NZZ

Herausforderung für Banken und den Staat

Blockchain – der nächste Wohlstandsschock

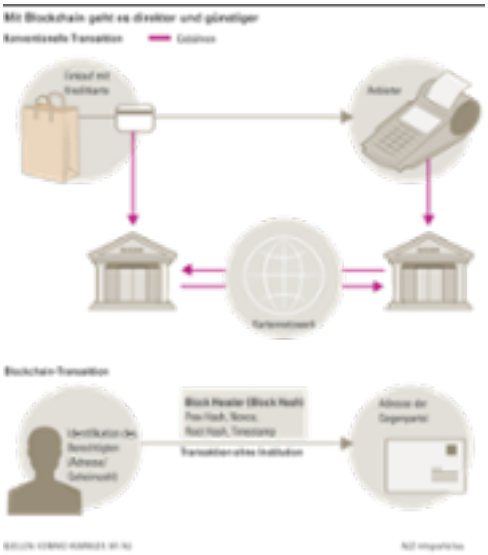
von Konrad Hummler 3.5.2016
Blockchain ist mehr als eine digitale Technologie. Es ist ein System, das die Chance bietet, Eigentumsverhältnisse viel einfacher und günstiger zu sichern und zu ordnen. Das wird Konsequenzen haben.

Eigentum etabliert eine herrschaftliche Beziehung zwischen Person und Sache. (Bild: Imago)

Viele Artikel werden derzeit zu Blockchains geschrieben. Den meisten ist gemein, dass sie sich mit der Komplexität der Materie schwertun. Die Leser werden anhand von immer wieder abgeschriebenen Beispielen in die Geheimnisse der eine Blockchain definierenden Kryptografie eingeweiht. Bereits existiert eine Blockchain-Sondersprache und grassiert jene Verschworenheit einer Priesterschaft von Eingeweihten, die naive Fragen ahnungsloser Laien in der Kehle ersticken lässt. Doch was ist eine Blockchain tatsächlich? Wie lässt sich der Kern dieses Phänomens beschreiben? Was wäre die kürzeste aller Definitionen? Mein Versuch lautet folgendermassen: Blockchain ist ein System, das kraft seiner lückenlosen und nicht veränderbaren Historie Beweiskraft erlangt, um Eigentumsverhältnisse zu regeln. Was aber heisst das?

Eigentum gewährleisten

Eigentum etabliert eine herrschaftliche Beziehung zwischen Person und Sache. Ausser wenn eine Person buchstäblich auf einer Sache sitzt, ihr Eigentum also besitzt und selber verteidigt, ergibt sich die Herrschaftlichkeit der Beziehung zwischen Person und Sache erst durch den Bezug auf eine durchsetzungsfähige Instanz, die Eigentum gewährt. In den meisten Rechtssystemen der Welt gibt es deshalb auch die Unterscheidung zwischen Besitz und Eigentum, da das Besitzen nicht zwingend vom Eigentümer ausgeübt werden muss.



Eigentum kommt ohne Verankerung bei einer Instanz nicht aus. Eigentum muss erstritten werden können, sonst ist es wertlos. Die Verteidigung des Eigentums auf eigene Faust ist in einer komplexen, zivilisierten Gesellschaft impraktikabel. Um die Rechtmässigkeit des Eigentums und die Echtheit der Sache feststellen und garantieren zu können, braucht es im Alltag ordnende Institutionen, dank deren die Erwartungen in der Gesellschaft und der effektive Sachverhalt weitgehend deckungsgleich gehalten werden können.

