forma futura

Vermögen nachhaltig investieren

seit 2006

Hintergrundpapier

Blockchain

forma futura

Zusammenfassung

Im Zuge der digitalen Transformation ist die Blockchain-Technologie ein vielbeachtetes Element. Ihr Aufbau und die Funktionsweise tragen ein disruptives Potenzial in sich, das herkömmliche Strukturen auf verschiedenen Ebenen umgehen und somit obsolet machen kann.

Die Kerneigenschaften der Blockchain-Technologie sind Transparenz, Dezentralität und Sicherheit vor Manipulationen. Diese Eigenschaften bieten Chancen, das heutige Wirtschaftssystem über verschiedene Zugänge nachhaltiger zu gestalten.

Doch wie so oft gilt es genau hinzuschauen, da bei der Umsetzung sowie bei der Skalierung Effekte entstehen können, welche die positiven Aspekte überlagern. Ein prominentes Beispiel, wo ein solcher Skalierungseffekt zu extremen Auswüchsen geführt hat, ist Bitcoin. Genauer geht es um den Energieverbrauch, den das Bitcoin-Netzwerk verursacht und der praktisch täglich zunimmt. Zurzeit wird die Jahresproduktion von rund sechs KKW Gösgen pro Jahr verbraucht.

Es ist wichtig hervorzuheben, dass Kryptowährungen nur eine Anwendung der Blockchain-Technologie sind, das mögliche Potenzial jedoch viel breiter ist. Beispiele gibt es bereits in Bezug auf Lieferketten oder in der Versicherungsbranche. Andere angedachte Anwendungen behandeln die Fake News Problematik oder sehen Wege vor, wie Geräte über das Internet of Things (IoT) miteinander kommunizieren und selbstständig verhandeln können.

Für Forma Futura bedeutet es, die Entwicklung genau zu beobachten und jede Anwendung umfassend zu betrachten, so dass positive und negative Effekte beleuchtet und gegeneinander aufgewogen werden können.

forma futura

Inhaltsverzeichnis

Einleitung

Im Zuge der digitalen Transformation stösst man immer häufiger auf den Begriff der Blockchain-Technologie und deren Potenzial, als disruptives Element herkömmliche Strukturen auszuhebeln. Die Grundlage für diese Technologie wurde bereits Anfang der 90er Jahre des letzten Jahrhunderts beschrieben. Eine breitere Wahrnehmung in der Öffentlichkeit entstand jedoch erst durch die auf der Blockchain-Technologie basierenden Kryptowährung Bitcoin (BTC), welche 2009 entstanden ist.

Die disruptive Kraft ergibt sich aus zwei grundlegenden Eigenschaften: Transparenz und Dezentralität. Insbesondere die Dezentralität ist der Hebel, der bisherige Geschäftsmodelle ins Wanken bringen könnte. Aufgaben, welche bisher von einem zentralen Organ, wie beispielsweise einer Bank übernommen wurden, können nun im kollektiven Netzwerk aller Benutzenden gelöst werden.

Eine weitere grundlegende Eigenschaft einer Blockchain ist die Verschlüsselung (Kryptografie), woraus sich der Name Kryptowährung ableitet. Zusammen mit der Dezentralisierung, der Verteilung der Informationen auf alle Beteiligten, ergibt sich ein hohes Mass an Sicherheit.

Eine Blockchain (Block-Kette) ist einfach gesagt ein Buchhaltungssystem bzw. ein Verzeichnis für Transaktionen und die Information, was übertragen wird. Jeder Block dieser Kette enthält mindestens die Angaben zu einer Anzahl von Transaktionen sowie die Information über alle vorangehenden Blöcke. Ein neuer Block wird mittels einer mathematischen, sogenannten Hashfunktion verschlüsselt, wodurch aus allen Eingabeinformationen ein Hashwert berechnet wird, der immer dieselbe Länge (Anzahl Bit) hat.

Es ist dieser Hashwert (eine Abfolge aus Zahlen und Buchstaben), der in den darauffolgenden Block eingebaut wird und als Information über alle vorangegangenen Blöcke gilt. Sobald ein Block bearbeitet wurde und dessen Hashwert feststeht, muss dieser verifiziert werden, damit er anschliessend versiegelt werden kann. Ab diesem Zeitpunkt ist der Block fest in die Kette integriert und unveränderlich. Für die Verifizierung der Blöcke gibt es verschiedene Konsensusmethoden mit entsprechenden Vor- und Nachteilen. So variieren diese unter anderem im Stromverbrauch, der Geschwindigkeit und der Sicherheit.

