Bitcoin & Co.

Blockchain: Mining – wie Gold geschürft wird (Teil 2)

Im Teil 1 zeigten die Autoren aus ihrer Sicht die großen Vorzüge der innovativen Blockchain-Technologie auf und gingen auch auf Schwachstellen ein. Nach dem ersten großen Massenansturm auf den Bitcoin, mussten alle daran Beteiligten kräftig nachrüsten, um für eine neue, nachhaltigere Nachfrage und das Mining hoffentlich gut gewappnet zu sein. Jetzt wird es spannend für denjenigen, der sich konkret für Antworten auf folgende Fragen interessiert:

Quelle: A. Purwin

❷ **Symbolischer ep-Bitcoin**

Wie kann man Gold schürfen, wie ist nun der Ablauf dafür, was passiert bei einer Transaktion und wer spielt mit?

Procedere über Bitcoin-Blockchain-Netzwerk

Auf dem Handelsplatz bitcoin.de kaufe ich (A) von einer anderen Privatperson (B) z. B. 0,2 BTC und zahle der Person dafür echte Euro. Person B will also die 0,2 Bitcoins an mein Account beim online-Händler transferieren. Dieser Vorgang läuft über das Bitcoin-Blockchain-Netzwerk. Das Netzwerk kann man sich auf drei Ebenen vorstellen:

- normale Nutzer
- Knotenrechner (Node)
- Miner.

Knotenrechner – Verwalter der Blockchain

Die Knotenrechner sind weltweit verteilt, es gibt davon viele tausend. Diese sind untereinander vernetzt und bilden ein sogenanntes **Peer-to-Peer-Netzwerk** – ermöglichen sozusagen eine ständige „Telefonkonferenz". Solche Peer-to-Peer-Netzwerke sind kaum angreifbar. Auf jedem Knotenrechner liegt in der Regel die komplette Blockchain-Datenbank, die mittlerweile etwa 200 GByte beim Bitcoin BTC groß ist. Jeder könnte solch einen Knotenrechner betreiben, um das Netzwerk zu unterstützen – eine Art freiwillige Ehrenamtsleistung. Dafür eigenen sich beispielsweise Windows-Mini-PCs oder auch energiesparende Raspberry-Lösungen.
Diese Nodes sind die eigentlichen Verwalter der Blockchain. Sie fischen sich die Transaktionen aus dem Netz, prüfen den öffentlichen Schlüssel vom Empfänger, den Betrag und die digitale Signatur des Absenders, die beweist, dass dieser auch über ausreichendes Bitcoin-Guthaben verfügt. Außerdem verwalten sie die gültigen Blöcke, die von den Minern generiert werden.

Autor
Dipl.-Ing. (FH) Hannes Leidenroth, LeiTech GbR, Sandkrug, unterstützt von Co-Autor Dipl.-Ing. (FH) Thomas Imhoff.

Miner, die Goldschürfer

Damit kommt man zu den Minern, den „Gold-Schürfern". Satoshi Nakamonto wusste, dass Gold nur durch schwere Arbeit ans Tageslicht auf die Welt kommt. Daher hat er den Minern ebenfalls eine schwere, aber relativ stumpfsinnige Rechenarbeit aufgebürdet, die einem Würfelspiel ähnelt: Das Ermitteln von sogenannten Hash-Werten für einen neuen Block – ein Block verbrieft bis zu ca. 1 000 Transaktionen und ist etwa 1 MByte groß.
Alle 10 min wird ein neuer Block erzeugt und auf ewig an die vorhandene Blockchain angehängt. Aber nur derjenige Miner, der das Würfelspiel gewonnen hat – das beansprucht etwa 10 min –, hat das Recht, diesen neuen Block an die Kette anzuhängen. Dafür erhält er als Belohnung momentan 12,5 Bitcoins gutgeschrieben. Allerdings halbiert sich die Belohnung alle 4 Jahre, zum Beispiel wieder im Jahr 2020.
So kommen neue Bitcoins auf die Welt, aber mehr als 21 Millionen BTCs kann es absolut nicht geben – sprich: mehr Gold lässt sich nicht aus der Erde holen – eine wichtige Beschränkung für (Geld)werte. Das wird etwa im Jahre 2140 der Fall sein.
Man könnte jetzt einwenden, dass 21 Millionen BTCs ja nicht besonders viel ist. Aber die Sache ist etwas anders gelagert. Die Auflösung eines Bitcoins ist sehr hoch, also die Teilbarkeit: 0,00000001 Bitcoin wäre die kleinste Einheit, die den Namen „1 Satoshi" trägt. Beim Dollar wären es nur zwei Stellen hinter dem Komma (Cent). Daher ist der Bitcoin wesentlich feiner teilbar als die Beträge aller jemals gedruckten Dollarnoten oder geprägten Münzen, die im Umlauf sind.

