Blockchain Litigation Year in Review (Part 1): Lessons From 2019 And What's Ahead For 2020

When is a digital asset a security or a commodity? Are SAFTs safe? Does hyping blockchain create an expectation of profit? Is blockchain a trademark, trade secret or neither? Are free tokens tax-free? Who is Satoshi Nakamoto? Does cryptocurrency guarantee semi-anonymity even in discovery? Can blockchain demonstrate membership in a class action? Are blockchain regulatory bodies real or bogus? Can election candidates incentivize engagement with cryptocurrency? Do companies have a duty of care in managing customer tokens? Does hyping blockchain create an expectation of profit? These questions and many more were the subject of FinTech litigation in 2019.

2019 saw a wave of blockchain litigation in U.S. Federal District Courts, enforcement actions at the Securities And Exchange Commission (SEC), orders by the Commodity Futures Trading Commission (CFTC), revenue rulings by the Internal Revenue Service (IRS) and advisory opinions by the Federal Election Commission (FEC). While securities fraud remains the most active area for blockchain litigation, other areas of law saw an uptick in activity, including intellectual property, unfair competition, contracts, class actions, consumer privacy, consumer protection, commodities, tax, public utilities, immigration and elections law. So what have we learned about blockchain law in 2019 and what lessons can we carry forward in the decade ahead? Part one of this article covers lessons from U.S. District Court litigation, while part two focuses on learnings from SEC, CFTC, IRS and FEC administrative determinations. Part one of this article covers lessons from U.S. District Court litigation, while part two focuses on learnings from SEC, CFTC, IRS and FEC administrative determinations.

To summarize some of the takeaways from 2019, there are about a dozen different ways to get in trouble offering, selling or promoting tokens or coins that are unregistered and non-exempt. Self-reporting an unregistered ICO can save from civil penalties, while failing to disclose paid promotion of an ICO is a net loss. The penalty for noncompliance by a billion dollar ICO is pennies on the dollar, while the penalty for civil contempt is billions. A coin reward program is not necessarily an ICO. Tokens for "testing" may not count as "investing"; free tokens are not tax-free; but issuing tokens to incentivize election engagement is permitted. In addition, companies that manage customer tokens may need to exercise reasonable care.

We also learned that blockchain may be a protected mark, but not a protected trade secret. Blockchain regulatory bodies are bogus, so beware. To have a claim, invest on advice from social media moguls, if you dare. Public utilities can discriminate customers engaged in cryptocurrencies, but credit card companies cannot. Cryptocurrency guarantees semi-anonymity until a court orders discovery. A distributed ledger with no identifying information can show membership in a class action. A proof-of-concept and an office is enough to bring over a blockchain engineer on an H-1B visa. Hyping platform performance creates an expectation of profits; misrepresenting advisors is more serious than a mishap; and failing to verify accredited investor foregoes SAFT exemption.

1. "Blockchain" A Trademark And Not Just A Technology. (*Blockchain Luxembourg S.A. v. Paymium*, SAS, No. 18-cv-08612 (GBD), 2019 WL 4199902, at *1 (S.D.N.Y. Aug. 7, 2019)).

In perhaps the first trademark lawsuit over the term "Blockchain", crypto - exchange operator Blockchain Luxembourg sued rival exchange Paymium. Self-proclaimed as "the Most Trusted

Crypto Company", Blockchain Luxembourg owns and operates the coveted domain name "blockchain.com". Though Blockchain Luxembourg disclaimed exclusive right to the term 'Blockchain' during prosecution of a trademark application, it alleged that the term was still protected because it had derived secondary meaning as a source identifier for its products. The court for Southern District of New York found the allegations sufficient and denied Paymium's motion to dismiss Blockchain Luxembourg's trademark claim. The case is ongoing and the enforceability of "Blockchain" as a mark is still to be decided. For now at least, Blockchain Luxembourg has made enough claim over 'Blockchain' as a protected mark.

Blockchain Luxembourg also accused Paymium of false advertising. The allegation asserts that Paymium promoted itself as being "registered with the SEC" when it had only filed a Form D. A Form D simply notifies the SEC that a privately held company intends to raise capital by offering securities exempt from typical oversight. For example, capital raised from venture funds. False and deceiving statements about products in connection with federal and state regulations can constitute false advertisement in violation of the Lanham Act. If true that Paymium falsely claimed to be registered with the SEC, then it is form of unfair competition, as it could be misleading to consumers. What remains to be seen, however, is whether Blockchain Luxembourg can show commercial injury from Paymium's alleged assertion—a necessary element of a false advertising claim.

2. Blockchain Technology Is No Trade Secret. (*Invisible Dot, Inc. v. DeDecker*, No. 18-cv-08168-RGK-RAO, 2019 WL 1718621, at *5–6 (C.D. Cal. Feb. 6, 2019)).

While "Blockchain" as a term may have some protection, blockchain as a concept does not. As one California court clarified, "building virtual worlds" and "linking real world assets to those virtual worlds" is not distinguished from blockchain technology itself. Simply linking real world assets to a blockchain (or distributed ledger) is too general to be a trade secret.

