NORTON ROSE FULBRIGHT

Blockchain Law
Gaming the system

New York Law Journal

September 23, 2025 | By **Robert A. Schwinger**

People in the fintech world often like to say that "code is law," but do courts agree? Some argue that whatever outcomes might occur under a fintech system's programming are what the participants bargained for by agreeing to use that system, and thus must be accepted.

But sometimes users of those systems find ways to exploit opportunities or gaps in programming to obtain "windfalls" or other unanticipated or commercially unreasonable outcomes, perhaps even to the injury of others. What then?

In such situations, courts have been willing to step in and insist that legal principles can constrain what participants on such systems might do, even if the programming won't. Some recent cases show how courts have been responding to clever users who appear to be gaming the system.

The Peraire-Bueno brothers

A recent case involving a complex scheme to take advantage of the workings of the Ethereum network shows how actions that might seem technologically clever can in fact be legally precarious.

In *U.S. v. Peraire-Bueno*, 2025 WL 2062021 (S.D.N.Y. July 23, 2025), two MIT-graduate brothers who were "highly educated in mathematics and computer science" were charged with conspiracy to commit wire fraud, wire fraud, conspiracy to commit money laundering, and conspiracy to receive stolen property arising from what was characterized as "a 'very first of its kind' exploit of the Ethereum blockchain."

The indictment against the brothers charged that they had hatched a plan to take advantage of certain features of the Ethereum blockchain to obtain allegedly fraudulent gains of approximately $25 million worth of ETH, the "native cryptocurrency" on the Ethereum network. The brothers were alleged to have used their skill in mathematics and computer science to "trick" the Ethereum network and its traders into an alleged multi-million dollar fraud.

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

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

Attorney advertising

Reprinted with permission from the September 23, 2025 edition of the *New York Law Journal* © 2025 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. www.almreprints.com – 877-257-3382 – reprints@alm.com.

How the network operates

The Ethereum network is a decentralized blockchain that operates on a set of rules and protocols that are implemented through "smart contracts"—"self-executing computer protocols with if/then conditions … which allow transactions to occur on the network without a trusted intermediary." The network also relies upon "validators," who "are necessary participants responsible for confirming that new blocks on the blockchain are valid before they are added," and who "stake" certain ETH of their own into a smart contract as part of the validation process.

More specifically, as explained in the indictment:

> "When a user conducts a transaction on the blockchain, the pending transaction is placed with other pending transactions in a publicly visible memory pool ('mempool'). The pending transactions proceed according to their potential maximal extractable value (MEV), which is the maximum value that can be obtained by including, reordering, or excluding transactions when publishing a new block to the blockchain. In order of MEV, pending transactions are structured into proposed blocks, validated, and added to the blockchain. After a block is published to the blockchain, the block is closed, and it cannot be removed or altered."

Once "the network randomly selects a validator to validate a block," then "the validator has 12 seconds to complete the validation process." As compensation, "[f]or each validated block, the validator is paid an agreed-upon amount of cryptocurrency, which represents a portion of the MEV of the transactions in the block and other fees. Validators also earn newly minted ETH."

The payment the validator will receive for validating a proposed block is contained in a "blockheader," which contains limited information about the transaction. After receiving the blockheader, the validator "confirms through a digital signature that they will validate the proposed block as structured," and are subject to certain financial penalties for failing to properly do so.

The indictment alleged that approximately 90% of validators rely on a software program called "MEV-Boost" that outsources the block-building process and divides it across three functions: "Searchers," "Builders," and "Relays."

A Searcher uses automated MEV Bots to scan the network's "mempool" and locate profitable arbitrage opportunities. After an arbitrage opportunity is located, the Searcher sends the Builder a transaction bundle that the Searcher proposes in a precise order according to the arbitrage opportunity.

