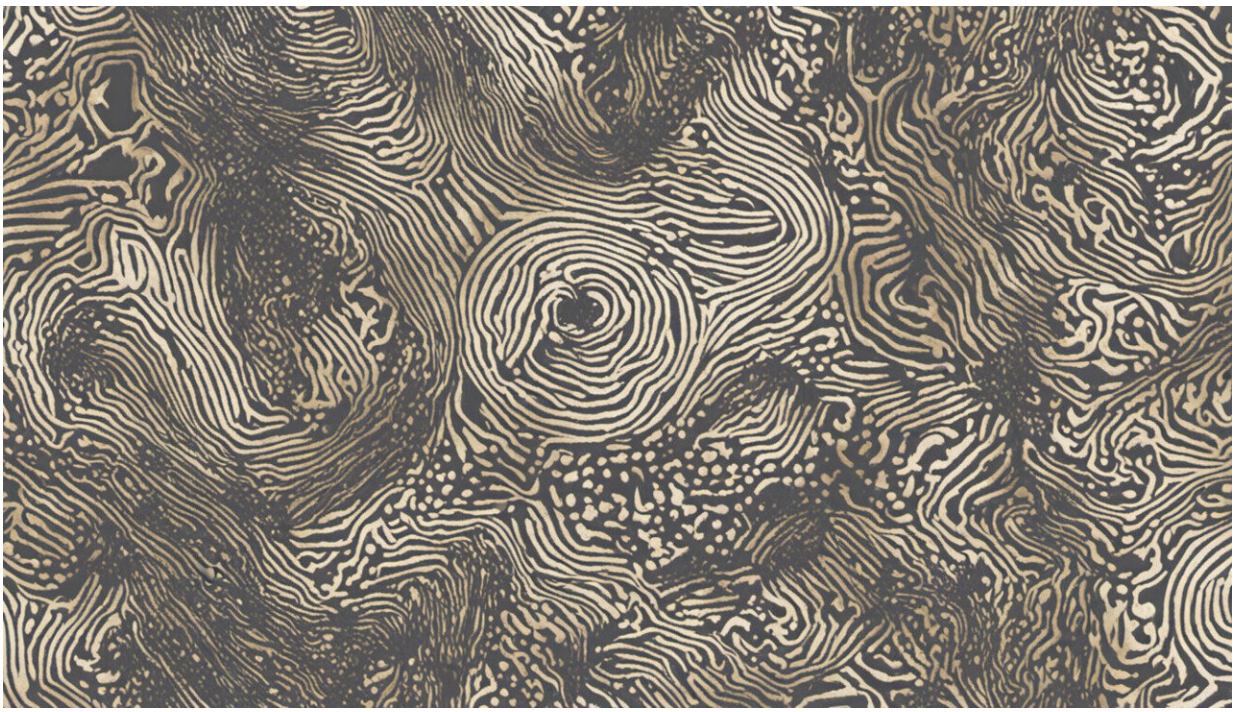
Crypto theft is on the rise: How the crimes are committed, and how you can protect yourself

February 3 2022, by Aaron M. Lane



Credit: AI-generated image (disclaimer)

News emerged overnight of the potential theft of more than US$326 million (A$457.7 million) of Ethereum tokens from a blockchain bridge (which connects two blockchains so cryptocurrency can be exchanged between them).

It's no surprise. Crypto crime has been on the rise—especially since the pandemic began. How are these crimes committed? And what can you do to stay ahead of scammers?

Direct theft vs scams

There are two main ways criminals obtain cryptocurrency: stealing it directly, or using a scheme to trick people into handing it over.

In 2021, crypto criminals directly stole a record US$3.2 billion (A$4.48 billion) worth of cryptocurrency, according to Chainalysis. That's a fivefold increase from 2020. But schemes continue to overshadow outright theft, enabling scammers to lure US$7.8 billion (A$10.95 billion) worth of cryptocurrency from unsuspecting victims.

Crypto crime is a fast-growing enterprise. The rise of the crypto economy and decentralized finance (or DeFi), coupled with record cryptocurrency prices in 2021, has provided criminals with lucrative opportunities.

Australian data confirm the global trends. The Australian Consumer and Competition Commission reported more than A$26 million was lost to scams involving cryptocurrency in 2020 from 1,985 reports. In December, federal police told the ABC crypto scam losses for 2021 exceeded A$100 million. That's despite many incidents likely left unreported, often due to embarrassment by victims.