In the lawsuit, a startup accused a former employee of trade secret theft, fraud, conversion and conspiracy. The startup, Invisible Dot Inc. ("Invisible Dot"), was developing products for recording ownership interest in real-world assets on blockchain and the defendant, its former COO, was retained the develop blockchain applications using the startup's IP. Unbeknownst to Invisible Dot, its COO was consulting on the side for another company—one believed to have ties to potential customers for Invisible Dot's technology. After making this discovery, Invisible Dot terminated its COO and filed a lawsuit alleging state and federal trade secret theft. But the court found Invisible Dot's alleged trade secret too broad to be meaningful. "Building virtual worlds" and "linking real wold assets to those virtual worlds" was, in court's view, general knowledge in blockchain.

Though California differs from other states because it requires trade secrets to be identified with particularity at the outset of a lawsuit, it's hard to imagine how Invisible Dot's alleged trade secret would have fared better in another jurisdiction. Also working against the company's claim was its own admission that its trade secret was "not limited to" to its overly general description. Hoping to maximize its scope of protection, Invisible Dot had broadened an already broad concept beyond what is protectable. So its trade secret claims were dismissed.

3. "Test" Tokens Not Necessarily An "Investment". (*Sec. & Exch. Comm'n v. Blockvest, LLC*, No. 18-cv-02287-GPB (BLM), 2019 WL 625163, at *1–3 (S.D. Cal. Feb. 14, 2019)).

Is the sale of tokens for testing a new blockchain platform an investment? Blockvest LLC ("Blockvest") didn't think so. The Wyoming-based company launched an Initial Coin Offering ("ICO") to fund development of a cryptocurrency exchange that never became operational. But when Blockvest failed to launch the exchange, the SEC sought to enjoin the company from selling more tokens.

Blockvest received more than $2 million in funds from seventeen investors and less than $10,000 from thirty-two "test participants". The SEC alleged that Blockvest had sold *both* the investors and the "test participants" unregistered securities. The court agreed as to the investors, but not as to the "test participants". The court believed a disputed issue of fact remained on whether the funds provided for testing were an investment. Still, the court enjoined Blockvest and its principal from offering and selling unregistered securities. Whether the sale of "test" tokens constitutes an unregistered investment is still at issue, but will likely turn on whether the "test participants" understood that they were contributing funds for test purposes only or whether they believed their contribution would yield a return.

4. Hyping Blockchain Creates An Expectation Of "Profits". (*Balestra v. ATBCOIN LLC*, No. 17-cv-10001-VSB, 380 F. Supp.3d 340, 346–48 (S.D.N.Y. 2019)).

In a securities class action lawsuit, purchasers of the "ATB" coin sued the coin issuer, ATBCOIN LLC and its two co-founders (collectively "ATB"), for selling unregistered securities. ATB aimed to facilitate rapid, low-cost financial transactions through blockchain and conducted an ICO to fund creation of the ATB Blockchain on which ATB coins would operate. The company touted its blockchain as "the fastest blockchain-based cryptographic network in the Milky Way galaxy," capable of delivering "blazing fast, secure and near-zero cost payments to anyone in the world." ATB raised over $20 million from coin sales and filed no registration statement with the SEC.

The complaint alleged that when the company launched the "ATB Blockchain" at the close of the ICO, the platform was not capable of the technological feats the ATB had advertised. One review described ATB's Blockchain as "a cheap reskinned [Bitcoin] wallet which is still in beta". The value of the ATB coin dropped precipitously thereafter to just 15% of its originally purchased value.

When coin holders sued the company for violations of the Securities Exchange Act, ATB tried to have the lawsuit dismissed. ATB argued that customers were not buying securities because they "had complete control over [their ATB] coins as soon as they were purchased, including the decisions of when and for how much to sell." But the court was unmoved by ATB's arguments. Rather, as alleged, purchasers had been led to believe that ATB's fabled blockchain technology would lead to profits and had no control over whether the new ATB Blockchain worked. The takeaway is that even well-intended statements hyping a blockchain's speed and efficiency can create an expectation of "profit" from an ICO "investment" (e.g., coin or token purchase).

5. Cryptocurrency Guarantees Semi-Anonymity Until Discoverability. (*ZG TOP Tech. Co. v. Doe*, No. 19-cv-00092-RAJ, 2019 WL 917418 (W.D. Wash. Feb. 25, 2019)).

For those who believe that cryptocurrency guarantees semi-anonymity, think again. Crypto-exchange ZG TOP lost 330,000 Tether ("USDT") and 100 Ether ("ETH") in a hack of its platform. By tracing the transaction trail, ZG TOP followed that the stolen cryptocurrency to single account with Bittrex, Inc. ("Bittrex")—a competing exchange. To locate the account holder and believed hacker, ZG TOP sued the unknown Doe and asked the court for expedited discovery from Bittrex. The court, finding good cause, granted the request for discovery on the identity of the unknown account holder.