The typical order of a Searcher's transaction bundle consists of (1) the Searcher's own purchase transaction through which the Searcher buys cryptocurrency that the Searcher expects will appreciate in value; (2) the pending transaction that the MEV Bot located in the "mempool" as being likely to increase the price of that cryptocurrency; and (3) the Searcher's own sell transaction through which the Searcher sells the cryptocurrency it purchased in the first transaction for an anticipated higher price than what the Searcher initially paid.

Once the Builder receives the transaction bundle from the Searcher, the Builder assembles the transactions into a proposed block and sends it to the Relay.

The Relay then holds the block privately until a validator confirms that it will publish the block in the exact order proposed. Once confirmation from the validator is received, the Relay releases the transactions within the block to be published by the validator.

The brothers' plan

According to the indictment, the brothers began the planning for their alleged fraud scheme by running online searches for "methods to launder cryptocurrency" and searching for cryptocurrency exchanges that had minimal "know your customer" protocols.

Their investigations also extended to visiting the website that hosts the open-source code used on the Ethereum network and running additional online searches relating to penalties that the Ethereum network imposes for misconduct.

Thereafter, the indictment charged, the brothers initiated their alleged scheme by staking enough ETH coins to create 16 potential validators on the Ethereum network.

They concurrently identified and targeted three traders who acted as Searchers (Victim Traders) by deploying a series of test transactions to learn the trading behavior used by the Searchers' MEV Bots.

Within a few months, the brothers were notified that one of their 16 validators had been selected to verify a block. The brothers then executed eight specific transactions that were intentionally designed to lure the Victim Traders into choosing those transactions for their proposed bundles (Lure Transactions). As planned, the Victim Traders included the Lure Transactions in the bundles that they proposed to the Builder.

But the brothers then allegedly used their position as a validator to interfere with the Victim Traders' proposed bundle.

Specifically, the indictment charged that they replaced the Lure Transactions with new transactions through which the brothers themselves sold the cryptocurrencies that the Victim Traders had just purchased (Tampered Transactions).

The tampering thereby prevented the final sell transaction proposed by the Victim Traders from taking place, but still allowed the brothers to extract approximately $25 million worth of cryptocurrency that the Victim Traders had intended to purchase for themselves.

The brothers then published the block to the blockchain, finalizing the transaction with the Tampered Transactions included.

The brothers allegedly did not stop there, however. They also allegedly laundered the proceeds they had obtained through various institutions, all the while conducting internet searches for "top cryptocurrency lawyers" and the statute of limitations for wire fraud and money laundering.

A year later, the government brought an indictment against the brothers for conspiracy to commit wire fraud, wire fraud, and conspiracy to commit money laundering, and then later added a charge of conspiracy to receive stolen property.

Challenges to the indictment

The brothers moved to dismiss the indictment on a two-pronged approach. First, they contended that applying these criminal statutes to their activity on the Ethereum blockchain violated their due process rights, arguing that given the novelty of their scheme they lacked "fair notice" from the government that their conduct might be deemed criminal under the cited criminal statutes, and that application of such statutes to them was a "novel construction" that was "unexpected" and should be barred as "void for vagueness."

Second, they argued that the indictment failed to charge the "essential elements" of the underlying criminal statutes they allegedly violated.

Due process and fair warning

The court held that the brothers' void-for-vagueness challenge was premature prior to actual conviction at trial. Outside of First Amendment contexts, it said, analysis of such a challenge requires a fully-developed factual record, from which it is "clear what the defendant did."

The post-conviction cases upon which the brothers relied were thus of no avail to them at the indictment stage. Such issues, said the court, should instead be raised at or after trial.

The court further held that it was premature to grant dismissal at this stage on the brothers' "novel construction" arguments, which likewise require a full factual record to assess.

The brothers had argued that the charges under the wire fraud statutes—which target "any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises"—"amount[ed] to a novel construction of these statutes" in this highly technical cryptocurrency context. Specifically, they argued that:

> (1) the indictment represents "an unusual government intervention into the Ethereum Network,"

(2) the network protocols that the brothers allegedly violated were "vaguely described" and remained "in flux in critical ways,"

(3) the indictment "is a strange and unexpected foray for the government into policing transactions among sophisticated parties on decentralized cryptocurrency markets," and

(4) "the government has not prosecuted other attempts to counter sandwich trades."

