Ausgabe 17

Blockchain: wie explosiv?

bergsicht

KAPITEL 1

Meine antike «Blockchain»

Einmal im Jahr, wenn die Kerzen am Weihnachtsbaum brennen und die Familie feierlich beisammensitzt, «Stille Nacht …» aus vereinten Kehlen verklungen ist, holt der *pater familias* jenen abgegriffenen, dicken Band aus dem Büchergestell, nämlich die aus dem 18. Jahrhundert stammende Bibel in der Lutherübersetzung. Sie überlebte schadlos die Aufklärung, die Französische Revolution, die Übersiedelung der liberalen deutschen Vorfahren in die Schweiz, zwei Weltkriege im 20. Jahrhundert und mithin den Erbgang von mehr als einem Dutzend Generationen. Auf dem Einband sind, zunächst in schwer leserlicher deutscher Schrift, später in helvetischen Blockbuchstaben, die jeweiligen Eigentümer der amüsant bis drastisch illustrierten Heiligen Schrift verzeichnet; die Übergabe der einen an die folgende Generation erfolgte jeweils aus Anlass der Hochzeit – wohl in der Erwartung, dass damit auch eine angemessene Grundlage für nachfolgenden Kindersegen geschaffen sei. Der bis dato auch unterbruchsfrei eintraf.

Besagte Lutherbibel ist eine Blockchain, beziehungsweise: der lückenlose Eintrag der Eigentümer *gleicht* einer Blockchain und wird deshalb in der Folge als Metapher verwendet. «Blockchains» sind derzeit in vieler Munde, ja, eine wahre Flut von Artikeln ergiesst sich derzeit durch einschlägige Magazine und Zeitungen, vom «Economist» über das «Wall Street Journal», die NZZ und die «Schweizer Bank» bis zum Samstagsmagazin der Tamedia-Gruppe. Sozusagen allen Artikeln ist gemeinsam, dass sie sich mit der Komplexität der Materie schwertun und viele Aspekte ausgeklammert bleiben müssen. Die Leser werden anhand von immer wieder abgeschriebenen Beispielen in die Geheimnisse der eine Blockchain definierenden Kryptographie eingeweiht; bereits existiert eine Blockchain-Sondersprache mit meist unscharfer Begrifflichkeit und grassiert jene Verschworenheit einer Priesterschaft von Eingeweihten gegenüber ahnungslosen Laien, die naive Fragen in der Kehle ersticken lässt. Gemeinsam ist den Artikeln auch die Androhung der nächsten Strukturkrise, die nach den Umwälzungen durch Internet 1.0 und 2.0 noch viel, viel mehr Jobs obsolet werden lässt.

Wir versuchen, in dieser bergsicht keinen einzigen unverständlichen Satz zum Thema Blockchain zu schreiben. Das ist bereits ein hoher Anspruch. Darüber hinaus wollen wir die Angelegenheit einordnen. Technologisch zunächst, dann aber vor allem im Hinblick auf die zu erwartenden sozialen, politischen und ökonomischen Konsequenzen. Da es sich um Neuland handelt und somit Investitionen zur Erschliessung der neuen Territorien bevorstehen, geben wir am Schluss einige Ideen für eine mögliche vermögensmässige Positionierung zum Thema Blockchain. Diese Ausgabe der *bergsicht* wird begleitet von einem Glossar, das dem Vertiefung suchenden Leserpublikum für die Lektüre zum Thema von Nutzen sein kann.

Zurück zu den handschriftlichen Einträgen in der Lutherbibel. Sie vermitteln die Übersicht, wer in der betreffenden Familie zu welchem Zeitpunkt rechtmässiger Eigentümer des Bandes gewesen ist. Das Hochzeitsdatum ist sozusagen der Zeitstempel [in der Blockchain-Sprache der «Timestamp»], mit welchem der Eigentumsübergang auf einen neuen Namen [für grundsätzlich jedermann einsehbarer «Public Key»] eindeutig bestätigt wird. Müsste man nun als Nachfahre den Beweis antreten, dass man wirklich rechtmässiger Eigentümer ist, dann böte sich in neuerer Zeit gewiss die DNA-Probe an, die fälschungssicher die Rechtmässigkeit des Eigentums bestätigen würde. Die Ahnenreihe wäre so etwas wie ein Sicherheitsschloss, das mit dem Schlüssel des DNA-Skripts [«Private Key»] geöffnet werden kann. Einen zweiten solchen Schlüssel kann es kaum geben, da es extrem unwahrscheinlich ist, dass zwei Individuen über dieselbe DNA verfügen, und noch viel unwahrscheinlicher, dass sich jenes unwahrscheinliche Individuum innert nützlicher Frist einfinden könnte, um seinerseits das Eigentum zu erstreiten. Der Zeitstempel wird gültig, wenn am Hochzeitstag die anwesenden Familienmitglieder durch Nichtintervention ihr Einverständnis zur Übergabe der Lutherbibel bestätigt haben.

Was also ist eine Blockchain? Ein System, das kraft seiner lückenlosen Historie Beweiskraft erlangt, um Eigentumsverhältnisse zu regeln. Damit ist eigentlich schon alles gesagt. Oder doch nicht ganz.

KAPITEL 2

Eigentum ist prekär

Eigentum, das heisst die herrschaftliche Beziehung zwischen Person und Sache, verlangt an dieser Stelle nach einigen Erläuterungen. Ausser im nicht so häufigen Fall, dass eine Person buchstäblich auf einer Sache sitzt, ihr Eigentum also be*sitzt* und gegebenenfalls selber verteidigt, ergibt sich die Herrschaftlichkeit der Beziehung zwischen Person und Sache erst durch den Bezug auf eine *durchsetzungsfähige Drittinstanz*, die Eigentum *gewährt*. In den meisten Rechtssystemen der Welt gibt es die Unterscheidung zwischen Besitz und Eigentum, da das buchstäbliche Besitzen nicht zwingend vom Eigentümer ausgeübt werden muss. Die Bibel im Büchergestell des pater familias steht unzweifelhaft sowohl in dessen Besitz als auch in dessen Eigentum. Er darf, qua seiner Stellung als Eigentümer, seine Rechte an der Sache ausüben, nämlich das Eigentum brauchen (usus), nutzen (usus fructus) und darüber verfügen, es zum Beispiel verkaufen oder sogar zerstören (abusus). Dem Besitzer, der nicht Eigentümer ist, steht namentlich letzteres Recht nicht zu. Ein ausgeliehenes Buch, in dessen Besitz man ist, darf man nicht einfach verkaufen oder wegschmeissen. Das bürgerliche Recht regelt in einfachen, den praktischen Lebensalltag eng nachbildenden Sätzen die für das einigermassen friedvolle Zusammenleben sehr grundlegende Beziehung zwischen Menschen und realen Gütern. Dazu gehört beispielsweise die Vermutung, dass der Besitzer einer Sache im Regelfall auch dessen Eigentümer ist, oder auch der Grundsatz, dass die Gewähr – Rechtmässigkeit des Erwerbs durch einen Vor-Eigentümer – vermutet werden darf. Im spezifischen Fall einer Banknote muss uns wenig oder gar nicht kümmern, auf welchen Wegen oder Abwegen sich das Stücklein Papier bei den Vorgänger-Eigentümern oder -Besitzern befand. Viele Noten in unserer Geldbörse könnten vermutlich halbe oder ganze Romane erzählen …

