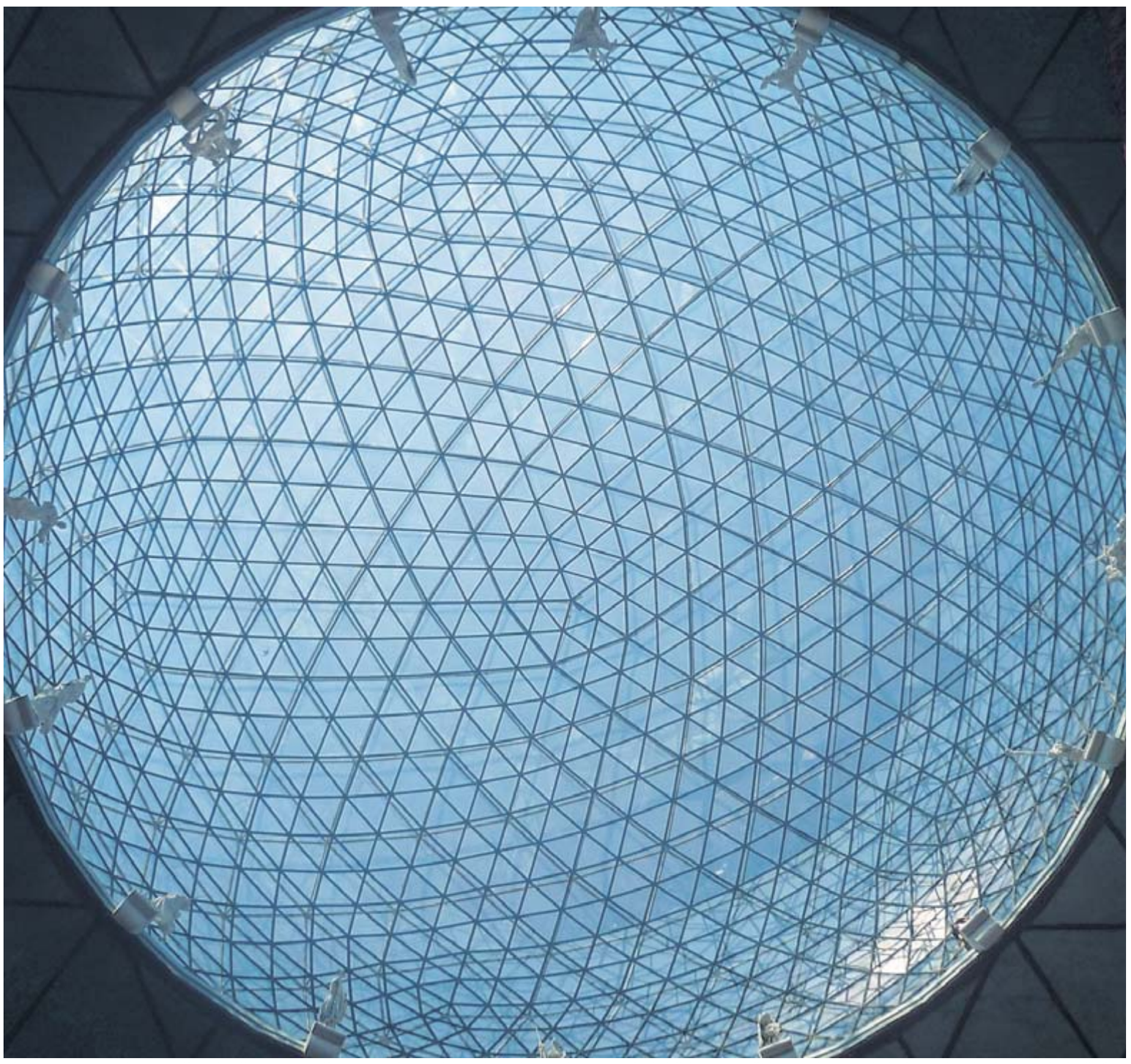
Das nächste große Ding

Ein faszinierender Überbau des Internets könnte verändern, wie wir leben, handeln, Entscheidungen treffen. Die Welt wäre nicht mehr dieselbe. Vorausgesetzt, wir erweitern unsere Vorstellung, was „Vertrauen“ heißt.