The court "acknowledge[d] that there appear to be numerous novel aspects of this case for which analogous cases are difficult to locate."

Among these novel aspects were the facts "that part of the allegations involve defendants exploiting a vulnerability in a software to further their alleged fraud, that the alleged fraud involved reordering transactions in a proposed block, and that the alleged fraud took place on the Ethereum Network, an allegedly trustless system."

Nevertheless, said the court, the focus should remain on the general purpose and consequences of the brothers' scheme and not on the specific means through which they executed it.

The "essence" of the indictment, the court observed, alleged that the brothers "devised a scheme to defraud and obtain money or property under false pretenses." From that standpoint, the court ruled, "the wire fraud statute provided defendants with adequate notice that their alleged conduct was criminal, despite any novel means used by defendants."

The court also noted prior prosecutions for activity like "spoofing conduct" where, like the brothers here, defendants had "placed orders for contracts they intended to cancel prior to execution, which communicated false and misleading information regarding supply or demand in order to deceive and entice other traders, in violation of the marketplace's rules."

While the brothers contested the indictment's charge that they acted "in violation of the protocols established for MEV-Boost users on the Ethereum Network," the court held that this was a fact issue for trial.

The court thus concluded that "at this juncture, the novel circumstances of this case as alleged do not amount to a due process violation," observing that "[a]ny novelty in this prosecution is based on the particulars of defendants' … scheme, not any originality in construing the relevant fraud statute."

Essential elements

The brothers were also unsuccessful in arguing that their indictment failed to allege certain "essential elements" of the crimes charged, namely (1) material misrepresentation, (2) deprivation of a traditionally-recognized, enforceable property right, and (3) intent to defraud.

The court held that the material misrepresentation element was satisfied by the Lure Transactions, which "effectively promised" that the brothers would publish those transactions in the exact order set forth, even though the brothers "allegedly had no plans to, and did not, move forward with the Lure Transactions as proposed."

The court noted prior cases that had been based on such "deceptive trading orders," and the indictment charged that such deceptions here were communicative acts that served as the but-for cause of the Victim Traders' transactions.

The court similarly held that the scheme as alleged infringed on a traditional property right. It noted that the indictment did not charge wire fraud based on "the value of profit the Victim Traders expected to receive," as the brothers had argued, but instead "allege[d] that defendants schemed to obtain the Victim Traders' money in the form of $25 million worth of cryptocurrency" — a fact sufficient to meet this element. The court explained:

> "The allegations in this case are not limited to whether the Victim Traders had a property interest in a fair process on the Ethereum Network. Instead, it is about the money the Victim Traders already possessed and were allegedly fraudulently induced to part with because of defendants' alleged scheme."

Last, the court ruled that intent to defraud was adequately pleaded. The brothers argued that such intent could not be

present because the Victim Traders "got precisely what they bargained for in their trades on the Ethereum blockchain."

The court held that this was a fact question for the jury, and that the indictment expressly charged that the brothers acted "with the intent of inducing Victim Traders to part with their cryptocurrency" and "then reordered transactions such that the Victim Traders' could not sell the illiquid cryptocurrency they purchased."

Such actions, said the court, were sufficient to allege an intent to defraud. The indictment as to the wire fraud- and money laundering-related charges was thus upheld, leaving the prosecution against the brothers to proceed.

The saga of 'Shin v. ICON Foundation'

The controversy over the scheme in *Peraire-Bueno* is reminiscent of the issues in the long-running saga of the *Shin v. ICON Foundation* litigation, which began in 2020 and reached its final conclusion in March 2025. *Shin*, like *Peraire-Bueno*, involved a transaction validator on a "proof of stake" blockchain who exploited the system's programming for arguably unintended gains involving the system's native cryptocurrency, there a token known as ICX.

