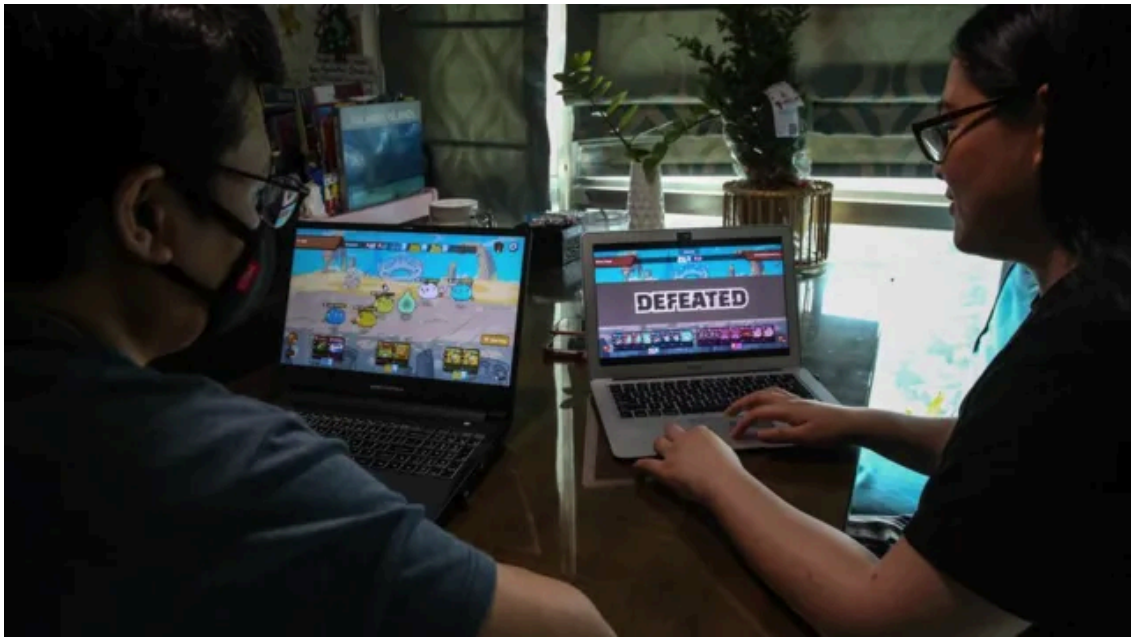
Ronin Network: What a $600m hack says about the state of crypto

By By Joe Tidy

Published: 2022-03-30 · Archived: 2026-04-05 17:43:07 UTC



Getty Images

Axie Infinity is a popular game allowing players to earn through NFTs and cryptocurrency

Thousands, if not millions, of people could have lost money in the second largest crypto hack in history.

Ronin Network, a key platform powering the popular mobile game Axie Infinity, has had $615m (£467m) stolen.

A 20-year-old from Wiltshire, Dan Rean, is one of those affected. He told the BBC: "I have lost 0.15 Ethereum, about $500. It's bad but I have friends in a worse position."

Jack Kenny is one of those friends, and said: "I'm down about $10,000."

The 23-year-old from Ireland added: "I don't think people fully understand the significance of this hack - $600m is a very big portion of all the assets in this network."

Another man from the US east coast says he has lost $8,000, but adds there are people who may have lost their "life savings" after saving up digital coins from playing Axie Infinity.

Axie Infinity

Players fight in game with Axies

In the game, players fight cartoon pets called Axies to earn cryptocurrency.

The game is hugely popular with millions of players around the world hoping to win cryptocurrency and collect the game's non-fungible tokens (NFTs).

Its particularly big in the Philippines, where playing has become a full-time and potentially lucrative job.

- The real victims of mass crypto-hacks
- Crypto-exchange loses $150m to hackers

Ronin Network, which is also owned by Vietnamese parent company Sky Mavis, allows players to exchange the digital coins they earn in Axie Infinity with other cryptocurrencies like Ethereum.

It says a hacker transferred $540m worth of cryptocurrency to themselves six days ago, but the company only noticed on Tuesday when a customer was unable to withdraw their funds.

The stolen stash has since risen in value with the price of cryptocurrencies to be worth about $615m.

It's just the latest in a string of mass crypto heists in the last year totalling well over $2bn.

The sequence of events around the hack tells us a lot about the perils of cryptocurrency and decentralised finance.

Will customers get their money back?

Ronin Network says it is "working with law enforcement officials, forensic cryptographers, and our investors to make sure all funds are recovered or reimbursed".

Initially, it put out one statement on its substack - a newsletter service - and taken its website offline.

It has also disabled comments on its company posts on social media.

Later the company replied to the BBC's requests for comment saying it was "committed" to reimbursing customers but would not give a guarantee.

"I've not tried customer support because I know it'll be useless," says Dan.

"I just have to wait to hear from them if and when it'll be fixed, and I can hopefully get my Ethereum out. Crypto companies don't really work in the same way as regular companies," Dan explains sympathetically.

Retuers

73,600 Ethereum and 25.5M USDC were stolen from the Ronin bridge in two transactions

Ronin Network has not yet told customers what's happening with their funds or when they will get their money back.

In most cases of mass crypto hacks, customers are reimbursed in some way, but it can take months or years.

Cryptocurrency writer David Canellis, from Protos, says direct communication with cryptocurrency companies is notoriously poor.

"When you're dealing with entities that are handling more than half a billion dollars you'd expect a little bit more avenues and openness to communication - especially when there has been such a lapse in security around this hack.

"But then again, one primary tenet of the ecosystem is that anyone at all can launch their own projects, and there should be no barriers to this."

How it happened

Ronin Network says that the hack started in November 2021, when Axie Infinity's user base swelled to an unsustainable size.

The company said the influx of players caused "immense user load", which forced it to loosen security procedures to cope with the increased demand.

It says that things calmed down in December, but that it forgot to retighten its security, and the hackers took advantage of the backdoor left open.

Economist and author Frances Coppola says: "This is pretty typical of crypto companies.

"We've seen so many hacks and exploits caused by - to be blunt - frank carelessness and lack of concern for the safety of people's funds.

"Crypto companies are sometimes so anxious to make 'loadsamoney', or simply accommodate high demand, that they put out badly designed and tested code, compromise security, or place too much reliance on infrastructure."

The five largest-ever cryptocurrency hacks

Figures from cryptocurrency analysis company Elliptic, based on the dollar value at time of hack:

- $325m - Wormhole, February 2022
- $470m - Mt Gox, February 2014.
- $532m - Coincheck, January 2018
- $540m - Ronin Bridge, March 2022.
- $611m - Poly Network, August 2021

Why does this keep happening?

Experts say cryptocurrency is increasingly being seen as low hanging fruit by hackers.

Cryptocurrency companies are "huge honeypots for hackers", says Tom Robinson, of Elliptic.

"Crypto transactions are irreversible, so if a hacker can get their hands on it, it's very difficult for anyone to retrieve it," he says.

Mr Robinson said it is also attractive because huge pay days are possible without the extra hassle of cybercrime like ransomware, where criminals have to negotiate with hacked companies.

It's not known who is behind this latest hack, but it is not necessarily cyber-criminals out to make money for themselves. For example, state-sponsored hackers have been identified as the culprits behind some crypto heists.

According to cryptocurrency researchers at Chainalysis, North Korean hackers stole almost $400m (£291m) worth of digital assets in at least seven attacks on cryptocurrency platforms last year.

Are crypto-currencies the future of money?

Source: https://www.bbc.com/news/technology-60933174