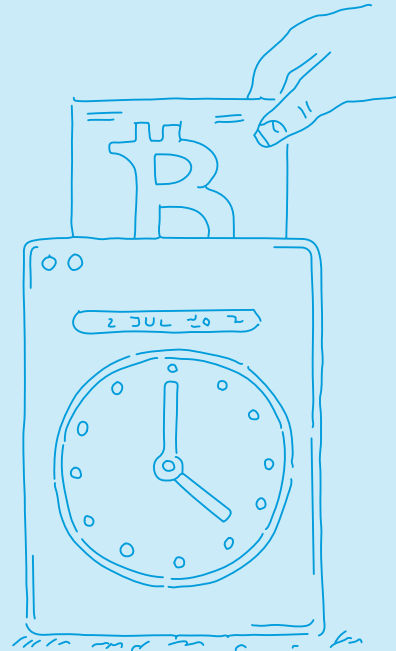


Zeit stempeln mit Bitcoins

Prof. Dr. Bela Gipp schuf mit OriginStamp einen fälschungssicheren Zeitstempel. Er nutzt die Möglichkeiten der Blockchain als System gegen Fälschungen.



„Wie können wir beweisen, dass ein Zeitstempel echt und ungefälscht ist?“



Wir leben in einer Welt voller Zeitstempel: Wenn wir morgens die Tageszeitung aufschlagen, finden wir als eine der ersten Informationen oben rechts das Datum. Was auch immer wir kaufen oder essen, es trägt unter Garantie ein Herstellungs- oder Haltbarkeitsdatum. Jede Datei, die wir auf einem Computer anlegen, wird ganz ohne unser Zutun mit einer Zeitsignatur versehen. Auf wissenschaftlichen Publikationen wird der Zeitpunkt ihrer Veröffentlichung nicht nur vermerkt, sie werden auch über dieses Datum katalogisiert.

Nichts scheint einfacher zu sein als ein solcher Zeitstempel, eine scheinbar banale Sache: Ein Datum wird auf einem Gegenstand, einem Dokument oder einer Datei angebracht, um festzuhalten, wann diese erstellt wurden. Sobald aber juristische Ansprüche ins

Spiel kommen, werden Zeitstempel schnell zu einer prekären Angelegenheit: Wie können wir beweisen, dass ein Zeitstempel echt und ungefälscht ist? Vor allem in der digitalen Welt lässt sich fast alles manipulieren; da ist es nicht weiter schwierig, ein falsches Datum in Umlauf zu bringen. Wenn vor Gericht aber ein zweifelsfreier Nachweis erbracht werden muss, dass zum Beispiel eine wissenschaftliche Idee vor ihrem Imitat existierte, muss ein Zeitstempel wirklich wasserdicht sein. Wer hat etwas erfunden, und vor allem, wann?

Menschen haben sich die eigenwilligsten Techniken einfallen lassen, um Dokumente mit einem glaubwürdigen Zeitstempel zu versehen. Erfinder haben versiegelte Briefumschläge an sich selbst geschickt, um anhand des Poststempels nachzuweisen, wann



Dr. Bela Gipp ist Juniorprofessor für Informationswissenschaft an der Universität Konstanz. Zu seinen Forschungsschwerpunkten gehören zählende Methoden der Gewinnung und Visualisierung von Informationen, Wissensmanagementsysteme sowie die Entwicklung von semantischen Methoden für Plagiatsoftware und Empfehlungssysteme.

der Inhalt bereits zirkulierte. Doch könnte ein versierter Fälscher nicht neue Dokumente in alte, längst abgestempelte Briefumschläge stecken? Andere Menschen haben wiederum ihre Ideen verschlüsselt in Tageszeitungen inseriert, um den Zeitpunkt anhand des Datums der Zeitung festzuhalten. Der Weg zum Patentamt dürfte die bislang wohl sicherste Methode gewesen sein, um eine Idee zu schützen, aber nicht jeder will für jeden Einfall zugleich ein Patent anmelden. Wie lässt sich also ein Zeitstempel erstellen, der absolut fälschungssicher und zugleich im Alltag praktikabel ist?

