Architekt der Krypto-Demokratie

Schon vor über 20 Jahren hat Christian Cachin kryptografische Protokolle entwickelt, wie sie heute in Blockchainsystemen wie Kryptowährungen einen Boom erleben. Er sagt der Blockchain eine grosse Zukunft voraus – mit mehr Regulierung und Nachhaltigkeit.

Von Isabelle Aeschlimann

Energieverschwendung oder Insidergeschäfte sind Probleme, die oft im Zusammenhang mit Kryptowährungen genannt werden. Dabei soll die zugrunde liegende Technologie der Blockchain eigentlich gerade das Gegenteil ermöglichen: Transparenz, Sicherheit und Verfügbarkeit. Das sind nur einige der Vorteile, die im Gespräch mit Christian Cachin zur Sprache kommen. Seit 2019 hat er eine Professur für Kryptologie und Datensicherheit am Institut für Informatik inne. Mit der Blockchain, das wird rasch klar, sind grössere Umwälzungen verbunden: «Es geht darum, dass man so etwas wie Demokratie automatisieren will. Man will einen Prozess, der bisher durch eine zentrale Instanz wie eine Bank oder einen Treuhänder versichert wurde, in einem Netzwerk verteilen. Damit tragen alle zusammen zur Sicherheit und Validierung von gegenseitigem Austausch und Handel bei.»

Zwischenakteure ausschalten

Doch wie geht das genau? Kurz erklärt: Blockchain ist eine Art Datenbank, die auf vielen verteilten Knotenpunkten betrieben wird. So entsteht eine breit einsehbare virtuelle Buchhaltung (Ledger), in der alle Transaktionen vermerkt sind. Diese Transaktionen sind in Blöcken festgehalten und werden mit kryptografischen Algorithmen – basierend auf schwierigen mathematischen Problemen – in eine Kette gereiht, daher auch der Name Blockchain. Bei Kryptowährungen, welche diese Technologie einsetzen, wird man für das Anhängen eines solchen Blockes in die Kette mit Coins belohnt.

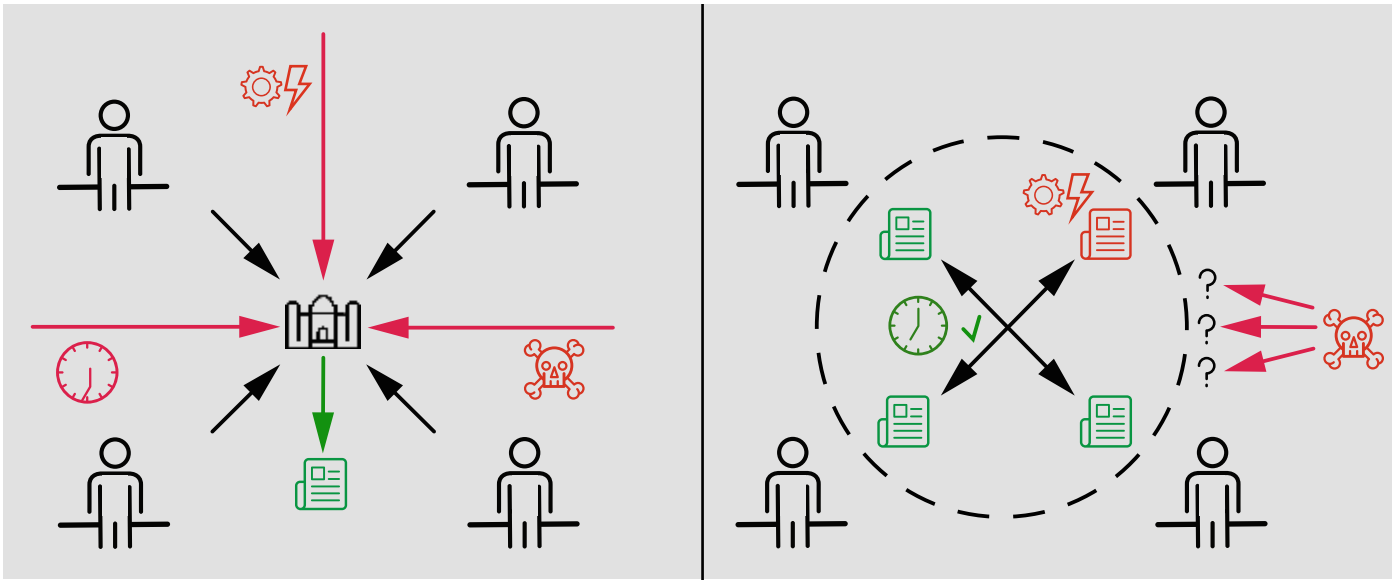
«Die Blockchain ist ein Logbuch, das transparent in einem Netzwerk verteilt geführt wird.»

