CRYPTO DECODED

The IRS has seized $1.2 billion worth of cryptocurrency this fiscal year – here's what happens to it

PUBLISHED WED, AUG 4 202112:15 PM EDTUPDATED WED, AUG 4 20216:31 PM EDT

MacKenzie Sigalos@KENZIESIGALOS

KEY POINTS

- The U.S. government regularly holds auctions for its stockpile of bitcoin, ethereum, litecoin and other cryptocurrencies it seizes and then holds in crypto wallets.
- It really kicked off with the 2013 takedown of Silk Road, a dark web marketplace trading in illegal goods, where bitcoin was often used for payment.
- Interviews with current and former federal agents and prosecutors suggest the U.S. has no plans to step back from its side hustle as a crypto broker.

In June, the U.S. government casually auctioned off some spare litecoin, bitcoin and bitcoin cash.

Lot 4TQSCI21402001 — one of 11 on offer over the four-day auction — included 150.22567153 litecoin and 0.00022893 bitcoin cash, worth more than $21,000 at today's prices. The crypto property had been confiscated as part of a tax noncompliance case.

This kind of sale is nothing new for Uncle Sam. For years, the government has been seizing, stockpiling and selling off cryptocurrencies, alongside the usual assets one would expect from high-profile criminal sting operations.

“It could be 10 boats, 12 cars, and then one of the lots is X number of bitcoin being auctioned,” explained Jarod Koopman, director of the IRS’ cybercrime unit.

Koopman’s team of IRS agents don’t fit the stereotypical mold. They are sworn law enforcement officers who carry weapons and badges and who execute search, arrest and seizure warrants. They also bring back record amounts of cryptocash.

“In fiscal year 2019, we had about $700,000 worth of crypto seizures. In 2020, it was up to $137 million. And so far in 2021, we’re at $1.2 billion,” Koopman told CNBC. The fiscal year ends Sept. 30.

As cybercrime picks up — and the haul of digital tokens along with it — government crypto coffers are expected to swell even further.

Interviews with current and former federal agents and prosecutors suggest the U.S. has no plans to step back from its side hustle as a crypto broker. The crypto seizure and sale operation is growing so fast that the government just enlisted the help of the private sector to manage the storage and sales of its hoard of crypto tokens.

Knowing what you don’t know

The 2013 takedown of Silk Road — a now-defunct online black market for everything from heroin to firearms — is where federal agents really cut their teeth in crypto search and seizure.

“It was totally unprecedented,” said Sharon Cohen Levin, who worked on the first Silk Road prosecution and spent 20 years as chief of the money laundering and asset forfeiture unit in the U.S. Attorney’s Office for the Southern District of New York.

Silk Road, which operated on the dark web, dealt entirely in bitcoin. It was good for users, because it promised them some degree of anonymity. Despite the reputational hit, it was good for bitcoin at the time, helping to pump up its price by giving the token a use case beyond programming circles.

When the government began to dismantle Silk Road, federal agents had to figure out what to do with all the ill-gotten bitcoin.

“There was a wallet with approximately 30,000 bitcoin in it, which we were able to identify and seize. At the time, it was probably the largest bitcoin seizure ever, and it sold for around $19 million,” said Levin.

“No one had ever done anything like it. In fact, there weren’t really companies that you could go to in order to sell the assets. The Marshals Service stepped up and conducted their own auction of the assets where they took bids,” she said.

That bitcoin batch went to billionaire venture capitalist Tim Draper. “It seemed like a large sum of money at the time, but if the government had retained those bitcoins, it would be worth way more today.”

The cache of coins sold in 2014 would be worth more than $1.1 billion as of Wednesday morning. But hindsight is 20/20, and the government isn’t in the business of playing the crypto markets.

What this entire exercise did accomplish, however, was to establish a workflow that remains in place today, one that uses legacy crime-fighting rails to deal with tracking and seizing cryptographically built tokens, which were inherently designed to evade law enforcement.

“I’ve just observed that the government is usually more than a few steps behind the criminals when it comes to innovation and technology,” said Jud Welle, a former federal cybercrime prosecutor of 12.5 years.

“This is not the kind of thing that would show up in your basic training. But I predict within three to five years ... there will be manuals edited and updated with, ‘This is how you approach crypto tracing,’ ‘This is how you approach crypto seizure,’” Welle said.

"‘Follow the money’ is not new. Seizure is not new. What we’re just doing is trying to find a way to apply these tools and techniques to a new fact pattern, a new use case,” he said.

Chain of custody

There are three main junctures in the flow of bitcoin and other cryptocurrencies through the criminal justice system in the U.S.

The first phase is search and seizure. The second is the liquidation of raided crypto. And the third is deployment of the proceeds from those crypto sales.

