

SWR2 Wissen

Die Blockchain-Technologie Bitcoin, Libra und andere Versprechen

Von Sebastian Felser

Sendung: Montag, 25. November 2019, 8.30 Uhr

Redaktion: Gábor Páal

Regie: Günter Maurer

Produktion: SWR 2019

Facebook will eine eigene Internet-Währung schaffen: „Libra“. Grundlage ist die Blockchain-Technik, bekannt durch die „Bitcoins“. Doch auch die Deutsche Bundesbahn interessiert sich für sie.

Bitte beachten Sie:

Das Manuskript ist ausschließlich zum persönlichen, privaten Gebrauch bestimmt. Jede weitere Vervielfältigung und Verbreitung bedarf der ausdrücklichen Genehmigung des Urhebers bzw. des SWR.

SWR2 können Sie auch im **SWR2 Webradio** unter www.SWR2.de und auf Mobilgeräten in der **SWR2 App** hören – oder als **Podcast** nachhören.

Kennen Sie schon das Serviceangebot des Kulturradios SWR2?

Mit der kostenlosen SWR2 Kulturkarte können Sie zu ermäßigten Eintrittspreisen Veranstaltungen des SWR2 und seiner vielen Kulturpartner im Sendegebiet besuchen. Mit dem Infoheft SWR2 Kulturservice sind Sie stets über SWR2 und die zahlreichen Veranstaltungen im SWR2-Kulturpartner-Netz informiert. Jetzt anmelden unter 07221/300 200 oder swr2.de

Die SWR2 App für Android und iOS

Hören Sie das SWR2 Programm, wann und wo Sie wollen. Jederzeit live oder zeitversetzt, online oder offline. Alle Sendung stehen mindestens sieben Tage lang zum Nachhören bereit. Nutzen Sie die neuen Funktionen der SWR2 App: abonnieren, offline hören, stöbern, meistgehört, Themenbereiche, Empfehlungen, Entdeckungen ...
Kostenlos herunterladen: www.swr2.de/app

MANUSKRIFT

Autor:

Im Sommer 2019 hat der US-Konzern Facebook überraschend eine Ankündigung gemacht. Er will schon 2020 eine eigene sogenannte „Krypto-Währung“ auf den Markt bringen. Ihr Name: „Libra“. Dafür hat sich Facebook mit zahlreichen anderen Konzernen zusammengeschlossen. Die Idee klingt revolutionär:

Musikakzent

Sprecherin (Stimme verzerrt):

Weltweit Geld zu verschicken, sollte so einfach und kostengünstig und sogar noch sicherer als das Senden einer SMS oder eines Fotos sein – unabhängig vom Wohnort, Beruf oder Einkommen. Die Welt braucht eine zuverlässige digitale Währung und Finanzinfrastruktur, die gemeinsam das Versprechen einhalten können, ein „Internet des Geldes“ zu schaffen.

Autor:

Auch wenn Facebook jüngst einige Rückschläge erlebt hat – mehrere große Finanz-Partner sind aus dem „Libra“-Projekt ausgestiegen, nachdem es von zahlreichen Regierungen ablehnende Signale gab: Facebook will jedoch weiter machen – und die Blockchain-Technologie verspricht deutlich mehr als nur Geldgeschäfte mit neuen Internet-Währungen. Sie soll das Wirtschaftsleben in vielen Bereichen revolutionieren – vor allem überall dort, wo Dinge von A nach B nach C gelangen. Das ist neben der Finanzwelt auch der Handel. Oder der Verkehr.

Musikakzent

Ansage:

Die Blockchain-Technologie: Bitcoin, Libra und andere Versprechen. Von Sebastian Felser.

Atmo – Durchsage Deutsche Bahn:

... nach Wilhelmshaven.

Atmo – Durchsage ICE:

Thank you for travelling with Deutsche Bahn – good bye!

Autor:

In Frankfurt, rund zehn Gehminuten über die Kaiserstraße vom Hauptbahnhof entfernt, steht der sogenannte „Silberturm“ – früher die Konzernzentrale der Dresdner Bank, heute unter anderem Sitz des „Innovation Lab“ der Deutschen Bahn.

Atmo – Eingangshalle Silberturm:

Stimmengemurmel, Autor: Schönen guten Tag, Sebastian Felser ist mein Name, vom Südwestrundfunk.