Eigentum, so wie es unseren Lebensalltag prägt, erweist sich dank diesen und weiteren «default-Regeln», also rechtlichen Vermutungen und Fiktionen, als weitgehend unkritisch. Man steigt jeden Tag selbstverständlich in sein Auto, freut sich daran und nutzt es, fährt es irgendwann vielleicht einmal zu Schrott. Täglich nehmen wir Banknoten und Münz entgegen und geben sie wieder weiter. Und keine Frau denkt daran, dass ihre geerbten Ohrringe der Kulturgüterschutzkonvention unterstehen könnten. Dennoch: Eigentum kommt ohne Verankerung bei einer Instanz, welche dank *übergeordneter* Herrschaftlichkeit der Durchsetzung der *privaten* herrschaftlichen Rechte der Person an einer Sache mächtig ist, nicht aus. Eigentum muss erstritten werden können, sonst ist es wertlos. Die Verteidigung des Eigentums auf eigene Faust oder durch die eigene Waffe ist in einer komplexen, zivilisierten Gesellschaft impraktikabel. Das Eigentum, dessen Rechtmässigkeit und die Echtheit der Sache – das heisst die erwähnte Gewährleistungsproblematik – verlangen für den praktischen Alltag und Umgang nach *ordnenden Institutionen*, dank derer die Erwartungen in der Gesellschaft und der effektiv eintreffende Sachverhalt weitgehend deckungsgleich gehalten werden können. So unsere Definition des Begriffs «Institution». Wer ein Grundstück erwirbt, denkt dank Grundbuchamt und Notar keine Minute daran, dass ein unbekannter Dritter ihm das Stück Land strittig machen könnte. Erwartung und effektiver Sachverhalt entsprechen sich. Selbst im etwas abenteuerlicheren Automobilhandel herrscht im grossen und ganzen Vertrauen zwischen den Kontrahenten, vorausgesetzt, der Händler habe sich als Quasi-Institution dieses Vertrauen durch Wohlverhalten in der Vergangenheit verdient. Auch im Automobilhandel sind Gewährleistungsstreitigkeiten relativ selten; Erwartungen und effektiver Sachverhalt decken sich weitgehend. Die Eigentum vermittelnden und regelnden Institutionen bewähren sich.

Wir sind uns kaum bewusst, wie selbstverständlich wir von der Existenz funktionierender Institutionen ausgehen und von ihnen Gebrauch machen. So wird unser Eigentum an einem Geldvermögen uns

durch eine Reihe von aneinander geketteter Institutionen glaubhaft gemacht, und nicht nur uns, sondern auch Dritten, mit denen wir bezüglich Geld in Verbindung stehen, indem wir zum Beispiel mittels einer Kontoüberweisung eine Rechnung bezahlen. Die Glieder dieser Kette der Institution heissen Banken, Zentralbanken, Clearinghäuser. Um die Vertrauenswürdigkeit dieser Institutionen zu untermauern, werden sie durch Meta-Institutionen wie die Finanzmarktaufsicht oder die Bank für Internationalen Zahlungsausgleich gelenkt und kontrolliert. Am Ende steht eine Zahl auf einem Kontoblatt, und dank dieser Zahl fühlen wir uns als Eigentümer, weil wir darauf *vertrauen*, dass die Kette von Institutionen glaubwürdig genug ist, um uns das *Eigentum zu gewährleisten*.

Täglich können wir diese Glaubwürdigkeit testen, wenn wir solchermassen abgeleitetes Eigentum in reale Werte konvertieren, also zum Beispiel Sachen erwerben oder Rechnungen bezahlen, wenn wir mit Geld Wertschriften kaufen oder es in andere Währungen umtauschen. Die nicht in Frage gestellte *Konvertibilität* entspricht einem laufend erbrachten konkludenten *Tatbeweis* für die Glaubwürdigkeit und für das geschenkte Vertrauen in die Institution. Falls die Konvertibilität dennoch einmal unterbrochen wird, wie es zum Beispiel in der Zypern- und der Griechenlandkrise geschah, kann das auf Vertrauen basierende, durch Institutionen untermauerte Eigentumssystem in unkontrollierbarer Weise implodieren. In den dunkelsten Momenten der Eurokrise half nur noch die Garantiezusage Angela Merkels, um eine solche Implosion zu verhindern. Ihr Scheck war zwar ungedeckt, aber dank ihrer institutionell bedingten Autorität gelang es der Bundeskanzlerin damals, den europaweiten Bank-Run abzuwenden.

Je weniger dinglich eine Sache ist – man vergleiche etwa besagte Lutherbibel mit einem Warenterminkontrakt auf Schweinebäuche zu einem bestimmten Preis in, sagen wir, drei Monaten – desto gewichtiger erweist sich die Rolle von Institutionen in der Regelung von Eigentumsrechten. Ganz besonders ist das der Fall bei der in höchstem Masse virtuellen Sache, dem *Geld*. Es widerspiegelt *nur Vertrauen*. Vertrauen, das täglich durch Wohlverhalten der verantwortlichen Personen verdient wird (oder auch nicht) und das durch laufende und unangefochtene Konvertibilität in weniger virtuelle Sachen untermauert wird (oder auch nicht). Vertrauen verhält sich unstetig-diskontinuierlich: Die Verletzung seiner Prinzipien kann lang unentdeckt oder unbeachtet bleiben, der Zusammenbruch ist für die Institution und die sich auf sie verlassenden Anspruchsnehmer jedoch plötzlich und verheerend. Deshalb kommt es immer wieder zu Stabilitätskrisen, in deren Mittelpunkt Institutionen und die für sie verantwortlichen Personen stehen, die über lange Zeit still und leise Vertrauen ausgenutzt und ausgehöhlt haben. Üblicherweise dauert es extrem lange, einmal verlorenes Vertrauen wieder aufzubauen.

Die Institutionen haben ihren Preis. Die Gewährleistung von Eigentum durch deren Einschaltung als dritte Instanz, eine Institution eben, ist *kostspielig*. Das können direkte Gebühren sein, wie sie beispielsweise von Banken, Depotstellen oder Clearinghäusern erhoben werden. Es können aber auch «Gebühren» versteckt erhoben werden, indem die Institutionen unmerklich ihre Glaubwürdigkeit etwas «ritzen» und am Ende Stabilitätskrisen verursachen, die dann als höhere Gewalt interpretiert werden, oder sei es, indem die eine oder andere Verwässerung des Eigentums zugelassen oder herbeigeführt wird, beispielsweise durch Inflation oder durch Vermögensverminderung infolge negativer Zinsen, was letztlich auf dasselbe hinausläuft. Ausserdem können oder müssen die mit der Gewährleistung von Eigentum beschäftigten Institutionen mit dem grössten Stakeholder des Bürgers, der Steuerbehörde, mehr oder weniger eng zusammenarbeiten, um diesem Anknüpfungspunkte zur legalen Enteignung mittels Steuern zur Verfügung zu stellen.

