

41 Blockchain/Bitcoin und Internet of Things

Die Blockchain-Technologie hat in ihrer konkreten Anwendung in der Kryptographie-Währung „Bitcoin“ öffentliche Wahrnehmung erlangt. Dabei ist jedoch untergegangen, dass es viele andere Anwendungsbereiche für öffentliche Reputationssysteme gibt die nicht unmittelbar im Finanzbereich liegen. Eine sehr stark wachsende Gruppe von Anwendungen betrifft Industrie 4.0 und zwar im Bereich „Internet of Things“.

Blockchain wendet das mathematische Prinzip der sog. Dirichlet-Reputation an. Dabei geht es darum, die Authentisierung einer Transaktion nicht von einer zentralen Wahrheitsfindungs-Maschine anhängig zu machen, sondern von einem dezentralen Wahrheitscluster. Die bevorzugte Wahrheitstheorie solcher Systeme ist die Korrespondenz-Wahrheit in Verbindung mit der Konsensus-Wahrheit (siehe WHSTA-IHI-Bericht 2006).

Der geometrische Aufbau einer Blockchain entspricht der digitalen Jordankurve (63. IHI Bericht) wobei die Kette durch die Kausalität der aufeinanderfolgenden Transaktionen gebildet wird. Zwischen den Knoten der Blockchain findet ein Anerkennungsprozess (Wahrheitsprüfung) statt, der nicht von einer zentralen, dazu ermächtigten „Wahrheitsmaschine“ (Gericht, Behörde) ausgeführt wird sondern nach fixen mathematischen Regeln von der Summe aller funktional benachbarten Netzwerkknoten. Dieser Vorgang wird vom jeweiligen Blockchain-Protokoll festgelegt.

In Wirklichkeit wird nicht der Transaktionsakt als solcher geprüft und verbucht, sondern ein zugehöriger kryptografischer Schlüssel. Dadurch basiert die Blockchain auf der bewährten Methode der asymmetrischen Verschlüsselung (z.B. RSA), wie sie derzeit für praktisch alle Finanztransaktionen im Internet Verwendung findet.

Wahrheitsstrukturanalytisch im Sinne der HI-Axiome ist interessant, dass Blockchain strikt nach der Konsensuswahrheit vorgeht, Nur wenn die Peer-to-Peer-Transaktion von einer ausreichenden Zahl anderer Rechner als wahr anerkannt wird kann sie ausgeführt werden.

Wikipedia drückt das so aus: unter einer Blockchain (auch Block Chain, englisch für Blockkette) wird eine verteilte Datenbank verstanden, die eine erweiterbare Liste von Datensätzen enthält und deren Integrität (Sicherung gegen nachträgliche Manipulation) durch Speicherung der (kryptografischen) Prüfsumme des vorangehenden Datensatzes im jeweils nachfolgenden gesichert ist.

Das Verfahren ist die technische Basis für sogenannte Kryptowährungen, kann aber ggf. auch darüber hinaus in verteilten Systemen zur Verbesserung/Vereinfachung der Transaktionssicherheit beitragen (gegenüber zentralen Systemen).

Die Funktionsweise ähnelt dem Journal der Buchführung. Eine Blockchain ermöglicht es, dass in einem dezentralen Netzwerk eine Einigkeit zwischen den Knoten erzielt werden kann.“

Im Wesentlichen handelt es sich also um ein Verbuchungsverfahren in einer verteilten Datenbank. Im Effekt bedeutet das, dass auf eine vermittelnde und überprüfende Instanz bei Peer-to-Peer Transaktionen verzichtet werden kann.

Das IHI hat, um mit der Praxis einer Kryptowährung vertraut zu werden ein Experiment aufgesetzt in dem mehrere sog. Wallets (Brieftaschen) eingerichtet wurden. Anschließend wurden einige Euros in Bitcoin-Bruchteile umgetauscht und in die Wallets verteilt. Da der Kurs für ein Bitcoin zum Zeitpunkt

des Projektstarts mit 537,57 EUR/BC notierte (Kraken), wurden nur einige Zehntel und Hundertstel eines Bitcoins erworben.

Die erste Erkenntnis des IHI war. Dass sich Bitcoins sehr ähnlich wie Nebenwerte an den Aktienbörsen verhalten. Es kommt nicht nur auf den Zeitpunkt der Notierung an, sondern auch auf den Handelsplatz. So betrug der Kurs am 24.9.2016 am Handelsplatz Bitpay 533,21 EUR aber am Handelsplatz Bitcoin.de 543,55. Immerhin eine Differenz von 1,94%.

Bitcoins sind sehr volatil und ein enger Markt, der sichtlich von Marketmakern kontrolliert wird. Das hat auch etwas damit zu tun, dass es nur eine gedeckelte Anzahl von Bitcoins zu einem gegebenen Zeitpunkt geben kann.

