NORTON ROSE FULBRIGHT

Blockchain Law

No virtual causation for virtual assets?

New York Law Journal

May 27, 2025 | By **Robert A. Schwinger**

The author states "Rather, for the most part, courts appear still to be seeking to apply longstanding principles about legal causation that were created decades ago, in contexts very different from the modern decentralized blockchain-based transactions from which injury claims may now arise."

Introduction

When a virtual asset transaction is claimed to cause injuries to a plaintiff, what kind of causation must be shown between the injury and persons having some relationship to the transaction in order for the plaintiff to get relief from them?

When transactions take place on decentralized systems that involve many persons playing different roles, how does the law assess which of them properly may bear some responsibility when transaction activity is alleged to have caused the plaintiff's injury?

Will courts find that, if a platform or its developers or operators have provided the infrastructure through which harm is done, they have virtually caused the harm?

A cluster of recent court rulings in different contexts illustrate that courts are not generally embracing loose theories of what might be termed "virtual causation" for such claims.

Rather, for the most part, courts appear still to be seeking to apply longstanding principles about legal causation that were created decades ago, in contexts very different from the modern decentralized blockchain-based transactions from which injury claims may now arise.

Actual and proximate cause

At common law and under many US statutes, the required element of causation has two components. The first is actual causation, in which the court assesses whether the defendant's actions were a "but-for" cause of the harm.

Robert A. Schwinger is a partner in the commercial litigation group at Norton Rose Fulbright US. Lindsay Bracken, an associate in the firm's litigation group, assisted in the preparation of this column.

The second component, which presents a more complex inquiry, is proximate causation. Proximate cause analysis looks at whether the harm suffered was a reasonably foreseeable result of the defendant's actions, and whether any intermediary or intervening actions or events represented a break in the causal chain. See, e.g., 57A Am. Jur. 2d Negligence §393 (2025).

Proximate cause analysis becomes all the more complex, though, when performed in the context of blockchain-based systems. Sometimes plaintiffs involved in blockchain-based transactions who have been injured may have no meaningful ability to obtain recourse from the core wrongdoers. e.g., because they cannot be identified or located, or have no assets against which a judgment might be enforced.

Such plaintiffs thus may turn instead to seeking recovery from the platforms that host and enable these transactions, or from persons involved with those platforms. Courts are then forced to reckon with whether to hold these platforms or parties related to them liable, despite what may be an attenuated relationship with the wrong perpetrated by the true wrongdoer.

The challenge in doing so, however, arises from the decentralized nature of blockchain systems. In many respects, blockchain systems can operate essentially autonomously without central control.

They may link together the actions of multiple persons, and those actions may not even all occur at the same time or in coordination.

Therefore, even when blockchain platforms may be used to facilitate illegal schemes, the link between actions of those platforms or persons related to them and the harm flowing from the illegal activities may seem attenuated, perhaps to the point where proximate causation may no longer be said to exist between the plaintiff's claimed injury and the defendant's complained-of conduct.

A number of recent court decisions have wrestled with the attenuation issues between conduct and injury that such claims present.

Platforms where scam token transactions have occurred

The Second Circuit's recent decision in *Risley v. Universal Navigation Inc.*, 2025 WL 615185 (2d Cir. Feb. 26, 2025), involved claims by plaintiffs who alleged they were injured by transactions in "scam tokens" involved in "rug pull" and "pump and dump" schemes.

These plaintiffs bought these scam tokens on a cryptocurrency trading platform called the Uniswap Protocol, in which users trade tokens through token swaps.

The plaintiffs alleged that the Protocol's smart contracts performed these token swaps through "liquidity pools," where users are matched in a "peer-to-peer system" that "determines the relative prices of the tokens, sets the rate for the exchange, and facilitates the trade if approved by the user," all without any "direct interaction with the original token issuer, the liquidity provider," or with the lead defendant that was alleged to operate the Protocol.

