Die Blockchain-Technologie in Zeiten zunehmender Staatseingriffe

Auch wenn viele Fachleute bereits von einer platzenden Blase sprechen, Kryptowährungen sind weiter im Vormarsch. Aber was ist eigentlich von der zugrundeliegenden Blockchain-Technologie zu halten? Wie funktioniert diese überhaupt? Welches sind ihre Stärken und Schwächen? Was dürfen wir in Zukunft von ihr erwarten? Und welche Rolle spielt diese Technologie im Verhältnis zwischen uns Bürgern und dem Staat?

VON MAGNUS PIROVINO, MANAGING DIRECTOR
OPIRO CONSULTING AG, TRIESEN

Der Begriff «alternative Fakten» wurde kürzlich zum Unwort des Jahres 2017 gewählt. Er stammt von Donald Trumps Beraterin Kellyanne Conway, die ihn benutzte, um die falsche Behauptung zu rechtfertigen, bei seinem Amtsantritt seien so viele Leute wie nie zuvor auf der Straße gewesen [1]. Nicht erst mit dem Einzug von Donald Trump ins Weiße Haus ist die Welt der Fakten ins Wanken geraten. Die sozialen Medien werden schon seit Jahren mit «Fake News» überschwemmt. Und auch millionenfach abgesicherte historische Tatsachen wie der Holocaust müssen durch die Gerichte immer wieder neu geschützt werden. (Jean-Marie Le Pen wurde vor nicht so langer Zeit zu einer Geldstrafe verurteilt, weil er die Gaskammern der Nazis wiederholt als «Detail der Geschichte» bezeichnet hatte [2].) Es ist wohl kein Zufall, dass die Blockchain-Technologie gerade jetzt, als es den mächtigsten Politikern in unseren Demokratien wieder zu gelingen scheint Medien und Fakten zu manipulieren, ihren Hype erlebt. Die Blockchain-Technologie, die von sich behauptet, historische Fakten so unwiderlegbar in einem Logbuch ablegen zu können, dass weder die mächtigsten staatlichen Autoritäten noch die kriminellsten Hackerbanden diese in Frage stellen oder sonst Einfluss auf sie nehmen können.

Viele reden von Blockchain, Bitcoin & Co., haben vielleicht sogar schon ein wenig investiert, aber niemand versteht es wirklich. «Dies spielt auch keine Rolle», höre ich mancherorts. «Wie die Transaktionen einer Kreditkarte funktionieren, weiß schließlich auch kein Mensch. Wichtig ist nur zu wissen, dass die Technologie sicher ist und von niemandem missbraucht werden kann.»

Aber wie sicher ist Blockchain wirklich? Wie bekommt man zumindest einen Eindruck davon? Der Blick auf ein paar einschlägige Internetseiten – zum Beispiel über Bitcoin – zeigt: Die Rechenleistung hat Anfang 2018 die astronomische Zahl von über zwanzig Trillionen «Hashes» (d.h. kryptografische Computerkalkulationen) pro Sekunde erreicht:

https://blockchain.info/charts/hash-rate

Die Anzahl Kopien von Logbüchern (sogenannte «Nodes») für die Transaktionshistorie von Bitcoin ist mittlerweile weltweit auf über elf Tausend gestiegen:

https://bitnodes.earn.com/dashboard/?days=730

Je größer die Anzahl Kopien dieses Logbuchs, die sich gegenseitig abgleichen, und je größer die Rechenleistung, die für eine Kryprowährung aufgewendet wird, desto sicherer ist die Technologie und desto mehr Bestätigung erhält eine Historie in der entsprechenden Kette von Transaktionsblöcken – eben der Blockchain.

Trump, Le Pen und die kriminellen Hacker zeigen: Fakten angreifen, also eine Geschichte angreifen ist einfach. Diese astronomisch anmu-

tenden Zahlen zeigen: Eine unwiderlegbare (Transaktions-)Geschichte zu konstruieren und aufrechtzuerhalten ist sehr, sehr aufwendig.

These 1: Blockchain verändert die Welt der Fakten. Sicherheit über Fakten hat ihren Preis: aufwendige (soziale) Koordination.

Wie funktioniert Blockchain?