Fortunate for ZG TOP, the exchange allegedly holding the hijacked tokens had an office in the U.S. Had the funds been transferred to an exchange with no U.S. presence, ZG TOP's request for expedited discovery would have been denied. Obtaining discovery from entities or individuals with no U.S. presence requires overcoming the hurdles of the Hague convention and working with foreign officials. The process can easily take six months just to get a response and the rate of success varies with from one foreign jurisdiction to another.

6. The Identity of Satoshi Nakamoto Will Not Be Decided But Billions In Bitcoin Will Be Divided. (*Kleiman v. Wright*, No. 18-cv-80176-BB, 2019 WL 4023392 (S.D. Fla. Aug. 27, 2019)).

Sometimes real life is stranger than fiction. In a lawsuit over billions, former partners David Kleiman and Dr. Craig Wright battled over ownership of a trove of Bitcoins. The estate of the now-deceased Kleiman claimed that he and Dr. Wright were partners in a Bitcoin mining venture entitling Kleiman to half the yield. Dr. Wright denied he and Kleiman were ever partners and claimed he could not access his bitcoins. But his apparent inability to access his Bitcoin fortune was beyond believable.

According to Dr. Wright, he created Bitcoin and designed it be an anonymous digital cash system with an evidentiary trail. To preserve his anonymity (until now that is), Dr. Wright alleges he took on the pseudonym, "Satoshi Nakamoto"—the enigmatic figure credited as Bitcoin's creator. (It's worth noting that Dr. Wright is not the only individual claiming to be Satoshi). After amassing well over 1,000,000 bitcoins, Dr. Wright claims he became disillusioned with his creation because it was adopted by drug dealers, human traffickers and darknet deviants for illicit activities. Despite his altruistic intentions, his invention had turned ignoble.

To save himself from his creation, Dr. Wright claims he engaged Kleiman to wipe all traces of Dr. Wright's involvement with Bitcoin from the public record. To further disassociate from Bitcoin, Dr. Wright says he put all his Bitcoin fortune into an encrypted file he entered into a "blind" trust (of which he is one trustee). He then claims to have given the encryption keys to Kleiman before he passed. Without the encryption keys, Dr. Wright alleges he cannot access his holdings. As a failsafe, however, Dr. Wright claims a bonded courier was engaged to deliver the decryption keys on an unknown date in 2020, but if that courier does not appear then his fortune is lost forever.

The Magistrate Judge didn't buy his story. Dr. Wright's claim that he neither knows the sum of his Bitcoin holding nor has access to it was too inconceivable in the court's view. The more plausible explanation was that Dr. Wright was trying to dodge discovery of his bitcoin fortune to avoid splitting with Kleiman's estate. In deciding whether to issue discovery sanctions for Dr. Wright's failure to come forward with information requested by Kleiman's benefactors, the Magistrate found it unnecessary to determine whether Dr. Wright is Satoshi Nakamoto. Nonetheless, because of Dr. Wright's implausible inability to comply with the Magistrate's prior discovery orders, the court held Dr. Wright in civil contempt and found he and Kleiman had entered into a 50/50 partnership, entitling Kleiman's estate to billions in Bitcoin if the order is adopted by the court. Dr. Wright stands by his story and is contesting the Magistrate's findings.

7. Creditors Can't Capriciously Treat Crypto Like Cash. (*Eckhardt v. State Farm Bank FSB*, No. 1:18-cv-01180, 2019 WL 1177954 (C.D. Ill. Mar. 13, 2019)).

Credit Card companies commonly charge higher interest rates for cash advances than for purchases. Seth Eckhardt had a credit card which he used to make several purchases of cryptocurrency in 2018. Under the cardholder agreement, cash advances and "quasi-cash transactions" were subject to higher interest rates. These included wire transfers, money orders, travelers' checks, foreign currency and tax payments. Cryptocurrency, however, was not addressed in the agreement.

Prior to February 2018, Eckhardt's cryptocurrency purchases had been treated as "purchases" and charged at the standard interest rate. But after February 2018, his purchases were treated as a cash advances and surcharges were applied. Eckhardt could not negotiate down the surcharges with his credit card company so he sued for breach of the cardholder agreement and violations of the Truth in Lending Act ("TILA", 15 U.S.C. § 1601(a)), a law enacted to protect consumers against inaccurate and unfair credit billing practices.

Though the court agreed that Eckhardt had sufficiently alleged breach of the cardholder agreement and violations of TILA, it left open the question of whether cryptocurrency is *cash-like*. The parties jointly agreed to dismiss the case shortly after having presumably reached a settlement.

Cryptocurrency has been treated as a security, a commodity and as property in other contexts, so it would not be unexpected if cryptocurrency is treated as "cash-like" for credit purposes. Because cryptocurrencies (and virtual currencies in general) can have different taxonomies in different circumstances and even change depending on a currency's application, institutions that transact directly or indirectly with cryptocurrency should update their policies and user agreements to address the treatment of cryptocurrency.

