https://www.wsj.com/articles/bitcoin-blockchain-hacking-arrests-93a4cb29

The U.S. Cracked a $3.4 Billion Crypto Heist—and Bitcoin's Anonymity

Federal authorities are making arrests and seizing funds with the help of new tools to identify criminals through cryptocurrency transactions

By Robert McMillan Follow
April 12, 2023 10:19 am ET

James Zhong appeared to have pulled off the perfect crime.

In December 2012, he stumbled upon a software bug while withdrawing money from his account on Silk Road, an online marketplace used to hide criminal dealings behind the seemingly bulletproof anonymity of blockchain transactions and the dark web. Mr. Zhong, a 22-year-old University of Georgia computer-science student at the time, used the site to buy cocaine.

"I accidentally double-clicked the withdraw button and was shocked to discover that it resulted in allowing me to withdraw double the amount of bitcoin I had deposited," he later said in federal court. After the first fraudulent withdrawal, Mr. Zhong created new accounts and with a few hours of work stole 50,000 bitcoins worth around $600,000, court papers from federal prosecutors show.

Federal officials closed Silk Road a year later on criminal grounds and seized computers that held its transaction records. The records didn't reveal Mr. Zhong's caper at first. Authorities hadn't yet mastered how to track people and groups hidden behind blockchain wallet addresses, the series of letters and numbers used to anonymously send and receive cryptocurrency. One elemental feature of the system was the privacy it gave users.

Mr. Zhong moved the stolen bitcoins from one account to another for eight years to cover his tracks. By late 2021, the red-hot crypto market had raised the value of his trove to $3.4

billion. He still lived in a modest house in Athens, Ga., and dressed in shorts and T-shirts. He also had a lake-house getaway in Gainesville, Ga., a Lamborghini sports car and a $150,000 Tesla.

In November 2021, federal agents surprised Mr. Zhong with a search warrant and found the digital keys to his crypto fortune hidden in a basement floor safe and a popcorn tin in the bathroom. Mr. Zhong, who pleaded guilty to wire fraud, is scheduled to be sentenced Friday in New York federal court, where prosecutors are seeking a prison sentence of less than two years.

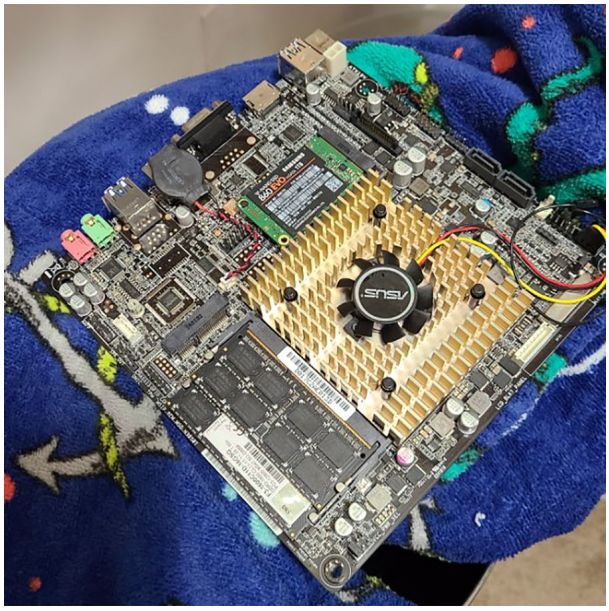
Mr. Zhong's case is one of the highest-profile examples of how federal authorities have pierced the veil of blockchain transactions. Private and government investigators can now identify wallet addresses associated with terrorists, drug traffickers, money launderers and cybercriminals, all of which were supposed to be anonymous.

James Zhong in an undated photo posted on his Foursquare profile page.

Law enforcement agencies, working with cryptocurrency exchanges and blockchain-analytics companies, have compiled data gleaned from earlier investigations, including the Silk Road case, to map the flow of cryptocurrency transactions across criminal networks worldwide. In the past two years, the U.S. has seized more than $10 billion worth of digital currency through successful prosecutions, according to the Internal Revenue Service—in essence, by following the money. Instead of subpoenas to banks or other financial institutions, investigators can look to the blockchain for an instant snapshot of the money trail.

Government investigators exploit a feature of bitcoin and many other digital currencies: Every transaction is stored forever in blockchain's online ledger and open for anyone to see. Since Mr. Zhong's heist, authorities and private firms have compiled the equivalent of a blockchain address book to aid the IRS, Federal Bureau of Investigation and state and local authorities investigating cybercrimes. The blockchain-analytics company Chainalysis Inc., based in New York, said it has mapped more than a billion wallet addresses, separating out legitimate and questionable holdings and identifying the exchanges where the cryptocurrency is converted to cash.

