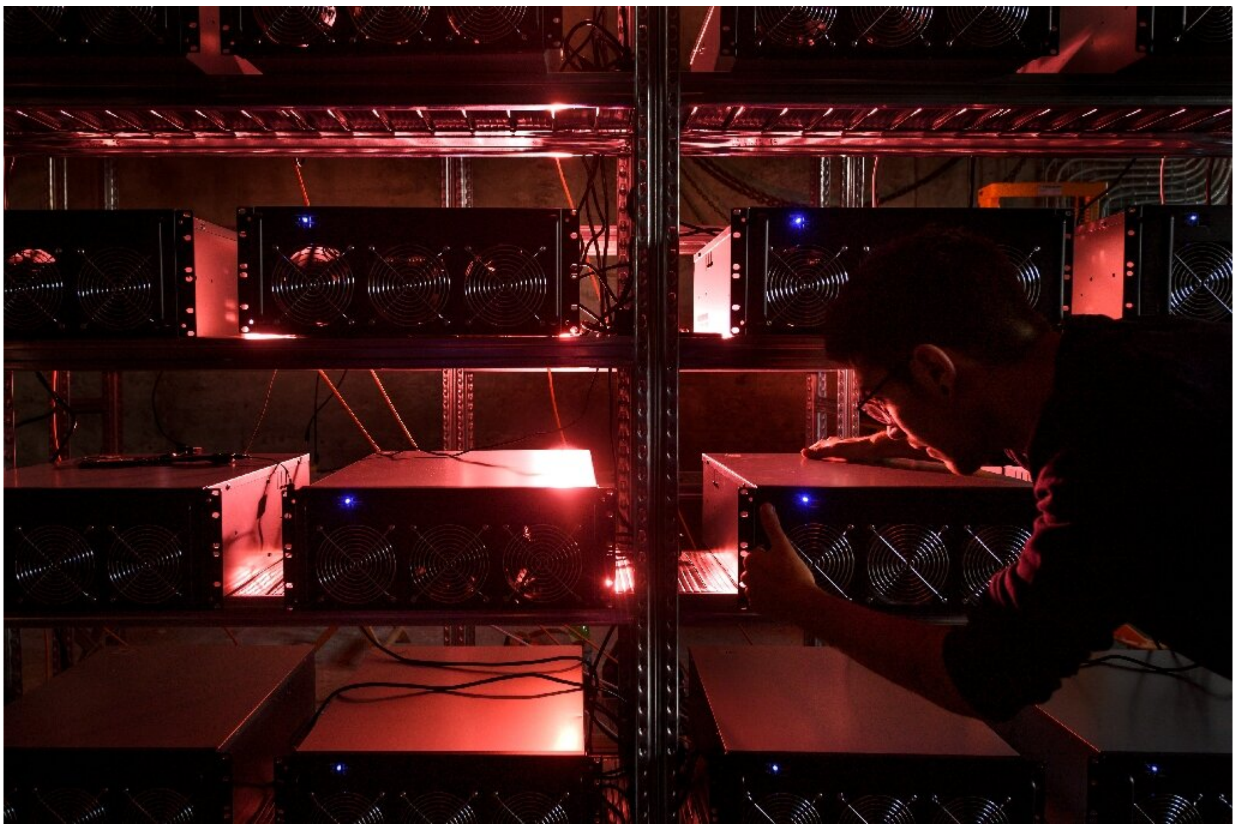
The curious case of the $600 million crypto heist

August 12 2021, by Katy Lee



Despite their volatility and concerns over the huge quantities of electricity involved in trading them, cryptocurrencies like Bitcoin and Ethereum have soared in popularity in recent years.

Cryptocurrency investors have been transfixed over the past few days by the antics of a mysterious hacker who stole more than $600 million—before gradually giving it back.

But was the thief a good samaritan who stole the money to expose a dangerous security flaw, or did they simply realise they were about to be caught?

The hacker struck Poly Network, a company that handles cryptocurrency transfers, on Tuesday in one of the biggest thefts of digital monies in history.

But by Thursday the perpetrator had given back almost all of the stolen funds in a slow trickle of transactions.

In messages embedded in the transfers, the thief insisted the money had been stolen with good intentions.

"I am not very interested in money!" the hacker wrote, adding it was "always the plan" to return the funds.

Digital sleuths

Despite their volatility and concerns over the huge waste of electricity they generate, cryptocurrencies like Bitcoin and Ethereum have soared in popularity in recent years.

Their combined market value currently stands at nearly $2 trillion, creating alluring prospects for hackers.

Most notoriously, thieves stole 850,000 Bitcoins from Japanese exchange Mt. Gox in 2014. Worth around $470 million at the time, the coins would today be worth a staggering $38 billion.

Another Japanese exchange, Coincheck, was hacked for nearly $500 million in 2018.

But in both cases, the technology that cryptocurrency uses allowed some of the funds to be traced—even though for Mt. Gox, it came too late to save the company.

US oil company Colonial Pipeline paid a $4.4 million ransom in Bitcoin to hackers in May, but the FBI was able to track down most of the coins and seize them.

Cryptocurrencies use blockchains, digital ledgers that record every transaction made.

Pawel Aleksander, an expert in tracking stolen cryptocurrency, said thieves typically try to cover their tracks by splitting the money up and moving it around—"sometimes using hundreds of thousands of consecutive transactions".

But his company Coinfirm is among a growing number that specialise in following dizzyingly complicated blockchain transactions, helping law enforcement agencies and investors to trace stolen assets.

While many crypto-aficionados are hailing the Poly hacker as a principled hero, others suspect they began handing the money back because sleuths were on their trail.

The returns began after SlowMist, another investigative firm, claimed to have identified some of the hacker's personal details, including their email address.

