Wie die Blockchain-Technologie Zertifikate fälschungssicher macht

Sicherheit in Ketten

WOLFGANG PRINZ

Zertifikate spielen eine wichtige Rolle in der Ausbildung, und individuelle Lernnachweise sind für die Dokumentation der während einer beruflichen Laufbahn erworbenen Qualifikationen unerlässlich. Daher ist es wichtig, dass diese Nachweise langfristig verfügbar sind und manipulationssicher verwaltet werden können. Die Blockchain-Technologie bietet dafür die notwendige Basis.

Universitäten und andere Bildungseinrichtungen bestätigen Abschlüsse und Leistungen bestimmter Lernergebnisse durch die Ausstellung von Zertifikaten. Diese werden bis heute meist auf Papier erstellt und enthalten in der Regel folgende grundlegenden Informationen: Art der Beglaubigung oder akademischer Titel, der bescheinigt wird; Name und Anschrift der ausgebenden Organisation; Name und Unterschrift des Zertifizierers, der die Tatsachen validiert hat und bescheinigt, dass die Qualifikation wahr ist; Name des Lernenden und Datum der Prüfung. Je nach Art des Zertifikats können zusätzliche Hinweise wie die Gültigkeitsdauer vorhanden sein. Die Lernenden erhalten das Zertifikat in der Regel als Papierdokument oder PDF. Beide Dokumenttypen haben den Nachteil, dass sie einfach zu fälschen sind und ihre Authentizität schwer zu überprüfen ist. Außerdem müssen die ausstellenden Institute über einen längeren Zeitraum ein Register oder eine Datenbank für ausgegebene Zertifikate unterhalten. Arbeitgeber können die Gültigkeit letztlich nur überprüfen, indem sie bei der ausstellenden Organisation nach der Echtheit und Gültigkeit des Zertifikats fragen. Dies ist ein zeitaufwändiger und teurer Prozess und wird daher oft unterlassen.

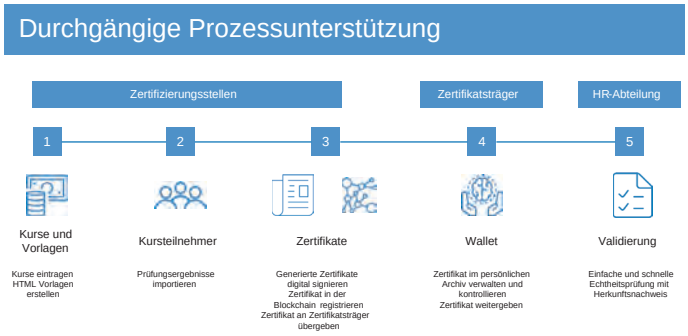
Weil sowohl als PDF als auch auf Papier ausgegebene Zertifikate leicht zu fälschen sind, lesen wir immer wieder Berichte über gefälschte Zeugnisse oder Abschlüsse oder – ganz aktuell – über gefälschte Impfpässe und Nachweise (Dursun & Saathoff, 2021). Zudem findet man im Internet problemlos Angebote zu käuflichen Diplomen oder Doktortiteln (Kolbeck, 2016). Zertifizierungsstellen, Universitäten und berufliche Weiterbildungseinrichtungen benötigen daher eine sichere, einfache und intuitiv nutzbare Lösung, die es erlaubt, Ausbildungsnachweise digital zu erstellen, zu verwalten und auf Echtheit zu prüfen. Die Blockchain-Technologie bietet mit ihrer Eigenschaft, Daten fälschungssicher und nachvollziehbar dezentral zu verwalten, die Grundlage für die Umsetzung entsprechender Lösungen (Prinz et al., 2018).

Sicherheit und Effizienz mit »Blockchain for Education«

Fraunhofer FIT hat mit der »Blockchain for Education«-Lösung eine webbasierte Plattform entwickelt, die fälschungssicheren Schutz sowie sicheres Management und einfache Überprüfung von Zertifikaten entsprechend den Bedürfnissen von Bildungseinrichtungen, Lernenden und Unternehmen unterstützt (Gräther et al., 2018). Die Lösung sorgt für höhere Effizienz und erhöhte Sicherheit für Zertifizierungsstellen durch die Digitalisierung aktueller Prozesse, durch das Ausstellen und die Registrierung von Zertifikaten in einer Blockchain sowie durch die automatische Überwachung von Zertifikaten. Das System unterstützt in der aktuellen Version maschinenlesbare Zertifikate auf Basis eines erweiterten Open Badges

