Die Bekämpfung von Kriminalität im Netz ist eines der Forschungsgebiete von Rainer Böhme. Foto: iStock/peterhowell

Lösungen für digitale Konflikte

Kryptografische Währungen wie Bitcoin werden zunehmend für Illegales verwendet. Wie man Kriminalität in diesem Zusammenhang Herr werden kann, erforschen unter anderem Innsbrucker Informatiker.

Rainer Böhme ist Professor am Institut für Informatik der Uni Innsbruck und forscht an Lösungen für digitale Konflikte: angefangen bei Kriminalitätsbekämpfung bis hin zu alltäglichen Problemen.

Euro, Dollar, Pfund, Rubel, Yen: Bekannte Währungen unterschiedlicher Länder. Sie und alle weiter verbreiteten physischen Währungen haben gemein, dass sie von einer zentralen Stelle, meist einer eigens dafür geschaffenen zentralen Notenbank, ausgegeben werden. Diese Zentralbanken steuern auch die Währungspolitik des jeweiligen Staates, vergeben Kredite an Geschäftsbanken und nutzen unterschiedliche Instrumente, um etwa den Wechselkurs zu anderen Währungen und die Inflation im Währungsraum zu beeinflussen. Seit einigen Jahren hat sich parallel ein von Banken weitgehend unabhängiges Währungssystem entwickelt: „Virtuelle kryptografische Währungen werden dezentral geschöpft und gehandelt, keine zentrale Stelle hat Einfluss auf den Wechselkurs oder die Menge einzelner Zahlungseinheiten“, erläutert Prof. Rainer Böhme. Er ist Professor für Security and Privacy (Datensicherheit und Datenschutz) am Institut für Informatik, seine Professur ist eine

Stiftungsprofessur der Archimedes-Stiftung Innsbruck. Mit kryptografischen Währungen – die bekannteste ist Bitcoin – kann inzwischen auch in vielen „echten" Läden bezahlt werden. Mit ihnen beschäftigt sich Rainer Böhme unter anderem in BITCRIME, einem vom deutschen Bundesministerium für Bildung und Forschung und dem österreichischen Ministerium für Verkehr, Innovation und Technologie geförderten Projekt, das er koordiniert: „Durch ihre dezentrale Struktur werden kryptografische Währungen nicht nur für legale Zahlungsvorgänge, sondern vielfach auch von Kriminellen verwendet."

Kriminelle Energie

Virtuelle Währungen wie Bitcoin kennzeichnet im Gegensatz zu herkömmlichen Währungs- und Banksystemen, dass sie mangels einer zentralen Instanz nicht oder nur sehr schwierig gesetzlich reguliert werden können, dass Überweisungen nicht rückgängig gemacht werden können und dass die Systeme an sich zwar offen und transparent sind, Kontoinhaber ihre reale Identität allerdings nicht bekannt geben müssen. „Geldwäsche, der Handel mit illegalen Gütern wie Drogen oder Waffen und Erpressung

«Durch ihre dezentrale Struktur werden kryptografische Währungen nicht nur für legale Zahlungsvorgänge verwendet.» Rainer Böhme

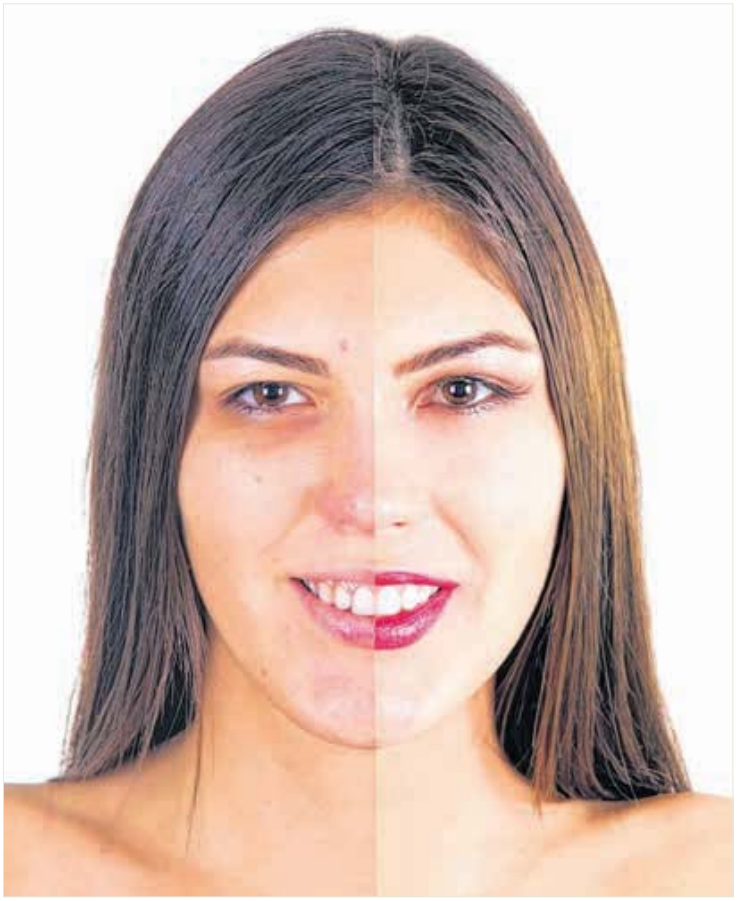
finden zunehmend mittels dieser Währungen statt – ein Umstand, dessen sich auch Behörden bewusst sind. Sie stehen aber teils vor offenen rechtlichen, regulatorischen und technischen Fragen", sagt Rainer Böhme. BITCRIME bringt Forscherinnen und Forscher aus Rechtswissenschaft, Ökonomie und Informatik aus Deutschland und Österreich zusammen, um genau diese Probleme zu lösen. „Eine zentrale Frage ist etwa, wie Prävention aussehen kann: Wie können Währungen wie Bitcoin reguliert werden? Immer wieder wird sogar über ein komplettes Verbot diskutiert, was aber absolut nicht zielführend wäre." Die Regulation ist etwa eine Frage, mit der sich Ökonomen beschäftigen; die an BITCRIME beteiligten Juristen arbeiten unter anderem an der Frage, welche Strafrechtsbestände etwa illegale Verkäufe, die über kryptografische Währungen abgewickelt werden, überhaupt erfassen – zumal die Überweisungen meist über Ländergrenzen hinweg passieren. Die Informatiker erforschen hingegen die Nachvollziehbarkeit von Überweisungen – diese Daten sind zwar ohnehin öffentlich, können aber nicht zwangsläufig realen Personen zugeordnet werden.

