idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Ruhr-Universität Bochum
Dr. Julia Weiler

28.06.2016
http://idw-online.de/de/news655184

Forschungsergebnisse
Informationstechnik
überregional

Bitcoin: Energieeffiziente Sicherheitsmechanismen für digitale Währungen

IT-Experten der Ruhr-Universität Bochum haben ein neues kryptografisches Rätsel entwickelt, das als Sicherheitsmechanismus für digitale Währungen wie Bitcoin fungieren könnte. Es basiert auf Speicherplatz anstatt auf Rechenleistung und braucht somit wesentlich weniger Energie als das bisher verwendete Prinzip. Das Wissenschaftsmagazin Rubin berichtet.

IT-Experten der Ruhr-Universität Bochum haben ein neues kryptografisches Rätsel entwickelt, das als Sicherheitsmechanismus für digitale Währungen wie Bitcoin fungieren könnte. Es braucht wesentlich weniger Energie als das bisher verwendete Prinzip. Das Wissenschaftsmagazin Rubin berichtet.

Kryptografisches Rätsel als Sicherheitsmechanismus

Eine besondere Herausforderung bei digitalen Währungen ist es zu verhindern, dass Nutzer ihr virtuelles Geld doppelt ausgeben. Daher besitzt das Bitcoin-System einen ausgeklügelten Sicherheitsmechanismus. Spezielle Nutzer, die Miner, überprüfen alle getätigten Transaktionen. Das System gilt als sicher, solange ehrliche Miner mindestens 50 Prozent der Rechenleistung im Netzwerk kontrollieren.

Um Transaktionen für gültig zu erklären, müssen sie derzeit ein kryptografisches Rätsel lösen, das eine immense Rechenpower erfordert. Dieser Mechanismus verhindert, dass ein Nutzer sich auf einem Rechner zig Identitäten zulegt und damit das Bitcoin-Netzwerk unter seine Kontrolle bringt. Denn nur wer extrem viel Rechenleistung besitzt, kann Transaktionen bewilligen.

Extremer Energieverbrauch

„Experten schätzen, dass das Bitcoin-Netzwerk wegen dieser Proof-of-Work-Methode inzwischen eine höhere Rechenleistung hat als Google – und damit ist es nicht gerade umweltschonend“, sagt Prof. Dr. Sebastian Faust vom Bochumer Horst-Görtz-Institut für IT-Sicherheit. Zusammen mit einer Forschergruppe am Institute of Science and Technology Austria in Wien und der Universität in Warschau hat er sich eine energieschonendere Alternative ausgedacht, das Proof-of-Space-Rätsel. Es basiert auf Speicherplatz anstatt auf Rechenleistung.

Neues Rätsel basiert auf Speicherplatz

Der Nutzer muss das Rätsel zunächst einmal rechenintensiv in Gang bringen; dabei wird eine große Menge an Festplattenspeicher belegt. Dann kann er es ohne großen weiteren Rechenaufwand lösen. Das ist jedoch nur möglich, solange er tatsächlich ausreichend Speicher zur Verfügung hat.

Vereinfacht dargestellt funktioniert das System wie folgt: Der Rätsellöser muss eine Reihe von Zahlen nach aufsteigendem Wert sortieren und die sortierte Liste speichern. Wenn er das Rätsel veröffentlichen will, wird er nach der

Zahl an einer bestimmten Position in der Liste gefragt. Hat er die sortierte Liste wie erfordert gespeichert, kann er die Antwort schnell auslesen. „Das ist die Grundidee, aber in Wahrheit ist das Rätsel natürlich komplizierter“, erklärt Sebastian Faust.

