

RUBIN

SCIENCE MAGAZINE

SPECIAL ISSUE

IT SECURITY

Three tough nuts for quantum computers to crack

This is how artificially generated images reveal their true colours

Start-up: Ready for the new generation of mobile communications



Cryptocurrencies

SHARED IRRESPONSIBILITY

Cryptocurrencies are not subject to centralised governance.

The community holds the power – but fails to do all that needs to be done. As a result, the collateral of the currency might be at risk.

Bitcoin, Litecoin, Dogecoin, Digibyte – the list of all currently existing cryptocurrencies is very long. So long, in fact, that it would be hard to decipher their names if they were all squeezed onto one A4 page. Thousands of virtual currencies are out there, and they have long ceased to be a niche product. Millions of people use them. When using cryptocurrencies, IT security is of paramount importance. After all, money is nothing more than data, which, like all data, is potentially vulnerable to cyberattacks.

Professor Ghassan Karame addresses the question of how watertight various cryptocurrencies really are. He heads the Chair for Information Security at the Horst Görtz Institute for IT Security at Ruhr University Bochum and is an advocate for decentralised platforms, like the ones on which cryptocurrencies are based. The idea behind it is simple: power is not bundled in one central entity, for example in a bank. Rather, decisions are always made by some majority of users. “In such systems, it should be very hard for a central body



Bitcoin is one of the best-known cryptocurrencies. The source code is freely available on the internet – and has been extensively copied. This is how so many new virtual currencies have been created.

to impose censorship, and they are robust against faults and misbehaviour because a large community of developers monitors the technology,” as Karame outlines two advantages of decentralised platforms. “The idea is brilliant, and more likely than not, it is the future,” he adds. Just like any other IT technology, however, cryptocurrencies are also vulnerable to security breaches. As early as 2012, Karame and his collaborators detected a critical issue in the usage of the Bitcoin system that allowed people to spend the same Bitcoins multiple times to pay for different transactions. “It was as though you could buy a burger with a five-euro note and then use the same note again to pay for an ice cream,” explains the researcher.

In 2015, Karame and his collaborators documented another critical vulnerability that emerged after Bitcoin adapted its system to a larger number of users. “We showed that if we had control over as few as tens of laptops in the system, we could stop information flow in the entire Bitcoin system,” as Ghasan Karame describes the severity of the vulnerability. Bitcoin ►

i CRYPTOCURRENCIES

When it comes to virtual currencies, the money is not issued resp. controlled by a central bank. Rather, it's the users who take care of all that. Sums of money are allocated to individuals who can store them in a digital wallet. Probably the best-known cryptocurrency is Bitcoin.

In Germany, people own cryptocurrency mainly for the sake of experimentation, speculation or as an asset in their financial investments. Whereas in countries under autocratic leadership, virtual money is often considered an attractive option, because crypto-financial transactions aren't regulated by the state. In countries with extreme inflation, they can also offer financial stability: if the currency of a country collapses, cryptocurrency won't be affected by the crash.

has long since addressed both security gaps. But Bitcoin is not the only currency out there, there are plenty of copies floating around. The source code for Bitcoin is freely available on the internet. Anyone can copy it and launch their own cryptocurrency. This is how Dogecoin was created, for example, which has become the No. 1 cryptocurrency in the gaming industry. “There are so many cryptocurrencies that we don’t even know all of them, and we certainly don’t know who is running them,” points out Ghassan Karame; he is one of the Hub Leaders in the Cluster of Excellence CASA. That’s the trouble with decentralised systems. Since decision-making power is shared, it is complicated for researchers to report security vulnerabilities.

IT security is governed by the ethical imperative of “responsible disclosure”. If a security vulnerability is detected and confirmed, the researchers must always notify the operator of the compromised product first and allow them sufficient time to fix the bug before it is publicly disclosed. This is to ensure that the exposures are patched before attackers can exploit them. But to whom are you supposed to report errors in a decentralised system, when it sometimes isn’t even clear who is running the system? Or if you don’t even know how many and which systems are affected? Who decides in such a structure whether the software has to be updated to close security gaps? And how can you control whether a vulnerability has been patched? There are no answers to these questions yet.

Regarding the security vulnerabilities described above, Karame and his collaborators were in discussion with the various Bitcoin developers. “There, the staff responded diligently and swiftly,” he recalls. But no advance warning ever came for the numerous copies of Bitcoin. Ghassan Karame intends to find out what the real-world impact of these unclear structures really is. He and his team examined various virtual currencies that are slightly modified copies of Bitcoin. They are widely known under the umbrella term “altcoins”. The researchers checked how long it took until security vulnerabilities in various altcoin source codes were closed after they had transpired – including the serious security vulnerability detected by Karame’s team and disclosed in 2015, for example.

“In a nutshell: the results were a shock,” as Ghassan Karame puts it. 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 cryptocurrency system with tens of laptops,” Ghassan Karame points out and illustrates the scale of the problem: “Imagine if it took Visa three years to fix a security flaw in credit card payments.”