Atmo – Aufzug:
26. Obergeschoss

Autor:
Wer wissen möchte, was die Deutsche Bahn mit der Blockchain-Technologie anfangen will, muss weit nach oben zu Matthias Felder.

Atmo:
Gemurmel von Matthias Felder

Autor:
Felder denkt bei der Bahn über mögliche Blockchain-Anwendungen nach. In gewisser Weise ein Traumberuf: Er darf im Dienst mit Modell-Eisenbahnen spielen, und das zeigt er Besuchern gern. In einem eigenen Präsentationsraum hat er mit seinem Team eine elektrische Eisenbahn aufgebaut.

Atmo – Eisenbahnplatte:
Elektromotor der Modell-Eisenbahn und Schienen-Rattern

Autor:
Die Eisenbahnplatte im Maßstab H0 sieht erst mal genau so aus, wie jede andere: Berge, Tunnel und Brücken für die Eisenbahn, eine kleine Kirche, die aussieht, als könnte sie irgendwo in Süddeutschland stehen. Dazu Straßen, Autos, Pferdeweiden, ein Restaurant mit kleinen Figuren. Und zwischen all dem fahren zwei Züge. Das Besondere an dieser Modelleisenbahn zeigt der Blick nach oben. Über der Landschaft hängen GPS-Empfänger, die den jeweiligen Standort der beiden Züge auf der Platte erfassen – sie entsprechen im Modell den GPS-Satelliten in der Erdumlaufbahn. Neben der Eisenbahnplatte ist ein Touchscreen angebracht. Er zeigt die Positionen der beiden Loks auf einem Gleisplan der kleinen Strecke an. Über diesen Touchscreen kann Felder den Zügen auch Befehle erteilen:

O-Ton – Matthias Felder:
Ich möchte hier in den nächsten Bahnhof reinfahren – das ist der Bahnhof Blumenfeld. Jetzt werden mir verschiedene Streckenführungen und Streckenabschnitte vorgeschlagen. Wenn ich sage, ja, die Strecke passt für mich, dann buche ich diese Strecke, die Weichen wurden jetzt automatisiert durch das System gestellt, und der Zug fährt jetzt selber bis ins Ziel hinein.

Atmo – Eisenbahnplatte:
Elektromotor der Modell-Eisenbahn und Schienen-Rattern

Autor:
Matthias Felder gibt dabei nur das Ziel des Zuges ein und die Strecke, aber um die konkrete Ausführung kümmern sich die Züge selbst. Sie schließen per Blockchain-Verfahren untereinander sogenannte „Smart Contracts“, also digitale Verträge, wer wann wo fahren darf.

O-Ton – Matthias Felder:

Ich möchte als Zug von A nach B kommen, möchte eben einen Streckenabschnitt reservieren: Das System prüft diesen Streckenabschnitt, ob er schon geblockt ist durch einen anderen Zug. Wenn nicht, gibt er mir die Reservierung frei, ich bestätige die Reservierung – wie eine Hotel-Reservierung kann man sich das vorstellen – und wenn dann die Zeit gekommen ist, dass der Fahrplan sagt: So, jetzt muss der Zug losfahren, wird nochmals geprüft, sind die Streckenabschnitte noch belegt oder ist es schon frei – ähnlich wie beim Hotelzimmer, wie gesagt – ist es schon geputzt oder nicht, kann ich da jetzt rein. Und dann beginne ich, die Strecke abzufahren und die Strecke verwaltet und schaltet sich selbst. Das haben wir jetzt in Form einer Minitatur-Eisenbahn im Kleinen dargestellt.

Autor:

Die Lok startet jetzt rückwärts, fährt hier den Berg hoch und kommt auch langsam in Richtung der Brücke, die das Nadelöhr darstellt, wo sich die Züge einigen müssen. Jetzt ist der Streckenabschnitt freigegeben und jetzt kann die Bahn auch wieder runter, wo sich die Gleise wieder aufteilen und ist wieder im Bahnhof Blumenfeld angekommen.

O-Ton – Matthias Felder:

Jeder Kilometer Schiene kostet Geld, jeder Halt in einem Bahnhof kostet Geld und wir sind auch in der Lage, jeden dieser Streckenabschnitte anzuschauen und zu sagen: Hey, wann hatte denn welcher Streckenabschnitt eigentlich welche Buchung gehabt? Man muss nämlich dazu sagen, die Deutsche Bahn ist eben nicht der einzige Anbieter von Zügen auf der Schiene in Deutschland, sondern in Deutschland haben wir über 340 verschiedene Eisenbahnverkehrsunternehmen, die das Netz der Bahn nutzen, und damit man das verbrauchergerecht zuordnen kann, muss man natürlich auch wissen, wer ist denn da wann gefahren und von wo nach wo?