Das Ziel einer Blockchain ist es, eine anonymisierte Transaktionshistorie so eindeutig zu bestätigen, dass alle daran interessierten Parteien dieser zustimmen. Und zwar ohne eine zentrale Autorität oder einen sonstigen «glaubwürdigen» Intermediär dazwischen (Notenbank, Geschäftsbank, Handelsplattform, etc.), der für die Rechtmäßigkeit der Transaktion bürgen müsste. Dabei kann es sich um Transaktionen in einer Kryptowährung wie Bitcoin, Ether, Ripple, etc. handeln. Aber nicht nur. Es können auch ganze Grundbücher, Urheberrechtstransaktionen, sogar die Einhaltung von Verträgen (über «Smart Contracts» [3]) mit dieser Technologie dezentral verwaltet, überwacht und abgewickelt werden.

Aber wie macht man das?

Eine Blockchain setzt dieses Ziel (der dezentralen Verifikation einer anonymisierten Transaktion, der alle zustimmen) in drei Schritten um.

In einem ersten Schritt muss eine **Basistechnologie** die Verifikation von anonymisierten Transaktionen ermöglichen. In einem zweiten Schritt muss es einen **Ausgleichsmechanismus** geben, damit Unstimmigkeiten über den historischen Verlauf der Transaktionen geklärt werden können. Und in einem dritten Schritt gewährleistet ein **Feintuning** zwischen dem ersten und zweiten Schritt – also zwischen Basistechnologie und Ausgleichsmechanismus – die stabile Synchronisierung des gesamten Blockchain-Netzwerks.

Schritt 1: Basistechnologie. Dazu wird das Prinzip der zwei digitalen Schlüssel verwendet. Eine Transaktion von A nach B wird mit einem «privaten» digitalen Schlüssel (den nur A kennt) «signiert». Diese Signatur kann dann mit einem «öffentlichen» digitalen Schlüssel, den A allen Logbüchern zur Verfügung stellt, beglaubigt werden. Diese Logbücher werden auf den sogenannten «Nodes» gespeichert, den teilnehmenden Computern des Netzwerks, die jeweils die gesamte Transaktionshistorie einer Blockchain mitführen. Wichtig ist, dass das Logbuch der Transaktionen, engl. auch «Ledger» genannt, nicht zentral bei einer «glaubwürdigen» Stelle verwahrt wird, sondern eben dezentral im Netzwerk der «Nodes». Diese dezentral verwalteten Logbücher nennt man auch «Distributed Ledger»-Netzwerk.

Die Basistechnologie liefert uns schon mal eine sehr hohe Sicherheit. Mit einem privaten Schlüssel hat jeder die (gegen außen anonyme) Hoheit über sein Eigentum und mit dem von ihm generierten öffentlichen Schlüssel gibt er jedem Teilnehmer die Möglichkeit seine Transaktion zu beglaubigen. Da jeder, der über ein Logbuch verfügt, eine Transaktion beglaubigen kann – und auch prüfen kann, ob aufgrund der vollständigen Transaktionshistorie genügend Deckung dafür vorhanden ist –, ist es für einen einzelnen bereits ziemlich schwer, wenn nicht unmöglich, eine solche zu fälschen, zu verhindern oder das System betrügerisch auszurauben.

Man kann sich das so vorstellen. Eine Transaktion von A nach B wird nur beglaubigt, wenn der Sender A über genügend Mittel (Deckung) dafür verfügt. Sein (Bitcoin-)Saldo darf nach der Transaktion nicht negativ werden. Durch das Logbuch kann das jeder nachrechnen. Aber ist diese Einschränkung immer sinnvoll? Einem Teilnehmer, der heute zwar noch über keine Mittel verfügt, aber schon weiß, dass er morgen zehn Bitcoins bekommen wird, könnte doch erlaubt werden, dass er seine heute fälligen Schulden von fünf Bitcoins schon begleicht? Morgen wären so ja alle Salden wieder positiv? Das Problem ist nur, wenn solche «vorübergehende» Negativsaldi möglich wären, wäre es für einen Betrüger aufgrund der Anonymität des Systems ein Leichtes es auszurauben. Er bräuchte nur an einen befreundeten Hehler eine Anzahl Bitcoins zu transferieren, die er vorgibt später zu bekommen, und die dieser ihm dann auf ein drittes Bitcoin-Konto, auf das er Zugriff hat, gutschreiben lässt. Wenn das System morgen von ihm verlangt, den Negativsaldo auf dem ersten Konto auszugleichen, meldet er sich einfach nicht mehr, er ist ja nur als anonyme Adresse im System vermerkt. In einer Blockchain muss also die Transaktion, die diesen Negativsaldo ausgleicht, immer schon vorher stattgefunden haben, eben um solchen Betrügereien – unter Wahrung der Anonymität – einen Riegel zu schieben. **Eine eindeutige Reihenfolge der Transaktionen ohne Negativsaldi ist also wichtig.**

