NORTON ROSE FULBRIGHT

Blockchain Law

Going after blockchain coders—and perhaps even the code?

Robert A. Schwinger, *New York Law Journal* — November 28, 2023

A number of recent cases involving blockchain platforms illustrate the difficulties that sometimes emerge in understanding what roles software coders do and don't play when it comes to such systems, and thus whether they may potentially be faced with liability.

Some 425 years ago, a villainous character in Shakespeare's "Henry VI, Part II" famously exclaimed, "The first thing we do is, let's kill all the lawyers" (Act IV, Scene II). Were Shakespeare today a lawyer litigating blockchain cases, would his character be suggesting that the first thing we should do is sue the software coders, or even the code itself?

A number of recent cases involving blockchain platforms illustrate the difficulties that sometimes emerge in understanding what roles software coders do and don't play when it comes to such systems, and thus whether they may potentially be faced with liability. These cases also show how confusion can arise in distinguishing between code itself and the actions and interests of the humans and entities who may lie behind that code.

Suing crypto coders in the United Kingdom

As noted in a prior column, R. Schwinger, "The British Are Coming — To the Aid of Crypto Scam Victims", N.Y.L.J., July 24, 2023, the England and Wales Court of Appeal created a stir earlier this year when it held there was at least a triable issue about "whether the developers who look after bitcoin may arguably owe fiduciary duties or duties in tort to an owner of that cryptocurrency" to make coding changes to a crypto platform to help redress customer injuries. *Tulip Trading v. van der Laan*, [2023] EWCA Civ 83 (Feb. 3, 2023).

In *Tulip Trading*, the plaintiffs who had lost the private keys to their bitcoin in a hack sued the platform developers to force them to make coding changes that would enable plaintiffs to access and recover their bitcoin. Plaintiff argued that these developers "ow[e] fiduciary duties to the true owners of bitcoin cryptocurrency" which "should extend to implementing the necessary software patch to solve [plaintiff's] problem and safeguard [plaintiff's] assets from the thieves."

The appellate court, reversing the trial court, cited competing factual submissions about what the true state of decentralization on the platform actually was to conclude that plaintiffs' allegations about the extent of defendants'

Robert A. Schwinger is a partner in the commercial litigation group at Norton Rose Fulbright US LLP.

More than 50 locations, including London, Houston, New York, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg.

Attorney advertising

"authority" and "discretionary decision making" over the code and their alleged ability to "introduce a change in the source code" meant that plaintiffs' fiduciary duty claim against the persons who allegedly "control this software" and can "update the software" should be permitted to proceed. It conceded, though, that recognizing such a claim "would involve a significant development of the common law on fiduciary duties."

Looking beyond common law for claims against coders in the United States

For claims against coders, US common law may not be quite as favorable as was English law in *Tulip Trading*. Two years ago, for example, this column explored cases in which plaintiffs who had suffered losses on cryptocurrency exchange platforms brought various kinds of creative common-law claims against the operators of the platform, seeking unsuccessfully to recoup their losses. See R. Schwinger, "When Plaintiffs Raise Claims of Platforms Behaving Badly", N.Y.L.J., July 19, 2021, discussing cases such as *Berk v. Coinbase*, Inc., 840 Fed. Appx. 914 (9th Cir. Dec. 23, 2020) (not for publication), rev'g 2019 WL 3561926 (N.D. Cal. Aug. 6, 2019), and *BMA v. HDR Global Trading*, 2021 WL 949371 (N.D. Cal. Mar. 12, 2021), where courts held that platform operators did not owe any non-contractual duties to platform users.

But in view of the ongoing ferment over whether digital token sales on online platforms may constitute sales of "securities" under the federal securities laws, see, e.g., R. Schwinger, "Crypto, the SEC and a Tale of Two Judges", N.Y.L.J., Sept. 25, 2023, some plaintiffs who claim to have suffered losses in their online trading activity now have attempted to seek redress under the federal securities laws from the coders behind those the trading sites, or the site operators. A recent decision and one earlier this year, however, suggest that bringing statutory claims for relief under the securities laws against coders may prove as unsuccessful as the various common-law theories that had been tried in US courts earlier.

The most recent example of this was Judge Katherine Polk Failla's decision in *Risley v. Universal Navigation d/b/a Uniswap Labs*, 2023 WL 5609200 (S.D.N.Y. Aug. 29, 2023), commonly termed the "*UniSwap* case," where the court in a strongly worded decision rejected all the claims under the securities laws that the plaintiffs had attempted to raise against operators, developers and coders of cryptocurrency exchange platforms, for damages that platform users claim to have sustained from cryptocurrency transactions conducted on the platform.