In practice, that first stage of the process is a group effort, according to Koopman. He said his team often works on joint investigations alongside other government agencies — think government arms such as the Federal Bureau of Investigation, Homeland Security, the Secret Service, the Drug Enforcement Agency, and the Bureau of Alcohol, Tobacco, Firearms and Explosives.

“A lot of cases, especially in the cyber arena, become ... joint investigations, because no one agency can do it all,” said Koopman, who worked on the two Silk Road cases and the 2017 AlphaBay investigation, which culminated in the closure of another popular and massive dark web marketplace.

Koopman explained that his division at the IRS typically handles crypto tracing and open source intelligence, which includes investigating tax evasion, false tax returns, and money laundering. Other agencies that have more money and resources focus on the technical components.

“Then we all come together when it’s time to execute any type of enforcement action, whether that’s an arrest, a seizure or a search warrant. And that could be nationally or globally,” he said.

During the seizure itself, multiple agents are involved to ensure proper oversight. That includes managers who establish the necessary hardware wallets to secure the seized crypto. “We maintain private keys only in headquarters so that it can’t be tampered with,” Koopman said.

Once a case is closed, the U.S. Marshals Service is the main agency responsible for auctioning off the government’s crypto holdings. To date, it has seized and auctioned more than 185,000 bitcoins. That cache of coins is currently worth nearly $7 billion, though many were sold in batches well below today’s price.

It’s a big responsibility for one government entity to take on, which is part of why the Marshals Service no longer shoulders the task alone.

The U.S. General Services Administration, an agency that typically auctions surplus federal assets such as tractors, added confiscated cryptocurrencies to the auction block earlier this year.

And just last week, following a more than yearlong search, the Department of Justice hired San Francisco-based Anchorage Digital to be its custodian for the cryptocurrency seized or forfeited in criminal cases. Anchorage, the first federally chartered bank for crypto, will help the government store and liquidate this digital property. The contract was previously awarded to BitGo.

“The fact that the Marshals Service is getting professionals to help them is a good sign that this is here to stay,” said Levin.

The process of auctioning off crypto, in blocks, at fair market value, likely won’t change, according to Koopman. “You basically get in line to auction it off. We don’t ever want to flood the market with a tremendous amount, which then could have an effect on the pricing component,” he said.

But other than spacing out sales, Koopman said, trying to “time” the market to sell at peak crypto prices isn’t a thing. “We don’t try to play the market,” he said.

In November, the government seized $1 billion worth of bitcoin linked to Silk Road. Because the case is still pending, those bitcoins are sitting idle in a crypto wallet. Had the government sold its bitcoin stake when the price of the token peaked above $63,000 in April, coffers would have been a whole lot bigger than if they liquidated at today’s price.

Where the money goes

Once a case is closed and the crypto has been exchanged for fiat currency, the feds then divvy the spoils. The proceeds of the sale are typically deposited into one of two funds: The Treasury Forfeiture Fund or the Department of Justice Assets Forfeiture Fund.

“The underlying investigative agency determines which fund the money goes to,” Levin said.

Koopman said the crypto traced and seized by his team accounts for roughly 60% to 70% of the Treasury Forfeiture Fund, making it the largest individual contributor.

Once placed into one of these two funds, the liquidated crypto can then be put toward a variety of line items. Congress, for example, can rescind the money and put that cash toward funding projects.

“Agencies can put in requests to gain access to some of that money for funding of operations,” said Koopman. “We’re able to put in a request and say, ‘We’re looking for additional licenses or additional gear,’ and then that’s reviewed by the Executive Office of Treasury.”

Some years, Koopman’s team receives varying amounts based on the initiatives proposed. Other years, they get nothing because Congress will choose to rescind all the money out of the account.

Tracking where all the money goes isn’t a totally straightforward process, according to Alex Lakatos, a partner with DC law firm Mayer Brown, who advises clients on forfeiture.

The Justice Department hosts Forfeiture.gov, which offers some optics on current seizure operations. This document, for example, outlines a case from May where 1.04430259 bitcoin was taken from a hardware wallet belonging to an individual in Kansas. Another 10 were taken from a Texas resident in April. But it is unclear whether it is a comprehensive list of all active cases.

“I don’t believe there’s any one place that has all the crypto that the U.S. Marshals are holding, let alone the different states that may have forfeited crypto. It’s very much a hodgepodge,” said Lakatos. “I don’t even know if someone in the government wanted to get their arms around it, how they would go about doing it.”

A Department of Justice told CNBC he’s “pretty sure” there’s no central database of cryptocurrency seizures.

But what does appear clear is that more of these crypto seizure cases are being trumpeted to the public, like in the case of the FBI’s breach of a bitcoin wallet held by the Colonial Pipeline hackers earlier this spring.

“In my experience, folks that are in these positions in high levels of government, they may be there for a short period of time, and they want to get some wins under their belt,” said Welle.

“This is the kind of thing that definitely captures the attention of journalists, cybersecurity experts, right, a lot of chatter around it.”