"It's hard to say what the hacker's initial intention was," said Aleksander's colleague Roman Bieda.

"The hacker could be simply afraid of action taken against him," he suggested, although he added that "white hat" ethical hackers do often seek to publicly shame companies for their security flaws.

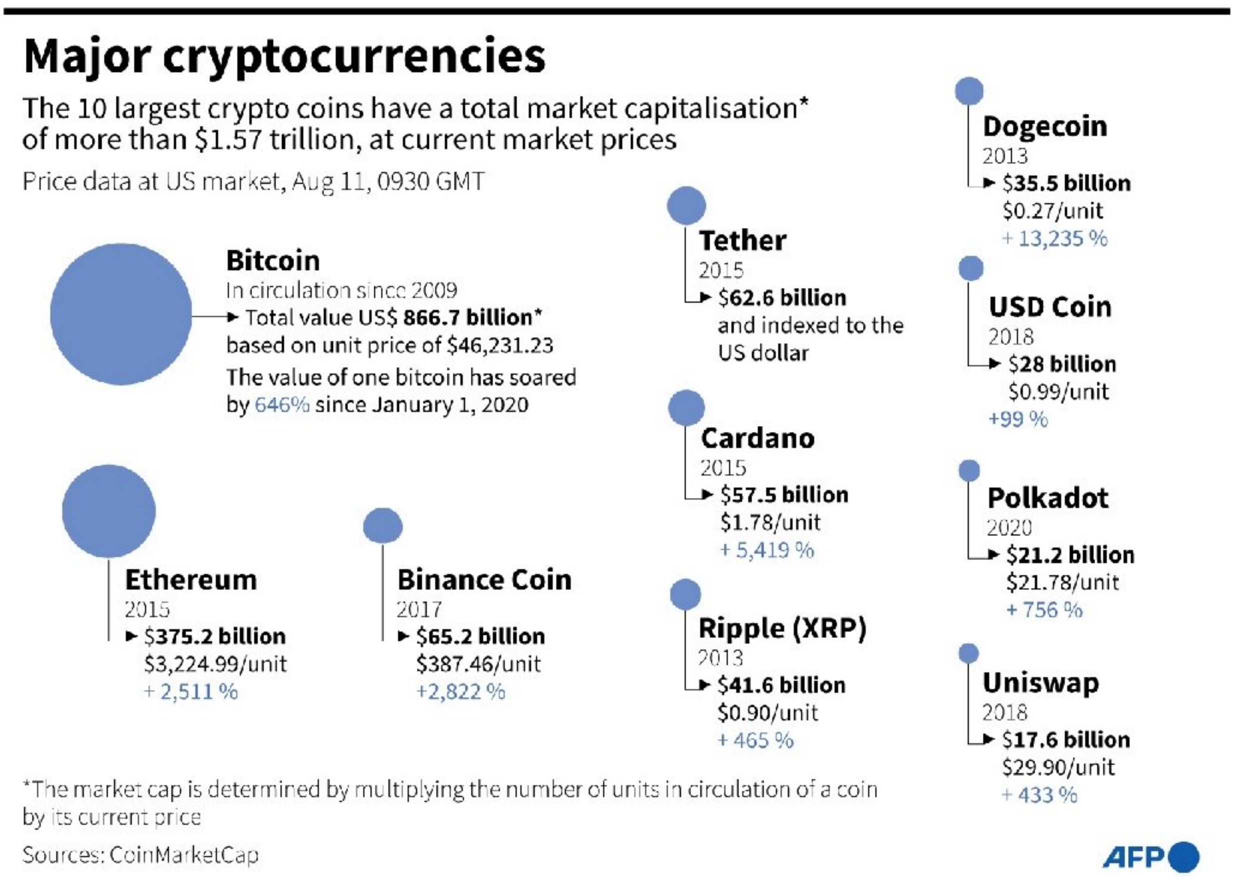
In an encrypted exchange with the hacker dubbed "Mr White Hat", Poly offered $500,000 as a reward and promised: "We assure you that you will not be accountable for this incident."

But the hacker wrote that they had refused the bounty, saying: "I will send all of their money back."

End of the Wild West?

Crimes involving cryptocurrencies are on a downward trend, despite spectacular thefts like this one and concerns about their use by criminal gangs.

A report this month by security firm CipherTrace estimated global crypto-crime losses at $1.9 billion last year, down from $4.5 billion in 2019.



The 10 biggest cryptocurrencies by current market capitalisation, as of August 11.

It did, however, warn of an alarming rise in hacking and fraud linked to decentralised finance, or "defi"—a form of crypto-financing, including loans, designed to cut out intermediaries like banks.

The Poly heist is part of that trend, with the company calling it the biggest hack "in defi history".

"The imagination of fraudsters in this industry is constantly developing," said Syedur Rahman, a British lawyer who specialises in cases involving cryptocurrencies.

But he added that tighter regulations are increasingly forcing cryptocurrency exchanges to verify users' identities, while law enforcement agencies are growing more experienced in handling crypto-crimes.

Hackers extracted a $4.4 million ransom in Bitcoin from oil company Colonial Pipeline in May, but the FBI was able to track down most of the coins and seize them.

Retrieving stolen crypto-assets can still be difficult, however.

"Criminal activities in crypto are very much multinational," said Aleksander.

"It's typical that the victims sit in different jurisdictions, and the exchanges are registered in different jurisdictions."

Victims' battle to claw back money stolen in the Mt. Gox hack has been bogged down in years of international litigation.

And hiring sleuths to trace stolen assets is an expensive option that is often out of reach for individual investors hit by hackers.

"When you have a consumer who has lost a nominal sum, there's not much that can be done," said Rahman.