Manipulationssichere und per Knopfdruck verifizierbare Digital Credentials: Die Blockchain als Initiator internationaler Kooperationsprojekte

Anastasia Bertini, Annelie Pentenrieder, Jan Rebentisch, Samer Schaat und Robert Rentzsch

Zusammenfassung

Digital Credentials sind digitale Nachweise, die in verschiedenen Kontexten erbrachte Lernleistungen und Qualifikationen erfassen. Die automatische Verifizierbarkeit solcher Nachweise bildet die Grundlage für ihren sicheren und effizienten Austausch. Dafür setzen derzeit verschiedene nationale und internationale Projekte auf die Blockchain-Technologie. In diesem Beitrag werden vier internationale Hochschulkoperationen mit deutscher Beteiligung betrachtet: Credentify, DigiCerts, das Digital Credentials Consortium und EduCTX.

Die fünf Autorinnen und Autoren haben zu gleichen Teilen zum Artikel beigetragen. Die Projektleitung lag bei R. Rentzsch.

A. Bertini · A. Pentenrieder · J. Rebentisch · S. Schaat · R. Rentzsch (✉)
Institut für Innovation und Technik (iit), Berlin, Deutschland
E-Mail: rentzsch@iit-berlin.de

A. Bertini
E-Mail: bertini@iit-berlin.de

A. Pentenrieder
E-Mail: pentenrieder@iit-berlin.de

J. Rebentisch
E-Mail: rebenisch@iit-berlin.de

S. Schaat
E-Mail: schaat@iit-berlin.de

Auf der Grundlage umfassender Recherchen und qualitativer Interviews werden die Projekte einerseits beschrieben, wobei auch grundlegende technische Konzepte erläutert werden. Andererseits werden die von den Projekten geteilten Herausforderungen sowie die Erwartungen, die von den verschiedenen Seiten an die Entwicklung von Digital-Credentials-Systemen gestellt werden, diskutiert.

Schlüsselwörter

Digital Credentials • Digitale Leistungsnachweise • Digitale Nachweise • Digitale Zertifikate • Blockchain • Hochschulkooperation • Internationale Netzwerke

1 Einführung

Eine Vielzahl von Initiativen konzentriert sich derzeit auf die Entwicklung digitaler Lern- und Qualifikationsnachweise, sogenannter Digital Credentials (DC). Gegenüber papierbasierten Nachweisen sollen DC vor allem schnell und unkompliziert ausstellbar, teilbar und verifizierbar sein. Gerade der letzte Punkt, die Erkennung von Urkundenfälschungen, bindet bei Hochschulen und Arbeitgebern bislang personelle Ressourcen und könnte durch die zunehmende internationale Mobilität von Studierenden und Arbeitskräften ein immer größeres Problem werden (Ezell 2019; Ronnie und Goodman 2019). Dies zeigt bereits eine einfache Websuche: Die Abfrage „fake diploma“ führt schnell auf Seiten, die hochqualitative Fälschungen anbieten.

Für die Verwaltungs- und IT-Infrastrukturen an Hochschulen stellen Systeme zur Ausstellung, Speicherung und zum sicheren Austausch von DC eine neue Herausforderung dar (Christmann-Budian et al. 2018; Orr und Rampelt 2018). Ein möglicher Lösungsansatz ist die Blockchain-Technologie (Camilleri et al. 2019; Grech und Camilleri 2017), die neben der Schaffung alternativer Währungen wie Bitcoin prinzipiell überall dort einsetzbar ist, wo viele Akteur*innen an der manipulationssicheren, dezentralen Speicherung eines gemeinsamen Registers von zeitlich aufeinanderfolgenden Transaktionen (oder einfacher: Einträgen) interessiert sind (Klebsch et al. 2019). Bei Ausstellung eines DC kann beispielsweise ein Eintrag in einer Blockchain erfolgen, der dessen Originalzustand durch eine Art digitalen Fingerabdruck unveränderbar festhält. Die wachsende Blockchain selbst wird dabei als stets aktuelle Kopie von allen Teilnehmenden vorgehalten.

In diesem Beitrag werden beispielhaft vier aktuelle internationale Hochschulkooperationen mit deutscher Beteiligung betrachtet, die jeweils mehrere

Hochschulen und/oder weitere Einrichtungen aus dem Bildungssektor in mindestens zwei europäischen Ländern umfassen und die zunächst nicht kommerzieller Natur sind. Die Grundlage hierfür bilden Recherchen und Interviews mit Projektbeteiligten¹ zwischen Januar und April 2020. Es werden zunächst einige grundlegende Konzepte, die in der Folge zum technischen Verständnis nötig sind, erläutert. Auf dieser Basis folgt die Vorstellung der Projekte, an welche sich ein Vergleich verschiedener Kernaspekte anhand der geteilten Herausforderungen anschließt. Die Erwartungen und Rollen der verschiedenen Prozessbeteiligten bei der Etablierung künftiger DC-Systeme werden gesondert diskutiert, bevor ein abschließender Ausblick erfolgt.

2 Grundlegende technische Konzepte

Für eine umfassende Erläuterung konzeptioneller und technischer Aspekte, die für den Einsatz der Blockchain-Technologie im Bildungssektor relevant sind, sei hier auf zwei existierende Publikationen (Camilleri et al. 2019; Grech und Camilleri 2017) verwiesen. Zum Verständnis werden im Folgenden aber einige grundlegende technische Konzepte vorausgesetzt. Zunächst sind dies drei (nicht nur) im Blockchain- und DC-Kontext wichtige kryptografische Techniken: Hashing, digitale Schlüsselpaare und digitale Signaturen.

