Andreas Schütz

WE WILL BLOCK YOU!

Der Blockchain gehört die Zukunft. Viele Experten prognostizieren, dass die Technologie das Internet, wie wir es kennen, verändern wird. Wie groß die Revolution aussehen wird, steht allerdings noch in den Sternen. In einigen Branchen hat die Blockchain auf jeden Fall ausreichend Potenzial, um die Geschäftsmodelle gehörig durcheinanderzuwirbeln. Falls Sie jetzt „Block… was?“ denken – haben Sie keine Angst: Dieser Artikel macht sie zum Blockstar. We will block you!

Blockchain – fast schon ehrfürchtig wird der Begriff auf vielen Konferenzen der Digitalbranche diskutiert. Vor allem der Finanz- und Energiesektor wird von der Technologie magisch angezogen. Während das Thema noch vor einigen Jahren bestenfalls in den Pausenräumen der IT-Abteilungen diskutiert wurde, geistert der Begriff inzwischen durch die langen Korridore und schaffte es mittlerweile bis in die Vorstandsetagen. Dort wird die Technologie kritisch beäugt. Denn die Blockchain hat das Potenzial, die Riesen einiger Branchen zum Taumeln und Fallen zu bringen, Start-ups in kürzester Zeit auf den Thron zu setzen und ganze Geschäftsmodelle zu verändern. Dies führt zu Innovationsdruck und einem Wettrennen um die besten Plätze in der noch unbekannten neu entdeckten Blockchain-Welt. Höchste Zeit, sich mit der Technologie zu beschäftigen.

Am Anfang war der Bitcoin

Die Geschichte der Blockchain ist untrennbar mit dem Projekt „Bitcoin“ verbunden. Satoshi Nakamoto stellte 2008 das Konzept für die digitale Währung vor und mit ihm die Blockchain als realisierende Technologie. Obwohl er der Vater der revolutionären Technologie ist, sieht man ihn auf keiner Blockchain-Konferenz und liest keine Interviews. Es gibt noch nicht einmal ein Bild von ihm, denn Satoshi Nakamoto ist keine reale Person. Es ist auch nicht geklärt, wer hinter dem Pseudonym steckt. Vielleicht trug genau dieses Mysterium dazu bei, die Faszination der Bitcoins und damit auch der Blockchain noch zu steigern. Wer auch immer er ist: Sein Ziel war es, eine Währung zu schaffen, die ohne Mittelsmänner, wie beispielsweise Banken, auskommt.

2009 ging das Bitcoin-Netzwerk online und geriet immer mehr in den Fokus der Öffentlichkeit. Nachdem mehrfach der Tod des Projektes vorausgesagt wurde, überraschten die Bitcoins im Jahr 2013 die Beobachter der Szene. Bereits zu Beginn des Jahres war der Kurs auf über 200 US-Dollar gestiegen, explodierte schließlich im Dezember 2013 und schoss auf über 1200 US-Dollar. Trotz Ups and Downs liegt der Preis aktuell (steigend) wieder bei rund 730 Dollar. Ein Problem ist allerdings noch die Akzeptanz der Währung. Zwar stieg die Anzahl der Akzeptanzstellen in den vergangenen Jahren, der Marktanteil ist allerdings immer noch homöopathisch. Im Darknet etablierte sich Bitcoin jedoch längst und hat so bei vielen Verbrauchern immer noch einen kriminellen Beigeschmack. Während die Währung selbst noch ihren Weg sucht, stieg das Interesse an der Technologie im Hintergrund jedoch exponentiell. Die Blockchain ist Open Source und somit gibt es mittlerweile einige Projekte, die eine eigene Blockchain nutzen. Auch die Banken, die in Nakamotos Grundgedanken überflüssig gemacht werden sollten, wollen die Technologie jetzt für ihre Zwecke nutzen.

DER AUTOR

Andreas Schütz ist Masterstudent und leidenschaftlicher Blockchain-Fan. Zusammen mit seinem Team bietet er auf www.etherbasics.com Erklärungen und Tutorials rund um das Thema Blockchain an.

