WHITEPAPER

Digitalisierung von Zeugnissen

mit Unterstützung von Blockchain-Technologie

Stand: März 2020

Version: 1.0

Inhalt

Inhalt

Genderhinweis

Allein aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten für alle Geschlechter.

Bildnachweis

Titelbild: Avel Chuklanov, Lizenzfrei über Unsplash
Grafiken: Bundesdruckerei GmbH

1. Management Summary

Das Koordinierungsprojekt „Blockchain“[1] des IT-Planungsrates[2], die Themenfeldverantwortlichen „Bildung“ des Online-Zugangs-Gesetzes (OZG), weitere Akteure im Bildungssystem der Bundesrepublik Deutschland sowie der internationalen Bildungsarbeit haben es sich zum Ziel gesetzt, das Zeugniswesen zu digitalisieren und dabei fälschungssicher und arbeitseffizient zu gestalten.

Das vorliegende Whitepaper fasst die Ergebnisse der bisherigen Analyse- und Diskussionsphase zusammen. Es soll in einem erweiterten Kreis von Schulen, Hochschulen, Ministerien und Unternehmen das Konzept validieren, die Konsensbildung für eine deutschlandweite Lösung voranbringen sowie angesichts globaler Mobilität und grenzüberscheitender Bildungsbiografien einen Beitrag zum internationalen Dialog über Interoperabilität und Harmonisierung im Bildungswesen leisten. Dabei sollen auch lebenslange, individuelle Bildungswege über alle Wege unterstützt werden (auch Berufsausbildung).

Heute werden Zeugnisse für Schul- und Studienabschlüsse in Schriftform ausgegeben, während Bewerbungsprozesse vorwiegend schon online durchgeführt werden.

Das vorliegende Whitepaper beschreibt, wie Zeugnisse zusätzlich zur Schriftform digital erstellt, ausgegeben und fälschungssicher repräsentiert werden können, sodass ihr Ursprung und ihre Integrität über einen lebenslangen Zeitraum geprüft werden können. Zudem sind diese Zeugnisse maschinenlesbar, sodass die Daten in nachgelagerte Fachverfahren automatisiert übernommen werden können.

Das Konzept ist so entworfen, dass Bildungseinrichtungen kaum zusätzlichen Aufwand bei der Erstellung der zusätzlichen digitalen Zeugnisse haben und dass ein empfangenes Zeugnis einfach auf Echtheit überprüft werden kann. Zielsetzung ist nicht die Vorgabe einer einzigen Lösung, sondern die Interoperabilität entstehender Lösungen.

Das Konzept ist DSGVO-konform, weil keine personenbezogenen Daten verarbeitet und die Zeugnisse selbst nicht zentral gespeichert werden.

Das Konzept sieht die Nutzung einer oder mehrerer Distributed-Ledger-Infrastruktur(en) (Blockchain) zur Registrierung und Sicherung der Prüfsummen der Zeugnisse vor und garantiert so die Fälschungssicherheit. Hierbei setzt das Konzept auf Open-Source-Technologie zur Steigerung der IT-Sicherheit und des Vertrauens in das System. Aufbau und Betrieb dieser Infrastruktur(en) sind im Konzept noch nicht abschließend festlegt. Grundsätzlich sollte jedoch

[1] https://dezentraleverwaltung.de

[2] https://it-planungsrat.de

eine Permissioned Blockchain mit definierten Governance-Strukturen verwendet werden, um sich von Blockchains wie Bitcoin abzugrenzen.

Es liegen bereits mehrere prototypische Umsetzungen zur Erprobung des Konzeptes vor. Vorführungen können bei den Entwicklern (siehe Ansprechpartner unter 7.1) angefragt werden.

2. Ausgangssituation und Lösungsbeschreibung

Bewerbungsprozesse, sowohl für Studien- als auch für Arbeitsplätze laufen heute in vielen Ländern in der Regel digital ab. Der Bewerber trägt seine persönlichen Daten in ein digitales Bewerbungsformular ein und überträgt diese an die Hochschule oder das Unternehmen. Schwierig wird es beim Nachweis der Qualifikation in Form von Bildungsabschlüssen. Diese werden den Bewerbern nur in ausgedruckter, gesiegelter und unterschriebener Form (Schriftform) übergeben. Der aktuelle Weg, das Papierdokument einzuscannen und im Nachgang die Echtheit durch Vorlage einer beglaubigten Kopie zu bestätigen, verursacht einen hohen Aufwand bei allen am Prozess Beteiligten und bietet Betrugsmöglichkeiten durch Manipulation oder komplette Fälschung von Dokumenten.

Das vorliegende Whitepaper beschreibt für den deutschen Raum einen nutzerzentrierten Lösungsvorschlag, der zusammen mit Anwendern entwickelt und auf deren Bedürfnisse, insbesondere in Bezug auf die einfache Anwendbarkeit, abgestimmt wurde. Der Lösungsvorschlag berücksichtigt weiterhin die föderale Organisation des deutschen Bildungssystems, die Anforderungen des Datenschutzes und der Datensicherheit sowie die Kompatibilität mit bestehenden Lösungen, auch über die Grenzen Deutschlands hinweg. Angesichts zunehmend international verlaufender Bildungsbiografien unterstreicht es die Bedeutung offener Standards und zielt auf größtmögliche Interoperabilität im sich global entwickelnden Ökosystem rund um digitale Bildungszertifikate ab. Das Konzept ist herstellerneutral, offen für Partizipation weiterer Institutionen und so gestaltet, dass es verschiedene Zeugnistypen wie Abitur, Ausbildungsnachweis, Bachelor, Master, aber auch Einzelergebnisse aus Kursen wie Erasmus-Auslandsaufenthalte unterstützt. Es ist außerdem übertragbar auf Anwendungen im Bereich berufliche und interne Weiterbildung.

Technologische Voraussetzung für die Umsetzung des Konzeptes ist ein dezentral betriebenes Absicherungssystem, z. B. eine Blockchain. Dieses könnte von einem vertrauenswürdigen Konsortium aus öffentlichen Rechenzentren betrieben werden.

Das vorliegende Konzept beschreibt eine Ergänzung zum aktuellen Prozess in Deutschland und gibt Impulse für die internationale Kooperation. Zeugnisse in Schriftform werden weiterhin wie gewohnt erstellt und ausgegeben. Zusätzlich wird eine digitale Datei erzeugt, welche sowohl menschen- als auch maschinenlesbar ist. Das System erzeugt automatisch über eine mathematische Einwegfunktion eine Prüfsumme der Datei, einen sogenannten Hashwert[3], der zusammen mit der Identitätskennung der ausstellenden Institution manipulationssicher in eine Blockchain geschrieben wird. Aus dem Hashwert ist technisch keinerlei Rückschluss auf den

[3] Zur Frage, ob Hash-Werte z.B. von Zeugnissen Rückschlüsse auf Personendaten ermöglichen, gibt es noch keine abschließende Meinung bzw. Rechtsprechung.
Eine spanische Einschätzung ist hier https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf zu finden. Technisch könnte diese Problematik z.B. durch Einführung eines SALT-Wertes lösbar sein.