8. Power Company Can Discriminate Miners From Other Customers. (*Blocktree Properties, LLC v. Pub. Util. Dist. No. 2 of Grant Cty. Washington*, No. 2:18-cv-00390-RMP, 380 F. Supp. 3d 1102, 1110 (E.D. Wash. 2019), *aff'd*, No. 19-35277, 2019 WL 5704281 (9th Cir. Nov. 5, 2019)).

Mining cryptocurrency is a power-intensive operation. Much like a server farm, a crypto-mining operation can fill an entire facility with specialized computer hardware; hardware that

continuously draws power to resolve blockchain transactions. It's no wonder that the mining operations crop up in areas with record-low power rates. For this reason, Blocktree Properties LLC ("Blocktree") and other mining ventures began operations in Grant County, Washington. Grant County has some of the lowest electricity rates in the country due to its proximity to abundant hydroelectric power.

In late 2017, Grant County's Public Utility ("the Public Utility") experienced a record load on its grid. The uptick was believed to be the result of mining operations cropping up in the county. By some estimates, power usage had more than double from 600 MW to 1,500MW in a single year. To alleviate the strain on its grid, the Public Utility proposed heightened rates for cryptocurrency miners and those engaged in "evolving industry". Under the proposal, rates could increase 295%-400% over a three year period. In addition, the Public Utility proposed servicing its "traditional" customers before servicing miners. Cryptocurrency miners would pay higher rates for less service. More troubling to Blocktree and its mining cohorts, the Public Utility planned to use a subjective determination to pick out customers subject to the heightened rate schedule.

The proposed rate-hike and service change was made public so customers could submit written comments. When the proposal passed, Blocktree and other miners filed for a preliminary injunction to enjoin the Public Utility from proceeding with its plan. The miners argued that the rate change was discriminating and violated due process. Under federal law, "the rates charged and the service rendered" to customers of a public service must be "reasonable, nondiscriminatory and just to the customer and all unreasonable discriminatory and unjust rates or services are prohibited and declared to be unlawful." 16 U.S.C. § 813.

The court considered the rate hike and found it was not arbitrary, capricious or unreasonable. The court was persuade that the rate change was needed to address the sudden influx of industry threatening the stability of the county's power service. Because the court was not convinced the miners would succeed on their claims, the court denied the preliminary injunction. The 9th Circuit upheld the denial on appeal. Having lost on the preliminary injunction, Blocktree and the other plaintiffs are presently pursuing summary judgment against the Public Utility.

9. Floyd Mayweather Delivers Deathblow to Defrauded Investors and DJ Khaled Racks Up Another One: Why You Need To Take Investment Advice From Celebs on Social Media (To Have A Claim). (*Rensel v. Centra Tech, Inc.*, No. 17-cv-24500, 2019 WL 2085839, at *1 (S.D. Fla. May 13, 2019)).

Looking to make purchases with cryptocurrency more user friendly, Centra Tech, Inc. ("Centra Tech") launched an ICO to raised funds for a crypto debit card. The card would purportedly allow users to instantly use cryptocurrencies to make everyday purchases supported by Visa or Mastercard – bridging the gap between cryptocurrency and conventional payment processing. Centra Tech's widely successful ICO raised more than $32 million from thousands of investors, which may have been due to its marketing efforts. As part of its strategy, Centra Tech recruited celebrities to promote its card on social media. And who better to promote a blockchain-backed debit card than Floyd 'Money' Mayweather and Miami hit-maker DJ Khaled?

Both celebrities were compensated for promoting Centra Tech's crypto-card through social media. Mayweather tweeted a selfie holding a Centra Tech debit card in which he boasted

"*Spending bitcoins Ethereum and other types of cryptocurrency in Beverly Hills ...*" DJ Khaled similarly fashioned an Instagram of himself holding the card with the caption, "*I just received my titanium centra debit card. The Centra Card & Centra Wallet app is the ultimate winner in Cryptocurrency debit cards powered by CTR tokens! Use your bitcoins, ethereum, and more cryptocurrencies in real time across the globe. This is a game changer here. Get your CTR tokens now!*" For these promotions, Mayweather reportedly received $100,000, while Khaled received a paltry $50,000.

After the excitement died and the Centra Card never came to be, a group of the ICO investor's filed a lawsuit not only against the company and its founders, but also against Mayweather and Khaled. The complaint alleged the two celebrities violated the Securities Exchange Act by soliciting the purchase of unregistered securities. While the court agreed that Mayweather and Khaled had solicited sales of unregistered securities, the court found that the plaintiff's had not alleged reliance on those solicitations in purchasing CTR tokens. The court found it persuasive that none of the plaintiffs had actually followed Mayweather or Khaled on social media, or had seen their promotions prior to purchasing the tokens. Because the plaintiffs failed to show their purchases were made in reliance of the social media solicitations, they failed to state a claim against the two celebrities. The court dismissed all allegations against Mayweather and Khaled as a result.