Foto: DenisKot / thinkstockphotos.de

Abb.1: Durchschnittlicher Marktpreis in USD auf großen Bitcoin-Börsen *(Quelle: blockchain.info)*

Die Blockchain weiß alles

Computer vernetzen sich, um untereinander Informationen auszutauschen, egal ob ein Bild oder eine Nachricht verschickt, Geld überwiesen oder ein Facebook-Post abgesetzt wird. Der Austausch von Informationen, die sogenannten Transaktionen, stehen auch bei Blockchain-Netzwerken im Mittelpunkt. Die Transaktion von Bitcoins ist schließlich nichts anderes als die Information, dass der Besitz eines bestimmten Betrages der Währung auf einen anderen Besitzer übergeht. Die Blockchain ist das Gedächtnis des Netzwerkes. In ihr werden alle Transaktionen festgehalten. Aus der Blockchain ist abzulesen, wer was an wen zu welchem Zeitpunkt transferierte. Sie ist also eine Art Datenbank. Diese Funktionalität würde aber nicht den Hype um die Technologie rechtfertigen.

Das große Alleinstellungsmerkmal liegt im Speicherort der Blockchain. Wenn in einem klassischen Netzwerk Daten ausgetauscht oder gespeichert werden, wird dafür aktuell eine zentrale Instanz genutzt. Wird eine E-Mail versendet oder eine Überweisung in Auftrag gegeben, werden die Informationen an einen zentralen Server übermittelt und erst von dort an den Empfänger weitergeleitet. Auch wenn online oder in einem Firmennetzwerk Daten gespeichert werden, geschieht dies in der Regel auf einem zentralen Server. Trotz vieler Sicherheitsmechanismen stellt so ein zentraler Punkt immer eine Angriffsfläche dar. Durch einen Hack oder eine Naturkatastrophe können Informationen verloren gehen. Außerdem können Informationen an einem zentralen Ablageort, beispielsweise durch unbefugten Zugriff oder Korruption, verfälscht werden.

Die Blockchain-Technologie verzichtet auf eine zentrale Instanz und speichert einfach eine Kopie der Blockchain auf jedem Computer (Knoten) im Netzwerk. Somit sind die Transaktionen für jeden transparent einsehbar. Diese dezentrale Verteilung sorgt für Sicherheit. Um die Blockchain zu zerstören, müsste jeder Computer im Netzwerk zerstört werden. Um die Blockchain zu kontrollieren, müsste es jemandem gelingen, mehr als 50 Prozent der Rechenleistung im Netzwerk zu besitzen. Denn die Mehrheit entscheidet über die Wahrheit in der Blockchain.

Sicherheit durch Mining

Um zu garantieren, dass die Knoten im Netzwerk immer eine aktuelle und richtige Kopie der Blockchain besitzen, stellt die Technologie ein ausgefeiltes System zur Verfügung: das Mining. Miner sind Personen oder Firmen, die im Netzwerk nach Rewards, meist in Form einer zu der Blockchain gehörenden Kryptowährung, suchen. Ihre Rechenleistung wird dazu genutzt, die Blockchain sicher zu halten. Um das Mining zu verstehen, ist es nötig, die Blockchain genauer unter die Lupe zu nehmen. Wie der Name bereits suggeriert, nehmen Blöcke eine zentrale Stellung in der Technologie ein. Diese Blöcke werden aneinandergereiht und bilden gemeinsam die Chain. Ein Block ist wie eine Seite in einem Buch. In ihn werden solange Transaktionen geschrieben, bis er voll ist. Die maximale Blockgröße in der Bitcoin-Blockchain beträgt beispielsweise 1 Megabyte. Das Mining lässt sich am besten anhand der ersten Blockchain erklären, die mittlerweile 88 Gigabyte groß ist: die Bitcoin-Blockchain.