Methode bereits im Einsatz

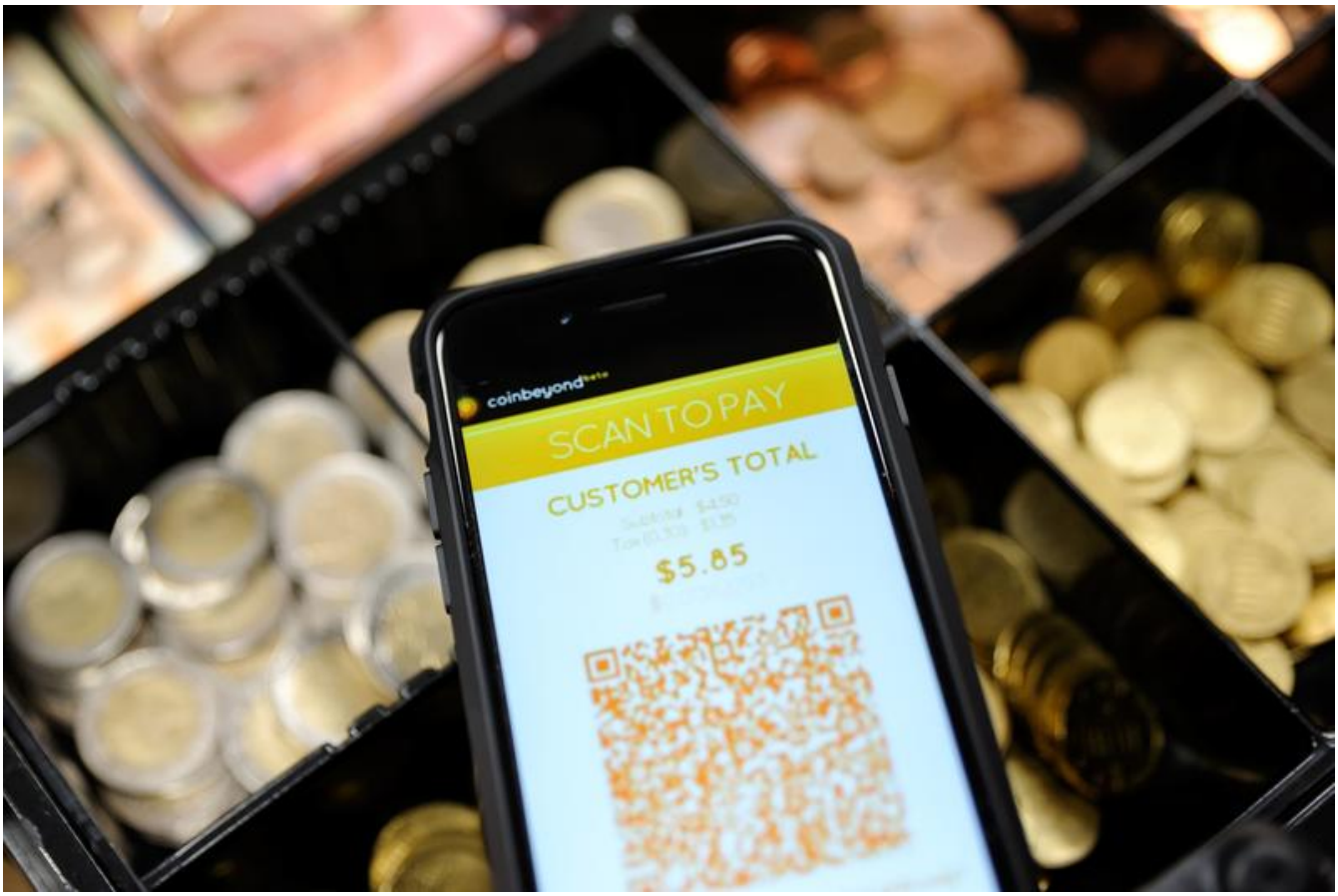
Eine Gruppe am Massachusetts Institute of Technology in Boston und am Institute of Science and Technology Austria hat das Proof-of-Space-Konzept bereits erweitert und darauf basierend eine neue digitale Währung erfunden.

