requirement, such as encryption coupled with the destruction of the encryption key, it is an aspect that blockchain developers need to keep in mind.

Key Takeaways

In general, the application of the CCPA to blockchain technology will require a case-by-case and pragmatic approach, especially since the final CCPA regulations are still being finalized. In addition, developers should consider the merit of storing personal information "on-chain." However, developers should not assume the CCPA will not apply to blockchain technology, and they should seek legal guidance as how their platforms, protocols and distributed applications are in compliance.

Both reports stress that where blockchain technology is used, GDPR compliance needs to be integrated from the outset at the design and implementation stages, and that actors should store data "off-chain" whenever feasible as well as maximize the use of data obfuscation, encryption and aggregation techniques. The Observatory Report also makes the point that the burden in this area is not solely on the developers, as the regulators themselves need to deeply understand the technology and the impact of any guidance they issue.

The Observatory Report also returns a few times to the important distinction between public, permissioned blockchains in which anyone can participate as a "validating node" (to validate the blockchain's transactions) or a "participating node" (to store or add data to the chain) and private, permissioned blockchains where the validating nodes and participating nodes must be approved by a central actor or consortium (*e.g.*, a blockchain created by a group of banks to transact with one another). GDPR compliance, in many cases, will be easier where the blockchain is private and permissioned, since it is easier to identity the key actors and data protection rules can therefore more easily be applied.

Blockchain Litigation Gives Rise to Novel Discovery Questions

Private litigation and government enforcement actions have followed the increasing use of blockchain technology and, in particular, cryptocurrencies. Litigating these cases may prompt issues of first impression in the discovery context as courts apply existing principles to the unique characteristics of blockchain technology, including discovery of information that is public and transparent, the decentralized and immutable nature of blockchain transactions and the use of "smart contracts" to execute transactions.

Transparency

Because blockchain transaction records are transparent — and thus viewable to all — and decentralized — meaning that, for public blockchains, there is no central governing or managerial body — there arguably is no one in "possession, custody or control" of transaction records. As a result, a party receiving a discovery request for such information might have legitimate grounds to object to producing certain types of information that are equally obtainable by the requesting party. However, some blockchain projects involve data stored on a blockchain as well as "off-chain," which could yield discovery battles concerning where the line is drawn and what information a party actually controls.

In addition, the parties to blockchain transactions are anonymous or "pseudonymous," such that the public can only see the wallet addresses engaged in a transaction, while cryptocurrency exchanges and third parties may hold information linking wallets to identities. In certain cases, therefore, plaintiffs and enforcement agencies have sought discovery of actual ownership information. For example, plaintiffs accusing a cryptocurrency exchange of operating a Ponzi scheme were permitted to obtain disclosure of all cryptocurrency wallet addresses, trading account addresses and the identity of account holders. *See Paige v. Bitconnect Int'l PLC*, No. 3:18-cv-00058-JHM, at 3 (W.D. Ky. Jan. 30, 2018). Similarly, in *United States v. Coinbase, Inc*., No. 17-cv-01431-JSC, 2017 WL 5890052, at *6-7 (N.D. Cal. Nov. 28, 2017), the court ordered a digital exchange to provide the Internal Revenue Service with information regarding account holders' identities to the extent the account holder had a taxable gain.

Jurisdiction

The decentralized nature of blockchain networks also means that they generally involve a limitless number of computers that are globally distributed. Accordingly, these networks may not have a presence, or involve parties engaging in activities, in any one physical location. This creates questions in blockchain litigation related to personal jurisdiction, extraterritorial application of U.S. laws and judgment collection, and jurisdictional discovery may be sought where these issues arise.

In some cases, courts are able to navigate disputes over jurisdiction where a party is an identifiable "on-ramp" to a blockchain or where the conduct at issue occurred before full decentralization took place. For example, one court has held that the defendant was subject to personal jurisdiction based on factual allegations that the websites were in English, hosted in the U.S. and the offering was designed to accommodate U.S.-based participation. In finding there was proper extraterritorial application of the Securities Exchange Act, the court considered where the website was hosted and operated, and whether "a network of global 'nodes'" in the blockchain were "clustered more densely in the United States than in any other country." *In re Tezos Sec. Litig.*, No. 17-cv-06779-RS, 2018 WL 4293341, at *6, *8 (N.D. Cal. Aug. 7, 2018).