Momentan sind von den 21 Millionen BTCs bereits 17 Millionen geschürft. Wenn die Miner keine Coins mehr schürfen können, müssen sie von Transaktionsgebühren leben, die auch jetzt schon berechnet werden.
Ursprünglich konnte jeder Knoten auch Miner spielen, aber das Wettrüsten mit Rechenleistung nahm schnell seinen Lauf. Mittlerweile haben sich riesige sogenannte Miningfarmen gebildet, die sich in kälteren Regionen ansiedeln, wo elektrische Energie günstig zur Verfügung steht, z. B. Kanada und Island.
Mit dieser Konzentration der Miner hat Satoshi wohl kaum gerechnet, denn er hatte ursprünglich auf volle Dezentralität gesetzt – die Konzentration von relativ wenigen Mining-Unternehmen kann Nachteile mit sich bringen. Diese Farmen sind endlose Hallen, deren Regale mit speziellen Hash-Rechnern bestückt sind. Sie machen alle nichts anderes als „Würfeln". Auf den Sinn dieser Aktion wird im Folgenden eingegangen.

Ausflug in die Informatik

Miner: Hash mich

Diese Ausführungen wenden sich nur an besonders Interessierte, die vor allem den hohen Energiebedarf der Miner kritisieren und daher Hintergrundinformationen nötig haben. Reine Anwender müssen das nicht zwingend wissen. Dennoch ist dieser Ausflug in die Informatik für den Autor unverzichtbar.
Konkurrierende Miner müssen gleichzeitig eine Art Würfelspielrätsel absolvieren und gewinnen, um einen neuen Block an die Blockchain anhängen zu dürfen und die Belohnung (Reward) zu kassieren. Dabei sind zwei Dinge unterscheiden:
Das Würfelrätsel zu knacken mit PoW, der Proof-of-Work-Methode, ist extrem schwierig und verlangt einen hohen Rechenaufwand.

Beispiel

Hash-Wert ermitteln

Man stelle sich folgendes vor: Eine Schulklasse besteht aus 30 Kindern. Jedes von ihnen ist ein Miner und erhält einen Würfel. Die Ziffer 6 gibt es darauf nicht, dafür aber die „0“. Die Aufgabe lautete nun: Wer es schafft, zehnmal in Folge die Null zu würfeln, darf sich melden. Derjenige hat gewonnen und muss dann nur noch zeigen und beweisen, wie er das gemacht hat. Er hat den einen gültigen Hash-Wert für den Datenblock gefunden. Wieviel Nullen in Folge jeweils verlangt werden, bestimmt der Algorithmus (Schwierigkeitsgrad, difficulty). Das ist also ein dynamischer Prozess, sodass die Rätsellösung immer ungefähr 10 min beansprucht. Der Schwierigkeitsgrad steigert sich praktisch kontinuierlich. Rüsten manche Miner ihre Hardware massiv auf, um schneller als die Konkurrenz zu sein, und lösen die Aufgaben dadurch schneller, werden alle zukünftig mit schwereren Aufgaben konfrontiert (noch mehr führende Nullen), sodass erneut ca. 10 min Lösungszeit entstehen.