Die sich somit vierfach manifestierende Kostenträchtigkeit der Institution – Gebühren, um die eigenen Kosten zu decken und gegebenenfalls Gewinn zu erwirtschaften, Stabilitätskrisen, Verwässerungstendenzen sowie die Zurverfügungstellung fiskalischer Anknüpfungspunkte – rufen sachlogisch nach einem System, das idealerweise *Eigentum ohne institutionelle Verankerung* zuliesse. Ganz einfach deshalb, weil das institutionell gewährleistete Eigentum zu kostspielig und letztlich zu unsicher ist. Der schleichende *Verrat des Eigentümers* durch die das Eigentum gewährleistende Instanz ist *spieltheoretisch gegeben* und *vorhersehbar*. Wir wiesen in der *bergsicht* Ausgabe 14 («Geld, Glaubwürdigkeit und Zwang») darauf hin, dass die aus unserer Sicht äusserst fragwürdige Politik der Notenbanken, Staatsschulden des eigenen Landes beziehungsweise aus dem eigenen Währungsraum zu finanzieren, das Bedürfnis nach einer solchen generellen Abwendung von der Institution beschleunigen könnte. Heute sehen wir diese Sichtweise mit dem Aufkommen der Blockchains bestätigt. Grundsätzlich lässt sich folgendes festhalten: Die Art, wie Eigentum wahrgenommen wird – institutionell, wie soeben beschrieben, durch manifesten Be*sitz* oder aber künftig, wie zu beschrieben sein wird, durch algorithmischen Beweis – entscheidet sich an der Höhe der Kosten, welche die eine oder die andere Art nach sich zieht.

KAPITEL 3

Verschlüsselung und Dezentralisierung als Stabilitätsfaktoren

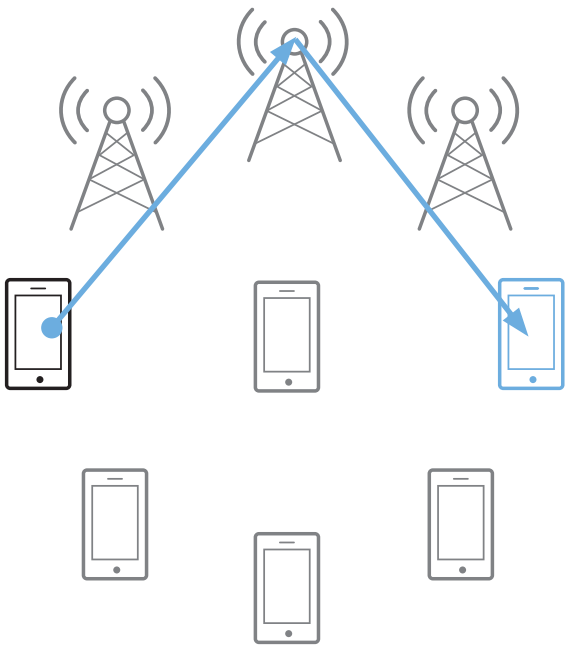
Die Technik macht's möglich, dass die *Institution* als stets übergeordnetes und damit für eine Viel-

heit von Individuen tätiges, mithin *zentrales System* ersetzt wird durch die Umkehrung ins pure Gegenteil, die denkbar extremste De-Zentralisierung, im Sinne eines eigentlichen Non-Zentralismus (Robert Nef). Verwenden wir zur Illustration zunächst ein Beispiel, das nichts oder wenig mit der danach zu beschreibenden Blockchain-Technologie zu tun hat. So sind wir es bis heute gewohnt, unser Smartphone bei einem grossen Systembetreiber, etwa bei der Swisscom, bei Sunrise oder Vodafone, zu erwerben, dort ein Abonnement zu lösen und unsere Gespräche über die diesen *Carriern* gehörenden und von ihnen betriebenen Antennen und Anlagen zu führen. Diese Carrier sind gewichtige Institutionen mit satten Erträgen. Vorderhand sind wir gezwungen, mit ihnen zusammenzuarbeiten. Es führt kein Weg an der zentralen Bündelung und Übermittlung aller geführten Gespräche vorbei.

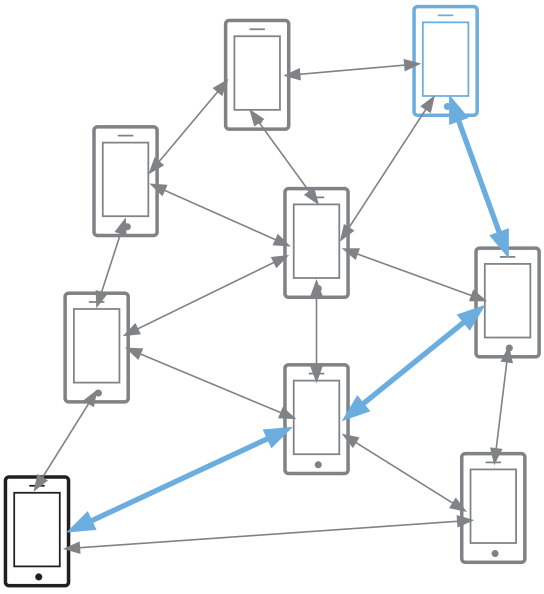
Denkbar und technisch durchaus machbar wäre aber auch eine Telefonie, welche ausschliesslich über die millionenfach vorhandenen Antennen der individuellen Mobiltelefone abgewickelt wird, also ohne Carrier auskommt. Jeder von uns würde auf diese Weise sozusagen zu einem Mini-Carrier, indem er Antennenleistung für Dritte zur Verfügung stellt und auch solche von Dritten in Anspruch nimmt. Dank der hohen Dichte vorhandener Mobiltelefone würden die Gesprächsbits mit Lichtgeschwindigkeit von Handy zu Handy hüpfen und so an ihr Ziel gelangen. Swisscom, Sunrise und Vodafone hätten ausgedient beziehungsweise könnten bestenfalls noch in ihren Verkaufsläden, Kiosken gleich, Apparate anbieten. Phantasterei? Nicht wirklich. Aus unserer Sicht eher eine Frage der Zeit. Eine Wertschöpfung, die es aus technischen Gründen nicht mehr braucht, ist keine Wertschöpfung mehr und fällt dahin. So geschah es den Kerzen- und Zündholzproduzenten bei Einführung des elektrischen Lichts, so geschah es den Kutschern, als aufs Automobil umgestiegen wurde, den Schreibmaschinenherstellern beim Siegeszug des Laptops und des PCs. Mit dem einen grossen Unterschied, dass jene technischen Entwicklungen *Produkte* obsolet machten, die neuste Entwicklung in ihren Konsequenzen jedoch die *Institution*.

⟶ *Fortsetzung auf Seite 8*

Kommunikation über Carrier-Antennen



Kommunikation über Mobile-Phone-Antennen



Glossar

Die wichtigsten Begriffe

[«Blockchain»]

Algorithmus

Handlungsschema, bestehend aus einer endlichen Anzahl aufeinanderfolgender und definierter Einzelschritte, zur Lösung eines bestimmten Problems.