Ein Hashing-Algorithmus übersetzt eine Zeichenkette beliebiger Länge, beispielsweise den Inhalt einer Datei, in eine Zeichenkette mit fester, in der Regel deutlich kürzerer Länge – den Hashwert. Die Funktion ist dabei so gewählt, dass erstens der gleiche Input immer zum gleichen Output führt, zweitens schon bei kleinsten Änderungen des Inputs ein vollkommen anderer Output erzeugt wird und drittens der Output nur mit unverhältnismäßig großem Aufwand in den Input zurückübersetzt werden kann. Hashwerte spielen neben ihrer oben genannten Nutzung als Fingerabdruck für Dokumente auch eine entscheidende Rolle im Blockchain-Konzept selbst (siehe unten). Ein digitales Schlüsselpaar hingegen bilden zwei Zeichenketten fester Länge, von denen eine nur dem Eigentümer des Paares bekannt ist (privater Schlüssel), während die andere Dritten allgemein oder selektiv zugänglich gemacht wird (öffentlicher Schlüssel). Beliebige Zeichenfolgen – zum Beispiel E-Mails oder Dateien – können jeweils mit einem der beiden Schlüssel algorithmisch chiffriert werden. Eine spätere Dechiffrierung

¹Wir bedanken uns herzlich bei Stefanie Bock, Anthony F. Camilleri, Jochen Ehrenreich, Bernd Kleinheyer, Davor Orlic, Dr. Hans Pongratz, Prof. Dr. Ulrich Schäfermeyer, Ass.-Prof. Dr. Muhamed Turkanović und Andreas Wittke.

kann nur mit dem jeweils anderen Schlüssel erfolgen. Bei einer digitalen Signatur schließlich werden beide Konzepte verknüpft: Eine zu signierende Datei wird zunächst gehasht, daraufhin wird der Hashwert mit dem privaten Schlüssel der oder des Signierenden verschlüsselt. Der verschlüsselte Hashwert und der öffentliche Schlüssel der oder des Signierenden bilden zusammen die Signatur. Zur späteren Prüfung, ob die Datei verändert wurde, wird zunächst der öffentliche Schlüssel aus der Signatur verwendet, um den ebenfalls enthaltenen Original-Hashwert zu entschlüsseln. Die Datei wird dann erneut gehasht. Nun können die beiden Hashwerte verglichen werden: Nur wenn sie übereinstimmen, weist die Datei den unveränderten Originalzustand auf.

Damit lässt sich auch verstehen, wie eine Blockchain, die stets bei allen an ihr teilnehmenden Knoten als Kopie vorliegt, wächst:

„In jeden neuen Datensatz (,block‘) wird eine kryptografische Prüfsumme (Hashwert) der bisherigen Kette (,chain‘) von Datensätzen geschrieben, sodass eine Manipulation der Daten durch einzelne Teilnehmende im Prinzip unmöglich ist. Jeder neue Block wird durch ein dezentrales Konsensverfahren geschaffen und an die Blockchain angehängt, durch das die Reihenfolge der Datensätze in der Blockchain festgelegt wird“ (VDI Technologiezentrum 2018, S. 2).

In jedem neuen Block werden normalerweise viele neue Transaktionen (hier DC-Ausstellungen) zusammengefasst, bevor dieser geschrieben wird. Abb. 1 skizziert eine von Hochschulen und sonstigen Bildungsorganisationen gemeinsam genutzte Blockchain für DC. In diesem Fall betreiben diese auch selbst die Blockchain, fungieren also als Knoten. Eine Auslagerung dieser Aufgabe auf bestehende Infrastrukturen ist allerdings möglich.

Nachdem es schon nach Einführung der Bitcoin-Blockchain Versuche gegeben hatte, diese auch für Anwendungen jenseits der Erfassung von Währungstransaktionen zu nutzen, wurden hierfür später alternative Blockchain-Frameworks entwickelt. Das bekannteste, das auch die unten vorgestellten Projekte nutzen, ist Ethereum. Ethereum-Blockchains können nicht nur Transaktionen der Währung Ether erfassen, sondern auch solche beliebiger anderer, jeweils einzigartiger Token. Dies kann etwa ein Kinoticket sein oder, wie in einem der Beispiele unten, ein DC. Das Framework ist außerdem performanter als Bitcoin, da Blöcke deutlich schneller validiert werden.

Abb. 1 Modell einer Blockchain für digitale Leistungsnachweise. Hochschulen und sonstige Bildungsanbieter stellen DC in Dateiform aus, wobei die Dateien die Informationen zum DC üblicherweise sowohl als visuelle Komponenten (etwa eine beschriftete Urkunde oder ein Abzeichen) als auch in maschinenlesbarer Form enthalten. In die Blockchain wird bei einer klassischen Implementierung nur ein Hashwert, eine Art Fingerabdruck der Datei, geschrieben. Mit diesem kann später deren Integrität verifiziert werden, insbesondere von anderen Bildungsorganisationen und Unternehmen. Die Sammelmappe entspricht einem Onlineportfolio, über welches Individuen ihre DC verwalten und diesen Akteur*innen sowie ggf. anderen Webseiten selektiv zugänglich machen können. (Eigene Darstellung)

3 Laufende Projekte

Die im Folgenden vorgestellten Projekte verbindet das Ziel, eine zuverlässige und gemeinsam genutzte digitale Infrastruktur zur Ausstellung und Verifikation von DC auf Blockchain-Basis zu entwickeln. Ihre Genese, die beteiligten Bildungseinrichtungen, der konzeptionelle Fokus und auch die technische Umsetzung unterscheiden sich jedoch teils deutlich. Die Reihenfolge der Projekte wurde hier so gewählt, dass im Zuge der Projektbeschreibungen dem Lesenden gleichzeitig auch geteilte technische und konzeptionelle Aspekte jeweils am Praxisbeispiel vermittelt werden können, dabei aber Redundanz vermieden wird. So kam auch

der unterschiedliche Entwicklungsstand der Projekte zum Tragen, keinesfalls jedoch eine inhaltliche Bewertung.

