» Print

Mt. Gox bitcoin debacle: huge heist or sloppy glitch?

9:10am EST

By Jeremy Wagstaff

SINGAPORE (Reuters) - Close to half a billion dollars worth of the bitcoin virtual currency has gone missing from an exchange in Tokyo - in what is either the bank heist of the century or a sloppy glitch, or a combination of the two.

Mark Karpeles, the 28-year-old French CEO of Mt. Gox, which once handled around 80 percent of the world's bitcoin trades, filed for bankruptcy at a Tokyo District Court late on Friday. His lawyer said that nearly all the bitcoins in the exchange's possession - 850,000 of them - were missing. Karpeles blamed hackers.

At current bitcoin rates on other exchanges, that would mean $473 million is lost - around 7 percent of all bitcoins minted.

"If the theft is true," said Campbell Harvey, a professor at Duke University's Fuqua School of Business, "it's the biggest bank heist in history," aside from when Saddam Hussein ordered his son to withdraw $1 billion from Iraq's central bank in 2003.

How this happened remains a mystery. But most observers say Mt. Gox's laxness played a key role in the debacle.

"When I first signed up to it, it was clearly not fit to be a financial services company," said Jon Rushman, who researches and lectures about bitcoin at England's University of Warwick. But things got better, he said: "It has been a process of learn-by-doing that they have discovered all sorts of things they should be doing, but were not."

No official explanation has been forthcoming beyond blaming hackers and weaknesses in Mt. Gox's system.

A document circulating on the internet that purports to be a crisis strategy paper prepared on behalf of Mt. Gox blamed the hole on a "malleability-related theft which went unnoticed for several years." Mt. Gox has not confirmed the authenticity of the document.

The phrase, says Ethan Heilman, a research fellow at Boston University, refers to a bug in the bitcoin process whereby someone could trick Mt. Gox into thinking a transaction had failed - and therefore keep repeating it.

This, say Heilman and others, could explain the disappearance of the money - even though the bug has been known for a while, and has been fixed on other exchanges.

STRETCHING CREDIBILITY

More problematic is another part of the document's purported explanation.

Usually bitcoins' private keys - something similar to a personal bank PIN code - are stored offline, where hackers can't get them. This 'cold storage' is unconnected to the online part - the hot wallet. The document says "the cold storage has been wiped out due to a leak in the hot wallet" - a statement experts say doesn't make sense.

If true, this suggests the vast majority of Mt. Gox's bitcoin deposits were leaking out without anyone noticing.

This stretches credibility, says Anthony Hope, who heads compliance for Hong Kong-based bitcoin company MatrixVision. Once Mt. Gox was aware of the malleability bug, why didn't they check their cold storage? "This is like someone saying that you put your wine in a cellar to keep cool, then someone tells you that a particular vintage had loose corks," he said. "You'd presumably go into the cellar to ensure your bottles were not affected."

At Singapore-based Coin Of Sale, Tomas Forgac said: "If this was long-term leakage which went unnoticed, it shows an unbelievable level of incompetence."

'THOUSANDS OF SOCKS'

If the bitcoins have been stolen, the thief or thieves would have several options to convert them into cash, said Boston University's Heilman.

They could have used a "mixing service" to mix one group of funds with those of other people. They could also have used a service like localbitcoins.com to trade bitcoins for cash in person. "There are many possibilities for cashing out, although fencing this many bitcoins would be difficult," he said.

To do that, says Charles McFarland, a research engineer at online security company McAfee, the thief or thieves would have to conceal their tracks by spreading the bitcoin around prior to laundering it into cash.

Trying to do so from a single bitcoin wallet would have been like stuffing thousands of socks in a dryer while everyone else is throwing in only a single pair.

"For this reason it's a safe bet to say the stolen bitcoins are most likely paid out in numerous wallets so each transaction can hide among the trees," McFarland said. That, he said, would make it "expensive, if not impossible, to track."

Knowing whether this was theft or negligence, or both, will take time, and may never happen. U.S. federal prosecutors have subpoenaed Mt. Gox - and other bitcoin businesses - to seek information on a spate of disruptive cyber attacks.

But bitcoin is an unregulated industry, requires no technical audits or risk management procedures - and offers few ways of prosecuting those who might have acted illegally, says Zennon Kapron, who runs a finance consultancy in Shanghai.

"The unfortunate part is that we may never know exactly how this happened," he says.

(Additional reporting by Sophie Knight in TOKYO; Editing by Ian Geoghegan)