Diese Institutionen haben ihren Preis. Es kann sich dabei erstens um direkte Gebühren handeln, wie sie beispielsweise von Banken, Depotstellen oder Clearinghäusern erhoben werden. «Gebühren» können aber auch indirekt und versteckt anfallen, etwa wenn zweitens Institutionen unmerklich ihre Glaubwürdigkeit ritzen und am Ende Stabilitätskrisen verursachen, die dann als höhere Gewalt interpretiert werden. Kostspielig wird es drittens auch, wenn Institutionen eine Verwässerung des Eigentums zulassen oder herbeiführen, beispielsweise durch Inflation oder durch Vermögensverminderung infolge negativer Zinsen, was auf dasselbe hinausläuft. Viertens müssen die mit der Gewährleistung von Eigentum beschäftigten Institutionen je länger, je mehr mit dem grössten Stakeholder des Bürgers, den Steuerbehörden, zusammenarbeiten, um Anknüpfungspunkte zur legalen Enteignung mittels Steuern zur Verfügung zu stellen.

Wie Blockchain funktioniert

Wenn aber die herkömmliche Gewährleistung von Eigentum gleich vierfach kostspielig und letztlich auch unsicher ist, so ruft dies geradezu nach einem System, das idealerweise Eigentum ohne institutionelle Verankerung zulässt. Ein solches System, das kraft seiner lückenlosen und nicht veränderbaren Historie Beweiskraft erlangt, um Eigentumsverhältnisse zu regeln, ist Blockchain.

Aber um welches System handelt es sich, und wie können wir es verstehen? Die erforderliche «lückenlose Historie» entsteht bei Blockchain durch Aneinanderreihung von nicht veränderbaren Richtigbefundanzeigen («block»). Diese bestehen aus vier Komponenten: erstens der Vergangenheit (dem vorangegangenen Block), zweitens dem aktuellen Zeitstempel («timestamp») zur Einordnung auf der Zeitachse, drittens den noch nicht bestätigten, laufenden Transaktionen, heruntergebrochen in einen kryptografischen Code («root hash»), sowie viertens einer Einmalnummer, welche über Versuch und Irrtum gefunden werden muss («number used once = nonce»). Das System stellt sicher, dass eine neue Richtigbefundanzeige nur entstehen kann, wenn sie am neusten Block andockt. Deshalb wird bildlich von einer Kette, von Blockchain, gesprochen.

Dass mit Blockchain Transaktionen, das heisst Inhaltsveränderungen, durchgeführt werden können, dafür sorgt ein System von Schloss (einem «public key» als Adresse) und Schlüssel (einem «private key» in Form einer persönlichen Geheimzahl). Über den Schlüssel kann nur der Berechtigte verfügen. Die Grundlage des Blockchain-Systems bildet dabei eine Verschlüsselungstechnik («Hashfunktion») , bei welcher der Zielwert ohne viel Aufwand graduell, aber um Potenzen verschärft werden kann. Das System läuft seinen Gegnern deshalb sozusagen hoffnungslos voraus und davon. Es ist extrem sicher, weil die Richtigbefundanzeigen dezentral – im Extremfall in jedem teilnehmenden Computer auf der Welt – abgespeichert sind. Eine von einem Hacker herbeigeführte Veränderung an einem Ort würde von den millionenfach vorhandenen weiteren

Teilnehmern verzugslos erkannt und überschrieben werden. Letztlich kann jeder PC eines Teilnehmers am System Netzknotenfunktionen übernehmen. Ein Systemausfall ist deshalb schwer vorstellbar. Er erscheint jedenfalls deutlich weniger plausibel als ein Ausfall herkömmlicher Institutionen, die derzeit relativ zentral den Nachweis von Eigentum sicherstellen.

Welche Eigentumsrechte können mittels einer Blockchain geregelt werden? Eigentlich alle. Im Vordergrund stehen selbstverständlich Rechte und Dienstleistungen, die in direktem Zusammenhang mit dem Internet stehen. So könnte man, wenn man denn wollte, das Eigentum und damit das Leserecht an einer Zeitung im Internet eindeutig einer Person zuordnen. Es könnte sich aber auch um ein Geheimdokument handeln. Oder um ein verbotenes Bild. Oder um die Anleitung zum Bau einer Atombombe. Oder um einen Liebesbrief. Oder um ein Guthaben. Oder um das Recht auf Speicherkapazität in einer Cloud; um Musik, Filme: Eine Blockchain kennt keine materiellen Grenzen und auch keine Moral. Darin liegen ihre Stärken und Schwächen zugleich, ähnlich dem Streichholz, mit dem man eine Kerze anzünden oder einen Waldbrand entfachen kann.