Bitcoin

Bekanntestes dezentrales Zahlungssystem und Name der Kryptowährung. Die Marktkapitalisierung beläuft sich auf derzeit über 6 Milliarden USD.

Bitcoin Protocol

Digitale Dokumentation der Transaktionsblöcke.

Block

Jeder Block beinhaltet den vergangenen Block, die aktuellen Transaktionen, einen Timestamp und einen Nonce. Diese Bestandteile werden jeweils mit der Hashfunktion verschlüsselt.

Blockchain

Kette aus Blöcken mit verschlüsselten Informationen.

Blockchain 1.0

Entwicklung und Anwendung von auf Kryptowährungen basierenden Applikationen mit Bezug zu Geld, Währungen und Zahlungen.

Blockchain 2.0

Umfassende Anwendungen mit Bezug auf die gesamte Ökonomie.

Blockchain 3.0

Applikationen, welche über Währungen, Finanzen und Märkte hinausgehen. Zum Beispiel: Staatsorganisationen, Gesundheitswesen, Wissenschaft, etc.

Glossar

Die wichtigsten Begriffe

Blockhash

Hashwert eines kompletten Blocks.

Clearing

Feststellen gegenseitiger Forderungen oder Verbindlichkeiten und Lieferverpflichtungen.

Crowdfunding

Finanzierungsmethodik, bei welcher die Kapitalgeber eine Vielzahl von Personen sind, welche jeweils kleine Beiträge leisten. Die Teilnehmer finden sich üblicherweise über das Internet.

Ethereum

Dezentralisierte (Programm-)Plattform für Blockchain-basierte Anwendungen (Unternehmen mit Sitz im Kanton Zug).

Hashfunktion

Funktion, welche einen umfassenden Eingabewert (Schlüssel) in einen Zielwert (Hashwert) mit einheitlicher Grösse zerlegt. Dies ist eine Verschlüsselungsmethodik.

Hashwert

Zielwert, welcher durch eine Hashfunktion generiert wird.

Internet 1.0

Der Nutzer tritt lediglich als Konsument des vom Internet bereitgestellten Inhalts auf.

Internet 2.0

Interaktives Internet. Der Nutzer konsumiert nicht nur Inhalt, er stellt auch Inhalt zur Verfügung.

Internet 3.0

Semantisches Web. Inhalt des Webs soll für Maschinen besser verständlich werden, die Maschine denkt eigenständig.

Kryptographie

Verschlüsselung von Informationen zur Informationssicherheit.

Kryptowährung

Digitale Währung, welche auf einem verschlüsselten (kryptographischen) Code basiert.

Merkle Tree

Datenstruktur, welche einen Baum aus Hashwerten bildet. Dies stellt die Integrität von Daten sicher. Benannt nach dem amerikanischen Mathematiker Ralph Merkle.

Miner

Teilnehmer am Netzwerk, welcher Mining betreibt.

Mining

Rechenprozess, bei welchem neue Blöcke generiert werden. Dies beinhaltet das Lösen eines komplexen mathematischen Problems. Für das Mining werden die Miner entschädigt. Dies entspricht dem Schöpfungsprozess einer Notenbank.

Glossar

Die wichtigsten Begriffe

Nodes

Knoten, respektive Teilnehmer am dezentralisierten System.

Nonce

Schlüssel, welcher nur einmalig verwendet werden kann (number used once). Den Schlüssel zu finden entspricht dem mathematischen Problem (siehe Mining), welches mit Versuch und Irrtum gelöst wird.

Peer-to-Peer

Kommunikation unter Gleichen – direkte Interaktion zwischen Personen oder Unternehmen ohne einen Intermediär.

Private Key

Geheimer, persönlicher (Bestätigungs-)Code.

Proof-of-Work

Arbeit, welche von einem Dienst verlangt wird, um übermässigen Gebrauch zu verhindern.

Public Key

Öffentliche «Adresse» eines Teilnehmers.

Root Hash

Wurzel des Hash-Baums (Merkle Tree). Mit diesem können die einzelnen Zweige des Merkle Trees auf ihre Integrität überprüft werden.

Satoshi Nakamoto

Gründer von Bitcoin. Seine physische Identität ist unbekannt.

Smart Contract

Digitaler Vertrag für Transaktionen, welche mit Smart Property abgewickelt werden. Der Vertrag basiert nicht auf Vertrauen im klassischen Sinne, sondern auf Kryptographie und der Blockchain.

Smart Property

Güter welche über die Blockchain gehandelt, verwaltet und genutzt werden können.

Timestamp

Zeitstempel; damit kann ein Block einem Zeitpunkt eindeutig zugeordnet werden.

Transaktion

Unterschriebener Abschnitt von Daten einer Veränderung, welche verschlüsselt in das Netzwerk ausgestrahlt und in Blocks gesammelt wird.

Turing-vollständig

System, welches unbegrenzt, das heisst auch für sich selbst, programmierbar ist. Die Anforderungen formulierte der Mathematiker Alan Turing. Es handelt sich im Prinzip um eine Programmiersprache.

Wallet

Digitale, kryptographische Geldbörse, kontrolliert über Public Key und Private Key.

⟶ *Fortsetzung von Seite 4*

Nach diesem Ausflug in die noch recht gut vorstellbare Welt der mobilen Kommunikation nun aber zu der Blockchain. In Kapitel 1 hielten wir am Schluss fest, eine Blockchain sei nichts anderes als ein System, das kraft seiner lückenlosen Historie Beweiskraft erlangt, um Eigentumsverhältnisse zu regeln. Soviel zur Funktion der Blockchain. Aber um welches System handelt es sich, wie können wir es verstehen? Die «lückenlose Historie» wird bei der Blockchain herbeigeführt über die Aneinanderreihung von nicht veränderbaren *Richtigbefundanzeigen* [«Block»], bestehend aus vier Komponenten: der Vergangenheit (das heisst dem vorangegangenen Block); dem aktuellen Zeitstempel [«Timestamp»] zur Einordnung auf der Zeitachse; den noch nicht bestätigten, aktuellen Transaktionen, heruntergebrochen in einen kryptographischen Code [«Root Hash»]; sowie einer «Einmalnummer» [«Number used once» = «Nonce»], welche über Versuch und Irrtum gefunden werden muss [«Proof of Work»]. Dieser Prozess von Versuch und Irrtum ist der so genannte Mining-Prozess. Netzwerkteilnehmer [«Nodes»], welche aktiv an diesem Prozess mitwirken, generieren einen Mehrwert im System und werden bei erfolgreichem Abschluss entschädigt. Das System stellt sicher, dass eine neue Richtigbefundanzeige nur entstehen kann, wenn sie am *neusten Block* andockt. Deshalb das Bild einer Kette. Dass Transaktionen, das heisst Inhaltsveränderungen, durchgeführt werden können, dafür sorgt ein System von Schloss [«Public Key», gleichbedeutend mit einer Adresse] und Schlüssel [«Private Key», das heisst einer persönlichen Geheimzahl]. Über letzteren kann nur der Berechtigte verfügen. Das System der Blockchain ist deshalb extrem sicher, weil die Richtigbefundanzeigen *dezentral* – im Extremfall in jedem teilnehmenden Computer auf der Welt – abgespeichert sind. Eine beispielsweise auf einen Hacker zurückzuführende Veränderung an einem Ort würde von den millionenfach vorhandenen weiteren Teilnehmern verzugslos erkannt und überschrieben werden. Solange nicht mehr als 50 Prozent die «falsche» Version als korrekt bezeichnen, ist der Hacker chancenlos. Aber die Wahrscheinlichkeit, dass ein solcher irgendwann einmal Erfolg haben könnte, ist extrem gering, denn gegen ihn spielt die brutale *Asymmetrie* von Vergangenheit und aktueller Entwicklung neuer Blocks. Er wird immer zu spät sein. Die Eliminierung von verfälschten Blocks gleicht jener von Tumorzellen, welche täglich in jedem gesunden menschlichen Körper zerstört werden. Es gibt insofern nichts Neues unter der Sonne.

