

»Im Moment ist Bitcoin im freien Fall«

Professor Erik Zenner von der Hochschule Offenburg spricht über Blockchain-Technologien / Brauchbare Anwendungen sind noch nicht vorhanden

Die Hochschule Offenburg ist im Bereich Internetsicherheit gut aufgestellt, wie Erik Zenner, Professor für Informatik, im Interview erläutert. Er erklärt, welche Bedeutung Blockchain-Technologien für unsere Gesellschaft haben und wie man sich vor Hackerangriffen schützen kann.

VON SASCHA BÄUERLE

Woher kommt die Blockchain-Technologie?

ERIK ZENNER: Das ist aufgekommen über Bitcoin, eine Online-Währung. Ihre ursprüngliche Idee war, dass man eine Währung und ein Bezahlsystem haben wollte, die von Regierungen nicht mehr kontrolliert werden können. Die Frage ist nun, wie bastelt man sich ein Bezahlsystem, an dem sich ganz viele beteiligen? Der Begriff Bitcoin ist da etwas irreführend, da es sich eigentlich um ein Kontenbuch und keine Coins handelt. Im Prinzip wird über alle Überweisungen buchgeführt. Und die Idee ist, dass jeder eine Kopie von diesem Kontenbuch hat.

Was ist die Problematik dabei?

ZENNER: Wenn ich jetzt Ihnen etwas bezahlen möchte, müssen Sie Dritten gegenüber beweisen können, dass ich Ihnen das bezahlt habe. Das macht man mit einer Anweisung, die digital unterschrieben wird. Das zweite Problem ist, wie kommt diese Unterschrift, die Sie haben, auf diese ganzen Kontenbücher. Es könnte nämlich sein, dass Sie diese an ein paar Leute verschicken und manche haben sie nicht. Es könnte auch jemand unterwegs fälschen. Man muss es hinkriegen, dass sich alle auf eine gemeinsame Version des Kontenbuchs einigen, und da kommt die Blockchain ins Spiel.

Können Sie das erklären?

ZENNER: Wir stellen uns ein gedachtes Blatt in unserem Kontenbuch vor. Dort hat jemand reingeschrieben, dass er 15 Euro von A an B überwiesen hat. Nach einer bestimmten Anzahl an Überweisungen ist das Blatt voll. Im klassischen System, würde jetzt eine zentrale Instanz prüfen, was richtig und falsch ist. Die haben wir bei diesem System aber nicht. Bitcoin verwendet stattdessen eine Art Lotteriansatz. Das heißt, jeder kann versuchen, derjenige zu werden, der das unterschreiben darf. Das nennt man Bitcoin-Mining.

Wie funktioniert Bitcoin-Mining?

ZENNER: Jeder zieht eine Zufallszahl. Am Ende kommt in einem bestimmten Algorithmus eine Gewinnerzahl raus. Wenn ich der erste bin, der die richtige Zufallszahl gefunden hat, habe ich diesen Block gewonnen und darf die letzte Überweisung reinschrei-



Professor Erik Zenner erläutert anhand einer Grafik, wie Blockchain funktioniert. Er unterrichtet an der Fakultät Informatik der Hochschule Offenburg. Seine Interessengebiete sind Kryptologie, digitale Bezahlfverfahren und Entscheidungslehre. Fotos: Ulrich Marx

ben. Außerdem darf ich den Block unterschreiben. Jetzt könnte es trotzdem sein, dass ausgerechnet derjenige gewonnen hat, der vorher eine falsche Überweisung reingeschrieben hat.

Wie kann man das verhindern?

ZENNER: Man sagt, wir berechnen nochmal eine Prüfsumme aus diesem Blatt und wenn wir das nächste Blatt anlegen, kommt oben die Prüfsumme des letzten Blatts rein. Irgendwann gewinnt die Lotterie wahrscheinlich nicht mehr der gleiche, und dann fliegt der Betrug auf.

Warum ist Bitcoin für Verbraucher interessant?

ZENNER: Jede neue Technologie wird erstmal gehypt. Das war bei Blockchain eine Zeitlang der Fall, im Moment ist aber gerade Bitcoin im freien Fall. Ich tue mich noch schwer, richtige Anwendungsfälle für die Blockchain zu finden. Die große Frage ist, wie viele Leute wollen diese dezentrale Technologie? Bei Bitcoin stellt sich heraus, dass die meisten in Wirklichkeit nur Geld verdienen wollen. Als bei Bitcoin der Kurs abgestürzt ist, sind sie wieder ausgestiegen. Meiner Meinung nach sollte man ein Auge darauf haben, wie sich die dezentrale Blockchain entwickelt. Bitcoin hat ein gewaltiges Missbrauchspotenzial. Diese Kryptowährungen werden auch eifrig für dunkle Geschäfte, wie zum Beispiel Drogenhandel und Waffenschmuggel, genutzt. Wenn ich jetzt die Möglichkeit habe, über die Blockchain sogar digitale Verträge abzuschließen, über die der Staat keine Kontrolle hat, bin ich zurück im Hardcore-Kapitalismus.