UniSwap rejected the attempt by plaintiffs (who claimed to represent a class of persons who had been the victims of "rug pull" and "pump and dump" scams on the platform) to seek rescission of the contracts for their trades under § 29(b) of the Securities Exchange Act of 1934, 15 U.S.C. § 78cc(b), based on the claims that the platform was effectively operating to an unregistered securities exchange in violation of §5 of the Exchange Act, 15 U.S.C. §78e, and that the defendants were acting as unregistered broker-dealers in violation of § 15(a)(1) of that statute, 15 U.S.C. §78o(a)(1).

UniSwap also rejected plaintiffs' attempt to obtain relief under §12(a)(1) of the Securities Act of 1933, 15 U.S.C. §77l(a)(1), based on the claims that the platform effected sales of unregistered securities in violation of §5 of the Securities Act, 15 U.S.C. § 77e.

The problems in *UniSwap* arose from the use of so-called "liquidity pools" and "liquidity providers" in decentralized crypto exchanges. As explained by the court:

> Liquidity pools allow an issuer to create a new token by contributing a pair of tokens — token A being a preexisting token with some inherent value (*e.g.*, ETH), and token B being the issuer's new token (often with little to no inherent value) — to a pool where buyers can trade their token A in exchange for the issuer's new token B.

"Liquidity providers are thus crucial to the functioning of a decentralized crypto exchange, . . . " However, "for issuers and liquidity providers to deposit tokens, and for traders to buy and sell them, each must engage with the Protocol's smart contracts, without which the Protocol could not function."

But "the liquidity providers for a given pool cannot immediately access the transaction fees," because "pursuant to [the protocol's] coded smart contracts," a structure is implemented using so-called "liquidity tokens" whereby "liquidity providers may be incentivized to not 'burn' their tokens (that is, take their liquidity out), and instead use their liquidity tokens—themselves tradeable asset elsewhere," in order to avoid a "drain of liquidity" that "can devalue the issuer's token."

The problem, as noted by the court, is that "[t]he Protocol, while innovative and more efficient than centralized systems, is nonetheless subject to fraud" through the use of so-called "scam tokens," such as through "'rug pulls' and 'pump and dumps.'" In a "rug pull," "instead of keeping their underlying liquidity assets in the pool, the issuer prematurely withdraws or 'burns' their liquidity tokens, thereby removing all liquidity from the pool and leaving other investors with now-worthless tokens." In a "pump and dump," an issuer secretly "sends millions or more of the new token to themselves," uses social media and other means to "entice investors to drive up demand," and then cashes out at a high price, "leaving investors with now-worthless tokens."

The *Uniswap* plaintiffs brought various securities law claims, arguing that the developer of the platform was aware of these schemes but did nothing to stop them because it profited from various resulting fees. They argued that "[b]y providing a marketplace for buyers and sellers, by assisting with the drafting of smart contracts, and by and through their ownership of governance tokens," the defendant developers and investors facilitated the scams by which the plaintiffs were victimized.

The court held that these allegations did not provide basis for imposing liability under the federal securities laws on the *UniSwap* developers who had created the smart contracts through which their platform ran.

For example, with respect to the plaintiffs' attempt to seek rescission of the transactions in which they were defrauded under §29(b) of the Exchange Act, the court held that the plaintiff crypto traders simply were not "in contractual privity" with the defendant developers and investors in the platform, as was required for the assertion of a statutory rescission claim. The court stated bluntly that "it defies logic that a drafter of computer code underlying a particular software platform could be liable under Section 29(b) for a third-party's misuse of that platform."

Plaintiffs likewise could not succeed on their §29(b) claim against the coders by arguing that they had been duped into entering into illegal contracts. The court, while noting that "no court has yet decided this issue in the context of a decentralized protocol's smart contracts," reasoned that since the platform was as capable of executing lawful trades as fraudulent ones, the drafting of the smart contract code used on the platform was merely "collateral" to the illegal activity and thus too "tangential" to give rise to § 29(b) liability. In the court's view, "collateral, third-party human intervention causes the harm, not the underlying platform."

Plaintiffs fared no better with their attempt to hold the developers and investors liable for selling unregistered securities in violation of § 12(a)(1) of the Securities Act. The fundamental problem, explained the court, was that the coders were not themselves parties to the complained-of sale transaction with the plaintiffs and were not the ones who transferred title to the claimed securities from themselves to the plaintiffs.

The court rejected plaintiffs' argument that "because Defendants wrote the [smart] contracts that allow the Protocol to function . . . Defendants are statutory sellers for every transaction that takes place on the Protocol," explaining:

> Just as Section 12(a)(1) does not apply to those who draft base-level agreements for traders to access the stock market, it does not apply to software coders who create an exchange to efficiently facilitate trades. In both circumstances, the party sued facilitated — but was not party to — the contested transaction.

