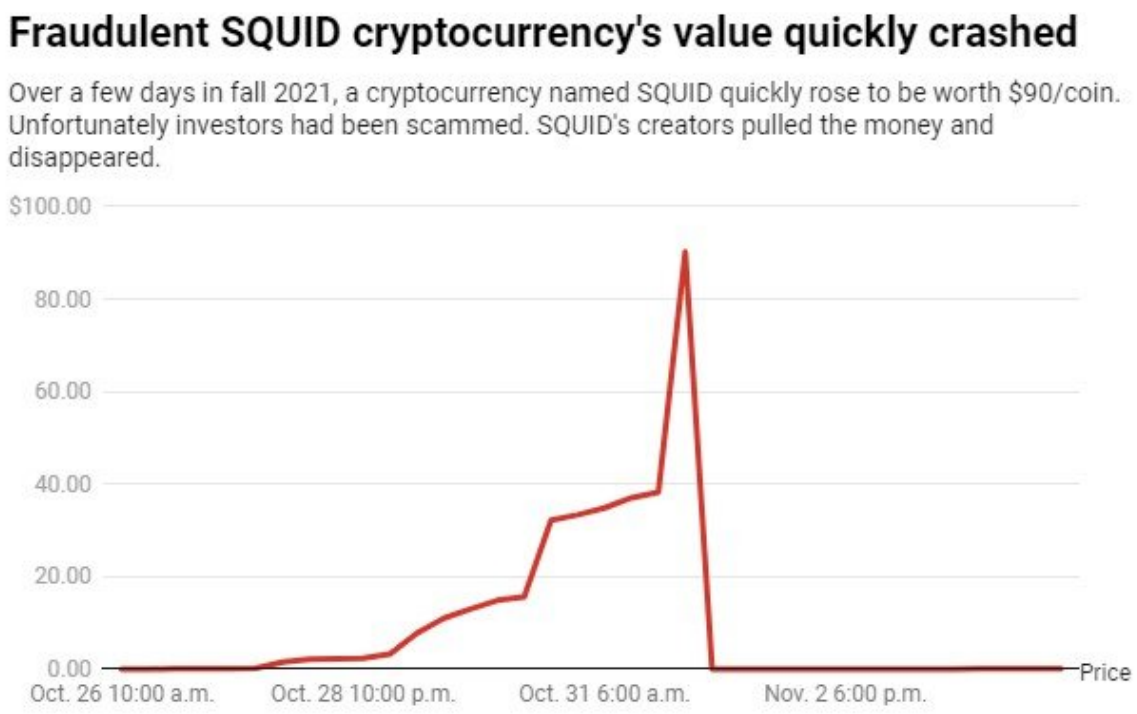
Scams and cryptocurrency can go hand in hand. How they work and what to watch out for

June 22 2022, by Yaniv Hanoch and Stacey Wood



Credit: Chart: The Conversation, CC-BY-ND Source: CoinMarketCap

When one of our students told us they were going to drop out of college in August 2021, it wasn't the first time we'd heard of someone ending their studies prematurely.

What was new, though, was the reason. The student had become a victim of a cryptocurrency scam and had lost all their money—including a bank loan—leaving them not just broke, but in debt. The experience was financially and psychologically traumatic, to say the least.

This student, unfortunately, is not alone. Currently there are hundreds of millions of cryptocurrency owners, with estimates predicting further rapid growth. As the number of people owning cryptocurrencies has increased, so has the number of scam victims.

We study behavioral economics and psychology—and recently published a book about the rising problem of fraud, scams and financial abuse. There are reasons why cryptocurrency scams are so prevalent. And there are steps you can take to reduce your chances of becoming a victim.

Crypto takes off

Scams are not a recent phenomenon, with stories about them dating back to biblical times. What has fundamentally changed is the ease by which scammers can reach millions, if not billions, of individuals with a press of a button. The internet and other technologies have simply changed the rules of the game, with cryptocurrencies coming to epitomize the leading edge of these new cybercrime opportunities.