This, they alleged, "allow[ed] the Protocol to operate as a decentralized exchange." The plaintiffs further alleged that certain additional defendants, including the lead defendant's CEO and certain venture capital investors, exerted operational control over the Protocol, including by having developed the automated "smart contract" computer code that facilitated these transactions.

Plaintiffs charged that in these scam token transactions conducted on the Protocol, these defendants had engaged in selling unregistered securities under §§5 and 12(a)(1) of the Securities Act of 1933, 15 U.S.C. §§77e, 77l(a)(1).

They also sought contractual rescission under §29(b) of the Securities Exchange Act of 1934, 15 U.S.C. §78cc(b), and made claims under the "control person" liability provisions of both statutes, 15 U.S.C. §§77e, and 15 U.S.C. §78t. The Second Circuit affirmed the District Court's rejection of all these claims.

Citing *Pinter v. Dahl*, 486 U.S. 622 (1988), the Second Circuit noted that to obtain recovery for claimed violations of §12(a)(1) of the Securities Act, "plaintiffs must prove that defendants either were the sellers of the tokens in question" — i.e., "were

'the owner who passed title, or other interest in the security, to the buyer,'" — "or that, for their own financial gain, [they] actively solicited the sale of the tokens to plaintiffs."

However, such liability would not extend to "participants[] collateral to the offer or sale" of the securities.

The court refused to find the defendants to be statutory "sellers" in these circumstances. It noted that in this decentralized platform, "the hosts of the Protocol do not hold title to the tokens placed in the liquidity pool by third party users of the platform.

Rather, the token issuers and liquidity providers make each particular token available for purchase." Thus, "the token issuers and liquidity providers . . . retain title of their tokens through pool tokens that may be turned in at any time of their choosing to recover the value of their originally-deposited tokens that created the trading pool."

The court held that the fact that smart contracts were involved did not change this. "The role of the smart contracts in the Protocol accords with that of base-level agreements for traders who access the stock market, whose '[function] is solely to execute the trades,' and is collateral to the actual token sale."

To impose liability here, it said, would be like holding NASDAQ and the New York Stock Exchange liable for "fraudulent stock purchases on their exchanges." This would remain true, said the court, even if title to the tokens had "temporarily passed" to the Protocol for a "split-second" in the course of the transaction.

Even then, it said, "they would be 'participants only remotely related to the relevant aspects of the sales transaction[s],'" i.e., too attenuated from plaintiffs' purchase of the scam tokens to be subject to liability.

Plaintiffs fared no better in accusing the defendants of having "solicited" the scam token transactions in violation of §12(a)(1).

The court held that defendants' having promoted their platform on social media, or having used the platform to sell a token of their own, did not render them statutory sellers in this context, holding that "such conduct is too attenuated from plaintiffs' purchase of scam tokens to show that defendants 'successfully solicit[ed] the purchase [of a security], motivated at least in part by a desire to serve [their] own financial interests or those of the securities owner.'"

The court then rejected plaintiffs' separate claim for rescission of contract for the allegedly unlawful transactions under §29(b) of the Exchange Act, which plaintiffs had based upon the "smart contracts" through which the Protocol operated.

Plaintiffs alleged that these smart contracts were "self-executing and self-enforcing computer programs that autonomously write the terms of an agreement between the traders of a certain cryptocurrency token into the program's code, obviating the otherwise traditional, centralized role that exchanges, broker dealers, and their banks, lawyers, or accountants would play in facilitating trades."

The rub, however, as noted by the Second Circuit, is that "only unlawful contracts may be rescinded, not unlawful transactions made pursuant to lawful contracts." In a §12(a)(1) claim, "the purportedly unlawful contract is between the token issuer or liquidity provider and the purchaser—not between the purchaser and defendants."

But the plaintiffs here, it said, "have failed to adequately allege the existence of an unlawful contract between defendants and plaintiffs capable of recission under Section 29(b)."

Here, said the court, "th[e smart] contracts are not subject to recission because they are more analogous to overarching user agreements than to securities transactions conducted by traditional broker dealers."