Die Sicherheit in der Blockchain entsteht durch die Verwendung kryptografischer Verfahren. Bereits bei der Erstellung einer Transaktion kommt ein Verschlüsselungsverfahren zum Einsatz. Möchte Peter seinem Freund Norbert einen Bitcoin schicken, benötigt er dafür Norberts öffentlichen Public Key. Public Keys sind Adressen oder Kontonummern im Netzwerk und werden in den sogenannten Wallets verwaltet. Bitcoins sind immer mit dem Public Key des jeweiligen Besitzers verknüpft und können so zugeordnet werden. Der geheime Private Key stellt den Schlüssel und damit die Verfügungsgewalt zu dem „Konto“ dar. Bei der Transaktion wird nun der Public Key von Norbert an den Coin angehängt, um zu zeigen, dass er der neue Besitzer ist. Um die Richtigkeit zu gewährleisten, wird die Transaktion mit dem Private Key von Peter, dem alten Besitzer, signiert. Anschließend geht es ab in den Block. Die Transaktion ist aber erst endgültig, wenn sie bestätigt ist. Hier kommen die Miner ins Spiel.

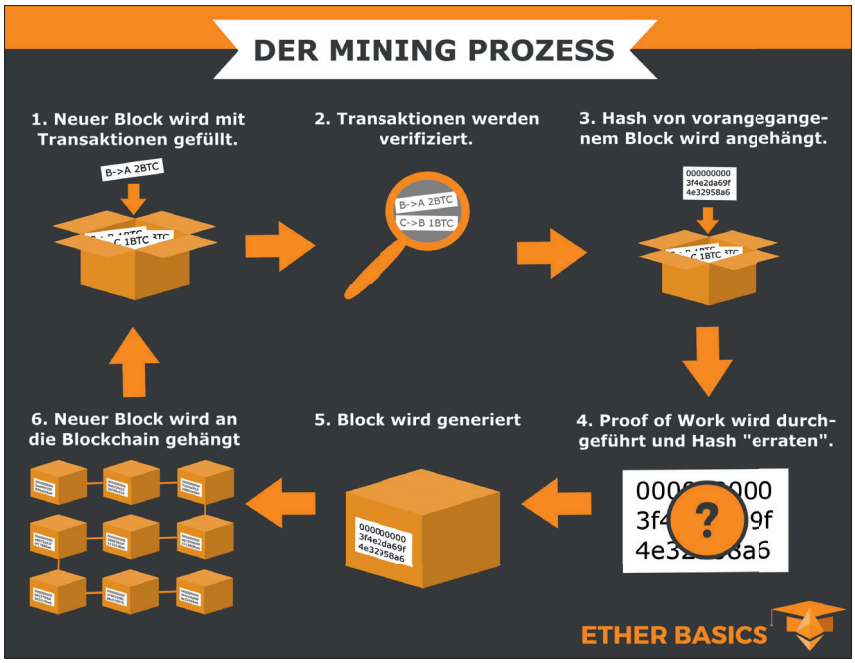

Abb.2: Der Mining-Prozess im Bitcoin-Netzwerk

Zuerst werden genügend Transaktionen gesammelt, um den Block zu füllen. Anschließend wird von den Minern überprüft, ob bei der Transaktion alles mit rechten Dingen zugeht und sie den Regeln entsprechen. Jetzt kann der Block sozusagen zugemacht werden. Aus den im Block enthaltenen Informationen wird von den Minern ein Hash gebildet, also eine vereinfachte Prüfsumme, die die spätere Kontrolle der Blockchain erleichtert. Der Hash-Algorithmus (bei Bitcoin SHA-256) ist dabei deterministisch und liefert für gleichen Input auch immer gleichen Output. Falls jemand also nachträglich versucht, etwas an den Informationen im Block, zum Beispiel einer Transaktion, zu ändern, wäre er gezwungen, auch den Hashcode zu verändern. Immer noch zu einfach für Angreifer? O. k., wie ist es hiermit: Um einen Hash zu erzeugen, wird auch immer der Hash des vorgehenden Blocks verwendet. Ändere ich also den Hash des einen Blocks, würde sich auch der Hash der nachfolgenden Blöcke verändern und würde nicht mehr zu den Transaktionen passen. Und obwohl es einfach ist, aus den Transaktionen den Hashwert zu berechnen, ist es umgedreht sehr schwierig, vom Hashwert auf die Transaktionen zu schließen. Für einen Angreifer wird es also unmöglich, die nachfolgenden Transaktionen so zu fälschen, dass sie wieder zu den veränderten Hashwerten passen. Die Tatsache, dass die einzelnen Blöcke durch die Hashs verkettet sind, führt auch zum Namen Blockchain.