Wenn dann aber ein Miner ruft: „Ich habe die Lösung als erster gefunden“ und diese Lösung samt neuem Block allen Knoten mitteilt, können diese Knoten sofort mit minimalem Aufwand feststellen, dass die Lösung des Rätsels richtig ist. Nur darum geht es (Beispiel).
Ist es umgekehrt und geben Miner auf, weil ihnen das Mining zu teuer wird (Energiekosten), wird die durchschnittliche Rätsellösungszeit zunächst ansteigen. Der Algorithmus wird dann bald weniger Nullen verlangen, um wieder die 10 min anzustreben (Bild 5). Das Bild zeigt die berechneten Hash-Werte der letzten neuen Blöcke vom 18.06.2018.
Von einem Datenblock – egal wie groß – ermittelt der SHA256-Verschlüsselungs-Algorithmus einen Hash-Wert mit immer derselben Zeichenzahl. Würde man in dem Datenblock nur eine Winzigkeit am Inhalt ändern (zum Vergleich: ein Buchstabe im Word-Dokument), käme ein komplett anderer Hash dabei heraus.

Kein Rückschluss auf Inhalte

Und ganz wichtig: Es kann niemals ein Rückschluss vom Hash-Wert auf den Inhalt des zugehörigen Datenblocks gezogen werden. Diese Verfahren wenden beispielsweise auch viele Online-Anbieter an. Aus Benutzername und Passwort wird bei der Registrierung ein Hash erzeugt und nur dieser lagert z. B. beim „Elektropraktiker“. Meldet man sich an, werden nur die Hash-Werte verglichen. Sollte ein Hacker beim ep diese Hash-Werte stehlen, kann er nichts damit anfangen. Ein Rückschluss auf die tatsächlichen Login-Daten ist nicht möglich.

Probe aufs Exempel

Um das auszuprobieren, geht man auf blockchain-basics.com, wählt „Zusatzmaterial und Hash-Funktionen“ und gibt ein: **Elektropraktiker1** und erzeugt den SHA256-Hash. Dabei ist nur auf „SHA256“ zu achten (Bild 6). Sind die dort führenden Nullen zu sehen? Nein, leider Pech gehabt, daher ist neu zu würfeln und **Elektropraktiker2** auszuprobieren – immer noch keine führende Null? Dann geht es so weiter – vgl. Bild 6: Hash-Generator zum Ausprobieren (SHA256).
Auf derselben Seite gibt es auch die Funktion „hash-puzzle“. Damit geht es schneller. Folgendes ist einzugeben:

- Data: Elektropraktiker
- Nonce: 1 – das ist die einzige veränderbare Variable
- Ganz unten „führende Nullen“: z. B. gewünscht „2“.
- Anwenden: der Hash (hier: verkürzte Version) mit zwei führenden Nullen wird berechnet.

Bei Nonce lässt sich dann die Zahl der nötigen Würfelversuche, die im Hintergrund abliefen, ablesen: 145 – und das bei nur 2 verlangten führenden Nullen.

Energieverbrauch: IT-Sicherheit fordert Tribut

Ist bekannt, wie oft Bitcoin-Hash-Werte pro Sekunde berechnet werden, wie oft pro Sekunde gewürfelt wird? Das sind 56 Trillionen Mal, 56-mal „10 hoch 18“.
Warum dieser „Wahnsinn“, der tatsächlich einen sehr hohen Energieverbrauch zur Folge hat? Manche Medien titeln nur „Bitcoinschürfen“ verbraucht so viel Strom wie Österreich oder so ähnlich. Es wird aber nie geschrieben, warum das so ist.
Die Antwort lautet: Der hohe Energieverbrauch ist eine direkte Folge der Forderung, die Blockchain extrem sicher vor Angriffen zu machen. Dieses PoW-Verfahren, sprich – diese extreme IT-Sicherheit – gibt es eben nicht zum Nulltarif. Das ist das Hauptargument, das den Verbrauch rechtfertigt. Der Autor wünschte sich, dass dieses hohe Maß an IT-Sicherheit bei den Energieversorgungsunternehmen und der Regierung vorliegen würde.
Und man könnte noch weiterdenken: Die Kryptowelt benötigt keine Banken, deren weltweiter Energieverbrauch mehr als dreimal so groß ist (etwa 100 TWh im Jahr 2017, Quelle: cointelegraph.com). Hinzu kommt noch der Energieverbrauch der Angestellten, um zum Arbeitsplatz zu kommen.