Standards (IMS Global Learning Consortium Inc.), der bereits seit vielen Jahren zur Dokumentation von Kompetenzen und Lernnachweisen verfügbar ist.[1]

ABB. 1 Zertifikatserstellung & Zertifikatsmanagement in der Blockchain



Quelle: eigene Darstellung

→ ABB. 1 illustriert den Prozess der Zertifikatserstellung und des Zertifikatsmanagements in der Blockchain – von der Verwaltung der Zertifikatsvorlagen und Prüfungsdaten über die Registrierung der signierten Zertifikate in der Blockchain bis hin zur abschließenden Überprüfung der Gültigkeit des Zertifikats z. B. durch eine Personalabteilung. Zur Wahrung der Datenschutzgrundverordnung (DSGVO) werden in der Blockchain keine personenbezogenen Daten, sondern verschlüsselte »Fingerabdrücke« (so genannte Hashwerte) der digitalisierten Zertifikate gespeichert, anhand derer die Echtheit überprüft werden kann. Darüber hinaus ermöglicht die Plattform den Zertifizierungsstellen, Zertifikate zu widerrufen. Diese Funktion kann angewendet werden, wenn Plagiate entdeckt wurden, ein Fehlverhalten des zertifizierten Lerners nachgewiesen wurde oder die Lernenden die erforderlichen Auffrischungstrainings nicht absolviert haben.

Über eine einfach zu nutzende App, die auf Smartphones, Tablets und PCs läuft, können die Lernenden ihre Zertifikate und Abschlüsse sicher in einem Wallet, d. h. einer elektronischen Brieftasche verwalten. Die Brieftasche visualisiert die importierten Zertifikate, überwacht Zertifikate mit zeitlich begrenzter Gültigkeit, sie zeigt Ablaufzeiten an und bietet eine einfache Möglichkeit, Zertifikate mit potenziellen Arbeitgebern zu teilen.

Die Überprüfung der Zertifikate wird für Arbeitgeber durch einen einfach zu bedienenden webbasierten Prüfdienst gewährleistet. Wenn der Arbeitgeber das Zertifikat erhält, kann er es per Drag & Drop auf den Prüfdienst hochladen

1 https://openbadges.org/
2 www.w3.org/TR/did-core
3 www.w3.org/TR/vc-data-model

Blockchain für Bildungseinrichtungen

Die Blockchain-Technologie, außerhalb von Fachkreisen am ehesten bekannt durch die Aufmerksamkeit, die Kryptowährungen wie Bitcoin derzeit erhalten, beruht auf der dezentralen Sicherung, Verwaltung und Transaktion von Daten von und mit unterschiedlichen Partnern. Dabei kann niemand eine Änderung an den Daten vornehmen, ohne dass dies für alle nachvollziehbar wäre, sodass die so gesicherten Daten als fälschungssicher gelten.

Die »Blockchain for Education«-Plattform basiert auf verschiedenen miteinander integrierten Komponenten. In einer Quorum Blockchain, die in dem zugangsbeschränkten Digicerts.de-Netzwerk betrieben wird, werden Smart Contracts dazu genutzt, die Identitäten von Zertifizierungsstellen und Zertifizierern zu registrieren und die Fingerabdrücke der Zertifikate zu verwalten. Das InterPlanetary File System (IPFS) wird genutzt, um Profilinformationen von Zertifizierungsstellen zu sichern. Ein Dokumentenmanagementsystem für ausstellende Institutionen verwaltet die tatsächliche Nutzlast von Zertifikaten und den am Prozess beteiligten Parteien, d. h. Akkreditierungs- und Zertifizierungsstellen, Zertifizierer, Lernende und Personalabteilungen. Verschiedene Schnittstellen ermöglichen die Integration mit vorhandenen Infrastrukturen wie dem Lernmanagementsystem Moodle.

Die Plattform »Blockchain for Education« wurde iterativ in enger Zusammenarbeit mit Zertifizierungsstellen und Universitäten entwickelt. Ein erster Plattform-Prototyp wurde bereits auf der CEBIT 2018 erfolgreich demonstriert. Aktuell wird das System von der Fraunhofer Personalzertifizierungsstelle, der TH Lübeck und anderen Institutionen genutzt und erprobt. Dazu dienen Netzwerke wie das von uns mitgegründete DigiCerts (digicerts.de) und das Netzwerk Digitale Nachweise. Beides sind Netzwerke von Universitäten und Bildungseinrichtungen, die sich zum Ziel gesetzt haben, gemeinsam Standards und Lösungen in Zertifizierungsprozessen zu entwickeln. Beide Netzwerke sind offen, und wir freuen uns, sie mit anderen Mitgliedern zu erweitern.