Though the two social media moguls won the first round, the SEC won the last. After dodging civil liability, Mayweather was fined more than $600,000 and Khaled more than $150,000 for failing to disclose payment received for their promotions. In addition, both agreed not to promote ICOs or securities for a term of years. In the end, an undefeated pugilist took a loss and a Miami music-maker showed he doesn't always '*win win win no matter what*.'

10. Even Regulation A+ Offerings Can Flunk For Fraud. (*In re Longfin Corp. Sec. Class Action Litig.*, No. 18-cv-2933-DLC, 2019 WL 1569792, at *1 (S.D.N.Y. Apr. 11, 2019), *on reconsideration,* No. 18-cv-V2933-DLC, 2019 WL 3409684 (S.D.N.Y. July 29, 2019)).

Viewed by some as a midway between unregistered ICO and registered IPO, Regulation A+ ("Reg A+") promised a regulated way to raise funds from the public without the rigorous registration requirements of an IPO. But immune it is not from fraud.

Longfin Corp ("Longfin"), a finance and technology corporation that provides foreign exchange and finance solutions, publicly offered shares through a Reg A+. To underwrite the offering, Longfin retained broker-dealer Network 1 Financial Securities Inc. ("Network 1"). As precondition to listing its shares on the NASDAQ, Longfin needed to have at least one-million publically-held shares (not held directly or indirectly by an officer or director of the company). When Longfin was short of the requirement, it issued over 400,000 Class A shares to twenty-four individuals for $0 in consideration. Thereafter, Longfin put out false and misleading press releases announcing its acquisition of a "[b]lockchain technology empowered solutions provider" named Ziddu.com, a multi-billion dollar investment in the company, and the company's listing on performance indexes. The price of Longfin's Class A stock skyrocketed for a time but then fell as quickly as it rose and was eventually de-listed. Later it was uncovered that recipients of the 400,000 free shares included company officers and insiders—a direct violation of exchange rules.

Shareholders formed a class action and sued both Longfin and Network 1 for securities fraud. Network1, who brokered the public offering, moved to dismiss the claims against it. Initially, the court sided with shareholders and found the allegations that Network 1 was aware of Longfin's scheme sufficient to make Network complicit in the scheme. On a motion for reconsideration, however, the court reversed itself. Reviewing the record a second time, the court found that the shareholders had merely raised an inference that Network 1 knew of Longfin's fraudulent issuance of stock. The inference alone, in the court's view, could not show the requisite "scienter" needed for fraud. Because it was more plausible from the alleged facts that Network 1 was unaware of the scheme by Longfin, the allegations were inadequate to show Network 1 was a party to Longfin's scheme. All claims against Network 1 as the broker-dealer of the offering were dismissed. As to Longfin, the plaintiffs have moved for default judgment.

11. Distributed Ledger Can Show Membership In A Class Action. (*Audet et al. v. Garaza et al.*, No. 3:16-cv-00940-MPS, 332 F.R.D. 53 (D. Conn. 2019)).

In perhaps a case of first impression, the issue of whether distributed ledger technology can establish membership in a class action lawsuit was addressed.

GAW Miners LLC ("GAW Miners") launched as the brainchild of Homero Garza and Stuart Fraser. What began as a simple importation business, quickly devolved into a drawn-out Ponzi scheme. Garza and Fraser founded GAW Miner to import cryptocurrency mining hardware for sale in the U.S. When the company could not secure enough hardware it pivoted to a cloud-services model. Under a cloud-services model, GAW Miners would sell customers equipment that the company would host and maintain. When that didn't pan out, the company sold equity rights to the mining profits. Customers could purchase the right to profit from a slice of computing power operated by the company. They called this form of profit sharing a "Hashlet." Investors could buy Hashlets with Bitcoin or acquire Hashlets by converting the value of their cloud-hosted mining equipment.

Yet the scheme didn't stop there. When Hashlets didn't live up to customers' expectations, the company announced the launch of its own cryptocurrency called a "Paycoin." Before the coin's release, customers were offered "Hashpoints" – promissory notes that could be purchased or mined that could later be exchanged for Paycoin when it launched. Customers could also convert their Hashlets to Hashpoints to eventually obtain Paycoin. GAW Miners promised that the value of the Paycoin would never dip below $20 per coin and represented that banks and investment firms were backing the coin. Untoward that end, the value of the coin fell below $20, and no bank or investment firm had backed the coin. When the whole business imploded, the SEC stepped in. Garza plead guilty to wire fraud and was sent to prison.