Quelle: H. Leidenroth

5 **Hash-Werte von neuen Blöcken**

Früher konnte man mit dem normalen PC selbst Mining betreiben. Dann kam der Run auf die Grafikkarten, die das Hash-Rechnen wesentlich besser beherrschten. Zeitweise gab es daher am Markt keine Grafikkarten mehr. Dann wurden spezielle Chips (ASICs) entwickelt, die noch mehr Rechenleistung aufweisen, aber sparsamer sind – z. B. das Mining-Gerät AntMiner 9 mit dem Chip von Bitmain (China, Marktanteil 75 % aller mining-ASICs).

Möglicher Schwachpunkt des Systems

Angeblich soll Bitmain auch die beiden größten Mining-Pools kontrollieren: BTC.com und Antpool – zusammen demnach etwa 40 % Miningpower. Somit steigt die Gefahr einer 51 %-Attacke auf die Blockchain.
Das ist nach Meinung des Autors momentan die größte Schwachstelle im System, zumal eine Attacke auch mit weniger als 51 % Mininganteil möglich ist – nur, dass die Erfolgswahrscheinlichkeit dann kleiner wäre.
Wer das Mining beherrscht, kann neue Blöcke an die Chain hängen. Er könnte auch ältere Blöcke manipulieren. Allerdings geht man davon aus, dass rückwirkend maximal 6 Blöcke manipuliert werden könnten, was etwa 1 h verstrichener Zeit in die Vergangenheit entspricht. Für alles andere wäre der dann erforderliche Rechenaufwand nicht mehr finanzierbar oder würde zu lange dauern.
Aber dieser Vertrauensverlust könnte wahrscheinlich der Todesstoß der Blockchain-Welt sein. Allerdings würde solch eine Aktion auch die Geschäftsgrundlage der Miner selbst zerstören, inklusive der teuren Infrastruktur, was auch keinen Sinn ergibt.

Schwachstellen – kritisch beleuchtet

Dieser Beitrag soll jedoch auch die negativen Punkte offen nennen, damit sich jeder ein eigenes Urteil bilden kann.
Der chinesische Bitmain-Chip bekommt jetzt ernsthafte Konkurrenz aus Japan. Das ist also ggf. eine sehr gute Nachricht – bezogen auf verbesserte Mining-Dezentralisierung: Der Hersteller GMO bringt das Mining-Gerät G2 heraus. Dessen Chip basiert auf einer 7-nm-Technologie, die den Energiebedarf nochmals um etwa Faktor 4 reduziert.
Der signifikante Energieverbrauch der Miner-Leistung mindestens ab etwa 3,5 GW aufwärts (beim AntMiner 9, Quelle: Christoph Bergmann www.bitcoinblog.de, tägliche Pflichtlektüre) – ist selbstverständlich vielen ein Dorn im Auge – auch wenn der Grund dafür bekannt ist.
Daher gibt es große Anstrengungen, energiesparendere Lösungen zu finden. Miner verlagern ihre Farmen z. B. nach Kanada/Quebec, Island oder Norwegen, denn Mining lohnt sich nur dort, wo ein Überangebot an Strom besteht. Quebec hat beispielsweise einen der weltweit höchsten Anteile an günstiger Wasserkraftenergie.
Daneben gibt es Kryptowährungen, die ein anderes Verfahren, z. B. „Proof-of-Stake" verwenden, bei dem eine bestimmte Zahl von Minern, z. B. per Losverfahren, die Erlaubnis zur Schaffung eines neuen Blocks erhält.
Aber das ist nicht im Sinne des Erfinders S. Nakamoto, der keine „privilegierten Miner" haben wollte, da niemand in eine gewisse Machtposition gelangen darf.
Alles soll dezentral ohne Bevorzugung ablaufen.
Alternative Verfahren sind weniger sicher als Proof of Work (PoW) und schon im Monat Mai d. J. wurden solche Blockchains gehackt, wie z. B. „Bitcoin-Gold" oder der Krypto Verge XVG. Auch ein weiteres Konsortium verfolgt energiesparende Entwicklungen, die der Zentralisierung von Minern entgegenwirken soll.