Atmo:

Zugfahrgeräusche

Autor:

Die Bahn kann also genauer mit Regionalverkehrsbetrieben abrechnen. Und wenn Gleise und Züge über die Blockchain-Technologie selbst miteinander ausmachen, wer, wann, wo fährt, dann lastet das auch das Schienennetz besser aus. Das Ergebnis, so die Hoffnung: weniger Verspätungen, ein reibungsloserer Ablauf und natürlich Kosteneinsparungen. Das Modell auf das komplette Schienennetz der Deutschen Bahn zu übertragen, wird noch Jahre dauern, sagt Felder. Wenn es aber einmal soweit ist, hätte konkret jeder Zug in Deutschland – egal von welchem Unternehmen – einen sogenannten „Personal Key“. Dieser Schlüssel ist eine ellenlange Nummer. Mit dieser Nummer lässt sich der Zug im Blockchain-Verfahren eindeutig identifizieren. Genau solch einen „Personal Key“ bekäme dann auch jedes Stück Infrastruktur – von der Hochgeschwindigkeitstrasse bis zum Abstellgleis am Bahnhof. So können Züge und Gleise verbindliche Verträge schließen und sich selbst lenken. Stellwerke, wo heute noch zahllose Bahn-Mitarbeiter händisch die Weichen stellen, sind dann nur noch Netzwerk-Knoten. Über diese Knoten läuft die Kommunikation zwischen Zügen und Gleisen. Hier zeigt sich auch, warum sich die Bahn davon weniger Verspätungen erhofft: Wenn heute ein Stellwerk ausfällt, müssen in seinem Bereich alle Züge stehenbleiben. Fällt dagegen ein Netzwerkknoten aus, übernehmen die anderen Knoten im System. Parallel laufen die

Abrechnungen zwischen Nutzer-Zügen und benutzten Gleisen automatisch ab. Die Blockchain-Technologie bietet also eine Eisenbahn-Maut, gekoppelt mit einem automatisierten Verkehrslenksystem.

O-Ton – Matthias Felder:

Eine der größten Haupt-Aufgaben bei mir besteht auch darin, nicht nur innerhalb des Konzerns zu arbeiten – die Blockchain ist eine übergreifende Technologie, wo wir auch viel mit anderen Unternehmen arbeiten müssen, und mit denen auch zu gucken, wie können wir denn gemeinsame Plattformen, gemeinsame Lösungen schaffen.

Autor:

So arbeitet Matthias Felder mit seinem Team bereits an einer Plattform, über die sich komplette Reisen buchen lassen – unabhängig vom Verkehrsträger. Dafür müssen sie keine neue Super-App programmieren, die sich dann jeder runterladen muss. Der Kunde soll da buchen, wo er sich wohl fühlt.

O-Ton – Matthias Felder:

Eine schöne Reise ist zum Beispiel, wenn ich von Frankfurt nach Manerola – das ist ein kleines, schönes Küsten-Örtchen in Italien – möchte. Ich habe in jedem Fall zwischen drei und vier Unternehmen heutzutage, wo ich über drei bis vier verschiedene Buchungsportale gehen muss, um mir die einzelnen Tickets zu buchen und aufeinander anzupassen. In der Idealwelt, die wir uns erhoffen, für die wir im Hintergrund die Plattform schaffen, über die sich die Reiseanbieter verketteten können, krieg' mein Ticket aufs Handy und fahr' dann los und muss nur noch dieses eine Ticket vorzeigen und muss mich nicht noch 17 Mal ausweisen und nachweisen, dass ich verschiedenste Tickets für verschiedene Anbieter habe.