Defrauded customers brought a class action lawsuit against GAW Miners, Fraser, Garza and another company owned operated by the two founders. As with any class action, before a group of plaintiffs can proceed together as a class, the class must be "certified" by the court. In deciding whether to certify the class, the court considered two potentially novel issues: (1) whether acquiring a security by 'mining' or 'converting' counts as a "purchase" or "sale" under the Securities Exchange Act, and (2) whether customer Bitcoin transfers to GAW Miners recorded on the Bitcoin blockchain sufficed as a record of purchase (even though the Bitcoin

blockchain doesn't record personally identifying information). The court answered both questions affirmatively. Those individuals who acquired Hashpoints and Paycoin through mining or through conversion qualified as part of the member class because the act of mining or converting still qualified as a sale or purchase, and those customers who purchased Paycoin with Bitcoin could rely on the Bitcoin blockchain transaction trail to prove their membership. Addressing these and other class-related questions, the court certified the cheated customers, allowing the customers to proceed with their claims as a class.

12. Coin Reward Program Not An Illegal ICO In Disguise. (*In re Xunlei Ltd. Sec. Litig.*, No. 18-cv-00467-PAC, 2019 WL 4276607 (S.D.N.Y. Sept. 10, 2019)).

In another securities class action against a cloud-services platform offering coins as incentives, a different result befell. Chinese internet company Xunlei Limited ("Xunlei") got its start providing a content delivery services and distributed cloud storage. As primarily a Chinese company, it offered American Depositary Shares ("ADSs") on the NASDAQ Global Select Market as "XNET". Xunlei initially operated as a subscription–based service, hosting all content and services on its network. In 2017, the company flipped its strategy from hosting to crowed-sourcing. Rather than purchasing and maintaining additional servers, Xunlei sold a personal cloud-server customers could use to host and exchange files on their own. Customers could then "Make Money" by contributing their idle bandwidth, storage, and computer power to Xunlei's content delivery service.

Xunlei followed with the launch of the "OneThing" cloud and "OneCoin" rewards program. The OneThing cloud linked customer servers through blockchain technology. Customers who contributed their idle storage and computer power could earn OneCoin similar to the way miners earn cryptocurrency for contributing storage and computing power to a blockchain.

Xunlei also created a wallet application that allowed users to send and receive OneCoin. Officially, Xunlei's reward program only supported exchange of OneCoin for other products and services that would otherwise cost money. But speculators created secondary markets for trading OneCoin that allowed customers to exchange OneCoin for money or other cryptocurrencies like Bitcoin or Ether. Xunlei never sponsored or affiliated with these third-party exchanges, but it supported extraction of OneCoin from its wallet application to these exchanges. In addition, the Xunlei's reward program mimicked some of the market dynamics of an ICO. The company, for one, created a sense of urgency and greater upside for early adopters of OneCoin.

Following the launch of the rewards program in the September 2017, XNET shares grew steadily from roughly $5 a share up to $27. That same month however, Chinese authorities banned ICOs in China. The prohibition included services supporting the trading and exchanging of coins, as well as token-based financing. Though Chinese authorities took no legal action against Xunlei, the National Internet Finance Association of China ("NIFA")—a self-regulatory organization—issued a "Risk Alert" for Xunlei's reward program, given China's ban. Xunlei's stock volleyed up and down from October 2017 through January 2018, before settling around $16 a share.

XNET investors who incurred a loss during the volatile period after launch of OneCoin sued the company and its CEO for securities fraud. Investors alleged the stock's volatility was owing to omissions and misleading statements by Xunlei about the legality of its OneCoin rewards program because of China's ICO ban. But the court for the Southern District of New York disagreed.

The court, unpersuaded by the investors, noted there were no allegations (1) that Xunlei used OneCoin to fundraise, (2) "that Xunlei ever offered OneCoin in exchange for legal of virtual tender" or (3) that OneCoin "participants obtained any rights as stock or bond holders". The court concluded that, under Chinese law, OneCoin was not an illegal ICO in disguise. Xunlei, as such, neither had to report its activities as illegal, nor made misleading statements when it reported abiding local regulations and laws and representing that OneCoin was not an ICO. Pivotal to the court's ruling was the observation that, as alleged, Xunlei used OneCoin to encourage customers to share their idle storage and computing power, and that, officially, OneCoin was exchangeable only for Xunlei affiliated products and services. The investors had alleged that Xunlei encouraged the trading of OneCoin on secondary markets set up by speculators or, at minimum, stood idly by. Yet the court viewed this inaction as inconsequential. All claims against Xunlei and its CEO were dismissed.

13. Blockchain Operators May Have A Duty Of Care In Managing Tokens. (*Fabian v. LeMahieu*, No. 4:19-cv-00054-YGR, 2019 WL 4918431, at *1 (N.D. Cal. Oct. 4, 2019)).

In perhaps another first, a California federal court considered whether coin issuers (e.g., ICOs) and exchanges must exercise reasonable care in managing customer tokens. A class action was brought against Nano (f/k/a/ RaiBlocks), BitGrail and half-a-dozen others for securities fraud and various state torts in connection with the "Nano Coin" (f/k/a "XRB").