As detailed in the initial ruling in that case, *Shin v., ICON Found.*, 2021 WL 1893117 (N.D. Calif. May 11, 2021), the plaintiff Shin discovered after a software revision for the ICON blockchain network was issued that each time he re-staked his tokens, 25,000 new ICX tokens suddenly appeared in his wallet.

Shin thus began repeating this process over and over, and by the end of the day he had amassed approximately 14 million ICX tokens.

Shin analogized this scenario to "a slot machine that continued to provide jackpot winning [sic] each time he put quarters in and pressed the same buttons," but the ICON Foundation did not view his conduct as quite so benign.

After discovering what happened, ICON blocked Shin from transferring any ICX tokens—even those he owned before the software revision—and coordinated with other exchanges where Shin had transferred his ICX tokens to have them freeze Shin's accounts there too.

ICON also promulgated a further software revision, which ICON stated was designed to address a "vulnerability," but which Shin argued was specifically intended to restrict his ICON account and ensure that all of his ICX tokens remained frozen.

Shin responded by filing suit against ICON seeking a declaratory judgment that the frozen ICX tokens were his property. He also asserted claims for conversion and trespass to chattel, and other torts. ICON responded by moving to dismiss his complaint and counterclaiming for unjust enrichment.

In its initial ruling on ICON's motion to dismiss, the court held that Shin had failed to plead claims for conversion and trespass to chattel, and that his claim for declaratory relief was "needlessly duplicative" of those other claims.

Shin had based his conversion claim on his argument that ICON had "substantially interfered" with his tokens when it released the new software revision that "blacklist[ed]" and "effectively froze" both his past ICX tokens and the ones he had obtained through the short-lived software anomaly.

While the court conceded that certain of Shin's allegations "plausibly establish that ICON had de facto control over" the software revision, it found Shin's allegations contradictory regarding to what extent he continued to have access or at least restricted access to some amount of the tokens in question. The court thus dismissed the conversion claim but with leave to amend.

The court likewise dismissed Shin's trespass to chattel claim. It held that such a claim required Shin to show that ICON had interfered with Shin's "possessory interest in personal property," but that this had not been properly alleged given the lack of clarity regarding what access Shin still had over the tokens in his ICON account.

The court also held that Shin had not made sufficient allegations of "intermeddling" by ICON with respect to the ICX tokens that Shin had moved to other exchanges, which ICON did not control.

Establishing a property right

Shin amended his complaint, and several years later the court ruled on the parties' cross-motions for summary judgment on Shin's amended complaint and ICON's unjust enrichment counterclaim. The court granted summary judgment in favor of ICON and against Shin on both. *Shin v. ICON Found.*, 2024 WL 2883659 (N.D. Calif. June 6, 2024).

The court's assessment of Shin's conduct in its 2024 summary judgment ruling was blunt:

> "Plaintiff Mark Shin exploited a bug in software 557 times to generate cryptocurrency tokens worth $9 million from the ICON Network . . . . While the cryptocurrency context of this case makes it somewhat unique, the legal principles are clear cut: Shin has no legitimate claim to exclusivity over the bug-generated cryptocurrency that he obtained contrary to the rules and practice of the network and no right to retain the benefit of his willful decision to exploit what he knew was a flaw in the network 557 times."

The court thus awarded summary judgment dismissing Shin's amended conversion claim. It stated that such a claim requires "a legitimate claim to exclusivity" for the property at issue but held that "Shin lacks a legitimate claim to exclusivity over the bug-generated ICX," pointing to several factors.

The court noted that under the ICON network's constitution, users of the network were obliged to "strive to ensure that the network runs properly" and to "oppose any transgression against" the network.

It characterized Shin as having employed "[i]llegitimate [m]eans of [a]cquisition," whereas, by contrast, "legitimate claims to exclusivity are established through legitimate means of property acquisition that favor the public interest" and usually reflect "reasonable investment-backed expectations."