3.1 DigiCerts

Neun Institutionen aus dem Forschungs- und Bildungsbereich sind Mitinitiatoren der Blockchain-Allianz DigiCerts.² Dazu gehören neben den Hochschulen RWTH Aachen und TH Lübeck (samt deren Onlinekursportal oncampus) sowie dem Fraunhofer-Institut für Angewandte Informationstechnik (eines von drei Fraunhofer-Mitgliedern) auch Kiron Open Higher Education und die Gesellschaft für Akademische Studienvorbereitung und Testentwicklung e. V. Weiterer Partner ist iMooX, eine MOOC-Plattform der Universität Graz und der TU Graz. Aktuell betreibt DigiCerts ein Testnetzwerk aus elf und ein produktives Netzwerk aus fünf Knoten. Das in DigiCerts verwendete Blockchain-Framework ist der Ethereum-Ableger Quorum, das Gesamtkonzept basiert auf der zuvor veröffentlichten „Blockchain for Education“ (Gräther et al. 2018) und wurde seitdem weiterentwickelt und modifiziert.

Im April 2020 hat die TH Lübeck mit oncampus erstmals DC an Absolvent*innen eines Onlinekurses vergeben, die über diese Blockchain fälschungssicher und jederzeit automatisch verifizierbar sind. Um der bisher schwierigen Anbindung an existierende Hochschulinformationssysteme (HIS) als Kernsoftware der Hochschulen vorerst aus dem Weg zu gehen, wurde zur Erstellung und Vergabe der DC ein von Lehrenden einfach zu nutzendes Moodle-Plugin entwickelt; eine analoge Entwicklung für das in Deutschland verbreitete Lernmanagementsystem ILIAS ist geplant. DigiCerts-DCs werden von einzelnen jeweils von der vergebenden Institution autorisierten Bearbeitenden ausgestellt, wobei jede Institution selbst zunächst durch eine übergeordnete Instanz akkreditiert werden muss. Dieses Rechtemanagement wird, zusätzlich zur folgenden Kernaufgabe, ebenfalls über die genutzte Blockchain implementiert. Bei DC-Vergabe werden die relevanten Daten, wie Institution, Empfänger*in und Kurstitel, zunächst in einem standardisierten Format erfasst. Initial wird hierfür eine Erweiterung des Open-Badges-Standards³ verwendet. Danach wird aus dieser Datenstruktur ein Hashwert gebildet und dieser in der Blockchain gespeichert. Gleichzeitig erhält die/der Empfänger*in das DC als Urkunde in Form einer PDF-Datei, welche mit

²Siehe: www.digicerts.de. Zugegriffen: 27.04.2020.

³Siehe: <https://www.imsglobal.org/activity/digital-badges>. Zugegriffen: 27.04.2020.

dem privaten Schlüssel der bearbeitenden Person signiert wird. In diese ist zusätzlich die mit den sichtbaren Inhalten übereinstimmende, aber maschinenlesbare Datenstruktur integriert. Zur späteren Verifikation durch Dritte, etwa Arbeitgeber oder Hochschulen, kann die Datei auf einer Webseite der TH Lübeck hochgeladen werden. Dort wird die Datenstruktur extrahiert und erneut gehasht. Der resultierende Hashwert wird dann mit dem Original aus der Blockchain abgeglichen und damit die Gültigkeit des DC verifiziert. Zusätzlich soll künftig auch die Signatur der Datei geprüft werden, um sicherzustellen, dass auch deren sichtbarer Inhalt unverändert ist.

3.2 EduCTX

EduCTX⁴ geht auf ein Projekt des „Blockchain Lab“ der Universität Maribor zurück und hat mittlerweile drei weitere Partner, die Universität Sarajevo, die TU Brunn und die FH Bielefeld. Im Rahmen dieses Vorhabens wird eine blockchainbasierte Plattform zum Austausch von DC für Hochschulen entwickelt (Turkanović et al. 2018)⁵. Das Netzwerk besteht derzeit aus vier Knoten und basiert auf dem Blockchain-Framework Hyperledger Besu⁶. Es wird bereits mit Studierendendaten der beteiligten Hochschulen getestet. Bei der Implementierung unterstützt die Universität Maribor die weiteren Projektpartner, welche dann im Sinne eines Wachstums iterativ neue Partner gewinnen und unterstützen sollen. Um an EduCTX teilzunehmen, müssen Studierende zunächst ein Ethereum-Konto erstellen, wobei auch ein damit verbundenes Schlüsselpaar generiert wird. Hierfür kann zum Beispiel das populäre Browser-Plugin MetaMask⁷ genutzt werden, welches danach außerdem als sogenanntes Wallet (in Abb. 1 als Sammelmappe abgebildet) fungiert. Dies dient den Nutzenden einer Blockchain einerseits zur Verwaltung ihrer Kontoschlüssel und andererseits zur Abfrage ihres derzeitigen Bestandes an Coins und/oder anderen Tokens (sowie ggf. dem Auslösen von Überweisungen). Mit dem Schlüsselpaar können sich die Studierenden danach

⁴Siehe: <https://www.eductx.org>. Zugegriffen: 27.04.2020.

⁵Der Ansatz hat sich seit dieser Publikation technisch und konzeptionell stark verändert, siehe EduCTX-Webseite.

⁶Hyperledger Besu, als Teil des Hyperledger-Projektes für Blockchain-Anwendungen (<https://www.hyperledger.org/>. Zugegriffen: 27.04.2020), ist ein Ethereum-Ableger, der häufig für Blockchains eingesetzt wird, bei denen nur autorisierte Nutzende Schreibrechte haben.

⁷Siehe: <https://metamask.io>. Zugegriffen: 27.04.2020.

auf der EduCTX-Plattform anmelden, um eine EduCTX ID zu erhalten. Die Verwaltung der jeweiligen Hochschule muss diese ID dann mit der existierenden Studierenden-ID (etwa einer Matrikelnummer, langfristig aber eher einer national oder international geteilten digitalen Identität, siehe unten) verknüpfen.

