Futures

Cash is king

A currency you can count on. **By D. J. Rozell**

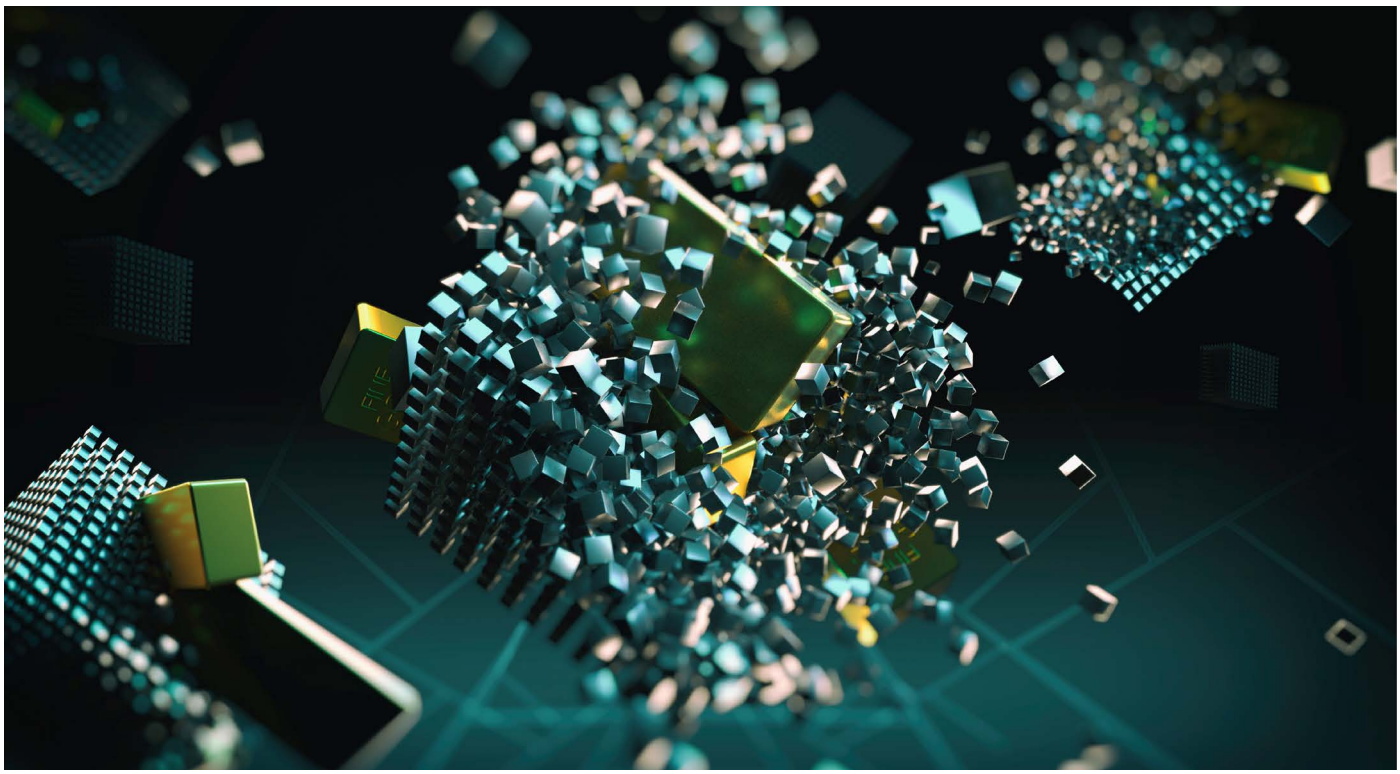

ILLUSTRATION BY JACEY

Regular readers of my column know me to be a long-time sceptic of cryptocurrency. Speculators have been hoarding crypto for years as it skyrocketed – all based on the assumption that it will someday be a universal method of payment. But a functional currency should have a relatively stable value. So, which is it, an investment or a currency? Well, it turns out the crypto question has been resolved, because now it is neither.