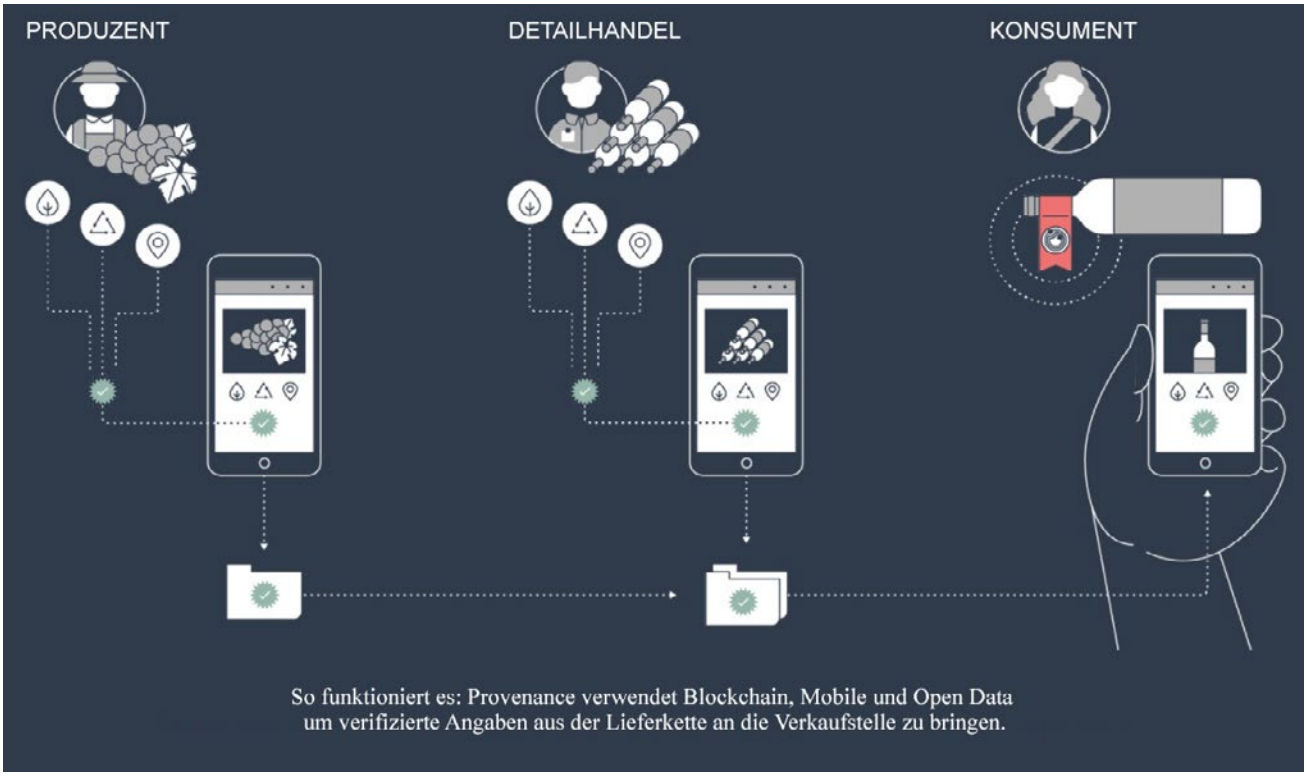
Die Blockchain-Technologie als Chance für die Nachhaltigkeit

Die grundlegenden Eigenschaften der Blockchain-Technologie, Transparenz, Dezentralität und die Resistenz gegenüber Manipulationen bieten allesamt Chancen, die Wirtschaft auf verschiedenen Ebenen nachhaltiger zu gestalten. Auf der anderen Seite ist es zentral, wie die Technologie effektiv implementiert wird. Ein Beispiel dafür ist die bereits erwähnte Konsensusmethode, die, wie im Fall von Bitcoin, zu einem enormen Ressourcenverbrauch führen kann. Hinzu kommt, dass mit dem disruptiven Charakter neue Herausforderungen entstehen. Herkömmliche Regulationen greifen nicht mehr und neue können erst entstehen, wenn verstanden wird, wo und für welche Aspekte diese benötigt werden.

Die Blockchain als Infrastruktur

Ein naheliegendes Einsatzgebiet, wo Transparenz eine massgebliche Verbesserung der heutigen Probleme bringen könnte, ist die Lieferkette. Befasst man sich beispielsweise mit Palmöl oder Konfliktmineralien, wird schnell klar, dass die Rückverfolgbarkeit bis zur Quelle ein zentrales Anliegen ist. Aber auch bei Lebensmitteln oder Textilien steigt das Bedürfnis, die Herkunft zu kennen. Eine Firma, die diesbezüglich eine Lösung anbietet, ist Provenance.

Auf ihrer Plattform können Produktinformationen ab ihrem Ursprung bis zum Ziel, wo das Produkt verkauft wird, digital erfasst und dort vom interessierten Käufer abgerufen werden.



Quelle: https://www.provenance.org/how-it-works

Die Eigenschaften der Blockchain-Technologie finden auch in sogenannten **«Smart Contracts»** ihren Einsatz. **Diese Verträge werden automatisch ausgeführt, wenn die Bedingungen von den Vertragspartnern erfüllt werden.** Diese Erfordernisse stehen in der Blockchain, was sie vor einer Manipulation schützt. **Die Vertragsklauseln können vom Blockchain-Netzwerk selbst überprüft und ausgeführt werden, was die Beteiligung einer Drittpartei überflüssig macht.** Dies setzt natürlich voraus, dass alle benötigten Daten in digitaler Form vorhanden sind.

Unseren Erachtens birgt dieser Punkt eine grosse Herausforderung an die Manipulationssicherheit der Blockchain-Technologie. **Der Übergang von der physischen in die digitale Welt ist vermutlich die grösste Sicherheitslücke, wo Daten manipuliert werden können.** Smart Contracts versprechen, die Prozesse kostengünstiger, schneller, weniger fehleranfällig und transparenter zu gestalten.

Ein prominentes Beispiel einer Plattform, auf der Smart Contracts ausgeführt werden können, ist Ethereum. Genauer gesagt, ist Ethereum die Blockchain, die als dezentralisierte Infrastruktur angesehen werden kann, auf der die Smart Contracts ausgeführt werden. Damit diese Infrastruktur genutzt werden kann, benötigt man lediglich «Ether», der als Kryptowährung gehandelt wird. Es ist sozusagen die Zugangsberechtigung zur Ethereum-Blockchain, damit dort Einträge gemacht werden können.

So gibt es verschiedene Anbieter, welche Dienstleistungen oder Produkte anbieten, welche auf der Ethereum Blockchain aufbauen und diese Infrastruktur als Fundament verwenden. Ein Beispiel ist das **Startup ChainThat, welches eine Blockchain-Lösung für Versicherungen und Rückversicherungen anbietet.** Dieses soll die Verhandlungen zwischen den Versicherern, Rückversicherern und Versicherungsmaklern erleichtern, sowie die Transparenz und die Geschwindigkeit der Abläufe erhöhen.