Inhalt der Zeugnisdatei möglich. Die digitale Zeugnisdatei wird von der ausstellenden Institution auf einem sicheren Weg an den Schüler weitergeleitet, der für die Aufbewahrung und Verwaltung seines digitalen Zeugnisses verantwortlich ist, wie dies auch in der Version der Schriftform der Fall ist. Der Besitzer des Bildungsabschlusses behält die Hoheit über seine Daten und entscheidet souverän, wem er seinen Bildungsabschluss vorlegt.

Im Bewerbungsprozess reicht der Bewerber nun statt eines Scans des Papierzeugnisses die digitale Zeugnisdatei ein. Der Empfänger hat die Möglichkeit, mit einfachen technischen Mitteln die Echtheit dieser zu überprüfen. Dies kann auf unterschiedliche Weise erfolgen:

- über eine sichere Webseite mit Online-Prüfservice,
- über ein Client-Programm, welches auf dem Rechner des Empfängers läuft,
- über eine Schnittstelle (API), die z. B. in HR-Systeme integriert ist und die eine automatische Prüfung im Hintergrund durchführt,
- über mobile Apps, die einerseits die Verwaltung der Zeugnisse durch den Benutzer ermöglichen und zusätzlich eine Prüfung durchführen.

Zur Validierung wird die Prüfsumme der Zeugnisdatei im lokalen Gerät des Empfängers berechnet. Ist diese Prüfsumme in der Blockchain auffindbar, sind Echtheit und Unverfälschtheit der Datei zweifelsfrei nachgewiesen. Als zusätzliche Information liefert das System den Schreibzeitpunkt und die Institution, die das Zeugnis ausgestellt hat, sowie die Auflösung der sogenannten Vertrauenskette. Über die Vertrauenskette kann der Anwender nachvollziehen, welche Institution das Zeugnis ausgestellt hat und welche übergeordnete Institution die Berechtigung zur Ausstellung von Zeugnissen erteilt hat.

Ein weiterer Vorteil ergibt sich für Empfänger von digitalen Zeugnissen durch deutlich verschlankte Prozesse. Dank einer automatischen Echtheitsprüfung der digitalen Zeugnisversion erübrigen sich alle bisherigen Prozesse auf Grundlage der Originalzeugnisse (Papier) und deren Beglaubigungen (Papier). Diese Papierversionen müssen zu keinem Zeitpunkt mehr eingesandt, vorgelegt, geprüft, archiviert oder rückversendet werden. Alle damit verbundenen Kosten entfallen für die Zeugnisinhaber, die zentralen Vergabestellen für Studienplätze sowie später für alle Hochschulen und Unternehmen.

Für Empfänger digitaler Zeugnisse ist die elektronische Weiterverarbeitung der enthaltenen Daten von Bedeutung. Das vorliegende Konzept sieht vor, einen maschinenlesbaren Teil in die digitale Zeugnisdatei einzubetten (bevor der Hash erzeugt wird), so dass die Daten automatisiert ausgelesen und in IT-Systeme übertragen werden können. Hierbei legt das Konzept großen Wert auf Datenschutz, Datensicherheit und die Kompatibilität zu bereits bestehenden Standards wie OpenBadge[4] oder dem europäischen Zeugnisaustauschformat ELMO, welches auf dem europäischen Standard CEN EN 15981 2011 EuroLMAI[5] basiert. ELMO wird beispielsweise für

[4] https://openbadges.org/
[5] European Learner Mobility - Achievement information (EuroLMAI)

den digitalen Transfer von Studierendendaten im EMREX-Projekt[6] verwendet und weiterentwickelt.

Bildung wirkt global Vorurteilen, sozialer Ungerechtigkeit, Arbeitslosigkeit und Hunger entgegen. Dementsprechend haben Bildungsabschlüsse, sowohl von Sekundarschulen als auch von Hochschulen, für Bürger eine große Bedeutung. Sie beweisen den Abschluss einer mehrjährigen, teilweise akademischen Ausbildung und dienen im beruflichen Kontext als wichtiges Entscheidungskriterium für die Einstellung von Mitarbeitern. Trotz ihrer großen Bedeutung für die Entwicklung der Karriere ihres Trägers sind Bildungsabschlüsse im Jahr 2019 immer noch nicht oder nur schwach gegen Fälschung oder Manipulation gesichert. Zeugnisse werden in Deutschland und vielen anderen Ländern aktuell ausschließlich in Papierform ausgestellt.

Den größten Mehrwert für alle Beteiligten bildet die Digitalisierung von Bildungsabschlüssen, wenn das entstehende Ökosystem möglichst inklusiv, nachhaltig und innovationsoffen angelegt ist. Im Idealfall können darin alle bestehenden sowie zukünftig hinzukommende Bildungseinrichtungen miteinander interagieren und Zertifikate austauschen. Lernende, öffentliche Administrationen, Arbeitgeber und HR-Dienste haben Zugang zu sicheren, vertrauenswürdigen, nachhaltig betriebenen und nutzerzentriert gestalteten Validierungsdiensten. Offene, interoperable Standards sorgen dafür, dass es auf Systemanbieterseite zu Wettbewerb um die besten Dienste kommt.

Im konkreten Fall zielt das Konzept auf die Einrichtung eines Systems ab, das breite Zustimmung findet, indem es Anforderungen hiesiger Aussteller und Anwender adressiert. Auf Seiten der Schulen sollen beispielsweise keine zusätzlichen Aufwände verursacht werden. In diesem Sinne legt das Konzept großen Wert auf Kompatibilität zu bestehenden Lösungen wie beispielsweise der in Hessen und Berlin im Einsatz befindlichen LUSD[7] und der in NRW genutzten Software Schild-NRW[8].

Aus internationaler Perspektive zeichnen sich Forschungsfragen ab, die über das vorliegende Konzept hinausgehen. Sie betreffen Technologie und Bildungs-Governance. Offen ist etwa, wie sich die angestrebte Konnektivität zur global wachsenden Anzahl von Zertifikatssystemen etablieren und nachhaltig vertrauenswürdig unterhalten lässt. Ein Zertifikat soll auch in 50 Jahren validiert werden können, wenn die ausstellende Bildungsinstitution vielleicht aufgrund von Krisen, Kriegen oder Klimakatastrophen nicht mehr existiert oder die Infrastruktur nicht mehr wie ursprünglich betreibt. Damit sich Lernende weltweit langfristig auf die Überprüfbarkeit ihrer digitalen Nachweise verlassen können, muss gewährleistet sein, dass Validierungsdienste verfügbar und die entsprechenden Speicherorte – hier: Blockchains – technisch allein vom Zertifikat aus auffindbar und erreichbar sind. Die mit derartigen Szenarien

[6] https://emrex.eu/
[7] https://www.egovschool-berlin.de/node/975
[8] https://www.svws.nrw.de/download/schild-nrw

verbundenen Fragen verweisen auf den emergenten Charakter der verwendeten Technologien ebenso wie auf das große Potenzial digitaler Bildungszertifikate für die digital-vernetzte, globale Gesellschaft.

3. Stakeholder und Anforderungen

3.1. Stakeholder

Stakeholder, also Beteiligte im System, sind im Wesentlichen:

Ausstellende Institutionen wie Schulen, Hochschulen, Universitäten. Bei entsprechender Verbreitung des Systems auch weitere Institutionen, die Bildungsabschlüsse bescheinigen, z. B. die Industrie- und Handwerkskammern, Volkshochschulen, Online-Bildungseinrichtungen, Institutionen für berufliche Weiterbildung oder Unternehmen, die Arbeitszeugnisse ausstellen.

