Ihre digitale Identität in der Blockchain verwalten

Identity and Access Management mit der Blockchain: So kommen Sie zu einer digitalen Identität, mit der Sie Ihre persönlichen Daten und Berechtigungen verwalten und entscheiden, wem Sie welche Daten wofür zur Verfügung stellen. ***Veröffentlicht am 01.06.2017 auf www.pcwelt.de***

Verwalten Sie persönliche Daten und Berechtigungen mittels digitaler Identitäten in der Blockchain.

Einleitung

Die zahlreichen Abfragen von Benutzernamen und Passwörtern beim täglichen Surfen durch das Internet führen uns dessen Wesen als gewaltige dezentral gewachsene Struktur ständig vor Augen.

Demgegenüber steht die zunehmende Ballung zahlreicher Online-Dienste in den Händen weniger großer Anbieter. Genau diese Online-Dienste sprechen gegen die dezentral gewachsene Struktur: Personenbezogene Daten der Kunden werden zentral von einer Instanz verwaltet und verarbeitet, wodurch ein starkes Vertrauen in diese Instanz vorausgesetzt ist.

Aus dieser Situation heraus entwickelt sich immer stärker die Vision einer eigenen, selbstverwalteten digitalen Identität, die den Nutzer ausweist und so das Potenzial hat, die Verwaltung dutzendfacher separater Accounts überflüssig zu machen. Heute gibt es schon viele IDaaS (Identity as a Service)-Lösungen, die es ermöglichen, mit nur einem Account bzw. einer Authentifizierung auf verschiedene Services zuzugreifen (Single-Sign-On).

Das Problem hierbei: Wieder wird das Vertrauen in eine zentrale Instanz, nämlich den Betreiber der IDaaS-Lösung, vorausgesetzt. Um wirklich Herr über die eigenen Daten zu werden, ein Vertrauen in eine zentrale Instanz zu relativieren und trotzdem eine Single-Sign-On-Funktionalität zu gewährleisten, sollte

man den Gedanken der dezentralen Struktur des Internets forcieren.
Die Technologie, die dies ermöglichen könnte, ist eines der maßgeblichen zukunftsweisenden Themen des Jahres 2017: Blockchain.

Hinter dem Schlagwort „Blockchain" verbirgt sich das Konzept einer auf ein globales Netzwerk verteilten Datenbank, die von verschiedenen Teilnehmern betrieben wird. Transaktionen oder Aktualisierungen der Informationen in der Datenbank werden in Datenblöcken (Blocks) organisiert, die wiederum in linearer Abfolge aneinandergekettet (Chain) werden. Auf diese Weise wird die Datenbank beständig erweitert, sobald sich die Teilnehmer bzw. Betreiber einer Blockchain auf einen neuen hinzuzufügenden Block verständigt haben.

Mehr Informationen zur Funktionsweise der Blockchain und zum Konzept „Bring Your Own Identity" finden Sie im Positionspapier „Blockchain" des Teletrust – Bundesverband IT-Sicherheit e. V.

Jeder Teilnehmer (Node) ist im Besitz einer Kopie der kompletten Datenbank. Die durch Hashwerte bezeugte lineare Abfolge von Blöcken macht die rückwirkende Änderung von Transaktionen praktisch unmöglich. Zusammen mit der Absicherung der Nutzer durch Public-Key-Kryptographie machen diese Eigenschaften die Blockchain-Technologie besonders sicher.

Digitale Identität in der Blockchain

Derzeit liegt die Hauptverantwortung für die Verwaltung großer Mengen an Identitätsdaten (inklusive Vergabe maßgeschneiderter Zugriffsberechtigungen) noch bei den entsprechenden Unternehmen.

Projekte wie Uport oder Blockstack deuten ein grundlegend neues Konzept an: Die Verwaltung von persönlichen Daten und Berechtigungen mittels digitaler Identitäten über die Blockchain.

Das Prinzip einer solchen digitalen Identität ist nicht nur auf Personen beschränkt, auch Unternehmen oder Services können hinter einer digitalen Identität stehen. Diese Identitäten können mit weiteren Informationen, etwa personenbezogenen Daten, angereichert werden. Die Freigabe dieser Daten zur Nutzung durch Dritte obliegt dann dem Inhaber.

Man kann punktuell entscheiden, welche personenbezogenen Daten zu welchem Zweck kommuniziert werden, beispielsweise beim Kauf von Waren, die ein bestimmtes Alter voraussetzen. Der Verkäufer fragt beim Nutzer nach der Information „Alter über 18" an. Nur diese Information wird durch die digitale Identität weitergegeben - weitere personenbezogene Daten von Ausweisdokumenten, wie die Anschrift, bleiben im Verborgenen.

