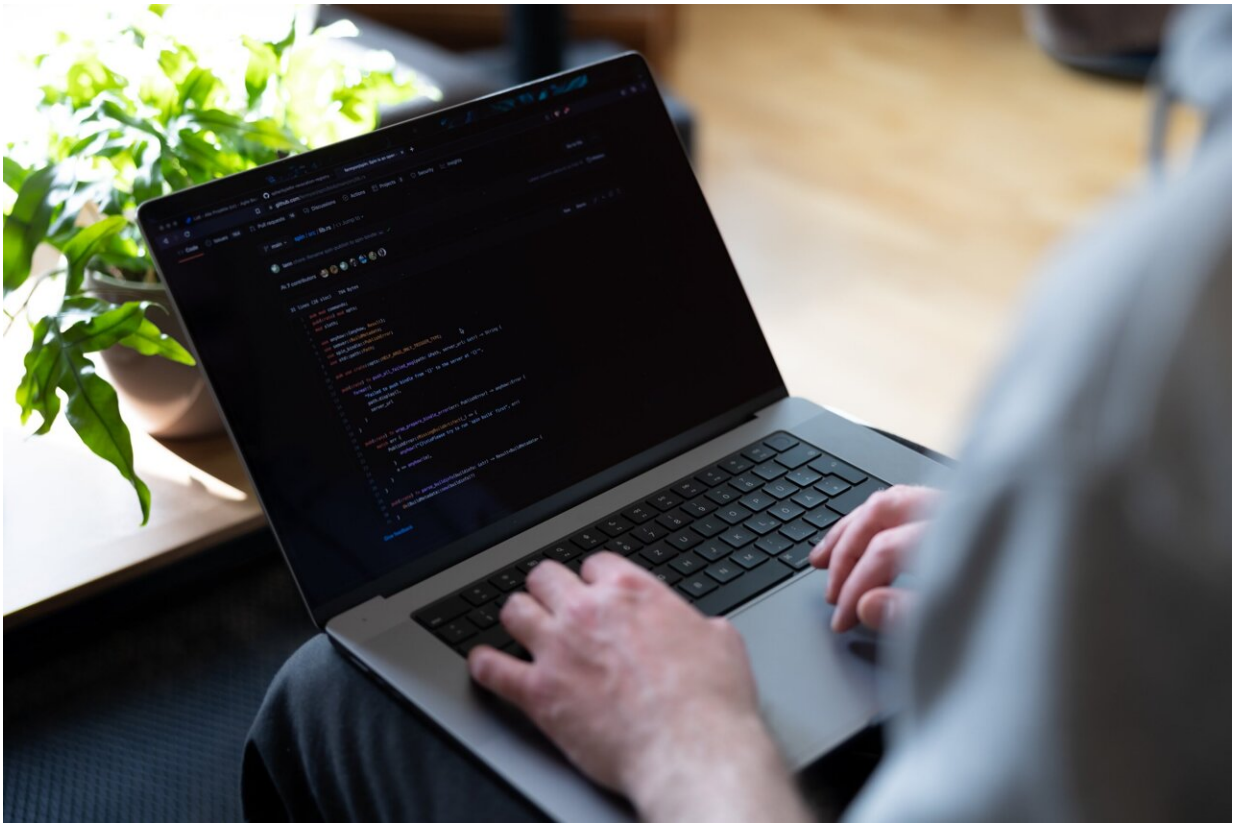
Patching up security gaps in cryptocurrencies often takes a long time, find researchers

May 8 2023



The source code for many applications, also for the crypto currency Bitcoin, is freely available on the internet—you can easily copy it and launch your own cryptocurrency. Credit: Michael Schwettmann

A defining characteristic of cryptocurrencies is that they are organized

in a decentralized system and are not managed by a central bank like conventional currencies. This creates problems when researchers detect security vulnerabilities in the systems of virtual currencies. Sometimes it's unclear who runs a system, whether a system is affected by a certain vulnerability or whether a bug has been patched.

Researchers working with Professor Ghassan Karame, who is a member of the Cluster of Excellence CASA—Cybersecurity in the Age of Large-Scale Adversaries at Ruhr University Bochum, Germany, have examined how long it takes until proven security vulnerabilities in various cryptocurrencies are patched up. The Ruhr University's science magazine Rubin is reporting on their findings, and a pre-print version is available on *arXiv*.

44 severe security vulnerabilities tested

The source code of Bitcoin, probably the best-known cryptocurrency, is openly available on the internet. Anyone can copy it and launch their own cryptocurrency. This is how a number of Bitcoin variations have been created, which are widely known under the umbrella term altcoins.

Security vulnerabilities found in the Bitcoin code usually also affect the altcoin code. Together with his colleagues, Ghassan Karame investigated how different cryptocurrencies have responded to 44 of the most severe network security vulnerabilities that have been documented in recent years.

This included a vulnerability that Karame and his collaborators had exposed in 2015. "Back then, we showed that if we had control over as few as tens of laptops in the system, we could shut down the information flow in the entire Bitcoin system," says Karame.

Many cryptocurrencies take months or even years to patch up vulnerabilities

Using a tool developed specifically for this purpose, the researchers approximated the time it took for various cryptocurrencies to close the security gap described above. "In a nutshell: the results were a shock," says Ghassan Karame.

While Bitcoin fixed the vulnerability in just seven days, it took, for example, Litecoin 114 days, Dogecoin 185 days and Digibyte almost three years. "Three years in which you could have crashed the entire system of the respective cryptocurrency with as few as tens of laptops," says Karame.

Invariably, the same pattern emerged over and over again in the analyses of other security gaps: for many altcoins, the number of days it took to fix the flaws was in the three-digit or even four-digit range.

More information: Sebastien Andreina et al, Estimating Patch Propagation Times across (Blockchain) Forks, *arXiv* (2022). DOI: 10.48550/arxiv.2205.07478

Provided by Ruhr-Universitaet-Bochum