Zertifikatsträger wie Schüler, Studenten oder andere Personen, denen eine Bildungsqualifikation bezeugt wird. Ein Zertifikat im Sinne des Konzepts kann ein Schul- oder Hochschulzeugnis oder eine andere Bescheinigung sein.

Anwendende Institutionen sind Einrichtungen, bei denen ein Zertifikatsträger sein Zeugnis vorlegt, wie Hochschulen, Universitäten, zentrale Bewerbungseinrichtungen oder Unternehmen.

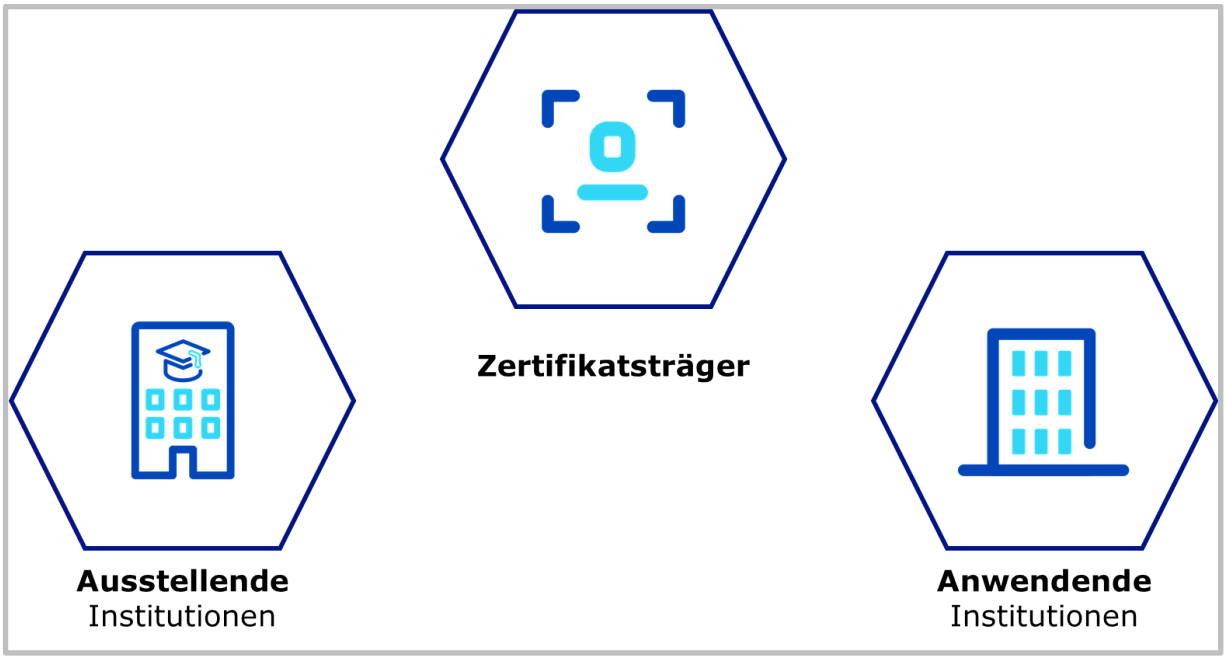

Abbildung 1: Stakeholder im System

3.1.1. Ausstellende Institutionen

Aufgabe im System	Erstellt Zeugnisse und verteilt sie an Zertifikatsträger wie Schüler oder Studierende
Hauptbedürfnis	Einfache Erstellung von Zeugnissen Kompatibilität zu ggf. vorhandenen Legacy-Systemen Anbindung an vorhandenes Managementsystem der Einrichtung
Interaktionen	Benutzt Service, welcher Zeugnisse erstellt und absichert

3.1.2. Zertifikatsträger

Aufgabe im System	Empfängt Zeugnis vom Aussteller, verwahrt es in seinem Hoheitsbereich und gibt es im Rahmen von Bewerbungsprozessen weiter an anwendende Institutionen
Hauptbedürfnis	Möchte vertrauenswürdiges Zeugnis (gleichwertig dem Original oder einer beglaubigten Kopie) ohne Behördengänge mehrfach elektronisch weitergeben
Interaktionen	Empfängt Zeugnisse, verwaltet diese eigenständig und gibt sie selbstbestimmt elektronisch weiter

3.1.3. Anwendende Institutionen

Aufgabe im System	Empfängt elektronische Zeugnisse von Zertifikatsträgern und prüft diese
Hauptbedürfnis	Digitaler Empfang und effiziente (maschinelle) Prüfung und Weiterverarbeitung
Interaktionen	Benutzt einen Service, der Zeugnisse prüft, die Daten digital ausliest und weiterverarbeitet

3.2. Anforderungen

Im Rahmen der Erstellung des vorliegenden Konzeptes wurden in Gesprächen mit Anwendern und Experten im Bildungswesen Anforderungen an ein System für den digitalen Austausch von Bildungsnachweisen erhoben. Die folgende Liste stellt einen Auszug dieser Anforderungen dar, ohne Anspruch auf Vollständigkeit zu erheben.

- Ein Zeugnis kann vielfältig sein (Abitur, Diplom, Approbation, Leistungsnachweis über Kurs im Studium, Schweißer-Pass, Weiterbildungsnachweis); in Bundesländern ohne zentrale Abiturzeugniserstellung unterscheiden sich die Zeugnisse von Schule zu Schule
- Ein Bewerber muss direkten Zugriff auf das beglaubigte Zeugnis haben, um dieses während eines Bewerbungsprozesses zu verwenden
- Das System muss Student Mobility unterstützen und Hochschulen einen digitalen Austausch von Leistungspunkten auf Modulebene ermöglichen
- Digitale Zeugnisse liegen nur bei dem Zertifikatsträger selbst und bei denen, denen er das Zeugnis gesendet hat vor[9]
- Es muss sichergestellt sein, dass ein Zeugnis ausschließlich durch den Besitzer autorisiert verwendet werden kann; es darf nicht von anderen Bewerbern genutzt werden
- Das System soll über das Internet verfügbar sein und ohne Papier funktionieren; eine Installation von Spezialsoftware ist nicht nötig
- Papierdokumente können wie bisher parallel ausgestellt und verwendet werden; sie sind für den Prozess nicht notwendig
- Die Daten des Zeugnisses (Schule/Hochschule, Inhaber, Noten) sind elektronisch auslesbar
- Ein Zeugnis ist maschinell prüfbar (Ausstellende Institution, Ausstelldatum, Integrität)
- Institutionen, die in das System schreiben (Zeugnisse durch Eintrag der Prüfsumme absichern) müssen entweder im System registriert sein und/oder über eine digitale Identität verfügen
- Lesender Zugriff (prüfen einer Prüfsumme) ist öffentlich und für jeden möglich
- Das System ist kompatibel zu bestehenden Lösungen und Standards und lässt sich über Schnittstellen integrieren

[9] Im Rahmen gesetzlicher Archivierungsvorgaben, evtl. auch bei der für die Archivierung verantwortlichen Institution. Möglichkeiten elektronischer Archivierung werden im vorliegenden Konzept nicht betrachtet.