Auch hier wieder Wikipedia: Ein Problem bei der Einführung von Bitcoin als Währung war die anfängliche Verteilung der Geldeinheiten. Moderne staatliche und private Währungen sind im Gegensatz zu Bitcoin durch ein Zahlungsverprechen der ausgebenden Stelle gedeckt. Da Bitcoin als neues Zahlungsmittel anfangs kein Vertrauen genoss und der Rücktausch von keiner Stelle garantiert wird, waren Bitcoins anfänglich praktisch wertlos. Auch eine Nutzbarkeit war aufgrund des fehlenden Angebots an Waren gegen Bezahlung in Bitcoins zunächst nicht gegeben.

Im Fall von Bitcoin werden neue Einheiten nach einem Prinzip verteilt, das die Unterstützung des Netzwerks durch Bereitstellen von Rechenleistung belohnt (siehe Abschnitt Mining). Eine weitere Eigenschaft des Systems ist es, dass im Laufe der Zeit immer weniger Geldeinheiten erzeugt werden. Dadurch konnten die Teilnehmer in der Anfangsphase des Systems erheblich schneller und mit geringerem Aufwand Geldeinheiten generieren. Mit fortschreitender Zeit und steigender Teilnehmerzahl bzw. Rechenleistung wird es für den einzelnen Teilnehmer zunehmend schwieriger, Bitcoins zu erzeugen.

Im Januar 2015 wurden knapp 21% aller Bitcoins von 100 Adressen bzw. etwa 33% aller Bitcoins von 500 Adressen gehalten“ Zitat Ende.

Das IHI hat mit einem führenden österreichischen Miner ein Interview geführt, um herauszufinden ob Bitcoin-Mining ein Geschäftsfeld für BEKO sein könnte. Dabei kam klar heraus dass Mining mittlerweile eine sehr Energie-aufwendige Angelegenheit geworden ist, weil die mathematischen Berechnungen zur Erzeugung der kryptografischen Schlüssel der ja ein Bitcoin in Wirklichkeit ist so hohe Rechenleistungen erfordern, dass die professionellen Miner inzwischen nicht nur ganz spezielle Hochleistungsrechner-Hardware einsetzen, sondern sich darüber hinaus noch mit einem Stromversorger verbünden, um günstigen Strom zu kaufen weil sich sonst Mining nicht mehr rechnet. Die dem Bitcoin-Protokoll unterlegte Mathematik hat die beabsichtigte Wirkung, dass sich der Rechenaufwand für die Erzeugung neuer Bitcoins asymptotisch gegen Unendlich entwickelt je näher man der geplanten Höchstzahl von 21 Millionen Bitcoins nähert.

Geometrisch wird daher die Bitcoin-Kette zu einer geschlossenen Jordankurve. Das hat die Wirkung, dass nur über Teilung einer fixen Währungsmenge disponiert werden kann und nicht wie bei den derzeit weltweit gültigen Zahlungsmitteln mit einer offenen Jordankurve (Geldmenge). Die Schöpfer des Bitcoin-Systems haben das bewusst so eingeführt, um dieses Zahlungsmittel der Willkür politischer Instanzen zu entziehen.

Selbstverständlich hat diese technische Unabhängigkeit von Behördenwillkür auch Widerstand bei den etablierten Institutionen des Geldwesens ausgelöst, wie das IHI schon bei dem FNSL-Bank-Experiment erlebt hat. Zur Erinnerung: auf BEKO-Island dem virtuellen „Staat“ des Avatars BEKO Kurosawa im Second Life (23. IHI Bericht). Bekanntlich hat das mit der Einstellung des Experimentes geendet, weil unseren beratenden Anwälten die rechtlichen Risiken zu hoch erschienen. Das hatte im Wesentlichen auch damit zu tun, dass Second Life im Gegensatz zu Bitcoin und der Blockchain noch auf einer

Serverfarm lief, die unter die Hoheit der USA stand, weil die Firma Linden Lab. als Second Life Betreiber eine US-Firma ist.

Bei Bitcoin ist die Situation völlig anders. Bitcoin ist ortlos im Internet. Der EuGH hat außerdem über die Frage, ob Bitcoin von der Mehrwertsteuer befreit werden soll oder nicht, am 22. Oktober 2015 eine klare Antwort verfasst und Bitcoin als Währung eingestuft. Damit wird klar, dass beim Kauf oder Verkauf von Bitcoin keine Mehrwertsteuer anfällt.

Inzwischen werden Bitcoins aufführenden Finanzplattformen wie Teletrader als Devisen mit laufenden Kursen öffentlich ausgewiesen. Bitcoin-Broker wie die Firma Coinimal in Wien oder die Bitcoin Group SE in Deutschland handeln mit Devisen gegen Bitcoins in namhaftem Ausmaß. So wurden z.B. am 23.9.2016 laut Bitcoinity 2,42 Mill Bitcoins gehandelt. Zum Kurs von 533 EUR/BC ergibt das einen Umsatz von ca. 1300 Mill EUR.

Um festzustellen, wie das Bitcoin-Business funktioniert, hat das IHI eine explorative Beteiligung als Kleinstaktionär bei der einzigen derzeit in Deutschland an der Börse Düsseldorf notierten Firma Bitcoin Group SE ISIN DE000A1TNV91 eingegangen.