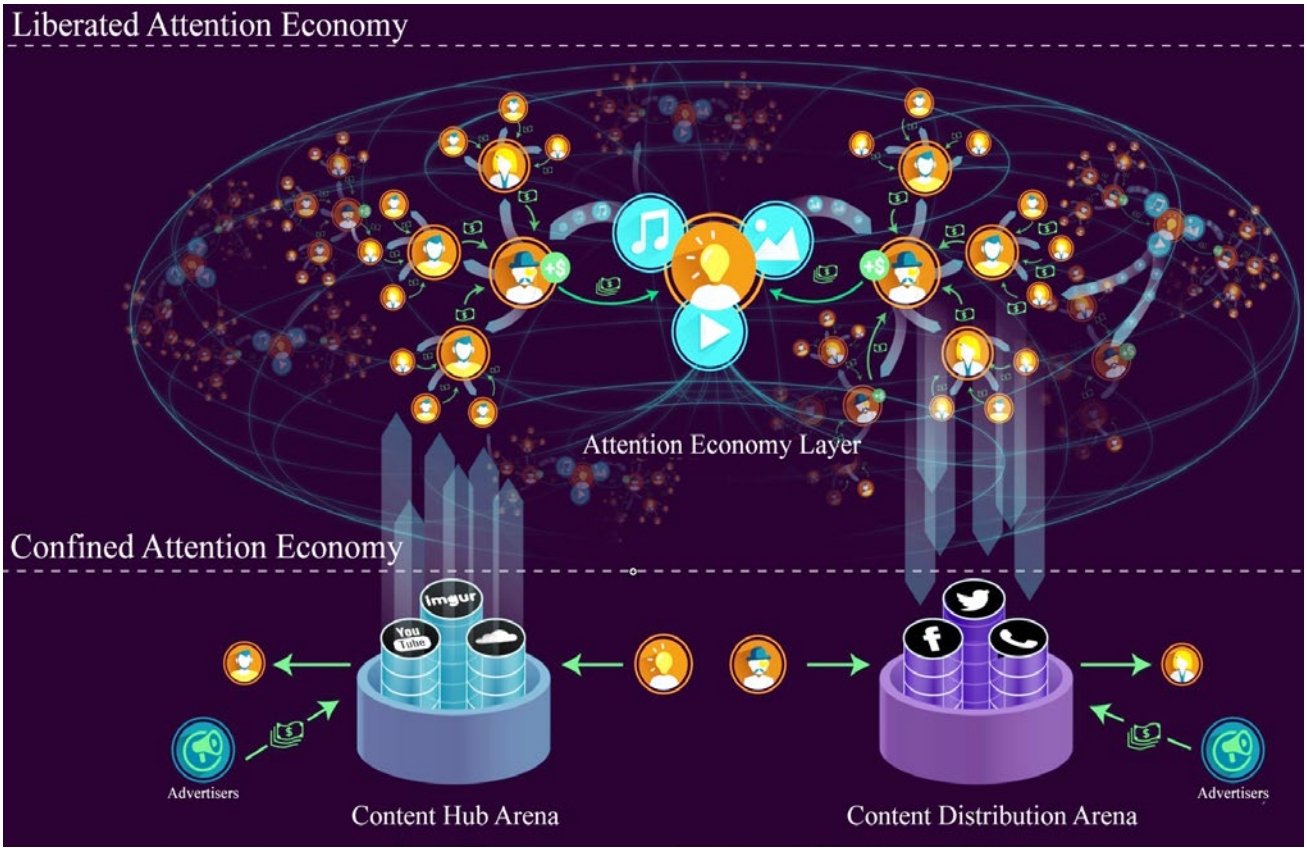
Verschiedene Anwendungen von Kryptowährungen

Am Beispiel der Ethereum-Blockchain und dem dazugehörigen «Ether» zeigt sich ein Mechanismus, der von vielen Anwendungen, welche die Blockchain-Technologie nutzen, verwendet wird. Mit der Einführung einer eigenen Kryptowährung wird die Unabhängigkeit von Drittparteien auch auf das Zahlungssystem übertragen. Zusätzlich entsteht eine Zweckgebundenheit, so dass die Kryptowährung nur für die vorgesehenen Anwendungen innerhalb des spezifischen Blockchain Netzwerks genutzt werden kann.

Ein Beispiel, das diesen Mechanismus verdeutlicht, stammt von der Firma Synereo mit der Anwendung «WildSpark». Synereo spricht ein Problem an, welches mit dem Internet exponentiell zugenommen hat: Die Verteilung von Gewinn, der mittels Inhalt geschaffen wird.

Konkret bedeutet es, dass Autoren von Inhalt, der im World Wide Web hochgeladen wird, gerecht entlöhnt werden. Zusätzlich sollen auch die Verbreiter, die sogenannten Kuratoren, dafür belohnt werden, dass sie Inhalte weiterverbreiten. In der heutigen Form sind es die Plattformen, wie Youtube, Facebook oder Instagram, welche den Löwenanteil des Gewinns abschöpfen, der durch die freiwillige und kostenlose Veröffentlichung von Inhalten entsteht.

Die Entlöhnung erfolgt über die eigene Kryptowährung «AMP». Mitglieder des Netzwerks können Inhalte wie Musik, Videos oder Texte, die sie mögen, mit einer gewissen Summe von AMPs belohnen. Dadurch werden sie selbst zu Kuratoren des Inhalts, den sie belohnt haben. Diese AMPs werden dann nach einem definierten Schema an den Autor/die Autorin sowie an die Kuratoren des Inhalts verteilt.