While Shin "denie[d] that [his] behavior was 'exploitation' in what his counsel described as a 'decentralized ecosystem[,]'" the court declared "I will not debate morality with Shin."

The key point, explained the court, was that Shin's "actions were not 'authorized' by the network." Rather, the software simply "contained a bug" and "[a] bug belies authorization." Thus, "[n]o matter what type of 'ecosystem' Shin was operating in, he has no legitimate claim to the bug-generated ICX."

As a result, the court concluded, "he has no ownership or property interest in it, and his conversion claim fails as a matter of law."

On the amended claim for trespass to chattel, the court similarly explained that "[t]here can be no trespass where the defendant has interfered with property over which the plaintiff has no personal right."

The court thus held that, "[f]or the same reasons that ICON prevails on summary judgment against Shin's conversion claim, it prevails on his trespass to chattels claims."

The court also granted summary judgment to ICON on its unjust enrichment counterclaim. Noting that "[u]njust enrichment focuses on the wrongdoer's gain, not the victim's loss," it held that "ICON does not need to establish that it, or any network user, [had] a property interest in the tokens before Shin generated them for Shin to have been unjustly enriched."

The court also held that "Shin caused harm" because "the price of ICX decreased by nearly 40%" over the two weeks that followed "ICON's public disclosure of what Shin did."

The court thus held that Shin had been unjustly enriched, condemning his actions as "inequitable not only because he caused ICON direct harm, ... but also because he exploited, received, and knowingly retained a benefit that was conferred to him via his willful decision to manipulate what he understood to be a flaw in the network."

The court later amplified the unjust enrichment point in a subsequent March 2025 ruling in which it held that ICON should be awarded attorneys' fees under the "common fund" exception to the usual "American rule" that litigants bear their

own attorneys' fees. *Shin v. ICON Found.*, 2025 WL 672936 (N.D. Calif. Mar. 3, 2025).

That exception enables a party "who recovers a common fund for the benefit of persons other than himself or his client" to recover "a reasonable attorney's fee from the fund as a whole." The court observed that "[w]hile Shin's actions injured all ICX holders," it was ICON, "[o]n behalf of itself and for the benefit of other ICX holders," who "successfully defended Shin's conversion and wrongful taking claims and prevailed on its counterclaim against Shin for unjust enrichment."

Under these circumstances, the court held that ICON was entitled to attorneys' fees and costs totaling just under $3.5 million, to be paid out of the ICX seized and recovered from Shin that was being held by a receiver and awaiting destruction.

Conclusion

For those contemplating "gaming the system" in cryptocurrency transactions, whether involving staking, validation functions, transacting orders or other areas, cases like *Peraire-Bueno* and *Shin v. ICON Found.* show that some good pragmatic advice might simply be "don't be a wiseguy."

A fundamental legal guidepost in commercial matters is that people engage in business and financial transactions for reasonable commercial purposes and to realize ordinary reasonable commercial expectations, and that the law therefore should reflect this in its outcomes whenever possible.

Judges do not aspire to issue rulings reaching absurd or outrageous outcomes because their hands are tied by some claimed technicality or the intricacies of some highly debatable theory. To the contrary, judges more commonly seek to show that the legally correct result in a case in fact aligns with broader society's basic notions of fairness and morality.

While it may not be the job of the courts to rewrite parties' foolish contracts or bad laws passed by legislatures, cases such as *Peraire-Bueno* and *Shin v. ICON Found.* show that courts do not extend similar deference to things like software bugs or system designs that fail to block certain methods of circumventing their intended operation.

Those who devise clever schemes to exploit limitations in the programming or design of fintech systems would thus be well advised, it appears, not to assume that code alone will provide them a free pass for conduct that offends ordinary commercial or legal norms.

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 3000 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa.

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 City, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg. For more information, see nortonrosefulbright.com/legal-notices.

© Norton Rose Fulbright US LLP
67115_US – 09/25