Rainer Böhme untersucht Kryptowährungen wissenschaftlich. Foto: Universität Innsbruck

„Heute einfacher als 1997 eine Webseite“

Bitcoin ist die bekannteste Kryptowährung. Wie sie funktioniert, welche Gefahren von ihr ausgehen und warum es heute einfacher ist, eine Kryptowährung einzurichten als vor 20 Jahren eine Webseite, erklärt Prof. Rainer Böhme im Interview.

Inzwischen gibt es eine Vielzahl an Kryptowährungen, auch Unternehmen bringen zum Teil eigene Währungen auf den Markt. Warum das alles?

Der Informatiker Rainer Böhme ist Professor für IT-Sicherheit und Datenschutz am Institut für Informatik. Er forscht unter anderem zu Kryptowährungen wie Bitcoin und deren Entstehung und Verbreitung. Im Interview erklärt er Bitcoins und deren Nachfolger. Angefangen haben wir aber mit einer grundsätzlicheren Frage: Was ist eigentlich eine Kryptowährung?

Rainer Böhme: Eine Kryptowährung ist ein Zahlungssystem im Internet, das ohne Bank auskommt und stattdessen Kryptografie verwendet. Kryptografie ist grundsätzlich Verschlüsselungstechnik, wird aber bei Kryptowährungen verwendet, um die Integrität der Zahlungen sicherzustellen: Nämlich, dass die Zahlung an den richtigen Empfänger geschickt wird und dass man Geld nicht doppelt ausgeben kann. Die bekannteste Kryptowährung ist Bitcoin.

Klassisch verschlüsselt wird nicht? Das ist ja eine Vorstellung, weshalb Bitcoin vermeintlich unter Kriminellen beliebt ist.

Böhme: Verschlüsselt wird

nicht. Kryptografie kann vieles, eben auch Integritätssicherung. Typischerweise denkt man bei Kryptografie an Verschlüsselung, aber bei Bitcoin wird nichts verschlüsselt. Bitcoin ist auch nicht anonym, die Zahlungen sind gut nachverfolgbar. Bei konventionellen Zahlungssystemen, also Überweisungen zwischen Banken, ist – aus Sicht der Strafverfolgungsbehörden – bekannt, wem die Konten gehören, aber die Transaktionsflüsse sind zuerst unklar. Bei Bitcoin ist es umgekehrt: Wir haben Kontonummern und es ist öffentlich sichtbar, welches Konto an welches andere Zahlungen leistet. Wir wissen aber nicht sofort, wer dahinter steht. Den Konten reale Personen zuzuordnen, ist einfach eine Detektivaufgabe, die wir computerunterstützt lösen können. Bitcoin ist deshalb maximal pseudonym. Es gibt Leute, die sagen, Bitcoin ist Twitter für das Bankkonto.

Was hat es mit der Beliebtheit von Bitcoin für Illegales auf sich, zum Beispiel im Darknet?

Böhme: Ich würde gar nicht sagen, dass Bitcoins im Darknet so beliebt sind. Es gab eine gewisse Naivität der Teilnehmer, die geglaubt hatten, dass sie anonym sind mit Bitcoins, aber die Darknet-Marktplätze wechseln inzwischen auf andere Kryptowährungen. Bitcoin ist beliebt bei Cyber-Kriminalität, etwa bei Ransomware. Das ist Schadsoftware, die Daten in Gefangenschaft nimmt, verschlüsselt, und erst gegen Zahlung von Bitcoins freigibt. Hier sind die Kriminellen auf Bitcoin angewiesen, weil das Zahlungssystem für Opfer zugänglich ist. Deshalb hat Bitcoin da im negativen Sinn eine gewisse Berühmtheit erlangt.

Wie viele Kryptowährungen neben Bitcoin existieren eigentlich, kann man das sagen?

Böhme: Man muss irgendwo einen Schlussstrich ziehen, was man als Kryptowährung ansieht. Aktuell haben wir analysiert, wie viele Unterwährungen auf einem großen Währungssystem, auf Ethereum, entstanden sind. Wir haben um die 40.000 gefunden. Von denen werden allerdings nur rund 2000 ernsthaft benutzt und nur ein klitzekleiner Bruchteil kann an einer Wechselbörse auch gehandelt werden. Aber es gibt mehrere Währungssysteme neben Ethereum, die 40.000 sind also wiederum nur ein Teil.

Eng verbunden mit Bitcoins ist die Blockchain, was ist das?

