Blockchain

Digital und authentisch

[16.11.2021] Behörden müssen wichtige Dokumente dauerhaft sicher und unverfälscht aufbewahren. Dazu hat govdigital mit der Public Permissioned Blockchain eine Lösung entwickelt. Digitale Schulzeugnisse und Corona-Testzertifikate werden darüber bereits validiert.

Blockchain – Begrifflichkeit und Thema prägen seit mehreren Jahren immer wieder auch ideologisch aufgeheizte Diskussionen in der IT-Szene. Während sich die Blockchain-Technik in manchem industriellen Zweig nun auch praktisch Bahn zu brechen scheint, nähert man sich im öffentlichen Sektor insgesamt nur zögerlich. Eine der treibenden Kräfte ist die Ende 2019 gegründete Genossenschaft govdigital, die seit Sommer 2021 eine produktive Blockchain betreibt und der öffentlichen Hand Blockchain Infrastructure as a Service anbietet.
govdigital nutzt dafür eine so genannte Public Permissioned Ethereum Hyperledger Besu Blockchain, die über neun öffentliche Rechenzentren läuft. Zu diesen Knotenbetreibern aus der govdigital-Mitgliedschaft gehören ausschließlich renommierte IT-Dienstleister, die sich über ganz Deutschland verteilen. Anders als bekannte Systeme wie Bitcoin wird die govdigital-Blockchain also durch absolut vertrauenswürdige öffentliche Akteure betrieben: Sämtliche Rechenzentren „kennen“ sich sehr gut. Alle sind mindestens durch den internationalen Standard 27001 zertifiziert.

Systemisches Misstrauen entfällt

Dieses Umfeld bringt eine Reihe von Vorteilen mit sich. Im Vergleich zu anonymen Blockchain-Systemen entfällt das systemische Misstrauen gegenüber anderen Teilnehmern. So entsteht etwa beim Bitcoin ein enormer Energieverbrauch im so genannten Mining-Prozess, weil Akteure ihre Blockchain-Einträge mit Hardware und sehr viel Rechenkapazität durch das Lösen komplexer mathematischer Aufgaben verifizieren müssen (Proof of Work). Denn bei jedem neuen Block muss die Mehrheit zustimmen, dass die aktualisierte Version der verteilten Datenbank korrekt ist, um sie als neue Variante zu akzeptieren. Dabei darf kein Akteur über 50 Prozent der Blockchain übernehmen. Das würde dem Netzwerk die Legitimation nehmen. Die Public Permissioned Chain von govdigital funktioniert nach einem anderen, moderneren Prüfsystem.
Die Konsensmechanismen Proof of Stake (PoS) und dessen Ableger Proof of Authority (PoA) basieren auf einem Vertrauensmodell von wenigen und sich gegenseitig bekannten Akteuren. Die Knotenbetreiber haften dabei sozusagen mit ihrem guten Namen. Dadurch entfällt der Wettbewerb um Rechenleistung. Stattdessen wird jeder neue Block durch die bekannten Teilnehmer des Netzwerks auf einfache Weise validiert. Das spart enorme Ressourcen: Während die Bitcoin-Blockchain mittlerweile so viel Strom verbraucht wie ein mittleres Industrieland, kommt ein einzelner Knoten im govdigital-Netzwerk in etwa mit der Menge eines heutigen Standard-PCs aus.

Nachvollziehbar und manipulationssicher

Was macht nun eine Public Permissioned Chain aus? Jeder kann die Blockchain von außen erreichen und lesen, was und welche nicht-personenbezogenen Hash-Werte in den Blöcken stehen – das ist public. Allerdings kann nur eine begrenzte Zahl von Befugten darüber entscheiden, was in die Chain aufgenommen wird (permissioned). So ist die Plausibilität der Informationskette von Anfang bis Ende auch

von außen nachvollziehbar und manipulationssicher – Transaktionen können nur durch die knotenbetreibenden Genossenschaftsmitglieder validiert werden. Eine weitere Besonderheit der Lösung liegt in der Servicequalität. Während Anwenderinnen und Anwender bei kommerziellen Blockchain-Angeboten nur FAQs finden, stehen bei govdigital konkrete Ansprechpartner zu festen Servicezeiten zur Verfügung. Das ist bundesweit einzigartig.
Die govdigital-Blockchain wird künftig noch weitere Knotenbetreiber hinzugewinnen. Das dezentrale Verfahren hat aber schon jetzt einen maßgeblichen sicherheitstechnischen Vorteil. Das System ist weder abhängig von lokalen noch von regionalen Ereignissen. Selbst wenn es zu mehreren Ausfällen käme, bliebe das Netzwerk durch seine Dezentralität, automatische Mechanismen und die enge betrieblich-organisatorische Zusammenarbeit produktiv – weder gehen Daten verloren, noch wird die Funktionsfähigkeit beeinträchtigt. Jederzeit können Informationen in die Chain aufgenommen und einzelne Blöcke ausgelesen werden.
Das ist nicht nur mit Blick auf die IT-Sicherheit wichtig, sondern künftig wohl auch aufgrund der Auswirkungen des Klimawandels. Zuletzt haben die Überschwemmungen in Rheinland-Pfalz und Nordrhein-Westfalen gezeigt, welche Konsequenzen diese sowohl für Leib und Leben als auch für leitungsgebundene Infrastrukturen vor Ort haben können. Ob Überflutungen, Brände oder Stürme – wichtige Leistungen der Daseinsvorsorge müssen auch in der Krise funktionieren und sind deshalb entsprechend aufzustellen.

Einsatz der Blockchain beim Corona-Testzertifikat

Genutzt wird die govdigital-Blockchain etwa für das Digitale Corona-Testzertifikat von Cybersecurity-Spezialist Ubirch. Führt ein Labor, das vom govdigital-Mitglied Bundesdruckerei authentifiziert wurde, einen Coronatest durch, verankert die Ubirch-Technologie einen digitalen Fingerabdruck des Ergebnisses in der govdigital-Blockchain. In Übereinstimmung mit der Datenschutz-Grundverordnung (DSGVO) und höchsten Datensicherheitsstandards liegt die Kontrolle über die Daten ausschließlich bei der betreffenden Person. Auf diese Weise lässt sich der zertifizierte SARS-CoV-2-Status einer Person jederzeit schnell und unkompliziert mithilfe eines QR-Codes überprüfen. Beispielsweise könnten so Passagiere ihr Testergebnis vor Abflug direkt am Gate verifizieren lassen.
Seit Sommer 2021 läuft in Deutschland zudem der Pilotbetrieb zum digitalen Schulzeugnis. Das System hat die Bundesdruckerei entwickelt, um Schulzeugnisse zu erstellen, zu sichern und datenschutzkonform zu prüfen. Dafür wird ebenfalls die govdigital-Blockchain genutzt (wir berichteten). Auftraggeber der Lösung ist das Finanzministerium Sachsen-Anhalt im Rahmen des Onlinezugangsgesetzes (OZG). Erste Anwender sind die Bundesländer Berlin, Nordrhein-Westfalen und Rheinland-Pfalz. Auch Hessen kündigte jüngst an, bis Ende dieses Jahres am Testbetrieb teilnehmen zu wollen. Schließlich könnten bis Ende 2022 alle interessierten Bundesländer an das Projekt angeschlossen werden – wiederum zunächst zur Probe, ab 2023 dann im Echtbetrieb.

()

Dieser Beitrag ist in der Ausgabe November 2021 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Blockchain, govdigital