STANDPUNKT.

IRE|BS Immobilienakademie
International Real Estate Business School
Universität Regensburg

Ausgabe 73 | 11. Januar 2019

Blockchains bekömmlich erklärt – Hype vs. Realität

Viktor Weber, Gründer - Future Real Estate Institute

Blockchain polarisiert. Die einen halten die Technologie für überschätzt und fühlen sich aufgrund des medialen Hypes an die Zeit kurz vor dem Platzen der Dotcom-Blase der frühen 2000er erinnert. Die anderen versprechen, dass Blockchains nicht nur die Welt sicherer machen und disruptive Geschäftsmodelle hervorbringen werden, sondern auch helfen könnten, den Welthunger und andere globale Probleme zu lösen.

Dabei liegt die Wahrheit in der Mitte.

Auch in der Immobilienbranche sind Blockchains fester Gesprächsbestandteil, wenn es um zukunftsprägende Technologien und die digitale Transformation von Geschäftsmodellen geht. Keine Konferenz, kein Innovationsworkshop und keine digitale Transformationsstrategie ohne einen Beitrag zu Blockchain. Gerade bei Klienten aus der Immobilienbranche begegnet mir als Berater für Innovation sowie digitale Transformation eine sehr optimistische Erwartungshaltung, die leider von einigen Blockchain Experten und Startups befeuert wird.

Fakt ist, dass ich als Informatiker viele Herausforderungen für massenmarkttaugliche Anwendungen von Blockchains, smarten Verträgen und Kryptowährungen sehe, die man auf der betriebswirtschaftlichen Seite gerne vernachlässigt. Auf der technischen Seite ist also noch viel zu tun und die Zeit sollte man den Entwicklern geben. Gleichwohl sehe ich als Ökonom spannende Geschäftsmodelle, die sich in Zukunft monetarisieren lassen könnten. Es gilt also eine Balance aus Erwartung und Machbarkeit zu finden, um bessere strategische Entscheidungen treffen zu können.

Aus diesem Grund möchte ich in diesem IREBS-Standpunkt einige zentrale Fragen zu Blockchains beantworten, die mir regelmäßig gestellt werden, um ein realistisches Bild dieser Technologie zu vermitteln.

Wie kann ich als Nicht-Informatiker Blockchains verstehen?

Kurz: Hier gibt es leider keine Abkürzungen 😉

Ausführlich: Es gibt einige Ressourcen im Internet, die einen guten Überblick über Anwendungsmöglichkeiten und die technischen Mechanismen von Blockchains vermitteln. Insbesondere empfehle ich den YouTube-Kanal Computerphile von der Universität Nottingham. Hier werden relevante Fakten gut verständlich vermittelt. Als Nicht-Informatiker wird man jedoch zwangsläufig über viele Begriffe stolpern, die erstmal einen „Was zur Hölle?“-Moment auslösen. Hier nicht verzagen, sondern einfach die jeweiligen Videos dazu von Computerphile und weiteren Kanälen anschauen.

Ferner empfehle ich die E-Learning Plattform edX.org, auf der es ein paar interessante Kurse von der Linux Foundation und BerkeleyX gibt. Jedoch gilt es zu bedenken, dass diese Kurse einen sehr positiven Tonus haben und einige bestehende Probleme ausblenden.

Jedoch wird man als Fachfremder ein Wissensplateau erreichen, da hierzu notwendige Grundkenntnisse in den Bereichen Datenbanken, Software Engineering, Rechnernetze, Kryptografie, IT-Sicherheit, Lineare Algebra, Analysis und Statistik fehlen. Wer also wirklich die Grenzen und Möglichkeiten von Blockchains verstehen und damit sinnhaft arbeiten will, sollte mehr Zeit investieren. Hier empfehle ich für Führungskräfte mit dem Titel Head of Digital/Head of Innovation/Chief Innovation Officer usw. ein nebenberufliches Informatikstudium in Teilzeit an der Fernuniversität Hagen. Das Curriculum ist machbar und spannend. Man muss natürlich nicht nochmal studieren, sondern kann über E-Learning auch relevante Kurse selbstständig absolvieren.

Lernen muss so oder so für alle Mitarbeiter/innen fester Bestandteil des Arbeitsalltags werden, wenn sich ein Unternehmen gesamtheitlich digital Transformieren möchte. Eine entsprechende Strategie muss auf dem vorhandenen Wissensfundament aufbauen und sich an den Unternehmenszielen sowie individuellen Interessen der Lernenden orientieren. Da es unrealistisch ist, dass sich Mitarbeiter/innen konstant in ihrer Freizeit weiterbilden, muss das Lernen in der bezahlten Arbeitszeit erfolgen. Ein gutes Fortbildungskonzept wirkt sich zudem positiv auf Mitarbeiterbindung, Innovationsprozesse und Produktivität aus.