Für seine Arbeit bekommt der Miner, der den Block versiegelt, derzeit 12,5 frisch generierte Bitcoin, die helfen, die Ausgaben für die Hardware, die Zeit und die Stromkosten zu decken. So gesehen dürfte das kein Problem sein, denn der Gegenwert ist beim aktuellen Kurs mehr als 7.500 Euro. Da muss doch ein Haken an der Sache sein! Ja, ganz so einfach ist es wirklich nicht. Bei so viel Geld stehen natürlich sehr viele Miner auf der Matte, um den Block abzuschließen. Um das Ganze schwieriger zu machen und dadurch auch die Menge der generierten Bitcoins im Zaum zu halten, stellt das Bitcoin-Protokoll den Minern eine Art Rätsel. Nur wer das Rätsel lösen kann, darf an den begehrten Block. Die Schwierigkeit des Rätsels (Difficulity) variiert, je nachdem, wie groß der Ansturm im Netzwerk ist. Das Rätsel ist eigentlich eine Art Ratespiel und hat eher mit Glück als mit Können zu tun. Die Miner raten einen Wert (Nonce), mit dem der Hash erzeugt wird. Nun wird geprüft, ob der Hash den festgelegten Zielvorgaben entspricht. Tut er das nicht, wird der Hash verworfen und es wird neu geraten, bis jemand das Rätsel lösen kann. Der „Gewinner“ versiegelt den Block schließlich und hängt ihn an die Blockchain. Dieses Verfahren wird auch „Proof of Work“ (PoW) genannt, da mit ihm sichergestellt wird, dass für das Lösen des Blockes ein Arbeitsaufwand erbracht werden muss. Bei PoW gilt, dass der Miner mit der besten Hardware-Leistung letztendlich auch die besten Chancen auf den Block hat. Als Alternativverfahren wird im Blockchain-Umfeld auch das „Proof of Stake“-Verfahren (PoS) diskutiert. Hier erhöht nicht die beste Rechenleistung die Chancen auf den Block, sondern wie viele Coins der jeweiligen Kryptowährung sich im Besitz des Miners befinden. Mit PoS würde das Ratespiel überflüssig werden und somit könnte viel Rechenleistung und Strom eingespart werden. Mit Ethereum plant bereits ein großes Projekt, auf PoS zu wechseln.

Die maximale Anzahl der generierbaren Bitcoins beträgt 21 Millionen Coins, von denen aktuell bereits mehr als 76 Prozent generiert wurden. Je mehr Bitcoins es gibt, umso langsamer geht auch die Generierung. Durchschnittlich alle vier Jahre wird der Reward für das Abschließen eines Blocks halbiert. Das letzte sogenannte Halving fand in diesem Jahr statt. Häufig wird die Frage gestellt, was mit den Minern im Bitcoin-Netzwerk passiert, wenn der letzte Bitcoin generiert wurde. Wenn dieser Moment gekommen ist, wird die Belohnung für die Miner über Transaktionsgebühren geregelt. Transaktionen, für die mehr Gebühren hinterlegt wurden, werden auch schneller ausgeführt. Dies wird allerdings erst in 2140 der Fall sein.