Atmo:

Druckergeräusch

Autor:

Denn dieses eine Ticket kann ich buchen, wo ich will. Wenn ich das Buchungsportal der Deutschen Bahn nutze, könnte ich dort meinen Zug-Fahrschein zum Flughafen, das Flugticket nach Italien, die Weiterreise mit der italienischen Bahn und noch die letzte Meile mit dem Öffentlichen Nahverkehr oder auch mit einem Mietwagen kaufen. Das alles geht in einer App und es gibt nur ein Ticket. Dieselbe Reise könnte ich aber auch im Buchungsportal der Fluggesellschaft oder des Mietwagen-Anbieters buchen. Im Hintergrund verständigen sich alle über das Blockchain-Verfahren. Die Anbieter schließen automatisiert vorprogrammierte digitale Verträge, eben „Smart Contracts“. Damit machen sie auch intern ihre Abrechnung – ähnlich wie beim Maut-System auf der Schiene. Wenn alles gut läuft, soll dieses blockchain-basierte Angebot schon 2020 auf den Markt kommen.

O-Ton – Thomas Rose:

Der Komfort-Gewinn bei der Blockchain ist eigentlich immer, wenn sich Parteien zusammentun, die vorher nicht zusammengearbeitet haben.

Autor:

Das sagt Thomas Rose. Er ist Forschungsbereichsleiter am Fraunhofer Institut für Angewandte Informationstechnik, FIT, und arbeitet im Blockchain-Labor des Instituts. Blockchain-Anwendungen eignen sich prinzipiell für alle Systeme, in denen einzelne Akteure bestimmte Werte austauschen. Bei Werten denken wir ja immer zunächst an Geld. Tatsächlich war das auch die erste Anwendung der Blockchain-Technik: Ein System, um digitales Geld zu transferieren. Damit war im Jahr 2009 der „Bitcoin“ geboren – die bis heute führende Internetwährung. Ihr Kurs lässt sich wie der von Dollar, Yen oder jeder anderen nationalen Währung jederzeit im Internet abrufen. Nur eben: Münzen und Scheine gibt es nicht.

O-Ton – Thomas Rose:

Man kann sich das vielleicht so vorstellen: Früher haben wir Kontobücher gehabt, in denen wir alle Informationen und Transaktionen dokumentiert haben, und die Idee ist jetzt, diese Kontenbücher auf verschiedene Knoten zu verteilen.

Musikakzent

Autor:

Ein Beispiel: Angenommen, Herr Rose hat mir 50 Euro geliehen und ich will sie ihm erstatten. In der heutigen Welt gehe ich mit den Konto-Informationen von Herrn Rose zu meiner Bank und sage: Liebe Bank, bitte überweise Herrn Rose 50 Euro. Die Bank prüft die Verbindung, meine Liquidität und nimmt dann Kontakt zur Bank von Herrn Rose auf. Er erhält die 50 Euro. Am Ende wissen von der Transaktion: Herr Rose, unsere beiden Banken und ich. Alle anderen Kunden der Bank haben damit nichts zu tun. Für die Korrektheit des Vorgangs steht die Bank gerade.

O-Ton – Thomas Rose:

Was macht die Bank? Die Bank speichert alle diese Transaktionen zentral in einer Datenbank und sorgt dafür, dass in dieser Datenbank Konsistenz herrscht. Sprich: Das ist so eine vollständig zentralistische Welt. Und die Idee der Blockchain ist jetzt, diese zentralistische Welt zu verteilen.

Autor:

In der Blockchain-Welt gibt es keine zentrale Verwaltung. Nehmen wir also an, jede und jeder von Ihnen wäre Teil eines fiktiven Computer-Netzwerks. Wieder möchte ich Herrn Rose 50 Euro überweisen. Diese Information fließt in der Blockchain-Welt an sämtliche Mitglieder des Netzwerks, einschließlich Herrn Rose. In der Blockchain-Sprache wäre das dann ein Block: „Sebastian Felser überweist Thomas Rose 50 Euro.“ (Stimme verzerrt). Eine Kopie dieses Informationsblocks ist in dieser Sekunde aber auch bei Ihnen allen, die dem Netzwerk angehören, angekommen, und wird in Ihrer Kopie der Gesamt-Datenbank abgelegt.

Natürlich geht es außer Herrn Rose und mich niemanden etwas an, was ich ihm überweise. Deshalb stehen in diesem Block keine Klarnamen, sondern anonymisierte Nummern. Das ist der Clou der Blockchain: die Verbindung aus einerseits Anonymität und andererseits voller Transparenz. Jeder kennt jede Transaktion und kann sie nachvollziehen, ohne diese Informationen personalisieren zu können. Auf diese Weise ist die Blockchain-Datenbank immer in sich schlüssig und im Nachhinein unveränderbar.

O-Ton – Thomas Rose:

Wenn Sie die jetzt verändern wollen, müssen Sie quasi den aktuellen Inhalt verändern und alle danach erfolgten Einträge in die Blockchain.