Es fände also ein Paradigmenwechsel statt. Anstelle der zentralen Verwaltung von Identitäten durch Unternehmen oder Dienstleister tritt künftig der Nutzer selbst als Herr über seine eigenen Daten und den Zugriff auf diese auf. Die umfassende Adaption einer solchen Blockchain-Lösung und die Schaffung einer effizienten Berechtigungsstruktur zwischen verschiedenen Diensten und Nutzern würde ein „Bring Your Own Identity" ermöglichen und das eingangs formulierte Dilemma lösen.

Mit der Realisierung digitaler Identitäten über Blockchains profitieren alle Beteiligten vom hohen Maß an Sicherheit. So können bei der Nutzung einer digitalen Identität auf Basis der Blockchain-Technologie neue Anforderungen im Datenschutz durch die EU-Datenschutz-Grundverordnung (EU-DSGVO) gelöst werden, da die Idee, dem Nutzer wieder die vollständige Kontrolle seiner eigenen Daten wiederzugeben, mit den Schutzzielen der EU-DSGVO einhergeht.

Konsensfindung

Ein charakteristisches Merkmal einer jeden Blockchain ist das verwendete konsensfindende Verfahren. Dieses regelt, wie sich die Nodes auf eine Aktualisierung oder

Transaktion der Datenbank, also die Akzeptanz eines neuen Blocks, einigen und so ihre Integrität sichern.

Diese Konsensfindung ist zwingend notwendig, damit Vertrauen in eine blockchain-basierte Identity-and-Access-Lösung gewährleistet werden kann und eine vertrauenswürdige zentrale Instanz überflüssig wird.

Zu den am weitesten verbreiteten Verfahren der Konsensfindung zählen Proof-of-Work sowie Proof-of-Stake, die nachfolgend erläutert werden.

Doch zunächst lohnt sich ein Ausflug in die Kryptowährungen, um die Evolution der konsensfindenden Verfahren nachvollziehen zu können.

Mit der Aufnahme von Transaktionen in der Blockchain erhalten diese im Use-Case der Kryptowährungen (wie Bitcoin) ihre Gültigkeit. Bei einem - wenn auch nur temporären - Dissens könnte ein und dieselbe Währungseinheit (Coin) mehrfach (jeweils einmal pro kursierender Version der Blockchain) ausgegeben werden, wobei bei einer erneuten Einigung auf den „richtigen" Zweig der Blockchain alle nicht in diesem enthaltenen Transaktionen hinfällig werden – mit fatalen Auswirkungen für damit verbundene Geschäfte.

Diese Einigkeit beim Fortsetzen der Kette ist nötig, um einem solchen sogenannten Double Spending entgegenzutreten. Der (von Bitcoin verwendete) Proof-of-Work-Mechanismus ist das erste etablierte Konsensverfahren. Das Recht, einen neuen Block mit Transaktionen an die Blockchain anzuhängen und im Gegenzug Transaktionsgebühren und/oder neu erzeugte Coins zu erhalten, ist mit der - in der Regel nur mit erheblichem Rechenaufwand bestimmbaren - Erstlösung einer kryptographischen Aufgabe (u.a. Bezug nehmend auf die Transaktionen und den Vorgängerblock) verbunden.

Mit der Veröffentlichung der so erweiterten Kette im Netzwerk beginnt die Suche nach dem nachfolgenden Block. Neben krypto-ökonomischen Fragestellungen wird mit diesem Verfahren auch der öffentlichen Natur der in diesem Bereich genutzten Blockchain Rechnung getragen: Jeder Node darf nicht nur die getätigten Transaktionen einsetzen, sondern kann auch die Erstellung eines neuen Blocks initiieren. Damit ist die Motivation vorhanden, Transaktionen sauber und beständig weiter zu verbuchen.

Als ältestes Konsensverfahren für Blockchains ist der Proof-of-Work auch das am häufigsten untersuchte Verfahren im Hinblick auf Nachteile und (wenn auch oft nur hypothetische) Angriffsflächen. In diesem Zusammenhang kursiert oft der Begriff der 51-Prozent-Attacke. Dies beschreibt ein Szenario, in dem eine Fraktion mehr als die Hälfte der Netzrechenleistung kontrolliert und auf lange Sicht durch Propagierung eines eigenen Blockchain-Zweigs mutwillig Transaktionen ausschließen oder Double Spendings durchführen kann.

Auch unter Umständen überdurchschnittlich profitable Strategien, etwa das geschickte Geheimhalten von gefundenen Blöcken und das Nutzen des Vorsprungs beim Finden neuer Blöcke (Selfish Mining), wurden bereits durch Forschungen erörtert.

Mit dem Proof-of-Stake-Konsensverfahren erfolgt ein Perspektivwechsel. Nicht durch Investitionen in eine externe Ressource in Form leistungsstarker Hardware, sondern durch Besitz von Coins, einer internen Größe, erhöhen sich die Chancen, einen Block hinzufügen zu dürfen (und wiederum entlohnt zu werden). Diese Bevorzugung größter Anteilseigner erfolgt im Vertrauen, dass diese das wenigste Interesse an möglichen Manipulationen oder Angriffen und einem folgenden Währungsverfall haben.

