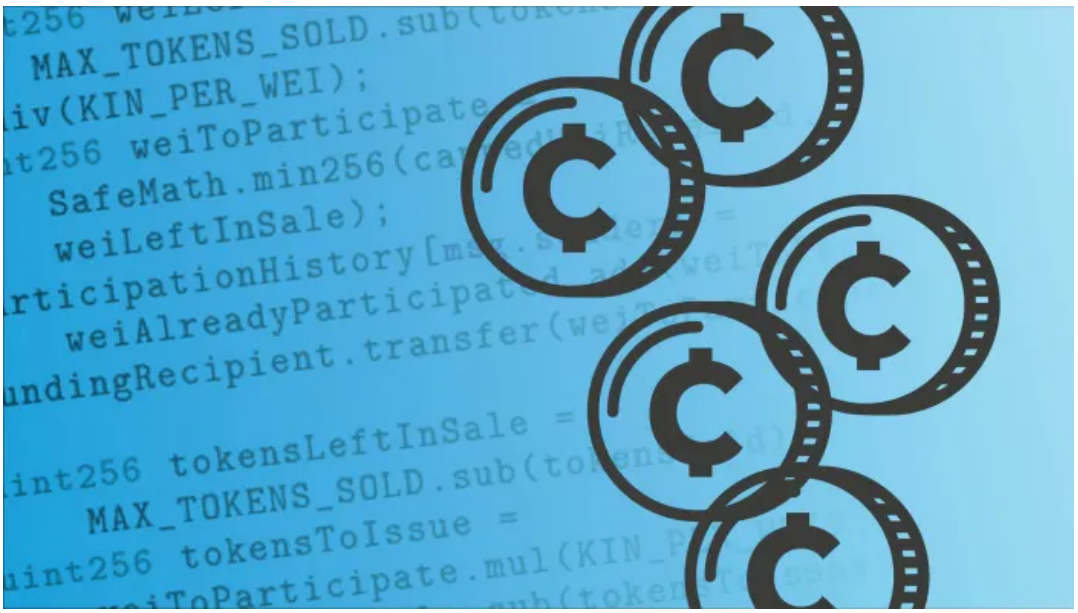
Opinion **Cryptocurrencies**

Cryptocoin computer code fails to deliver on promoter claims

Marketing for currency offerings promise investor protections that the assets do not deliver

DAVID HOFFMAN



© FT montage

David Hoffman JUNE 13, 2019

Between 2016 and 2018, cryptocurrencies produced a bona fide financial bubble. Nothing typified the madness better than the craze for initial coin offerings meant to fund software projects that promised to revolutionise everything from online gaming to file storage. Maybe you invested. More likely, you intuited something was awry when your Uber driver started asking for crypto recommendations and a friend began touting a blockchain-based ledger designed to track marijuana supply chains.

ICOs birthed a thousand millionaires before asset prices plummeted in late 2018. Now as bigger players such as Facebook start to enter cryptocurrencies, regulators at the US Securities and Exchange Commission are having to grapple with the problems caused by these investments.

So far, the watchdog has focused on bringing ICOs under its traditional regime of disclosure-based investor protection rules. But my research with David Wishnick into the ICO market reveals some disquieting facts.

The central innovation in ICOs rests on the possibility of using computer code to deliver on contractual promises. So we surveyed the 50 offerings that raised the most capital in 2017 and

asked a simple question: did the promoters deliver on their promises to protect investors through computer code?

We specifically compared the promises promoters made in their offering documents with the actual function of the cryptoassets they delivered. We audited each coin's smart contract, the automated "if this, then that" rules coders design to govern cryptoassets.

We found that most of the offerings promised forms of investor protection that the code did not deliver. Take the issue of supply. An investor in a given cryptoasset needs to know that a promoter cannot simply print more, inflating away its value. In more than 20 per cent of ICOs in our sample where cryptoasset supply restrictions were promised, we could not observe restrictions hard-coded into smart contracts.

More starkly, in 25 of the 36 ICOs where promoters promised to impose restrictions on insiders selling assets and walking away, we could not find those restrictions in the code. Finally, we found 12 offerings where the code allowed a central party to modify the way the smart contract worked, but only four of them disclosed that ability in their promotional materials.

Even if the SEC does expand its regulatory umbrella over ICOs, its ability to police against fraud will be limited by resource constraints; and it is not clear that private class-action lawsuits can pick up the slack. Moreover, these offerings are truly global, allowing promoters to switch jurisdictions, seeking lighter regulation. That means the market will be largely left to police itself.

But our analysis found no evidence that investors punished firms for failing to put investor protections into code. Even today, crypto rating agencies look at code only to check that it is protected against hackers. We found no sign that they tried to match code with investor protections. That task is left to individual investors, who are expected to read, and understand, smart contracts. This is a hopeless enterprise.

It is well documented that few people read the "click I agree" user contracts they encounter online, and the same is true for smart ones. Regulators need to step in. Here are two simple suggestions. We should require ICOs to guarantee a match between the key promises made in marketing and code. Or we should demand that promoters provide plain-English translations of principal code elements.

Such market integrity measures won't just protect investors, they will also build trust in the asset class itself and enable it to move from a curiosity to something of real economic worth.

The writer is a law professor at the University of Pennsylvania. David Wishnick, a fellow there, also contributed