"If there's one thing the blockchain does really well, it preserves evidence perfectly," said Jonathan Levin, a pioneer cryptocurrency sleuth and one of the founders of Chainalysis.



The popcorn tin where authorities found a computer motherboard. The motherboard held some of the digital keys to James Zhong's cryptocurrency fortune.

UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK (2)

When bitcoins are stolen, the criminal is now "like a guy that robbed a bank in the snow," said Matthew Price, a former IRS investigator who now runs investigations for cryptocurrency exchange Binance Inc. The criminal's name might be unknown, he said, but digital breadcrumbs, like footprints in the snow, remain for authorities to follow.

Federal investigators have used blockchain-tracing techniques to shut down a child pornography website, disrupt funding for terrorist organizations and, in the Justice Department's largest-ever financial seizure, retrieved $3.6 billion from a New York couple charged with laundering the proceeds of the 2016 hack of cryptocurrency exchange Bitfinex. With each case, more accounts are added to the government's blockchain address book.

These advances make it difficult for criminals to convert their spoils to cash. After government officials publish wallet addresses connected to crooks, no legitimate cryptocurrency exchange wants to do business with them, fearing legal consequences.

Last year, a group that U.S. officials linked to North Korea stole about $720 million by hacking two cryptocurrency services—Harmony's Horizon Bridge and Sky Mavis's Ronin Network. In February, the FBI published a list of wallet addresses linked to the $100 million Horizon Bridge theft, effectively stonewalling hackers from withdrawing cash through

legitimate exchanges.

Nick Carlsen, an analyst with crypto-security company TRM Labs, said North Korea, which has previously denied involvement in hacking attacks, "can steal huge amounts of crypto, but they seem to have exceeded the illicit crypto industry's capacity to turn those funds into dollars."

Bitcoin breakthrough

In a groundbreaking case, Mr. Levin and his business partner Michael Gonager were brought in to investigate the 2014 collapse of Mt. Gox, a cryptocurrency exchange that was once the world's most popular online destination for buying and selling bitcoin.

They developed software to monitor cryptocurrency transactions, using state-of-the art research, their own data crunching and dogged detective work. "It was really the first time that it had been possible to create a whole entity view of something on the blockchain," Mr. Levin said.

Working from a San Francisco Airbnb, it took three months for Mr. Levin, an economist, and Mr. Gonager, a computer scientist, to learn that Mt. Gox held fewer bitcoins in reserve than it believed. Today, Mr. Levin said, that kind of investigation would take 30 seconds. All told, thieves had stolen 600,000 bitcoins from the exchange.

The work prompted Messrs. Levin and Gonager to start Chainalysis, which now flags risky sources of funds for more than 200 clients, including the IRS, FBI and the Drug Enforcement Administration, as well as banks and cryptocurrency exchanges. The company was recently hired by business partners and creditors of the failed cryptocurrency exchange FTX.

Michael Gonager, seated, and Jonathan Levin, founders of Chainalysis at the company offices in New York City.

PHOTO: SASHA MASLOV FOR THE WALL STREET JOURNAL

Blockchain analytics provide law enforcement investigators with an important piece of the blockchain puzzle—mapping the flow of cryptocurrency belonging to specific people and groups. Greater regulatory scrutiny of cryptocurrency exchanges has also helped. Exchanges have stepped up systems to identify the parties they do business with—under so-called know-your-customer requirements—and are more responsive to law-enforcement inquiries.

A host of blockchain-analytics companies, including Elliptic and CipherTrace, which is owned by MasterCard Inc., have sprung up. Many of them have hired federal investigators who spearheaded the government's first cryptocurrency investigations.

Ransomware victims worldwide paid at least $457 million last year to bitcoin addresses controlled by criminals, according to Chainalysis. Ransomware refers to hackers locking up a computer network by encrypting hard drives and demanding money to reopen them. Blockchain-tracking techniques have made it possible for federal officials to recover more

stolen funds, which has contributed to a slowdown in ransomware payments. The DOJ has seized about $40 million in ransom payments as of November, according to Eun Young Choi, the director of the DOJ's national cryptocurrency enforcement team.

In January, about 150 people gathered at a Palo Alto, Calif., community center to learn more about the new investigative tools, including a Los Angeles County Sheriff's Department detective, a prosecutor from New York's Queens district attorney's office and a police cybercrime investigator from Calgary, Alberta.