DC werden von entsprechend autorisierten Hochschulen entweder über das EduCTX-Webportal ausgestellt oder direkt aus ihrem HIS durch den Zugriff auf eine entsprechende Webschnittstelle. Dafür wird zunächst eine DC-Datei mit sämtlichen relevanten Daten erstellt, etwa Institution, Art- und Titel des Nachweises sowie Name und EduCTX-ID der oder des Studierenden. Diese wird mit dem öffentlichen Schlüssel der oder des Studierenden verschlüsselt und so in einem verteilten Dateisystem⁸ gespeichert. Gleichzeitig wird in der Blockchain ein Token auf das Konto des oder der Studierenden ausgestellt, wobei die Transaktion von der Hochschule digital signiert wird. Der Token verweist auf den Speicherort der DC-Datei und enthält zudem ihren Hashwert. Damit kann über die EduCTX-Plattform jederzeit das entsprechende DC heruntergeladen, entschlüsselt und als PDF-Datei (bzw. als ZIP-Datei bei mehreren DC) exportiert werden. Die exportierte Datei kann danach an Dritte zur Verifikation gesendet werden, welche das DC über das EduCTX-Portal durch einen Abgleich der Hashwerte (wie bei DigiCerts) verifizieren können.

3.3 Credentify

Der Ursprung von Credentify⁹ ist das EU-geförderte Projekt MicroHE¹⁰, welches Angebote im Bereich Microcredentials (DC für kurzformatige Lernangebote innerhalb und außerhalb von traditionellen Bildungseinrichtungen und -kontexten) bzw. deren mögliche künftige Anrechnung und Anerkennung für Studiengänge untersucht; weiterhin floss das in MicroHE entwickelte Datenmodell zur standardisierten Erfassung von DC in die Europass Digital Credentials Infrastructure (EDCI) des neuen Europasses¹¹ ein. Die Credentify-Mitglieder umfassen neben Hochschuleinrichtungen aus Deutschland (Duale Hochschule Baden-Württemberg), Finnland, Italien und Slowenien auch Stiftungen und Think-Tanks. Federführend ist die britische „Knowledge 4 All Foundation“.

⁸Dieses wird wie die Blockchain, aber separat von dieser von den EduCTX-Knoten betrieben; siehe <https://ipfs.io>. Zugriffen: 27.04.2020.

⁹Siehe: <https://credentify.eu>. Zugriffen: 27.04.2020.

¹⁰Siehe: <https://microcredentials.eu>. Zugriffen: 27.04.2020.

¹¹Siehe: <https://ec.europa.eu/futurium/en/eupass/new-eupass>. Zugriffen: 27.04.2020.

Entwickelt wird Credentify als Webschnittstelle bzw. als Infrastructure-as-a-Service, mit der sowohl HIS als auch Lernmanagementsysteme wie Moodle interagieren können sollen, um DC auf einer Ethereum-Blockchain auszustellen. „Auf“ ist hier wörtlich zu nehmen, denn anders als in den oben vorgestellten Projekten sollen nicht nur Hashwerte in die Blockchain geschrieben werden, sondern das gesamte DC in verschlüsselter Form. Als Datenstandard nutzt Credentify, wie nunmehr auch die oben genannte EDCI, hierfür den „Verifiable Credentials“ bzw. VC-Standard¹² des World-Wide-Web-Konsortiums (W3C). Dieser soll DC aus verschiedensten (auch außerhochschulischen) Quellen unterstützen. Wie bei EduCTX nutzen sowohl Hochschulen als auch Studierende in diesem Szenario Schlüsselpaare aus selbst erstellten Ethereum-Konten und verwalten diese beispielsweise mit MetaMask. Ein prototypischer Einsatz im Bereich nonformale Bildung ist auf dem freien MOOC-Portal VideoLectures.NET des Instituts Jožef Stefan in Ljubljana geplant. Weiterhin wird das System derzeit mit einer Reihe von Universitäten und anderen Bildungsanbietern getestet.

3.4 Digital Credentials Consortium

Das Digital Credentials Consortium¹³ (DCC) wird von derzeit zwölf Universitäten aus Europa und Nordamerika getragen, darunter das MIT, dessen Media Lab bereits 2016 den für die hier vorgestellten Projekte gewissermaßen prototypischen Standard Blockcerts¹⁴ veröffentlichte, damals noch auf Basis der Bitcoin-Blockchain. Aus Deutschland sind die TU München und das Hasso-Plattner-Institut am Konsortium beteiligt. Seine Ziele hat das DCC in einem umfangreichen Whitepaper dargelegt (Duffy et al. 2020). Demnach soll zum einen ein möglichst weltweiter Standard zur Ausstellung und Verifikation von DC geschaffen werden, zum anderen eine korrespondierende Infrastruktur, höchstwahrscheinlich auf Blockchain-Basis (betont wird ausdrücklich eine jeweils anwendungsgerechte Umsetzung, jenseits jeden Hypes). Beim Datenstandard orientiert sich die Initiative, wie auch Credentify, eng am W3C-VC-Standard und entwickelt diesen aktiv mit. In jedem Fall soll es sich beim Datenformat um eine Art Container beziehungsweise Umschlag handeln, in den etwa auch existierende Open Badges eingebettet werden können und innerhalb dessen diverse existierende Vokabularien zur standardisierten Beschreibung der Lerninhalte und des

¹²Siehe: <https://www.w3.org/TR/vc-data-model>. Zugriffen: 27.04.2020.

¹³Siehe: <https://digitalcredentials.mit.edu>. Zugriffen: 27.04.2020.

¹⁴Siehe: <https://www.blockcerts.org>. Zugriffen: 27.04.2020.