Quelle: H. Leidenroth

6 **Hash-Generator zum Ausprobieren (SHA256)**

Projekt Hyperledger

Die Linux Foundation gründete im Jahr 2015 das Projekt Hyperledger, an dem sich u. a. 100 Firmen beteiligen, wie vor allem:

- SAP
- IBM („Hyperledger Fabric Blockchain")
- Airbus
- Daimler
- Nokia
- Deutsche Börse.

Überraschen diese Namen? Die Industrie hat erkannt: Blockchain-Lösungen gehört die Zukunft. Dort wird weltweit schon geklotzt, man wartet nicht auf Politik, sondern eher auf eine maßvolle und vernünftige Regulierung, auf die später noch einzugehen ist.
Am Ende dieses kleinen Hash-Exkurses soll noch auf eines hingewiesen werden: Änderungen an der Software der Blockchain sind prinzipiell schwierig, weil es immer eine „Operation am offenen Herzen" darstellt, denn das System ist ständig online und in Verwendung. Das stellt bei einem Softwareprodukt natürlich einen gewissen Nachteil dar.
Aber der Beitrag soll ja gerade auch die Nachteile nicht verschweigen. Wie Änderungen dennoch erfolgen können, wird später beschrieben (Soft-Fork, Hard-Fork). Hier eine Grafik über die Aufteilung der Bitcoin-Miner (Bild 7).

Blockchain: Es geht um viel mehr als nur Bitcoins

Wer jetzt immer noch glaubt, die Blockchain-Technologie wurde nur erfunden, um Bitcoins für Nerds zu erzeugen, liegt falsch. Die technische Revolution, die damit ausgelöst

wurde, ist nicht mehr aufzuhalten. Mittlerweile gibt es weit mehr als 1 000 verschiedene Kryptowährungen, was höchstwahrscheinlich vollkommen unsinnig ist.
Mittlerweile meint ja jeder Promi (z. B. Fußballstar), er müsse zu Marketingzwecken seinen eigenen Coin auf den Markt bringen oder jedes Start-up bringt seinen eigenen Token heraus, von dem nach durchschnittlich einem Jahr nichts mehr zu hören ist. Dieser Effekt der völligen Übertreibung ist selbstverständlich typisch menschlich und durchaus erlaubt – sollte aber vom Wesentlichen nicht ablenken.
Eine erste Orientierung gibt die Hitparade der Kryptowährungen an, die sogenannte Marktkapitalisierung, die man unter **www.coinmarketcap.com** einsehen kann. Allerdings stellt diese nicht den realen Geldfluss in eine Kryptowährung dar. Ruft man auf derselben Seite zum Beispiel das Handelsvolumen auf, ergibt sich schon eine andere Reihenfolge.
Bei der Marktkapitalisierung steht der Bitcoin BTC an erster Stelle, gefolgt von Ethereum. Der Coin des Systems Ethereum heißt Ether ETH. Eigentlich war er gar nicht als virtuelle Währung gedacht, sondern sollte den Betreibern von Ethereum-Knotenrechnern die Rechenleistung vergüten. Aber trotzdem wird er quasi zum Teil wie eine Kryptowährung ge- und behandelt. Weil die Technologie des Ethereum wesentlich komplexer als die des Bitcon ist, vermuten manche, dass Ethereum den Bitcoin bald vom Platz 1 verdrängen könnte.