Christian Cachin

Blockchains sind unter anderem deshalb sicher, weil jeder Block die Informationen des vorherigen Blocks mitnimmt. Damit wird es schwierig, irgendwo einzugreifen – denn dann müsste die ganze Kette abgeändert werden. Ausserdem werden Manipulationen erkannt, weil dieselbe Transaktionskette auf unzähligen Knotenpunkten in einem global verteilten Netz abgebildet ist. Das heisst, dass eine Änderung gleichzeitig auf sehr vielen Knoten geschehen müsste, was praktisch ein Ding der Unmöglichkeit ist. Solch eine sichere Abwicklung ist normalerweise nur möglich, wenn sie durch Zwischenakteure wie Banken verbürgt wird. Mit dieser Technik kann man nun aber Transaktionen direkt zwischen zwei Parteien sicher abwickeln.

Transparente und effiziente Prozesse

Mit den kryptografischen Protokollen, welche die Informationsblöcke verbinden, beschäftigt sich Christian Cachin seit etlichen Jahren. Die bekanntesten Anwendungsfälle davon, die Kryptowährungen, haben viel Aufmerksamkeit auf dieses



Ohne Blockchain
Transaktionen laufen über einen einzigen Knoten, bei dem sich die Macht konzentriert. Das Konstrukt ist undurchsichtig, da Teilnehmende nicht direkt verbunden sind. Es gibt eine einzelne Schwachstelle für Angriffe, Ausfälle und weitere Unterbrüche.

Mit Blockchain
Die Teilnehmenden sind selbst Knotenpunkte. Das System wird gemeinsam betrieben und validiert, ist direkt zugänglich und daher schneller. Es ist ausserdem kryptografisch gesichert und hat keine einzelne Schwachstelle für Angriffe, Ausfälle oder Störungen.

Gebiet gelenkt. Es gibt aber auch andere Einsatzbeispiele wie Unternehmensblockchains, die enger definieren, wer was einsehen und editieren darf. In seiner langen Zeit in der Industrieforschung, unter anderem bei IBM, hat Cachin ein solches System mitenwickelt: Hyperledger Fabric. Davon profitieren Unternehmen beispielsweise, indem sie Lieferketten von der Produktion über die Spedition bis hin zu Endkundinnen und Endkunden transparent abbilden können. Die Macht über die Daten konzentriert sich so nicht bei einer einzigen Partei und das Missbrauchspotenzial sinkt. Ein weiterer Vorteil dieser Systeme ist die Effizienz: So automatisieren Blockchains etwa bereits heute Verzollungsprozesse, indem Länderunterschiede bei Formularen und Abläufen ausgeglichen werden.

Enger Austausch zwischen Forschung und Praxis

Die Forschung und die Praxis seien wieder näher zusammengerückt, freut sich Christian Cachin: «15 Jahre nachdem wir beispielsweise die Frage der Konsensprotokolle erforscht haben und keine Abnehmer für unsere Ideen fanden, wurde das plötzlich extrem relevant. Viele Blockchainfirmen haben heute auch einen engen Austausch mit der Forschung, weil sie verstanden haben, dass sie wissenschaftliche Erkenntnisse einfliessen lassen müssen.» Die Wissenschaft könne nämlich beweisen, dass ein System nicht nur schnell und gut ist, sondern auch sicher bleibt. Unabdinglich für solche Beweise seien präzises Denken und mathematische Kenntnisse, wie sie an der Universität gepflegt werden. Darin sieht Cachin den Unterschied zur Industrie: «Wir müssen modellieren, formalisieren und beweisen, dass ein System unter bestimmten Annahmen sicher ist. Es reicht nicht, einfach zu behaupten, dass ein System bisher gut gelaufen ist und es dies daher weiterhin tun wird.»