Quelle: https://blog.synereo.com/2017/03/27/a-liberated-network-is-born

Dadurch soll ein Netzwerk geschaffen werden, welches ohne den Einbezug einer Drittpartei hochgeladene Daten aufgrund ihrer Relevanz oder Beliebtheit entlöhnt und somit auch bewertet. Dieser zweite Teil, die Bewertung, soll auch gegen die Verbreitung von Fake News angewendet werden.

Das polnische Startup «Userfeeds» hat genau das im Sinn. Im Gegensatz zu heutigen Systemen von Links, Likes und Upvotes, welche zur Bewertung von Inhalten genutzt werden und über einen zentralen Anbieter kontrolliert werden, kann die Blockchain Lösung aufgrund ihrer Dezentralität und Transparenz vor Manipulationen schützen. Somit schliesst sich ein grosses Einfallstor für Fake News, einer Problematik, welche sich mit dem Internet enorm verschärft hat.

Gute Beispiele für die Anwendung einer Kryptowährung unter Berücksichtigung der Nachhaltigkeit sind SolarCoin oder FairCoin. Der SolarCoin wurde ins Leben gerufen mit der Intention, die Produktion von Solarstrom mit einem zusätzlichen Anreiz zu steigern. Grundsätzlich kann sich jeder am SolarCoin-Netzwerk beteiligen.

Als Besitzer einer Photovoltaikanlage (PVA) und Mitglied des SolarCoin-Netzwerks wird die Produktion einer MWh Solarstrom mit einem Solarcoin belohnt. Das Netzwerk richtet sich auch an die Monteure von PVA. Diese werden belohnt, wenn sie ihre Kunden für das SolarCoin-Netzwerk gewinnen können. Mit SolarCoin sollen Dienstleistungen und Produkte anderer Mitglieder des Netzwerks gekauft werden können. SolarCoin können aber auch an verschiedenen online-Börsen gegen andere Kryptowährungen oder konventionelle Währungen gehandelt werden.

Der FairCoin ist eine Kryptowährung, die 2014 aus dem FairCoop-Netzwerk entstanden ist. Die Vision von FairCoop ist es, ein globales Netzwerk von selbstorganisierten und selbstbestimmten lokalen Gemeinschaften und Individuen zu bilden.

Es geht dabei um Zusammenarbeit, Ethik, Solidarität und Transparenz. In diesem unabhängigen Ökosystem soll ein neues Wirtschaftssystem entstehen, das dezentral, basisdemokratisch und ohne Zentralgewalt funktionieren soll. Der FairCoin ist die Währung dieses Systems.

Einen Einblick, was mit dem FairCoin bereits gekauft werden kann, gibt es auf der online-Plattform FairMarket, wo verschiedene Produkte aus 23 Ländern, inklusive der Schweiz, angeboten werden. Es ist zudem möglich, selbst Produkte anzubieten.

Damit es nicht zu Kursschwankungen wie bei Bitcoin oder anderen Kryptowährungen kommt, soll die Mehrheit der FairCoins innerhalb des FairCoop-Netzwerks bleiben. Lediglich 17 Prozent aller FairCoins werden ausserhalb des FairCoop-Ökosystems gehandelt[1].

Kooperation bildet beim FairCoin auch das Rückgrat der Konsensusmethode, die Proof-of-Cooperation Methode. Die Erlaubnis zur Generierung des nächsten Blocks wird abwechslungsweise unter den sogenannten Cooperatively Validated Nodes (CVN) verteilt. Im Gegensatz zu anderen Kryptowährungen entstehen durch die Berechnung eines neuen Blocks keine neuen FairCoins. So entsteht kein Wettbewerb und es ist keine spezialisierte Hardware nötig, was zu einem Bruchteil des Stromverbrauchs führt.

1 https://fair-coin.org/en/faircoin-faqs

IOTA ist ein weiteres Beispiel das sich die Etablierung eines neuen Wirtschaftssystems auf die Fahne geschrieben hat. Dieses System soll auf das Internet der Dinge (IoT) angewendet werden.

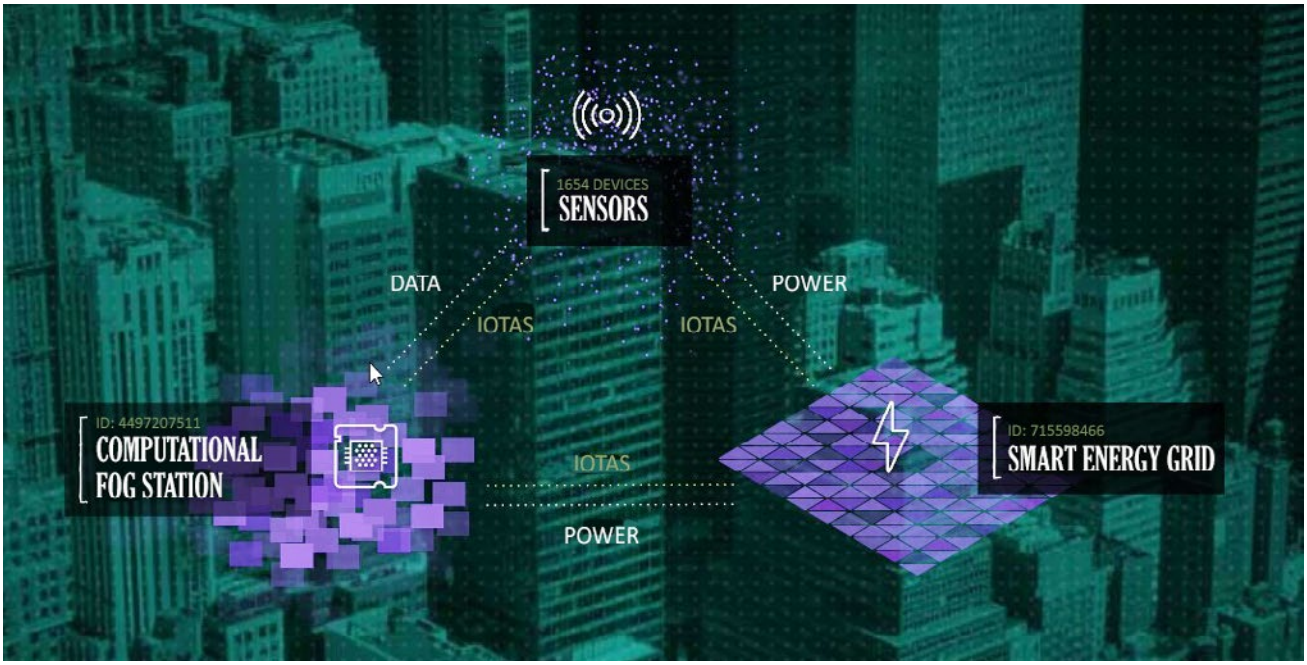
In dem Netzwerk aus Geräten, die über das Internet verbunden sind, soll die IOTA-Blockchain die Grundlage für Datenaustausch, Verhandlungen und Bezahlung sein. Es geht soweit, dass diese Geräte selbstständig miteinander kommunizieren, Daten austauschen, Verhandlungen führen und den Zahlungsverkehr abwickeln. **IOTA schwebt vor, die «Sharing Economy» als vorherrschendes Geschäftsmodell zu etablieren.**