Autor:

Denn in einem echten Blockchain-Netzwerk können nicht nur Thomas Rose und ich einen Block in die Daten-Kette einspeisen. Alle teilnehmenden Rechner können das, so dass die Datenkette – und damit auch die Datenmenge – kontinuierlich wächst.

O-Ton – Thomas Rose:

Das hieße, Sie müssten alle anderen Informationen neu berechnen und neu bestätigen. Und dieser Aufwand, der ist einfach viel zu groß, da haben Sie keine Rechen-Kapazität für.

Musikakzent

Autor (verzerrte Stimme):

Die Blockchain-Technologie gilt als manipulationssicher, denn sie arbeitet mit einem aufwändigen Verschlüsselungsverfahren, also über Kryptografie – daher auch der verbreitete Name „Krypto-Währung“. Konkret funktioniert das so: Übermittle ich eine Transaktion, gebe ich ein kleines Mathematik-Rätsel mit. Eine einfache Version könnte so aussehen: „Nimm eine zufällige Zahl zwischen 1 und 5 – multipliziere mit zwei – subtrahiere 1 – multipliziere mit 9. Das Ergebnis hat eine Quersumme, also die Summe der Ziffernwerte der Lösung. Wenn alles richtig gelaufen ist, lautet die Quersumme wieder 9.“

Autor:

Alle im Netzwerk rechnen mit und die oder der erste, die das Ganze bestätigen, schreiben den neuen Block. Er wird über Rätsel und Lösung mit dem vorangegangenen Block unwiderruflich verschränkt. So lässt sich auch nicht einfach heimlich ein Block „dazwischenschieben“, denn sonst passen Rätsel und Lösung nicht mehr zueinander.

Musikakzent

Autor:

Die Rätsel in einer echten Blockchain-Anwendung sind natürlich deutlich komplizierter. Es ist sehr aufwendig, sie zu lösen. Und weil alle mitrechnen müssen, ist auch der Energie-Aufwand für Blockchain-Netzwerke derzeit enorm. Jeder rechnende Computer verbraucht schließlich Strom. Dafür ist das Ergebnis fälschungssicher.

Das macht das Blockchain-Verfahren so sicher, obwohl es keine zentrale Autorität gibt, wie zum Beispiel eine Bank. Im Moment sind unzählige Menschen im Bankensektor nur damit beschäftigt, die Korrektheit der Transaktionen zu gewährleisten. Wenn diese Aufgabe über das Blockchain-Verfahren erledigt würde – dann eröffnete das ein gigantisches Spar-Potenzial. Die spanische Bank Santander hat berechnet, dass sich so weltweit 15 bis 20 Milliarden Dollar einsparen ließen – pro Jahr! Nicht

schön für die Beschäftigten, die auf diese Weise überflüssig würden. Umso schöner für viele Markt-Teilnehmer, die von der Technik profitieren – wie eben auch Facebook mit seinem Digital-Geld „Libra“.

O-Ton – Dirk Elsner:

Den Haken bei Libra suche ich noch. Ich fand das doch sehr durchdacht für so eine frühe Phase. Das ist meine persönliche Meinung. Da wird man sich als Bank insgesamt Gedanken machen müssen.

Autor:

Räumt Dirk Elsner ein. Er ist Projektleiter im Innovationslabor der DZ-Bank – das ist die Geschäftsbank der Volks- und Raiffeisenbanken. Tatsächlich könnten auch die Bank-Kunden von den Einsparungen durch die Blockchain-Technik profitieren. Angenommen, ich verwalte mein Geld nicht mit einem Konto bei einer klassischen Bank, sondern per Blockchain-Anwendung, zahle ich weder Kontoführungs- noch Überweisungsgebühren. Damit wirbt auch das „Libra“-Konsortium:

Musikakzent

Sprecherin (Stimme verzerrt):

Auf der ganzen Welt zahlen unvermögende Menschen mehr für Finanzdienstleistungen. Das hart verdiente Einkommen wird durch Gebühren aufgefressen. Libras Mission ist es, eine einfache, globale Währung und eine finanzielle Infrastruktur für Milliarden von Menschen bereitzustellen, die ihnen das Leben leichter machen. Die Zeit ist reif für die Schaffung einer neuartigen digitalen Währung, die auf Blockchain-Technologie basiert.