Nano launched in 2014 as a "low-latency payment platform" that leverages blockchain. Nano and its developers were alleged to have to have promoted, offered, traded and sold to Nano Coins to the public without registering with the SEC or seeking an exemption. According to the complaint, Nano worked with the BitGrail to create a cryptocurrency exchange primarily focused on creating and sustaining a market for Nano Coins (the "BitGrail Exchange"). Nano allegedly directed the public to purchase Nano Coins on the BitGrail Exchange and store them there. The plaintiff class alleged Nano had (1) commissioned and contributed to the creation of the BitGrail Exchange, (2) provided specific investment instructions and assurances that the BitGrail Exchange was secure and could be trusted to safeguard investment assets and (3) collaborated with the BitGrail in maintaining the exchange. Nano was further alleged to have encourage individuals to purchase, sell and trade Nano Coins on the BitGrail Exchange. Nano Coin was promoted by Nano through social-networks such as Reddit and Twitter.

The lead plaintiff—in deciding to invest in Nano Coins, open an account on the BitGrail Exchange, and stake his investment holdings in XRB there—relied upon the Nano's promotions on social media channels and statements made on Nano's website representing the BitGrail Exchange as a safe and reliable platform on which to purchase and stake XRB. However, on February 8, 2018, fifteen million Nano coins stored on the BitGrail Exchange (worth approximately $170 million) were lost. According to the complaint, BitGrail announced that it had "lost" $170 million worth of Nano Coins due to "unauthorized transactions"; the loss represented

nearly fifteen percent of all Nano coins in circulation. The lead plaintiff claimed to have lost all 23,033 Nano Coins in his BitGrail wallet, worth approximately $275,000.

Nano moved to dismiss the federal securities fraud claim and state tort claims for breach of implied contract, breach of fiduciary duty, negligence, fraud and unjust enrichment. Because the plaintiff waited more than a year to sue after his last purchase of Nano Coins, the federal securities fraud clam was barred by the 1-year statute of limitations. On the breach of implied contract claim, the court found that the plaintiff had not alleged conduct inferring mutual assent of an offer and acceptance as between the plaintiff and Nano. On the breach of fiduciary duty, the court held that the plaintiff failed to demonstrate that custodianship confers a fiduciary duty under California law. Addressing unjust enrichment, the court reasoned that the appreciation of Nano's coin holdings from the plaintiff's purchase of Nano Coins did not show a monetary benefit was conferred on Nano by the plaintiff. In other words, the plaintiff at best alleged conferring an indirect benefit (by virtue of coin market dynamics) and that was not sufficiently direct.

However, on the state claims for negligence, fraud and negligent misrepresentation, the court found the allegations enough to deny dismissal. That is, the court found it plausible that Nano had a duty to exercise reasonable care in managing Nano Coins on the BitGrail Exchange. The court noted that "[i]t was foreseeable that a lack of security on the primary exchange for Nano Coins would cause harm to individuals who, like plaintiff, deposited their Nano Coins on that exchange"; that Nano's alleged conduct, if true, "could be viewed as morally reprehensible"; and that "[i]mposing a duty to exercise care in this instance will not result in an undue burden on the Nano Defendants or the industry at large."

Although the ruling is based on California law, other states favoring strong consumer protection may take a similar approach and find a duty of care where a coin issuer maintains customer coins, or, as alleged here, the coin issuer worked closely with an exchange maintaining customer coins. One way for companies to avoid this pitfall would be to simply transfer custody of coins to customers.

14. Beware of Bogus Blockchain Regulatory Bodies. (*Commodity Futures Trading Comm'n v. Diamonds Trading Investment House and First Options Trading*, No. 18-cv-00807-O, 2019 WL 3926809 (N.D. Tex. June 28, 2019)).

In more than one instance involving allegations of fraud, the offending entity or individual created a bogus blockchain regulatory body. In the SEC enforcement action against Blockvest (*Sec. & Exch. Comm'n v. Blockvest, LLC* (No. 3)), Blockvest admitted to creating a false regulatory body called "Blockchain Exchange Commission". Blockvest even used a government seal, logo and mission statement nearly identical to the SEC's. In a matter involving enforcement by the Commodity Futures Trading Commission (CFTC), a defendant operating as "First Options Trading" falsely claimed he had completed examination and training by the "Blockchain Counsel" to become a "Certified CryptoCurrency Expert." The fraudster included on his website a certificate purportedly signed by the fictitious executive director of the fabricated Blockchain Council. If fabricating bogus blockchain regulatory bodies weren't bad enough, Blockvest and First Options had also claimed to be regulated by the SEC and CFTC, landing them square in the crosshairs of the real regulators.