Aber wie kann sich ein Netzwerk (von Logbüchern) auf eine eindeutige Reihenfolge von beglaubigten Transaktionen einigen? Es kommen ja ständig neue Transaktionen hinzu? In einem Logbuch wird zum Beispiel eine neue Transaktion T1 vor der Transaktion T2 verbucht. Ein anderes Logbuch wird erst später auf T1 aufmerksam und verbucht T2 schon vorher (immer angenommen, beide Varianten sind ohne Negativsaldi möglich). Es gibt plötzlich zwei unterschiedliche Versionen des Logbuchs im Netz. Das Ziel, den Verlauf einer Transaktionshistorie so eindeutig zu bestätigen, dass alle dieser zustimmen, wird verfehlt. Die Basistechnologie wird ineffektiv. Häufen sich solche Fälle, versinkt das System rasch im Chaos.

Wie könnte ein solches System wieder stabilisiert werden? Und zwar so, dass die Basistechnologie trotzdem unverändert weiterbenutzt werden kann? Der ineffektive Zustand (verschiedene Versionen von Logbüchern) rührt daher, dass es offensichtlich zu einfach war, das Logbuch weiterzuführen. Als Ausgleich setzt die Blockchain eine Hürde für das Eintragen neuer Transaktionen. Die Hürde heißt «hoher Rechenaufwand» oder «Mining».

Schritt 2: Ausgleichsmechanismus: «Mining». Der Ausdruck stammt vom bildlichen «Schürfen» z.B. von neuem Silberstücken in einer Mine. Nur wer den Aufwand betreibt mühselig zu schürfen, soll nach dieser Vorstellung neue Münzen ausgeben können. Bei Bitcoin ist es ähnlich: Nur wer den Rechenaufwand betreibt, ein kryptografisches Puzzle zu lösen (eine genauere Beschreibung finden Sie im APPENDIX [I]), bekommt neu herausgegebene Bitcoins und darf einen neuen Block von Transaktionen als erster beglaubigen und an das Logbuch anhängen – und bekommt zusätzlich noch die Transaktionsgebühren von allen im Block zusammengefassten Transaktionen. Dies ist bereits eine große Hürde, damit nicht zu viele verschiedene Logbuchversionen im Netz vorhanden sind. Endgültig bestätigt wird ein Block von Transaktionen aber erst, wenn alle konkurrierenden Versionen verworfen wurden. Das System

macht das so, indem immer diejenige Version mit der längsten Historie bevorzugt wird, also die, in welchem die größte Rechenleistung steckt. Wenn nun ein Bitcoin-Schürfer ein Puzzle zu einem Block von noch unbeglaubigten Transaktionen gelöst hat, hängt er ihn daher immer an das längste Logbuch an, das er im System sieht. Sieht er zwei gleichlange, aber verschiedene, wählt er nach dem Zufallsprinzip eines der beiden aus. Dadurch bestätigt er automatisch alle früheren Transaktionen des von ihm ausgewählten Logbuchs ein weiteres Mal. Das andere Logbuch ist jetzt um einen Block kürzer und dessen Transaktionen weisen eine Bestätigung weniger auf. In ihm steckt weniger Rechenleistung. Im Netz gibt es keinen Anreiz mehr dieses weiter zu berücksichtigen.

So schafft das «Mining» also den Ausgleich in der Konkurrenz zwischen verschiedenen Logbuchvarianten und klärt so Unstimmigkeiten über den historischen Verlauf der Transaktionen. Derjenige, der viel Rechenleistung einsetzt, soll bei dieser dezentral organisierten Konkurrenz auch die größten Chancen haben das Rennen zu machen.

Schritt 3: Feintuning. Was aber geschieht, wenn das Rechenspiel so populär wird, dass jeder mitmachen will? Wenn zum Beispiel plötzlich so viel Rechenleistung in das Lösen des kryptografischen Puzzles eingesetzt wird, dass in zehn Minuten nicht ein oder zwei Lösungen gefunden werden, sondern Tausende? Ist es dann im Netzwerk überhaupt noch möglich, sich genügend rasch auf eine gewinnende Lösung zu einigen? Oder umgekehrt, wenn das Puzzle so schwer wird, dass es kaum jemand mehr in nützlicher Frist schafft? Wenn Transaktionen zum Beispiel Stunden brauchen, um abgewickelt zu werden? Damit das System stabil wird, muss es also ein Feintuning vornehmen zwischen zu viel schürfen und zu wenig, zwischen zu großer Rechenleistung und zu kleiner.