Aus Nachhaltigkeitssicht wäre eine solche Entwicklung zu begrüssen, da damit auch bessere Grundlagen für eine Kreislaufwirtschaft geschaffen werden. Denn sobald ein Produkt nicht mehr als Ganzes verkauft wird, sondern lediglich seine Dienstleistung, ist die Langlebigkeit wieder ein Vorteil. Zudem lohnt es sich, die Produkte so zu entwickeln, dass sie möglichst repariert, wiederverwertet und zuletzt rezykliert werden können.

Neben diesen neuen Firmen und Startups, deren Geschäftsmodell Anwendungen der Blockchain-Technologie im Kern tragen, gibt es auch Beispiele etablierter Firmen, die das Potenzial dieser Technologie für ihre Geschäfte nutzen möchten.

Ein prominentes Beispiel ist IBM, die sich in Bezug auf Blockchain-Technologie als Serviceanbieter versteht. Mit der IBM-Blockchain-Plattform ist es jedem möglich, seine Ideen für die Anwendung einer Blockchain zu testen und gegebenenfalls zu skalieren. IBM hat bereits Blockchain-Lösungen zusammen mit der Transportfirma Maersk, der Stadt Dubai, der Food and Drug Administration (FDA) oder der Bank Standard Chartered entwickelt.

AXA ist die erste grosse Versicherungsgesellschaft, welche mit fizzy eine Flugverspätungsversicherung anbietet, die komplett auf Blockchain basiert. Als Serviceanbieter versteht sich auch SAP, die mit Blockchain-as-a-Service registrierten Kunden die Möglichkeit bietet, Blockchain-Lösungen für ihren Geschäftsbereich zu testen. Das Augenmerk von SAP liegt in der Kombination der Blockchain mit dem IoT.



Quelle: https://iota.org

Meinung von Forma Futura

Wie die verschiedenen Beispiele andeuten, birgt der Einsatz der Blockchain-Technologie Chancen für die Nachhaltigkeit, die sich auf verschiedenen Ebenen zeigen können.

Es gilt jedoch die Umsetzung genau und mit kritischen Augen zu beobachten. Der exorbitante Stromverbrauch des Bitcoin-Netzwerks ist ein prominentes Beispiel für Probleme, die es im Sinne der Nachhaltigkeit zu verhindern gilt.

Aufgrund des disruptiven Charakters dieser Technologie werden sich gewisse Problemfelder wohl auch erst während der Anwendung manifestieren, da eine Einschätzung mit dem bisherigen Wissen nur begrenzt möglich ist. Umso wichtiger ist es, in der Euphorie einen kühlen Kopf zu bewahren und die Heilsversprechen nüchtern zu betrachten. Gewisse Chancen entpuppen sich möglicherweise als weniger effektiv als angenommen, so dass deren negative Effekte dann wieder stärker ins Gewicht fallen.