3.3. Funktionalität des Systems

3.3.1. Funktionalität für Ausstellende Institutionen

Der Fokus des Systems liegt auf Absicherung von Bildungsabschlüssen und der Aufbereitung dieser für die maschinelle Weiterverarbeitung in nachgelagerten Prozessen. Sofern nicht bereits durch vorhandene Systeme abgedeckt, kann das System von autorisierten Institutionen zur Ausstellung von Bildungsabschlüssen genutzt werden.

Die Ausstellende Institution importiert über eine Webschnittstelle (API) oder ein geeignetes Austauschformat (z.B. json, xml, openbadge) die Zeugnisdaten aus einem Schul- oder Campusverwaltungssystem (im Schulbereich z.B. LUSD, Schild-NRW oder ähnliches) oder überträgt diese manuell. Bei Bedarf kann auch eine menschenlesbare Datei wie z. B. PDF erzeugt werden die die Datendatei enthält oder andersherum. Über einen Genehmigungsworkflow wird diese Datei von den verantwortlichen Stellen (z. B. Prüfungskommission, Schulleitung) freigegeben. Anschließend wird die Prüfsumme der Zeugnisdatei errechnet und zusammen mit der eindeutigen Identität der ausstellenden Institution dauerhaft und unveränderbar in eine Blockchain geschrieben. Die menschenlesbare Datei kann wie gewohnt ausgedruckt und dem Zertifikatsträger übergeben werden. Zusätzlich übergibt die ausstellende Institution dem Zertifikatsträger auf sicherem Weg die digitale Datei. Die Verarbeitung der Zeugnisdaten findet auf dem Client der ausstellenden Institution statt. Inhalte der Zeugnisdatei werden zu keinem Zeitpunkt übertragen (Security by Design).

3.3.2. Funktionalität Zertifikatsträger

Der Zertifikatsträger (z. B. Schüler, Student) erhält von der Bildungseinrichtung wie gewohnt ein Zeugnis in Papierform. Zusätzlich erhält er eine digitale Datei zur eigenen Verwahrung. Diese Datei kann er mithilfe von frei verfügbarer Standardsoftware öffnen, beliebig oft digital kopieren und nach eigenem Ermessen speichern und weitergeben. Eine Änderung des Dateinamens stellt keine Veränderung der Datei im Sinne des Sicherheitskonzepts dar. Der Zertifikatsträger kann die Echtheit seines Zeugnisses jederzeit über einen frei verfügbaren Webservice prüfen. Im Rahmen von Bewerbungsprozessen gibt der Zertifikatsträger die digitale Datei nach eigenem Ermessen an Dritte (z. B. Hochschulen, Unternehmen) zum Beleg eines erreichten Bildungsabschlusses weiter.

3.3.3. Funktionalität für anwendende Institutionen

Anwendende Institutionen (z. B. Hochschulen, zentrale Vergabestellen wie die Stiftung für Hochschulzulassung oder Unternehmen) erhalten im Rahmen von Bewerbungsprozessen schon heute Zeugnisse im PDF-Format von ihren Bewerbern. Bei den heute übertragenen Dateien handelt es sich in der Regel um Scans (Bilder) der Papierzeugnisse. Diese sind manipulationsanfällig und nicht für eine maschinelle Weiterverarbeitung geeignet. Die nach dem vorliegenden Konzept erstellten Dateien stellen für die anwenden Institutionen einen Mehrwert dar, da sie von konstant hoher Qualität sind, mit einfachen technischen Mitteln auf Echtheit und Integrität geprüft und maschinell weiterverarbeitet werden können. Anwendende

Institutionen, die eine digitale Zeugnisdatei erhalten, können diese ohne Installation zusätzlicher Software über einen Webservice prüfen. Der Webservice errechnet hierbei im Browser des Anwenders des zur Datei gehörigen Hashwert, ohne die Datei über das Internet zu übertragen. Eine Abfrage des Hashwerts in der Blockchain gibt direkt Auskunft über die ausstellende Institution sowie die Unverfälschtheit des Dokuments. Mithilfe zusätzlicher Software können von autorisierten Institutionen die maschinenlesbaren Daten des Zeugnisses ausgelesen und in die eigenen Systeme (z. B. Campus-Management-Systeme) übertragen werden.

4. Architekturkonzept

4.1. Dezentrales Architekturkonzept

Das vorgeschlagene Konzept setzt auf Dezentralität und Open Source. Es gibt keine einzelne Stelle, die das System oder die Blockchain beherrscht.

Die Architektur besteht aus drei wesentlichen Teilen:

Blockchain als Datenbank

Die Datenbank (Blockchain) speichert keine personenbezogenen Daten, sondern nur öffentliche Schlüssel, Hashes[10] und Referenzen zu öffentlichen Institutionen wie Schulen und Hochschulen. Sie ist durch den Betrieb mehrere Knoten ausfallsicher und wird gründlich gegen Angriffe gehärtet[11]. Nach Vorstellung der Autoren dieses Whitepapers wird die Infrastruktur von einem Konsortium aus kommunalen und öffentlichen Rechenzentren betrieben. Dies erleichtert die Absicherung und erhöht damit das Vertrauen in das System. Die Blockchain ist privat und zugriffsgeschützt. Eine Prüfung von Zeugnisdateien durch Zertifikatsträger oder Anwender erfolgt über den angebotenen Webservice oder Schnittstellen, die mit einem oder mehreren Blockchain-Knoten interagieren. Das System profitiert von den bekannten Vorteilen einer Blockchain (Fälschungssicherheit, Unveränderbarkeit, etc.) und vermeidet gleichzeitig Nachteile komplett öffentlicher Blockchain-Infrastrukturen (z. B. erhöhter Stromverbrauch durch Methoden zur Vertrauensbildung). Die vorgesehene Infrastruktur bietet kein Kryptogeld[12], das spekulativ verwendet werden kann. Die Kosten für den Betrieb der Blockchain sind vergleichbar mit denen anderer verteilter IT-Systeme.

Web-Client zum Erzeugen von Zeugnissen

Die Erzeugung der Zeugnisse erfolgt über einen Webservice, der entweder im Browser der ausstellenden Institution laufen oder über eine Schnittstelle in ein bestehendes System integriert werden kann. Bei Bedarf ist die Integration des Webservice in eine Clientsoftware denkbar. Der Webservice ist grundsätzlich nur autorisierten Institutionen zugänglich deren Identität sowie Berechtigung zur Ausstellung von Zeugnissen durch übergeordnete Instanzen bestätigt wurde. Erstellte digitale Zeugnisse werden dem Zertifikatsträger auf einem sicheren Weg übergeben. Das aktuelle Konzept sieht keine Speicherung der digitalen Zeugnisdatei (weder zentral noch bei der ausstellenden Institution) vor. Sollten zukünftig vom Gesetzgeber Anforderungen an eine digitale Archivierung von Zeugnissen gestellt werden, können diese mit dem vorliegenden Konzept leicht umgesetzt werden.