Theft from exchanges

Most consumers obtain cryptocurrency from an exchange. This involves opening an account and depositing currency, such as Australian dollars, before converting it to a chosen cryptocurrency.

Typically the cryptocurrency is held in a "custodial wallet." That means it's assigned to the consumer's account, but the private keys that control the cryptocurrency are held by the exchange. In other words, the exchange stores the cryptocurrency on the consumer's behalf.

But just as a bank doesn't hold all of its deposits in cash, an exchange will only hold enough cryptocurrency in "hot" wallets (connected to the internet) to facilitate customer transactions. For security, the remainder is held in "cold" wallets (not connected to the internet).

Unlike a bank, however, the government does not have a financial claims scheme to guarantee cryptocurrency deposits if the exchange goes bust.

The recent BitMart hack is a cautionary tale. On December 4, the exchange announced it had "identified a large-scale security breach" resulting in the theft of about US$150 million (A$210.6 million) in crypto assets from hot wallets.

BitMart temporarily suspended withdrawals and later promised it would use its "own funding to cover the incident and compensate affected users." It's unclear when this will happen, with the CNBC reporting in January that customers were still unable to access their cryptocurrency. BitMart wasn't the first exchange to be hacked, and it won't be the last.

Similarly, consumers may be left with losses if an exchange fails for commercial reasons, rather than theft. Australians were left stranded in December when liquidators were appointed over Melbourne-based exchange myCryptoWallet.

One way consumers can protect themselves from exchange theft, or insolvency, is to transfer their cryptocurrency from the exchange to a software wallet (a secure application installed on a computer or smartphone) or a hardware wallet (a hardware device that can be

disconnected from the computer and internet).

The cryptocurrency will then be under your direct control. But be warned, if you lose your private keys, you lose your cryptocurrency.

Types of scams

Drawing on the ACCC's latest edition of the Little Black Book of Scams , the following types of scam are commonly observed in the cryptocurrency space, where the scammer is not personally known to the target:

- Email phishing: The scammer sends unsolicited emails asking for personal login details, which can be used to steal cryptocurrency. Alternatively, they may offer "prizes" or "rewards" in exchange for a deposit.
- Investment scams: The scammer creates a website that resembles a legitimate investment trading platform. It may be a fraudulent copy of a real business, or a completely bogus one. They may even post fake advertisements on social media platforms, with fake celebrity endorsements. In the latest news, billionaire mining magnate Andrew "Twiggy" Forrest has launched criminal proceedings against Meta (previously Facebook) for allowing scam ads using his image. More sophisticated operations will have multiple scammers emailing and calling victims to give the impression of being a legitimate organization. After cryptocurrency deposits are made, victims may be able to "trade" on the fake platform but can't withdraw their supposed earnings. Delay tactics include asking for further deposits to be made for fees or taxes.
- Romance scams: The scammer creates a fake profile and matches with victims on a dating app or website. They may then ask for funds to help them with a personal crisis, such as needing

a surgery. Or they may say they're trading cryptocurrency and encourage the target to get involved, leading the victim into an investment scam, as described above.

If a victim doesn't already have a cryptocurrency exchange account, scammers may also coach them on how to open one. Some will mislead victims into installing remote access software on their computer, granting the scammer direct access to their internet banking or exchange account.

Practical challenges

There are practical legal challenges in the crypto crime environment. While reporting scams can be helpful in providing data and intelligence for regulators and law enforcement, it's unlikely to result in the recovery of funds.

Taking civil legal action may be possible, too, but identifying perpetrators is difficult. Since cryptocurrency is by its very nature global and decentralized, payments are often made to parties outside of Australia.

So prevention is easier than a cure. The main way to avoid being scammed is to ensure you know exactly who you're dealing with, transact through a reputable exchange and ensure all the channels you go through are verified. If an offer sounds too good to be true, it almost certainly is.

Regulation on the horizon

In Australia, cryptocurrency exchanges must be registered with AUSTRAC, in compliance with anti-money laundering and counter-terror financing obligations. But there are currently no other licensing

requirements (such as capital requirements or cybersecurity, for example).

Last year, the Senate Select Committee into Australia as a Technology and Financial Centre recommended a more comprehensive licensing framework. The Australian government agreed with the recommendation, and the federal treasury department is due to begin consulting on what this will look like.

Mandatory measures to curb cryptocurrency crime at the exchange level will likely be high on the agenda.

Provided by The Conversation