DAILY NEWS
MEDIA GROUP

Don’t Punish Crypto for The Sins of SBF’s FTX

Jack Solowey and Jennifer Schulp

November 29, 2022

“I’m sorry. That’s the biggest thing. I f---ed up, and should have done better,” tweeted FTX CEO and founder Sam Bankman-Fried, a.k.a. SBF, on the eve of announcing FTX’s bankruptcy.

The implosion of crypto middleman FTX will soon get multiple hearings on Capitol Hill. While Senate and House hearings likely will explore a mountain of misdeeds by SBF and his organizations, policymakers should not use the occasions to condemn crypto technologies broadly — particularly those that seek to minimize the role of all-too-human financial intermediaries — for the sins of FTX.

Rather, because decentralized software projects can help to reduce risks from centralized financial exchanges like FTX that hold customer assets and keep private balance sheets, lawmakers ought to draw clear lines between centralized and decentralized exchanges, not subject them to collective punishment.

According to the grown-up hired to replace SBF as CEO, John J. Ray III, there’s a lot SBF should have done better. In Ray’s words, “Never in my career have I seen such a complete failure of corporate controls and such a complete absence of trustworthy financial information as occurred here.” That career included unwinding Enron.

Revelations about FTX’s mismanagement are ongoing, but a couple of things are noteworthy at this point: FTX reportedly lent customer assets to SBF’s own hedge fund, Alameda Research, to keep it afloat, and SBF allegedly hid such transfers from FTX’s books.

Courts of law should determine what crimes and violations took place here, though one needn’t be an attorney, accountant, or — for that matter — clinical psychologist to understand peoples’ propensity toward stealing and lying.

But what if there were another tool, beyond courts, that could help address the risks of financial frauds like unauthorized transfers and false bookkeeping? That’s the question the first cryptocurrency sought to answer. It did so by offering an alternative to the banks and brokers we traditionally rely on to faithfully hold and transfer our assets and to keep honest ledgers.

In broad strokes, cryptocurrencies replace "the books" with a public digital ledger for recording and verifying transactions with cryptographic proof (a "blockchain"). They also replace "the bookkeepers" with software running on redundant computers that check each other's work.

Trainwrecks like FTX understandably cause people to question crypto's ability to mitigate such risks by removing the middleman. But centralized exchanges like FTX, which are at heart traditional intermediaries, are not the only way to exchange crypto tokens.

Like a traditional bank or broker, FTX took possession of peoples' assets, including both cash and crypto. How does one possess crypto assets? By controlling the "private key" (a unique alphanumeric string) that, in essence, unlocks the line on a ledger documenting crypto holdings and allows them to be transferred. FTX controlled customers' crypto assets because it controlled the relevant private keys. And FTX kept the books — poorly, it seems.

Decentralized exchanges, or DEXs, however, are alternatives to such centralized marketplaces. In their purest form, DEXs do not control a customer's assets because the customer, and not the exchange, controls her own private keys.True DEXs do not keep their own sets of books either, but rather document transactions directly on a public blockchain ledger.

DEXs do have human programmers. But DEXs do not rely on a middleman keeping his word because they are composed of software programs ("smart contracts") that are open and auditable. In addition, because bona fide DEXs are written in open-source code, if users do not like every nuance of one DEX version, they can iterate on it and start anew.

That's not to say that DEXs solve every problem or eliminate every risk. For example, they let users swap between certain cryptocurrencies but do not let them buy cryptocurrencies with debit or credit cards. Smart contracts also can be vulnerable to hacking.

But conducting due diligence on a DEX, such as by auditing its open-source software code for performance and vulnerabilities, is not the same as what's called for when trusting a guy on an island not to steal and lie. Different risks ought to be treated differently.

Accordingly, our ask of lawmakers at this point is simple: get to the bottom of what happened at FTX, but also get to the bottom of how to distinguish DEXs from centralized exchanges. This task is critical, because forcing DEXs to comply with one-size-fits-all rules designed for traditional intermediaries undermines what makes DEXs unique. It's also counterproductive because, unsurprisingly, complying with rules designed for intermediaries tends to require delegating tasks to intermediaries, reintroducing some of the very risks that DEXs seek to mitigate.

To distinguish centralized exchanges from decentralized exchanges, we suggest starting with one question: whether one person tweeting that they "f---ed up, and should have done better" can plausibly signal the exchange's demise. If so, that's no DEX. If not, it just might be.

Solowey is a policy analyst at the Cato Institute's Center for Monetary and Financial Alternatives. Schulp is the director of financial regulation studies at the CMFA.