Autor:

Trotz dieser Versprechen glaubt Elsner nicht, dass Banken bald überflüssig sein könnten. Er rechnet damit, dass die Banken die Blockchain-Technologie in ihre Systeme integrieren werden. Nicht nur, weil viele Staaten befürchten, ein Konzern wie Facebook könnte sich mit „Libra“ zu einer Schatten-Zentralbank aufspielen. Nein, die Verbraucher selbst seien schlicht nicht bereit, die Banken aus der Pflicht zu nehmen und selbst das Verlust-Risiko ihrer Geld-Bestände in der Blockchain zu übernehmen.

O-Ton – Dirk Elsner:

das Risiko, dass ich etwas verliere oder überfallen werde. Das wäre die Alternative, wenn man kein Konto hat. Da kann jeder selber mal überlegen, was einem das wert ist. Ich denke, da liegen die Preise für Konten, für Zahlungsverkehr deutlich drunter.

Musikakzent

Autor:

Wer sein Geld in Form von „Bitcoin“ oder künftig vielleicht „Libra“ hortet, ist selbst für die Sicherung seiner Zugangsdaten verantwortlich. Es gibt keinen Notruf-Service, keine Zentral-Instanz, die mein Konto gegen Missbrauch sperrt. Es gibt auch niemanden, der einen Zugriff wiederherstellen kann. Geht bei „Bitcoin“ etwa der 81-stellige persönlichen Zahlenschlüssel, der „Personal Key“, verloren, ist das ein

echtes Problem. Es ist sogar *das* zentrale Problem der neuen Technologie heute, sagt der Blockchain-Unternehmer Julian Hosp:

O-Ton – Julian Hosp:

Wie speichert man diesen Key so ab, dass man ihn selbst nicht verliert, dass aber andere Leute nicht darauf zugreifen können und genau dieses Problem, ist die größte Hürde meiner Ansicht nach, dass das massentauglich wird.

Autor:

Denn kommt einem der „Personal Key“ abhanden oder gerät er in die falschen Hände, ist er auf immer verloren. Nutzer, die sich etwa bei „Bitcoin“ registrieren, können ihn nämlich nicht selbst festlegen. Erstellt ein Nutzer einen neuen „Bitcoin“-Account, sucht ein Zufallsgenerator den „Personal Key“ aus. Das soll eigentlich ein Sicherheitsmerkmal des Blockchain-Verfahrens sein.

O-Ton – Julian Hosp:

Das klingt immer am Anfang so wahnsinnig, weil man denkt, was ist, wenn sich jetzt zwei Leute dasselbe Konto aussuchen? Die Wahrscheinlichkeit, dass sich zwei Leute dasselbe Konto aussuchen, ist deutlich geringer, als dass in der nächsten Sekunde ein Asteroid, den wir komplett übersehen haben, bei uns auf die Erde stürzt und uns komplett auslöscht. Das heißt, wahrscheinlichkeitstechnisch brauchen Sie sich überhaupt keine Sorgen machen, dass sich irgendjemand dasselbe Konto aussucht wie jemand anders, weil es einfach so unglaublich viele Möglichkeiten gibt.

Autor:

Mehr Kombinationsmöglichkeiten als Atome im sichtbaren Universum bietet dieser 81-stellige „Personal Key“, betont Hosp. Die Macher von „Bitcoin“ waren sich ihrer Sache so sicher, dass es noch nicht mal ein Passwort braucht. Das führt aber auch in ein Dilemma: Kaum ein Mensch kann sich diesen „Personal Key“ merken. Also müssen Nutzer ihn speichern. Aber was ist, wenn Unbefugte Zugang zu diesem Speicherort bekommen? Wenn das Speichermedium abhanden kommt? Jeder, dem das passiert, ist sein Vermögen los. Das ist zahlreichen Früheinsteigern bei „Bitcoin“ passiert, die jetzt Millionäre sein könnten. Sie kommen nie mehr an ihr Geld ran. Also selbst wenn die Leute im ersten Schritt auf Banken verzichten würden, brauchen sie doch jemanden, der sie gegen einen möglichen Verlust absichert. Hier wittern die Banken wiederum ihre Chance, sagt Banker Dirk Elser:

O-Ton – Dirk Elser:

Die Challenger- oder Fintech-Banken, wie man die heute kennt, bieten Ihnen zum Beispiel an, dass Sie diese Krypto-Guthaben dort auf ein Konto speichern können in einer Wallet dort. Das heißt, die verwalten für Sie die Wallet und vereinfachen den Vorgang ganz erheblich.

