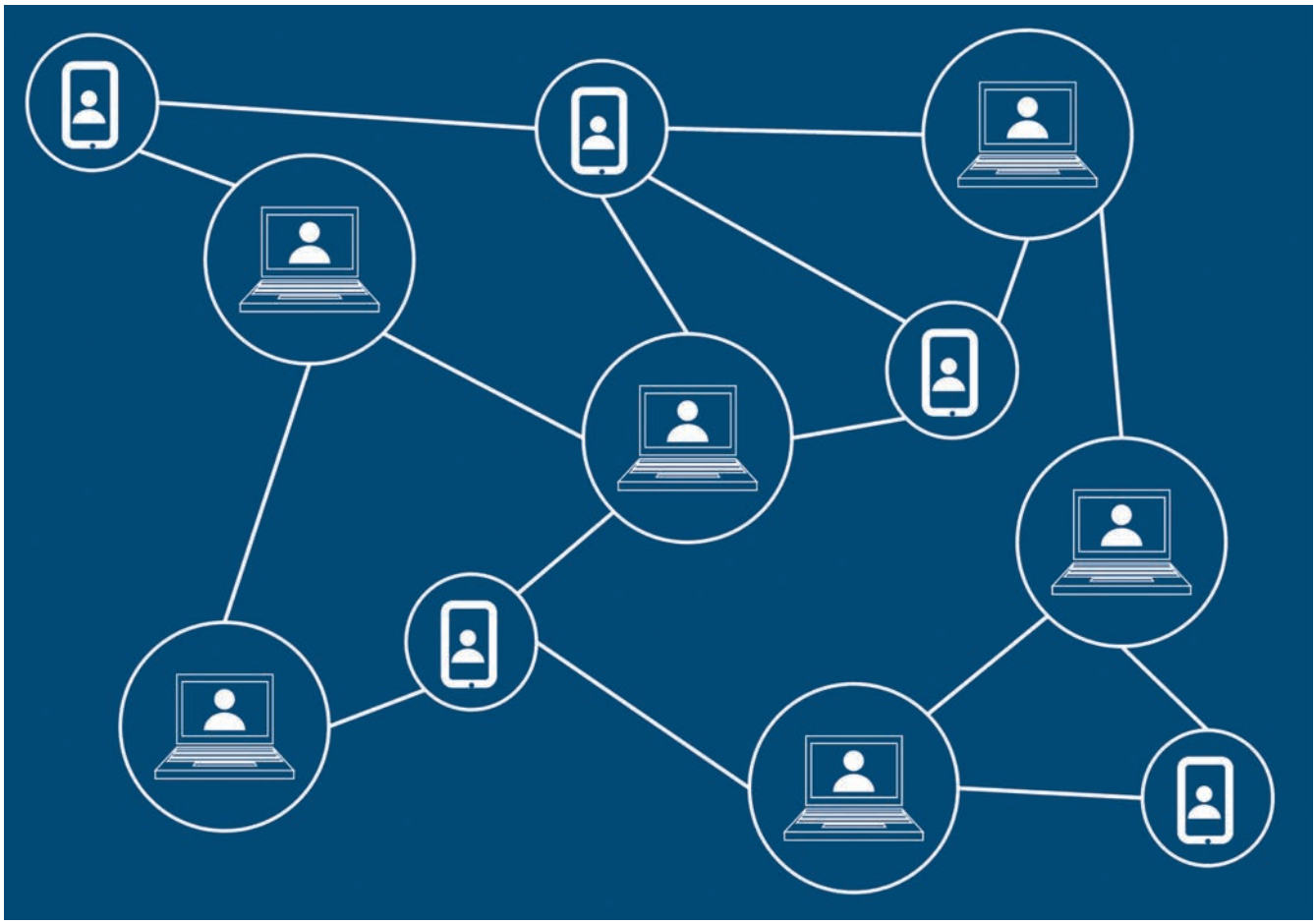

Wann lohnt sich der Einsatz von Blockchains?

Möglichkeiten und Grenzen | Blockchain-Konferenzen und -Symposien erfreuen sich heute einer grossen Popularität, denn viele Fragen sind noch offen, obwohl schon einige Projekte realisiert wurden. Noch ist nicht völlig klar, wie wirtschaftlich Blockchains sein werden und wann man besser auf sie verzichtet.

Bulletin: In den Medien wird Blockchain als Hype präsentiert. Wie steht es aber eigentlich um diese Technologie? Ist die Hype-Welle schon vorbei?
Roger Wattenhofer: Ja, die erste Welle ist wohl vorbei. Viele Anwendungen sind nun schon unterwegs. In der Schweiz gibt es besonders viele Projekte. Die Schweizer Firmen und Start-ups sind bei diesem Thema vorne dabei. Nur die Verwaltung verschläft das Thema leider. Aber es gibt positive Ausnahmen, zum Beispiel Zug oder Genf.

Wenn man Transaktionen beispielsweise aus Ressourcengründen nicht mit einer Blockchain lösen möchte, welche Alternativen hat man?
Blockchains müssen nicht ressourcenintensiv sein. Eine kleine geschlossene Blockchain braucht nicht mehr Ressourcen als eine replizierte Datenbank. Geschlossene Blockchains werden vielleicht bei manchen Anwendungen Datenbanken ersetzen, aber oft ist eine Datenbank immer noch die vernünftigere Lösung.