It noted that "the transaction-specific terms of a token swap are not determined as a result of the conduct of defendants" in creating the smart contracts. Thus, "defendants' smart contracts were, at best, collateral to the third parties' scam token activities and the type of tangential activity that falls outside of Section 29(b)."

For all these reasons, the Second Circuit held, "it 'defies logic' that a drafter of a smart contract, a computer code, could be held liable under the Exchange Act for a third-party user's misuse of the platform." The court thus affirmed the district court's dismissal of plaintiffs' federal securities claims.

Exchanges receiving proceeds of "pig butchering" schemes

Licht v. Binance Holdings Ltd., 2025 WL 625303 (D. Mass. Feb. 5, 2025), *report and recommendation adopted*, 2025 WL 624025 (D. Mass. Feb. 26, 2025), involved a motion to dismiss RICO claims brought by plaintiffs who claimed that they lost money in so-called cryptocurrency "pig butchering" schemes, and that the assets stolen from them were ultimately "laundered" through the Binance cryptocurrency exchange.

In "pig butchering" schemes, "scammers lure victims into investing money, often beginning with contact on social media." Next, they "convince the victims to invest money in supposedly safe and lucrative opportunities.

Then, they falsify information showing that the 'investments' are increasing in value, luring the victims into investing more money. Eventually, the scammers disappear, along with the money."

Plaintiffs did not allege, however, that Binance or any of its personnel were themselves the "butcherers," or that they purportedly lured a plaintiff, on Instagram, into buying and transferring cryptocurrency, before laundering and cashing out the cryptocurrency and disappearing.

Rather, they alleged that Binance and its related defendants had willfully failed to comply with United States laws imposing certain requirements on money transmitting businesses (MTBs).

They alleged that if the defendants had complied with the laws, their cryptocurrency transactions, which had first passed through various intermediary exchanges, "would have been flagged as suspicious by Binance, the scammers' accounts would have been frozen, and the suspicious transactions would have been reported to regulators, allowing law enforcement officials to investigate and then seize the cryptocurrency and return it to plaintiffs, thus stopping the schemes before the 'butchering.'"

Plaintiffs sought relief against the Binance defendants under RICO's private cause of action provision, 18 U.S.C. §1964(c), which provides a treble-damage remedy to any person injured in his business or property "by reason of" a substantive RICO violation under 18 U.S.C. §1962.

The court noted that under this provision, a civil RICO plaintiff must "show that the defendant's actions were not only a 'but for' cause of the plaintiff's injury, but the proximate cause as well" (cleaned up) (citing, inter alia, *Holmes v. Sec. Inv. Prot. Corp.*, 503 U.S. 258 (1992)).

The court explained:

> "Proximate cause is a flexible concept that does not lend itself to a black-letter rule that will dictate the result in every case, yet the central question in the RICO context is whether the alleged violation led directly to the plaintiff's injuries. Proximate cause requires some direct relation between the injury asserted and the injurious conduct alleged. A link that is too remote, purely contingent, or indirect is insufficient." (Cleaned up.)

Despite plaintiffs' argument that proximate causation is typically an issue of fact for the jury, the court stated that in an appropriate case a lack of proximate causation can be found as a matter of law based on the pleadings in a motion to dismiss.

In addition to noting "the absence of non-conclusory, non-speculative allegations in support of a plausible conclusion that the scammers' transactions in these pig butchering schemes would have been flagged as suspicious by Binance and their accounts would have been frozen and the suspicious transactions reported to FinCEN," the court determined proximate cause to be absent given their allegations in any event:

> "The cause of plaintiffs' injury was a set of actions (pig butchering schemes) entirely distinct from the operation of Binance as an unlicensed, unregistered MTB (defrauding the United States), and even entirely distinct from putative money laundering."

The court elaborated on the "attenuation" in causation presented by these allegations. Even though defendants' "fraud on the third party–the United States–purportedly made

it easier for a fourth party–the scammers–to cause harm to the plaintiffs, the pig butchering scheme victims," the defendants' "obligation was to register with FinCEN, not the pig butchering scheme victims, and the victims' harm was directly caused by the scammers, not [the defendants]."