Autor:

Eine Wallet ist eine digitale Brieftasche. Sie enthält den „Personal Key“, also den Zugang zum Konto. Das Ganze lagert dann dort, wo das Geld schon immer lag: auf der Bank. Die Banken verfügen bereits über die Infrastruktur, einen solchen Service gegen Gebühr anzubieten – Filialen, Mitarbeiter, Service-Hotlines und sichere Computer-Netzwerke. Sie sind aber nicht die einzigen, die hier ihre Chance wittern.

Wenn Facebook und das „Libra“-Konsortium im Jahr 2020 tatsächlich an den Markt gehen, nutzen sie genauso ihre Macht und Infrastruktur. Denn über zwei Milliarden Menschen weltweit verfügen bereits über ein Konto bei Facebook, WhatsApp oder Instagram. Diese Nutzer-Konten im Hintergrund mit einem Blockchain-System zu verbinden, um Zahlungen zu ermöglichen, bringt den Machern per Knopfdruck mehr Kunden ein als jede Bank hat. Gewinner der großen Blockchain-Wette auf die Zukunft wird, glaubt Julian Hosp, die Firma...

O-Ton – Julian Hosp:

... die dieses Problem löst: Wie kann denn jemand, der technisch nicht affin ist, der das System auch überhaupt nicht versteht, der das nicht kapiert, diesen Key abspeichern? Das muss ja die Zukunft sein. Der Grund, warum das Internet heute so gut funktioniert, ist: Die Leute verstehen das Internet nicht. Brauchen sie nicht. Alles, was sie wissen, ist, ich schalte mein Handy ein und nutze WhatsApp. Ich schalte mein Handy ein und gehe ins Internet. Das ist alles – ich muss ja nicht die ganzen Protokolle dahinter verstehen. Die ganzen Smart Contracts bauen alle auf demselben Konzept auf, dass du dir einen Key generierst per Zufallsgenerator und du den irgendwie irgendwo speichern musst und das ist die riesengroße Hürde.

Autor:

Eine Hürde, die das „Libra“-Konsortium überwinden könnte: Für die Nutzer verkompliziert sich nämlich nichts. Sie loggen sich über Benutzernamen und Passwort in ihr Facebook-, WhatsApp- oder Instagram-Konto ein. Damit haben sie auch Zugang zu „Libra“. Das Speichern des „Personal Keys“ für das Blockchain-System im Hintergrund übernimmt der Konzern.

Atmo:

Maschinenfahrgeräusche

Autor:

Neben der Bahn und den Banken prüfen noch sehr viele andere Unternehmen derzeit, ob sie das Blockchain-Konzept für sich nutzen können. Ähnlich wie die Bahn wollen etwa Handels- und Transportunternehmen ihre Lieferketten via Datenkette effizienter gestalten. So könnte zum Beispiel ein Supermarkt automatisch ans Großlager melden, wenn die Schokoriegel ausgehen. Hier hätten dann Supermarkt-Regale und Waren-Chargen jeweils ihre „Personal Keys“ und könnten über digitale Verträge den Nachschub regeln – ebenfalls reibungsärmer und mit deutlich weniger Personal. Niemand müsste mehr nachzählen, ob wirklich noch 50 Kisten Snickers, Kinderschokolade oder Toblerone da sind.

Autor:

Der Blockchain-Unternehmer Julian Hosp hat sich mit einem weiteren Anwendungsfall beschäftigt: der Medizin. Hosp hat nämlich als Arzt gearbeitet, bevor er ins Blockchain-Geschäft eingestiegen ist.

O-Ton – Julian Hosp:

Dann habe ich zum ersten Mal wirklich verstanden: Wow, über diesen dezentralen Datenspeicher, wo niemand und jeder irgendwie alles speichert, wäre es möglich, dass Patienten ihre eigenen Daten speichern. Die könnten dann zu einem anderen

Krankenhaus gehen, zu einem anderen Arzt gehen – hätten dort wieder die Daten, aber schlussendlich könnte sie niemand hacken.

Autor:

Die Bundesregierung versucht sich schon lange an der Digitalisierung der Patientenakte – bisher vergeblich. Die digitale Patientenakte soll viele Vorteile bringen: Wechsle ich zu einer neuen Ärztin, könnte die sofort auf alle meine Daten zugreifen. Im Notfall auch ein Krankenhaus. Dort wären dann etwa auch Unverträglichkeiten zum Beispiel für Narkose-Mittel angegeben.