The court further explained:

> Every aspect of the liquidity providers' transactions (other than their individual decisions as to when to deposit and when to withdraw tokens and fees) happens automatically through the code baked into the smart contracts. As Plaintiffs themselves note, the 'self-executing, self-enforcing' code of the contracts merely sets a given formula for transactions taking place on the Protocol, ... As such, that Defendants may have drafted the contracts underlying the Protocol does not mean that they have title in the assets traded there.

The court also rejected basing § 12(a)(1) liability on the claim that the defendants had "solicited" the transactions for their own benefit or that of the sellers, simply by having claimed that their platform was "safe" or "secure."

A similar ruling had been issued earlier in 2023 in *Underwood v. Coinbase Global*, 2023 WL 1431965 (S.D.N.Y. Feb. 1, 2023). While the claims there had been directed solely against Coinbase as the platform operator, similar legal issues were addressed.

The court noted that because the terms of use for the platform expressly stated that title to the tokens traded on the platform at all times remained with the users and that the platform never took title to the tokens (e.g., did not use a centralized wallet for trades), the platform could not be subject to §12(a)(1) liability as a seller, or a §29(b) claim for rescission of the transaction, since the platform itself did not sell anything to the plaintiffs and was not a party to the transaction sought to be rescinded. *Underwood's* reasoning thus aligns with the holding in *Uniswap*.

Taking action against the code rather than the coder?

A recurring issue that has been arising of late concerns blockchain systems that run essentially automatically through the use of "smart contracts," with perhaps only minimal governance over them being exercised by DAOs (distributed autonomous organizations) and the members of those DAOs. In these situations, the law is sometimes challenged as to who is responsible for what, or indeed whether anyone is responsible for anything. See R. Schwinger, "Can the Autonomous Remain Anonymous?", N.Y.L.J., May 22, 2023; R. Schwinger, "Can There Be Law Without People?", N.Y.L.J., Jan. 23, 2023.

As noted in these prior columns, some cases from the past year have taken the view that a DAO which exercises a governance role for a platform may, under appropriate facts, be subject to suit at common law as an unincorporated association or a kind of general partnership, comprised of the DAO members. See *CFTC v. Ooki DAO*, 2022 WL 17822445 (N.D. Cal. Dec. 20, 2022) (DAO subject to suit as unincorporated association); *Sarcuni v. bZx DAO*, 2023 WL 2657633 (S.D. Cal. Mar. 27, 2023) (DAO and its members subject to suit as a general partnership, and potentially liable in negligence to the plaintiffs, for claimed lack of adequate platform security). Such judicial conclusions may be driven by the sentiment voiced in *CFTC v. Ooki DAO* that, in these situations, "*someone* must be responsible" (emphasis in original).

A similar issue arose again recently in *van Loon v. Department of Treasury*, 2023 WL 5313091 (W.D. Tex. Aug. 17, 2023). That case addressed questions raised by the issuance of international economic sanctions by the Treasury Department's Office of Foreign Assets Control (OFAC) against "Tornado Cash", a cryptocurrency tumbler or mixing service that allegedly was utilized by some users to conceal their illicit transfers of cryptocurrency to sanctioned persons and countries, such as North Korea. The OFAC sanctions against "Tornado Cash" were challenged by persons who alleged they used "Tornado Cash" not for illicit purposes but simply to better protect their privacy (e.g., for anonymity in connection with sensitive political and First Amendment activity).

The plaintiff challengers argued that the nature of "Tornado Cash" was such that it could not properly be made the subject of a sanctions designation. They argued that "Tornado Cash" was not a foreign "national" or a "person" subject to being sanctioned under the terms of the relevant underlying economic sanctions statutes and executive orders, nor was it the "property" of such persons; that "the smart-contracts components of the designation are not 'property' that can be regulated" under those legal authorities; and that "Tornado Cash cannot have a property interest in those components."

Contending "that Tornado Cash is a decentralized, open-source software project comprised of a subset of smart contracts, or 'pools,' on the Ethereum blockchain," plaintiffs argued "that Tornado Cash is not an entity but an autonomous software."

The U.S. government took a very different point of view. It argued that "Tornado Cash is an entity that may be designated and that it has a property interest in the smart contracts," characterizing "Tornado Cash" as "an organization that runs a cryptocurrency mixing service."

On cross-motions for summary judgment, the court rejected the challengers' attempt to portray the government's sanctions designation as an attempt to sanction mere software code, and thus upheld the sanctions designation. It found that "Tornado Cash is an entity that may be properly designated as a person" under the sanctions regime.