Möglicher Einsatz der Blockchain-Technik

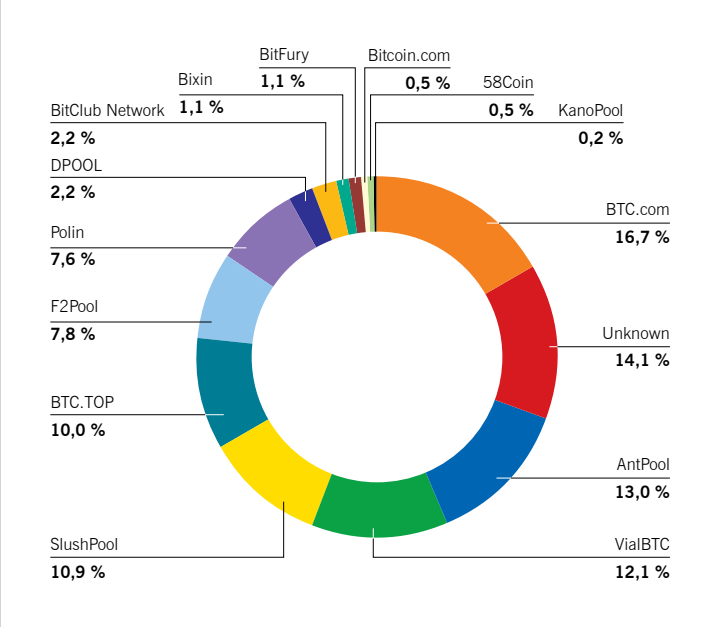
Momentan gibt es unzählige Ideen, Ansätze und fertige Lösungen, die Blockchain-Technik einzusetzen. Daher ist es schwierig, die bislang erkennbaren Ziele mit wenigen Sätzen zu beschreiben. Stichpunktartig soll es versucht werden:

- **Vertrauen und Transparenz.** Menschen sollen nichtkorrumpierbaren Open-Source-Algorithmen ihr Vertrauen schenken, wenn es um die Aufbewahrung und den Transfer von Werten geht.
- **Zugang zum Finanzwesen.** Etwa 2,5 Mrd. Menschen in ärmeren Ländern haben keinen Zugang zum Banken- und Finanzwesen. Sie sind vom Handel praktisch ausgeschlossen. Mit einer Wallet-App auf dem Handy könnten sie schlagartig Geld empfangen, senden und aufbewahren – und das praktisch ohne Zusatzkosten und Gebühren. Auf solche Wallets wird noch eingegangen. Es sind praktisch digitale

Portemonnaies in Form einer App für Kryptowährungen. Eine Hürde besteht allerdings noch oft: der Analphabetismus. Aber selbst dafür hat die Technik Lösungsvorschläge: Z. B. ein iPhone. Dort gibt es unter Bedienungshilfen die Funktion VoiceOver, und schon wird der Bildschirminhalt vorgelesen.