VON RONNY SCHILDER



Ein Netz von Rechnern, die wie die Knoten dieser Glaskuppel miteinander verbunden sind, bildet das Rückgrat der Blockchain-Technologie. An sie knüpfen sich hohe Erwartungen. Manche wirken surreal wie die Visionen Salvador Dalís, in dessen Theatermuseum in Spanien dieses Foto entstand. FOTO: RONNY SCHILDER

MITTWEIDA – Niemand weiß, wer das Rad erfunden hat. Es kam in vielen Kulturen gleichzeitig auf. Ein Umsturz, der Gewohnheiten beendete und neue hervorrief. Zuerst wurde das Rad zur Töpferscheibe und revolutionierte den Transport. Dass es sich dereinst in Turbinen, Uhren und Schnellzügen drehen würde, hätte sich kein Erstbenutzer ausmalen können.

Das verheißungsvolle, unheimliche, nächste große Ding im Internet lässt sich so einfach beschreiben wie ein Rad – und ist so schwer zu erfassen. Andreas Ittner, Professor für Informatik und Verteilte Informationssysteme an der Hochschule Mittweida, regt dazu an, sich eine abgelegene Insel vorzustellen, auf der die Insulaner miteinander Muscheln gegen Mangos tauschen. „Wie schaffen Sie Vertrauen in die Transaktion? Wie klären Sie, dass hinterher keiner behauptet, der andere hätte ihn übers Ohr gehauen? Alte Inselvölker haben das gelöst, indem sie die Gemeinschaft zusammentrommelten und den Tausch vor aller Augen machten. Jeder konnte dann bezeugen, was war. Eine Blockchain macht dasselbe. Die Öffentlichkeit drückt der Transaktion ihren virtuellen Stempel auf: Alles korrekt.“

Blockchain, Transaktionen, virtuelle Stempel? Diese Begriffe verändern die Welt. Die Technologie der Blockchain – zu deutsch: „Blockkette“ – euphorisiert die Wirtschaft wie ein Bonbongewitter. Ittner sagt: „Ich denke, in jedem großen Unternehmen gibt es heute Arbeitsgruppen, die sich mit Blockchain befassen.“

Der Professor hält sich jetzt nicht länger mit den abgelegenen Inseln auf, fährt seinen Laptop hoch und nimmt das Smartphone zur Hand, um sein Bitcoin-Konto aufzurufen. Bitcoin, die digitale Währung, ist so etwas wie die Töpferscheibe der Blockchain – die erste große, brauchbare Anwendungsidee.

Für Bitcoin war das Blockchain-Prinzip entwickelt worden. Der Urheber ist unbekannt, ein Anonymus, auch wenn es einen Namen gibt. „Satoshi Nakamoto“ ließ am 18. August 2008 die Internetdomain „bitcoin.org“ registrieren. Zwei Monate später veröffentlichte er einen Arbeitsplan, in dem er das Bitcoin-Prinzip umriss. Vom 3. Januar 2009 datiert der Bitcoin-Urblock („Genesis Block“), vom 12. Januar 2009 die erste Bitcoin-Transaktion. Inzwischen hat die Blockchain eine Höhe von fast 500.000 Blocks erreicht (https://blockexplorer.com). Der Bitcoin-Markt floriert – und „Nakamoto“ ist abgetaucht, seine (oder ihre) Identität bis heute nicht geklärt.

