Can there be a digital university without blockchain?

Why we need a Blockchain Alliance for Digital Certificates

Andreas Wittke[1], Jan Rieger[2], Marc Vorreiter[3] and Stefanie Bock[4]

Abstract: Since at least the invention of the smartphone, we have been living in a technological society. Every area our life is influenced by digitalization, of course also education and here especially educational documents, such as certificates or diplomas. They come with special requirements, especially in terms of standardisation, but also in terms of protection against counterfeiting. The newly founded DigiCerts Alliance of the Technical University of Lübeck, RWTH Aachen, Kiron open higher education, g.a.s.t. e.V., iMooX together with Fraunhofer FIT has developed a prototype for digital certificates. DigiCerts is an alliance of like-minded people whose goal is to change the global certification processes. These processes should be digital, automated and unchangeable to ensure the trust of users, such as universities and employers.

Keywords: Certificates, Open Badges, Blockchain, Quorum, Ethereum, Moodle, Plugin

Digital certificates on the smartphone

The smartphone has taken on a central position in our lives. More and more people are using it for music, navigation, communication, but also as a wallet for cashless payments, and they will probably use it in the future as a document folder for certificates and testimonials. Whether or not this will happen should no longer be discussed. Rather, the question is: when will it happen and who will offer this service?

However, there are certain preconditions that have to be met for digital certificates to be accepted and to work. Firstly, there must be a digital infrastructure that is reliable and highly available. Furthermore, the technology must be reliable, transparent (trustworthy) and unchangeable. The blockchain technology fulfils all these requirements and everyone who wants to use the blockchain must adhere to standards or a common uniform scheme.

[1] TH Lübeck, ILD, Mönkhofer Weg 239, 23552 Lübeck, Andreas.Wittke@th-luebeck.de
[2] TH Lübeck, ILD, Mönkhofer Weg 239, 23552 Lübeck, Jan.Rieger@th-luebeck.de
[3] TH Lübeck, ILD, Mönkhofer Weg 239, 23552 Lübeck, Marc.Vorreiter@th-luebeck.de
[4] TH Lübeck, ILD, Mönkhofer Weg 239, 23552 Lübeck, Stefanie.Bock@th-luebeck.de

DOI: 10.18420/delfi2019-ws-110

Kann es eine digitale Hochschule ohne Blockchain geben?

Warum eine Blockchain Allianz für Digitale Zertifikate gebraucht wird

Andreas Wittke[5], Jan Rieger[6], Marc Vorreiter[7] und Stefanie Bock[8]

Abstract: Wir befinden uns spätestens seit der Erfindung des Smartphones in einer technologischen Gesellschaft. Jeder Lebensbereich wird durch die Digitalisierung beeinflusst, natürlich auch die Bildung und hier speziell die Bildungsnachweise wie z.B. Urkunden, Diplome oder Zertifikate. Letztere haben spezielle Anforderungen, was vor allem die Standardisierung aber auch die Fälschungssicherheit betrifft. Die neugegründete DigiCerts Allianz der TH Lübeck, RWTH Aachen, Kiron open higher education, g.a.s.t. e.V., iMooX zusammen mit dem Fraunhofer FIT hat einen Prototyp für digitale Zertifikate entwickelt. DigiCerts ist eine Allianz Gleichgesinnter, die sich das Ziel gesetzt haben, globale Zertifizierungsprozesse zu verändern. Diese Prozesse sollen digital, automatisiert und gleichzeitig unveränderbar sein, damit das Vertrauen der User, wie bspw. Hochschulen und Arbeitgeber, sichergestellt ist.

Keywords: Certificates, Open Badges, Blockchain, Quorum, Ethereum, Moodle, Plugin

Digitale Zertifikate auf dem Smartphone

Das Smartphone rückt in den Mittelpunkt des Menschen. Immer mehr Menschen nutzen es für Musik, Navigation, Kommunikation aber auch als Wallet für das bargeldlose Bezahlen oder wahrscheinlich auch zukünftig als Dokumentenmappe für Urkunden und Zeugnisse. Ob dies kommt, sollte nicht mehr diskutiert werden. Die Frage ist, wann es kommt und wer es anbietet.

Es gibt jedoch bestimmte Vorbedingungen, die erfüllt sein müssen, damit digitale Zeugnisse akzeptiert werden und auch funktionieren. Zum einen muss es eine digitale Infrastruktur geben, die zuverlässig und hochverfügbar ist. Außerdem muss die Technologie zuverlässig, transparent (vertrauensvoll) und unveränderbar sein. All diese Voraussetzungen erfüllt die Blockchain-Technologie und jeder, der die Blockchain nutzen will, muss sich an Standards bzw. ein gemeinsames einheitliches Schema halten.