Ein häufig beschriebener Nachteil beim Proof-of-Stake ist eine als „Nothing at Stake" bezeichnete Problematik. Konsensfindung wird dabei dadurch erschwert, dass für Block-Ersteller keine wirtschaftliche Notwendigkeit besteht, nur eine Version der Blockchain fortzuführen, sondern auch ein Ansetzen von Blöcken an Verzweigungen der Kette profitabel sein kann.

Attraktiv für die Verwirklichung digitaler Identitäten sind nach derzeitigem Forschungsstand etwa Public Permissioned Blockchains, die die gewohnte Transparenz bei der Einsicht der Transaktionen bieten, die

Verarbeitung von Transaktionen allerdings einem dazu berechtigten Konsortium übertragen. Ein solches Konsortium könnte aus Unternehmen bestehen, die ihrerseits vom geringeren administrativen Aufwand durch digitale Identitäten auf der Blockchain und einfacheren, branchenübergreifendem Standards profitieren.

Die Konsensfindung beim Erstellen neuer Blöcke gestaltet sich in diesem Rahmen einfacher und schneller. Während etwa beim Proof-of-Work durchschnittliche Block-Erstellungszeiten im Minutenbereich durchaus verbreitet sind, können beispielsweise BFT-Algorithmen (Byzantine Fault Tolerance) in einem gut vernetzten Konsortium einen annähernd sofortigen Konsens finden. Die Erstellung neuer Identitäten oder Vergabe von Berechtigungen geschieht also nahezu in Echtzeit. Abgesehen davon werden viele Angriffsszenarien der Public Permissionless Blockchains hinfällig.

Die genaue Abgrenzung zwischen Public und Private bzw. Permissioned und Permissionless im Themenbereich der Blockchains können Sie im Positionspapier „Blockchain" des Teletrust – Bundesverband IT-Sicherheit e. V. nachlesen.

Neben diesen Konsensverfahren existieren eine Reihe weiterer Methoden, die auch meist einen wettbewerbsartigen Charakter haben. Ein Ende dieser Entwicklung ist nicht absehbar, und es werden regelmäßig neue Konzepte und Hybridverfahren vorgestellt, um die Nachteile der Vorgänger zu eliminieren.

Die eine digitale Identität …

… für jeden Webservice, für die Nutzung beim Arbeitgeber oder auch bei Behörden. Das Konzept, seine Identität selber zu verwalten und überall mitzubringen, wo man es möchte. Bring Your Own Identity ohne Vertrauen in eine zentrale Instanz ist selbstverständlich nur möglich, wenn man einem dezentralen System Vertrauen schenkt. Genau hierfür benötigt man unanfechtbare konsensfindende Verfahren, bei denen aktuell sichtbare Umbrüche in den verschiedenen Blockchains stattfinden.

Verfahren wie Proof-of-Work, die die Bereitstellung hoher Rechenkapazitäten voraussetzen, sind gerade wegen des hohen Ressourcenverbrauchs nicht immer die erste Wahl. Proof-of-Stake, ausgestattet mit einer immer besser werdenden Absicherung gegen die Nothing-at-Stake-Problematik (etwa der Casper-Algorithmus, der bei Ethereum eingesetzt werden soll), erfreut sich wachsender Beliebtheit. Mit neuen Methoden zur kostengünstigen und schnellen Konsensfindung im Netz ist eine entscheidende Voraussetzung für das Erschließen neuer Anwendungsbereiche für Blockchains abseits der Kryptowährungen erfüllt.

Identity and Access Management via Blockchain-Technologie könnte eine Revolution im Markt der IDaaS-Provider hervorrufen. Innovativer, disruptiver Ansatz oder doch nur Hype? 2017 wird dafür ein entscheidendes Jahr sein, in dem sich die oftmals nur theoretischen Ansätze praktisch umsetzen lassen müssen.

Die **esatus** AG ist ein mittelständisches IT-Beratungsunternehmen. Als „The CISO Consulting Company" ist die esatus AG der qualifizierte, erfahrene und flexible Ansprechpartner für Projekte rund um das Thema Informationssicherheit. Für Kunden werden optimale und individuell gestaltete Lösungen für Herausforderungen in den Bereichen Identity & Access Governance, IT Security, sowie Governance, Risk und Compliance angeboten. Zudem bietet die **esatus** AG eine umfassende Beratung zur Thematik des IT-Sicherheitsgesetzes an, beispielsweise zur Einrichtung einer Meldestruktur. Die Zufriedenheit von Kunden ist der Leitfaden, nachdem sich das gesamte Handeln de Unternehmens richtet.

Herausgeber **esatus** AG

Grafik Seite 1 © Fotolia / Denys_Rudy

Weitere Informationen zum Thema „Blockchain" bei der **esatus** AG finden Sie unter: esatus.com

Stand der Informationen im vorliegenden Whitepaper: Juni 2017