Wie würden Sie Blockchain definieren?

Kurz: Eine Blockchain ist ein Register in dem alle jemals getätigten Transaktionen aufgezeichnet werden.

Ausführlich: Der Begriff Blockchain fiel erstmalig 2008 in einem technischen Papier von Satoshi Nakamoto, wobei bis dato nicht bekannt ist, wer sich hinter dem Namen wirklich verbirgt.

Eine Blockchain ist eine stetig wachsende Liste von kryptographisch signierten, unabänderlichen Einträgen, welche von allen Teilnehmern des dezentralen, verteilten Netzwerks gespeichert wird.

Es handelt sich um eine append-only Datenbankstruktur in den Transaktionen zwischen Teilnehmern des Netzwerkes gespeichert werden. Das bedeutet, dass man immer nur Daten hinzufügt, aber nichts entfernt.

Kann man Blockchains auch weniger kompliziert erklären?

Stellen Sie sich vor 100 Regensburger/innen wollen untereinander Tauschhandel betreiben. Das Problem ist nur, dass man sich nicht persönlich kennt und somit auch nicht vertraut. Die IT-interessierte Irmgard hatte folgende Idee:

Jede Transaktion zwischen den 100 Regensburgern soll in ein Transaktionsregister geschrieben werden, welches für alle einsehbar ist. Um nicht Gefahr zu laufen, dass der arglistige Alfons das Transaktionsregister fälscht oder vernichtet, entschließt man sich, dass jeder der 100 Regensburger/innen eine Kopie des aktuellen Transaktionsregisters haben muss. Jetzt müsste Alfons alle Register gleichzeitig fälschen oder vernichten, was aufgrund der räumlichen Verteilung der 100 Regensburger/innen fast unmöglich ist.

Da man jedoch nicht immer einen passenden Tauschpartner findet, kam die pfiffige Paola auf die Idee, dass man eine Währung erschaffen sollte, um den Handel zu erleichtern. Hier kommt der Ratisbona Coin ins Spiel. Möchte also Josef an Ibrahim eine Zahlung tätigen, so teilt er dies den übrigen 99 Regensburgern (inkl. Ibrahim) mit. Da jeder Ratisbona Coin eine einmalige Seriennummer hat, schauen die 99 Regensburger/innen jeweils in ihrer lokalen Registerkopie nach, um zu prüfen ob Josef wirklich der rechtmäßige Eigentümer der Ratisbona Coins ist und diese nicht schon an jemand anderen überwiesen hat. Da Josef ehrlich war, bestätigen alle 99 Regensburger, dass die Transaktion gültig ist und schreiben sie in ihr lokales Register. Auch Josef aktualisiert sein Register und alle 100 Regensburger/innen haben eine inhaltsgleiche Kopie.

Um den Prozess effizienter zu machen, kam der tüchtige Taylor auf die Idee, dass man immer 20 Transaktionen in einer Datei sammelt und dann gebündelt, wie am Fließband, bearbeitet. Jede Datei mit 20 Transaktionen erhält wiederum eine eindeutige Kennung. Ist eine Datei voll und alle Transaktionen akzeptiert, fängt man wieder an in eine neue Datei neue Transaktionen hineinzuschreiben. Die erste Datei mit 20 Transaktionen heißt Ursprungsblock. In die zweite Datei, kommen aber nicht nur die 20 neuen Transaktionen, sondern auch die eindeutige Kennung des Ursprungblocks. Jede neue Datei beinhaltet somit immer die eindeutige Kennung der vorherigen Datei. So entsteht eine Verkettung der Dateien beziehungsweise Blöcke, was man Blockchain nennt.

Wie würden Sie Kryptowährung definieren?

Bei einer Kryptowährung werden auf der Blockchain sämtliche in der Währung getätigten Zahlungen gespeichert. Diese Währung ist jedoch nicht durch eine Zentralbank reguliert und auch meist nicht mit einem physischen Wertgegenstand hinterlegt.