Qualifikationsniveaus des jeweiligen DC genutzt werden können. Infrastrukturell geht es, wie bei allen anderen Projekten, zunächst um eine Referenzimplementierung mit den teilnehmenden Hochschulen. Betont wird vom DCC aber auch, dass diese später nicht zwingend die Betreiber bzw. Knoten sein müssten, sondern dies auch an externe Anbieter oder in bestehende Infrastrukturen ausgelagert werden könnte.

3.5 Geteilte Herausforderungen

Allen oben beschriebenen Projekten ist zunächst gemein, dass sie bisher nur sehr kleine Blockchain-Netzwerke betreiben. Deren Manipulationssicherheit wächst generell mit der Anzahl der Knoten, kann aber bei kleinen Netzwerken und insbesondere, wenn, wie beim DC-Anwendungsfall, komplexe Konsensmechanismen vermieden werden sollen, auch an die Vertrauenswürdigkeit der einzelnen Knotenbetreiber gekoppelt werden. Deshalb bieten oder planen alle Projekte eine (technisch unterschiedlich implementierte) Form der Erfassung autorisierter Teilnehmender mit Schreib- und damit DC-Ausstellungsrechten für die jeweilige Blockchain. Im Gegensatz zu monetären Anwendungen wie Bitcoin ist demnach nur das Auslesen von Daten (etwa zur DC-Verifikation) auch für Dritte möglich. Weiterhin betreiben oder planen alle Projekte ihre Blockchains mit einem sogenannten Proof-of-Stake- bzw. Proof-of-Authority-Konsensverfahren statt dem etwa bei Bitcoin eingesetzten und für seine hohen Energiekosten bekannten Proof-of-Work. Der Anreiz, die Blockchain nicht zu manipulieren sowie neue Blöcke zu validieren und zu schreiben, liegt hier grundsätzlich im Interesse aller Beteiligten (vor allem derer, die viele DC ausstellen) und muss nicht, wie etwa bei Bitcoin, über ein Belohnungssystem implementiert werden. Deshalb entfällt auch jegliches Mining und die Validierung neuer Blöcke kann sehr schnell und ressourcenschonend erfolgen.

Alle befragten Projekte sind sich weiterhin der verschiedenen Herausforderungen an eine DC-Blockchain-Infrastruktur im Bereich Datenschutz bewusst. Die europäische Datenschutzgrundverordnung (DSGVO) ist dabei von zentraler Bedeutung (Camilleri et al. 2019). Mindestens problematisch ist demnach das Speichern von Identifikatoren, die eindeutig Einzelpersonen zugeordnet werden können, in Datenstrukturen wie der Blockchain. Dies gilt selbst dann, wenn es nicht namentlich, sondern in pseudonymisierter Form (etwa über eine Matrikelnummer oder einen öffentlichen Schlüssel) erfolgt. Dieser Punkt gewinnt durch die inhärente Unveränderbarkeit der Blockchain und das damit durch sie

allein nicht erfüllbare Recht auf Vergessen personenbezogener Daten der DSGVO zusätzlich an Gewicht.

Die Projekte verfolgen hierzu verschiedene Strategien. DigiCerts und EduCTX umgehen das Problem, was die Blockchain betrifft, gänzlich, indem sie nur Hashwerte der DC-Daten in die Blockchain schreiben. Ein externes Rechtsgutachten hat DigiCerts demnach bereits DSGVO-Konformität bescheinigt. Wichtig ist ganz allgemein, dass die Identität der DC-Vorweisenden im Verifikationsprozess nicht mitgeprüft werden kann: Es ist zumindest denkbar, dass Dritte, die sich (etwa durch eine vorherige Rolle als Verifizierende) Zugang zur DC-Datei verschaffen, diese womöglich in einer Mail unter Vorgabe der Identität der auf dem DC genannten Person für eigene Zwecke missbrauchen. Zu umgehen wäre dies, wenn man von Verifizierenden DC-Dateien zum Beispiel nur in Form signierter Mails akzeptiert. Hierfür müssten Studierende allerdings generell ein Schlüsselpaar zur sicheren elektronischen Kommunikation erstellen und entsprechend nutzen. Es bräuchte zudem eine öffentlich zugängliche (bestenfalls staatliche) Datenbank, in welcher Personen eindeutig ihren öffentlichen Schlüsseln zugeordnet werden, um erhaltene Mails bzw. deren Signaturen auch prüfen zu können (ähnlich zu etwa den seit Langem genutzten Zertifizierungsstellen zur sicheren Kommunikation mit Webseiten). Das generell komplexe Sicherheitsthema digitale Identität und Identitätsmanagement ist demnach auch laut den untersuchten Projekten für diese hochrelevant. Eine Anbindung an entsprechende laufende Entwicklungen, wie beispielsweise das Projekt eSSIF¹⁵ oder die europäische eID¹⁶, wird deshalb angestrebt.

Ein weiterer wichtiger Datenschutz- und Datensicherheitsaspekt sind die DC selbst, also die entsprechenden Dateien bzw., bei Credentify, die Blockchain-Einträge. Sowohl EduCTX als auch DigiCerts wollen (nicht im beschriebenen Prototypen, aber im zugrunde liegenden Fraunhofer-Konzept), in Analogie zum heimischen Schrank für papierbasierte Nachweise, die DC-Dateien verschlüsselt in einem Onlinedateisystem speichern, auf welches die DC-Empfänger*innen zugreifen können. Die Credentify-Lösung, bei der die DC selbst in der Blockchain gespeichert werden, könnte den Transfer von Dateien ggf. gänzlich vermeiden, aber auch mit den oben genannten DSGVO-Vorgaben kollidieren. Im Gegensatz zu DigiCerts und den Plänen des DCC erhalten Studierende bei EduCTX und Credentify außerdem selbst (zu verwaltende) Blockchain-Konten.

