The New York Times https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html

Pipeline Investigation Upends Idea That Bitcoin Is Untraceable

The F.B.I.'s recovery of Bitcoins paid in the Colonial Pipeline ransomware attack showed cryptocurrencies are not as hard to track as it might seem.

By Nicole Perlroth, Erin Griffith and Katie Benner

June 9, 2021

When Bitcoin burst onto the scene in 2009, fans heralded the cryptocurrency as a secure, decentralized and anonymous way to conduct transactions outside the traditional financial system.

Criminals, often operating in hidden reaches of the internet, flocked to Bitcoin to do illicit business without revealing their names or locations. The digital currency quickly became as popular with drug dealers and tax evaders as it was with contrarian libertarians.

But this week's revelation that federal officials had recovered most of the Bitcoin ransom paid in the recent Colonial Pipeline ransomware attack exposed a fundamental misconception about cryptocurrencies: They are not as hard to track as cybercriminals think.

On Monday, the Justice Department announced it had traced 63.7 of the 75 Bitcoins — some $2.3 million of the $4.3 million — that Colonial Pipeline had paid to the hackers as the ransomware attack shut down the company's computer systems, prompting fuel shortages and a spike in gasoline prices. Officials have since declined to provide more details about how exactly they recouped the Bitcoin, which has fluctuated in value.

Yet for the growing community of cryptocurrency enthusiasts and investors, the fact that federal investigators had tracked the ransom as it moved through at least 23 different electronic accounts belonging to DarkSide, the hacking collective, before accessing one account showed that law enforcement was growing along with the industry.

That's because the same properties that make cryptocurrencies attractive to cybercriminals — the ability to transfer money instantaneously without a bank's permission — can be leveraged by law enforcement to track and seize criminals' funds at

the speed of the internet.

Bitcoin is also traceable. While the digital currency can be created, moved and stored outside the purview of any government or financial institution, each payment is recorded in a permanent fixed ledger, called the blockchain.

That means all Bitcoin transactions are out in the open. The Bitcoin ledger can be viewed by anyone who is plugged into the blockchain.

"It is digital bread crumbs," said Kathryn Haun, a former federal prosecutor and investor at venture-capital firm Andreessen Horowitz. "There's a trail law enforcement can follow rather nicely."

Ms. Haun added that the speed with which the Justice Department seized most of the ransom was "groundbreaking" precisely because of the hackers' use of cryptocurrency. In contrast, she said, getting records from banks often requires months or years of navigating paperwork and bureaucracy, especially when those banks are overseas.

Deputy U.S. Attorney General Lisa Monaco, center, announcing the recovery of part of the Colonial Pipeline ransom on Monday. Pool photo by Jonathan Ernst

Given the public nature of the ledger, cryptocurrency experts said, all law enforcement needed to do was figure out how to connect the criminals to a digital wallet, which stores the Bitcoin. To do so, authorities likely focused on what is known as a "public key" and a

"private key."

A public key is the string of numbers and letters that Bitcoin holders have for transacting with others, while a "private key" is used to keep a wallet secure. Tracking down a user's transaction history was a matter of figuring out which public key they controlled, authorities said.

Seizing the assets then required obtaining the private key, which is more difficult. It's unclear how federal agents were able to get DarkSide's private key.

Justice Department spokesman Marc Raimondi declined to say more about how the F.B.I. seized DarkSide's private key. According to court documents, investigators accessed the password for one of the hackers' Bitcoin wallets, though they did not detail how.

The F.B.I. did not appear to rely on any underlying vulnerability in blockchain technology, cryptocurrency experts said. The likelier culprit was good old-fashioned police work.

Federal agents could have seized DarkSide's private keys by planting a human spy inside DarkSide's network, hacking the computers where their private keys and passwords were stored, or compelling the service that holds their private wallet to turn them over via search warrant or other means.

"If they can get their hands on the keys, it's seizable," said Jesse Proudman, founder of Makara, a cryptocurrency investment site. "Just putting it on a blockchain doesn't absolve that fact."

The F.B.I. has partnered with several companies that specialize in tracking cryptocurrencies across digital accounts, according to officials, court documents and the companies. Start-ups with names like TRM Labs, Elliptic and Chainalysis that trace cryptocurrency payments and flag possible criminal activity have blossomed as law enforcement agencies and banks try to get ahead of financial crime.

Their technology traces blockchains looking for patterns that suggest illegal activity. It's akin to how Google and Microsoft tamed email spam by identifying and then blocking accounts that spray email links across hundreds of accounts.