Für dieses Papier spricht der Umstand, dass die operative Tochter der Bitcoin Group SE die Plattform Bitcoin.de betreibt, die ihrerseits eng mit der Münchner Fidor Bank zusammenarbeitet und einer der führenden Bitcoin-Broker ist. Die Fidor Bank wiederum hat sich auf FinTech-Produkte spezialisiert und wurde als deutscher Partner der Firma Payward Inc. in den USA bekannt, die die Bitcoin-Trading-Plattform „Kraken“ betreibt, welche derzeit die umsatzstärkste der Welt ist. Fidor selbst wiederum wurde am 28.7.2016 von der zweitgrößten französischen Bankengruppe BPCE gekauft. BPCE spielt mit ihren 35 Millionen Kunden in Frankreich eine ähnliche Rolle wie die Raiffeisen-Gruppe in Österreich.

Die den Aktionären zustehenden Rechte an Information und Mitsprache werden dazu verwendet, um eine Wissensbasis über dieses neue Phänomen der Internet-Welt aufzubauen.

Dem Zweck des IHI entsprechend ist aber nicht der kaufmännische Aspekt im Vordergrund (für den wäre evtl. die Aufnahme der Aktie ins Portfolio der BEKO Holding von der GF zu erwägen), sondern die theoretischen Grundlagen der Blockchain-Technologie in Verbindung mit dem Problem der Wertzumessung.

Streng theoretisch ist die Blockchain-Technologie eine Anwendung der Omnitopologie wie sie im 62. IHI-Bericht beschrieben wurde. Je nachdem ob eine Blockchain als offene oder als geschlossene Jordankurve strukturiert wurde ergeben sich zwingende mathematische Wirkungsmechanismen. Die Verbindung zur realen Außenwelt findet über den Wertzumessungsakt statt. So ist beispielsweise ein Bitcoin so lange lediglich ein Paar von kryptografischen Schlüsseln als es nicht zu realen Güter austauschen kommt. Erst dann wird der Bitcoin zu wirklichem Geld. Das Gleiche gilt übrigens auch für jede andere Währung (Fiat-Geld) so sie keine fixe Golddeckung hat (Vollgeld).

Die wichtigsten neuen Geschäftsmodelle, die auf der Blockchain-Technologie basieren, werden über Wertzumessungs-Verfahren laufen. Da bei der Blockchain-Technologie keine zentrale Autorität das Sagen hat, kann die Wertzumessung ausschließlich zwischen den Kontrahenten vorgenommen werden. Allerdings vollautomatisch nach fixen Algorithmen. Das macht es möglich, zwischen vielen Marktteilnehmern sehr hohe Anzahlen von Klein- und Kleinsttransaktionen sehr kosteneffizient abzuwickeln und dadurch überhaupt erst möglich zu machen.

So haben z.B. in New York in der Regent Street die Hausbesitzer ihre am Dach liegenden Solarstrom-Anlagen zu einem Stromverbund zusammengeschlossen wo die Energieflüsse vollautomatisch zwischen den Teilnehmern verrechnet werden können ohne über das öffentliche Stromnetz zu laufen.

Obwohl die öffentlichen Leitungen benutzt werden. Das hier eine Fülle neuer und noch nicht ausjudizierter Problemfelder auftreten werden, ergibt sich von selbst.

Ein anderes Beispiel stammt aus dem Hause BEKO selbst: in „BEKO-das Buch“, (veröffentlicht im Jahre 1998), wurde auf Seite 150 als Themenschwerpunkt des IHI die „Vermögensbildung im Netz“ erstmals genannt. Damals konnte das IHI nur theoretische Spekulationen pro Futura liefern, weil zu dieser Zeit die technischen und rechtlichen Rahmenbedingungen fehlten. 2003 hat dann der IHI-Leiter eine Lehrveranstaltung an der Wirtschaftsuniversität Wien abgehalten, in der über die Möglichkeiten und Chancen für virtuelle Wirtschaftskörper im Rahmen der Abteilung „Entrepreneurship und Gründungsforschung“ gearbeitet wurde. Die Vermögensbildung im Netz war damals schon wesentlich konkreter erkennbar als 1998 aber in Österreich wegen der rigiden Rechtslage noch immer nicht machbar. Mit dem laufenden Bitcoin-Experiment kann das IHI nun alle Komponenten eines Vermögensaufbaues im Internet als Beratungsservice bieten der voll funktionsfähig und in weiten Grenzen skalierbar ist.

Auch im Projekt „Home-Butler“ wäre mit der Blockchain-Technologie ein Revival organisierbar, das neue Zielgruppen eröffnen könnte.

Das IHI hat inzwischen die Voraussetzungen geschaffen, diese Phänomene zu erforschen, zu analysieren und der GF der BEKO Holding auf Verlangen zur Verfügung zu stellen.

64. IHI Bericht, 9.9.2016