¹⁵Siehe: <https://essif-lab.eu>. Zugegriffen: 27.04.2020.

¹⁶Siehe: <https://ec.europa.eu/digital-single-market/en/e-identification>. Zugegriffen: 27.04.2020.

Die Unveränderbarkeit der Blockchain wirft nicht nur im Kontext des oben erwähnten Rechts auf Vergessen – also der von Datenhaltenden prinzipiell einzurichtenden Möglichkeit einer Löschung von Einträgen – Fragen auf, sondern bereits beim sehr konkreten Szenario einer Modifikation: Grundsätzlich sollte die Ausstellung von DC eine Statussetzung ermöglichen, um zum Beispiel Einsprüche von Studierenden oder die Wiederholung von Prüfungen, aber auch eine Aberkennung zu berücksichtigen. Hierfür enthalten die Konzepte hinter allen vorgestellten Projekten gesonderte (technisch verschieden implementierte) Statuserfassungsmethoden, beispielsweise wiederum dezentrale Register. Das DCC formuliert dies wie folgt:

„The issuer may need to revoke a credential after issuance. For cases like this, credential status registries are part of our decentralized infrastructure. Issuers have control over their respective credential status registry where they can update the status of the validity of credentials. During the verification process this registry is consulted“ (Duffy et al. 2020).

4 Erwartungen und Aufgaben der Beteiligten

Bei der Beschäftigung mit dem Thema DC und insbesondere, wenn, wie hier, konkrete Projekte untersucht werden, wird klar, dass die verschiedenen Prozessbeteiligten im Bildungs- und Berufssystem – Studierende, Bildungseinrichtungen, Politik und Arbeitgeber – unterschiedliche Erwartungen an künftige DC-Systeme stellen, ob blockchainbasiert oder nicht. Diese Erwartungen berühren häufig nicht nur technische oder konzeptionelle Aspekte, sondern richten sich auch in Form von Wünschen bzw. Aufgaben an die jeweils anderen Beteiligten.

4.1 Studierende

Wenngleich in dieser Studie keine Studierenden direkt befragt wurden, so gilt bei hochschulischen Organisationsstrukturen ganz allgemein – seien sie technischer oder sozialer Natur –, dass sie hauptsächlich den Studierenden dienen sollten. Dies gilt für die Verwaltung von DC sogar über den Hochschulaufenthalt hinaus, für den gesamten beruflichen Werdegang. Aus Projekten wie den hier vorgestellten sollten sich also für Studierende überwiegend oder gar ausschließlich Vorteile ergeben, etwa die schnellere Ausstellung und das leichtere Teilen von Nachweisen. Um dies zu gewährleisten, müssen die Projekte zwei Aspekte besonders

berücksichtigen: erstens den erwarteten Grad an technischem und konzeptionellem Verständnis der Funktionsweise des DC-Austauschs auf Blockchain-Basis. Hier erheben alle Projekte den Anspruch, dass eine Nutzung auch ohne ein solches problemlos möglich sein soll, und entwickeln bzw. planen entsprechende Webportale. Allerdings, und dies ist der zweite Punkt, setzen nach derzeitiger Konzeption zumindest EduCTX und Credentify Blockchain-Konten auf Studierendenseite voraus, deren digitale Schlüsselpaare von diesen verwaltet und verwahrt werden müssen. Trotz Assistenzsoftware wie MetaMask wird dadurch sowohl ein gewisses Maß an technischer Versiertheit als auch ein Bewusstsein von den Konsequenzen des Verlustes eines privaten Schlüssels vorausgesetzt. Im Gegensatz zu rein portalbasierten Systemen könnte mindestens der Erklär- bzw. Schulungsaufwand hier größer ausfallen, andererseits könnte es bei den Studierenden sowohl wahrgenommen als auch tatsächlich zu größerer Autonomie, Eingebundenheit und Verantwortlichkeit führen.

4.2 Hochschulen

Aus Sicht der Hochschulen ist das wohl wichtigste Argument für schnell und sicher verifizierbare DC der schon in der Einleitung skizzierte (wachsende) Aufwand, der mit der manuellen Prüfung von papierbasierten Leistungsnachweisen verbunden ist. Da hierbei vor allem internationale Bildungskarrieren eine Herausforderung darstellen, wird das Potenzial von DC und der mit ihnen verknüpften Verifikationsinstrumente (hier die Blockchain) für Verbesserungen in diesem Bereich langfristig nur dann voll genutzt werden können, wenn auch Bildungsanbieter internationale, bestenfalls weltweite Netzwerke dafür etablieren. Besonders klar folgt schon jetzt das DCC dieser Logik, wobei ihm die Reputation und Mittelausstattung der Gründungsmitglieder helfen. Gleichzeitig ist allen vorgestellten Projekten gemein, dass die Beteiligten mit der inhärenten Vernetzung, welche die Blockchain-Technologie mit sich bringt, eine grundlegende Entscheidung gegen technische Insellösungen gefällt haben. Dieser Aspekt wurde in allen Interviews betont. Ein wesentliches Kriterium für die Skalierbarkeit der jeweiligen Lösungen, so die Projekte, sei das Vertrauen, das durch die Vereinbarung und Nutzung gemeinsamer Datenstandards unter den Beteiligten entstünde, denn dieses zöge auch neue Partner*innen an.