Webservice zum Prüfen von Zeugnissen

Zur Prüfung der Echtheit und Integrität von Zeugnisdateien, wird ein öffentlich zugänglicher Webservice zur Verfügung gestellt. Dieser Webservice ist für jedermann benutzbar, der eine

[10] https://de.wikipedia.org/wiki/Kryptologische_Hashfunktion
[11] Unter anderem durch Umsetzung der Empfehlung des BSI Blockchain sicher gestalten
[12] https://de.wikipedia.org/wiki/Kryptow%C3%A4hrung

Zeugnisdatei besitzt, also von dem Zertifikatsträger selbst sowie allen dritten Personen und Institutionen, denen der Zertifikatsträger seine digitale Zeugnisdatei vorlegt. Durch Vorzeigen der Datei wird im Browser der Hashwert berechnet und auf Vorhandensein in der Blockchain geprüft. Das Zeugnis selbst verlässt den Browser hierbei nicht. Während eine negativ ausfallende Prüfung verschiedene Ursachen haben kann (Hash nicht in Blockchain geschrieben, Datei manipuliert, etc.), bestätigt eine positive Prüfung zweifelsfrei die Echtheit, die Integrität sowie die ausstellende Institution.

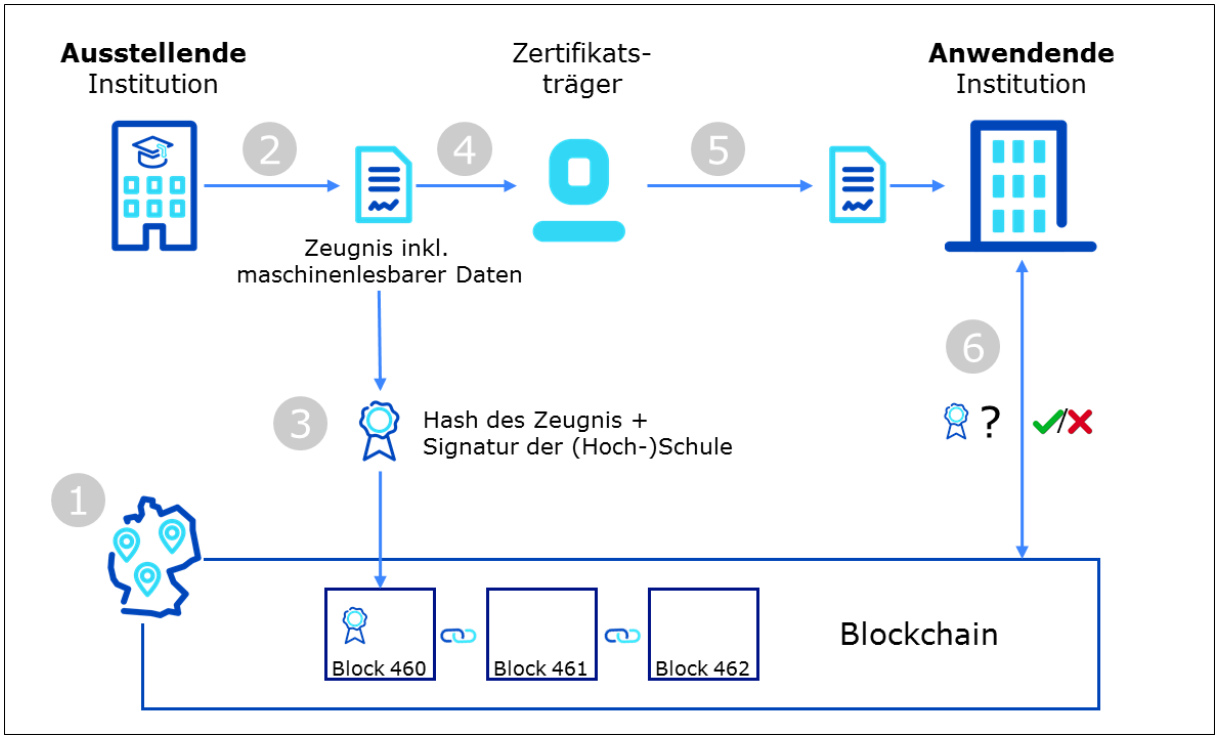

Abbildung 2: Systemarchitektur

Prozessablauf

1. Vertrauenswürdiges Konsortium auf Basis und in der Trägerschaft kommunaler und öffentlicher Rechenzentren betreibt eine verteilte Infrastruktur bestehend aus einer Blockchain und darüber liegenden Webservices
2. Berechtigte, autorisierte Schulen erzeugen digitale Zeugnisse. Diese enthalten das Druckbild des Zeugnisses und maschinenlesbare Zeugnisdaten
3. Berechtigte Schulen schreiben einen dem Zeugnis zugehörigen Hashwert gemeinsam mit der Identität der Schule in die Blockchain
4. Digitale Zeugnisse werden auf sicherem Weg an Zertifikatsträger verteilt[13]
5. Schüler nutzt digitales Zeugnis zur Bewerbung in einem Webportal oder per Mail

[13] Weg noch zu spezifizieren. Denkbar sind verschiede Lösungen, z.B. ein gesichertes Downloadportal

6. Anwendende Institutionen können Unverfälschtheit des Zeugnisses durch Aufruf eines Webservice zum Prüfen der Zeugnisse sicherstellen. Dieser Service berechnet den Hash der Zeugnisdatei und vergleicht ihn mit den Daten in der Blockchain. Die Identität der ausstellenden Institution wird angezeigt.

4.2. Autorisierung von ausstellenden Institutionen

Ein zentraler Punkt zur Herstellung von Vertrauen in das System ist die Autorisierung der ausstellenden Institutionen. Es ist sicherzustellen, dass nur berechtigte Institutionen in die Blockchain schreiben können. Neben technischen Sicherungen ist die sogenannte Vertrauenskette von Bedeutung. Diese gibt an, von welcher übergeordneten Instanz eine ausstellende Institution zum Schreiben in die Blockchain berechtigt wurde.[14]

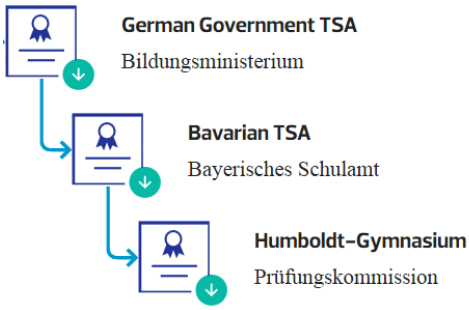

Abbildung 3: Beispielhafte Darstellung einer Vertrauenskette

4.3. Kompatibilität zu Standards und bestehenden Systemen

Zur Sicherstellung größtmöglicher Akzeptanz und Verbreitung des Systems, wird bei Konzeption und Entwicklung große Sorgfalt auf die Kompatibilität und zu bereits bestehenden Systemen sowie zu nationalen und internationalen Standards gelegt. Unter anderem werden die folgenden Standards und Initiativen berücksichtigt.