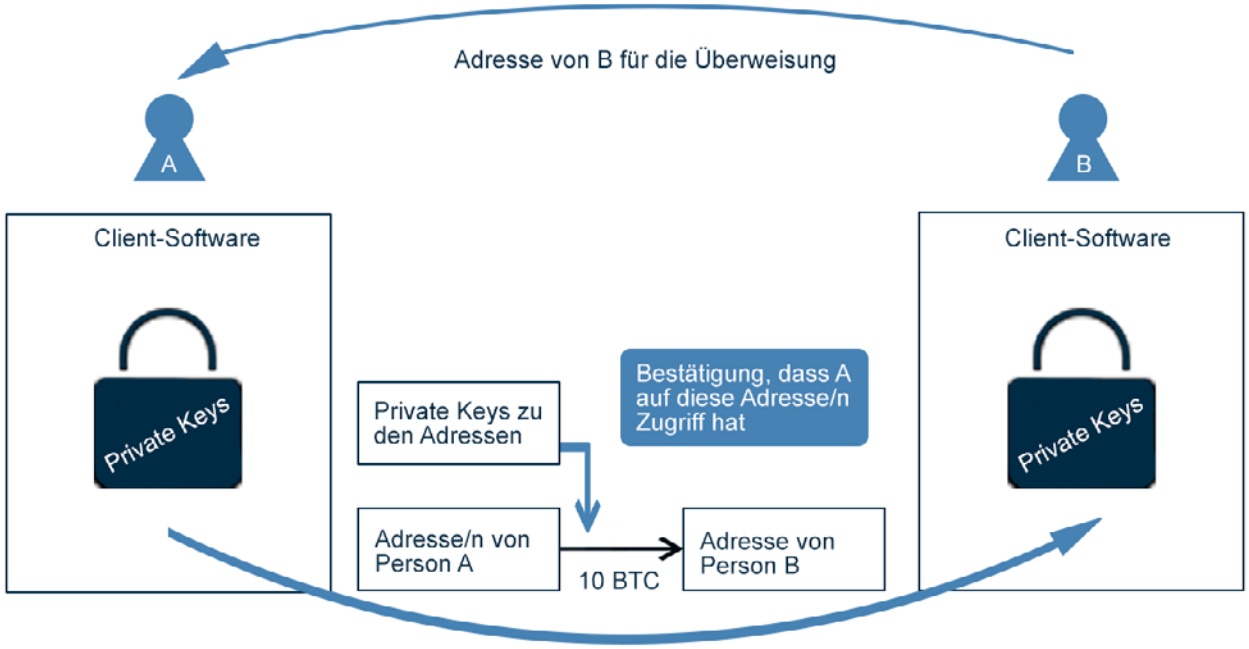
Im Rahmen der Nachhaltigkeitsanalysen bei Forma Futura gilt es, diese verschiedenen Aspekte zu berücksichtigen und genau hinzuschauen sowie im Engagement mit den Unternehmen mögliche Chancen und Risiken zu thematisieren.

In Bezug auf Kryptowährungen vermuten wir, dass sich das regulatorische Umfeld verschärfen wird. Denn mit dem steigenden Wert und der Anzahl von Kryptowährungen im Umlauf sind Themen wie Steuerhinterziehung, Schwarzgeld und Betrug nicht mehr zu vernachlässigen. Zudem werden vermutlich vermehrt Hacker versuchen, bestehende Sicherheitslücken auszunutzen. Dabei ist nicht die Blockchain an sich gemeint, die manipuliert wird. Vielmehr geht es um die Zugangsdaten, respektive den privaten Schlüssel.

Ein hoher Preis, der für die Dezentralität beziehungsweise die Absenz einer Drittpartei bezahlt wird: Es gibt keine Ansprechperson, an die man sich wenden kann. Gehen die Zugangsdaten verloren, sei es durch Diebstahl oder Fahrlässigkeit, gibt es keine Möglichkeit, seine Zugangsdaten zurückzusetzen oder auf einem anderen Weg das verlorene Guthaben zurückzuerhalten. Dies gilt grundsätzlich für alle Anwendungen der Blockchain, vermutlich sind es aber die Kryptowährungen, bei welchen dieses Problem am stärksten ins Gewicht fällt.

In Bezug auf Investitionen in Kryptowährungen ist zu bedenken, dass diese aufgrund der hohen Volatilität lediglich für Spielernaturen geeignet sind. Zudem sollte man sich bewusst sein, dass hier viel Schwarzgeld im Spiel sein kann und dass man z. B. mit dem Kauf von Bitcoins klimaschädliche Auswirkungen unterstützt.

Wie funktioniert eine Blockchain?



Transaktionsvorgang

Doch schauen wir uns die Funktionsweise der Blockchain am Beispiel Bitcoin an. Nehmen wir an, Person A möchte Person B 10 Bitcoins (BTC) überweisen. Voraussetzung dafür ist, dass beide Personen Mitglied des Bitcoin-Netzwerkes sind, die auch Knoten («nodes») genannt werden.

Dazu wird eine entsprechende Client-Software benötigt, welche auch als «wallet» (Brieftasche) dient. In dieser Brieftasche werden bei jeder Person die privaten Schlüssel (ein Code aus Buchstaben und Zahlen) gespeichert, aus denen die entsprechenden Adressen berechnet werden können.

Eine solche Adresse ist öffentlich einsehbar, während der private Schlüssel die Bestätigung ist, dass man auf die Bitcoins, die auf dieser Adresse liegen, Zugriff hat. Es ist hervorzuheben, dass eine Adresse nicht als Pendant zu einer Kontonummer angesehen werden darf. Denn es wird empfohlen, für jede Transaktion eine neue Adresse zu verwenden.

Ein anderes Beispiel, welches den Unterschied zwischen einer Kontonummer und einer Bitcoin-Adresse verdeutlicht, ist das Folgende: Auf einer Adresse befinden sich fünf Bitcoins. Von dieser Adresse wird nun ein Bitcoin an eine andere Adresse überwiesen. Die restlichen vier Bitcoins bleiben nun nicht auf der Ausgangsadresse liegen, sondern werden an eine dritte Adresse gesendet. Der Auftraggeber muss diese definieren, da sie sonst an eine zufällige Adresse übertragen werden. In diesem Fall ist das «Rückgeld» für den Auftraggeber verloren, da er nicht im Besitz des zugehörigen privaten Schlüssels ist.

Die Brieftasche kann am ehesten mit einem Konto verglichen werden, da darin alle privaten Schlüssel zum eigenen Bitcoin-Besitz abgelegt werden können.

Doch zurück zu unserem Beispiel, bei dem Person A 10 Bitcoins an Person B überweisen möchte. Dazu benötigt Person A eine Adresse von Person B, an die sie den Betrag senden kann. Wird nun von Person A der Auftrag für die Überweisung der 10 Bitcoins aus einer oder mehreren ihrer Adressen an die von Person B erhaltene Adresse über die Client-Software abgeschickt, wird abschliessend die Transaktion mit den privaten Schlüsseln aller Sender-Adressen signiert.

