Blockchain in Echt

Blockchains versprechen großangelegte offene Internetanwendungen, die vollständig dezentral organisiert sind. Der Preis dafür ist eine zähe Geschwindigkeit bei jeder Transaktion, die von dem System verarbeitet wird. Kryptographie-Forscher um Professor Sebastian Faust erzielen weltweit Aufmerksamkeit mit ihren Ansätzen, Echtzeit-Transaktionen über Blockchains wie beispielsweise Ethereum zu ermöglichen.

Von Boris Hänßler

Mit Kreditkarte geht das Bezahlen schnell: Sobald ein Kunde die Karte in ein Lesegerät steckt oder im Internet seine Daten eingegeben hat, ist die Zahlung in wenigen Sekunden erledigt. Eine zentral organisierte Firma wie Visa kann so in Stoßzeiten beispielsweise mehr als 50.000 Transaktionen pro Sekunde bewältigen. Bei Kryptowährungen wie Bitcoin, die dezentral über eine Blockchain abgewickelt werden, sind derzeit maximal sieben Transaktionen pro Sekunde möglich – ein immenser Unterschied, der die Nutzbarkeit der Technologie stark einschränkt. Zudem kann die Verarbeitung einer einzelnen Transaktion mehrere Minuten in Anspruch nehmen. Dies gilt nicht nur für Bitcoin. Auch komplexere Anwendungsfälle, die über intelligente Verträge – so genannte Smart Contracts – abgewickelt werden, sind kostenintensiv und langsam.

„Die Blockchain ist erst relevant, wenn es zum Streitfall kommt."

Dabei ist die Blockchain für genau solche Fälle gedacht: Jeder Nutzer kann etwas hochladen und darüber vertreiben, und jeder kann selbst Teil der Blockchain werden. Sie ist dezentral, neutral und sozusagen ideale Mischung aus Vermittler und Richter, aber sie ist eben auch langsam. Mit ihr kostengünstig und in Echtzeit zu interagieren – das ist die Vision von Sebastian Faust, Professor für Angewandte Kryptographie, und seines Teams. Die Herausforderung dabei ist, dass der Gewinn an Geschwindigkeit nicht auf Kosten der Sicherheit gehen darf. Die Forschungen sind Teil des von der Deutschen Forschungsgemeinschaft geförderten Sonderforschungsbereichs CROSSING.

Eine Blockchain besteht aus einer Kette von Blöcken, die den Zustand des dezentralen Systems enthält. Im Falle einer Währung wie Bitcoin wären dies zum Beispiel Transaktionsdaten – wer also wie viel an wen bezahlt. Jeder Block enthält zudem einen sogenannten Hash aller darin enthaltenen Daten, eine Art Fingerabdruck. Dies führt bei einer Modifizierung der Daten zu einem geänderten Hashwert. Zudem verweist jeder Block auf den Hash des vorigen Blocks. Dadurch entsteht eine zusammenhängende Kette. Im Durchschnitt wird alle zehn Minuten ein neuer Bitcoin Block von einem der Teilnehmer des Netzwerkes – einem sogenannten Miner – erstellt. Dieser Block wird dann von allen anderen Teilnehmern geprüft und als neuer Block der Kette akzeptiert, wenn alle Transaktionen und Berechnungen korrekt sind. Damit wird der Block Teil der Blockchain, auf der aufbauend alle Miner versuchen, den nächsten Block zu finden. Sollte der Block inkorrekt sein, wird er ignoriert. Eine Transaktion in einem Block wird nur akzeptiert, wenn sie in der Blockchain veröffentlicht und idealerweise von mehreren Blöcken – meist sechs – bestätigt wurde. Dies verhindert, dass ein Angreifer falsche Transaktionen oder Blöcke publizieren kann. Der Nachteil ist, dass ein Nutzer bis zu 60 Minuten auf die Bestätigung der Transaktion warten muss.

Smart Contracts ermöglichen es, neben einfachen Bezahlungen auch komplexere Transaktionen auszuführen. Dabei können ähnlich zu Computerprogrammen komplexe Regeln beschrieben werden, nach denen Zahlungen erfolgen müssen. „Hierbei handelt es sich um Verträge, die über die Blockchain abgewickelt werden", sagt Sebastian Faust. „Smart bedeutet, dass die Verträge logische Bedingungen enthalten. Will zum Beispiel jemand einen Film als Datei online verkaufen, enthält der Smart Contract die Bedingung: Erst wenn die richtige Datei geliefert wird, wird das Geld ausgezahlt." Dies geschieht automatisch, was für beide Seiten sicher ist. Das Geld bleibt dabei in der Blockchain, solange der Kunde die Datei nicht sendet, es kann aber auch nicht vom Käufer anderweitig ausgegeben werden.