Zur Verbesserung der Vorstellbarkeit sei nebst der eingangs geschilderten Genealogie in der Lutherbibel eine andere, einer Blockchain nahekommende Analogie genannt: das Aktienbuch. Wer immer als Verwaltungsrat einer Unternehmung einmal in den Genuss kam, ein solches zu führen, weiss, dass der beste Schutz vor Fehlern – es geht immerhin um Haben oder Nichthaben von Anteilen an einer Unternehmung – darin besteht, die aufeinanderfolgenden Versionen allesamt in einem grossen Ordner aufzubewahren. Wenn Veränderungen im Aktionariat infolge Vererbung, Kauf oder Verkauf von Anteilen, Kapitalerhöhungen und dergleichen abgewickelt werden müssen, empfiehlt sich ein jederzeit nachvollziehbares Andocken an der vorherigen Aufstellung und sodann die Genehmigung der neuen Version des Aktienbuchs durch den Verwaltungsrat oder einen dazu bestimmten Ausschuss. Um – eben – mit dem Zeitstempel des Verwaltungsratsbeschlusses dem Richtigbefund Rechtskraft bis zur nächsten Änderung zu verleihen. Ein Vorgang, dem höchste Aufmerksamkeit geschenkt werden muss, denn eingeschlichene Fehler sind verheerend.

Die Grundlage des Systems der Blockchain bildet eine *Verschlüsselungstechnik* [«Hashfunktion»], bei welcher die Schwierigkeit zur Ermittlung des Zielwertes ohne viel Aufwand graduell, aber um Potenzen, verschärft werden kann. Das System läuft seinen Gegnern deshalb sozusagen hoffnungslos voraus und davon. Nochmals: Dank seiner dezentralen Aufstellung ist es zudem kaum angreifbar; letztlich kann jeder PC eines Teilnehmers am System Netzknotenfunktionen übernehmen. Ohne buchstäblichen Weltuntergang kann man sich einen Systemausfall eigentlich nicht vorstellen, jedenfalls deutlich weniger als einen Ausfall von Institutionen, die herkömmlicherweise relativ zentral den Nachweis von Eigentum sicherstellen.

KAPITEL 4

Grenzenlose Einsatzfähigkeit?

Welche Eigentumsrechte können nun 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 im Internet erscheinenden Zeitung eindeutig einer Person zuordnen. Es könnte sich aber auch um ein Geheimdokument handeln. Oder ein verbotenes Bild. Oder die Anleitung zum Bau einer Atombombe. Oder einen Liebesbrief. Oder ein Guthaben. Oder das Recht auf Speicherkapazität in einer Cloud. 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.

Nun mag man einwenden, dass zwischen dem am Bildschirm statuierten Eigentumsrecht und der den Bildschirm bedienenden Person doch noch einen Unterschied besteht. Das stimmt. Die *Schnittstelle Mensch-Maschine* ist *kritisch*. Der Schwachstelle kann bis zu einem gewissen Grade mit Identifikations-

techniken begegnet werden. So ist die Verwendung des Fingerabdrucks zur Entsperrung des Mobiltelefons bereits weitverbreitete Usanz. Darüber hinaus gibt es selbstverständlich noch viel weitergehende Methoden, um sicherzustellen, dass Unberechtigte ein schwierigeres Spiel haben. Eine letzte Sicherheit wird es aber wohl kaum geben, denn die Schwachstelle Mensch-Maschine hängt eng mit der Unvollkommenheit des Menschen selber zusammen. Er kann, beispielsweise, ab und zu auch unzurechnungsfähig sein. Oder er kann unter gewaltsamer Dritteinwirkung stehen. Im Wegfall der Institution als mögliches Korrektiv für die Schwachstelle Mensch liegt aus unserer Sicht einer der limitierenden Faktoren in der Ausbreitung der Blockchain. Darauf ist zurückzukommen.

Die zweite logische Schnittstelle, nämlich jene zwischen *Maschine und Sache*, für die eine Eigentumsregelung etabliert wird, ist in zunehmendem Masse *einfacher zu bewältigen*. Beim Verfassen dieser Zeilen schauten wir uns das Werbevideo von www.slock.it an. Es handelt sich um ein Schliesssystem für Wohnungen, das auf der Blockchain-Technologie beruht, beispielsweise geeignet, um den Zugang zu AirBnB-Wohnungen zu regeln, ohne einen physischen Schlüssel übergeben zu müssen. Der Vorteil liegt vor allem darin, dass man die Bezahlung für die Wohnung direkt mit dem «Sesam-öffne-dich» verbinden kann, ebenso selbstverständlich die Schliessung. Solche «intelligenten» Schlösser sind erst der Anfang des Siegeszugs des «Internet der Dinge», für das die Blockchain-Technologie einen entscheidenden Fortschritt bedeutet. Denn beim Internet der Dinge wird es unter vielem anderem stets um Berechtigungen und um Ein- beziehungsweise Ausschluss von Personen und Personengruppen gehen. Über die Blockchain lassen sich diese Dinge höchst effizient regeln und den laufenden Gegebenheiten anpassen.

Es ist absehbar, dass es zu einer Konvergenz zwischen dem Funktionieren von Anlagen und der Regelung von spezifischen Eigentums-(bzw. Nutzungs-)rechten kommen wird. In der neu entstehenden Fachsprache redet man von «*Smart Contracts*», intelligenten Verträgen. So ist vorstellbar, dass man das Risiko im internationalen Handel drastisch reduzieren kann, indem beispielsweise Anlagen und Maschinen dank Smart Contracts erst in Betrieb genommen werden können, wenn die Freigabe in der Blockchain eindeutig bestätigt ist, und der Betrieb auch nur so lange aufrechterhalten wird, als die im Smart Contract gesetzten *Bedingungen* erfüllt sind. In diesem Zusammenhang ergeben sich ungeahnte Möglichkeiten zur verbesserten Durchsetzung im Immaterialgüterrecht. Gerade im Bereich des Patentwesens ist ja die Schwäche des institutionellen Schutzes des Eigentums eklatant und sind die Kosten exorbitant.

