Blockchain: Schau mal wer da prüft!

Eine Übersicht über die Blockchain-Prüfverfahren: Proof of Work (PoW), Proof Of Stake (PoS) und Proof of Authority (PoA)

Wolfram M. Walter, PMD Akademie, März 2018

Ein sehr häufig genanntes Argument gegen den Einsatz einer Blockchain ist der gigantische Stromverbrauch. Der mittlerweile im Kontext Bitcoins benötigte Energiebedarf liegt im Terrawatt-Bereich, mehr als manche Kleinstadt verbraucht. Grund dafür ist das Prüfverfahren proof-of-work (POW), welches zum ersten Mal wohl 1999 in einer wissenschaftlichen Arbeit beschrieben wurde. Richtig bekannt wurde es dann 2008 durch Satoshi Nakamoto.

Bevor die verschiedenen Prüfverfahren beschrieben werden ist wichtig zu wissen, dass es zwei Arten von Blockchain gibt.

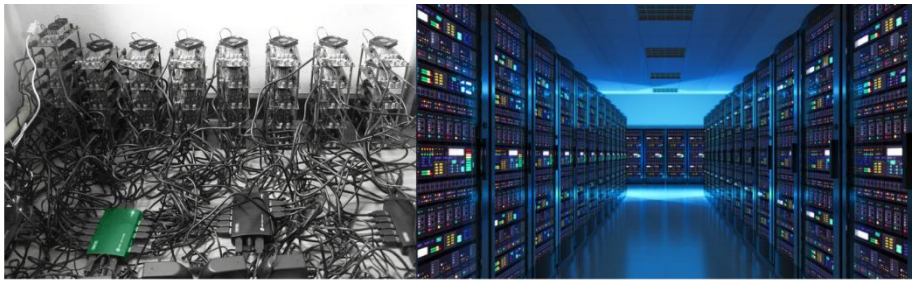
Es gibt zunächst einmal die Blockchain-**Philosophie**. Diese besagt, dass Datenblöcke in Form von Ketten aneinandergefügt werden und der Konsens mittels Prüfalgorithmen hergestellt wird. So basiert z. B. Etherium genauso auf der Blockchain-Philosophie wie Bitcoin.

Als zweites gibt es die Blockchain-**Anwendungen**. Die bekannteste dürfte wohl Bitcoin sein. Bei Etherium liegt der Fokus z. B. nicht auf der kryptischen Währung sondern auf virtuellen Verträgen, den Smart Contracts.

Wie der Name schon sagt, geht es bei dem **Proof of Work (PoW)-Verfahren** um Arbeit, genau genommen um Rechnerarbeit. Findet z. B. ein Ladevorgang von Energie an einer Ladesäule statt oder wird Kryptogeld von A nach B überwiesen, greifen die in einem Rechnerverbund (Pool) zusammengeschlossenen Rechner (node) diese Transaktion auf. Kommen parallel vergleichbare Transaktionen zusammen, weil z. B. 10 Personen sich untereinander kryptisches Geld überweisen, werden diese Transaktionen zu einem Block zusammengefasst. Dieser Block wird an dem bereits bestehenden Block angehängt, eine Kette entsteht (Chain). Damit diese Transaktion als „gesichert“ validiert wird, müssen die nodes eine sehr rechenintensive kryptische Aufgabe lösen. Derjenige node, der die Aufgabe als erster gelöst hat, wird für seine Arbeit in Form von kryptischem Geld belohnt, wie z. B. durch Bitcoins. Den Vorgang nennt man „schürfen“ bzw. mining. Die nodes, die sich an diesem Prozess beteiligen, nennt man Miner. Da alle in dem Pool befindlichen nodes Konkurrenten sind und leider nur der Schnellste bezahlt wird, rüstet man entsprechend auf: Hochleistungsrechner, komplexe Rechnerverbünde, sehr viel Speicherplatz, superschnelle Grafikkarten.

Beim PoW soll die Rechenleistung über viele nodes verteilt werden. Durch den Bitcoin-Hype und die damit verbundenen Gewinnmöglichkeiten haben sich immer schnellere und immer größere Rechnerverbünde in den öffentlichen Pools (public pool bzw. public blockchain) breit gemacht. Aufgrund der Größe stieg u.a. der Strombedarf. Dies ist ein Grund dafür, weshalb über 80 % der Miner in China stehen, wo der Strom noch äußerst günstig ist.
Neben dem hohen Strombedarf und dem hohen Speicherbedarf, die Bitcoin-Kette ist über 100 GByte groß, gibt es aber ein weiteres Problem, welches dem Vertrauensprinzip einer Blockchain

widerspricht: Wenn sehr große Miner über 51 % der Leistung in diesem Pool besitzen (eine sogenannte „51 %-Attacke“), besteht zumindest rechnerisch die Gefahr einer Manipulation der Blockchain und somit auch der vergangenen, validierten Transaktionen.