- EU eIDAS-Verordnung
- W3C Decentralized Identifiers (DIDs)
- W3C Verifiable Credentials Data Model 1.0
- OpenBadges
- Blockcerts
- PESC
- ELMO und EMREX[15];
- Erasmus without Paper
- Lehrkräfte-Unterrichts-Schul-Datenbank (LUSD)

[14] Eine detaillierte Konzeption des Autorisierungsverfahrens wird mit Update des Whitepapers veröffentlicht.
[15] Vergleich PESC und ELMO

- Schulverwaltungsprogramm des Landes NRW (SCHILD-NRW)

Initiativen

- European Blockchain Partnership
- Groningen Declaration
- StudIES+
- Digital Credentials Initiative

5. Umsetzung

Gegenwärtig existieren verschiedene Prototypen, die die technische Machbarkeit des Systems belegen. Zusätzlich wurden im Rahmen nutzerzentrierter Entwicklung sogenannte Klick-Dummys entwickelt und fortlaufend mit Anwendern getestet, um einen hohen Grad an Nutzbarkeit, positiver User Experience (UX) und Akzeptanz für das System zu erreichen.

Die vorhandenen Prototypen und UX Konzepte können über die Ansprechpartner der Bundesdruckerei, Fraunhofer FIT, regio IT, Trustcerts sowie Deutsche Gesellschaft für Internationale Zusammenarbeit angefragt werden.

Die Autoren dieses Whitepapers regen die zeitnahe Umsetzung eines Pilotprojektes an, in enger Abstimmung mit den politisch verantwortlichen Stellen und in Zusammenarbeit mit Schulen, einer zentralen Vergabestelle für Studienplätze sowie Hochschulen.

5.1. Universelle Prüfseite

Ein Zertifikatsträger erhält Zertifikate, die durch unterschiedliche Verifikationssysteme ausgestellt wurden. Damit sich die Überprüfung von verschiedenen Zertifikaten möglichst einfach gestaltet, wird eine universelle Prüfseite erstellt, die Überprüfungen von Zeugnissen verschiedener Systeme bereitstellt. Auf solch einer Prüfseite wird ein Zertifikat geladen, die Prüfseite analysiert das Zertifikat und kann dann entsprechende Methode des jeweiligen Systems zur Überprüfung und Darstellung anwenden. Dabei werden jeweils spezifische Prüfalgorithmen der jeweiligen Herausgeber aufgerufen

Universelle Prüfseiten sollten von vertrauenswürdigen übergeordneten Stellen bereitgestellt werden. Dabei werden nur allgemein akzeptierte Systeme angeboten. Der Nutzer solch einer Seite muss erkennen, welche Systeme die Prüfseite anbietet.

Die Prüfseite ist öffentlich aufrufbar.

Verfahren

Die Prüfseite erkennt das Format des Zeugnisses und ermittelt die passende Prüfroutine und führt mit dieser die Prüfung durch und stellt die Ergebnisse dar.

Dazu stellen die verschiedenen Verfahren jeweils eine JavaScript-Bibliothek bereit, die einen REST-Service des jeweiligen Anbieters aufruft und dort die Prüfung durchführt.

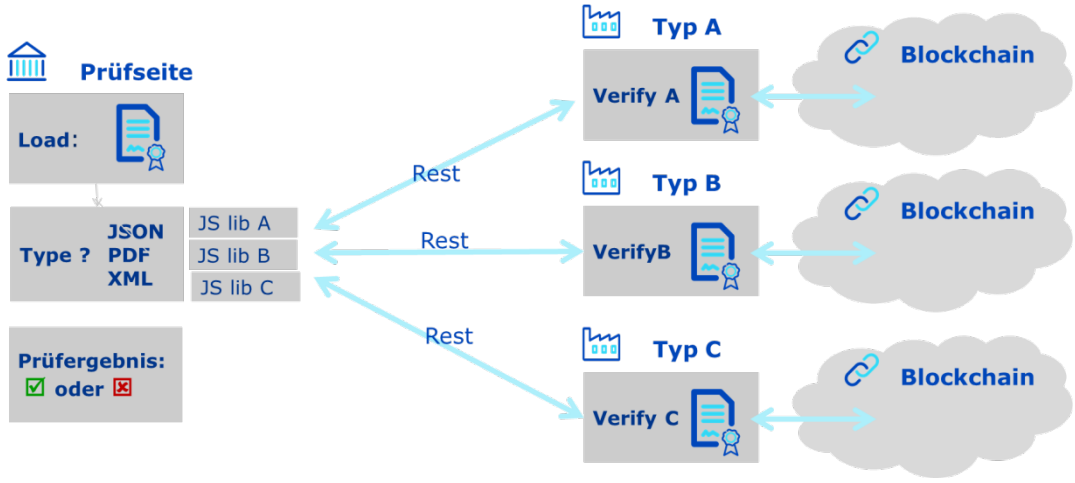

Abbildung 4: Aufbau der Prüfseite

Detaillierte Beschreibung:

- **Analyse des Formats, Berechnung und Überprüfung des Hash-Werts**
  - **Erkennen des Formats**
    - Anhand eines im Zeugnis eingetragenen Property-Attributes wird der Typ des Zeugnisses bestimmt um die passende Verification Routine aufrufen zu können.
    - Danach wird eine für den jeweiligen Typ spezifische Javascript-Bibliothek aufgerufen mit der Funktion checkCertificate().

  - **Berechnung des Hash-Werts**
    Die Java Script Bibliothek berechnet den spezifischen Hash und ruft die spezifische Verification über ein Rest API auf.

  - **Verifikation des Hash-Werts**
    der Hashwert wird in der jeweiligen Blockchain überprüft.

Darstellung des Ergebnis und des Zertifikats
Die einzelnen Systeme definieren eine Methode, die das Ergebnis der Überprüfung interpretiert, aus den Daten eine Darstellung des Zertifikats erzeugt und beides anzeigt mit Funktion displayCertificate().

6. Ausblick

6.1. Regulatorische Aufgaben

Neben den technischen Herausforderungen gilt es auch, rechtliche Rahmenbedingungen im Blick zu behalten.

- ist es rechtlich abbildbar, nur ein digitales Zeugnis auszugeben,
- Sind das Papierzeugnisse und das „elektronisches Zeugnis“ (und Kopien davon) jeweils Originale?

6.2. Technische Aufgaben

In vielen Bereichen wird derzeit das Konzept der so genannten „Verifiable credentials“ (VC) diskutiert. Die Seite des W3C W3C Verifiable Credentials Data Model 1.0 [16] bietet eine gute Informationsgrundlage zu diesem allgemein anwendbaren Konzept. In einer zukünftigen Version dieses Whitepapers werden wir uns damit befassen, wie VC im Bildungsbereich konkret eingesetzt werden könnten.