As of yet, there is no federal regulatory body on blockchain. The Federal Trade Commission (FTC), National Institute of Standards and Technology (NIST) and SEC have all formed blockchain working groups, but none are charged with blockchain oversight. Congress is looking to form a blockchain working group of its own, but with the objective of standardizing blockchain terminology in federal legislation much like state lawmakers have done in Arizona, Delaware, Illinois, Nevada, Tennessee, Vermont and Wyoming . Industry leaders also made steps in 2019 towards regulation, or at least, steps towards industry responsibility. A contingency of cryptocurrency exchanges formed the Crypto Rating Counsel (CRC) with the mission of clarifying whether cryptocurrencies are securities, or more like a utility token. The CRC assigns ratings from 1 to 5: 1 being very uncharacteristic of security and 5 being strongly characteristic of a security. The CRC's stated goal is "responsible growth and maturation of cryptocurrency markets and related financial infrastructure". While the CRC is not yet a self-regulatory organization (SRO) like the New York Stock Exchange (NYSE) or the Financial Industry Regulatory Authority (FINRA), which have the power to create and enforce standards and regulations, it is perhaps a step in the right direction.

15. A Proof-Of-Concept And A 4500 Square-Foot Office Is Sufficient To Secure An H-1B Visa For A Blockchain Engineer. (*Innova Sols., Inc. v. Baran*, No. 18-cv-09732-DDP-RAO, 019 WL 5748215, at *4 (C.D. Cal. Nov. 5, 2019)).

An H-1B visa allows a U.S. employer to bring over a non-citizen to work on a temporary basis for a "specialty occupation". Innova Solutions, LLC ("Innova") filed for an H-1B for Dhesinghu Alagarsamy. Alagarsamy was retained as a "Solutions Architect" to develop Innova's "proprietary software and hardware", including a "new blockchain system". The company indicated that Alagarsamy would work "in-house at [Innova's] corporate headquarters in Santa Clara, California." With its application, Innova submitted (1) a proof-of-concept PowerPoint presentation for its blockchain system, (2) a commercial lease for a 4,500 square foot work space and (3) the company's tax returns. Yet, the United States Citizenship and Immigration Services ("USCIS") denied Innova's H-1B application. USCIS believed that Innova had failed to establish an employer-employee relationship—including demonstrating that Alagarsamy would be working in-house (not with third-parties)—and to show the company had enough office space during the visa period. Innova appealed the decision for violating the Administrative Procedure Act.

The court presiding over the appeal reviewed Innova's applicant and USCIS is grounds for dismissal. On whether Innova had demonstrated an employer-employee relationship, the court found Innova's blockchain proof-of-concept presentation adequate. USCIS had dismissed the presentation simply because Innova had no product yet, which, in the court's view, was the reason for the proof-of-concept. On office space, USCIS had suggested that the 4,500 square-foot office Innova had leased was insufficient space to develop a blockchain product. On this point, the court wholly disagreed with the government's conclusion and found that the space was more than adequate. In sum, the court found the reasoning behind the government's denial of Innova's H-1B visa implausible. Innova was granted summary judgment on its claim.

Blockchain Litigation 2020

So what's ahead for blockchain litigation in 2020? Further determinations in the ongoing lawsuits addressing blockchain issues relating to trademark, unfair competition, class actions, discovery, securities, commodities, public utilities and common law duties of care. In addition, a pair of recently filed lawsuit against crypto-exchange Bitfinex, stable coin Tether, their parent company, iFinex, Inc. and others will test the waters on antitrust, racketeering and price manipulation of Bitcoin and Bitcoin futures contracts. The cases are *David Leibowitz et al. v. iFinex Inc. et al*., 1:19-cv-09236-KPF (S.D.N.Y) and *Young et al. v. iFinex Inc. et al*., 2:19-cv-01902, (W.D. Wash.). The latter case was transferred from the U.S. District Court for the Western District of Washington to the Southern District of the New York where the earlier case is being prosecuted. The defendants are scheduled to file motions to dismiss in early February and the court may decide in the second quarter of 2020 whether the claims can proceed.

Also in 2020, the Supreme Court will decide whether the SEC can lawfully seek disgorgement in civil proceedings. The question turns on whether discouragement (i.e., ceasing illegal profits) is a form of "equitable relief" or "penalty". If "equitable relief" then it is authorized remedy and if a penalty, then not, or so the parties have argued. The case, *Liu v. Securities and Exchange Commission*, Dkt. No. 18-1501, is scheduled for oral argument on March 2, 2020 and is being watched with much interest. Some see the high Court's acceptance of the petition is itself a sign that that the Court will curb the Commission from requesting disgorgement in civil lawsuit unless and until expressly authorized by Congress to do so. Though the Court's decision will not affect the SEC's ability to levy discouragement in administrative proceedings, it could impact the SEC's ability to seek discouragement in district court, including the SEC's $100 million dollar securities fraud case against Canadian mobile messenger maker Kik Interactive, and a recently filed lawsuit by the Commission against a founder for allegedly raising funds through SAFTs and using the funds for dating services and litigation settlement. The cases are *Securities And Exchange Commission v. Kik Interactive Inc.*, 19-cv-05244-AKH (S.D.N.Y), and *Securities And Exchange Commission v. Eyal et al.*, 19-cv-11325-LLS (S.D.N.Y).

In the second part of this article we will look at lessons from SEC and CFTC administrative actions against blockchain companies, from the IRS revenue ruling on taxability of tokens and from the FEC's advisory opinion on candidate cryptocurrency.