Conference organizer Erin West, a Santa Clara County, Calif., prosecutor, described how her county recovered more than $2 million in stolen funds last year from victims of an online scam known as "pig butchering." The scheme involved offshore criminals befriending victims via text and persuading them to put money into phony crypto investments.

Chris Janczewski, a former IRS agent and now the head of global investigations at TRM Labs, told the story of his rise from auditing small-town tax cheats to his work helping break up a global child-pornography distributor. Like many pioneering blockchain investigators, Mr. Janczewski said he was largely self-taught.

"Chris is the real deal. He's a detective's detective that happened upon cryptocurrency at just the right time and figured out how to use the blockchain to identify horrific perpetrators of crimes worldwide," Ms. West said. "He didn't have any tools at that time. He just figured stuff out as any good detective would."

Buying friends

Mr. Zhong told people he had been bullied growing up in Georgia. As a high-school junior, pranksters pulled down his pants while he was at a football game, according to court documents filed in his defense. "I always hated school," he said in the documents. "At least upstairs in my house, I was myself being on a computer."

Computers also provided a financial escape. Mr. Zhong was a cryptocurrency pioneer, who in 2009 was mining hundreds of bitcoins a day. They weren't worth much at the time. But by the time he was in college, he converted some of his digital wealth into $700,000 in cash. He wanted to have a "case full of money like in the movies," Mr. Zhong said, according to a psychological assessment filed with the court. "He hoped the visual appeal of the cash would impress a female into having sexual relations with him. He stated his plan did not work."

For five years after the Silk Road theft, Mr. Zhong sat on his digital treasure. In 2017, he embarked on a $16 million spending spree, much of it spent trying to win friends, according to court papers and his lawyer, Michael Bachner. Mr. Zhong gave away 258 bitcoins, many of them on digital devices each loaded with 50 bitcoins and now worth close to $1.5 million. He hosted friends on chartered planes and boats, at sporting events and in fancy hotels, according to court papers and Clayton Kemker, a former bond salesman who became Mr. Zhong's business partner.

Some of the items recovered during the November 2021 search of James Zhong's house. Authorities reported finding $661,900 in cash.

PHOTO: UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK

Mr. Zhong made his big mistake on Dec. 16, 2020, according to court records and an analysis of his bitcoin transactions by Elliptic. He combined crypto funds the IRS had linked to the Silk Road thefts with legitimate funds he kept in a cryptocurrency exchange.

With Mr. Zhong's Silk Road link in hand, authorities went to the bitcoin exchange that handled the transaction. The exchange gave IRS agents an IP address, 45.20.67.1, and Mr. Zhong's internet service provider confirmed that he had been using that address since 2016. A month later, federal agents searched Mr. Zhong's house and found the digital storage

devices that helped clinch the investigation.

The government seized more than 50,000 bitcoins from Mr. Zhong, which at the time were worth $3.36 billion. A DOJ spokesman declined to comment on the case.

Messrs. Zhong and Kemker had planned a real-estate development that was to encompass 340 apartments, 60,000 feet of retail space and a rooftop bar in Memphis, Tenn. Mr. Zhong pledged $42 million for the project, which has since been abandoned, Mr. Kemker said.

The partnership with Mr. Zhong cost him his life savings, Mr. Kemker said. "He didn't know how to navigate the business world. He just knew coding and tech."

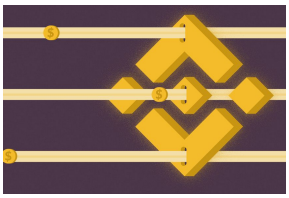
Write to Robert McMillan at robert.mcmillan@wsj.com

Crypto Spotlight

The latest on cryptocurrencies following a spate of challenges, selected by editors

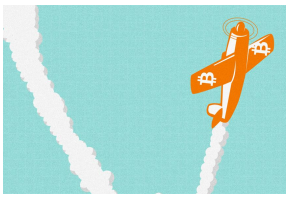
SIGN UP FOR THE WSJ CRYPTO NEWSLETTER

Crypto Crisis: A Timeline of Key Events

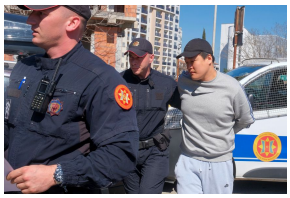


Crypto Giant Binance Courted High-Frequency Traders

Bitcoin Booms in Wake of Bank Crisis



Crypto ETFs Have Bounced Back. But Don't Get Too Excited.



U.S., South Korea Vie for Extradition of Do Kwon

Hong Kong's Crypto Ambitions Get a Boost

Banks Step Up to Serve Crypto Firms

The Couple Behind El Salvador's Bitcoin Experiment