

Hackers Have Walked Off With About 14% of Big Digital Currencies

By **Olga Kharif**

January 18, 2018, 8:49 AM EST

-
- Cybercriminals compromise Bitcoin, Ether supply, blockchains
 - Crypto-crazed users adopt technology without weighing risks
-

Digital currencies and the software developed to track them have become attractive targets for cybercriminals while also creating a lucrative new market for computer-security firms.

In less than a decade, hackers have stolen \$1.2 billion worth of Bitcoin and rival currency Ether, according to [Lex Sokolin](#), global director of fintech strategy at Autonomous Research LLP. Given the currencies' explosive surge at the end of 2017, the cost in today's money is much higher.

“It looks like crypto hacking is a \$200 million annual revenue industry,” Sokolin said. Hackers have compromised more than 14 percent of the Bitcoin and Ether supply, he said.

All told, hacks involving cryptocurrencies like Bitcoin have cost companies and governments \$11.3 billion through lost potential tax revenue from coin sales and illegitimate transactions, according to Susan Eustis, chief executive officer of WinterGreen Research. The blockchain ecosystem -- the decentralized “distributed ledgers” that track crypto transactions -- is also vulnerable.

Those losses could snowball as more companies and investors rush into the white-hot cryptocurrency market without weighing the dangers or taking steps to protect themselves.

Super-Secure?

Blockchain records are shared, making them hard to alter, so some users see them as super-secure. But in many ways they are no safer than any other software, Matt Suiche, who runs the blockchain security company Comae Technologies, said in a phone interview.

And since the market is immature, blockchains may even be more vulnerable than other software. There are thousands of them, each with its own bugs. Until the field is winnowed to a few favorites, as happened with web browsers, securing them all will be a challenge.

“Each implementation is going to have its own problems,” Suiche said. “The more implementations, the harder it is to cover all of them.”

Blockchains can track identity information, property records and even digital car keys, not just cryptocurrency. But of course, they do that too, and stolen Bitcoins can be converted into hard cash.

So while hacking a blockchain may be harder than breaking into a retailer's database, "the rewards are greater," according to Andras Cser, an analyst at Forrester Research. "You have much more information you can steal."

Exploiting Forks

Many blockchains started as forks that diverged from existing crypto ledgers, and as Taiwanese security researchers have [pointed out](#), every fork gives hackers a new way to try to falsify data.

In a Dec. 25 paper, researchers at the Institute of Electrical and Electronics Engineers outlined ways hackers can spend the same Bitcoins twice, the very thing blockchains are meant to prevent. In a Balance Attack, for instance, hackers delay network communications between subgroups of miners, whose computers verify blockchain transactions, to allow for double spending.

"We have no evidence that such attacks have already been performed on Bitcoin," the IEEE researchers [said](#). "However, we believe that some of the important characteristics of Bitcoin make these attacks practical and potentially highly disruptive."

'Sensitive Data'

A researcher from Cisco Talos, a security group, found [vulnerabilities](#) in Ethereum clients, including a bug that "can lead to the leak of sensitive data about existing accounts." A security hole in the Parity wallet resulted in losses of [\\$155 million](#) in November.

In December, Yobit, an exchange in South Korea, said it [would file](#) for bankruptcy following an attack in which it lost 17 percent of its assets. The same month, mining service NiceHash said hackers stole as much as \$63 million in Bitcoin from its virtual wallet.

Smart contracts -- blockchain-based programs that automate asset transfers -- are also vulnerable. In 2016, hackers stole at least \$50 million out of the DAO, a venture-capital smart contract. Only an update to Ethereum allowed users to get their money back.

Programmers' old-school mindsets are partly to blame for the technology's flaws.

“When you have a bug, you release a patch,” Richard Ma, co-founder of Quantstamp, a company backed by venture-capital firm Y Combinator Inc. “With a smart contract, you deploy it to the network, and it’s not possible to ever change it again.”

Opportunity Knocks

But Ma sees an opportunity. In March, Quantstamp will release an automated tool that scours smart contracts for bugs. Established security firms such as McAfee Inc. may also repurpose their wares for the blockchain crowd.

“In many cases, our existing products can help secure the ecosystem,” Steve Grobman, chief technology officer of McAfee, said in a phone interview. “In general, it will be vulnerable to threats just like any other software system.”

The market for software, services and hardware to secure blockchain activity should grow to \$355 billion as the digital economy moves to cybercurrency and banks and the financial community totally restructure, according to WinterGreen. It was \$259 million in 2017.

Let’s hope they put all that money somewhere safe.


For digital currency prices and other data, visit:

XBT <Curncy> GP D

VCCY

For more on cryptocurrencies, check out the *Decrypted* podcast:

<https://cms.megaphone.fm/channel/BLM3923153289?selected=BLM2696398548>

Before it's here, it's on the Bloomberg Terminal. 

[LEARN MORE](#)