Welche Bedeutung hat die Blockchain-Technologie für Banken?

ZENNER: Ich glaube, die Banken haben das als große Bedrohung ihres Geschäftsmodells gesehen. Die Blockchain baut sich im Prinzip ein System, das kein Vertrauen mehr erfordert. Und gerade dieser Vertrauensaufbau ist das, wovon Banken leben. Ansonsten haben sie natürlich auch gesehen, dass sie massiv Kosten einsparen können, wenn sie eine eigene, private Blockchain bauen.

Wie sicher ist die Blockchain-Technologie?

ZENNER: Der technische Kern der Technologie ist extrem sicher. Mathematisch ist da kaum etwas zu machen. Das Problem ist die Implementierung. Es ist ein Riesensunterschied, ob ich so ein Modell an die Tafel male oder ob ich real existierende Menschen daran setze. Möglicherweise gibt es beispielsweise Betrüger im System. Das ging ja neulich erst wieder durch die Presse.

Was ist passiert?

ZENNER: Es ging um eine Bitcoin-Wallet, eine Bitcoin-Geldbörse. Das ist im Prinzip eine Firma, die verwaltet Ihr Geld, Ihre Bitcoins oder Ihre digitale Währung für Sie. Die verwaltet das nicht bei Ihnen auf dem Handy, sondern bei sich auf dem Server. Nun ist der Firmenbesitzer, der das Passwort hatte, überraschend gestorben, woran einige zweifeln. Fakt ist aber, er ist weg und das Passwort ist auch weg. Wir reden hier von einem dreistelligen Millionenbetrag, der verschwunden ist. Solche organisatorischen Probleme sind immer wieder das Problem seit Existenz der Blockchain-Technologie gewesen. Es sind Bitcoin-Börsen Pleite gegangen. Es ist immer wieder Wallet-Software angegriffen worden. Und sie haben natürlich die üblichen Probleme mit Computerviren.

Was sind die wichtigsten Anwendungen der Blockchain-Technologie?

ZENNER: Die wichtigste Anwendung ist immer noch das Bezahlfverfahren. Das ist nicht nur Bitcoin, es gibt mittlerweile hunderte Anbieter. Es gibt welche, die sind mehr darauf spezialisiert, dass sie komplett anonym sind. Mit denen wird dann gerne im Darknet gehandelt.

Wo sehen Sie im Bereich der IT-Sicherheit die künftigen Herausforderungen für Unternehmen, die im Internet tätig sind?

ZENNER: Es wird immer noch von allen Windows benutzt, obwohl man weiß, dass Microsoft jede Menge Daten an ihre eigenen Server überträgt. Es sind immer noch alle auf Facebook, es benutzen immer noch alle WhatsApp. Man versucht unter anderem Webseiten abzusichern. Darin ist man sicherlich etwas besser geworden. Wenn ich es mal ganz abstrakt sage, würde ich sagen, das ganz große Problem ist immer noch die Bequemlichkeit der Personen, die da involviert sind. Ein klassisches Beispiel aus meiner eigenen Berufserfahrung: Ich habe früher für eine Bank gearbeitet. Irgendwann hat der IT-Leiter gesagt, dass wir das System umstellen müssen. Jeder sollte dann eine neue Software erhalten. Er sagte dann auch, dass er selbst die alte behalten möchte, damit er sich nicht neu einarbeiten muss. Damit war das System in seiner Gesamtheit natürlich unsicher. Und das sind diese Stellen, an denen es ganz typisch menschelt.

Wie kann man sich vor Cyberangriffen schützen?

ZENNER: Absolut schützen kann man sich gar nicht. Es gibt natürlich ein paar Regeln, die man beachten kann. Dazu gehört eine vernünftige Anti-Viren-Software. Da kann man

eine bezahlte, aber auch kostenlose Software nehmen. Auch gilt die übliche Vorsichtsregel: Wenn Sie irgendwas geschickt kriegen per Mail, dass Sie sich erstmal überlegen, kann das überhaupt stimmen? Ist das wirklich von der Telekom? Muss ich den Link klicken, der da drin angegeben ist? Muss ich den Anhang aufnehmen, der da hinten dranhängt? Denn darüber erfolgen immer noch die meisten Angriffe, die funktionieren. Ein bisschen gesundes Misstrauen ist da sicherlich ganz hilfreich.

Woher erkenne ich einen solchen Angriff?