The court termed Tornado Cash "an association within [the] ordinary definition" of the term, and as such the kind of legal person or entity that was subject to being sanctioned. The court held that this entity's members were "its founders, its developers, and its DAO," noting "substantial evidence" that they constitute "'[a] body of persons who have combined to execute [the] common purpose' of developing, promoting, and governing Tornado Cash," noting in this regard that "Tornado Cash has been able to place job advertisements, maintain a fund to compensate key contributors, and adopt a compensation structure for relayers, among other things."

Thus, as "an association within the ordinary meaning of the term," Tornado Cash was "therefore an entity that may be designated per OFAC regulations."

The court further held that the smart contracts through which Tornado Cash operates were "property" within the meaning of the statutes and regulations, and specifically were property of the Tornado Cash entity that the court had described. The challengers had argued that "smart contracts are not property because they are incapable of being owned," and that in any event "Tornado Cash does not have a 'legal or equitable claim or right in property' to them." But citing the broad definitions of "property" and "interest in property" set forth under OFAC regulations, the court upheld the designation.

While "Plaintiffs argue that the smart contracts cannot be considered property because they are immutable and therefore cannot be owned," the court stated that "OFAC's definition of property encompasses 'contracts of any nature whatsoever,' and—as other courts have recognized — smart contracts are merely a code-enabled species of unilateral contracts." Further, "[e]ven if not every smart contract can be considered a contract, the record shows that Tornado Cash promoted and advertised the contracts and its abilities and published the code with the intention of people using it—hallmarks of a unilateral offer to provide services."

Building upon the plaintiffs' own argument that "smart contracts are 'like a vending machine' because 'the smart contract automatically carries out a particular, predetermined task without additional human intervention,'" the court noted that this argument simply "reinforces the court's point":

> Vending machines are examples of unilateral contracts. And like vending machines, a smart contract is a tool that carries out a particular, predetermined task. The fact that smart contracts do so without additional human intervention, like a vending machine, or that they are immutable, does not affect its status as type of contract and, thus, a type of property within the meaning of the regulation.

The court further held that "Tornado Cash has a beneficial interest in the deployed smart contracts because they provide Tornado Cash with a means to control and use crypto assets." It noted that "Tornado Cash receives a regular stream of revenue from the smart contracts," and that the term "interest in property" in the relevant statutes has been construed "to encompass this kind of economic potential." Thus, "Tornado Cash has a beneficial interest based on its expectation that the smart contracts it deployed will continue to generate this revenue."

The court rejected plaintiffs' proffered analogy that this was akin to saying a power company has a "property interest in the weather" because it may "profit from hot summer weather." "Tornado Cash may not own the crypto-economy, but, within the meaning of the statute, it has a property interest in smart contracts, which are simultaneously contracts and tools that allow it to provide privacy to its users."

Most fundamentally, the court took issue with plaintiffs' argument that the Tornado Cash sanctions were an attempt to sanction "abstract and ownerless software code," which they claimed was really no different than "intangible concepts" of any other kind. The court stated:

> This argument is circular, as it relies on the assumption that the smart contracts are indeed 'abstract and ownerless,' which the record does not support. Furthermore, unlike abstract ideas, deployed smart contracts convey an ongoing benefit for Tornado Cash, in the form of fees transmitted to

> the DAO. Tornado Cash has a property interest in this ongoing benefit.

Accordingly, the plaintiffs' attempt to challenge the Tornado Cash sanctions on the ground that "Tornado Cash" was nothing but mere abstract software code was rejected.

Conclusion

When faced with novel areas of the law, and applications of law in novel contexts, lawyers often turn to metaphors and analogies. Sometimes they prove apt and sometimes not. These recent cases about how best to think of the role played by coders in various FinTech applications and the nature of the software code in those applications show that properly conceptualizing code and coders can be trickier than it may first appear.

As we continue to move forward into a more computer-driven future, whether involving blockchain technology or other areas, courts and advocates will continue to have to struggle with how best to think about the nature and role of coders and code in the systems being created.

NORTON ROSE FULBRIGHT

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3500 lawyers and other legal staff based in Europe, the United States, Canada, Latin America, Asia, Australia, Africa and the Middle East.

Law around the world

nortonrosefulbright.com

Norton Rose Fulbright Verein, a Swiss verein, helps coordinate the activities of Norton Rose Fulbright members but does not itself provide legal services to clients. Norton Rose Fulbright has offices in more than 50 cities worldwide, including London, Houston, New York, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg. For more information, see nortonrosefulbright.com/legal-notices. The purpose of this communication is to provide information as to developments in the law. It does not contain a full analysis of the law nor does it constitute an opinion of any Norton Rose Fulbright entity on the points of law discussed. You must take specific legal advice on any particular matter which concerns you. If you require any advice or further information, please speak to your usual contact at Norton Rose Fulbright.

56041_US – 11/23