[5] TH Lübeck, ILD, Mönkhofer Weg 239, 23552 Lübeck, Andreas.Wittke@th-luebeck.de
[6] TH Lübeck, ILD, Mönkhofer Weg 239, 23552 Lübeck, Jan.Rieger@th-luebeck.de
[7] TH Lübeck, ILD, Mönkhofer Weg 239, 23552 Lübeck, Marc.Vorreiter@th-luebeck.de
[8] TH Lübeck, ILD, Mönkhofer Weg 239, 23552 Lübeck, Stefanie.Bock@th-luebeck.de

1 Brauchen wir Blockchain-Zertifikate?

Brauchen Hochschulen Blockchain-Zertifikate? Diese Frage ist eine logische Konsequenz der Digitalisierung von Hochschulen. Digitale Zertifikate scheinen vor allem hinsichtlich der globalen Mobilität von Studierenden von Vorteil. Zertifikate sind heute schon oft „elektronisch", vielfach sowohl als PDF, Word oder als Bild-Datei erzeugt. Doch wie unterscheiden sie sich von einem eingescannten papierbasierten Zertifikat? Kaum ein Format ist wirklich fälschungssicher. Wenn es das ist, dann ist die Lösung proprietär und/oder die Standards sind nicht offen. Elektronische Formate sind meist nur dafür da, das Zertifikat auszudrucken – quasi als Übergangsformat für das analoge Primärformat, der Urkunde aus Papier. Eine maschinelle digitale Verarbeitung der Zertifikate inkl. der Metadaten ist meist nicht geplant. Gerade in der internationalen Mobilität wäre dies aber hilfreich, um Anrechnungsprozesse bspw. an Hochschulen zu vereinfachen und zu beschleunigen. Das digitale Zertifikat sollte standardisierte Metadaten in einem maschinenlesbaren XML-Format haben, damit der Austausch transparent und sicher ist und die Prozesse automatisierbar sind.

Das bisherige Zertifikat mit seinen definierten Inhalten, wie z.B. Vor- und Nachname, Institution, Leistung, Workload etc., ist nur ein Teilbereich der Informationen. Natürlich sollte man zukünftig auch über Anrechnungen und Anerkennung von Leistungsübersichten und Zeugnissen nachdenken und hier kommen dann internationale Austauschprogramme ins Spiel. Dafür benötigt man digitale Verwaltungssysteme, Austauschformate und Metadaten. Liegen also z.B. Lerninhalte, Modulhandbücher oder Kompetenzprofile auch als PDFs vor, so ist ein zukünftiger elektronischer Vergleich nur sehr aufwendig möglich.

Hier beginnt die „Digitalisierung der Hochschule", die offene Schnittstellen und Austauschformate für die Internationalisierung braucht, aber auch eine zukünftige Zusammenarbeit, z.B. mit den Personalabteilungen von Firmen oder eine Integration in Portale wie LinkedIn. Hier sollte in Prozessen gedacht werden, und der Austausch mit anderen Systemen steht im Vordergrund, statt wie früher die Sicherung und Verwaltung von lokalen Dateien im eigenen Intranet.

2 PDFs und DOCX sind keine Standards für digitalisierte Prozesse

Ein Grundproblem der bisherigen IT-Welt waren lokale Lösungen. Seien es lokale Dateien, oder lokale Lösungen von einzelnen Servern. Das Internet hat dies verändert. Durch den Austausch von Dateien musste jeder z.B. das gleiche Format nutzen. Als Dateiformate haben sich daher Word oder das PDF-Format durchgesetzt. Jedoch lassen diese zu viel Freiraum für die maschinelle automatisierte Verarbeitung. Man kann zwar eine Überschrift definieren, aber, wie schon erwähnt, keine Metainformation mitgeben, also z.B. welcher Kontext die Überschrift hat. Dies ändert sich durch das XML-Format. Bei Open Badges werden z.B. alle Daten in einem JSON Format abgelegt, die vom IMS

Konsortium festgelegt werden[9]. Erst die Arbeit in JSON lässt eine strukturierte Prozessverarbeitung zu, und hier sollte man weiterdenken.

Das sind jedoch bekannte Datenverarbeitungsprozesse. Was neu ist, ist die Verbindung mit einer Blockchain. Die Blockchain liegt verteilt im Netz und kann als Peer-to-Peer Datenbank gesehen werden, die nicht veränderbar und hochverfügbar ist. Umso mehr Teilnehmende die einzelnen Knoten hosten, umso sicherer ist die Blockchain. Sie ist ein Layer, die verschiedene Knoten im Netz verbindet. Jeder muss mit seinem System eine eigene Verbindung herstellen, wobei der Aufwand überschaubar sein sollte. Wurde dies jedoch einmal entwickelt, erhält man eine hohe Flexibilität, eine Datenhoheit und ein sehr sicheres System, das weltweit funktioniert.