Ergänzend zum Open Badge Standard hat das World-Wide-Web Consortium (W3C) zwei sehr wichtige Standards entwickelt, die wesentlich für die zukünftige Verwaltung von Zertifikaten sein werden. Der Standard für Decentralized Identifiers (W3C-DID)[2] ermöglicht die Registrierung und Verwaltung von digitalen Identitäten für Zertifizierungsstellen und Zertifikatsträger. Dieser Standard wird durch den Standard für Verifiable Credentials (W3C-VC)[3] ergänzt, der die Ausstellung digitaler Zertifikate beschreibt und standardisiert. Die »Blockchain for Education«-Lösung wird ebenfalls diese beiden Standards anwenden. Dies geschieht in den vom BMBF im Rahmen des INVITE-Programms (s. Einblick auf S. 43) geförderten Projekten KUPPEL und Triple-Adapt. Weitere wichtige Aktivitäten laufen auf EU-Ebene im Rahmen der EBSI-Aktivitäten (→ https://ebsi4be.eu/).

oder einen auf der Papierversion des Zertifikats gedruckten QR-Code mit einem Smartphone einscannen. Der Verifikationsdienst überprüft die angegebenen Daten in der Blockchain, führt den Ursprungsnachweis durch und präsentiert das Prüfergebnis. Neben der Überprüfung einzelner Zertifikate können Personalabteilungen auch Übersichten der Zertifikate von Mitarbeitenden erhalten. Dies vereinfacht und beschleunigt z. B. im Finanzsektor die Verfahren gegenüber den Regulierungsbehörden.

»Ausbildungsorganisationen und Zertifizierern bietet sich daher die Möglichkeit, ihre Prozesse weiter zu digitalisieren und mit der Ausgabe von digitalen Zertifikaten ihre Dienstleistung zu professionalisieren.«

Fazit

Dieser Beitrag zeigt, dass sowohl die technischen Grundlagen und erste Lösungen für eine nachvollziehbare und fälschungssichere Verwaltung digitaler Zertifikate als auch die notwendigen Standards für einen Austausch zwischen verschiedenen Lösungen verfügbar sind. Ausbildungsorganisationen und Zertifizierern bietet sich daher die Möglichkeit, ihre Prozesse weiter zu digitalisieren und mit der Ausgabe von digitalen Zertifikaten ihre Dienstleistung zu professionalisieren.

Auch in der Erwachsenen- und Weiterbildung werden digitale Zertifikate – und damit ihre Fälschungssicherheit und Nachprüfbarkeit – über kurz oder lang eine wachsende Bedeutung haben. Schon jetzt gibt es erste Anbieter in der betrieblichen Weiterbildung, die Zertifikate digital als Open Badges ausstellen. Und in der Erwachsenenbildung gibt es in Kooperation mit dem Landesverband der Volkshochschulen in NRW ein erstes Pilotprojekt zur Implementierung von digitalen Zertifikaten an der VHS Mönchengladbach über die »Blockchain for Education«-Plattform.

Dursun, M. & Saathoff, C. (2021). *Gefälschte Impfpässe werden zum Problem.* www.tagesschau.de/investigativ/report-mainz/gefaelschte-impfpaesse-101.html

Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C. & Wendland, F. (2018). Blockchain for Education: Lifelong Learning Passport. In *European Society for Socially Embedded Technologies (EUSSET)*, ERCIM Blockchain Workshop 2018. Amsterdam. https://dl.eusset.eu/handle/20.500.12015/3163

Kolbeck, C. (2016). *Doktortitel als Schnäppchen für 35 Euro.* www.medical-tribune.de/meinung-und-dialog/artikel/doktortitel-als-schnaeppchen-fuer-35-euro/

Prinz, W., Rose, T., Osterland, T. & Putschli, C. (2018). Blockchain. In R. Neugebauer (Hrsg.), Digitalisierung: Schlüsseltechnologien für Wirtschaft und Gesellschaft (S. 311–319). Berlin, Heidelberg: Springer.

PROF. WOLFGANG PRINZ, PHD,

ist stellv. Institutsleiter des Fraunhofer Institute for Applied Information Technology FIT und Professor für Kooperationssysteme an der RWTH Aachen.

wolfgang.prinz@fit.fraunhofer.de