Datenschutz

Blockchain sichert Datenintegrität

[15.08.2022] Digitale Dokumente sind leicht manipulierbar, können gefälscht und verändert werden. Ihre Authentifizierung wird für viele Prozesse im Rahmen der Digitalisierung jedoch immer wichtiger. Hier kann die Blockchain-Technologie Abhilfe schaffen.

Die EU-Datenschutz-Grundverordnung (DSGVO) sieht den Schutz personenbezogener Daten als besonders wichtig an. Sie müssen so verarbeitet werden, dass eine angemessene Sicherheit gewährleistet wird – dazu gehört der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung. Vertraulichkeit und Integrität der Daten sowie Verfügbarkeit und Belastbarkeit der Systeme müssen zu jeder Zeit gegeben sein. Um das angemessene Schutzniveau vorhalten zu können, müssen Unternehmen, die personenbezogene Daten verarbeiten, gemäß Artikel 32 DSGVO geeignete technische und organisatorische Maßnahmen treffen: Artikel 5 legt eine Vielzahl von allgemeinen Grundsätzen für die Verarbeitung fest. Jeder Verantwortliche muss diesen nachkommen – es besteht eine Rechenschaftspflicht.

Notarisierung mit der Blockchain

Elektronische Dokumente mit personenbezogenen Daten sind leicht zu manipulieren, sie können kopiert und verändert werden. Dieses Problem wird auch von einer digitalen Signatur nur unzureichend gelöst. Mit der Blockchain kann die Authentifizierung von Dokumenten, die analog zum Beispiel mit einer Unterschrift verifiziert wurden, digital erfolgen. Damit sind Dokumente ortsunabhängig als echt zu erkennen, können zur Verfügung gestellt und verarbeitet werden: Mit Blockchain-Technologie können also Integrität, Vertraulichkeit und Verfügbarkeit und damit der Datenschutz gewährleistet werden.
Die Blockchain ist vor allem durch die Kryptowährung Bitcoin, die 2009 als erste Anwendung überhaupt eingeführt wurde, bekannt geworden. Sie ist dezentral (Peer to Peer) organisiert – alle Teilnehmer sind gleichberechtigt – und bietet eine hohe Ausfallsicherheit und Transparenz, da jede Aktion öffentlich einsehbar ist. Gleichzeitig sind die Nutzer nicht rückverfolgbar, was wiederum Anonymität und Vertraulichkeit schafft: Daten, die in der Blockchain abgelegt wurden, erlauben keine Rückschlüsse. Zudem sind sie unveränderbar; sie können nicht gelöscht werden, es ist lediglich möglich, neue hinzuzufügen. Die Blockchain-Technologie verhindert so, dass hinterlegte Daten manipuliert oder gefälscht werden können. Auch ein Diebstahl ist ausgeschlossen.

Transaktion mit mehreren Teilen

In der Blockchain werden Dokumente mit der Notarisierung, einer Transaktion mit mehreren Teilen, authentifiziert: Beim Erstellen einer Notarisierung wird ein eindeutiger digitaler Fingerabdruck des Dokuments, der so genannte Hashwert, berechnet und mit einem Zeitstempel und einer Transaktions-ID in einer Blockchain unveränderbar protokolliert. Damit kann bewiesen werden, dass ein elektronisches Dokument zu einem bestimmten Zeitpunkt in einer bestimmten Form existiert hat und seither nicht verändert wurde.
Für die Notarisierung wird das ausgewählte Dokument nicht auf den Server hochgeladen, sondern der Hashwert wird lokal im Browser errechnet: Das bedeutet, dass keine Inhalte oder sonstige personenbezogene Daten in die Blockchain übertragen werden. Soll später verifiziert werden, dass das

betreffende Dokument zu einem gewissen Zeitpunkt existiert hat und nicht verändert wurde, werden die Daten aus der Blockchain abgerufen und mit den vorliegenden Informationen verglichen. Zur Überprüfung müssen entweder die Transaktions-ID oder der Hashwert vorliegen. Letzterer kann auch neu errechnet werden. Die entsprechenden Daten werden in der Blockchain gesucht und ausgegeben.