Ausführlicher Artikel in Rubin

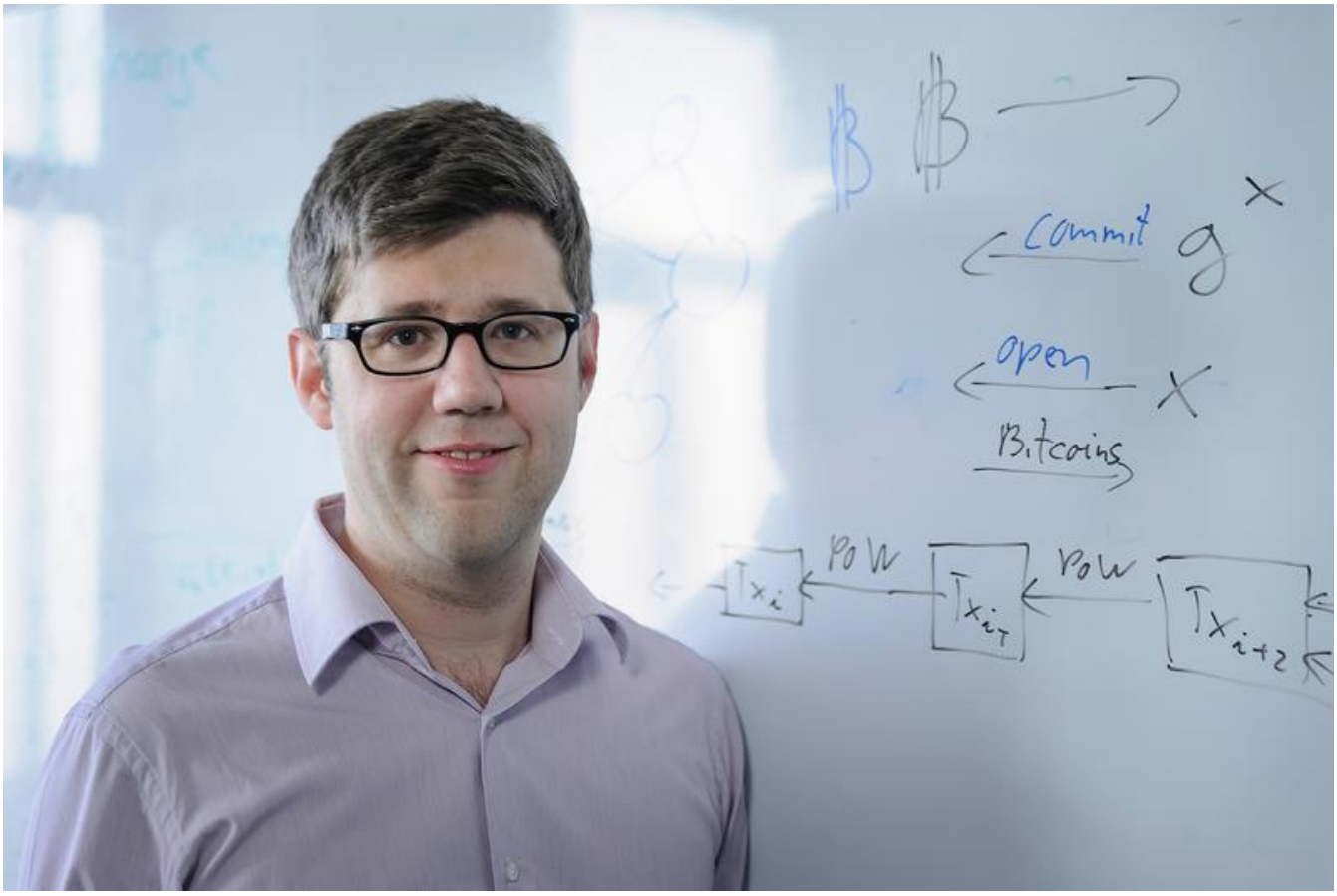
Ein ausführlicher Beitrag zu diesem Thema findet sich in Rubin, dem Wissenschaftsmagazin der Ruhr-Universität, unter http://rubin.rub.de/de/energieeffiziente-sicherheitsmechanismen-fuer-digitale-waehrungen. Texte auf der Webseite und Bilder aus dem Downloadbereich dürfen unter Angabe des Copyrights für redaktionelle Zwecke frei verwendet werden.

Pressekontakt

Prof. Dr. Sebastian Faust, Angewandte Kryptographie, Horst-Görtz-Institut für IT-Sicherheit, Ruhr-Universität Bochum, Tel.: 0234 32 23265, E-Mail: sebastian.faust@rub.de



An einigen Orten können Kunden inzwischen mit der digitalen Währung Bitcoin zahlen.
© RUB, Roberto Schirdewahn



Sebastian Faust
© RUB, Roberto Schirdewahn