Wer nun im Sommer 2017 auf die Blockchain schaut wie unsere Vorfahren aufs Rad, sieht Anwendungsfälle von begrenzter Tragweite. Ja, man kann auf einigen Webseiten mit Bitcoins bezahlen. Ja, die Bitcoins eignen sich für billige und rasche Überweisungen ins Ausland, besonders in ärmere Länder mit schwacher Bankenstruktur. Ja, man kann auf Bitcoin-Kurse spekulieren wie auf herkömmliche Wechselkurse. Eine Einheit dieser aus dem Nichts geschöpften Währung ist inzwischen mehr als 2000 Dollar wert. Das Angebot ist begrenzt, die Nachfrage (zurzeit vor allem in China) treibt den Preis.

Aber rechtfertigen diese Fakten den Hype? Zumal die Bitcoin-Geschichte auch Tiefschläge zu verzeichnen hat. Im Bundesgefängnis von Manhattan sitzt auf Lebenszeit Ross Ulbricht ein, Deckname Dread Pirate Roberts, der im Darknet des Internets einen Umschlagplatz für Drogen und andere illegale Waren betrieb. Auf dem „Silk Road“-Markt („Seidenstraße“) wurde in Bitcoins bezahlt. Zwar wird Bar- und Bankengeld von Kriminellen viel öfter missbraucht. Dem Image des Digitalgeldes aber hat „Silk Road“ geschadet.

„Das Entscheidende ist etwas anderes“, erläutert Professor Ittner. „In der Netzwelt herrscht grundsätzlich Misstrauen. Es gibt dauernd technische Ausfälle, Hackerangriffe, Manipulationsversuche, in jedem Augenblick. Und doch hat sich die Blockchain der Bitcoin als widerstandsfähig erwiesen. Sie existiert und funktioniert. Inzwischen gibt es Zusammenschlüsse internationaler Großbanken, die nichtöffentliche, sogenannte Konsortial-Blockchains planen, um Kosten zu senken. Wenn man das Bitcoin-Prinzip auf andere Bereiche überträgt, schafft das unglaubliche Möglichkeiten.“

Professor Ittner schlägt jetzt eine Richtung ein, die Laien an die Grenzen der Vorstellung führt. Er spricht vom „Internet der Werte“ und vom „Internet der Dinge“, das sich wie eine Kuppel, eine zweite Ebene über das herkömmliche Internet legt. Das bekannte Netz nennt er das „Internet der Kopien“: „Wer E-Mails versendet, Dateien herunterlädt oder Fotos teilt, arbeitet mit Duplikaten“, erklärt er. „Was man weggibt, behält man selbst auch zurück, eine Mail etwa im Gesendet-Ordner des Mailprogramms. Blockchain ermöglicht einen wirklichen Übergang von Informationen, so sicher und nachvollziehbar, als wenn der eine dem anderen einen Geldschein in die Hand drückt.“ Aus einer beliebig kopierbaren Information wird damit ein digitaler Wert.

Was damit anfangen? Ittner sagt, man könnte die Welt verändern.

Die Blockkette macht atomare Transaktionen möglich, Ware-Geld-Geschäfte im Nu. In dem Augenblick, in dem ein Käufer das neue Auto bezahlt, öffnet sich automatisch und per Impuls die Wagentür. Elektromobile könnten beim Ampelstopp frisch aufgeladen werden, per Induktion, der Preis würde abgebucht. Jeder Klick auf digitale Werte im Netz, Songs, Filme oder Lesestoff, ließe sich in Echtzeit abrechnen, auch kleinste Bruchteile von Centbeträgen. Die Zeit der Flatrates und Abonnements, der Bindungen und Bündelungen wäre vorbei.

Die Möglichkeit, Transaktionen sicher abzuwickeln, ohne einen Dritten einzuschalten, der Vertrauen schafft, macht Banken und Notare, Behörden und Autoritäten potenziell überflüssig. Ein Blockchain-basierter Notariatsservice wie Proof of Existence (https://proofofexistence.com) gibt Dokumenten einen Zeitstempel mit, der sich öffentlich nachweisen, aber nicht abändern lässt. Damit beglaubigt er das Dokument. Im Staat Honduras denkt man darüber nach, die Führung von Grundbüchern als Blockchain ins Netz zu verlagern. Korruption und Fälschungen wären passé.