Bei Bitcoin sind zwei Parameter für dieses Feintuning verantwortlich. Diese Parameter werden durch eine sogenannte Open-Source-Referenzsoftware gesteuert (Open-Source heißt: Der Code für die Software ist für jedermann frei zugänglich). Mit dem einen Parameter versucht das System sicherzustellen, dass im Schnitt nur alle zehn Minuten ein neues kryptografisches Puzzle gelöst werden kann. (Das Logbuch soll also alle zehn Minuten um einen neuen Transaktionsblock erweitert werden. Dabei ist der maximal zulässige Speicherplatz eines Blocks auf 1 Megabyte beschränkt, was gut 3'000 Transaktionen pro Block entspricht.) Dazu variiert die Referenzsoftware die Schwierigkeit des Puzzles. Wird zu viel geschürft – beteiligen sich also sehr viele Rechner am Lösen des Puzzles –, so wird die Schwierigkeit hochgeschraubt. Wird zu wenig geschürft, wird sie wieder hinabgesetzt. (Zurzeit – Anfang 2018 – wird von den «Schürfern» verlangt, dass der von ihnen generierte Schlüssel eines neuen Blocks mit 72 Nullen beginnt. Am Anfang der Bitcoin-Historie vor neun Jahren waren es nur 32 Nullen. Das Puzzle war damals also bedeutend einfacher zu lösen, vgl. auch APPENDIX [I].)

Der zweite Parameter ist die Höhe der Schürfprämie in Form neu erzeugter Bitcoins, die bei der Verbuchung eines Transaktionsblocks anfallen. Damit wird die Gesamtmenge aller sich im Umlauf befindenden Bitcoins gesteuert. Begonnen hat die Bitcoin-Blockchain am 9. Januar 2009. Die einzige Transaktion, die in Block #1 verbucht wurde, ist die Inbesitznahme der ersten Schürfprämie von fünfzig Bitcoins:

https://blockexplorer.com/blocks-date/2009-01-09

In den ersten Monaten wurden übrigens nur solche Transaktionen verbucht: Inbesitznahmen der Schürfprämie von fünfzig Bitcoins. Erst mit der Zeit fanden auch Handwechsel-Transaktionen von Bitcoins statt. Die Bitcoin-Referenzsoftware ist so eingestellt, dass sich die Schürfprämie nach der Verbuchung von 210'000 Transaktionsblocks jeweils halbiert. Da im Schnitt ein Block pro zehn Minuten erzeugt wird, bedeutet das: Halbierung der Prämie alle vier Jahre. Zurzeit ist die Schürfprämie bei 12.5 Bitcoins pro Block. Im Jahr 2021 wird sie auf 6.25 Bitcoins fallen im Jahr 2025 auf 3.125 usw. So stellt das System sicher, dass nie mehr als 21 Millionen Bitcoins im Umlauf sind.

Mit diesen beiden Feintuning-Parametern (Höhe der Schürfprämie und Schwierigkeit des kryptografischen Puzzles) versucht die Referenzsoftware also sicherzustellen, dass die dezentrale Verifikation einer eindeutigen Transaktionshistorie, der alle zustimmen, stabil im Netzwerk synchronisiert werden kann.

Der Natur abgeschaut…

Die Funktionsweise von Blockchain lässt ein Muster erkennen, das sich überall im Leben widerspiegelt. Alle Lebensprozesse – auch die kleinsten mikrobiologischen Prozesse – stabilisieren sich nach dem gleichen Schema wie die Blockchain: gemäß dem Dreischritt «Basistechnologie – Ausgleichsmechanismus – Feintuning». Nehmen Sie als Beispiel den Prozess der Synthese eines bestimmten Proteins in einer lebenden Zelle [4]. **Schritt 1: Basistechnologie.** Als Basistechnologie hat die Evolution den genetischen Code hervorgebracht, in welchem die Zusammensetzung des zu erstellenden Proteins sicher verschlüsselt, aufbewahrt und von dort ausgelesen werden kann. **Schritt 2: Ausgleichsmechanismus.** Zellprozesse – wie die Synthese eines Proteins – benötigen Energie sowie weitere Ressourcen und Ausgangstoffe als Input. Gleichzeitig fallen Abfallstoffe an, die ausgeschieden werden. Damit die Zelle immer wieder neu in die Lage versetzt wird, ihre «Basistechnologie» anzuwenden, braucht sie einen «Ausgleich» der Stoffe, einen sogenannten «Metabolismus». **Schritt 3: Feintuning.** Dieser Metabolismus muss mit den inneren Zellaktivitäten abgestimmt sein. Die zugeführten Ausgangsstoffe müssen dem entsprechen, was gerade gebraucht wird. Es muss also ein Feintuning zwischen der Aktivität der Basistechnologie (Auslesen des genetischen Codes) und dem Metabolismus geben. Der durch diesen Dreischritt stabilisierte Zellprozess ist eine durch die Evolution entstandene «emergente» Struktur. Man könnte diese Struktur auch als eine spontan entstandene «Institution der Zelle» bezeichnen. Dieser «Institution» liegt wie beim «Distributed Ledger»-Netzwerk keine zentrale Steuerungseinheit zugrunde, sondern sie entsteht wie gesagt spontan als Zusammenspiel der verschiedenen dezentralen Netzwerk-Komponenten im Zellumfeld.