Smarte Anwendungen

Absehbar wird die Digitalisierung eine Konvergenz zwischen dem Funktionieren von Anlagen und der Regelung von spezifischen Eigentumsrechten (bzw. Nutzungsrechten) mit sich bringen. In der neu entstehenden Fachsprache redet man von Smart Contracts, intelligenten Verträgen. So könnte man beispielsweise das Risiko im internationalen Handel drastisch reduzieren, wenn Anlagen und Maschinen dank Smart Contracts erst in Betrieb genommen werden könnten, wenn deren Freigabe in der Blockchain eindeutig bestätigt wäre. Im gleichen Sinne könnte definiert werden, dass der Betrieb nur so lange aufrechterhalten wird, wie die im Smart Contract gesetzten Bedingungen erfüllt sind. Das eröffnet ungeahnte Möglichkeiten zur verbesserten Durchsetzung des Immaterialgüterrechts. Gerade im Bereich des Patentwesens ist ja die Schwäche des institutionellen Schutzes des Eigentums eklatant und sind die Kosten exorbitant.

Für mich steht ausser Frage, dass für die Abwicklung von Smart Contracts, für den Handel mit Wertschriften oder für die Vermittlung von Gütern und Dienstleistungen aller Art die Kombination eines Blockchain-Systems mit einer Blockchain-basierten Transaktionswährung ideal ist. Die Transaktionswährung kann die umstrittene Bitcoin sein, muss aber nicht. Der grosse Vorteil einer solchen Kombination liegt in der fast atemraubend einfachen Abwicklung (vgl. Grafik). So erfordert eine herkömmliche Wertschriftentransaktion zwischen zwei oder mehreren Parteien zwingend je eine Bank, je eine Depotstelle und eine Clearingstelle sowie ein auf Vertrauen und gegenseitig ausgetauschten Sicherheiten basierendes Kreditierungssystem. In der Blockchain-Welt kann dieselbe Transaktion mit einer Blockchain-Transaktionswährung als kleinstem Nenner Zug um Zug abgewickelt werden. Damit solches tatsächlich Fuss fassen kann, müssen allerdings im Internet wohl vorerst noch neue Standards definiert werden, auf denen dann die institutionenfreie oder -arme Welt aufgebaut werden kann.

Was tun Banken und der Staat?

In der Finanzbranche herrscht derzeit eine Mischung aus Aufbruchstimmung, Angst und Panik. Denn eines ist klar: Wie auch immer die Strukturen am Ende aussehen mögen, die Blockchain-Technologie wird sehr vieles ersatzlos überflüssig machen. Die Margen werden schrumpfen, neue Anbieter auftauchen; voraussichtlich wird kein Stein auf dem anderen bleiben. Für die Banken stellt sich somit ein ähnliches Problem wie seinerzeit für die grossen Medienhäuser zu Beginn der Verbreitung von geschriebenen Inhalten im Internet: Mitmachen und mithin am eigenen Ast sägen? Oder definitiv alle Chancen verpassen? Oder (und nicht unwahrscheinlich) sich geschickt mit einem Regulator verbinden, um den Übergang in die neue Welt erträglicher zu gestalten?