Im kleinen sind wir bereits Subjekte oder Objekte von solchen Smart Contracts. Wenn wir ein Auto mieten und zu dessen Inbetriebnahme einen auf unser Smartphone gesandten Code benötigen, wenn wir als Mitglied des Verwaltungsrats einer Unternehmung uns über einen sogenannten TAN-Code (ein Einmalpasswort) Zugang zum Datenboardroom verschaffen oder wenn wir unseren Liebsten Zugang zu unserer Foto-Cloud erlauben wollen, dann bewegen wir uns in – teilweise nur temporär gewährten – Eigentumsrechten, ohne dass eine Drittinstanz, eine Institution, tätig werden muss. Die Blockchain-Technologie wird voraussichtlich ein neuer Standard für solche und weitere Selbstverständlichkeiten des modernen Alltags werden.

Grenzen sind der Technologie in Bezug auf das Verhältnis Maschine-Sache gesetzt, wo die Ausübung der Eigentumsrechte (Gebrauch, Nutzung und Verfügung) unabhängig von jeglicher Technik erfolgen kann, also beispielsweise bei der eingangs erwähnten Lutherbibel. Die Blockchain wäre an sich ideal, um künftig Ordnung im Kunstbereich zu schaffen. Alle Museen der Welt sind gegenwärtig damit beschäftigt, die Rechtmässigkeit des Eigentums an Bildern und anderen Kunstwerken aufzuarbeiten. Zwischen maschinengebundener Historie und der Sache als solcher wird es aber dennoch Identifikationsprobleme geben. Wird den Bildern ein eindeutig identifikationsfähiger RFID-Chip eingebaut werden müssen? Würde er fälschungssicher einpflanzbar sein?

Sowohl die Schwachstelle des Übergangs von Mensch zur Maschine als auch der Schnittstelle Maschine-Sache zeigt auf, dass für die Regelung von Eigentumsverhältnissen trotz allem die übergeordnete Institution wohl weiterhin eine Rolle spielen und insofern auch überleben wird. Wo Personen und Sachen nicht anders als über manifeste Macht und Anwendung letztlich gewaltsamer Mittel geschützt werden können, ist die Institution nicht wegzudenken. Das heisst allerdings nicht, dass sie nicht massiv an Bedeutung einbüssen wird.

KAPITEL 5

Blockchain-Währung als kleinster Nenner

Es mag aufgefallen sein, dass wir in unserem Text zum neuen Phänomen der Blockchain die in Mode gekommene Kryptowährung Bitcoin bisher unerwähnt gelassen haben. Dies mit gutem Grund. Denn bei Bitcoin handelt es sich nur um eine von unbeschränkt vielen Anwendungsmöglichkeiten der Blockchain-Technologie. Neben Bitcoin existieren bereits Dutzende weitere Kryptowährungen; allerdings beträgt ihr geschätzter Marktanteil im Vergleich zu Bitcoin lediglich etwa 10 Prozent. Bemerkenswert ist die Zunahme von Bitcoin-Transaktionen von weniger als 10'000 pro Tag (zu Kleinstbeträgen) im Jahr 2012 auf nunmehr weit über 150'000. Bereits wurden erste Kapitalmarkttransaktionen lanciert,

so zuletzt die Kapitalerhöhung für die Blockchain-Unternehmung Ethereum im Kanton Zug in der Höhe von immerhin 18 Millionen Dollar Gegenwert. Entgegen allen Unkenrufen und Diffamierungskampagnen sind Bitcoin und andere Kryptowährungen kaum mehr aus der Welt zu schaffen.

Trotz der dezidierten Sicht der bekannten und auch von uns respektierten Volkswirtschaftler Eugene Fama und Richard Thaler, wonach Bitcoin lediglich einen Wert hätte für «Crooks and Tax Cheats», unterzogen wir uns in den letzten Wochen einem Selbstversuch und erwarben für einen limitierten Betrag bitcoins. Die Transaktion war eher abenteuerlich, galt es doch, über eine Londoner Firma mit Hauptsitz in Kalifornien ein Bitcoin-Wallet zu eröffnen und dieser Firma bei einer estnischen Bank den Gegenwert in Euro zur Verfügung zu stellen. Geld- und Briefkurs für Bitcoins schwanken stark; von einer problemlosen Konvertibilität kann keine Rede sein. Wenn man sich dann aber einmal in der Bitcoin-Welt bewegt, dann eröffnet sich durchaus ein neues Universum mit einer erstaunlichen Zahl von Unternehmungen, die offensichtlich diese Welt gar nie verlassen. Gemäss «Tages-Anzeiger» kann man in einem Pub in Sydney, Australien, gegen Bitcoin Bier beziehen. Das wäre gegebenenfalls eine Endverwendung für die erworbene Kryptowährung. Vorderhand wollen wir uns aber noch in dieser sehr eigenen Welt umschauen und da und dort unsere unauslöschbaren, aber anonymen Blockchain-Spuren hinterlassen.

Worin liegt das Spannende an einer Kryptowährung wie Bitcoin? Ganz klar im Umstand, dass es möglich ist, Transaktionen *ohne den Umweg über Banken*, also Peer-to-Peer, zu tätigen. Wer der Bitcoin-Welt angehört, kann direkt von einem anderen Teilnehmer begünstigt werden oder andere begünstigen; die bitcoins fliessen aus dem einen Wallet in das andere. Die Transaktionskosten sind vernachlässigbar gering; für eine rasche Abwicklung (innerhalb weniger Minuten) zahlt man zwar etwas mehr als für Transaktionen mit tiefer Priorität, die allerdings auch nicht lange dauern, kostenträchtiger sind auch Transaktionen mit mehrfachen Adressaten. Dennoch: Man bewegt sich im Mikrobereich. Ist Bitcoin eine gute oder schlechte Anlage? Eine gute ganz gewiss im Sinne einer klaren Diversifikation zu den klassischen Währungen. Ob sich der Wechselkurs allerdings weiterhin so nach oben bewegt wie in den Jahren 2013 oder 2015, kann nicht gesagt werden. Seit Einstand erzielten wir selber eine Rendite von drei Prozent, immerhin etwas mehr als die Null Prozent auf dem Bankkonto abzüglich aller Gebühren … Insgesamt hat sich Bitcoin, wie fast alles Neue, bislang enorm volatil verhalten. Fazit: Nichts für risikoscheue Anleger.

Für uns 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, muss aber nicht Bitcoin sein. Der Vorteil einer solchen Kombination liegt in der fast atemberaubenden Einfachheit der Abwicklung. Während beispielsweise eine Wertschriftentransaktion nach klassischer Manier zwischen zwei oder mehreren Parteien zwingend je eine Bank, je eine Depotstelle und eine Clearingstelle erfordert sowie ein auf Vertrauen und gegenseitig ausgetauschten Sicherheiten basierendes Kreditierungssystem, kann dieselbe Transaktion in der Blockchain-Welt mit einer Blockchain-Transaktionswährung als kleinstem Nenner *Zug um Zug* abgewickelt werden. Damit solche Kombinationen tatsächlich Fuss fassen können, müssen im Internet wohl neue Standards definiert werden, auf denen dann die institutionenfreie oder -arme Welt aufgebaut werden kann.