By contrast, a Colorado federal court recently dismissed on personal jurisdiction grounds a class action brought by an investor in a defunct online digital currency exchange after its operators allegedly froze customer funds while descending into insolvency. The court held there was no evidence that the account process involved any negotiations or that the defendants purposefully directed their activities at Colorado or even knew that the injury would be felt there. *Shaw v. Vircurex*, Civ. No. 1:18-cv-00067-PAB-SKC, at 9-11 (D. Col. Feb. 21, 2019).

Immutability

The ultimate admissibility of relevant evidence at trial often is considered during the discovery phase as parties collect information, and another issue of first impression may be the admissibility and authenticity of blockchain records at trial. While courts have not yet addressed the admissibility of blockchain records specifically, they are arguably more reliable than other data sources given their immutable nature and could provide an indisputable chain of custody.

In addition, blockchain records may qualify as computer-generated information that can be self-authenticated under Rule 902 of the Federal Rules of Evidence, provided that the party seeking to introduce the records can submit a written certification from a qualified person. Indeed, the state of Vermont has enacted a statute permitting blockchain records to be authenticated and admitted when accompanied by a written declaration of a qualified person, unless there is an indication of a lack of trustworthiness. Blockchain records also may be deemed analogous to statements or information generated by computers, which some courts have held do not constitute hearsay. *See*, *e.g.*, *United States v. Lizarraga-Tirado*, 789 F.3d 1107, 1109-10 (9th Cir. 2015). Interesting questions may arise, however, regarding the accuracy or completeness of information reflected on a distributed ledger in light of potential evidence of "off-chain" transactions and so-called "forks" in the ledger based on errors and other events.

Smart Contracts

Going forward, many blockchain transactions will be conducted using “smart contracts,” or pieces of code that automatically effectuate transactions on a blockchain, such as moving funds upon certain triggering events.

The use of smart contracts, and disputes arising therefrom, may create novel discovery issues relating to the contracting parties’ intent and what steps the code actually executes. Unlike traditional contracts, the “drafter” of a smart contract generally is a third-party programmer that may not be involved in any other way in the transaction at issue. Litigants will thus need to consider how to obtain (and ultimately present in court) admissible evidence regarding what might otherwise be straightforward issues of contract interpretation, including whether to rely on technical experts or other third parties to explain how the parties’ agreement is accurately reflected in a given smart contract’s code. Furthermore, because nonprogrammers may struggle to understand the technology, litigants may need to rely more heavily on expert discovery to explain how the smart contract operates and the manner in which its program carried out the parties’ supposed intent and ultimate agreement.

The Distributed Ledger
Blockchain, Digital Assets and Smart Contracts

Contacts

Alexander C. Drylewski
Partner / New York
212.735.2129
alexander.drylewski@skadden.com

Ryan J. Dzierniejko
Partner / New York
212.735.3712
ryan.dzierniejko@skadden.com

Gregory A. Fernicola
Partner / New York
212.735.2918
gregory.fernicola@skadden.com

Eytan J. Fisch
Partner / Washington, D.C.
202.371.7314
eytan.fisch@skadden.com

Nathan W. Giesselman
Partner / Palo Alto
650.470.3182
nathan.giesselman@skadden.com

Alex Jupp
Partner / London
44.20.7519.7224
alex.jupp@skadden.com

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James A. McDonald
Partner / London
44.20.7519.7183
james.mcdonald@skadden.com

Peter B. Morrison
Partner / Los Angeles
213.687.5304
peter.morrison@skadden.com

Danny Tricot
Partner / London
44.20.7519.7071
danny.tricot@skadden.com

Mark D. Young
Partner / Washington, D.C.
202.371.7680
mark.d.young@skadden.com

Jonathan Marcus
Of Counsel / Washington, D.C.
202.371.7596
jonathan.marcus@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

This communication is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This communication is considered advertising under applicable state laws.

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000