Benefits der Blockchain

Die Blockchain-Technologie ist so beliebt, weil sie eine ganze Reihe von Vorteilen mit sich bringt. Einen großen Faktor stellt die Sicherheit dar. Von den drei Schutzzielen der IT-Sicherheit – Vertraulichkeit, Integrität und Verfügbarkeit

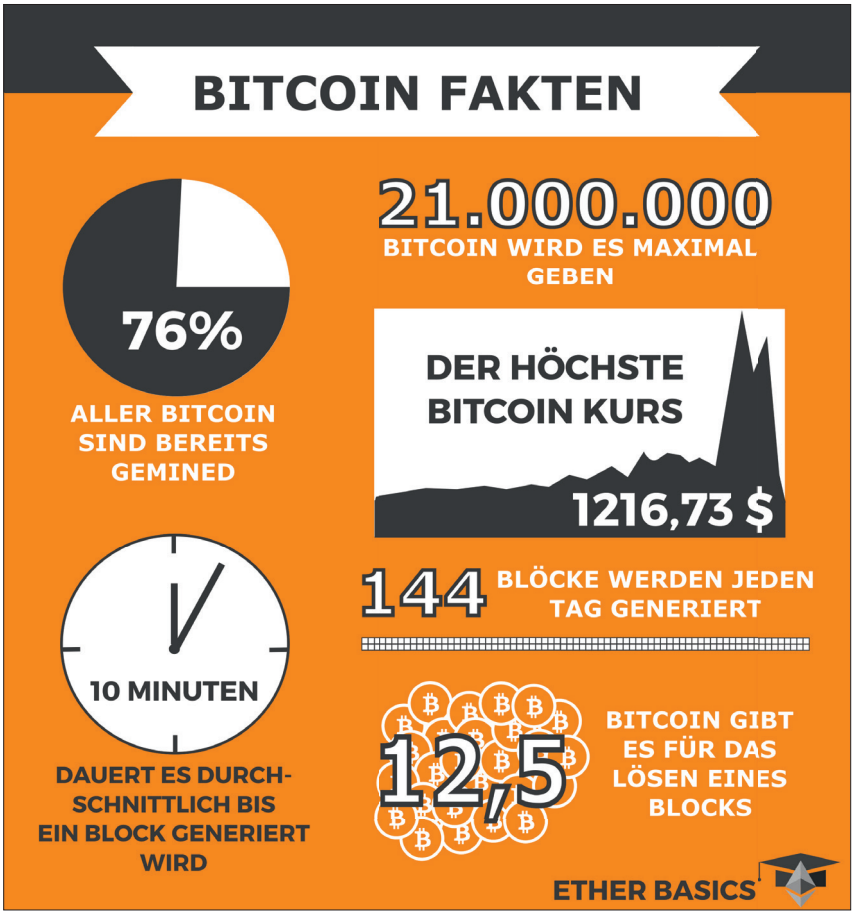

Abb.3: Zahlen und Fakten zum Thema Bitcoin

– erfüllt sie zwei mit Bravour. So ist die Integrität der Informationen sichergestellt, da nachträgliche Änderungen durch oben genanntes Verfahren ausgeschlossen sind. Neue Änderungen werden vor dem Propagieren geprüft. Auch die Verfügbarkeit ist durch die Dezentralität enorm hoch. Es können sogar mehrere Knoten ausfallen, da genügend Knoten im Netzwerk sind, um die Verfügbarkeit der Blockchain sicherzustellen. Lediglich die Vertraulichkeit lässt zu wünschen übrig. Zwar wird häufig die Anonymität von Bitcoin gelobt, da die Teilnehmer durch die Public Keys im Netzwerk identifiziert werden. Sobald aber jemand weiß, wem die Adresse gehört, zum Beispiel, weil er dem Inhaber etwas überwiesen hat, kann er sämtliche vergangene und zukünftige Transaktionen der Adresse einsehen. Das Projekt ZCash will diesen Nachteil aus dem Weg räumen.