Nicht umsonst bemühen sich derzeit alle grossen Geschäftsbanken, den Anschluss an diese neue Welt zu finden. So haben sich 42 global tätige Institute, darunter auch die Credit Suisse und die UBS, der Finanzinnovationgesellschaft R3 angeschlossen. R3 bringt nach eigenen Worten Veteranen aus dem Finanzbereich, Technologen, Kryptographen und Spezialisten für digitale Währungen zusammen, um solche institutsunabhängigen Standards zu definieren. Auch die Initiativen der London Stock Exchange Group (LSEG) lassen aufhorchen, wohl getrieben von den Anstrengungen des Chi-X Gründers Peter Randall, der mit einer neuen, Blockchain-basierten Settlement-Plattform namens SETL aufwartet. Derweil gibt Goldman Sachs bekannt, dass sie eine intern entwickelte *digitale Währung* namens SETLcoin patentieren (!) liess. SETLcoin soll, in Anlehnung an das Bitcoin-Konzept, dereinst Transaktionswährung für den Wertschriftenhandel werden. Die Schweizer Grossbank UBS nähert sich mit ihrem firmeninternen Fintech-Inkubator Level39 dem bereits erwähnten Zuger Startup Ethereum an. Ethereum ist angeblich weit fortgeschritten im Bereich der Standardisierung einer umfassend gültigen Programmiersprache für Blockchains. Hinter der Firma Ethereum steckt als «Brain» der 21-jährige Russe Vitalik Buterin, kürzlich in einem Porträt des Tages-Anzeiger Magazins beschrieben als «knabenhaftes Enigma».

Es entspricht einer Mischung aus Aufbruchstimmung und von Angst getriebener Panik, die in der Finanzbranche herrscht. Denn eines ist klar: Wie auch immer die Strukturen am Ende aussehen mögen, die Blockchain-Technologie wird sehr, sehr vieles ersatzlos überflüssig machen; die Margen werden sich verengen, neue Anbieter werden 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 Internetverbreitung von geschriebenen Inhalten: Mitmachen und mithin am eigenen Ast sägen? Oder definitiv alle Chancen verpassen? Weitere, nicht unwahrscheinliche Möglichkeit: sich geschickt mit einem Regulator verbinden, um den Übergang in die neue Welt erträglich zu gestalten.

KAPITEL 6

Dinosaurier sterben langsam und später

Das Dilemma liegt tief, denn es entspricht einer *contradictio in adiecto*, wenn sich Institutionen, wozu Banken, Börsen und Clearinghäuser zweifelsohne gehören, am Aufbau eines institutionenfreien oder -armen Systems beteiligen wollen. Es könnte ihnen ergehen wie den Carriern im Telefoniebereich, wenn dereinst anstatt die Grossantennen lediglich noch die kleinen Sender und Empfänger der millionenfach gestreuten Smartphones die Übermittlung der Gespräche besorgen. Es braucht sie nicht mehr. Sie werden sich zu Anbietern von Produkten degradieren und können ihre stolzen Filialen zu feudalen Kiosken umbauen. Systemrelevanz? Ein Phänomen der Vergangenheit, in der Welt der Blockchain axiomatisch undenkbar, weil sie ja ohne Institutionen auskommt und nur Institutionen systemrelevant sein können. Aus der Systemrelevanz bezogen die grossen Institute ihre Monopolrenten, mit denen sie den Kapitalismus verteuerten. Schnee von gestern. Aber brauchen wir uns Sorgen zu machen? Nein, denn Banken sind privatwirtschaftlich organisiert, wissen, wie man sich neu orientieren kann, gehen im schlechtesten Fall unter oder werden von anderen vereinnahmt, passen sich an, packen neue Chancen und erfreuen sich einer neuen, weit effizienteren Art des Kapitalismus. Und rund um die alten Kolosse werden neue Unternehmungen mit ungeahnten Geschäftsmöglichkeiten und -tätigkeiten entstehen.

Weit mehr Sorgen bereitet uns die Anpassung der Institution par excellence, des Staates. Er bezog bisher seine 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. Im «Economist» wurde prominent das Grundbuch angeführt. Auch wir meinen: Ja, aber vor allem dort, wo es bislang kein wirklich funktionierendes Grundbuch gab, nämlich in sämtlichen Entwicklungs- und in vielen Schwellenländern. Die Chance ist gross, dass dadurch, endlich möchte man sagen, die schwächeren Mitglieder in den Genuss kommen, Eigentum zu erwerben, und dank diesem Eigentum dann auch kreditwürdige Wirtschaftssubjekte werden – ein Traum, der vom südamerikanischen Schriftsteller Hernando de Soto schon einmal literarisch vorweggenommen worden war und der nun dank Blockchain-Technologie Wirklichkeit werden könnte. Der Wachstumsschub in diesen Gegenden der Welt wäre programmiert, vorausgesetzt, die Einführung der Grundbuch-Blockchain geht mit einer die neuen Eigentumsverhältnisse begründenden Landreform einher.

Dennoch plagen uns Sorgen. Denn mit der Unvollkommenheit der Institutionen, welche vom Staat schlecht und recht betrieben wurden und werden, stehen *Macht- und Unterdrückungsverhältnisse* im Zusammenhang, die nicht verschwinden werden, einfach so. Der Moloch wird sich gegen seinen teilweisen Untergang zur Wehr setzen. Das kann sich harmlos bis amüsant in einer querbeet praktizierten Kohlenschauflerstrategie äussern: Bekanntlich fuhr in Grossbritannien noch Jahrzehnte nach der Einführung von elektrisch betriebenen Lokomotiven ein Heizer mit, dessen Funktion zu Zeiten des Dampfbetriebs im eifrigen Schaufeln von Kohle bestand, der nun aber überflüssig geworden war. Erst Margaret Thatcher konnte sich gegen die Übermacht der Gewerkschaften durchsetzen und dem Unfug ein Ende bereiten.

Weniger harmlos und weniger amüsant dürfte die Agonie überflüssig werdender Institutionen ausfallen, wo Macht, Gewaltanwendung und mithin die dem Staat ausschliesslich zugeordneten Mittel im Spiel sind und auf dem Spiel stehen. Werden dezentral basierte Kryptowährungen dereinst die von der Institution Zentralbank etablierten und kontrollierten staatlichen Währungen ersetzen? Oder wenigstens konkurrieren? Wird man das zulassen? Unter welchem Titel und mit welchen Argumenten wird man es zu verhindern versuchen? Es geht um sehr viel, notabene. Beispielsweise um die Vorherrschaft des US Dollars im Welthandel. Andrerseits: In freien Gesellschaftsordnungen erlangt eigentlich stets die effizientere Lösung (im Sinne der Pareto-Optimalität, wo also insgesamt alle besser gestellt werden, ohne dass jemand anders dadurch benachteiligt würde) die Oberhand.