„Bitcoin-Konten können zum einen mit eigener Software angelegt werden, zum anderen gibt es Intermediäre, die Bitcoins kaufen und Konten auf ihren Plattformen zur Verfügung stellen", erklärt Rainer Böhme. Eine mögliche Regulation von kryptografischen Währungen setzt bei diesen Intermediären an: Sie könnten beispielsweise verpflichtet werden, regelmäßige Kontrollen bei ihren Nutzern durchzuführen oder eine Identifikation mit einem Ausweisdokument zu verlangen.

Digitale Konflikte lösen

Neben Methoden, Verbrechen im digitalen Raum kontrollierbar zu machen und zu verhindern, forschen Rainer Böhme und sein Team am Institut für Informatik ganz allgemein an Techniken, die aus begründeten Prinzipien in der Lage sind, Konflikte im digitalen Raum zu lösen oder ganz zu vermeiden. „Diese Aufgabe ist bewusst breit gefasst: Damit sind sowohl Konflikte unter Nachbarn gemeint, die sich etwa eine Internetleitung teilen müssen und so mit jeweils langsamerer Geschwindigkeit leben müssen, wenn der Nachbar auch im Internet ist, als auch etwa die Aussagekraft von digitalen Beweismitteln vor Gericht oder bei der Polizei", sagt der Informatiker. Ganz konkret etwa bei Fotos: Wenn zum Beispiel ein digital aufgenommenes Foto als Grundlage für eine Anzeige dient, muss die Polizei sicherstellen können, dass dieses Foto nicht manipuliert ist. „Dieses Problem ist durch die statistische Analyse der jeweiligen Dateien lösbar: So sieht man, ob die Bildaufnahme konsistent und damit nicht manipuliert ist. Spuren der Bildbearbeitung, etwa, wenn ein Bild mehrfach neu komprimiert abgespeichert wird, können mit unseren Forschungsmethoden nachgewiesen werden."

stefan.hohenwarter@uibk.ac.at



Nicht immer sind Bilder ganz offensichtlich bearbeitet – Spuren der Bearbeitung sind aber mit Ergebnissen von Rainer Böhmes Arbeitsgruppe nachweisbar. Fotos: iStock/GoodLifeStudio; Böhme

ZUR PERSON

RAINER BÖHME

Rainer Böhme (geboren 1978 in München) studierte Kommunikationswissenschaft, Wirtschaftswissenschaften und Informatik an der TU Dresden. Nach seinem Studienabschluss arbeitete er mehrere Jahre bei der Europäischen Zentralbank und kehrte später als Doktorand an die TU Dresden zurück. Im Anschluss an seine Promotion 2008 zu einem Thema der Signalverarbeitung und Informationssicherheit war er Gastwissenschaftler in der Arbeitsgruppe für Computernetzwerke am International Computer Science Institute in Berkeley, Kalifornien. Von dort aus wurde er zum Juniorprofessor für Wirtschaftsinformatik, insbesondere IT-Sicherheit, an die Westfälische Wilhelms-Universität Münster berufen, wo er von 2010 bis 2015 forschte und lehrte. Seit dem Frühjahr 2015 ist er Professor an der Universität Innsbruck, methodische Schwerpunkte seiner Arbeit sind Signalverarbeitung, Kodierungstheorie und Spieltheorie sowie empirische Methoden der Sozial- und Verhaltenswissenschaften. Anwendungsschwerpunkte sind digitale Forensik, Zahlungssysteme, Steganographie, Techniken des Selbstdatenschutzes, Benutzungsschnittstellen sowie strategische und operative Aspekte des Sicherheits- und Risikomanagements in verteilten Systemen.