Joyce und David Mondrus waren 2014 bei der Disney World's Bitcoin Conference in Orlando, Florida, das erste Paar, das seine Ehe in der Blockkette besiegelte, ohne staatlichen Beistand zu bemühen. Die Ukraine versteigerte staatliche Lizenzen in einer Blockchain-Auktion.

Im Internethandel dämmert die nächste Revolution herauf, sollten Blockchain-Experten wie Ittner mit ihren Prognosen recht behalten. Der E-Commerce der ersten Welle hatte viele Zwischenhändler ausgeschaltet, denn nun begegnen sich Hersteller und Kunden im Netz direkt. Künftig geraten Portale und Türsteher wie Amazon oder Ebay unter Druck, die über Bewertungssysteme den Vertrauensbedarf der Kunden bewirtschaften.

Der Reiseveranstalter Tui geht nach einem aktuellen „Handelsblatt“-Bericht gerade dazu über, Hotelkontingente via Blockchain zu verwalten. Portale wie Expedia und Booking.com verlören damit ihre wichtigste Funktion: zu garantieren, dass der Verhandlungspartner wirklich existiert und das Gegenüber nicht mit gefälschten Angaben zockt. Die erste Blockchain-Bank wird in Estland gegründet, einem Land von außerordentlich hoher Internet-Affinität. „Ich könnte mir dort auch vorstellen, dass neue demokratische Prozesse ausprobiert werden“, sagt Andreas Ittner. „Ein digitaler Token“, also quasi ein Informationsschnipsel, „der von A nach B transferiert wird, ließe viel mehr Möglichkeiten für effiziente Abstimmungen zu.“ Ein zukunftsweisender Weg zur Lösung der Vertrauenskrise in der Demokratie?

Smart Contracts, „smarte Verträge“, bringen Investoren und Kapitalsammelstellen mit Unternehmern oder Versicherungsnehmern zusammen, ohne dass eine Bank oder Versicherung mitkassiert. Am Deutschen Institut für Normung (DIN) wird gerade ein Rahmen für solche Verträge erarbeitet, der vielleicht zum internationalen Standard reift.

Als Jahr des Durchbruchs für Bitcoin in den USA gilt 2013. Ende 2015 gab es weltweit bereits mehr als 700 Start-ups im Blockchain-Bereich. „Blockchain ist im Moment vor allem ein europäisches Thema, keine Angelegenheit des Silicon Valley“, hebt Professor Ittner hervor. „Die deutschsprachigen Länder, Deutschland, Österreich, Schweiz, haben hier die Chance, weltweit mitzuspielen.“ An der Hochschule Mittweida haben Ittner und Fachkollegen ein Blockchain-Kompetenzzentrum aus der Taufe gehoben, das Techniker, Mathematiker, Juristen und Ökonomen zusammenbringt. Auch wenn zum Kreis der Unterstützer digitale Riesen gehören, wünscht sich Ittner viele „kleine, freche Projekte unter dem Radar“, zum Testen und Lernen, und um zu sehen, wohin die Reise geht.

Denn hinterm „Internet der Werte“ vermuten Visionäre wie er noch etwas Größeres: das „Internet der Dinge“. Die Utopie einer Welt, in der auch Geräte und Programme eigene Bitcoin-Konten besitzen könnten. In dieser Vorstellung gehört zum Beispiel ein Taxi sich selbst und kassiert Nutzungsgebühren, aus denen es die eigene Unterhaltung finanziert.

Ein Gedanke von philosophischer Tragweite, vielleicht weit weg wie die Turbine vom Urrad, auch wenn es uns diesmal keine Jahrtausende kosten dürfte, den Weg zurückzulegen. Was wäre das für eine Gesellschaft, in der Maschinen rational und unbehelligt von emotionsgetriebenen Menschen agierten? Eine bessere, eine schlechtere Welt?