Mining 2009 Mining 2017

Quelle: Google 2017

Bei dem **Proof of Stake (PoS)-Verfahren** sieht das Vorgehen deutlich anders aus. Möchte ein Unternehmen mit seinen Blockchain-Anwendungen im Markt aktiv sein, wird zunächst Geld von Investoren benötigt. Dies kann z. B. mittels ICO-Methode (Initial Coin Offering) im Rahmen eines Crowdfundings erfolgen. Je nachdem, wie viel Geld jemand investiert, bekommt er eine gewisse Anzahl an Anteilen (Stake), sogenannten Token. Dabei gibt es eine Obergrenze der insgesamt zur Verfügung stehenden Token.

Quelle: W.M.Walter, 03/2018

Nun kann man sich vorstellen, dass jeder Token einer Glaskugel entspricht und jede Firma, die sich beteiligt, bekommt nun ihre Token in ihrer Farbe. Jede Farbe kommt dabei nur einmal vor. Alle Glaskugeln kommen jetzt in einen großen Sack.

Weil eine gewichtete Zufallsauswahl getroffen wird, besteht Konsens, welcher Teilnehmer den nächsten Block validieren darf. Gewichtet wird nach der Teilnahmedauer und dem Vermögen (Stake = Anzahl Token) eines Teilnehmers. Die Chance, „gezogen“ zu werden ist umso größer, je mehr Kugeln ein Unternehmen in dem Sack hat. Allerdings gibt es keine Garantie, dass man gezogen wird, denn für „das Ziehen der Kugel“ wird ein Zufallsalgorithmus eingesetzt.

Hat eine Transaktion stattgefunden, wird per o.a. Auswahlverfahren ein Rechner ausgewählt, der den neuen Block validieren darf. Mit der Validierung wird als Belohnung ein Token geschaffen. Dieser Token und die Transaktionsgebühren werden regelmäßig und zufällig über alle Token-Inhaber mithilfe eines Algorithmus ausgeschüttet, der neben dem wertmäßigen Anteil am Netzwerk auch die Dauer des Besitzes berücksichtigt. Das Proof-of-Stake-Mining wird auch als Forging (Schmieden) bezeichnet.

Der Vorteil bei dieser Methode liegt darin, dass kein zeitintensives Mining durchgeführt werden muss, welches bekanntermaßen auch noch sehr energieintensiv ist. Das Problem des 51 %-Angriffs besteht zwar auch, allerdings in einer eingeschränkten Form. Ein Angreifer müsste mehr als die

Hälfte des Gesamtvermögens (Anzahl Token) besitzen. Dann wäre es denkbar, dass eine parallele Kette aufgebaut werden kann.
Bei dem **Proof of Authority (PoA**)-Verfahren handelt es sich um einen Algorithmus, bei dem die Konsensfindung auf Basis der Identität des Nutzers erfolgt. Spezielle Private Keys werden an die Miner versendet, die es nur ihnen ermöglichen, diese Nachrichten zu entschlüsseln, zu lesen und die Blöcke zu generieren. Sowohl Sender als auch Empfänger benötigen diesen Schlüssel. Bei dieser Methode ist der Empfänger die Autorität, der erlaubt wird, den Mining-Prozess durchzuführen und die Blockchain zu sichern. Jeder generierte Block muss von der Mehrheit der Autoritäten abgezeichnet werden und wird genau protokolliert. Um das Missbrauchsrisiko gering zu halten, darf kein Validator aufeinanderfolgende Blöcke freigeben.

Bevor ein Rechner als Validator arbeiten darf, muss er den Nachweis erbringen, dass er über die benötigte Autorität verfügt. Dies geschieht durch eine Software-Emulation. Die Besonderheit hierbei ist, dass dieser Vorgang automatisiert abläuft und die Benutzer Aufträge nicht aktiv nachverfolgen müssen. Vorteile dieses Konzeptes im Grundsatz sind mehr Sicherheit und eine bessere Planbarkeit der generierten Blocks. Außerdem entstehen beim PoA geringere Kosten und es wird deutlich weniger Energie benötigt, da immer nur eine Autorität pro Block bemächtigt wird.