Beispiel:

> Überweist Viktor Weber am 01.01.19 100 Ratisbona Coins an Bob Builder, dann kann theoretisch in Zukunft jeder Teilnehmer der Blockchain einsehen, dass ich diese Transakation getätigt habe. In Wirklichkeit würden die Transaktionsbeteiligten nicht mit ihren Klarnamen auftauchen, sondern mit einer Adresse, bestehend aus Zahlen und Buchstaben.
>
> Überweist Bob Builder dann über ein Jahr später 100 Ratisbona Coins an Heike Hausler, wird die vorherige Transaktion von Viktor Weber an Bob Builder referenziert. So lässt sich genau nachvollziehen in welchen Transaktionen ein Ratisbona Coin beteiligt war.

Jeder Mensch kann theoretisch eine eigene Kryptowährung erschaffen, was den Markt sehr undurchsichtig, volatil und somit riskant macht. Auch sollte an dieser Stelle gesagt werden, dass Kryptowährungen ursprünglich nicht als Investment gedacht waren, sondern als alltägliche Zahlungsmittelalternative zu staatlich regulierten Währungen.

Um massenmarkttauglich zu werden, müssen Kryptowährungen bestehende technologische Hürden überwinden und aus meiner Sicht besser reguliert werden.

Wie würden Sie Smart Contracts definieren?

Smarte Verträge sind Computerprogramme, die bei Eintreten eines bestimmten Ereignisses, automatisch eine Aktion ausführen. Diese Verträge sind dabei in der Blockchain gespeichert und können von jedermann genutzt werden. Auch kann man selbst neue Programme (smarte Verträge) für bestimmte Anwendungsfälle (z.B. Immobilienkauf) entwickeln und in einer Blockchain speichern.

Beispiel:

> Kauft also der konsumliebende Konrad im Online Shop der geschäftstüchtigen Gertrud eine Drohne, so kann er 50 Ratisbona Coins an einen designierten Kaufvertrag schicken und im Verwendungszweck angeben, dass die Zahlung für Gertrud bestimmt ist und bei der Rechnung XYZ123 verrechnet werden soll. Der smarte Vertrag bestätigt den Zahlungseingang und leitet automatisch den Versand der Drohne ein. Als Konrad den Empfang der Drohne bestätigt, werden die 50 Ratisbona Coins an Gertrude ausbezahlt.

Was sind Vorteile von Smart Contracts?

Smart Verträge versprechen eine schnellere, transparentere, besser dokumentierte und automatische Abwicklung von Verträgen. Sollten smarte Verträge technisch und juristisch einwandfrei realisiert werden können, dann wären sie in der Tat ein bedeutender Treiber der Automatisierung. Im immobilienwirtschaftlichen Kontext wären beispielsweise smarte Mietverträge denkbar, die automatisch Mietzahlungen überprüfen, erhöhen, steuerlich veranlagen und Nebenkosten berücksichtigen. Ferner wird gerne als Beispiel gebracht, dass man mit Hilfe von smarten Verträgen die Beglaubigung eines Notars ersetzen könnte, wobei hier die Gemeinschaft der Blockchain-Nutzer die Funktion des Notars übernehmen würde.

Können wir Transaktionen über Blockchains abwickeln?

Kurz: Theoretisch ja, aber dabei muss man einige Fallstricke berücksichtigen.

Ausführlich: Im Prinzip lässt sich jede Form von Willenserklärung in einen smarten Vertrag übertragen. Dabei muss Ihnen bewusst sein, dass diese Form von Programm kein juristisches Verständnis hat und im Falle einer Fehlfunktion nicht mehr nachträglich verändert werden kann, da er Bestandteil einer Blockchain geworden ist.

Sie können also eine Transaktion entsprechend abwickeln, jedoch müssen Sie dennoch die gegenwärtige Regulatorik mit entsprechender Dokumentation einhalten. Ferner sind smarte Verträge noch von etlichen Problemen behaftet, zu denen ich separat eine Erläuterung gebe.

Was sind Probleme bei Smart Contracts?

Ihr smarter Vertrag kann kein Gesetz auslegen, berücksichtigt nicht die Intention ihres Vertrages, die aktuelle Rechtsprechung, die herrschende Meinung oder gesellschaftliche Normen. Es zählt, was programmiert und auf der Blockchain gespeichert wurde. Im Falle eines Disputs würde man also weiterhin genötigt sein, den konventionellen Weg über Anwälte und Gerichte zu gehen. Daher ist ein smarter Vertrag heute eher ein Zusatz.

Problematisch ist auch, dass Juristen kein Wissen über die technische Implementierung haben. Gleichwohl haben die implementierenden Informatiker keine Kenntnis über die Juristerei und sauber aufgesetzte Vertragswerke.