Es gibt offene Blockchains wie die von Bitcoin und geschlossene. Wie sieht es mit ihrer jeweiligen Skalierbarkeit aus?
Offene Blockchains sind oft auf Hunderten oder Tausenden von Computern repliziert, geschlossene meistens nur auf sehr wenigen. Manche behaupten, dass offene Blockchains deshalb sicherer sind. Ich glaube das nicht. Wenn alle Computer einfach die gleiche Software benutzen, ist ein Softwarefehler so oder so fatal.

Bilder: Pixabay, ETH Zürich

Wie viele Transaktionen können Blockchains verarbeiten?
Die Bitcoin-Blockchain kann nur wenige Transaktionen pro Sekunde verarbeiten. Andere offene Blockchains schaffen mehr, aber irgendwo in der Grössenordnung von zehntausend Transaktionen pro Sekunde ist momentan Schluss. Das ist bei geschlossenen Blockchains aber nicht anders. Das Grundproblem ist, dass jeder Computer jede Transaktion absegnen muss, was natürlich den Transaktions-Durchsatz beschränkt.

Wie kann die Geschwindigkeit erhöht werden?
Dafür gibt es verschiedene dezentrale Lösungsansätze. Meine favorisierte Lösung sind sogenannte Payment oder State Channels, wie die von uns entwickelten Duplex Micropayment Channels. Die Idee ist, dass die eigentlichen Transaktionen gar nicht in die Blockchain gehen, sondern (wie Datenpakete im Internet) nur zwischen den direkt beteiligten Parteien ausgetauscht und digital unterschrieben werden. Die Blockchain ist dann nur noch dafür da, um mögliche Streitigkeiten zwischen den beteiligten Parteien zu beurteilen. Die Blockchain findet den korrekten Zustand der Streitparteien durch die Überprüfung der digitalen Unterschriften, wie eine Art automatisiertes digitales Gericht. Die Blockchain braucht es also nur noch im Ausnahmefall, und dafür reichen Tausende Transaktionen pro Sekunde locker.

Was sind für Sie die wichtigsten Kriterien, um sich für oder gegen den Einsatz von Blockchains zu entscheiden?
Es braucht mindestens zwei Parteien, die miteinander ohne grossen administrativen Aufwand Daten austauschen wollen oder müssen. Das Ganze ist inbesondere dann interessant, wenn die bisherige Lösung viel Ressourcen kostet, weil man sich nicht nur ständig Daten hin- und herschickt, sondern im schlimmsten Fall sogar noch abtippt.

Welche Rolle spielt die Blockchain bei der Digitalisierung?
Die Grundfrage ist nicht, ob man eine Blockchain haben möchte oder nicht. Sondern viel profaner, ob man Daten austauscht und/oder abspeichert, und die Daten und Prozesse nicht lieber digitalisieren sollte. Bei einer Firmengründung zum Beispiel muss man viele Formulare ausfüllen, den Firmennamen schreibt man dabei etwa 30 mal ab. Solche Prozesse sollten digitalisiert werden, weil sie mühsam, langsam und fehleranfällig sind. Im Zentrum eines solchen Prozesses ist oft eine Organisation oder Berufsgruppe, die sich gegen eine Digitalisierung wehren wird. Wenn man einen Prozess digital plant, werden viele spannende Fragen zu beantworten sein: Wer speichert welche Daten? Wie stellt man die Privatsphäre sicher? Wie verwaltet man die Zugriffsrechte und die digitalen Identitäten? Gibt es Smart Contracts? Ob man das Ganze dann als Blockchain umsetzt oder mit einer Datenbank, ist zweitrangig.

Wie schätzen Sie die Blockchain als Technologie ein?
Das Wort Blockchain ist wie ein Schlüssel für die Türe Digitalisierung. Wir alle verwenden im Internet ständig Kryptografie, aber halt eher unbewusst. Der Browser zeigt «https» und das wars. Dank Blockchains nehmen wir die technischen Möglichkeiten bewusster wahr. Zero-Knowledge-Beweise, digitale Identitäten, fehlertolerante verteilte Systeme sind alles spannende Konzepte, die man in vielen Bereichen einsetzen kann.

INTERVIEW: RADOMÍR NOVOTNÝ

Zur Person

Roger Wattenhofer ist ein Schweizer Computerwissenschaftler, der auf dem Gebiet des verteilten Rechnens, der Vernetzung und der Algorithmen tätig ist. Seit 2001 ist er Professor an der ETH Zürich. Er hat zahlreiche Forschungsartikel in der Informatik und ein Buch über Blockchains veröffentlicht.

Im Jahr 2012 erhielt Wattenhofer den Innovationspreis für Distributed Computing, der jährlich im Rahmen der Sirocco-Konferenz verliehen wird. Zusammen mit Christian Decker entdeckte er 2014, dass fast 850 000 der von Mt. Gox verlorenen Bitcoins nicht durch Malleability-Angriffe gestohlen worden sein konnten, wie von Mt. Gox behauptet.

→ ETH Zürich, 8092 Zürich
→ wattenhofer@ethz.ch