Plaintiffs' allegation that the stolen assets first passed through one or more intermediary exchanges before reaching Binance further attenuated the chain of causation, the court noted. "Plaintiffs do not explain how Binance's non-compliance with United States laws or putative money laundering would have contributed to the intermediary cryptocurrency exchange's non-compliance."

Faced with all these difficulties, the court concluded that "plaintiffs have failed to plausibly allege causation" in their claims against the Binance defendants, and accordingly determined that dismissal was warranted.

Regulatory non-compliance allegedly enabling terrorist acts

Binance appeared in another recent decision that presented a more mixed and nuanced causation analysis. The plaintiffs in *Raanan v. Binance Holdings Ltd.*, 2025 WL 605594 (S.D.N.Y. Feb. 25, 2025), brought claims against Binance under the civil liability provision of the Antiterrorism Act (ATA), 18 U.S.C. §2333(a)), and the Justice Against Sponsors of Terrorism Act (JASTA), 18 U.S.C. §2333(d)).

The plaintiffs were "40 alleged victims, or representatives of victims, of the October 7, 2023 attacks perpetrated by Hamas and Palestine Islamic Jihad ('PIJ') in Israel," who "allege[d] that the defendants' provision of financial services to Hamas and PIJ substantially contributed to those attacks."

Plaintiffs alleged "that the defendants knew, or at least willfully disregarded, that Hamas and PIJ were using Binance to finance their terrorist activities" through cryptocurrency transactions, but that they "knowingly flouted" their legal obligations "to establish anti-money laundering (AML) programs, perform due diligence on customers through 'Know Your Customer' (KYC) investigations, and file suspicious activity reports (SARs) with regulators, among other things."

They alleged that "Binance's willful failure to implement the necessary internal controls and disclosure requirements . . . enabled Hamas and PIJ to use the platform to fund their terrorist activities, including the Oct. 7, 2023 attacks," and thus sought to impose liability on Binance under the ATA and JASTA.

An ATA civil liability claim requires "plaintiffs [to] allege plausibly that they were injured 'by reason of an act of international terrorism'" (quoting 18 U.S.C. §2333(a)). The court noted that "[t]he words 'by reason of' . . . restrict[] the imposition of [ATA] liability to situations where plaintiffs plausibly allege that defendants' actions proximately caused their injuries.'" (Quotations and citations omitted.)

Citing other cases where courts had rejected ATA claims against banks who were accused of providing financial services to terrorists, the court held:

> "The plaintiffs' allegations do not support the conclusion that the defendants committed a terrorist act. The Amended Complaint alleges that the defendants enabled customers associated with Hamas and PIJ to engage in cryptocurrency transactions. * * * [P]laintiffs allege only that Hamas and PIJ (or wallets associated with Hamas and PIJ) were able to transact on the Binance platform, not that the defendants donated money directly to Hamas or PIJ[, or] facilitated transactions . . . clearly earmarked for terrorist activity." (Quotations and citations omitted.)

The court further held that "the Amended Complaint fails to allege that the defendants' conduct proximately caused the plaintiffs' injuries," stating that "[a]s alleged, the causal link between Binance's provision of financial services and the plaintiffs' injuries is too attenuated to support a plausible finding of proximate cause."

> "At most, the plaintiffs' allegations plausibly support the following inferences: Hamas and PIJ (and affiliates of Hamas and PIJ) engaged in cryptocurrency transactions on the Binance platform to fund the groups' operations; the defendants knew that terrorist groups and affiliates were transacting on the platform; the defendants knew that Hamas and PIJ might use those funds for terrorist activity; and the defendants nonetheless continued to facilitate these transactions."

This, said the court, was insufficient to plead "nonconclusory allegations that the defendants' actions were a 'substantial factor' in causing the October 7, 2023 attacks and that the attacks would have been 'reasonably foreseeable' to the defendants as a 'natural consequence' of the defendants' actions," so as to make out an ATA violation.