Notiz auf einem digitalen Geldstück

Der Konstanzer Informatiker Prof. Dr. Bela Gipp griff dieses Problem auf und fand eine überraschende, aber sehr moderne Lösung. Eine Hauptrolle spielt darin ein kleines Geldstück, das es noch nicht einmal physisch gibt – der Bitcoin, die digitale Kryptowährung. Besser gesagt: Das Sicherungssystem hinter den Bitcoins, die sogenannte Blockchain, die eigentlich nie als Zeitstempel gedacht war, sich aber dennoch als genau solcher einsetzen lässt.

Die Idee ist einfach: An die Transaktion eines Bitcoins – oder eines Bruchteils eines Bitcoins – wird ein Dokument angehängt. „Als würde ich eine Notiz in den Brief einer Banküberweisung schreiben“, vergleicht Bela Gipp. Die Blockchain hält den Zeitpunkt der Transaktion – und damit des verknüpften Inhaltes – fest. Dies ist der Zeitstempel, um den es Gipp im Eigentlichen geht. Warum aber ist dieser

„Zeitstempel nach Art der Blockchain“ besonders fälschungssicher?

Der Grund dafür ist das Sicherungssystem der Blockchain. Die Datenbank der Bitcoins ist nicht auf einem zentralen Computer gespeichert, sondern über Rechner in der ganzen Welt verteilt. Um die Datenbank zu manipulieren, müsste die Mehrheit der beteiligten Rechner gleichzeitig beeinflusst werden, was nahezu unmöglich ist. Zudem werden die verschlüsselten Daten der Blockchain aufeinander aufbauend gespeichert, in einer Verkettung von Datenblöcken – daher der Name „Blockchain“ („Datenblock-Kette“). Über diese Datenkette lässt sich jede einzelne Transaktion eines jeden Bitcoins lückenlos zurückverfolgen. Ein Paradies für Zeitstempel.

Bela Gipp bietet seinen Zeitstempel „OriginStamp“ unter www.originstamp.org zur anonymen und kostenlosen Nutzung an. „OriginStamp“ erstellt zu einer eingegebenen Datei oder einem Text mittels einer Hashfunktion eine verschlüsselte Zeichenfolge (der sogenannte Hash) und hinterlegt diese Zeichenfolge in der Blockchain. Der Nutzer erhält daraufhin einen Link, über den die Datei aufgerufen und der Zeitpunkt ihrer Eingabe anhand der Blockchain verifiziert werden kann.

Mehr als „nur“ ein Zeitstempel

„Ich habe OriginStamp ursprünglich als Methode für Wissenschaftlerinnen und Wissenschaftler entwickelt, um bei Vorabdrucken ihrer Publikationen die Urheberschaft und den Zeitpunkt der Veröf-

fentlichung nachzuweisen“, erzählt Bela Gipp. Dasselbe Prinzip kann jedoch noch weitaus mehr leisten als „nur“ einen fälschungssicheren Zeitstempel. Ein weiteres Anwendungsgebiet ist beispielsweise eine sogenannte „Dashcam“. Gemeint ist eine Kamera hinter der Windschutzscheibe eines Autos, das die Fahrt aufzeichnet. Bei einer starken Erschütterung – etwa durch einen Auffahrunfall – sendet die „Dashcam“ automatisch ihre Aufnahmen der letzten Minute an die Blockchain und protokolliert somit den exakten Zeitpunkt. Auf diese Weise könnten Unfälle fälschungssicher dokumentiert werden.

Darüber hinaus arbeitet Bela Gipp mit der Human Bios International AG aus Kreuzlingen (Schweiz) zusammen, um physische und digitale Sicherheitsverfahren gegen Fälschungen miteinander zu kombinieren. Das Unternehmen entwickelt nicht-kopierbare, physische Sicherheitsmerkmale. Ein Beispiel hierfür sind die Muster von zufälligen Rissen, die bei der Trocknung einer Farbschicht entstehen und einen einzigartigen „Fingerabdruck“ bilden. Dieser physische Fingerabdruck kann wiederum mit dem „digitalen Fingerabdruck“ einer Zeichenfolge in der Blockchain verknüpft werden. Dies ermöglicht eine Kontrollkette, um Originale von Fälschungen zu unterscheiden. Die Forschungskooperation wurde im März 2017 geschlossen und umfasst jährliche Forschungsstipendien für bis zu vier Doktorandinnen und Doktoranden | g.r.a.