O-Ton – Julian Hosp:

Also, ich glaub, die ganze Datenspeicherung mit Medizin-Daten, das wird jetzt sicher gelöst werden von Firmen. Also, da weiß ich, dass Firmen dran sind. Das ist sicher etwas total Spannendes.

Musikakzent

Autor:

Ob tatsächlich so schnell so viele Daten in Blockchain-Anwendungen landen, ist allerdings fraglich. Das BSI, das Bundesamt für Sicherheit in der Informationstechnik, hat sich ausführlich mit den Risiken der Blockchain-Technologie beschäftigt.

Dort arbeitet Manfred Lochter. Er ist Mathematiker und Experte für Quanteninformatik am BSI. Die Quanteninformatik beschäftigt sich mit der Entwicklung von Quantencomputern. Sie nutzen anstatt der Gesetze der klassischen Physik die der Quantenmechanik. Ein Computer, der auf der Basis von Quantenzuständen rechnet, hat die Möglichkeit, mit unglaublich großen Zahlen zu rechnen. So kann er – in der Theorie – auch enorm große Datenmengen bewältigen. Ein 81-stelliger „Personal Key“ etwa wäre, lapidar ausgedrückt, für einen Quantencomputer ein Klacks. Das ist auch die Sorge von Manfred Lochter.

O-Ton – Manfred Lochter:

Die Sicherheit in der Blockchain, die wird im Moment garantiert durch kryptografische Mechanismen und keiner ist in der Lage, zu garantieren, dass die Algorithmen, die man heute verwendet, in 10 Jahren noch sicher sind. Insofern kann man da keine Ewigkeitgarantien abgeben. Wenn Sie sich jetzt denken: Ich lege Daten sicher in einer Blockchain ab, also verschlüsselt, ist das erst mal kein Schutz, weil die Daten ja verteilt gespeichert sind.

Autor:

Er hält Folgendes für denkbar: Kriminelle könnten eigentlich gewollte, legitime Kopien einer Blockchain-Datenbank vom Netzwerk trennen. Auch wenn sie sie heute vielleicht nicht entschlüsseln können – mit der übernächsten Computer-Generation wird das eventuell möglich sein.

O-Ton – Manfred Lochter:

Deswegen ist Speichern von Daten direkt auf der Blockchain bei Langzeit-Sicherheit sowieso ein Problem – da wird man vielleicht doch wieder zu einem externen Speicher übergehen müssen und nur Verweise auf die Daten speichern.

Autor:

Denn Blockchain-Datenbank ist nicht gleich Blockchain-Datenbank. Sollte ein Verbrecher heute eine Datenbank abgreifen und in zehn Jahren entschlüsseln, könnte er darauf ja die unterschiedlichsten Informationen finden: Ob der ICE 101 auf seiner Fahrt von Mannheim nach Karlsruhe einen Umweg nehmen musste, interessiert 2029 niemanden mehr. Ebenso wenig, ob ein Supermarkt zehn Kisten Schokoriegel nachbestellt hat. Dass ich Thomas Rose 50 Euro überwiesen habe, könnte schon eher von Interesse sein.

Wirklich heikel wird es aber bei den Medizin-Daten. Welche Krankheit einen Patienten vor zehn Jahren ein halbes Jahr außer Gefecht gesetzt hat, ist auch in zehn Jahren noch eine höchst sensible Information. Auch deswegen scheint weniger die Frage zu sein, ob, wie oder wann genau die Blockchain-Technologie kommt. Die Frage ist, wo sie sinnvoll sein kann, meint auch Thomas Rose vom Blockchain-Labor des Fraunhofer Instituts:

O-Ton – Thomas Rose:

Ich glaube, der erste Hype der Blockchain-Technologie ist vorbei, wo wir sehr viele Anwendungen gemacht haben, um zu demonstrieren, was damit geht. Das ist nur eine geringe Zahl von Anwendungen, die wirklich gut Blockchain-tauglich sind.

Autor:

Mit der Blockchain hat sich eine neue Technologie aufgetan, die große Wirkung entfalten kann. Schritt für Schritt wird sie in unseren Alltag einziehen. Oft werden wir sie gar nicht bemerken. Vielleicht wissen wir erst in 30 Jahren, was sie wirklich gebracht hat.