The result of the analysis made in Bochum sounds simple, but the path to the numbers was lengthy. Bitcoin’s full source code as well as each modification of the code are freely available on a platform called “GitHub”. This offers multiple opportunities for cloning and importing patches from this public project. For example, anyone who wants to create a Bitcoin



Ghassan Karame heads the Chair for Information Security at Ruhr University Bochum.



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.


copy, i.e. an altcoin, can copy the source code in GitHub into their own project using a simple command.

If a security update for Bitcoin is available and an altcoin developer decides to install it, they typically use the “rebase” command. This means they don’t have to laboriously rewrite their own code, but can transfer the necessary information directly from the Bitcoin code to the own. The researchers identified the problem as follows: while GitHub typically tracks the timestamp of each code modification, the use of the rebase command can result in the loss of this metadata. As a result, it’s no longer straightforward to tell from the source code when a security update was implemented.

Therefore, the team had first of all to develop a tool with which they could approximate the time of a security update for forked source code. The tool is based on an existing archive service that keeps track of all events on public repositories of GitHub, such as modifying the code or perform a rebase operation. This allowed the researchers to match updates in the code with the respective events in the archive, in order to estimate the timestamp of the security patch.

This is how the researchers analysed 44 of the most serious security vulnerabilities documented for Bitcoin and altcoins. Invariably, the same pattern emerged over and over again: for many altcoins, the number of days it took to fix the flaws was in the three-digit or even four-digit range. “We believe that some cryptocurrencies haven’t managed to patch some of the vulnerabilities to this day,” says Karame. He’s certain that the problem is actually much more serious than his initial analysis showed. “I’m almost afraid to dig down any deeper,” he continues. “We’ve seen only the tip of the iceberg so far, I’m sure.” Therefore, the researcher urges caution: “Users need to be more careful when picking a cryptocurrency. They shouldn’t base their decision solely on the prospects of profit. It’s no use at all to make a bunch of money if it can disappear in a puff of smoke the next day due to a security breach.” In theory, people should only trade cryptocurrencies whose operators have a policy of security updates. Currently, however, users have little chance of finding out whether this is the case. It remains to be seen whether this gap will be closed when decentralised platforms become even more popular.

text: jwe, photos: ms



”
THE
RESULTS
WERE
A SHOCK.
“

Ghassan Karame

EDITOR'S DEADLINE

The rabbits in the CASA Universe are startled: the seemingly well-secured access to Rabbit Mark's carrot stash has been hacked and all winter supplies have been stolen. The brave bunny Betty then starts looking for support at the nearby CASA Hub C – a mysterious place that is supposed to hold solutions for digital security. Thus begins the adventure of Betty the bunny, the protagonist of the first science comic from the Cluster of Excellence CASA. Along with Betty, the readers explore the Research Hub and learn about the research priorities and challenges that the scientists in the Research Hub C "Secure Systems" deal with on a daily basis. Find out how to read this and more CASA comics at no cost at:

➔ casa.rub.de/en/outreach/science-comics

Answers
DEEP FAKE-QUIZ
The following faces
are real:
1a, 2a, 3b, 4a, 5b, 6a

??



LEGAL NOTICE

PUBLISHER: Cluster of Excellence CASA at the Horst Görtz Institute for IT Security at Ruhr University Bochum in collaboration with the Corporate Communications Department at Ruhr University Bochum (Hubert Hundt, v.i.S.d.P.)

EDITORIAL ADDRESS: Corporate Communications Department, Editorial Office Rubin, Ruhr-Universität Bochum, 44780 Bochum, Germany, phone: +49 234 32 25228, rubin@rub.de, news.rub.de/rubin

EDITORIAL BOARD: Dr. Julia Weiler (jwe, editor-in-chief); Meike Drießen (md); Lisa Bischoff (lb)

PHOTOGRAPHER: Michael Schwettmann (ms), Dammstr. 6, 44892 Bochum, Tel.: +49 177 3443543, info@michaelschwettmann.de, www.michaelschwettmann.de

COVER: Sashkin – stock.adobe.com

PHOTOGRAPHS FOR TABLE OF CONTENTS: Michael Schwettmann

GRAPHIC DESIGN, ILLUSTRATION, LAYOUT:
Agentur für Markenkommunikation, Ruhr-Universität Bochum,
www.einrichtungen.rub.de/de/agentur-fuer-markenkommunikation

PRINTED BY: LD Medienhaus GmbH & Co. KG, Van-Delden-Str. 6-8, 48683 Ahaus, Germany, Tel.: +49 231 90592000, info@ld-medienhaus.de, www.ld-medienhaus.de

EDITION: 800

DISTRIBUTION: Rubin is published twice a year in German language; the regular issues are available from the Corporate Communications Department at Ruhr-Universität Bochum. The magazine can be subscribed to free of charge at news.rub.de/rubin/abo. The subscription can be cancelled by email to rubin@rub.de. The special issue 2021 is available from the Horst Görtz Institute for IT Security. In case of interest, please contact hgi-presse@rub.de.

ISSN: 0942-6639

Reprinting with reference to source and submission of proof copies