7. Beteiligte der Kooperation für Zeugnis-Digitalisierung

Koordinator der Kooperation

CIO NRW; Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie NRW
https://www.wirtschaft.nrw

Blockchain in der Verwaltung

Eine Initiative von Bund, Ländern und Unternehmen zur Entwicklung essentieller Basisinfrastruktur in Deutschland, für eine moderne und rechtssichere Verwaltung. Der BiVD möchte gemeinsam mit Partnern aus Behörden von Bund und Ländern, Partnern aus der Industrie, Startups und Institutionen und Initiativen in ganz Europa eine belastbare, rechtssichere und zukunftsorientierte Infrastruktur für digitale Verwaltungsdienste entwickeln.

http://bivd-initiative.de

Berlin Partner

Als einzigartiges Public Private Partnership stehen hinter Berlin Partner für Wirtschaft und Technologie sowohl der Senat des Landes Berlin als auch über 280 Unternehmen und Wissenschaftseinrichtungen, die sich für ihre Stadt engagieren. Zudem verantwortet Berlin Partner das weltweite Marketing für die deutsche Hauptstadt, beispielsweise mit der erfolgreichen „be Berlin“-Kampagne.

https://www.berlin-partner.de/

[16] http://www.w3.org/TR/vc-data-model/

Bundesdruckerei GmbH

Die Bundesdruckerei GmbH bietet innovative und komplette IT-Sicherheitslösungen für Unternehmen, Staaten und Behörden. Mit Technologien und Dienstleistungen „Made in Germany“ schützt sie sensible Daten, Kommunikation und Infrastrukturen. Die Lösungen basieren auf der sicheren Identifikation von Bürgern, Kunden, Mitarbeitern und Systemen in der analogen und digitalen Welt.

https://www.bundesdruckerei.de/

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Als weltweit tätiger Dienstleister der internationalen Zusammenarbeit für nachhaltige Entwicklung und internationale Bildungsarbeit entwickelt die GIZ mit ihren Partnern wirksame Lösungen, die Menschen Perspektiven bieten und deren Lebensbedingungen dauerhaft verbessern. Das GIZ Blockchain Lab ist Ideengeber für innovative Projektansätze. Es setzt derzeit einen Open-Source-Piloten zu fälschungssicheren Bildungszertifikaten um.

http://giz.de/blockchain

Deutscher Akademischer Austauschdienst

Der DAAD ist die weltweit größte Förderorganisation für den internationalen Austausch von Studierenden und Wissenschaftlern. Er wird als Verein von den deutschen Hochschulen und Studierendenschaften getragen. Seine Tätigkeit geht weit über die Vergabe von Stipendien hinaus: Der DAAD fördert die Internationalisierung der deutschen Hochschulen, stärkt die Germanistik und deutsche Sprache im Ausland, unterstützt Entwicklungsländer beim Aufbau leistungsfähiger Hochschulen und berät die Entscheider in der Bildungs-, Außenwissenschafts- und Entwicklungspolitik.

https://www.daad.de/de/

Digital Business University of Applied Sciences

Die DBU ist eine Wirtschaftshochschule für das digitale Zeitalter, die ihre Studienangebote und Forschungsleistungen konsequent auf die digitalisierte Wirtschafts- und Arbeitswelt ausrichtet. Ihr erklärtes Ziel ist es, den Studierenden umfangreiche Digitalkompetenzen zu vermitteln und sie so auf die sich verändernden beruflichen Anforderungen in einer zunehmend digitalen Arbeitswelt vorzubereiten.
https://dbuas.de

Fraunhofer FIT

Fraunhofer FIT besitzt rund 30 Jahre Erfahrung in der menschengerechten Gestaltung von intelligenten Systemlösungen, die sich nahtlos in Unternehmensprozesse integrieren. Unsere Kunden profitieren durch effizientere Prozesse bei gleichzeitiger Erhöhung der Qualität, der internen Unternehmensvernetzung und Mitarbeiterzufriedenheit. Fraunhofer FIT ist Ihr Partner bei der Digitalisierung, Industrie 4.0 Projekten und Lösungen im Internet der Dinge.

Das Blockchain Labor von Fraunhofer FIT beschäftigt sich seit 2015 mit der Blockchain Technologie und Anwendungen. Es unterstützt Unternehmen bei der Identifikation von Innovationen und Effizienzsteigerungspotentialen durch Blockchain und begleitet deren Realisierung.

https://www.fit.fraunhofer.de/

Institut für Angewandte Blockchain (IABC)

Das Institut für Angewandte Blockchain an der Digital Business University in Berlin ermöglicht die systematische Identifizierung von Blockchain basierten Anwendungsfeldern und vermittelt ein tiefes Verständnis in Kombination aus Wissenschaft und Wirtschaft. Im Zentrum der Aktivitäten des IABC stehen dabei die Aus- und Weiterbildung sowie Projekte zur Erforschung der Anwendung der Blockchain für die Industrie und öffentliche Verwaltung.

http://www.iabc.dbuas.de

Institut für Internet-Sicherheit

Das Institut für Internet-Sicherheit – if(is) wurde 2005 an der Westfälischen Hochschule, Gelsenkirchen von Prof. Norbert Pohlmann gegründet, um Innovationen im Bereich der anwendungsorientierten Internet-Sicherheitsforschung zu schaffen. Das if(is) hat seine Wurzeln im Fachbereich Informatik. Rund 50 MitarbeiterInnen befassen sich dort täglich mit der Forschung an lösungsorientierten Methoden zur Steigerung der Internet-Sicherheit für alle Zielgruppen – von Großunternehmen und Mittelständlern über die Betreiber kritischer Infrastrukturen, bis hin zum Endverbraucher in seinem digitalen Alltag.

Die Forschungsgruppe Blockchain beschäftigt sich mit der Blockchain Technologie als Enabler neuer Geschäftsmodelle und effizienterer Geschäftsprozesse. Abseits der Umsetzung von Pilotprojekten mit Partnern aus der öffentlichen Verwaltung und der Industrie betreibt sie akademische Forschung mit einem besonderen Schwerpunkt auf dem Themenkomplex Cyber-Security, Datenautonomie und Kryptographie.

https://www.internet-sicherheit.de/

regio IT

Die regio iT GmbH ist der ideale IT-Partner für öffentliche Auftraggeber – für Kommunen und Schulen, Energieversorger und Entsorger sowie Non-Profit-Organisationen. Mit Sitz in Aachen und Niederlassung in Gütersloh bietet das Unternehmen strategische und projektbezogene IT-Beratung, Integration, IT-Infrastruktur und Full-Service in vier Leistungsbereichen: IT-Service und Betrieb, Verwaltung und Finanzen, Energie und Entsorgung, Bildung und Entwicklung.

https://www.regioit.de/

Stiftung für Hochschulzulassung

Die Stiftung für Hochschulzulassung betreibt unter der Marke „hochschulstart.de“ einen Service bzw. eine Serviceplattform für den Zugang zum Studium an staatlich anerkannten Hochschulen. Im Auftrag der Bundesländer werden über hochschulstart.de zentral die Studienplätze für die bundesweit zulassungsbeschränkten Studiengänge Medizin, Tiermedizin, Zahnmedizin und Pharmazie vergeben. Außerdem werden im Auftrag der Hochschulen die Zulassungsangebote sowohl für örtlich zulassungsbeschränkte als auch für zulassungsfreie Studiengänge an weit über 100 Standorten koordiniert.

https://hochschulstart.de/

Technische Universität München

Die Technische Universität München (TUM) zählt zu den besten Universitäten Europas, in internationalen und nationalen Rankings schneidet sie regelmäßig hervorragend ab. An ihren 15 Fakultäten studieren über 41.000 Studierende, 30% von ihnen kommen aus dem Ausland. 566 Professorinnen und Professoren lehren und forschen an der TUM.