Die Transparenz der Blockchain kann aber auch Vertrauen schaffen. Wenn zwei Personen sich nicht vertrauen, kann die Blockchain treuhänderisch zur Seite stehen. Denn in der Blockchain sind getroffene Transaktionen unveränderlich nachvollziehbar. Diese Eigenschaft wird vor allem bei den Smart Contracts genutzt. Hierbei handelt es sich um Verträge zwischen Parteien, deren Vertragsbedingungen in der Blockchain festgelegt sind, beispielsweise beim Hauskauf. Hat der Käufer den ausgemachten Betrag über das Netzwerk an den Verkäufer transferiert, wird automatisch in der Blockchain der Käufer als neuer Eigentümer hinterlegt. Auch die Auszahlung eines Erbes könnte über einen Smart Contract abgewickelt werden. Die im gesamten Netzwerk einsehbare Blockchain stellt sicher, dass die Bedingungen genauso ausgeführt werden, wie sie festgelegt wurden. Keine der Parteien kann in der Blockchain nachträglich etwas an den Bedingungen ändern. Die Transparenz ermöglicht es auch, die Blockchain beispielsweise wie ein Grundbuch zu nutzen. Die Eigentumsverhältnisse können nicht gefälscht werden, außerdem sind sie von jedem einsehbar.

Die Blockchain löst außerdem ein Problem, von dem Kryptowährungen betroffen sind: das Double-Spending-Problem. Theoretisch können Daten beliebig oft vervielfältigt werden. Es muss also ein Verfahren geben, um zu verhindern, dass niemand, vereinfacht ausgedrückt, seine Bitcoins mit STRG C und STRG V vervielfacht. Während sich beim Online-Banking mit konventionellen Währungen die Banken-Rechner darum kümmern, übernimmt bei den Kryptowährungen die Blockchain diesen Job. Die Blockchain besticht zudem durch niedrige Kosten. Der Unterhalt der großen zentralen Serverfarmen fällt weg und wird auf das Netzwerk ausgelagert. Umsonst ist die Blockchain aber nicht. Denn auch die Miner wollen für ihre Arbeit entlohnt werden. Und um eine sichere Blockchain zu bekommen, gilt es, möglichst viele von ihnen anzuziehen, um ein großes dezentrales Netzwerk aufzubauen.

Branchen mit Blockchain-Potenzial

Die Blockchain hat das Potenzial, einige Geschäftsmodelle gehörig umzukrempeln oder auch neu zu erschaffen. Dabei ist sie aber sicher kein Allheilmittel für jeden Anwendungsfall. Einige Branchen sehen für sich besonders viel Potenzial in der Technologie.

Ganz vorne dabei ist sicherlich die Versicherungs- und Finanzbranche. Mit Bitcoin wurde bereits gezeigt, dass ein schneller, sicherer und günstiger Geldtransfer möglich ist. Denkbar wären aber auch der Handel und die Verwaltung von Wertpapieren in der Blockchain. Unter dem Namen B3i (Blockchain Insurance Industry Initiative) gründeten fünf große Versicherer kürzlich eine Blockchain-Initiative und sind aktuell dabei, die Möglichkeiten der Blockchain für sich auszuloten.

Auch die Energiebranche kann frischen Wind von der Blockchain erwarten. Mit Smart Contracts und der fehlenden zentralen Instanz wäre es möglich, den

Strom der eigenen Solaranlage direkt an den Nachbarn zu verkaufen. Der große Energieversorgungskonzern RWE arbeitet aktuell zusammen mit dem Start-up Slock.it eifrig daran, die Blockchain im Bereich der E-Mobility zu nutzen. Ladevorgänge von Elektrofahrzeugen sollen dabei über die Blockchain abgerechnet werden, am besten durch ein direktes Induktionsfeld an der Ampel. Da digitale Währungen fast beliebig klein teilbar sind, ermöglichen die sogenannten Micropayments auch die Abrechnung von Kleinstbeträgen.

Neben dem Projekt mit RWE hat Slock.it auch noch ein Hauptgeschäft: Mietvorgänge in der Blockchain. Slock steht dabei für Smart Lock, das schlaue Schloss. Das Motto des Start-ups ist: Alles, was abschließbar ist, kann auch über den Service vermietet werden. Seine Anwendungsbereiche sieht das Unternehmen zum Beispiel beim Geschäftsmodell von Airbnb. Der Anwender könnte mit dem Vermieter eines Apartments einen Smart Contract über den Mietvorgang abschließen. Nachdem er sich am smarten Lock an der Wohnungstür authentifiziert hat, erhält er Eintritt. Nach seinem Auschecken wird die Nutzungsdauer minutengenau über sein Wallet abgerechnet. Auch das Mieten eines Fahrzeugs könnte so abgebildet werden.

