cash

Online lesen

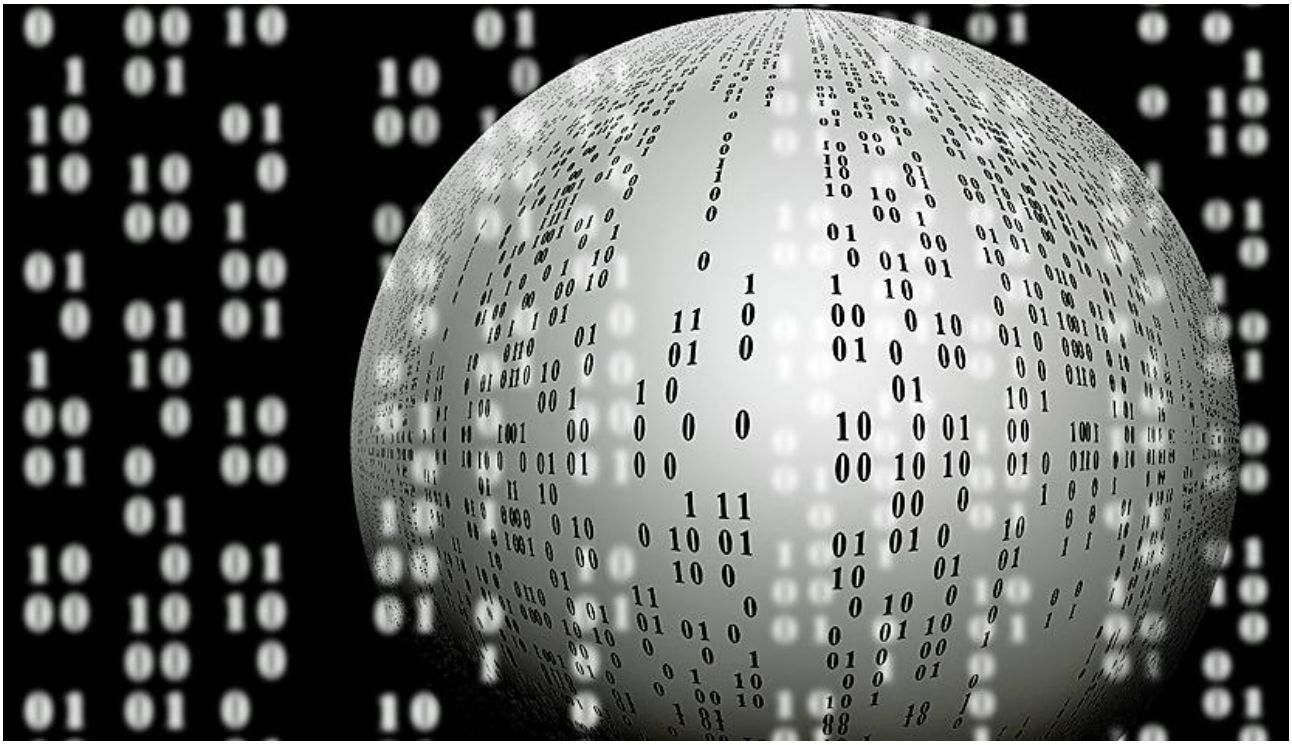
Datum: 08.11.2017

Kryptowährungen und IT-Sicherheit Werden Quantencomputer den Bitcoin zerstören?

Der Schweizer Forscher Marco Tomamichel von der University of Technology Sydney warnt: Quantencomputer können in zehn Jahren beliebig Bitcoins stehlen. Die Grossrechner dürften aber noch viel grössere Probleme bereiten.

08.11.2017 23:23

Von Pascal Züger



Schnelle Quantencomputer können in Zukunft für massive Sicherheitsprobleme sorgen.

Bild: Pixabay

Der weltweite Trend zu digitalen Währungen bricht nicht ab: Mittlerweile existieren gemäss coinmarketcap.com weltweit 1273 Kryptowährungen mit einer Gesamtmarktkapitalisierung von über 200 Milliarden Dollar. Deutlich am beliebtesten ist mit einem Marktanteil von über 60 Prozent weiterhin Bitcoin. Solche rein digitale Währungen können deshalb existieren, weil sie als sicher gelten und ihnen dadurch Vertrauen geschenkt wird.

Doch die Sicherheit könnte bald gefährdet sein, wie ein Forschungspapier des "Centre for Quantum Software and Information" der University of Technology Sydney in Zusammenarbeit mit weiteren Hochschulen beweist. Leistungsfähige Quantencomputer sollen sogenannte digitale Signaturen von Bitcoin-Transaktionen knacken können.