Vorteile einer Konsortium-Lösung

Die Blockchain-Anwendung, welche der Datenschutzspezialist Deudat entwickelt hat, basiert auf einer so genannten Konsortium-Blockchain. Bei dieser Variante des Aufbaus eines Blockchain-Netzes gehören die Betreiber der Blockchain-Knoten einem Konsortium an. Deudat betreibt einen solchen Knoten, die weiteren werden von den Vereinsmitgliedern der Blockchain Initiative Austria (bc-init. at) betrieben, in welcher der Hersteller Mitglied ist. Nur Teilnehmer der Blockchain Initiative Austria können Daten in die Blockchain schreiben.
Ein weiterer Vorteil liegt darin, dass im Gegensatz zu öffentlichen Blockchains kein unnötig hoher Energiebedarf notwendig ist. Durch den Aufbau des Netzes ist die Verfügbarkeit der Daten sichergestellt: Das Konsortium stellt die Server bereit – auch bei einem Ausfall können Daten verglichen und abgerufen werden.
Nach dem Eintrag der Informationen in die Blockchain werden die Ergebnisse wie Zeitstempel, Hashwert und Transaktions-ID angezeigt und können in Form einer Bestätigung als PDF-Datei heruntergeladen werden. Die Übergabe des Hashwerts plus Metadaten an ein API erfolgt automatisiert. Die Bestätigung wird ebenfalls automatisiert erzeugt und als PDF-Datei abgelegt.

Use Case Krematorium

Mit seiner Blockchain-Lösung hat Deudat für das Rhein-Taunus-Krematorium bei Koblenz, das größte Krematorium Europas, die ärztliche Leichenschau datenschutzkonform digitalisiert und damit eine Blockchain deutschlandweit zum ersten Mal für Datenschutzzwecke eingesetzt. Im Krematorium erfolgt vor jeder Einäscherung die offiziell vom Staat beauftragte Leichenschau vor Ort durch einen Amtsarzt. Er stellt die natürliche Todesursache fest, dokumentiert das und gibt den Toten damit zur Einäscherung frei. Danach erhält das Gesundheitsamt die Dokumente. Es muss sichergestellt werden, dass die Papiere zur richtigen Person gehören.
Der Amtsarzt scannt nun die Belege wie Todesbescheinigungen oder Einäscherungsnachweise der Sterbefälle, führt die Leichenschau durch und gibt den Status an. Alle Daten werden an ein geschlossenes System übertragen. Die Authentifizierung des Arztes erfolgt via Unterschrift samt biometrischem Abgleich (durch ein RSA Zertifikat und 4D-Unterschriftsdaten). Er signiert die digitalen Dokumente mit einer rechtsgültigen Unterschrift als qualifizierte elektronische Signatur (QES) über ein SignPad. Danach werden die Daten im Rahmen des standardisierten Datenaustauschformats XPersonenstand angereichert und ihre Integrität geprüft. Die Notarisierung erfolgt im Anschluss automatisch mit einer API. Die Dokumente werden danach gesichert an das Gesundheitsamt übertragen. Ohne die Blockchain-Lösung und damit die Authentifizierung der Dokumente und die Bestätigung ihrer Echtheit vor der Behörde hätte die amtsärztliche Leichenschau nicht digitalisiert werden können.

Weitere Anwendungsmöglichkeiten

Mit der Blockchain kann die Integrität von elektronischen Dokumenten und damit allen Arten von Dateien sichergestellt werden. Im öffentlichen Sektor in Österreich wird sie bereits eingesetzt. Nun werden auch privatwirtschaftliche Anwendungen möglich. Das Unternehmen Deudat nutzt sie, um personenbezogene Daten und Dokumente zu schützen.

Doch die Use Cases gehen darüber hinaus: Über die Blockchain kann zum Beispiel ein unbestreitbarer Beweis von Geschäftskorrespondenz erbracht werden, ebenso von Kauf- und Lieferverträgen oder Rechnungen. Möglich ist auch der Schutz geistigen Eigentums etwa von Entwürfen, Musikstücken, Texten und Fotos oder Software. Gleichzeitig kann die Blockchain als Langzeitbeleg für Daten aus dem Produktionsprozess von Chargen, Seriennummern oder Funktionstests bei Maschinen fungieren. Daten der Supply Chain bei Transport und Logistik werden nachverfolgbar. Auch alle Arten von Zertifikaten, Zeugnissen oder sonstigen Bestätigungen können authentifiziert werden.
Zudem ergeben sich für Endverbraucher Einsatzmöglichkeiten: So könnten Qualitätssiegel etwa für die Herstellung eines Produkts in der Blockchain hinterlegt werden, die der Verbraucher dann via QR-Code auf der Verpackung ansehen kann. Er hat damit den Nachweis, wann und wo ein Produkt hergestellt und dass es seitdem nicht mehr verändert wurde.

()

Stichwörter: IT-Sicherheit, Datenschutz, Blockchain, Deudat