Ein beliebtes Szenario ist auch die Verwaltung von Rechten und Eigentum über die Technologie. Länder mit unklaren Eigentumsverhältnissen bei Grundstücken oder mit korrupten Verwaltungen könnten von einem Blockchain-Grundbuch profitieren. Das Start-up Everledger knöpft sich Diamanten vor. In einer Blockchain verwaltet es die teuren Edelsteine und kann einem Käufer Auskunft geben, ob es sich um einen gefälschten oder gestohlenen Diamanten handelt. Auch Nutzungs- oder Urheberrechte könnten mit einer Blockchain verwaltet werden.

Wahlen könnten ebenfalls mit einer Blockchain abgewickelt werden, solange das Wahlgeheimnis gewährleistet wird. Dies spart zum einen Kosten, zum anderen würde es die Auswertung, Beobachtung und auch die Abstimmung selbst vereinfachen. In der Logistik könnte die Blockchain für eine lückenlose, transparente Lieferkette sorgen. Die aktuelle fieberhafte Suche nach weiteren Anwendungsfällen wird uns in Zukunft noch weitere Möglichkeiten für die Blockchain liefern, während andere Ideen vielleicht längst verworfen wurden.

INFO: BLOCKCHAIN-FORUM

Wo stehen wir bei der Adaption der Blockchain-Technologie in der Wirtschaft? Wo geht die Reise hin? Was sind Hemmnisse? Diese Fragen sollte das Blockchain-Forum am 21. Oktober an der Hochschule für angewandte Wissenschaften FHWS in Würzburg beantworten. Prof. Dr. Michael Müßig, Leiter des Schwerpunkts „Management digitaler Innovation", und Andreas Schütz, der sich seit einigen Jahren mit der Blockchain-Thematik beschäftigt, zeichneten für die Veranstaltung verantwortlich. Die Besucher wurden von Andreas Schütz intensiv in die Thematik Blockchain eingeführt und erhielten Informationen zur Funktionsweise und derzeit laufenden Projekten. Marco Streng, Co-Founder und CIO von Genesis Mining, gehört trotz jungem Alter zu den alten Hasen der internationalen Blockchain-Szene. Sein immenses Detailwissen faszinierte nicht nur die Teilnehmer aus der Frankfurter Finanzszene, sondern auch Vertreter anderer Branchen und Masterstudenten. Seine Firma Genesis Mining ist einer der größten Anbieter für Cloud Mining und betreibt riesige Serverfarmen, um in verschiedenen Blockchain-Netzwerken zu minen. Renny Rueda gab Einblicke in seine Forschungsarbeit im Umfeld von E-Democracy. Das Potenzial Blockchain-basierter Mietvorgänge wurde von Julian Lenhart von pad4rent unter die Lupe genommen. Dabei ging er auch auf die Projekte des Blockchain-Start-ups Slock.it ein. Die Veranstaltung mündete im Anschluss an die Vorträge in eine tiefe und teilweise kontroverse Diskussion.
Aufzeichnungen der einzelnen Vorträge sind im Youtube-Channel des Schwerpunktes „Management digitaler Innovationen" abrufbar.

Projekte für die Watchlist

Viele der gerade vorgestellten Anwendungsfälle sind noch sehr vage und in der Evaluierungsphase. Einige Blockchain-Projekte sind jedoch schon sehr konkret. Es lohnt sich, einige dieser Projekte in der Zukunft im Auge zu behalten.

