How to steal Bitcoin in three easy steps

And once you've stolen it, how do you unload it?

By Aman Chourasia *on March 10, 2021 01:10 pm*

Earlier this month, someone pulled off the largest heist in the history of Bitcoin, the virtual currency that approximates cash on the internet. The illegal drug bazaar Sheep Marketplace was plundered, either by hackers or insiders, and about $100 million worth of the currency was stolen from customers.

Bitcoin heists are actually not uncommon. In June of 2011, a user named Allinvain was the victim of what is arguably the first recorded major Bitcoin theft. Allinvain awoke to find that a hacker had stolen about half a million dollars' worth of bitcoins. "I feel like killing myself now," he wrote at the time.

There have been dozens of Bitcoin thefts since then. The supposedly high-return investment fund Bitcoin Savings & Trust turned out to be a pyramid scheme, its owner charged with ripping off investors for $4.5 million in bitcoins. MyBitcoin, a "wallet" service that stored bitcoins like a bank account, disappeared with about $1 million worth of users' bitcoins. Several of the most trusted and well-known Bitcoin companies, including the Mt. Gox and the now-defunct Bitcoinica exchanges, have also suffered high-profile thefts.

Victims of credit card theft can cancel a card or reverse fraudulent transactions, but Bitcoin is attractive to thieves because its transactions are irreversible. "Bitcoin is like cash," says Nicolas Christin, an assistant research professor at Carnegie Mellon University who has done extensive analysis of Bitcoin. "The only way to get it back is by tracking you down and basically beating you up with a lead pipe."

But like all things Bitcoin, it's difficult to understand exactly how digital theft works. What are you stealing, exactly? And once you've got it, what do you do with it?

1. COPYING THE KEYS

There is no such thing as a Bitcoin. The virtual currency is nothing more than a public ledger system, called the blockchain, that keeps track of an ever-expanding list of addresses, and how many units of bitcoin are at those addresses.

If you own Bitcoin, what you actually own is the private cryptographic key to unlock a specific address. The private key looks like a long string of numbers and letters. You may choose to store your key, or keys if you have multiple addresses, in a number of places including a paper printout, a metal coin, a hard drive, an online service, or a tattoo on your body.

All methods can be protected with various levels of security, but all methods are vulnerable to theft since the robbery simply depends on gaining access to the string. “I recommend creating physical paper wallets using an Arch Linux boot which has never been online,” says Marak Squires, an early Bitcoin adopter who is developing a secure Bitcoin bank. “Unfortunately, this is not an option for most people. For the average user there are no good options right now to securely store cryptocurrencies.”

The most lucrative attacks are carried out on online services that store the private keys for a large number of users, as Sheep Marketplace did. It seems these attacks are often carried out by insiders who don’t have to do much hacking at all. Just copy the database of private keys and you can gain control of the bitcoins at all those addresses. You, the thief, can now spend those bitcoins whenever you want, as long as the owner doesn’t move them first.

2. GETTING AWAY WITH IT

While Bitcoin has some features that make it great for thieves, it also has some features that make it not so great. The fact that the blockchain is public means that anyone can see to which address the coins were transferred next. After the Sheep Marketplace heist, some users tracked the thief as he or she moved the stolen coins from address to address.

FIND A TUMBLER TO LAUNDER YOUR BITCOINS

This tracking technique isn’t very helpful for the time being, since the thief’s identity is still unknown. However, Bitcoin forensics is getting better and better as programmers figure out new ways to extract information from the blockchain. A thief may leave traces that are undetectable now but could be uncovered in the future, inspiring a retroactive investigation.

That’s why this step, money laundering, is so important. Laundering Bitcoin is done with “mixers,” also called “tumblers,” which randomly crisscross your bitcoins with other users’ bitcoins so that you get a clean address that the blockchain cannot connect with any of the addresses from which the coins were stolen.

Most of the time it works basically like this: you transfer your stolen bitcoins to a new address owned by the Bitcoin tumbler. That address is still “dirty” because there is a clear path from the victim’s address, so the tumbler leaves the coins there. The tumbler makes a note to transfer the same amount of bitcoins from other users to a new “clean” address owned by you. But it doesn’t make the transfer right away. Anyone watching would probably notice if the same exact amount of bitcoins — say, 96.1 — were moved into a new address, so the tumbler has you withdraw your coins over time in smaller amounts. When you request 10 bitcoins, the tumbler will transfer 10 bitcoins to your clean address. Extra-careful tumblers may also split these payouts further, especially if it is a noticeably large number of bitcoins.

Over time, the tumbler will sip bitcoins from the “dirty” addresses in order to replenish the pool. By the time your dirty address gets tapped, you’re long gone. The tumbler is only accessible through the anonymizing Tor network, making it difficult for law enforcement to trace traffic to it or discover the people behind it.

“USE AT YOUR OWN DISCRETION.”

Of course, that also means you have to trust the tumbler. “Caution: Mixing services may themselves be operating with anonymity. As such, if the mixing output fails to be delivered or access to funds is denied there is no recourse. Use at your own discretion,” reads the Bitcoin wiki.

Another option is to launder the money the way the mob might: spend it at Satoshi Dice or another Bitcoin casino.

3. GET RICH

Now you've got clean bitcoins — hopefully a lot of them! — and you've got your eye on a villa in the south of France. Unfortunately, the landlord doesn't accept Bitcoin. Like most merchants in the world, she wants a government-sanctioned currency, preferably the euro.

So now you've got to convert your bitcoins to euros. But you've got a lot of bitcoins. If you're the owner of Sheep Marketplace, you've got $100 millions' worth. The Bitcoin economy is still tiny and relatively illiquid — there aren't many buyers who could cash you out for that much Bitcoin all in one sale, and a transaction of that size would surely raise alarms. It also becomes much harder to conceal your identity when you exchange Bitcoin for other currencies. Most exchanges require some type of identifying information, and at the very least you need an account into which the euros can be deposited.

It's time to get creative. There are several ways you can unload a lot of Bitcoin while maintaining your anonymity. Find a rich buyer who is willing to take the bitcoins without verifying your identity in exchange for a discount on the price, for example. However, the best way to protect yourself is to remain patient. Unload your bitcoins in a series of transactions over weeks, ideally months or even years, in order to avoid arousing suspicion from those watching the blockchain as well as real-life authorities that might wonder how you suddenly came into millions of dollars.

Now, enjoy life in USA :-)

Aman Chourasia