These 2: Blockchain wurde «engineered» als stabile «Institution» über die Deutungshoheit einer Transaktions-Geschichte. Diese «Institution» wird von keiner zentralen Steuerungseinheit kontrolliert, sondern entsteht – wie bei allen Lebensprozessen – emergent aus dem feingetunten Zusammenspiel vieler dezentraler Komponenten.

Die Achillesfersen

Eine Blockchain bietet eine geniale Alternative zu den herkömmlichen zentralisierten Institutionen, die über Fakten entscheiden. Die Vorteile liegen auf der Hand. Das System ist dezentral mehrfach abgesichert, es kommt ohne teuren (und unter Umständen korrupten) zentralen Akteur aus und es garantiert maximal die Privatsphäre aller Teilnehmer.

Hat dieses System aber auch Schwächen?

Wie jedes lebendige System ist natürlich auch eine Blockchain von allerlei Gefahren von außen bedroht. Versuchen wir ihre Achillesfersen entlang unseres Dreischritts «Basistechnologie – Ausgleichsmechanismus – Feintuning» zu identifizieren.

Achillesfersen der Basistechnologie. Die Verschlüsselungstechnik ist mittlerweile so ausgereift, dass hier kaum noch Gefahr droht. Diese Stärke der Technologie offenbart aber gerade auch eine ihre Schwächen. Wenn Millionen von Transaktionen sicher, aber anonym an den staatlichen Autoritäten vorbei abgewickelt werden können, hat das auch seine Schattenseiten. Das System kann für kriminelle Transaktionen missbraucht werden. Die Staaten reagieren durch Verbote oder strenge Regeln (wie kürzlich in China und Südkorea [5]) was die Zukunft der Technologie unberechenbar macht.

Eine weitere Herausforderung der Basistechnologie ist die sichere Aufbewahrung der digitalen Schlüssel. Die Hoheit über mein Eigentum habe ich bei Blockchain nur über meine Schlüssel. Kommt ein Hacker in deren Besitz, kann er mich ausrauben. Die Blockchain selbst mag gegen Hacker abgesichert sein, ich selbst bin es zum Vornherein nicht.

Achillesfersen des Ausgleichsmechanismus. Auch die Blockchain selbst könnte angegriffen werden. Dann nämlich, wenn mehr als die Hälfte der gesamten Schürfrechenleistung, resp. der «Nodes» von einem einzelnen Akteur kontrolliert wird. Ein solcher könnte dann leicht die Deutungshoheit über die Transaktionshistorie an sich reißen. Der faire und dezentral organisierte Ausgleichmechanismus zur Bestimmung einer eindeutigen Transaktionshistorie wäre massiv gestört. Schon jetzt kontrollieren einige wenige «Mining Pools» einen großen Teil des Schürfkuchens. Bei Bitcoin ist zum Beispiel der in Peking ansässige «Antpool» allein für fast fünfzehn Prozent der Rechenleistung verantwortlich:

https://blockchain.info/de/pools

Das mag jetzt noch kein Problem darstellen. Aber es zeigt die Gefahr auf, dass auch hier – wie überall in der Wirtschaft – schädliche Konglomerate und Kartelle (korrupte staatliche Gruppen miteingeschlossen) entstehen und großen Schaden anrichten können.