- **Smart contracts.** Die Datenblöcke einer Blockchain sind nicht nur dafür nutzbar, bestimmte Geldbeträge zu speichern oder zu dokumentieren, sie können auch ganz anders genutzt werden. Darauf setzen beispielsweise Ethereum ETH oder VeChain VEN. Sie betten intelligente Verträge (Smart Contracts) in die Blockchain ein, die dann komplexe Handlungen und Zahlungsvorgänge managen können. Ein einfaches Beispiel: Man kann einen Mietwagen, der online eingebunden ist, nur starten, wenn zuvor die Zahlung erfolgt ist.
- **Digitale Bezahlsysteme.** Das Wettrennen um digitales Zahlen ist eröffnet. Konzerne versuchen mit Macht, auch dieses Thema an sich zu reißen – wie Google Pay, Amazon Payments, Apple Pay, Alipay usw. Wollen wir das wirklich? Oder wählen wir einen neutralen Weg via Kryptowährung? Allerdings kann noch keiner vorhersagen, welcher Coin das Rennen machen wird oder ob es mehrere sein werden: Bitcoin, DASH, Lightcoin, Bitcoin-Cash, EOS – und wie sie alle heißen. Glaubt wirklich jemand, dass es in 10 Jahren noch Papiergeld und geprägte Münzen geben wird? Außerdem könnte gar nicht jeder sein (virtuelles) Guthaben in Schein & Münze ausgezahlt bekommen, weil dafür das physische Material fehlt. Daher die Angst vor einem „Bank-Run". Also: Wenn ohnehin schon virtuell, dann könnte es auch gleich krypto sein.
- **Stablecoins.** Auch die Finanzwelt hat den Trend mittlerweile erkannt – und wenn auch nur aus Angst, den technologischen Zug zu verpassen. Die Rede ist von sogenannten Stablecoins, die eben nicht unter großen Kursschwankungen leiden, wie das sonst (noch) bei Kryptos der Fall ist.
  - Beispiel: Goldman-Sachs unterstützt Circle, die den USD-Coin vermarkten wollen. Dieser soll in Parität zum Dollar stehen und auch durch Dollar gedeckt sein. Das hat zwar nichts mehr mit der Idee von Satoshi Nakamoto zu tun, aber die Finanzwelt will ihre Einflussmöglichkeiten nicht so einfach aufgeben. Laut einer Studie des Beratungsunternehmens Greenwich Associates wurden im Jahr 2017 etwa 1,7 Mrd. Dollar in die Entwicklung von Blockchain-Projekten investiert, bezogen auf die Bankenwelt (Quelle: BTC-Echo.de).
- **Sicheres Verbriefen.** Immer, wenn irgendwelche Rechte, Ereignisse oder Eigentumsansprüche sicher verbrieft und gespeichert werden müssen: Dafür ist die Blockchain besser und sicherer geeignet, als jeder andere Tresor. In Zukunft bedarf es keiner Grundbuchämter mehr. Wahlen und deren Ergebnisse werden manipulationssicher in einer Blockchain gespeichert und organisiert. Verträge und geistiges Eigentum (Urheberrechte) lassen sich sicher verwalten.
- **Transparenz.** Eine sehr wichtige Funktion wird ebenfalls mit dieser Technologie lösbar sein: Lieferketten lassen sich lückenlos, fälschungssicher und standardisiert dokumentieren: Vom Fischfang auf dem Meer bis zum fertigen Produkt auf dem Teller. Ebenfalls sehr wichtig: Mithilfe einer Blockchain könnten Medikamente von der Produktion bis zum Patienten lückenlos überprüft werden. Der riesige Markt von gefälschten und gefährlichen Medikamenten lässt sich so einfach austrocknen.

7 Anteile am weltweiten Mining (Oktober 2018)



Quelle: blockchain.info

Fazit

Wer hat diese Entwicklung ausgelöst? Der Bitcoin am 03.01.2009 um 18:15 Uhr – vgl. auch Beitrag: „Bitcoins & Co. – wie Blockchain und Kryptowährungen die Welt verändern (Teil 1)", ep-10-2018, S. 872–878).

Mit dem Bitcoin hat eine neue Technologie in die IT-Welt Einzug gehalten. Weil es sich um Open-Source-Software handelt, kann jedes Unternehmen diese Technik aufgreifen, für eigene Zwecke ändern oder erweitern – und dann auch selbst einsetzen.

So ist es beispielsweise damit möglich, die eigene Blockchain-Technik nicht auf öffentlichen Nodes zu implementieren, sondern diese auf eigenen (privaten) weltweit verteilten Nodes laufen zu lassen. Selbst das aufwendige Mining kann in solchen geschlossenen privaten Systemen entfallen.

Dieser Trend ist momentan stark ausgeprägt – nach dem Motto: „Danke Bitcoin für die Technik, aber dich brauchen wir nicht." Insofern könnte der Bitcoin selbst zum tragischen Helden werden.

Umgekehrt ließe sich argumentieren, dass Investoren die enormen Vorteile und die rasante Blockchain-Entwicklung zur Kenntnis nehmen und dort investieren. Als Folge dieser Akzeptanz könnte es schließlich bei Investoren auch heißen: „Wenn diese Technik so gut ist, warum soll sie dann beim Bitcoin selbst nicht auch gut sein", sodass auch hier die Vertrauensbasis künftig wächst. ■