Die TUM stellt sich den Herausforderungen der Digitalisierung unserer Gesellschaft. Sie setzt das Leitmotiv der „Digitalen Hochschule“ konsequent um – eine effiziente, sichere und benutzerfreundliche Informations- und Kommunikationsinfrastruktur ist die Grundlage für Forschung, Lehre und Administration auf höchstem Niveau.

https://www.tum.de/

TrustCerts

Das ausgegründete Unternehmen aus dem Institut für Internet-Sicherheit in Gelsenkirchen beschäftigt sich mit der Entwicklung von manipulationssicheren dezentralen Systemen. Eine eigens dafür entwickeltes Blockchainsystem garantiert vollkommene Unabhängigkeit durch Vermeidung eines Single Point of Failures oder Single Point of Controls.

In Forschungs- und Pilotprojekten konnten mehrere Ansätze evaluiert werden, wobei neben der Benutzerfreundlichkeit und Skalierung der Punkt langfristige Sicherheit sensibler Daten berücksichtigt wurden. Durch ein sehr generalisiertes Verfahren konnten bereits zwei Hochschulen in einer Testphase ihre Zeugnisse digital über die Blockchain absichern.

https://www.trustcerts.de/

7.1. Ansprechpartner / Kontakt

Institution	Ansprechpartner	Funktion	E-Mail	Telefon	Adresse
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie NRW	Helmut Nehrenheim	Referent	helmut.nehrenheim@mwide.nrw.de	+49 211 61772 512	Berger Allee 25 40213 Düsseldorf

Blockchain in der Verwaltung (BiVD)					
Berlin Partner für Wirtschaft und Technologie GmbH	Shoshana Schnippenkoetter	Projektmanager in Innovation im Bereich IKT	shoshana.schnippenkoetter@berlin-partner.de	+49 30 46302-106	Fasanenstr. 85 10623 Berlin
Bundesdruckerei	Eric Stange Jörg Rückriemen	Project Manager Technical Project Manager	eric.stange@bdr.de joerg.rueckriemen@bdr.de	+49 160 979 186 25 +49 172 383 6284	Kommandantenstr. 18, 10969 Berlin
Deutscher Akademischer Austauschdienst	Alexander Knoth	Senior Expert Digitalization	knoth@daad.de		Büro Berlin, Markgrafenstraße 37, 10117 Berlin
Fraunhofer FIT	Prof. Wolfgang Prinz, PhD	stellv. Institutsleiter	wolfgang.prinz@fit.fraunhofer.de	+49 2241 142730	Schloss Birlinghoven, 53754 Sankt Augustin
Institut für Angewandte Blockchain	Dr. Christoph Haupenthal	Institutsleiter	christoph.haupenthal@iabc.dbuas.de	+49 (0)30 40365992	Oranienstraße 185 10999 Berlin
Institut für Internet-Sicherheit	Kevin Wittek	Leiter Forschungsgruppe Blockchain	wittek@internet-sicherheit.de	+49 209 95 96 696	Neidenburger Straße 43, 45897 Gelsenkirchen
regio IT	Peter Niehues	Enterprise Architekt	Peter.Niehues@regioit.de	+49 241 41359-1595	Lombarden-straße 24, 52070 Aachen
Stiftung für Hochschulzulassung	Guido Bacharach	Leiter Stabsstelle Strategie und Digitalisierung	guido.bacharach@hochschulstart.de	+49 231 1081 – 1090	Sonnenstr. 171 44137 Dortmund
Technische Universität München (TUM)	Dr. Hans Pongratz	Vizepräsident / CIO	pongratz@tum.de	+49-89-289-28240	Arcisstr. 21 80333 München
TrustCerts	Mirko Mollik	Geschäftsführer	mollik@trustcerts.de	Büro: +49 209 95 96 877 Mobil: +49 1577 600 9706	Neidenburger Straße 43, 45897 Gelsenkirchen
GIZ Lab	Franz von Weizsäcker	Leiter	franz.weizsaecker@giz.de	+49 151-27671669	GIZ @Impact Hub, Friedrichstr. 246, 10969 Berlin

7.2. Beispiele für Formate

- JSON → OpenBadge Felder gefunden → B4E Felder gefunden -> Fraunhofer
- JSON → Claim-Daten gefunden → TrustCerts
- URL → Claim-Parameter gefunden → Parameter auswerten und Claim erzeugen -> TrustCerts
- PDF → QR-Code gefunden → URL
- PDF → JSON-Daten im Anhang gefunden → JSON
- PDF → ELMO Daten im Anhang → Bundesdruckerei
- XML → ELMO Daten gefunden → Bundesdruckerei

7.3. Beispielprozess für das Ausstellen eines Zeugnisses

Ausstellen eines Zeugnisses

- Issuer (Schule, Hochschule etc.) erstellt Account (z.B. in einem System wie „Schild-NRW“) und lässt diesen Account durch übergeordnete Stelle z. B. Schulbehörde autorisieren.
  (Sowohl die Accounts, als auch Autorisierung liegen in Blockchain)
- Issuer (Schule, Hochschule etc.) erfasst Daten des Zeugnisses (z.B. in einem System wie „Schild-NRW“) und erzeugt eine Zeugnisdatei im PDF Format.

- Issuer übergibt PDF und Zeugnisdaten (json liste) an Signier-Komponente, die im Schul Management System integriert ist.
  Signier Komponente prüft Autorisierung des Ausstellers und fügt dem pdf die Elmo xml datei zu und signiert diese Datei und das PDF. Danach wird der Hash in die Blockchain eingetragen und das komplette Zeugnis zurückgegeben.

- Issuer speichert das digitale Zeugnis auf seinen elektronischen Systemen und seinem Datenschutz-Voraussetzungen so lange, wie er auch ein analoges Zeugnis hätte aufbewahren müssen. Die Prozesse bzgl. Erstellung von Zweitzeugnissen analog zum Papierfall. (Dafür baut die BDR später noch eine Lösung)

Übergabe des Zeugnisses an Learner (Schüler, Studierender etc.)

- Das digitale Zeugnis wird
  - entweder auf einem Datenträger (Stick, CD o.ä.) dem Learner persönlich übergeben
  - oder vom Learner in einer gewissen Zeitfrist von einem Portal heruntergeladen.

Übergabe eines Zeugnisses (an einen dritten Empfänger)

Direkte Übergabe

- Der Learner sendet dem Empfänger das digitale Zeugnis als Datei direkt per Email o.ä.

Übergabe über Bewerbungsportal des Empfängers

- Der Learner benutzt das Bewerbungsportal eines Empfängers, um sich dort zu bewerben.
- Er wird während des Prozesses aufgefordert, sein digitales Zeugnis hochzuladen.
- Eine Funktionalität des Bewerbungsportals erlaubt dem Learner, sein digitales Zeugnis (von einem beliebigen Datenträger) hochzuladen.
- Das Bewerbungsportal ruft eine ***externe Validierungsfunktionalität*** auf. Diese validiert das digitale Zeugnis oder verwehrt den Upload.

Empfang eines Zeugnisses (durch einen Dritten)

Nach direkter Übergabe

- Der Empfänger nutzt ein ***externes Validierungsportal*** um das digitale Zeugnis zu validieren.
- Die Daten werden manuell übertragen.

Nach Übergabe über Bewerbungsportal des Empfängers

- Die empfangenen Klardaten werden von dem Bewerbungsportal des Empfängers ausgelesen und medienbruchfrei weiterverarbeitet.