Auch mangelt es an einer adäquaten und fehlerfreien Programmiersprache. Das heißt, dass ein smarter Vertrag unter Umständen Sicherheitslücken aufweist, die von bösartigen Dritten ausgenutzt werden könnten. Darüber hinaus besteht die Möglichkeit, dass sich ein Vertrag einfach anders verhält als gedacht.

Smarte Verträge und Kryptowährungen, die oft an die Verträge gekoppelt sind, werden in unterschiedlichen Jurisdiktionen unterschiedlich behandelt. Aufgrund der Regulatorik sind also viele Use-Cases schon heute eingeschränkt oder juristische Fragen noch unbeantwortet. Es mangelt also an Rechtssicherheit.

Sind Blockchains wirklich unabänderlich?

Kurz: Historische Daten sind i.d.R. unabänderlich, aber nicht die Modellierung der Blockchain.

Ausführlich: Es handelt sich um eine Datenbankstruktur, bei der alte Datenpunkte nicht gelöscht werden, sondern nur neue Datenpunkte hinzukommen. Aus diesem Grund bleibt das historische Transaktionsregister erhalten. Bevor die Transaktionen zu einem Block zusammengefasst werden, werden diese kryptographisch miteinander verbunden. Wird daher innerhalb der Blockchain nur ein Datenpunkt verändert oder auch nur ein einziges Bit unautorisiert modifiziert (z. B. durch Probleme bei der Datenübertragung), fällt dies sofort auf. Transaktionen oder Daten im Nachhinein zu verändern, ist somit nahezu unmöglich.

Aber aufgepasst…

Eine Blockchain entwickelt sich stetig weiter und wie sie sich weiterentwickelt, hängt von der verwandten Modellierung und den Teilnehmern der Blockchain ab. So kann eine Veränderung der Modellierung z. B. durch Mehrheitsbeschluss veranlasst werden, die zu Ihren Ungunsten sein könnte.

Sind Blockchains die beste Datenbankenstruktur auf dem Markt?

Kurz: Nein, es macht in vielen Fällen keinen Sinn eine Blockchain zu verwenden.

Ausführlich: In der Regel haben Teilnehmer (Nodes) ein vollständiges Transaktionsregister gespeichert. Im Falle der Bitcoin Blockchain bedeutet es, dass durchschnittlich 9288 Nodes jeweils circa 200 Gigabyte Daten bei sich lokal speichern müssen. Daraus folgt, dass wir eine um 928.700% aufgeblähte Datenstruktur haben. Aus diesem Grund sollte nicht alle Daten auf eine Blockchain gepackt werden. Würden Unternehmen IT-Sicherheit mehr in ihren Fokus rücken und Daten verschlüsseln, könnten auch zentralistische Datenbanken die notwendige Sicherheit bieten. Darüber hinaus gibt es viele weitere Datenbankenarchitekturen, mit ihren eigenen Vor- und Nachteilen, was an dieser Stelle zu weit führen würde.

Auch muss man sich überlegen ob man in einem funktionierenden Rechtsstaat tatsächlich alle zentralistischen Entitäten zu Gunsten eines anonymen Kreises von Teilnehmern einer Blockchain vermeiden sollte. Wird in Deutschland ein Vertrag gebrochen, hat jeder die Möglichkeit seine Interessen vor einem Gericht zu vertreten. Bei einer Blockchain muss man sich hingegen auf die Modellierung und das Zusammenspiel der Teilnehmer/innen verlassen. Ferner kann es sein, dass man niemanden im analogen Leben rechtlich belangen kann, da man abhängig von der Modellierung vielleicht nicht einmal den Klarnamen seines Vertragspartners kennt.

Notarielle Beurkundung mit Hilfe von smarten Verträgen?

Richtig ist, dass man durch digitale Signaturen und andere Werkzeuge der Kryptographie eine notarielle Beurkundung aussparen könnte, jedoch bedarf es dazu keines smarten Vertrags und keiner Blockchain.

Sind Blockchains wirklich 100% sicher?

Die kurze Antwort lautet: Nein.

Die richtige Antwort lautet: Es kommt auf die jeweilige Modellierung an.

Durch die redundante Datenspeicherung der gesamten Blockchain auf verschiedenen dezentral, verteilten Nodes, führt der Ausfall einzelner Teilnehmer nicht zu einem Systemausfall. Das Sicherheitsziel der Verfügbarkeit ist somit erfüllt. Die Nutzung von kryptographischen Verfahren sorgt dafür, dass eine unautorisierte Veränderung von Daten sofort auffällt. Daher wird das Schutzziel der Integrität ebenfalls erfüllt. Wie vertraulich Ihre Daten sind, hängt dabei von der Modellierung ab und ob Sie anonym an einer Blockchain teilnehmen können.