Ethereum ist neben Bitcoin das Projekt, auf das die meisten Hoffnungen der Szene gesetzt werden. Während Bitcoin nur Zahlungsvorgänge ermöglicht, will das Projekt die Blockchain für viel mehr nutzen. Hierfür etabliert die Plattform Blockchain-basierte Smart Contracts. Jeder Nutzer kann sich eigene Smart Contracts in der Ethereum-Blockchain erstellen und so die neue Technologie für sich nutzen. Ethereum ermöglicht beispielsweise eigene Kryptowährungen, Crowdfundings und dezentrale, autonome Organisationen (DAO). In einer DAO können Mitglieder in Abhängigkeit von ihren Anteilen an der Organisation über Anträge abstimmen oder Wahlen abhalten. Die Satzung der Organisation wird komplett in der Blockchain umgesetzt, die sich auch um die Einhaltung kümmert. Der Fantasie sind im Ethereum aber keine Grenzen gesetzt und so kann jeder seine eigene dezentrale Applikation bauen. Das Projekt befindet sich aktuell noch in der Entwicklungsphase, kann aber schon genutzt werden und erfreut sich einer großen Community. Nachdem im Sommer 2016 das größte Projekt im Ethereum „The DAO" gehackt wurde, erlitt Ethereum einen ersten Rückschlag. Bei dem Hack wurde allerdings nicht, wie vielfach missverständlich propagiert, die Ethereum-Blockchain gehackt, sondern vielmehr Lücken in der darauf aufgesetzten „The DAO"-Applikation ausgenutzt. Die Community entschied sich daraufhin mehrheitlich dafür, die Blockchain zurückzusetzen, um das im Hack gestohlene Geld zurückzubekommen.

ZCash wird aktuell als das „Next Big Thing" in der Blockchain-Szene gefeiert. Man kann sich das Projekt wie Bitcoin vorstellen, allerdings gibt es die Möglichkeit, eine Transaktion vollkommen anonym durchzuführen. Dies wird durch eine neuartige Verschlüsselungsmethode gewährleistet. Doch auch klassische Transaktionen können mit dem Projekt getätigt werden. ZCash launchte am 28. Oktober und die ersten durch die Miner frisch abgebauten ZCash-Coins wurden für schwindelerregende Kurse auf den Handelsplattformen verkauft. Sobald sich mehr Coins im Umlauf befinden, sollte sich der Kurs aber stabilisieren.

Möchte eine Firma die Blockchain-Technologie nutzen, steht sie erst mal vor einem großen Problem: Wie bekomme ich meine Blockchain dezentral verteilt, um meine Sicherheit zu erhöhen? Microsoft bietet auf seiner Cloud-Computing-Plattform Azure für diesen Zweck eine Blockchain as a Service (BaaS) an. Die Blockchain wird auf alle teilnehmenden Firmen verteilt und erzeugt so die Dezentralität. Je mehr Firmen das Angebot nutzen, umso sicherer ist letztendlich auch die Blockchain. Ein weiter Anbieter für BaaS ist Ardor. Die Firma verfolgt aber einen anderen Ansatz. Es existiert eine große verteilte Mainchain. Die BaaS-Kunden bekommen eine eigene, in sich geschlossene Childchain, die die Dezentralität der Mainchain für ihre Sicherheit nutzt.

Einen interessanten Anwendungsfall für die Blockchain setzt auch das Projekt Sia um. Nutzer auf der ganzen Welt können dort an andere Nutzer im Netzwerk ihren freien Festplattenplatz vermieten. Den Preis dafür können sie selbst festlegen. Der Vorgang wird über Smart Contracts in der Blockchain des Projektes abgebildet. Es entsteht also eine mit der Blockchain-Technologie verwirklichte Cloud.

Auf die Plätze … fertig … los

Die Blockchain-Technologie steckt noch in den Kinderschuhen und ist ein riesiger Spielplatz für Visionäre. Einige Projekte stehen schon in den Startlöchern, aber viele warten noch auf ihre Entdeckung. Gerade über die Smart Contracts ergibt sich eine Fülle von Anwendungen. Wer am Ende das Rennen für sich entscheidet, wird sich in den nächsten Jahren zeigen. Noch ist der Vorsprung noch nicht so groß. Also am besten Sportschuhe schnüren und loslaufen.