4.3 Politik

Auch die politische Dimension wurde von den Interviewten als sehr wichtig betrachtet. Genannt wurden verschiedene Maßnahmen im Bereich der Entwicklung und Standardisierung von DC-Konzepten und Blockchain-Systemen auf europäischer, nationaler und Länderebene. Diese werden zum einen als rahmengebende Instanzen gesehen, zum anderen aber auch als notwendige Impulsgeber zur Umsetzung, Standardisierung und Skalierung der Projekte (beziehungsweise der dahinterstehenden Idee). Konkret könnte dies als Aufgabe für die Verantwortlichen dieser Maßnahmen, wie Europass oder European Blockchain Services Infrastructure (EBSI)¹⁷, formuliert werden, hier künftig sowohl eine aktive Einbindung der Projekte als auch deren Vernetzung untereinander anzustreben. Erste Kontakte bestehen bereits, beispielsweise zwischen DCC und Europass durch die W3C-VC-Arbeitsgruppe bzw. den dort entwickelten Datenstandard, die weitreichende Vernetzung von Credentify (über MicroHE und das Thema Microcredentials) in den Bologna-Prozess hinein oder die Teilnahme der EduCTX-Entwickler am EU-H2020-Projekt „Digital Europe For All“¹⁸.

4.4 Arbeitswelt

Für Unternehmen und andere Stellen, welche die Echtheit von Bildungsnachweisen überprüfen müssen, versprechen DC und ihre automatische Verifikation die gleichen Erleichterungen wie für die Hochschulen selbst – insbesondere da Arbeitskräfte heute ähnlich international mobil sind wie Studierende. Aufwendige manuelle Prüfungen könnten damit entfallen. Sollten DC allerdings mittel- oder gar langfristig unterschiedliche Formate verwenden und über unterschiedliche Schnittstellen verifiziert werden müssen, würden sich diese Vorteile schnell relativieren: Die Anpassung der genutzten HR-Systeme, damit diese analog zu den HIS die entsprechenden Schnittstellen ansprechen können, wäre dann kein einmaliger, sondern ein sich mit jeder weiteren Anbindung wiederholender Prozess. Dieses Szenario sollte vermeiden werden, um die Annahme der DC-Idee (etwa durch konkrete Investitionen in Systeme) auch auf Arbeitgeberseite sicherzustellen.

¹⁷ Siehe: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI>.
Zugegriffen: 27.04.2020.

¹⁸ Siehe: <https://www.de4a.eu>. Zugegriffen: 27.04.2020.

5 Ausblick

Die Blockchain-Technologie kann ein Katalysator für Kooperationen zwischen geografisch verteilten und heterogenen Bildungsorganisationen sein, da sie den Vorteil bietet, Daten (hier zur DC-Verifikation) nicht bei einer zentralen Instanz, sondern in Kopie über das gesamte Netzwerk verteilt zu speichern. Dies ist auch im Hinblick auf sowohl von politischer wie zivilgesellschaftlicher Seite häufig vorgebrachte Bedenken gegenüber einer zentralen Speicherung eine Stärke. Ergänzt wird dies, gegenüber anderen Möglichkeiten der verteilten Datenhaltung, durch das Versprechen quasi garantierter Datenintegrität, auch was die temporale Abfolge der Transaktionen (hier DC-Ausstellungen) betrifft. Die Blockchain vergisst gleichsam nicht. Im Bereich Datenschutz wirft dies zwar auch neue Probleme auf, es ist allerdings sehr wahrscheinlich, dass sowohl die Entwicklung und Präzisierung von Rechtsvorschriften als auch technische Designentscheidungen, wie in den hier vorgestellten Projekten, diese mittelfristig lösen werden (Camilleri et al. 2019).

Während die Initiative zur Etablierung von DC im akademischen Bereich aktuell von den Hochschulen ausgeht, werden deren Vorteile für Studierende und Beschäftigte langfristig vor allem auch dann deutlich werden, wenn DC traditioneller Bildungsinstitutionen mit DC für Bildungsangebote aus dem informellen und nonformalen Bildungsbereich verknüpft werden können. DC und damit verbundene Onlineportfolios, auf denen diese gesammelt dargestellt und selektiv geteilt werden können, könnten so das lebenslange und individualisierte Lernen unterstützen, wie auch die Interviewten betonten. Zur Erreichung dieser Ziele bedarf es jedoch mindestens einer Vereinheitlichung der genutzten Datenstandards über alle Bildungsangebote hinweg, wofür der W3C-VC-Standard der derzeit wohl aussichtsreichste Kandidat ist: Credentify nutzt ihn bereits, das DCC plant ihn zu nutzen und sowohl DigiCerts als auch EduCTX erwägen derzeit einen Wechsel.

Langfristig sollte aber auch eine gemeinsame Blockchain-Infrastruktur angestrebt werden. Hier könnten europäische Projekte wie EBSI und/oder nationale Vorhaben wie govdigital¹⁹ oder das Netzwerk Digitale Nachweise²⁰ als vertrauenswürdige Betreiber auftreten. Die bereits etablierten Netzwerke der Projekte wiederum könnten als Keimzellen oder zumindest Blaupausen solcher – langfristig möglichst großen und geografisch weit verteilten – Blockchain-Infrastrukturen fungieren. Eine offene Frage in diesem Zusammenhang ist, ob Projekte wie

¹⁹Siehe: <https://www.govdigital.de>. Zugriffen: 27.04.2020.

²⁰Siehe: <https://netzwerkdigitalenachweise.de>. Zugriffen: 27.04.2020.

die hier vorgestellten zum jetzigen Zeitpunkt zusätzlich (jeweils einzeln) auch entsprechende Onlineportfolios entwickeln sollten, wie teilweise geplant, oder sich zunächst auf die blockchaingestützte Ausstellung und Verifikation von DC beschränken. Ein Argument für Letzteres könnte sein, dass etwa der neue Europass als Top-down-Entwicklung konzeptionell und technisch im Bereich des DC-Portfolios schon sehr weit fortgeschritten ist, während die Blockchain-Aspekte noch diskutiert werden (Stand April 2020). Die Prototypen der Projekte könnten hier demnach durch Einbringung ihrer Erfahrungen und Konzepte ein größeres Gewicht entfalten als durch die Entwicklung weiterer Portfoliolösungen.