Mehr Sorgen als die Auswirkungen auf den Finanzsektor bereitet mir, was das System der Blockchain für den Staat bedeuten könnte. Dessen Institutionen beziehen ihre Rechtfertigung aus der Stabilisierungsfunktion für das Zusammenleben der Bürger untereinander und in Bezug auf ihre privaten Herrschaftsverhältnisse gegenüber Sachen, dem Eigentum. Die Blockchain-Technologie wird einen Teil dieser Funktionen überflüssig machen. Die Zeitschrift «Economist» erwähnte das Grundbuch. Vor allem dort, wo es bisher kein funktionierendes Grundbuch gab, nämlich in sämtlichen Entwicklungs- und in vielen Schwellenländern, wäre das eine grosse Chance. Schwächere Mitglieder der Weltgesellschaft könnten endlich auch gesichert Eigentum erwerben und so kreditwürdige Wirtschaftssubjekte werden. Ein Wachstumsschub wäre programmiert, vorausgesetzt, die Einführung der Grundbuch-Blockchain ginge einher mit einer die neuen Eigentumsverhältnisse begründenden Landreform.

Dennoch plagen mich Sorgen. Denn so unvollkommen die vom Staat schlecht und recht betriebenen herkömmlichen Institutionen sind, sie begründen Macht- und Unterdrückungs-Verhältnisse, die nicht einfach so verschwinden werden. Der Moloch wird sich gegen seinen teilweisen Untergang zur Wehr setzen. Werden dezentral basierte Kryptowährungen dereinst die von der Institution Zentralbank etablierten und kontrollierten staatlichen Währungen ersetzen können? Oder wenigstens konkurrenzieren? Wird man das zulassen? Mit welchen Argumenten wird man es zu verhindern versuchen? Es geht um sehr viel; beispielsweise um die Vorherrschaft des US-Dollars im Welthandel. Allerdings stimmt mich optimistisch, dass sich in freien Gesellschaftsordnungen paretooptimale Lösungen eigentlich stets durchsetzen, bei denen insgesamt alle bessergestellt werden, ohne dass jemand anderes dadurch benachteiligt würde.

Anonymität als Achillesferse

Es gibt allerdings eine Achillesferse der Blockchain, die ich in deren durch die Verschlüsselung gegebenen totalen Anonymität sehe. Sie verunmöglicht es, Handlungen klar zuzuordnen. Im Zeitalter global einsatzfähigen Terrorismus und immer internationalerer Kriminalität ist Anonymität ein Killerkriterium, wie naheliegend und wohlstandsfördernd eine Technologie auch sein mag. Die Weltgemeinschaft und die sie repräsentierenden Instanzen müssen zwingend darauf bestehen, zu unglaublichen Schandtaten fähige Menschen einigermassen lückenlos kontrollieren zu können. Sonst wird es auf dem Planeten Erde zu gefährlich. Die anarchistisch bis libertär verdrahteten Vordenker der Blockchain-Technologie werden deshalb erkennen und akzeptieren müssen: Wenn die Blockchain ihren segensreichen Siegeszug antreten soll, dann muss ihre Anonymität zugunsten einer Kontrollierbarkeit aus dem Netz verbannt werden. Das ist ein hoher Tribut, der an die Institutionen der Macht zu zahlen ist, gewiss, aber er ist alternativlos. Die Institutionen brauchen Kontrollmöglichkeiten zur Aufrechterhaltung der Sicherheit und Anknüpfungspunkte zur Erhebung von Steuern.

Die Blockchain-Technologie sehe ich als ein weiteres Glied in der langen Kette, die mit der Verbreitung von PC und Mobiltelefonie ihren Anfang nahm, uns über das Internet an weltweit verbreiteten Inhalten teilnehmen lässt, wirtschaftliche und soziale Prozesse aufbricht, Intermediäre in die Knie zwingt und nun auch das Wesen der Institutionen im Kern angreift. Für mich steht jedenfalls ausser Frage, dass die Blockchain-Technologie wegen der weitestgehenden Elimination institutionell bedingter Kosten bald einmal zu einer bestimmenden Kraft in der weiteren Entwicklung des Internets und ganz generell von wirtschaftlichen, sozialen und politischen Abläufen werden wird.

Konrad Hummler war Teilhaber der Privatbank Wegelin und Verwaltungsratspräsident der NZZ.