

Project Syndicate

Whither Crypto?

Nov 15, 2023

Ari Juels and Eswar Prasad

Sam Bankman-Fried's recent fraud conviction over the collapse of the cryptocurrency exchange FTX has cast a harsh light on the industry. But looking ahead, blockchain-enabled tools have the power to improve transparency and strengthen the trustworthiness of the financial sector.

NEW YORK/ITHACA

The vertiginous fall of Sam Bankman-Fried, the disgraced founder of the cryptocurrency exchange FTX who was recently [convicted of fraud and money laundering](#), in New York, has cast a harsh light on a largely unregulated market. For all the supposed wonders of the blockchain technology underpinning cryptocurrencies, the headline-grabbing events of the past few years indicate an industry in turmoil.

In addition to the criminal activity that led to the [spectacular collapse of FTX](#) in 2022 and Bankman-Fried's guilty verdict in early November, US regulators have [sued](#) Binance, the world's largest crypto exchange, for allegedly operating a "web of deception." An industry-wide reckoning looms. Will crypto always be a magnet for fraud and malfeasance, or can it eventually transform and democratize finance?

An increasingly obvious paradox has emerged. Satoshi Nakamoto, the pseudonymous creator of Bitcoin, [proposed](#) the idea of a purely peer-to-peer version of electronic cash in the wake of the 2008 global financial crisis, when confidence in governments and central banks was at its nadir. Soon after the launch of Bitcoin in 2009, Nakamoto [wrote](#) that "the root problem with conventional currency is all the trust that's required to make it work." Today, the system that was supposed to eliminate the need for trust between people and in traditional financial institutions is experiencing a crisis of trust.

Cryptocurrencies such as Bitcoin and Ethereum rely on computer code and networks that are not controlled or managed by a central party.

Remarkably, such decentralization works. Transactions can be completed in a secure manner, without relying on a bank, credit-card company, or other institution. In principle, this should make financial systems less vulnerable to fraud and manipulation.

Unfortunately, grifters and unscrupulous companies have exploited customers and investors enamored with the new technology and, in the process, obscured crypto's most compelling innovation: blockchain-enabled tools that can improve transparency and strengthen the trustworthiness of the financial sector. Maintained on computers around the world and publicly accessible by anyone with human interaction, creates a robust money trail that traditional financial infrastructure lacks.

So, how did we end up with a crypto industry that often contradicts its founding ethos? One answer is that any innovation inevitably attracts speculative mania and chicanery, especially in the early stages of its development. In the nineteenth century, banks deceived examiners by padding gold reserves with [nails](#). More recently, the dot-com era gave us the likes of [Enron](#), while a biotech boom brought us Elizabeth Holmes and [Theranos](#).

Another problem is that the industry's consumer-facing platforms have simply grafted old ways of doing business onto a technology designed specifically to do away with them. For example, while FTX was an "exchange" – a gateway to blockchain-powered cryptocurrencies – it did not make fundamental use of decentralized technologies. Ironically, most crypto holders today store their assets [in exchanges](#) that require high levels of trust and carry many of the risks of traditional financial institutions.

Behind the scenes, the crypto industry has started using technology to shift the balance back toward innovation. One example is the development of [proof of reserves](#), a mathematically-based method that enables institutions to verify their crypto assets. Such tools could help prevent debacles like FTX, where the lack of transparency allowed Bankman-Fried to conceal financial fraud.

Importantly, proof of reserves and similar tools work best for cryptocurrencies, not for ordinary financial assets – including the US dollar. These technical advances have therefore prompted traditional financial institutions – the very ones Bitcoin sought to replace – to embrace crypto. JPMorgan, for example, has plans to move [trillions of dollars](#) of value on to

the blockchain, while monetary authorities are exploring [central bank digital currencies](#), which would involve using blockchain technology to issue digital versions of their fiat currencies.

To be sure, the crypto industry faces several daunting challenges: the [large environmental footprint](#) of Bitcoin mining, its use for illicit transactions, privacy shortcomings, and more. But, as proof of reserves suggests, the crypto community is innovating powerful new ways to harness the inherent transparency and trustworthiness of blockchain technology to create a more secure and flexible financial ecosystem.

As these innovations proceed, governments around the world are exploring ways to safeguard consumers from the crypto industry's excesses. They would do well to look past the headlines and seek a balanced approach that enables this remarkable technology to thrive.

Ari Juels, a professor at Cornell Tech, is Co-Director of the Initiative for CryptoCurrencies and Contracts (IC3), Chief Scientist at Chainlink Labs, and the author of the forthcoming [The Oracle](#) (Talos Press, 2024).

Eswar Prasad, Professor of Economics in the Dyson School at Cornell University, is a senior fellow at the Brookings Institution and the author of [The Future of Money: How the Digital Revolution Is Transforming Currencies and Finance](#) (Harvard University Press, 2021).