Achillesfersen des Feintunings. Lanciert wird eine Blockchain durch die Veröffentlichung einer Open-Source-Referenzsoftware. Bei Bitcoin geschah das wie gesagt 2009. Die Feintuning-Parameter – Höhe und Anpassung der Schürfprämie, Anpassung der Schwierigkeit des kryptografischen Puzzles, aber auch andere Parameter wie die maximal zulässige Größe eines Transaktionsblocks – wurden in dieser Software festgelegt. Ein Problem dieser Festlegung besteht darin, dass sie nachträglich nur mehr sehr schwer verändert werden kann. Die aktiven «Nodes» müssten mehrheitlich einer solchen Veränderung zustimmen. Treten nun unvorhergesehene «Umweltschwankungen» auf, die mit dem bestehenden Finetuning nicht mehr stabilisiert werden können, müsste auch das Finetuning in der Referenzsoftware darauf neu ausgerichtet werden. Auf «Unvorhergesehenes» kann die Referenzsoftware aber per definitionem nicht programmiert sein.

Ein Beispiel: Ab Mitte letzten Jahres ist die durchschnittliche Transaktionsgebühr bei Bitcoin von umgerechnet wenigen Cents auf weit über dreißig US Dollar pro Transaktion gestiegen. Wer also Bitcoins im Wert von z.B. zwanzig US Dollar transferieren wollte, musste zusätzlich nochmals mehr an Gebühren bezahlen, als er eigentlich transferieren wollte:

https://bitcoinfees.info/

Was ist passiert? Bitcoin wurde so beliebt, dass bedeutend mehr als 3'000 Transaktionen pro zehn Minuten in der Warteschlange ihrer möglichst raschen Abwicklung harrten. Die in der Referenzsoftware festgelegte Maximalgröße von 1 Megabyte pro Block erlaubt aber keine größere Zahl abgewickelter Transaktionen. Da jeder «Schürfer» frei ist, welche Transaktionen er in einen Block packen möchte, nimmt er gerne diejenigen, an welchen er am meisten verdient: die mit höheren Transaktionsgebühren. Die erhöhte Nachfrage trieb also die Gebühren in die Höhe und die Abwicklungszeit in die Länge. Um dieser Situation Herr zu werden, hätte das Finetuning angepasst werden müssen: entweder die Schwierigkeit des kryptografischen Puzzles herabsetzen, damit mehr als ein Transaktionsblock pro zehn Minuten abgewickelt werden kann oder die maximal zulässige Größe eines Transaktionsblocks erhöhen. Dies hätte aber eine Anpassung der Referenzsoftware erfordert. Eine solche ist allerdings bei der großen Zahl von «Nodes», die zustimmen müssten, schier unmöglich. Gebühren und die Abwicklungszeit sind ein nach wie vor ungelöstes Problem von Bitcoin. Computer-Freaks und Blockchain-Fans arbeiten natürlich an Lösungen für dieses Feintuning-Problem. Mit ungewissen Ausgang über deren langfristigen Auswirkungen. (Ein Lösungsansatz ist zum Beispiel die Kreierung einer neuen Kryptowährung vermittels einer sogenannten «Hard Fork». Eine für viele Leute unerwünschte Nebenwirkung einer solchen «Hard Fork» ist die Verdoppelung der Krypto-Geldmenge. Eine Beschreibung finden Sie in APPENDIX [II].)

Fassen wir die Gedanken um die Achillesfersen von Blockchain kurz zusammen.

- Basistechnologie: Sichere Anonymität begünstigt kriminellen Missbrauch. Staaten reagieren mit Verboten und Regulierung. Sichere Verwahrung der digitalen Schlüssel ist nicht zum Vornherein gewährleistet.

- Ausgleichsmechanismus: Bei den «Mining-Pools» und den «Nodes» könnten schädliche und korrupte Monopole entstehen mit dem Ziel eine Blockchain zu ihren Gunsten zu manipulieren.

- Finetuning: Die Stabilisierungsparameter einer Blockchain werden in ihrer «DNA», der Referenzsoftware festgelegt. Wie die Referenzsoftware auf «unvorhergesehene» Umweltschwankungen auf «vorhersehbare» Weise angepasst werden kann, ist (und bleibt wahrscheinlich) eine offene Frage.

In unserer komplexen Welt gibt es immer wieder Umweltschwankungen, die ein lebendes System destabilisieren können, also auch eine Blockchain. Die eigentliche Achillesferse der Blockchain-Technologie ist der Glaube, ihre Stabilität ließe sich durch «Engineering» garantieren. Blockchain wird dann langfristig überleben können, wenn wir für sie einen vernünftigen Rahmen finden, wie sie ihre «DNA» (die Referenzsoftware) an veränderte Umweltbedingungen anpassen kann. Eine solche Koordination können Computer nicht autonom vornehmen. Sie muss durch die beteiligten Menschen dahinter gesteuert werden. Entscheidungen von größeren Gruppen von Menschen tangieren aber immer auch die Interessen von Staaten (z.B. bei kriminellem Missbrauch, Terrorbekämpfung, etc., aber auch bei anderen Fragen der staatlichen Souveränität). Langfristig wird es keine Blockchain ohne den Staat geben.

