The New York Times | https://nyti.ms/3sgR63x

Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes

Bitcoin owners are getting rich because the cryptocurrency has soared. But what happens when you can't tap that wealth because you forgot the password to your digital wallet?

By Nathaniel Popper

Jan. 12, 2021

Stefan Thomas, a German-born programmer living in San Francisco, has two guesses left to figure out a password that is worth, as of this week, about $220 million.

The password will let him unlock a small hard drive, known as an IronKey, which contains the private keys to a digital wallet that holds 7,002 Bitcoin. While the price of Bitcoin dropped sharply on Monday, it is still up more than 50 percent from just a month ago, when it passed its previous all-time high of around $20,000.

The problem is that Mr. Thomas years ago lost the paper where he wrote down the password for his IronKey, which gives users 10 guesses before it seizes up and encrypts its contents forever. He has since tried eight of his most commonly used password formulations — to no avail.

"I would just lay in bed and think about it," Mr. Thomas said. "Then I would go to the computer with some new strategy, and it wouldn't work, and I would be desperate again."

Bitcoin, which has been on an extraordinary and volatile eight-month run, has made a lot of its holders very rich in a short time, even as the coronavirus pandemic has ravaged the world economy.

But the cryptocurrency's unusual nature has also meant that many people are locked out of their Bitcoin fortunes as a result of lost or forgotten keys. They have been forced to watch, helpless, as the price has risen and fallen sharply, unable to cash in on their digital wealth.

Of the existing 18.5 million Bitcoin, around 20 percent — currently worth around $140 billion — appear to be in lost or otherwise stranded wallets, according to the cryptocurrency data firm Chainalysis. Wallet Recovery Services, a business that helps find lost digital keys, said it had gotten 70 requests a day from people who wanted help recovering their riches, three times the number of a month ago.

Bitcoin owners who are locked out of their wallets speak of endless days and nights of frustration as they have tried to get access to their fortunes. Many have owned the coins since Bitcoin's early days a decade ago, when no one had confidence that the tokens would be worth anything.

"Through the years I would say I have spent hundreds of hours trying to get back into these wallets," said Brad Yasar, an entrepreneur in Los Angeles who has a few desktop computers that contain thousands of Bitcoin he created, or mined, during the early days of the technology. While those Bitcoin are now worth hundreds of millions of dollars, he lost his passwords many years ago and has put the hard drives containing them in vacuum-sealed bags, out of sight.

"I don't want to be reminded every day that what I have now is a fraction of what I could have that I lost," he said.

The dilemma is a stark reminder of Bitcoin's unusual technological underpinnings, which set it apart from normal money and give it some of its most vaunted — and riskiest — qualities. With traditional bank accounts and online wallets, banks like Wells Fargo and other financial companies like PayPal can provide people the passwords to their accounts or reset lost passwords.

"I would just lay in bed and think about it," Mr. Thomas said. Nicholas Albrecht for The New York Times

But Bitcoin has no company to provide or store passwords. The virtual currency's creator, a shadowy figure known as Satoshi Nakamoto, has said Bitcoin's central idea was to allow anyone in the world to open a digital bank account and hold the money in a way that no government could prevent or regulate.

This is made possible by the structure of Bitcoin, which is governed by a network of computers that agreed to follow software containing all the rules for the cryptocurrency. The software includes a complex algorithm that makes it possible to create an address, and associated private key, which is known only by the person who created the wallet.

The software also allows the Bitcoin network to confirm the accuracy of the password to allow transactions, without seeing or knowing the password itself. In short, the system makes it possible for anyone to create a Bitcoin wallet without having to register with a financial institution or go through any sort of identity check.

That has made Bitcoin popular with criminals, who can use the money without revealing their identity. It has also attracted people in countries like China and Venezuela, where authoritarian governments are known for raiding or shutting down traditional bank accounts.

But the structure of this system did not account for just how bad people can be at remembering and securing their passwords.

"Even sophisticated investors have been completely incapable of doing any kind of management of private keys," said Diogo Monica, a co-founder of a start-up called Anchorage, which helps companies handle cryptocurrency security. Mr. Monica started the company in 2017 after helping a hedge fund regain access to one of its Bitcoin wallets.

Mr. Thomas, the programmer, said he was drawn to Bitcoin partly because it was outside the control of a country or company. In 2011, when he was living in Switzerland, he was given the 7,002 Bitcoin by an early Bitcoin fanatic as a reward for making an animated video, "What is Bitcoin?," which introduced many people to the technology.

That year, he lost the digital keys to the wallet holding the Bitcoin. Since then, as Bitcoin's value has soared and fallen and he could not get his hands on the money, Mr. Thomas has soured on the idea that people should be their own bank and hold their own money.

"This whole idea of being your own bank — let me put it this way: Do you make your own shoes?" he said. "The reason we have banks is that we don't want to deal with all those things that banks do."

Other Bitcoin believers have also realized the difficulties of being their own bank. Some have outsourced the work of holding Bitcoin to start-ups and exchanges that secure the private keys to people's stashes of the virtual currency.

Yet some of these services have had just as much trouble securing their keys. Many of the largest Bitcoin exchanges over the years — including the onetime well-known exchange Mt. Gox — have lost private keys or had them stolen.

Gabriel Abed, 34, an entrepreneur from Barbados, lost around 800 Bitcoin — now worth around $25 million — when a colleague reformatted a laptop that contained the private keys to a Bitcoin wallet in 2011.

Mr. Abed said this did not dim his enthusiasm. Before Bitcoin, he said, he and his fellow islanders had not had access to affordable digital financial products like the credit cards and bank accounts that are easily available to Americans. In Barbados, even getting a PayPal account was almost impossible, he said. The open nature of Bitcoin, he said, gave him full access to the digital financial world for the first time.

“The risk of being my own bank comes with the reward of being able to freely access my money and be a citizen of the world — that is worth it,” Mr. Abed said.

For Mr. Abed and Mr. Thomas, any losses from mishandling the private keys have partly been assuaged by the enormous gains they have made on the Bitcoin they managed to hold on to. The 800 Bitcoin Mr. Abed lost in 2011 were a small fraction of the tokens he has since bought and sold, allowing him to recently buy a 100-acre plot of oceanfront land in Barbados for over $25 million.

Mr. Thomas said he also managed to hold on to enough Bitcoin — and remember the passwords — to give him more riches than he knows what to do with. In 2012, he joined a cryptocurrency start-up, Ripple, that aimed to improve on Bitcoin. He was rewarded with Ripple’s own native currency, known as XRP, which rose in value.

(Ripple has recently run into legal troubles, in part because the founders had too much control over the creation and distribution of the XRP coins.)

As for his lost password and inaccessible Bitcoin, Mr. Thomas has put the IronKey in a secure facility — he won’t say where — in case cryptographers come up with new ways of cracking complex passwords. Keeping it far away helps him try not to think about it, he said.

“I got to a point where I said to myself, ‘Let it be in the past, just for your own mental health,’” he said.