Überprüfung und Ausführung der Transaktion

Diese Transaktionsinformation wird nun an die nächsten verbundenen Knoten, d.h. andere Bitcoin-Nutzer, gesendet. Handelt es sich dabei um sogenannte «full nodes», wird die Transaktion gemäss den Konsensusregeln überprüft.

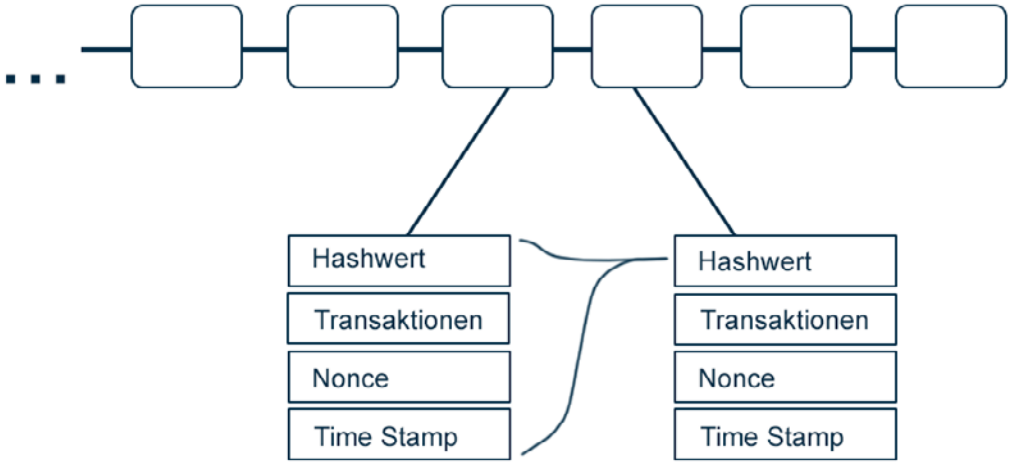
Dazu gehört, dass die Bitcoins vorhanden sind, dass die Schlüssel zu den entsprechenden Adressen passen sowie andere Regeln, welche Stabilität und Sicherheit des Netzwerks sicherstellen.

Wird die Transaktion bestätigt, senden die «full nodes» die Transaktion an die nächsten verbundenen Knoten usw. Damit die Transaktion in einen Block integriert wird und dadurch als ausgeführt gilt, kommt eine weitere Population innerhalb des Bitcoin-Netzwerks ins Spiel: die sogenannten «Miners».

Diese bearbeiten bzw. berechnen die Blöcke, die in die Blockchain gehängt werden. Wie bereits angesprochen, gilt ein Block als bearbeitet, wenn sein Hashwert feststeht. Die Vorgabe des Bitcoin-Netzwerks ist, dass die Hashwerte jedes Blocks kleiner oder gleich gross wie ein vorgegebener Zielwert sind. Es ist nun die Aufgabe der «Miners», diesen Hashwert zu finden respektive den sogenannten «Nonce», ein Wert, der sich im Block befindet und der verrechnet mit den anderen Werten im Block den Hashwert ergibt.

Der «Nonce» ist also eine Variable, mit deren Hilfe das Resultat bzw. der Hashwert beeinflusst werden kann. Das Lösen dieser Aufgabe lässt sich mit einer Lotterie vergleichen, wobei das Berechnen eines Hashwerts einer Ziehung entspricht. Die Aufgabe wäre dann beispielsweise, aus einem Sack mit 50 Kugeln, die mit 1 bis 50 beschriftet sind, eine Kugel zu ziehen, welche den Wert 20 oder kleiner hat.

Je kleiner dieser Zielwert ist, desto kleiner ist die Wahrscheinlichkeit, eine richtige Kugel zu ziehen. Nun enthält dieser Sack aber eine hohe Anzahl Kugeln (ca. 10^{77}), was einen grösseren Spielraum lässt, die Schwierigkeit respektive die Wahrscheinlichkeit anzupassen. Wurde ein Resultat gefunden, ist dieses schnell und ohne grosse Rechenleistung überprüft. Der erste «Miner», der eine Lösung gefunden hat, wird mit einer bestimmten Anzahl Bitcoins belohnt.



Mechanismen des «Schürfens»

Nach 2'016 Blöcken, die der Kette angehängt wurden, wird der Schwierigkeitsgrad der Aufgabe angepasst, so dass die Generierung eines Blocks stets etwa 10 Minuten benötigt.

Auch die Belohnung für das erfolgreiche Schürfen eines Blocks passt sich im Laufe der Zeit an. Alle 210'000 Blocks wird der Bitcoin-Betrag, der als Belohnung neu geschaffen wird, halbiert. Das entspricht einer Halbierung der Belohnung etwa alle vier Jahre. Zu Beginn waren dies 50 Bitcoins, mittlerweile sind es 12,5. Diese Vorgaben ergeben, dass es höchstens 21 Mio. Bitcoins geben wird, was im Jahr 2140 erreicht sein wird[2].

Neben der festen Belohnung aus neu geschaffenen Bitcoins werden auch Transaktionsgebühren erhoben, welche ebenfalls der «Miner» erhält. Auf der einen Seite dienen diese Transaktionsgebühren dazu, dass Transaktionen nicht leichtfertig in Auftrag gegeben werden, was vor falschen Transaktionen, welche das System zum Erliegen bringen könnten, schützen soll.

Auf der anderen Seite ergibt sich aus diesen Gebühren auch eine Priorisierung der Transaktionen, da ein «Miner» entscheiden kann, welche Transaktionen er in den Block, den er bearbeitet, integrieren möchte. So werden die Transaktionen, welche die höchsten Gebühren generieren, bevorzugt und somit am schnellsten bearbeitet. Die Höhe der Transaktionsgebühr kann der Auftraggeber selbst festlegen.

