



Lost and Never Found

Jeffrey Voas, IEEE Fellow

Nir Kshetri, University of North Carolina—Greensboro

Most of us have experienced the frustration of losing a password, but misplacing the private key to a bitcoin wallet can be disastrous.

Everyone loses things. Whether truly lost or temporarily misplaced, the aggravation is real.

To help, you can buy products to attach to key chains, purses, wallets, and so on to locate them. That's useful for physical items, but what about things that are less tangible? In this short message, we'll focus on passwords—something that, when lost, can drive a person to near madness.

People have, on average, 70–80 passwords.¹ When required to remember so many, they may opt to use weaker passwords or reuse them. This practice can lead to data breaches; according to the 2019 Data Breach Investigations Report, 80% of hacking-related breaches involved compromised and weak credentials.²

It's safe to assume that most of us have lost passwords. However, Bitcoin offers a unique perspective—the situation of being locked out from your money permanently.

Private keys are the passwords needed to unlock bitcoin wallets. If a wallet's private key is lost, the wallet's owner is locked out. Private key loss is not uncommon.

According to the U.S. blockchain research firm Chainalysis, about 20% of the existing 18.5 million bitcoins, which were worth around US\$140 billion then, were lost or stuck in accounts that could not be moved.³

Bitcoin owners provide interesting headlines when locked out. As reported in *The New York Times*, a programmer had a digital wallet holding 7,002 bitcoins, which was reported to be worth about US\$220 million in January 2021. The programmer has made eight failed attempts to access the cryptocurrency—only 10 consecutive attempts are allowed. If all attempts fail, there are no more.⁴

In 2013, a person in Wales discarded a hard drive that contained his digital wallet's private key, mistakenly believing that he had backed up all important files.⁵ The wallet contained 7,500 bitcoins, equivalent to approximately US\$304 million. He had disassembled the laptop into parts in 2010



and discarded the part with the keys.⁶ Since 2014, he has tried to get permission from his city to search for the drive in the city landfill. He has offered a donation of 25% to the city if successful; however, the city has not granted permission.⁷

What's the point? Keep your friends close, your enemies closer, and your passwords and private keys closest of all. ■

REFERENCES

1. "New research: Most people have 70-80 passwords." Newswire. <https://www.newswire.com/news/new-research-most-people-have-70-80-passwords-21103705> (accessed Feb. 15, 2021).
2. "2020 data breach investigations report." Verizon. <https://enterprise.verizon.com/resources/reports/dbir/> (accessed Feb. 15, 2021).
3. "Tens of billions worth of Bitcoin have been locked by people who forgot their key," NY Times, Jan. 13, 2021. <https://www.nytimes.com/2021/01/13/business/tens-of-billions-worth-of-bitcoin-have-been-locked-by-people-who-forgot-their-key.html> (accessed Feb. 15, 2021).
4. N. Popper. "Lost passwords lock millionaires out of their Bitcoin fortunes," NY Times, Jan. 14, 2021. <https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html> (accessed Feb. 15, 2021).
5. "A man who says he threw away a hard drive loaded with 7,500 Bitcoin in 2013 is offering his council \$70 million to dig it up from the city dump." Business Insider India. <https://www.businessinsider.com/man-offers-council-70-million-dig-up-bitcoin-hard-drive-2021-1> (accessed Feb. 15, 2021).
6. A. Cuthbertson. "Man accidentally threw Bitcoin worth \$108 million in the trash, says there's 'no point crying about it'." Newsweek. <https://www.newsweek.com/man-accidentally-threw-bitcoin-worth-108m-trash-says-theres-no-point-crying-726807> (accessed Feb. 15, 2021).
7. T. Moody. "Newport man offers council £52.5m to search for Bitcoin hard drive." South Wales Argus. <https://www.southwalesargus.co.uk/news/19009245.newport-man-offers-council-52-5m-search-bitcoin-hard-drive/> (accessed Feb. 15, 2021).

JEFFREY VOAS, Gaithersburg, Maryland, USA, is the editor in chief of *Computer*. He is a Fellow of IEEE. Contact him at j.voas@ieee.org.

NIR KSHETRI is the "Computing's Economics" column editor of *Computer* and a professor with the Bryan School of Business and Economics, University of North Carolina at Greensboro, Greensboro, North Carolina, 27412, USA. Contact him at nbkshetr@uncg.edu.

Call for Articles



IEEE Software seeks practical, readable articles that will appeal to experts and nonexperts alike. The magazine aims to deliver reliable information to software developers and managers to help them stay on top of rapid technology change. Submissions must be original and no more than 4,700 words, including 250 words for each table and figure.

DISCLAIMER

The authors are completely responsible for the content in this message. The opinions expressed are their own.

IEEE Software

Digital Object Identifier 10.1109/MC.2021.3087981

Author guidelines:
www.computer.org/software/author
Further details: software@computer.org
www.computer.org/software