"Cryptocurrency allows us to use these tools to trace funds and financial flows along the blockchain in ways that we could never do with cash," said Ari Redbord, the head of legal affairs at TRM Labs, a blockchain intelligence company that sells its analytic software to law enforcement and banks. He was previously a senior adviser on financial intelligence and terrorism at the Treasury Department.

Several longtime cryptocurrency enthusiasts said the recovery of much of the Bitcoin

ransom was a win for the legitimacy of digital currencies. That would help shift the image of Bitcoin as the playground of criminals, they said.

“The public is slowly being shown, in case after case, that Bitcoin is good for law enforcement and bad for crime — the opposite of what many historically believed,” said Hunter Horsley, chief executive of Bitwise Asset Management, a cryptocurrency investment company.

In recent months, cryptocurrencies have become increasingly mainstream. Companies such as PayPal and Square have expanded their cryptocurrency services. Coinbase, a start-up that allows people to buy and sell cryptocurrencies, went public in April and is now valued at $47 billion. Over the weekend, a Bitcoin conference in Miami attracted more than 12,000 attendees, including Twitter’s chief executive, Jack Dorsey, and the former boxer Floyd Mayweather Jr.

As more people use Bitcoin, most are accessing the digital currency in a way that mirrors a traditional bank, through a central intermediary like a crypto exchange. In the United States, anti-money laundering and identity verification laws require such services to know who their customers are, creating a link between identity and account. Customers must upload government identification when they sign up.

Ransomware attacks have put unregulated crypto exchanges under the microscope. Cybercriminals have flocked to thousands of high-risk ones in Eastern Europe that do not abide by these laws.

More than 12,000 people attended Bitcoin 2021 in Miami last week. Alfonso Duran for The New York Times

After the Colonial Pipeline attack, several financial leaders proposed a ban on cryptocurrency.

“We can live in a world with cryptocurrency or a world without ransomware, but we can’t have both,” Lee Reiners, the executive director of the Global Financial Markets Center at Duke Law School, wrote in The Wall Street Journal.

Cryptocurrency experts said the hackers could have tried to make their Bitcoin accounts even more secure. Some cryptocurrency holders go to great lengths to store their private keys away from anything connected to the internet, in what is called a “cold wallet.” Some memorize the string of numbers and letters. Others write them down on paper, though those can be obtained by search warrants or police work.

“The only way to obtain the truly unseizable characteristic of the asset class is to memorize the keys and not have them written down anywhere,” Mr. Proudman said.

Mr. Raimondi of the Justice Department said the Colonial Pipeline ransom seizure was the latest sting operation by federal prosecutors to recoup illicitly gained cryptocurrency. He said the department has made “many seizures, in the hundreds of millions of dollars, from unhosted cryptocurrency wallets” used for criminal activity.

In January, the Justice Department disrupted another ransomware group, NetWalker, which used ransomware to extort money from municipalities, hospitals, law enforcement agencies and schools.

As part of that sting, the department obtained about $500,000 of NetWalker's cryptocurrency that had been collected from victims of their ransomware.

"While these individuals believe they operate anonymously in the digital space, we have the skill and tenacity to identify and prosecute these actors to the full extent of the law and seize their criminal proceeds," Maria Chapa Lopez, then the U.S. attorney for the Middle District of Florida, said when the case was announced.

In February, the Justice Department said it had warrants to seize nearly $2 million in cryptocurrencies that North Korean hackers had stolen and put into accounts at two different cryptocurrency exchanges.

Last August, the department also unsealed a complaint outing North Korean hackers who stole $28.7 million of cryptocurrency from a cryptocurrency exchange, and then laundered the proceeds through Chinese cryptocurrency laundering services. The F.B.I. traced the funds to 280 cryptocurrency wallets and their owners.

In the end, "cryptocurrencies are actually more transparent than most other forms of value transfer," said Madeleine Kennedy, a spokeswoman for Chainalysis, the start-up that traces cryptocurrency payments. "Certainly more transparent than cash."

Nicole Perlroth is a cybersecurity and digital espionage reporter. She is the bestselling author of the book, "This Is How They Tell Me The World Ends," about the global cyber arms race. More about Nicole Perlroth

Erin Griffith reports on technology start-ups and venture capital from the San Francisco bureau. Before joining The Times she was a senior writer at Wired and Fortune. More about Erin Griffith

Katie Benner covers the Justice Department. She was part of a team that won a Pulitzer Prize in 2018 for public service for reporting on workplace sexual harassment issues. More about Katie Benner

A version of this article appears in print on , Section B, Page 1 of the New York edition with the headline: Cyber Cash Is Traceable After All