These 3: Ohne staatlichen Segen wird die Blockchain-Technologie im legalen Raum nicht überleben.

Ist Blockchain gekommen um zu bleiben?

Im ökonomischen und politischen Umfeld ist seit Jahren ein klarer Trend ersichtlich – der Trend zu mehr Staatseingriffen. Die Aktivitäten der Notenbanken, die zunehmende Regulierungsneigung der Behörden – auch zwischen den Staaten – sprechen eine deutliche Sprache. (Daran werden auch Präsident Trumps Liberalisierungsbemühungen nichts ändern. Seine Steuerreform zum Beispiel wird durch ein höheres Budgetdefizit finanziert. Die Staatsquote wird also nicht verringert, sondern eher noch ausgeweitet.) Man kann diese Entwicklungen bedenklich finden oder auch nicht. Ich ziehe den Versuch vor, mich mit Dingen zu arrangieren, die ich sowieso nicht ändern kann. Das heißt zum Beispiel zu fragen: Wo liegen denn die positiven Gestaltungspotenziale eines Trends zu mehr Staatseingriffen? Und wie können deren negativen Auswirkungen im Zaun gehalten werden? Die Blockchain-Technologie kommt im Prinzip ohne den Staat aus. Sie ist ein Gegenentwurf zu jeder zentralen Autorität, die sich alleine anmaßt, über gewisse Fakten zu entscheiden. Sie ist ein probates Mittel um die Macht eines Einzelnen, eines zentralen Akteurs, zu beschränken. So gesehen ist sie urdemokratisch. (Die Demokratie als Staatsform wird ja von vielen als nichts anderes als ein Mittel zu Beschränkung der Mächtigen angesehen.) Gerade hier liegt auch ihr größtes politisches Potenzial. Der Trend zu mehr Staatseingriffen fällt in eine Zeit, in der es den Mächtigen der Welt es immer besser gelingt, die Deutungshoheit über Fakten an sich zu reißen. In Zeiten von «Fake News» und «alternativen Fakten» – im «postfaktischen Zeitalter» – kann die Blockchain-Technologie einen positiven Beitrag zur Stärkung unserer Demokratien leisten. Dies setzt aber eine konstruktive Zusammenarbeit mit den staatlichen Autoritäten voraus. Im Wissen um ihre eigenen Achillesfersen (krimineller Missbrauch, monopolisierte «Mining Pools», Instabilität bei unerwarteten Umweltschwankungen) wird dies das Vertrauen in die Technologie weiter erhöhen. Er wird eine turbulente Lernphase geben. Aber dann wird Blockchain gekommen sein um zu bleiben.

Szenario 1: Blockchain arbeitet konstruktiv mit den staatlichen Autoritäten zusammen und kann so zu einer Schlüsseltechnologie im Ausgleich zwischen staatlichen und privaten Interessen werden.

Falls die Blockchain-Community aber – was ich nicht glaube – zu einer libertären Antiautoritätsbewegung verkommen sollte, dann wird die Technologie rasch in den illegalen Darkpools des Internets versinken.

Szenario 2: Blockchain versinkt in der Illegalität.

Anlagekonklusion

Wer Kryptowährungen als Anlageobjekte benutzt, muss wohl oder übel mit einer hohen Volatilität umgehen können. Kryptowährungen könnten sich als die ersten geplatzen Blasen dieses langen Bullmarkts erweisen. Was niemand vom vorsichtigen, langfristigen Investieren abhalten muss. Da sie eine völlig neue Techologie darstellen, wirken sie als Beimischung auf jeden Fall diversifizierend. Blockchain steht erst am Anfang ihrer Entwicklung. Sie ist Teil der Automatisierungswelle, die jetzt ihrem ersten euphorischen Höhepunkt zustrebt. Vieles bleibt dabei ungewiss. Gewiss scheint nur, dass ihr Erfolg von einer fruchtbaren Zusammenarbeit mit dem Staat abhängen wird. Blockchain zeigt eindrücklich auf wie aufwendig es ist, (historische) Fakten zu erzeugen und sie als solche aufrechtzuerhalten. Im Zeitalter von «Fake News» und «alternativen Fakten» bietet sie Chancen und Risiken nicht nur für Anwender, sondern auch für die Demokratie als Ganzes. Seien wir Optimisten, erwarten wir das Beste, nämlich dass die Demokratie gestärkt aus all diesen Entwicklungen hervorgehen wird.