Andreas Ittner steckt tief genug in der Materie, um auf solche Überlegungen nicht nur abwehrend zu reagieren. „Wir sind weit davon entfernt“, sagt er und vergleicht die momentane Situation mit dem Internet der frühen 1990er, als der Kick darin bestand, „eine Mail unfallfrei nach Amerika zu schicken, und man zwei Tage auf die Antwort wartete“.

Die älteste Blockchain, das Bitcoin-Netz, sieht sich momentan mit der Dominanz einiger Miner konfrontiert, deren Rechenkraft sie aus dem Gros der Netzknoten heraushebt. Es handelt sich um Serverparks in China, wo das Investment groß und der Strom billig sind. Werden also auch im „Internet der Werte“ manche gleicher sein als gleich? Ittner hebt die Schultern. Wir werden sehen.

WEITERE INFORMATIONEN zum Blockchain Competence Center Mittweida gibt es im Internet: **blockchain.hs-mittweida.de**

Das Blockchain-Prinzip: Verteilte Rechner, lückenloser Nachweis, öffentliche Kontrolle

Transaktion. Knoten sind Rechner in einem Netzwerk, die über die Blockchain-Software verfügen. Wenn eine Transaktion stattfindet, etwa ein Tauschhandel zwischen zwei Partnern, erfährt nach wenigen Sekunden jeder Knoten davon.

Miner. Einige der Knoten, sogenannte „Miner“, sammeln und bündeln Transaktionen. Früher konnte das jeder Teilnehmer am PC machen. Heute ist leistungsfähigere Hardware nötig. Die Miner packen mehrere Transaktionen in eine Box, deren Größe vom Design der Blockchain vorgegeben ist. Bei Bitcoin liegt die Grenze bei 1 Megabyte.

Prüfsumme. Wenn ein Block „voll“ ist, seine definierte Größe erreicht, versucht der Miner, eine Prüfsumme für seinen Kandidatenblock zu finden, den sogenannten Hashwert. Das kann Billiarden von Berechnungen erfordern. Nach durchschnittlich zehn Minuten kriegt der Miner ein Ergebnis. Er packt den Hashwert in die Box und meldet allen anderen: „Seht her, ich habe ein Ergebnis!“

Öffentlichkeit. Jeder in einem Netzwerkknoten gefundene Block wird zur Prüfung ausgerufen und von den anderen Rechnern gecheckt. Wird der Kandidatenblock als gültig anerkannt, bildet er das vorläufige Ende der Blockchain. Der vorletzte als gültig anerkannte Block gibt dem neuen seinen Hashwert mit. Damit ist das lückenlose Wachstum des Journals gesichert, das alle seit dem Start der Blockchain darin „verpackten“ Transaktionen enthält. So enthält die Bitcoin-Blockchain alle Bitcoin-Transaktionen seit der allerersten.

Dauer. Im Prinzip laufen Blockchain-Transaktionen in Echtzeit. So werden Zu- und Abflüsse in einem Bitcoin-Konto sofort registriert. Praktisch braucht die Erfassung und Sicherung im Netzwerk – das Verpacken im Block und dessen dezentrale Anerkennung – eine gewisse Zeit, da es im weltweiten Netz 30 bis 45 Sekunden dauern kann, bis wirklich alle Informationen bei den beteiligten Knoten sind. In der Bitcoin-Welt gilt als Erfahrungswert: Nach einer Stunde ist die Transaktion gebucht.

Motivation. Im dezentralen Netz gibt es idealtypisch keine Instanz, die korrumpiert oder bestohlen werden kann – ein wichtiges Designproblem. Die Miner, die das System am Laufen halten, werden für ihre Arbeitsleistung abgefunden und dadurch motiviert. Im Bitcoin-Universum haben sie Anspruch auf Transaktionsgebühren und werden bei der Neuschöpfung von Bitcoins bevorzugt. (ros)

Andreas Ittner
Informatikprofessor Hochschule Mittweida

FOTO: HS MITTWEIDA

„Wenn man das Bitcoin-Prinzip auf andere Bereiche überträgt, schafft das unglaubliche Möglichkeiten.“