Mitarbeit an neuer Gesetzesgrundlage

Oft steht Cachin also am Whiteboard oder jongliert mit Ideen auf dem Papier. Es ist aber auch viel Austausch gefragt, weil verteilte Systeme eben über verschiedenste Grenzen hinausgehen. Als Gastforscher war er schon am MIT und hat sechs Jahre lang die International Association for Cryptologic Research (IACR) präsidiert, welche Journals publiziert und internationale Konferenzen zum Thema durchführt. Ausserdem war er Teil einer Expertengruppe, die eine neue Schweizer Gesetzesgrundlage für Blockchainsysteme beraten hat. Das sogenannte DLT-Gesetz ist dieses Jahr in Kraft getreten und schafft Rechtssicherheit. Cachin erklärt: «Das ist schon eine schnelle Reaktion der Schweiz. Es braucht erst eine gewisse Regulierung, damit die Technik der Blockchain breiter akzeptiert wird und im Alltag ankommt.» Cachin betont aber auch: «Das DLT-Gesetz ist nur ein erster Schritt. Bis die letzten Schlupflöcher gestopft sind, könnte es noch länger dauern.»

Als Beispiel schildert Cachin einen Klassiker der Blockchainwelt: den DAO-Hack, bei dem in der Ethereum-Blockchain ein Fehler passiert ist und Geld abgezogen werden konnte. Wie konnte das passieren? Cachin legt aus: «Was im Protokoll innerhalb der Blockchain abgestimmt wird, gilt. Wenn nun die Mehrheit etwas Dummes abstimmt, dann geschieht das auch so.» Soll nun diese Attacke als unrecht eingestuft werden, obwohl das Abziehen des Geldes durch den Fehler im Code quasi vorgesehen

«Systeme mit exorbitantem Energieverbrauch haben wenig Zukunft.»

Christian Cachin

Fortsetzung Seite 45

und durch Teilnehmende abgesegnet war? Oder soll man gegen die Teilnehmenden vorgehen, die später in das System eingegriffen und den Angriff so gestoppt haben? Es sind neue Fragen, die sich so noch selten gestellt haben.

Nachhaltige Lösungen

Es gibt also noch einiges zu klären, bevor Blockchains richtig in der Gesellschaft ankommen. Christian Cachin ist aber zuversichtlich: «Eines Tages wird man kryptobasierte Systeme haben, weil sie bequemer, günstiger und praktischer sind. Zum Beispiel, weil dann eine internationale Geldüberweisung noch einen Bruchteil kostet.» Die Arbeit wird Cachin und seinen Kolleginnen in der Kryptografie nicht so rasch ausgehen: «Mit Quantencomputern kann man in der Theorie die heute angewendeten Systeme einfach brechen. In der Praxis gibt es diese zwar noch nicht, aber wir werden mit dem Fortschritt der Computertechnik sicher laufend neue Systeme und Sicherheitsbeweise brauchen.»

Damit eine Blockchain Zukunft hat, muss sie ausserdem nachhaltig sein, versichert Cachin: «Systeme wie Bitcoin, in denen Datenblöcke nur mit grossem Energieaufwand an die Kette angehängt werden können, werden wir eines Tages hinter uns lassen.» Alternativen zu diesen sogenannten Proof-of-Work-Protokollen existieren bereits und sollen demnächst beim System Ethereum zum Einsatz kommen. «Das effizientere System wird sich schliesslich durchsetzen», folgert er. Wird die Kryptowährung Bitcoin also aussterben? «Solange es Leute gibt, die das System weiter erhalten, kann es auch immer weiterlaufen. Es könnte aber gut sein, dass eine Währung wie Bitcoin irgendwann nur noch von Nostalgikern als Hobby betrieben wird», schmunzelt Cachin und wirft einen bedeutungsvollen Blick in die Ecke seines Büros. Dort steht ein originaler Apple Macintosh-Computer aus den 1980er-Jahren, der in seiner Blütezeit wohl ähnliche Diskussionen erlebt hat.

Kontakt

Prof. Dr. Christian Cachin
Institut für Informatik,
christian.cachin@inf.unibe.ch