Der Leiter der Studie ist der Schweizer Dr. Marco Tomamichel. Er forscht seit drei Jahren an der University of

Technology Sydney. Gegenüber cash.ch hält er fest: "Nach unserem Modell kann man frühestens in 10 Jahren mit einem Quantencomputer beliebig und unentdeckt Bitcoins stehlen, sofern keine Gegenmassnahmen getroffen werden."

Und so funktioniert der Hack: Wer Bitcoin senden will, muss dem Netzwerk einen Auftrag übermitteln, der elektronisch signiert wird. Damit wird klar, dass der Absender die Bitcoin-Adresse auch tatsächlich besitzt. Ein extrem schneller Rechner kann den ursprünglichen Auftrag aber manipulieren und so das ganze Geld von der Adresse stehlen. Alle Bitcoin im Wallet können so entwendet werden.

Ohne Update das Ende von Bitcoin

Dieser Hack benötigt eine Rechenleistung, zu der herkömmliche Computer nicht fähig sind. Quantencomputer - die bislang noch nicht kommerziell existieren - dürften solche komplexe mathematische Probleme jedoch in absehbarer Zeit lösen können. Google und IBM arbeiten derzeit mit Hochdruck an der Entwicklung von Quantencomputern und haben erste Prototypen entwickelt.

Bedeuten diese "Super-Rechner" das baldige Ende von Bitcoin? "Wenn Bitcoin bis dann kein Update erhält, auf jeden Fall", meint dazu Tomamichel, der in theoretischer Physik an der ETH Zürich doktoriert hat. Jedoch sei es prinzipiell möglich, die elektronische Signatur zu ersetzen, was vor Attacken durch Quantencomputer schütze. "Die Entwicklung solcher Signaturen ist momentan ein aktives Forschungsproblem, es gibt jedoch bereits einige gute Vorschläge."

Schlussendlich ist es ein Wettlauf mit der Zeit: Die Programmierer von Bitcoin und anderen Kryptowährungen müssen ihre Verschlüsselungen sicherer machen, bevor erste massentaugliche und genügend schnelle Quantencomputer auf den Markt kommen. Gemäss der vorliegenden Studie bleibt ihnen dazu noch 10 Jahre Zeit. Für Krypto-Experte Daniel Diemers, Partner bei PwC Strategy&, ist das ausreichend: "Es ist davon auszugehen, dass in diesem Zeitraum die Kryptographie und generell Cybersecurity nicht an Ort und Stelle verharren wird, sondern mit diesen Entwicklungen mitgehen wird."

Auch der Bitcoin- und Blockchain-Community ist das Sicherheitsproblem durch die Quanten-Technologie bestens bekannt. Einige Firmen tüfteln bereits an Lösungen, um sich gegen diese anbahnende Gefahr zu schützen. Vereinzelte Kryptowährungen sind sogar jetzt schon "quantensicher", etwa Hcash und QRL ("quantum resistance ledger").

Ganze IT-Sicherheit in Frage gestellt

Doch die Einführung von Quantencomputern nur als Herausforderung für Kryptowährungen zu bezeichnen, wird dem Ausmass des Problems nicht gerecht: Praktisch jede heute gebräuchliche IT-Verschlüsselung wird dadurch unbrauchbar werden. Etwa solche, die für Online-Banking oder Online-Shopping verwendet werden.

Dazu Niklas Nikolajsen, CEO von Bitcoin Suisse - dem grössten Schweizer Broker für Kryptowährungen: "Theoretisch könnte jemand in alleinigem Besitze eines leistungsfähigen Quantencomputers auf alle Bankkonten zugreifen, geheime Staatsdokumente einsehen und den Zutritt zu militärischen Einrichtungen rund um die Welt kontrollieren. In diesem Worst-Case-Szenario wäre das Wohlergehen von Bitcoin wohl eher zweitrangig."

Immerhin sieht Nikolajsen neben dieser düsteren Vision auch die Möglichkeit, dass der Wechsel zu den leistungsfähigeren Rechnern gelingt. Und dass sich die IT-Infrastruktur inklusive Bitcoin rechtzeitig an die neuen Gegebenheiten anpassen kann. Mit diesem positiveren Szenario der "Evolution anstatt einer Disruption", in dem auch die Kryptowährungen überleben können, rechnet Diemers von PwC.

cash

Datum: 08.11.2017

Thema Blockchain