APPENDIX

[I] Unter dem **kryptografischen Puzzle** kann man sich Folgendes vorstellen: Eine sogenannte «Hash-Function» – das ist ein bestimmtes Computerprogramm, das für alle Teilnehmer im Netz zugänglich ist und sehr leicht ausgewertet werden kann – verschlüsselt eine Liste von Transaktionen, die vorher um eine gewisse Puzzlezahl verlängert worden ist. Als Schlüssel resultiert eine 256 Stellen lange Zahlenfolge aus Nullen und Einsen. Für alle Teilnehmer ist es sehr einfach nachzurechnen, dass die «Hash-Function» aus der Puzzlezahl und den Transaktionen den entsprechenden Schlüssel erzeugt. Das Umgekehrte ist aber nahezu unmöglich: Aus dem Schlüssel kann nicht auf den Input – also zurück auf die Puzzlezahl und die Transaktionen – geschlossen werden, da der Schüssel immer wie eine zufällige Folge aus Nullen und Einsen aussieht, die sich stark verändert, wenn im Input auch nur ein Bit verändert wurde. Das kryptografische Rätsel für einen «Schürfer» besteht nun darin, eine Puzzlezahl so zu finden, dass der Schlüssel mit einer vorgegebenen Anzahl Nullen (z.B. mit 32 Nullen) beginnt. Weil man aus dem Schlüssel nie auf den Input schließen kann, ist das Beste, was der Schürfer machen kann, der Reihe nach viele Puzzlezahlvarianten (Puzzlezahl = 0, 1, 2, …) auszuprobieren. Sobald er eine Zahl findet, die passt – deren «Hash-Function» also einen Schlüssel ergibt, der mit den geforderten 32 Nullen beginnt –, ist das Puzzle gelöst. Die Lösung ist für alle anderen zugänglich und leicht überprüfbar. Damit hat er bewiesen, dass er den geforderten Rechenaufwand betrieben hat, und ist somit berechtigt, den entsprechenden Transaktionsblock zusammen mit seiner Puzzlezahl an die Blockchain anzuhängen – und hat damit als erster seinen Besitzanspruch auf die neu geschürften Bitcoins inklusive aller dabei anfallenden Transaktionsgebühren rechtmäßig bestätigt.

[II] **Kreierung einer neuen Kryptowährung vermittels «Hard Fork».** Ab einem bestimmten Zeitpunkt wird die neue Währung durch Verdoppelung der Blockchain-Historie aus der alten erzeugt. Für zukünftige Transaktionen in der neuen Währung wird eine neue Referenzsoftware mit neuen (Feintuning-)Parametern benutzt. Bitcoin Cash ist ein Beispiel einer solchen «Hard Fork». Sie ist durch Abspaltung aus Bitcoin am 1. August 2017 entstanden. Bitcoin Cash erlaubt achtmal größere Transaktionsblöcke als Bitcoin. Vor der Abspaltung sind die Transaktionshistorien von Bitcoin und Bitcoin Cash identisch. Nach der Abspaltung entwickeln sie sich völlig unabhängig. Ein wichtiger Nebeneffekt einer solchen «Hard Fork»-Lösung ist die Verdopplung der «Geldmenge». Im gerade besprochenen Fall können also neu maximal 21 Millionen Bitcoins plus 21 Millionen Bitcoins Cash im Umlauf sein.

---

[1] https://www.nbcnews.com/meet-the-press/video/conway-press-secretary-gave-alternative-facts-860142147643

[2] https://humanite.fr/detail-de-lhistoire-jean-marie-le-pen-nouveau-condamne-604001

[3] Roger Wattenhofer: Distributed Ledger Technology. The Science of the Blockchain. Inverted Forest Publishing. 2017.

[4] Besten Dank meinem Freund und Genetiker Dr. Bernard Conrad für die in vielen wertvollen Gesprächen entstandenen Einsichten über einige grundlegende Zusammenhänge der Mikrobiologie.

[5] https://www.nzz.ch/finanzen/suedkorea-plant-verbot-des-handels-von-kryptowaehrungen-ld.1346410

IMPRESSUM
AUSGABE: März 2018
HERAUSGEBER: OPIRO Consulting AG, Landstraße 40, FL-9495 Triesen
REDAKTION: Magnus und Lea Pirovino
GESTALTUNG: agentur mehrwert, Zelgweg 34, CH-5405 Baden
FOTO: Magnus Pirovino, Bündner Herrschaft mit Falknis