ZENNER: Zum Glück sind die meisten solcher Angriffe in der Vergangenheit eher simpel gestrickt gewesen. Wenn Sie von irgendeiner Firma eine Mail erhalten, in der viele Rechtschreibfehler sind, ist das meistens verdächtig. Wenn eine Firma vernünftig arbeitet, schickt die Ihnen eigentlich auch keinen Link, auf den Sie draufklicken sollen, um irgendwas zu machen. Eine ganz nette Funktion, die da schon mal hilft: Wenn Sie in Ihrem Mailprogramm sind und Sie gehen mit der Maus über diesen Link, den Sie gerade klicken wollen, dann schauen Sie in der Fußleiste mal, was das eigentlich für eine Adresse ist. Wenn die nicht zur Firma passt, dann stimmt etwas nicht.

Ist es sinnvoll, seine Daten zu verschlüsseln?

ZENNER: Natürlich wäre es sinnvoll, seine Daten, bevor man sie auf ein Netz schickt, zu verschlüsseln. Man sagt häufig, wenn Sie was ins Internet schicken, ist das wie, als ob Sie das irgendwo im Flur an die Pinnwand hängen. Ich muss mir überlegen, ob ich bereit wäre, diese Dokumente, die ich verschickt habe, an so eine Pinnwand zu hängen. Wenn ich damit ein Problem habe, ist es sinnvoll zu verschlüsseln.

Inwiefern sind Blockchain-Technologien Bestandteil im Curriculum der Hochschule?

ZENNER: Im Curriculum spielen sie keine große Rolle. Es gibt ein paar Veranstaltungen, bei denen das ein oder zweimal vorkommt. Bei unserem Studiengang Unternehmens- und IT-Sicherheit wird das natürlich auch thematisiert. Es gibt keine eigene Vorlesung dafür, aber wenn wir über neue Technologien reden oder Projekte durchführen, taucht das Thema auf.

Lernen die Studenten bei Ihnen hacken?

ZENNER: Die Studenten, die Unternehmens- und IT-Sicherheit studieren, definitiv. Wir haben über viele Jahre hinweg ein Hacking-Labor aufgebaut. Es gibt unter den Hackern, weil es eben lange Zeit da keine Vorlesungen und keine Ausbildung gab, ein

Prinzip, das sich CTF nennt. Das steht für Capture the Flag. Das ist ein Wettbewerb, bei dem man versucht, sich gegenseitig die Rechner zu hacken.

Wie läuft der Wettbewerb ab?

ZENNER: Die Hochschule sagt, hier stehen Server, die ihr angreifen könnt. Die haben wir so abgesichert, dass ihr damit sonst keinen Schaden anrichten könnt. Oder wir schicken euch einfach die Daten, damit ihr einen eigenen Server aufbauen könnt. Wir haben da ein paar Bugs reingebaut, die ihr angreifen könntet. Die Teilnehmer müssen dann versuchen, den Fehler zu reparieren, bevor die anderen den Rechner knacken können, und umgekehrt die Rechner der anderen hacken. Beim CTF-Labor, das einmal pro Woche stattfindet, gibt es Hilfestellungen von Tutoren, die Tipps geben, wie man so etwas schaffen kann. Das ist sehr erfolgreich und beliebt. Und wir bieten das auch für Schüler an. Wenn Schüler, die am Ende der weiterbildenden Schule sind, ein Interesse in die Richtung haben, können sie sich mit uns in Verbindung setzen und dürfen auch mitmachen.

Inwiefern kann die Hochschule Unternehmen bei der IT-Sicherheit unterstützen?

ZENNER: Das Fachwissen ist dafür vorhanden. Wir haben Kollegen, die im Penetration-Testing aktiv sind, die also Systeme auf Verwundbarkeit hin prüfen. Wir haben auch Forensiker, die einen angerichteten Schaden untersuchen und herausfinden, wer der Verursacher war. Meine Expertise ist die Kryptografie, also Verschlüsselungs- und Authentifikationstechnik. Allerdings sind wir vom Land angehalten, nicht mit Firmen, die das machen, zu konkurrieren. Wenn wir Unternehmen für wenig Geld unterstützen würden, wäre das unfairer Wettbewerb. Deswegen sind wir dazu verpflichtet, einen ganz normalen Beratervertrag abzuschließen.

Das komplette Interview können Sie auf www.bo.de/J5E lesen.

Ein Video zu diesem Thema finden Sie unter www.bo.de/videos | Videocode: GJX7

Ein Dossier zu diesem Thema mit weiteren Artikeln finden Sie online unter www.bo.de/hochschulseite-campus

Kontakt

Sascha Bäuerle (Mittelbadische Presse) sascha.baeuerle@reiff.de

Christine Parsdorfer (Hochschule) 07 81 / 2054 34 christine.parsdorfer@hs-offenburg.de

INFO

Zur Person

Erik Zenner ist gelernter Bankkaufmann, hat in Mannheim und Edinburgh Wirtschafts-informatik studiert und mit Schwerpunkt Kryptografie promoviert. Er hat in Dänemark als Kryptologe und als Professor für Mathematik gearbeitet und ist seit 2011 Professor für Informatik an der Hochschule Offenburg. Seine Interessengebiete sind Kryptologie, digitale Bezahlfverfahren und Entscheidungslehre.

