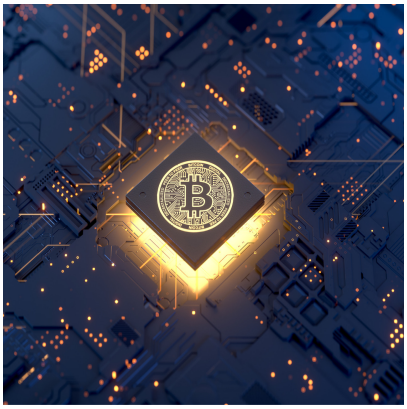

Governments Are Hoarding Crypto But Not How You Think

Description

Illicit, sanctioned, or stolen cryptocurrency has been making headlines, with Bitfinex-related charges against Heather Morgan and her husband, Ilya Lichtenstein, and the anti-vaccine protests in Canada serving as two recent examples.

But with so many Bitcoin proponents describing the flagship cryptocurrency as “resistance money”—a form of currency that can’t be censored by governments or law enforcement—it begs the question: How is ill-gotten Bitcoin actually recovered?

The short answer is, there really isn’t a short answer. There’s no simple strategy or process governments can use, and most evidence so far suggests that governments are reacting on a case-by-case basis.

“Because cryptocurrency has become such an integral component of cybercrime today, especially when it comes to ransomware, the U.S. government has recently focused on finding ways it can recover elicit funds in digital wallets. A great example of this is the FBI’s announcement of the launch of the Virtual Asset Exploration Unit last week,” former FBI analyst and current Director of Threat Intelligence at Abnormal Security, Crane Hassold.

Crane added that the precise methods of how the U.S. government recovers such funds haven’t been revealed, and that he “wouldn’t expect the U.S. government to make those tactics public.”

So what can we determine from recent examples in the public domain?

Bitfinex & The DOJ

The most recent—and arguably most high-profile—example of a government seizing Bitcoin happened last month in the United States.

On February 8, Morgan and Lichtenstein were arrested and charged with conspiring to launder Bitcoin tied to the 2016 Bitfinex hack. The Department of Justice seized $3.6 billion worth of the flagship cryptocurrency.

The seizure, according to Deputy Attorney General Lisa O. Monaco, represented the DOJ's "largest financial seizure ever," which showed that "cryptocurrency is not a safe haven for criminals."

According to the criminal complaint that accompanied both parties' arrests, the funds seized by law enforcement remain "secured in the U.S. Government's possession."

So how did the DOJ do it?

In this instance, the seizure was relatively straightforward. Lichtenstein stored his crypto keys—essentially access codes to cryptocurrency wallets—on the cloud. Once search warrants were obtained, law enforcement officers were able to access a file that contained 2,000 virtual currency addresses and the corresponding private keys.

"I think the entire case was cracked primarily because of poor infosec on behalf of the alleged criminals," told computer programmer and crypto critic Stephen Diehl recently.

$435 Million in UK

U.K. police have seized millions in cryptocurrency—just last week the Greater Manchester Police returned over $5 million to victims of an international scam, after recovering a USB stick that contained almost $10 million in stolen Ethereum.

An additional $12.7 million was found in what was described as a "cryptograph safety deposit box."

Per numerous freedom of information requests, British police have seized a total of $435 million in illicit Bitcoin as of January 2022.

While that may sound high, the U.K. and U.S. have different rules when it comes to such seizures. According to the U.K.'s Proceeds of Crime Act, cryptocurrency is classified as property, not cash, which means law enforcement must wait until a suspect is convicted before recovering crypto. If it were considered cash, it could be seized simply on suspicion of it being linked to criminal activity.

On other occasions, governments simply can't access cryptocurrency they're pursuing—for example, if those funds exist in non-custodial crypto wallets where no third party can be targeted—and in such cases simply freeze the funds instead.

Canada's Convoy

On February 15, the Canadian government invoked the Emergencies Act with the intention of restricting the flow of funds to truck drivers—collectively dubbed the "Freedom Convoy"—from protesting the nation's COVID-19 policy.

This allowed the government to freeze bank accounts without a court order. The government also issued a Mareva injunction, which came on February 17 as part of a wider lawsuit against the protestors.

This, according to Paul Champ, a lawyer for the residents of Ottawa (the plaintiffs), is the "first successful Mareva order in Canada targeting Bitcoin and cryptocurrency exchanges."

As part of the order, convoy protestors are restrained from selling, removing, dissipating, alienating, or transferring any assets, including crypto, that have been raised directly to support the protests. An additional 150 crypto wallets have been targeted by the injunction.

Those hit by the injunction now have to provide a “sworn statement” that describes the nature, location, and value of their holdings—or risk being found to be in contempt of court.

Of course, these developments should be seen in the broader context of hosted vs. unhosted wallets, or custodial vs. non-custodial wallets.

The CEOs of Coinbase and Kraken each have commented on the convoy protests, arguing for the importance of unhosted, or non-custodial, wallets.

Not only has this raised the ire of Canadian regulators, it’s highlighted an important nuance in any discussion about how governments can seize cryptocurrency.

“The problem with an unhosted wallet is, what is your pain point?” Amanda Wick, former chief of legal affairs at Chainalysis, told The Associated Press. “The only thing we have is civil contempt or criminal conviction. If someone is willing to sit in jail and the money is theirs on the other side because no one can access it, that’s a problem.”

Category

1. News
2. Public Sector
3. Stabilized Digital Finance

Date Created
July 2021