Last week, anonymous government sources confirmed that Quoherence Labs had created a quantum computer capable of breaking both the widely used RSA and elliptical curve encryption algorithms that underpin most cybersecurity protocols. With potentially every online financial transaction at risk, I became rather alarmed when I first heard the news. But before you start deleting your banking apps, I have been assured by a quantum computer expert that even sophisticated cyber criminals won't be able to build their own backyard quantum computer any time soon. Nonetheless, the advance is many years earlier than predicted and has set off a mad scramble to adopt quantum-secure protocols before the technology becomes more accessible.

Ordinarily, the defence-funded research would have been classified (and quietly exploited by the intelligence community) while countermeasures were developed. However, an unnamed Quoherence Labs employee used the new powerful quantum computer to wildly compromise the blockchain of several popular cryptocurrencies. When knowledge of the blatant hacks hit the markets, the value of cryptocurrencies, NFTs and anything even vaguely related to blockchain technologies collapsed globally in what has been dubbed Black Saturday. Even several cryptocurrencies that claimed to use quantum-secure encryption became victims of the backlash. If that doesn't kill off rational market theory, nothing will.

This leaves behind a few big questions. First, how did this all happen? Quoherence Labs is cooperating with federal authorities but has made no public announcements. This leaves a big hole of ignorance that science bloggers and tech pontificators are attempting to fill with jargon that no one understands. I asked a physicist who knows quantum computing better than most to give me a crash course on some of the terms I had been hearing – superconducting circuits, photonics, trapped ions, silicon spin, quasiparticles, Shor's algorithm, quantum annealing – it's all quite fascinating but quickly starts to feel like drinking from a fire hose. For now, I'm siding with the cybersecurity experts who all agree that the details are better left unknown until encryption protocols are updated and our bank accounts are secure.

The second big question revolves around motivation. Why crash cryptos? Multiple investigations are in their preliminary phase, but there is speculation that the rogue scientist may have been shorting several top cryptocurrencies and putting borrowed money into gold. After the crypto-crash, investors rushed to gold, which reached record

highs. However, even with highly leveraged positions, it is unlikely that the perpetrator could have offshored more than several million dollars while evading notice before the commodities markets locked down. Meanwhile, at least a trillion dollars of value associated with blockchain technology evaporated in a day. This will probably fuel economists' nightmares for years.

Some privacy activists have argued that this was the selfless act of a scientist who sacrificed a lucrative science career to alert the public to a grave threat. Breaking cryptocurrency was just an attention-grabbing means of ensuring that the public would learn of the new cybersecurity-crushing computer and its potential for online spying.

Others have suggested that this was the ultimate act of eco-terrorism. As crypto-mining ground to a halt, it became clear that this act of sabotage stopped more carbon emissions than any individual effort in the history of the world.

Perhaps the individual will someday write an anonymous social media post titled "I Crashed Crypto — Sorry, Not Sorry" explaining how they had become disenchanted with the crypto community when its utopian goal of creating a global egalitarian currency was hijacked by speculatory greed. But I wouldn't hold your breath waiting for that kind of closure.

The final big question is how do early investors recoup their crypto loses? This one has an answer: they don't. The entire point of cryptocurrency was to bypass the banks and government. This transfers all the benefits and risks to cryptocurrency users. And don't expect any special government bailout. This wasn't a hurricane. Central banks have a long history of hating cryptocurrency because it's competition and difficult to tax. I admit to feeling a bit of *Schadenfreude* after warning my nephew not to buy NFTs of sports video clips. He bought them anyway because strangers on the Internet told him to and what does his uncle who has a syndicated financial advice column know? Don't get me started.

In case you're wondering about the current whereabouts of the rogue scientist, so is everyone else. It's known that the person fled the country but not much more. Considering the person is smart enough to use a quantum computer, let's assume they are now enjoying life somewhere with no international extradition agreements and staying off the Internet.

Next week I'll discuss the latest financial trends. Hint: bonds are back and cash is still king!

D. J. Rozell is a professional worrier from New York. Other fiction can be found on Twitter @djrozell.

THE STORY BEHIND THE STORY

D. J. Rozell reveals the inspiration behind *Cash is king*.

Over the years, I've been watching the field of quantum computing advance from the realm of cool theory to functional devices. As the technology nears the goal of reliably solving otherwise intractable problems, it seemed like an appropriate time to imagine using a quantum computer to force a reset of cryptocurrencies — a potentially useful class of innovations that has been a real disappointment so far.