Die Validatoren werden für ihre Arbeit mit Token belohnt, weshalb hier jeder ein besonderes Interesse hat, den Validator-Status zu halten. Insbesondere spielt das positive Image eine entscheidende Rolle und muss aufrechterhalten werden. Ansonsten brauchen Nutzer keinen hohen Token-Bestand, um als Validator aktiv zu werden.
PoA eignet sich für private Netzwerke (private pool bzw. private blockchain) und nicht für öffentliche Netzwerke (public pool bzw. public blockchain)

Der Autor

Wolfram M. Walter
Professional Scrum Master
Member of German Speakers Association

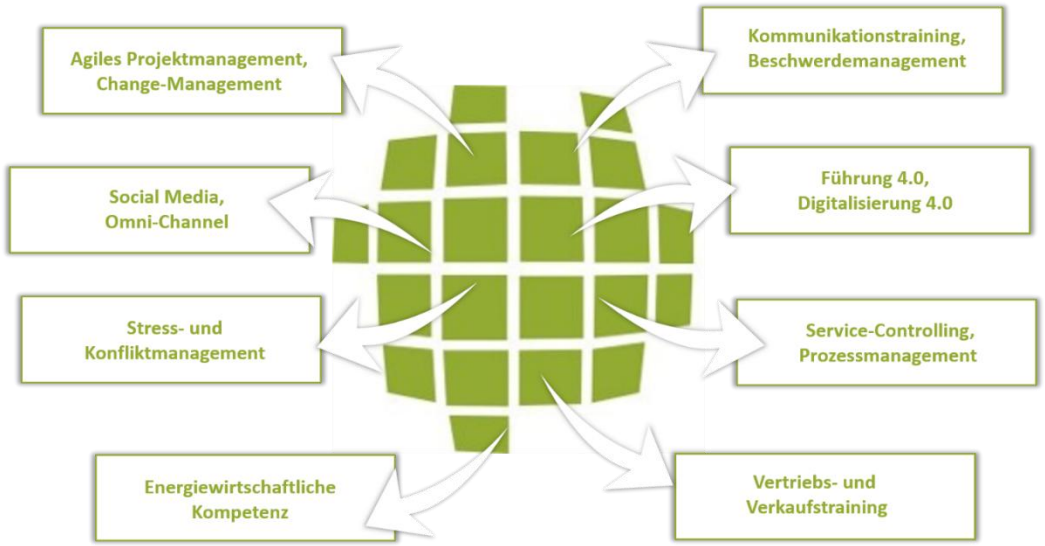
Geschäftsführer der PMD Akademie
w.walter@dms-gruppe.de
www.dms-gruppe.de
info@dms-gruppe.de

PMD Projektmanagement Deutschland Akademie GmbH

Die PMD Akademie ist das Weiterbildungsinstitut der DMS Gruppe und versteht sich als Dienstleister in der Aus- und Weiterbildung mit dem fachlichen Schwerpunkt Energiewirtschaft und mit in der Praxis erprobten Führungs- und Methodenseminaren.

Gemeinsam mit unseren Kunden identifizieren wir die Herausforderungen und entwickeln die passenden Qualifizierungskonzepte. Um Ihre Reisekosten zu minimieren, bieten wir unsere Seminare deutschlandweit an den Standorten der DMS Gruppe an und kommen natürlich auch zu Ihnen in Ihr Unternehmen. Dabei wird berücksichtigt, dass das Bildungskonzept den Menschen und den Anforderungen aus dem Tagesgeschäft angepasst wird.

Das Lernen fängt nach den Seminaren an. Gerne begleiten wir Sie bei dem Wissenstransfer in die Praxis und sorgen somit für eine nachhaltige Anwendung des Erlernten. Bei unseren train-the-trainer-Konzepten geben wir unser didaktisches Wissen gerne an Sie weiter.



Wenn Sie Interesse an den Leistungen der PMD Akademie oder an den aktuellen Seminarkatalogen haben, nehmen Sie bitte Kontakt mit uns auf unter **info@dms-gruppe.de** oder schauen Sie auf unsere Web-Seite **www.dms-gruppe.de**.

Wenn Sie an aktuellen Themen rund um die Energiewirtschaft und zu Führungs- und Methodenkompetenzen interessiert sind und sich gerne mit anderen Menschen austauschen, dann besuchen Sie doch unseren Blog unter **pmdablog.wordpress.com**.

Sie möchten sich einen Überblick über einzelne Themen verschaffen und sind sich noch nicht sicher, welches Seminar für Sie geeignet ist? Dann besuchen Sie unsere kostenlosen Webinare unter **webinare.pmd-akademie.de**.

Die gezeigten Unterlagen erhalten Sie ebenfalls kostenlos als PDF-Download.