How cryptocurrency scams work

May 13 2019, by Nir Kshetri

Don’t end up like this person. Credit: fizkes/Shutterstock.com

Millions of cryptocurrency investors have been scammed out of massive sums of real money. In 2018, losses from cryptocurrency-related crimes amounted to US$1.7 billion. The criminals use both old-fashioned and new-technology tactics to swindle their marks in schemes based on digital currencies exchanged through online databases called blockchains.

From researching blockchain, cryptocurrency and cybercrime, I can see that some cryptocurrency fraudsters rely on tried-and-true Ponzi

schemes that use income from new participants to pay out returns to earlier investors.

Others use highly automatized and sophisticated processes, including automated software that interacts with Telegram, an internet-based instant-messaging system popular among people interested in cryptocurrencies. Even when a cryptocurrency plan is legitimate, fraudsters can still manipulate its price in the marketplace.

An even more basic question arises, though: How are unsuspecting investors attracted to cryptocurrency frauds in the first place?

Fast-talking swindlers

Some cryptocurrency fraudsters appeal to people's greed, promising big returns. For example, an unknown group of entrepreneurs runs the scam bot iCenter, which is a Ponzi scheme for Bitcoin and Litecoin. It doesn't provide information on investment strategies, but somehow promises investors 1.2% daily returns.

The iCenter scheme operates through a group chat on Telegram. It starts with a small group of scammers who are in on the racket. They get a referral code that they share with others, in blogs and on social media, hoping to get them to join the chat. Once there, the newcomers see encouraging and exciting messages from the original scammers. Some newcomers decide to invest, at which point they are assigned an individual bitcoin wallet, into which they can deposit bitcoins. They agree to wait some period of time – 99 or 120 days – to receive a significant return.

During that time, the newcomers often use social media to share their own referral codes with friends and contacts, bringing more people into the group chat and into the investment scheme. There's no actual

investment of the funds in any legitimate business. Instead, when new people join, the person who recruited them gets a percentage of the new funds, and the cycle continues, paying out to earlier participants from each round of newer investors.

Some members work especially hard to bring in new funds, posting tutorial videos and pictures of themselves holding large amounts of money as enticements to join the scam.

Lies and more lies

Some scammers go for straight-up deception. The founders of scam cryptocurrency OneCoin defrauded investors of $3.8 billion by convincing people their nonexistent cryptocurrency was real.

Other scams are based on impressing potential victims with jargon or claims of specialized knowledge. The Global Trading scammers claimed they took advantage of price differences on various cryptocurrency exchanges to profit from what is called arbitrage – simply buying cheaply and selling at higher prices. Really they just took investors' money.

Global Trading used a bot on Telegram, too – investors could send a balance inquiry message and get a response with false information about how much was in their account, sometimes even seeing balances climb by 1% in an hour. With returns looking like that, who could blame people for sharing the scheme with their friends and family on social media?

Exploiting friends and family

Once a scheme has started, it stays alive – at least for a while – through social media. One person gets taken in by the promise of big returns on

cryptocurrency investments and spreads the word to friends and family members.

Sometimes big names get involved. For instance, the kingpin behind GainBitcoin and other alleged scams in India convinced a number of Bollywood celebrities to promote his book, "Cryptocurrency for Beginners." He even tried to make himself a bit of a celebrity, proclaiming himself a "cryptocurrency guru," as he led efforts that cost investors between $769 million and $2 billion.

Not all the celebrities know they're involved. In one blog post, iCenter featured a video that purported to be an endorsement by Dwayne "The Rock" Johnson, holding a sign featuring iCenter's logo. Videos of Justin Timberlake and Christopher Walken were deceptively edited so they appeared to praise iCenter, too.

Fraudulent initial coin offerings

Another popular scam technique is called an "initial coin offering." A potentially legitimate investment opportunity, an initial coin offering essentially is a way for a startup cryptocurrency company to raise money from its future users: In exchange for sending active cryptocurrencies like bitcoin and ethereum, customers are promised a discount on the new cryptocoins.

Many initial coin offerings have turned out to be scams, with organizers engaging in cunning plots, even renting fake offices and creating fancy-looking marketing materials. In 2017, a lot of hype and media coverage about cryptocurrencies fed a huge wave of initial coin offering fraud. In 2018, about 1,000 initial coin offering efforts collapsed, costing backers at least $100 million. Many of these projects had no original ideas – more than 15% of them had copied ideas from other cryptocurrency efforts, or even plagiarized supporting documentation.

Investors looking for returns in a new technology sector are still interested in blockchains and cryptocurrencies – but should beware that they are complex systems that are new even to those who are selling them. Newcomers and relative experts alike have fallen prey to scams.

In an environment like the current cryptocurrency market, potential investors should be very careful to research what they're putting their money into and be sure to find out who is involved as well as what the actual plan is for making real money – without defrauding others.

Provided by The Conversation