Wichtig ist es, neben den Versprechen von DC-Systemen wie den hier vorgestellten auch ihre Limitationen zu bedenken, insbesondere welche Probleme nicht (allein) durch sie gelöst werden können. Der wohl wichtigste Punkt ist hier der qualitativ-inhaltliche: Während die Echtheit von Nachweisen und die Autorisierung der ausstellenden Stellen künftig durch solche Systeme automatisch und verlässlich geprüft werden könnten, gilt dies jeweils nicht für deren Qualität. Die mit den Themen Anrechnung und Anerkennung (von zuvor bzw. anderswo erbrachten Leistungen und errungenen Qualifikationen) eng verknüpfte Qualitätssicherung von Bildungsangeboten und -organisationen wird zumindest mittelfristig kaum von der Blockchain-Technologie profitieren können. Langfristig könnten allerdings Assistenzsysteme für diese Prozesse entwickelt werden, wenn in DC nicht nur die Metadaten standardisiert erfasst würden, also der oben genannte metaphorische Umschlag, sondern auch der Brief, sprich die eigentlichen Lerninhalte, Qualifikationsniveaus etc. In diesen Bereichen gibt es schon seit Langem, auch vor und jenseits der DC-Idee, Standardisierungsbestrebungen, etwa die Taxonomie European Skills, Competences, Qualifications and Occupations²¹ (ESCO) und den Europäischen Qualifikationsrahmen. Sollte es hier zu Fortschritten kommen, könnten auch DC diese berücksichtigen und letztlich auch zur Erleichterung der oben genannten Prozesse beitragen.

Unabhängig vom konkreten Anwendungsfall können Hochschulk Kooperationen zur Implementierung einer technisch-konzeptionellen Lösung, wie hier einer Blockchain-Infrastruktur zur DC-Verifikation, einen übergreifenden, langfristigen Nutzen haben. Die Teilnehmenden zeigen damit ein gemeinsames Interesse an der Etablierung von Netzwerken und der Abkehr von (in der Vergangenheit häufig nicht hinterfragten) Insellösungen. Für Studierende, und damit auch für spätere Arbeitnehmer*innen und (immer häufiger) Weiterbildungsinteressierte, ist dies in jedem Fall ein gutes Signal.

²¹ Siehe: <https://ec.europa.eu/esco/portal/home>. Zugriffen: 27.04.2020.

Finanzierung

Das dieser Studie zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) unter dem Förderkennzeichen M532600 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autor*innen.

Literatur

- Camilleri, A., Werner, T., Hoffknecht, A., & Sorge, A. (2019). *Blockchain in der Hochschulbildung*. Essen: Edition Stifterverband 2019. <https://www.stifterverband.org/blockchain-in-der-hochschulbildung>. Zugriffen: 22. Apr. 2020.
- Christmann-Budian, S., Kuhne, J., Mah, D.-K., Mozhova, A., Paulicke, P., Rebentisch, J., & Schmidt, M. (2018). *Connected or Unconnected? – Synergiepotenziale und Herausforderungen von IT-Governance in Hochschulen*. iit Perspektive. Working Paper, 45. Berlin: Institut für Innovation und Technik (iit) in der VDI/VDE Innovation + Technik GmbH. <https://www.iit-berlin.de/de/publikationen/connected-or-unconnected-synergiepotenziale-und-herausforderungen-von-it-governance-in-hochschulen>. Zugriffen: 27. Apr. 2020.
- Duffy, K., Pongratz, H., & Schmidt, J. P. (2020). Building the digital credential infrastructure for the future. A white paper by the digital credentials consortium. <https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf>. Zugriffen: 30. Apr. 2020.
- Ezell, A. (2019). Academic fraud and the world's largest diploma mill. <https://www.aacrao.org/research-publications/quarterly-journals/college-university-journal/article/c-u-vol.-94-no.-4-fall-2019/academic-fraud-and-the-world-s-largest-diploma-mill>. Zugriffen: 30. Apr. 2020.
- Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C., & Wendland, F. (2018). Blockchain for education: Lifelong learning passport. In W. Prinz & P. Hoschka (Hrsg.), *Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies*. Bonn: EUSSET. https://doi.org/10.18420/blockchain2018_07.
- Grech, A., & Camilleri, A. F. (2017). Blockchain in education. <https://publications.jrc.ec.europa.eu/repository/handle/JRC108255>. Zugriffen: 27. Apr. 2020.
- Klebsch, W., Hallensleben, S., & Kosslers, S. (2019). Roter Faden zum Thema Blockchain. VDE Technik und Innovation. <https://www.vde.com/resource/blob/1880776/1c616e33e550c2f387202e7b8b8ad53a/roter-faden-blockchain-download-data.pdf>. Zugriffen: 30. Apr. 2020.
- Orr, D., & Rampelt, F. (2018). Bologna digital 2020. Towards a digital dimension in the bologna process, (2nd, revised version). Berlin: Hochschulforum Digitalisierung. https://hochschulforumdigitalisierung.de/sites/default/files/dateien/2018-12_Bologna_Digital_2020_Background_Paper.pdf. Zugriffen: 30. Apr. 2020.

- Ronnie, L., & Goodman, S. (2019). Fake qualifications are on the rise. How universities can manage the risk. <https://theconversation.com/fake-qualifications-are-on-the-rise-how-universities-can-manage-the-risk-109962>. Zugegriffen: 30. Apr. 2020.
- Turkanović, M., Hölbl, M., Košič, K., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access*, 6, 5112–5127.
- VDI Technologiezentrum. (2018). Blockchain – eine Technologie mit disruptivem Charakter. https://www.vditz.de/fileadmin/media/bekanntmachungen/documents/vdi_publication_blockchain_RZ_web_neu.pdf. Zugegriffen: 30. Apr. 2020.

Open Access Dieses Kapitel wird unter der Creative Commons Namensnennung 4.0 International Lizenz (<http://creativecommons.org/licenses/by/4.0/deed.de>) veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Kapitel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.