Ein weiterer Anwendungsfall ist die Kommunikation zwischen autonomen Fahrzeugen. Es gibt Lastwagen, die auf der Straße autonom fahren können. Aber sie sind teuer, weil sie viel Sensorik benötigen. Ein teilautonomer Lastwagen könnte nicht alleine fahren, aber von dem autonomen mitgesteuert werden. Dafür muss der Fahrer des teilautonomen Lkws einen Vertrag mit dem autonomen eingehen. Der Fahrer kann in dieser Zeit schlafen und muss nicht eigens dafür anhalten. Ein Smart Contract könnte dies alles regeln, wäre da nicht das Problem, dass die Blockchain derzeit zu langsam für rasche Verhandlungen auf der Straße ist.

„Unsere Idee ist, nicht alles in die Blockchain zu verlagern", sagt Faust. „Um zum Beispiel einen Vertrag abzuwickeln, braucht es keine Blockchain – die ist erst relevant, wenn es zum Streitfall kommt." Die Verträge werden also direkt zwischen den Parteien ausgeführt – „offchain". Nur wenn eine Partei die Vertragsbedingungen bricht, wird der Vertrag „onchain" ausgewertet. Hier werden die Bedingungen transparent überprüft und abgerechnet. „Man kann es mit einem Gericht vergleichen", sagt Faust. „Da Prozesse aufwändig und teuer

Informationen

Fachbereich Informatik
Prof. Dr. Sebastian Faust
Telefon: 06151/16 – 25710
E-Mail: sebastian.faust@cs.tu-darmstadt.de
https://bit.ly/2QtCzRS

zeit

sind, gehen die Parteien dort nur hin, wenn sie sich nicht einig sind.“ Der Vorteil dieses Ansatzes ist die Skalierbarkeit. Da im Alltag Streitfälle die Ausnahme sind, können Tausende Verträge in Echtzeit ausgeführt werden. Die Blockchain ist weniger belastet.

Komplexe Computerprogramme können jedoch auch fatale Sicherheitsprobleme enthalten. „Es kommt immer wieder vor, dass die Smart Contracts fehlerhaft implementiert werden und die korrekte Funktionsweise der Contracts nicht mehr garantiert werden kann“, sagt Sebastian Faust. So konnte beispielsweise im Smart Contract von „The DAO“ ein Hacker einen Programmierfehler ausnutzen und Kryptowährung im Wert von 50 Millionen Dollar stehlen. Das Ziel der Forschungen an der TU ist, die Effizienz von Blockchain-Systemen zu verbessern und gleichzeitig das Auftreten solcher Schwachstellen zu minimieren.

Die kryptographischen Protokolle für diese Prozesse zu entwickeln, ist aufwendig. Es muss genau definiert werden, wann die offchain-Algorithmen mit der Blockchain reden und welche möglichst minimalen Informationen ausgetauscht werden. Die Forscher konnten in formalen Modellen belegen, dass ihre Protokolle sicher sind. Sie sind Open Source und zudem unabhängig von der Blockchain-Technologie – man kann sie auch in anderen Systemen einsetzen, um Konflikte automatisiert und transparent zu lösen.

Die Protokolle heißen Perun – nach dem slawischen Gott für Gewitter. Und eingeschlagen haben sie: Die Ergebnisse stießen auf hohe Resonanz sowohl auf den wichtigsten Konferenzen der IT Security als auch bei Firmen wie Bosch oder der Ethereum Foundation, deren Blockchain Smart Contracts unterstützt.

Der Autor ist Technikjournalist.

Abbildung: Katrin Binner

Professor Sebastian Faust, Experte für Kryptografieverfahren.

Daten und Fakten

Die Forschungen um „Sichere und Skalierbare Blockchain Technology (S07)“ sind seit 2018 Teil des bereits seit 2014 an der TU Darmstadt geförderten Sonderforschungsprogramms 1119 der Deutschen Forschungsgemeinschaft mit dem Titel „CROSSING – Kryptografiebasierte Sicherheitslösungen als Grundlage für Vertrauen in heutigen und zukünftigen IT-Systemen“. Verantwortlich für das Projekt „Sichere und Skalierbare Blockchain Technology (S07)“ ist Prof. Dr. Sebastian Faust vom Fachgebiet für Angewandte Kryptographie.

Drei Papers der Forscher um Sebastian Faust wurden auf den führenden Konferenzen zur IT Security, der IEEE S&P und ACM CCS, akzeptiert, darunter:
Stefan Dziembowski, Lisa Eckey und Sebastian Faust: PERUN: Virtual Payment Hubs over Cryptocurrencies. In: 40th IEEE Symposium on Security and Privacy (S&P), 2019
Stefan Dziembowski, Sebastian Faust und Kristina Hostakova: Generalized State Channel Networks. In: 25th ACM Conference on Computer and Communications Security (CCS), 2018