idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Technische Universität Wien
Dr. Florian Aigner

26.06.2023
http://idw-online.de/de/news816675

Forschungsergebnisse, Wissenschaftliche Publikationen
Informationstechnik, Mathematik, Wirtschaft
überregional

Eine Brücke zwischen unterschiedlichen Kryptowährungen

Wie kann man eine Kryptowährung in eine andere umwechseln? Bisher musste man dafür großen Krypto-Anbietern vertrauen, oder sich mit ganz einfachen Tauschgeschäften zufriedengeben. Die TU Wien entwickelte nun eine dezentrales Protokoll, das neue Finanz-Instrumente erlaubt.

Bitcoin ist heute die wohl bekannteste Kryptowährung der Welt – aber es gibt noch viele andere, die unterschiedliche Möglichkeiten bieten. Will man eine Kryptowährung in eine andere Kryptowährung umtauschen, verwendet man meist sogenannte „Bridges“ – oft stecken dahinter Firmen, die große Summen unterschiedlicher Kryptowährungen halten und einen Tausch ermöglichen. Dabei kam es aber immer wieder zu Sicherheitsproblemen und spektakulären Kriminalfällen – Kryptowährungen im Wert von Milliarden Euro wurden dabei bereits gestohlen.

An der TU Wien wurde nun ein neuartiges Protokoll entwickelt, dass den Umtausch von einer Kryptowährung in eine andere auf effiziente und sichere Weise ermöglicht – und zwar völlig dezentral, ohne ein großes Krypto-Depot kommerzieller Anbieter nutzen zu müssen. „Glimpse“ heißt das neue Tool, das der Krypto-Welt nun ganz neue Optionen eröffnen soll. Die Arbeit wurde beim „USENIX Security Symposium“ angenommen, einer der prestigeträchtigsten Informatik-Konferenzen der Welt, die im August in Los Angeles stattfindet. Online ist das Paper über die neue Krypto-Technik bereits verfügbar.

Simple Überweisungen und Smart Contracts

Bei Kryptowährungen wird jede Transaktion für alle nachvollziehbar gespeichert – auf der öffentlich einsehbaren Blockchain, die den kompletten Verlauf aller bisherigen Transaktionen enthält. So herrscht immer Einigkeit darüber, von welchem Konto auf welches andere Konto welcher Betrag überwiesen wurde und wer wie viel Kryptowährung besitzt. Diese Transaktionen können auch komplizierter sein als simple Banküberweisungen: „Bei verschiedenen Kryptowährungen kann man etwa Überweisung ins System eingeben, die nur dann gültig werden, wenn bestimmte Bedingungen erfüllt sind“, erklärt Giulia Scaffino, die Erstautorin des Papers.

In einer mathematisch präzise definierten Sprache werden diese Bedingungen festgelegt, als vom Computer lesbarer Vertrag – einem sogenannten „smart contract“. Später wird dann automatisch verifiziert, ob die Bedingungen erfüllt sind oder nicht, und je nachdem wird dann die Überweisung getätigt oder abgebrochen.

Während solche Transaktionen schon bisher innerhalb einer Blockchain möglich waren, sind übergreifende Transaktionen von einer Kryptowährung zur anderen komplizierter und standardmäßig nicht unterstützt. Genau das wird nun aber durch ein neuentwickeltes Protokoll möglich. Die Forschung wurde im Rahmen des Christian-Doppler-Labors „Blockchain Technologies“ an der TU Wien durchgeführt, unter der Leitung von Prof. Matteo Maffei. Neben Giulia Scaffino waren auch Lukas Aumayr und Zeta Avarikioti an der Forschungsarbeit beteiligt.

Bitcoin gegen Ethereum

Angenommen, eine Bitcoin-Besitzerin möchte Bitcoins in Ethereum wechseln. Sie findet einen Ethereum-Besitzer, der zum Tausch bereit ist – wie lässt sich diese Transaktion zuverlässig und effizient bewerkstelligen, wenn Bitcoin und Ethereum technisch nicht miteinander verbunden sind?

Das Grundkonzept ist einfach: Zunächst generiert der Ethereum-Besitzer eine Zufallszahl und übergibt diese der Bitcoin-Besitzerin. Dann wird in der Ethereum-Welt ein Smart Contract aufgesetzt, der garantiert, dass eine bestimmte Ethereum-Menge an die Bitcoinerin überwiesen wird – aber nicht sofort, sondern erst, wenn bestimmte Bedingungen erfüllt werden: Die Bitcoinerin überweist nun nämlich Bitcoins an den Ethereum-Besitzer und fügt in diese Überweisung die eben erhaltene Zufallszahl mit ein, um Sicherheitsattacken anderer zu verhindern. Nun kann die Bitcoin-Besitzerin den aktuellen Block der Bitcoin-Blockchain, in dem nun auch die Zufallszahl gespeichert ist gemeinsam mit einer vorher vereinbarten Zahl weiterer Blocks verwenden, um zu beweisen, dass die Bitcoins tatsächlich transferiert wurden. Diese Daten werden nun auf der Ethereum-Seite verwendet, um den smart contract zu erfüllen – und so wird der vereinbarte Ethereum-Betrag überwiesen.

Effizient, kompatibel und flexibel

„Das genaue Protokoll, das wir dafür entwickelten, sollte mehrere wichtige Kriterien erfüllen“, sagt Zeta Avarikioti. „Es muss effizient sein – der Nachweis, dass die Summe tatsächlich überwiesen wurde, soll mit einer relativ kleinen Datenmenge möglich sein. Wären dafür große Teile einer Blockchain nötig, mit hunderten Gigabyte an Daten, wäre das völlig unpraktikabel. Außerdem soll das Protokoll eine möglichst große Kompatibilität aufweisen – möglichst viele Kryptowährungen sollten unterstützt werden.“

Das neuentwickelte Protokoll ließe sich direkt in bestehende Krypto-Software integrieren – Gespräche mit Bitpanda, einem österreichischen Finanzunternehmen, mit dem das Forschungsteam eng zusammenarbeitet, laufen. „Die Möglichkeiten des neuen Protokolls gehen weit über den Umtausch einer Kryptowährung in eine andere hinaus“, sagt Lukas Aumayr. „Wir zeigen zum Beispiel, dass Glimpse vewendet werden kann, um Krypto-Darlehen innerhalb von Smart Contracts auszudrücken, sowie andere spannende dezentrale Finanzinstrumente wie Asset-Migrationen und Wrapping und Unwrapping von Token.“

wissenschaftliche Ansprechpartner:

Dipl.-Ing. Lukas Aumayr
Institut für Logic and Computation
Technische Universität Wien
+43 1 58801 192611
lukas.aumayr@tuwien.ac.at

Dr. Zeta Avarikioti
Institut für Logic and Computation
Technische Universität Wien
+43 1 58801 192606
zetavar@tuwien.ac.at

Originalpublikation:

G. Scaffino, L. Aumayr, Z. Avarikioti, M. Maffei: Glimpse: On-Demand PoW Light Client with Constant-Size Storage for DeFi https://eprint.iacr.org/2022/1721

Das Forschungsteam: Zeta Avarikioti, Lukas Aumayr, Giulia Scaffino, Matteo Maffei.
TU Wien
TU Wien