Da die Bearbeitung von Blöcken ein Wettrennen unter den «Minern» ist, gilt ein Block und damit auch sein Inhalt erst als gesichert, wenn dieser mit einer gewissen Tiefe in der Blockchain eingebettet ist. Aus der Wahrscheinlichkeitsrechnung gilt eine Tiefe von sechs Blöcken als gesichert. Somit folgen dem angesprochenen Block sechs weitere Blöcke.

Aufgrund des Wettrennens und der Dezentralität ist es möglich, dass Blockchains mit verschiedenen Enden bestehen. Kommt es an einem Knoten (Mitglied des Bitcoin-Netzwerks) zu einem Widerspruch, das heisst, die neue Kette passt nicht in die Abfolge der alten Kette, so zählt die Version, in der mehr Rechenleistung steckt. Dies entspricht der längsten Blockchain.

Methoden zur Validierung von Transaktionen

Die Konsensusmethode, mit der ein Block in die Blockchain des Bitcoin-Netzwerks integriert wird, nennt sich «proof of work». Das heisst, die Berechnung eines neuen Blocks, respektive seine Verschlüsselung in einen Hashwert, der den Kriterien entspricht, ist zeitintensiv und verursacht Kosten in Form der Energie, welche für die Rechenleistung benötigt wird.

Die Überprüfung wiederum ist einfach und schnell. Die Sicherheit der Blockchain wird massgeblich durch die Konsensusmethode bestimmt, mit der ein Block in die Kette eingebaut wird. Mit Sicherheit ist der Schutz vor einer Manipulation der Daten, die auf der Blockchain liegen, gemeint. Im Fall von «proof of work» ist es die Energie, respektive Zeit, die in die Bearbeitung eines Blocks gesteckt werden muss, welche eine Manipulation verhindern soll. Möchte ein Angreifer die Daten eines Blocks manipulieren, so muss er diesen sowie jeden darauffolgenden Block neu berechnen.

In dieser Zeit arbeiten jedoch alle anderen «Miner» an der korrekten Kette weiter. Damit die manipulierte Kette des Angreifers vom Netzwerk übernommen wird, muss diese länger sein als die korrekte Kette. Dazu müsste die Rechenleistung des Angreifers diejenige aller restlichen «Miner» übersteigen, damit er dieses Rennen für sich entscheiden kann. Mit steigender Anzahl an «Minern» sinkt diese Gefahr.

2 https://en.bitcoin.it/wiki/how_bitcoin_works

«Proof of work» ist bei einer entsprechenden Population an «Minern» sehr sicher, jedoch birgt diese Sicherheit einem enormen Energieverbrauch. Dieser steigt praktisch täglich und wird durch den rasant steigenden Preis, der für einen Bitcoin bezahlt wird, weiter angetrieben.

Mit steigendem Preis steigt auch der Anreiz, an dieser Entwicklung mitzuverdienen. Mittlerweile wird der komplette Stromverbrauch des Bitcoin-Netzwerks auf 50,4 TWh pro Jahr geschätzt (Stand Februar 2018). 2014 produzierte das KKW Gösgen 8 TWh Strom. Verglichen mit dem Stromverbrauch von Ländern liegt Bitcoin auf Rang 51 zwischen Portugal und Usbekistan[3].

Da die Sicherheit einer Blockchain direkt von der Konsensusmethode abhängig ist, muss diese sorgfältig gewählt werden. Es gilt, eine Hürde zu wählen, die gerade so hoch ist, dass der Versuch einer Manipulation unattraktiv wird. Gleichzeitig muss es sich jedoch für die ehrlichen «Miner» auch lohnen, Arbeit in das Netzwerk zu stecken.

Andere Konsensusmethoden, die sich «proof of stake» oder «proof of burn» nennen, sind dabei weniger energieintensiv als die «proof of work»-Methode.

In der «proof of stake»-Methode wird das Recht, einen Block zu bearbeiten, anhand der Höhe des eigenen «Kontostandes» verteilt. Die Hürde bzw. Kosten, die ein «Miner» hier überwinden bzw. übernehmen muss, ist eine massgebliche Beteiligung an dem entsprechenden Blockchain-Netzwerk. Die Motivation, dem Netzwerk zu schaden, soll durch die signifikante eigene Beteiligung zusätzlich reduziert werden.

Unter «proof of burn» bestehen die Kosten darin, dass ein festgelegter Betrag einer anderen Kryptowährung «vernichtet» werden muss, um die Schürfrechte auf einen Block zu erhalten. Vernichten ist in dem Sinn gemeint, dass der festgelegte Betrag an eine Adresse gesendet wird, auf die niemand Zugriff hat, da es dazu keinen passenden Schlüssel gibt.

Bei jeder dieser Methoden gestaltet sich die Gefahr einer Manipulation der Blockchain sowie die Menge an realen Ressourcen, die zur Verhinderung dieser Gefahr aufgewendet werden müssen, etwas anders.

3 https://digiconomist.net/bitcoin-energy-consumption

forma futura

Quellenverzeichnis

(letzter Aufruf 08.02.18)

https://en.bitcoin.it/wiki/main_page

https://www.coindesk.com/

https://digiconomist.net/

https://www.provenance.org/

https://ethereum.org/

https://chainthat.com/

https://www.synereo.com/

https://userfeeds.io/

https://solarcoin.org/

https://fair-coin.org/

https://fair.coop/de

https://market.fair.coop/de_de/

https://iota.org/

Autor

Balthasar Bänninger
ist stellvertretender Leiter
Nachhaltigkeitsresearch