Cryptocurrencies—which are decentralized, digital currencies that use cryptography to create anonymous transactions—were originally driven by "cypherpunks," individuals concerned with privacy. But they have expanded to capture the minds and pockets of everyday people and criminals alike, especially during the COVID-19 pandemic, when the price of various cryptocurrencies shot up and cryptocurrencies became more mainstream. Scammers capitalized on their popularity. The pandemic also caused a disruption to mainstream business, leading to greater reliance on alternatives such as cryptocurrencies.

A January 2022 report by Chainanalysis, a blockchain data platform, suggests in 2021 close to US$14 billion was scammed from investors using cryptocurrencies.

> South African brothers, Ameer and Raees Cajee, Founders of Africrypt, a cryptocurrency platform have disappeared with $3.6 billion of clients' #Bitcoin pic.twitter.com/ssnkRClxK1
>
> — Africa story Live (@AfricaStoryLive) June 24, 2021

For example, in 2021, two brothers from South Africa managed to defraud investors of $3.6 billion from a cryptocurrency investment platform. In February 2022, the FBI announced it had arrested a couple who used a fake cryptocurrency platform to defraud investors of another $3.6 billion

You might wonder how they did it.

Fake investments

There are two main types of cryptocurrency scams that tend to target different populations.

One targets cryptocurrency investors, who tend to be active traders holding risky portfolios. They are mostly younger investors, under 35, who earn high incomes, are well educated and work in engineering, finance or IT. In these types of frauds, scammers create fake coins or fake exchanges.

A recent example is SQUID, a cryptocurrency coin named after the TV drama "Squid Game." After the new coin skyrocketed in price, its creators simply disappeared with the money.

A variation on this scam involves enticing investors to be among the first to purchase a new cryptocurrency—a process called an initial coin offering—with promises of large and fast returns. But unlike the SQUID offering, no coins are ever issued, and would-be investors are left empty-handed. In fact, many initial coin offerings turn out to be fake, but because of the complex and evolving nature of these new coins and technologies, even educated, experienced investors can be fooled.

As with all risky financial ventures, anyone considering buying cryptocurrency should follow the age-old advice to thoroughly research the offer. Who is behind the offering? What is known about the company? Is a white paper, an informational document issued by a company outlining the features of its product, available?

In the SQUID case, one warning sign was that investors who had bought the coins were unable to sell them. The SQUID website was also riddled with grammatical errors, which is typical of many scams.

Shakedown payments

The second basic type of cryptocurrency scam simply uses cryptocurrency as the payment method to transfer funds from victims to scammers. All ages and demographics can be targets. These include ransomware cases, romance scams, computer repair scams, sextortion cases, Ponzi schemes and the like. Scammers are simply capitalizing on the anonymous nature of cryptocurrencies to hide their identities and evade consequences.

In the recent past, scammers would request wire transfers or gift cards to receive money—as they are irreversible, anonymous and untraceable. However, such payment methods do require potential victims to leave their homes, where they might encounter a third party who can intervene and possibly stop them. Crypto, on the other hand, can be purchased

from anywhere at any time.

Indeed, Bitcoin has become the most common currency requested in ransomware cases, being demanded in close to 98% of cases. According to the U.K. National Cyber Security Center, sextortion scams often request individuals to pay in Bitcoin and other cryptocurrencies. Romance scams targeting younger adults are increasingly using cryptocurrency as part of the scam.

If someone is asking you to transfer money to them via cryptocurrency, you should see a giant red flag.

The Wild West

In the field of financial exploitation, more work has been done to study and educate elderly scam victims, because of the high levels of vulnerability in this group. Research has identified common traits that make someone especially vulnerable to scam solicitations. They include differences in cognitive ability, education, risk-taking and self-control.

Of course, younger adults can also be vulnerable and indeed are becoming victims, too. There is a clear need to broaden education campaigns to include all age groups, including young, educated, well-off investors. We believe authorities need to step up and employ new methods of protection. For example, the regulations that currently apply to financial advice and products could be extended to the cryptocurrency environment. Data scientists also need to better track and trace fraudulent activities.

Cryptocurrency scams are especially painful because the probability of retrieving lost funds is close to zero. For now, cryptocurrencies have no oversight. They are simply the Wild West of the financial world.