Die *Achillesferse* der Blockchain-Technologie ist in diesem Zusammenhang die Möglichkeit der durch die Verschlüsselung gegebenen totalen *Anonymität*, weil Anonymität die Zurechenbarkeit von Handlungen verunmöglicht. Im Zeitalter des unbeschränkt global einsatzfähigen Terrorismus und auch der entsprechend übergreifend global erfahrbaren Kriminalität ist Anonymität ein Killerkriterium, wie naheliegend und (wohlstands-)gewinnbringend eine Technologie auch sein mag. Die Weltgemeinschaft und die sie repräsentierenden staatlichen und überstaatlichen Instanzen müssen zwingend darauf bestehen, die von fehlerhaften, fehlgeleiteten, ver*rückten* und zu unglaublichen Schandtaten fähigen Menschen einigermassen lückenlos kontrollieren zu können. Sonst wird es auf dem Planeten Erde zu gefährlich. Den anarchistisch bis libertär verdrahteten Vordenkern der Blockchain-Technologie – es gibt deren viele – sei dies an dieser Stelle unmissverständlich ins Stammbuch geschrieben: Wenn die Blockchain ihren segensreichen, wohlstandsfördernden Siegeszug antreten soll, dann nur, wenn die totale Anonymität zugunsten einer Kontrollierbarkeit aus dem Netz verbannt wird. Das ist ein hoher Tribut, der an die

Institutionen der Macht zu zahlen ist, gewiss, aber er ist alternativlos. Die Institutionen der Macht wollen Kontrollmöglichkeiten zur Aufrechterhaltung der Sicherheit, und sie brauchen Anknüpfungspunkte zur Erhebung von Steuern. So einfach ist das.

KAPITEL 7

Ausblick

Wir wollen diese bergsicht jedoch nicht als Bedenkenträger beenden. Vielmehr gilt es am Schluss, zusammenfassend noch einmal auf die grossen Vorzüge der neuen Technologie aufmerksam zu machen und dann auch zu versuchen, einen Blick in die Zukunft zu werfen. Kommen wir zunächst zurück auf unsere Definition der Blockchain als einem System, das kraft seiner lückenlosen Historie in der Lage ist, Eigentumsverhältnisse zu regeln. Selbständig, ohne Bezugnahme auf eine mit Macht versehene Institution. Völlig dezentral und deshalb sicher. Hier gilt es, noch einmal innezuhalten. Anhand des unaufhörlichen Siegeszugs des Internets und nunmehr absehbar auch der Blockchains sind wir Zeugen eines gigantischen *Widerstreits zweier Prinzipien*, nämlich jenem des Gewinns von Stabilität durch Hierarchisierung und höchstmögliche Zentralisierung und jenem des Erstrebens von Verlässlichkeit durch denkbar disperseste Dezentralisierung.

Wenn ein Bild herhalten müsste: Es streiten sich die katholische Kirche mit ihrem angeblich von Gott eingesetzten, laut Dogmatik unfehlbaren Oberhaupt mit der Vielzahl völlig unabhängiger reformierter Gemeinden und Gemeinschaften, die von sich behaupten, dass Kirche sei, «wo zwei oder drei in meinem Namen versammelt sind». Es geht hier gewiss nicht darum, zu urteilen, was nun richtig oder falsch sei. Vielmehr stellen wir fest, dass seit und trotz der Reformation beide Prinzipien überlebt und sogar gelernt haben, miteinander zu koexistieren, wenngleich der Weg dahin ein schmerzvoller und blutiger war. Die Ursprünge des Internets (Arpanet) wurden bekanntlich vom amerikanischen Militär ersonnen, um Stabilität für Rechenfunktionen und Kommunikation zu gewährleisten, falls in einer nuklearen Auseinandersetzung mit der damaligen UdSSR grosse Teile der zentralen Infrastruktur ausfallen würden. Die Zweitschlagkapazität wäre ohne Arpanet kaum denkbar gewesen, und nur dank Zweitschlagkapazität konnte der zu einem Erstschlag kaum befähigte zivilisierte Westen den mit mutmasslich weniger Skrupel behafteten Osten davon abhalten, einen Erstschlag auszuführen. Dank der Idee des Arpanets funktionierte die Stabilität generierende Dissuasion. Die Pointe liegt darin, dass ausgerechnet im Inbegriff von *zentraler hierarchischer Machtballung*, der US-Militärmaschinerie, ein durch und durch dezentrales System gewählt wurde, um ultimative Stabilität zu erzeugen. Insofern hat also das «reformierte» Prinzip Oberhand über das «katholische» erlangt. Die in der Zwischenzeit erfolgte Ausbreitung dieses genial erdachten Netzes beziehungsweise der nicht unbedingt gewollten Nebenfolge und die bis in alle Kapillaren des Alltagslebens reichenden Auswirkungen zeugen von der Mächtigkeit einer institutionslosen oder -armen Struktur.

Die Blockchain-Technologie ist ein weiteres Glied in der langen Kette, die mit der Verbreitung von PC und Mobiltelefonie ihren Anfang nahm, uns über das Internet der Version 1.0 an weltweit verbreiteten Inhalten teilnehmen liess, mit der Version 2.0 wirtschaftliche und soziale Prozesse aufbrach und die Intermediäre in die Knie zwang sowie mit der Version 3.0 das Wesen der Institutionen im Kern angreift. Für uns steht ausser Frage, dass diese Technologie zur sozusagen alles bestimmenden Kraft in der weiteren Entwicklung des Internets, ganz generell aber eigentlich aller wirtschaftlichen, sozialen und politischen Abläufe werden wird. Zu Beginn stellten wir in Aussicht, investitionsbereitem Kapital ein paar Hinweise für zielführende Beteiligungen an diesem mit höchster Wahrscheinlichkeit extrem interessanten neuen Teil der Wirtschaft zu nennen. Das können wir selbstverständlich nicht, beziehungsweise, was wir nicht können und wollen: mit einer Liste von Investitionszielen aufwarten, die nach heutigem Wissensstand und vernünftigem Ermessen Gewinn aus der sich in den Anfängen befindlichen Technologie schlagen werden. Unsere Strategie besteht darin, nun auch unsrerseits die denkbar disperseste Dezentralisierung zu wählen, indem wir uns beinahe unbesehen einen weitgefächerten Korb von Unternehmungen zusammenstellen, die sich mit dem Thema Blockchain beschäftigen. Die Mehrzahl solcher Firmen wird voraussichtlich untergehen, dessen sind wir uns bewusst. Aber bei ein oder zwei späteren Unternehmungen, wie es einst Google oder Facebook waren, nicht wenigstens mit einer Zehenspitze dabei gewesen zu sein, würde uns schon ärgern.

Im übrigen gilt, was bei der Inbesitznahme neuer Territorien ohnehin und immer Gültigkeit haben muss: Augen auf und versuchen, die Geografie zu verstehen. Orientierungspunkte definieren. Gefahren wittern. Chancen wahrnehmen. Der neue Kontinent ist gross und weit.

KH, 25. JANUAR 2016

M1 AG
Postfach 344, Museumstr.1
9004 St.Gallen – Schweiz
Telefon +41 (0) 71 242 16 16
Telefax +41 (0) 71 242 16 17
info@m1ag.ch

Abonnieren: www.bergsicht.ch