Böhme: Die Blockchain ist eine Datenstruktur, die gemeinsam fortgeschrieben wird. Im Fall von Bitcoin können Sie damit überprüfen, ob das Guthaben, das Sie bekommen sollen, bereits an jemand anderen vergeben ist. Man kann also die Exklusivität von Guthaben sichern. Das ist etwas, was sonst in Digitaltechnik kaum möglich ist: Digital können Sie ja sonst perfekte Kopien herstellen. Geld darf man aber nicht kopieren können, nur so behält es seinen Wert. Deshalb braucht man eine Datenstruktur, in der Änderungen auffallen würden, so wie die Blockchain von Bitcoin. Diese Art von Strukturen gibt es grundsätzlich schon seit den 1980er-Jahren.

Welche verbreiteten Alternativen zu Bitcoin gibt es heute?

Böhme: Da gibt es drei wichtige Entwicklungen: Das eine sind so genannte Forks, Varianten von Bitcoin. Immer dann, wenn sich die Bitcoin-Gemeinschaft nicht einigen konnte, wie bestimmte Regeln zu funktionieren haben, und sich dann jemand abgespalten hat, entstand ein Fork. Da gibt es eine nennenswerte, Bitcoin Cash, alle anderen kann man vernachlässigen. Die zweite Entwicklung sind Währungen, die versuchen, noch mehr Funktionen bereitzustellen als Bitcoin, zum Beispiel Unterwährungen zu erlauben und flexibler programmierbar zu sein. Da ist Ethereum ein wesentliches Währungssystem, viele weitere Kryptowährungen basieren darauf. Und die dritte Entwicklung sind Währungen, die versuchen, die Nachvollziehbarkeit von Zahlungen zu reduzieren, also den Datenschutz zu verbessern. Da gibt es zwei nennenswerte Vertreter: An erster Stelle Monero, eine Währung, die auch bei Kriminellen verwendet wird. Und Zcash, das akademische Wurzeln hat, kryptographisch innovativer ist, aber nicht so verbreitet ist wie Monero.

Inzwischen gibt es Kryptowährungen sogar von großen Unternehmen. Warum macht ein Unternehmen das?

Böhme: Heute ist es einfacher, eine Unterwährung auf Ethereum einzurichten, als es 1997, in den Anfängen des Internets, war, eine Webseite aufzusetzen. Deshalb haben wir eben auch diese 40.000 Währungen gefunden. Am Schluss ist es dann Marketing. Und eine Motivation, zumindest von Einzelpersonen, eine Kryptowährung zu kreieren, ist wohl auch, reich zu werden. Die allermeisten Währungen sind allerdings nicht zum Bezahlen gemacht. Im Endeffekt bleibt die Möglichkeit übrig, Kapital unter hohem Risiko zu parken.

Womit beschäftigen Sie sich konkret in Ihrer Forschung?

Böhme: Mich interessiert zuerst einmal das Phänomen an sich, das ökonomische Verhalten mit und in diesen Systemen, wie stabil die Systeme sind, wie sie sich entwickeln. Als Sicherheitsforscher interessiere ich mich auch für Cyber-Risiken. Und ich sehe es als meine Aufgabe, diese der Öffentlichkeit zu erklären und Regierungen dazu zu beraten, natürlich auf Basis von wissenschaftlichen Befunden und mit wissenschaftlichen Methoden. Wir forschen deshalb auch viel an Kryptowährungen, messen und erheben Daten dazu. Dazu müssen wir eine eigene Methodik entwickeln, die tief in der Informatik verankert ist. Derzeit widmen wir uns in mehreren Projekten der Strafverfolgung in neueren Kryptowährungssystemen, auch in Kombination mit Darknet-Marktplätzen.

stefan.hohenwarter@uibk.ac.at

Neue Kryptowährungen

Neben Bitcoin sind in den vergangenen Jahren viele weitere Kryptowährungen entstanden, etwa Monero, Zcash oder die Ethereum-Hauptwährung Ether, die unterschiedliche Anwendungen finden. Auch die Praxis interessiert sich dafür: In einem Symposium am 19. Oktober in Wien tauschen sich Expertinnen und Experten zum aktuellen Stand der Forschung aus, Rainer Böhme ist Mit-Organisator der Veranstaltung.

Kryptowährungen gibt es in großer Zahl – aber nur wenige sind erfolgreich. Foto: iStock/jpgfactory