Auch wissen Sie nicht wer hinter der Entwicklung einer Blockchain steckt, ob diese konstant nach Schwachstellen untersucht wird und ob diese behoben werden. Blockchain-basierte Anwendungen sind also wie jedes andere System niemals 100% sicher.

Ergibt ein Blockchain-basiertes Grundbuch Sinn?

Könnte man Transaktionen rechtlich und technisch einwandfrei mit smarten Verträgen modellieren, dann wäre es natürlich spannend die neuen Eigentumsverhältnisse automatisch auch rechtskräftig in einem digitalen Grundbuch abzuspeichern. Jedoch ist das heute noch nicht möglich und ob beziehungsweise wann das technisch/rechtlich möglich sein wird, gleicht einem Blick in die Kristallkugel.

Ein nichtstaatliches Blockchain-basiertes Grundbuch ist rein regulatorisch in Deutschland nicht sinnvoll, da die Inhalte nicht vom Staat anerkannt werden würden. Ferner besteht dazu auch keine Notwendigkeit, da man in einer funktionierenden Demokratie mit dazugehörigem Rechtssystem dem Staat vertrauen kann. Es wäre hier riskanter, einer technischen Modellierung mit noch ungelösten Problemen zu vertrauen, die ein Großteil der Nutzer darüber hinaus nicht einmal nachvollziehen kann.

In Ländern, in denen man der Regierung nicht trauen kann, wäre ein nichtstaatliches Grundbuch zwar eine charmante Lösung, jedoch ist es hier fraglich, ob sich dann Ansprüche aus der relativ sichereren Blockchain in solch einem Rechtssystem durchsetzen ließen.

Beispiel:

> Sollte ein Warlord in Mali ein Grundstück enteignen, so würde zwar der rechtmäßige Eigentümer in der Blockchain stehen, jedoch könnte er sich im echten Leben deshalb nicht besser gegen die Enteignung wehren. Es kommt also auf die Durchsetzbarkeit und Verlässlichkeit in der analogen Welt an.

Sinnvoll wäre jedoch eine verteilte, digitale und verschlüsselte, jedoch zentral kontrollierte Speicherung des Grundbuchs, um beispielsweise der Vernichtung des Grundbuchs, wie z. B. in Haiti geschehen, vorzubeugen.

Eine staatliche Grundbuch-Blockchain würde zwar sehr innovativ klingen und ließe sich politisch vermarkten, wäre aber eine überkomplizierte „Lösung“ für kein wirkliches Problem in Deutschland und den meisten anderen Ländern. Erstmal sollte man überfällige E-Government Leistungen anbieten, für die man heute noch in diverse Ämter gehen muss.

Stimmt immer was in der Blockchain gespeichert wird z.B. ein Übergabeprotokoll?

Kurz: Nein.

Ausführlich: Sobald Daten aus der analogen Welt in digitale Form gebracht werden, können Fehler entstehen. Sowohl wissentlich als auch unbeabsichtigt. Der Input, z. B. dass das Gewerk XY in einem Neubau keine Mängel aufweist, kann zwar in der Blockchain unveränderlich gespeichert worden sein, muss aber nicht stimmen. Solange wir keine Garantie haben, dass die eingegebenen Daten stimmen, ist man mit dem Garbage-In-Garbage-Out Problem konfrontiert.

Aus diesem Grund sind viele Business-Cases wie Lebensmittelzertifizierungen oder eben smarte Übergabeprotokolle nicht wirklich sinnvoll.

Schlusswort

Hinterfragen Sie bitte utopisch klingende Versprechen von Startups, Beratern und Blockchain-Experten auf Konferenzen. Sollten die Erwartungen innerhalb der Branche nicht bald auf den Boden der Tatsachen geholt werden, laufen wir Gefahr, einen Crypto-Winter zu erleben. Dies würde sinnhafte Entwicklungen auf diesem Gebiet ausbremsen und der notwendigen Grundlagenforschung hinderlich sein.

Viktor Weber

Future Real Estate Institute
Weißgerbergraben 20
93047 Regensburg
E-Mail: contact@fre-institute.com
www.fre-institute.com

Viktor Weber (Gründer - Future Real Estate Institute) berät Unternehmen bei deren digitaler Transformation, publiziert international zu Zukunftsthemen und spricht auf Konferenzen über innovative Technologien, holistische digitale Transformation, Smart Cities sowie gesellschaftliche Aspekte des digitalen Wandels.