However, the court's analysis was more favorable to the plaintiffs on their claim under JASTA, which provides for civil liability against "'any person who aids and abets, by knowingly providing substantial assistance' to an act of international terrorism" (citing 18 U.S.C. §2333(d)).

This provision imposes liability upon a defendant who "consciously and culpably participated" in a terrorist act that injured the plaintiff "so as to help make it succeed" — an analysis that "call[s] for the balancing of 'the nature and amount of the assistance on the one hand and the defendant's scienter on the other.'"

The court allowed the JASTA claim against Binance to proceed.

It noted that the Amended Complaint "sufficiently alleges that the defendants were generally aware that they were playing a role in international terrorism at the time when Hamas and PIJ (and their affiliates) were transacting on the Binance platform," and alleged "that the defendants failed to comply with—indeed, intentionally evaded—[AML, KYC and SAR] regulatory requirements, thus fostering a financial ecosystem on which illicit actors, including terrorist organizations like Hamas and PIJ, transacted freely."

Moreover, the plaintiffs alleged that the defendants did this "intentionally . . . in order to retain illicit actors on the platform" as customers.

Thus, despite the lack of a "close nexus" between the defendants' activities and the Oct. 7, 2023 attacks, the court held that "the plaintiffs have alleged plausibly that the defendants knowingly and substantially assisted the Oct. 7, 2023 attacks." The defendants' motion to dismiss the JASTA aiding-and-abetting claim against the defendants was therefore denied.

Conclusion

While it has become fashionable among some to decry the application to the FinTech world of certain legal doctrines that were developed many decades earlier in contexts utterly unlike that of modern decentralized, autonomous and often international blockchain-based transactions, there has been little hesitation so far to apply age-old legal principles of proximate causation and attenuation to avoid liability to modern-day plaintiffs for injuries claimed to have arisen out of this new technology.

Recent cases suggest that causation principles and limitations developed in the context of local railway, automobile and factory accidents — that would have been familiar a century ago to Cardozo and Oliver Wendell Holmes — continue to hold sway for the most part even in this new modern setting.

Will there come a point where courts decide that the commercial and financial changes presented in a world of decentralized, autonomous blockchain-based system require a different and perhaps more liberal approach to thinking about causation in that world — that some kind of more attenuated "virtual causation" might in that setting suffice?

We can look back a century ago, for example, when Cardozo loosened the strictures of direct privity for consumers bringing claims in a new mass production economy that was operating through layers of distribution not previously seen, in cases like *MacPherson v. Buick Motor Co.*, 217 N.Y. 382, 111 N.E. 1050 (1916) (product liability), and *Glanzer v. Shepard*, 233 N.Y. 236, 135 N.E. 275 (1922) (tort duties owing to commercial third parties), while at the same time insisting that the permissible bounds of attenuation in law must not be unlimited, see, e.g., *Palsgraf v. Long Island R.R.*, 248 N.Y. 339, 162 N.E. 99 (1928) (bystander's ability to recover for injuries sustained in the vicinity of negligent conduct was limited by the reasonable foreseeability of the risk); *Ultramares Corp. v. Touche*, 255 N.Y. 170, 174 N.E. 441 (1931) (third parties have no negligence claim against accountant who erroneously certified client's balance sheet).

Bearing in mind Oliver Wendell Holmes' famous admonition that development in the law is driven by factors such "experience[,] [t]he felt necessities of the time, the prevalent moral and political theories, [and] intuitions of public policy, avowed or unconscious," O.W. Holmes, *The Common Law*, Lecture I (1881), might some latter-day jurist at some point determine that something similarly expansive needs to be done in regard to attenuation principles to facilitate effective avenues of recovery by injured persons in our new blockchain world?

Seventeen years after the putative invention of blockchain in 2008, we are still in early days. Legitimately injured plaintiffs in search of effective recovery will no doubt continue to push at the boundaries of legal responsibility in blockchain-related cases.

It remains to be seen whether at some point judges might advance any revolution in legal thinking applicable to this area, or whether cases like the recent ones that stick with longstanding notions of causation requirements will continue to hold sway.