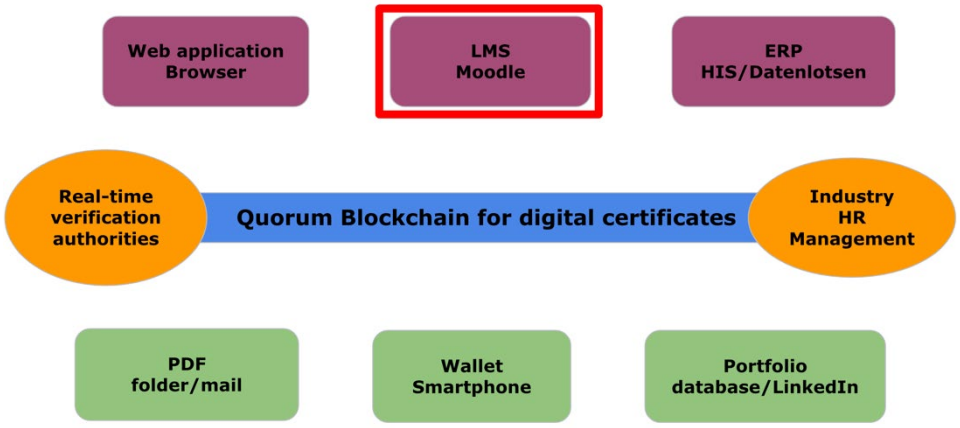

Abbildung 1: Schaubild DigiCerts Allianz

In der oberen Zeile der Abbildung 1 sieht man die verschiedenen Möglichkeiten, um Zertifikate in die Blockchain zu schreiben. Das Web Application Interface ist schon länger im Betrieb und ist z.B. ideal, wenn man per Excel-Tabellen die Zertifikate verwalten will. Es bietet einen manuellen Upload einzelner Zertifikate. Die TH Lübeck entwickelt im Rahmen des BMBF-geförderten Verbundprojekts IMPactDigital[10] eine Moodle-Schnittstelle. Damit wäre ein teilautomatisierter Upload in die Blockchain möglich, der jedoch sehr fein konfigurierbar ist.

Hier müssen aber die Anwendungsfälle genau analysiert werden. Eine Hochschule wird nur in wenigen Fällen die Zertifikate im Learning Management System verwalten wollen. Das ist meist die Aufgabe eines Hochschulverwaltungssystems wie z.B. HIS, Datenlotsen oder Graz Online. Jedoch könnten Schulen, Weiterbildungsanbieter oder

[9] Open Badge Standard V2.0 aufgrufen am 15.07.2019 https://www.imsglobal.org/sites/default/files/Badges/OBv2p0Final/index.html#badge-verification

[10] IMPactDigital Teilvorhaben der TH Lübeck aufgrufen am 15.07.2019 https://www.oncampus.de/pluginfile.php/132313/mod_resource/content/1/TH-L%C3%BCbeck_Blockchain_Architektur20190318.pdf

Volkshochschulen durchaus Bedarf an einer solchen Lösung haben, allein deshalb, weil sie häufig über kein anderes Verwaltungssystem verfügen.

3 DigiCerts Allianz

Die DigiCerts Allianz[11] ist ein bisher informeller Zusammenschluss mehrerer Institutionen mit einem gemeinsamen Ziel:

„Unsere Vision ist daher die Schaffung von innovativen Zertifizierungsprozessen, die den Anforderungen einer digitalen Gesellschaft an Bildungsangebote gerecht werden und global nutzbar sind. Wir wollen akademische und berufliche Mobilität unterstützen, indem wir Zertifizierungsprozesse digital abbilden und internationale Standards schaffen, die der akademischen und modernen beruflichen Realität gerecht werden."

Die Allianz soll den Anwendenden Vertrauen geben, dass die technische Lösung eine breite Unterstützung hat, eine hohe fachliche Kompetenz dahintersteht und das DigiCerts nachhaltig ist. Bei der Nutzung der Blockchain Technologie ist Vertrauen, Akzeptanz und Verbreitung wichtig. Je mehr Partner die Knoten der Blockchain betreiben, umso sicherer sind die Daten in der Blockchain[12]. Ein großer Kritikpunkt an der Blockchain ist oft, dass das Problem auch meist mit einer einzelnen Datenbank lösbar wäre. Wo es jedoch um Austausch und die Verwaltung von Informationen geht, was bei internationalen Studienabschlüssen der Fall ist, werden neue innovative technische Lösungen benötigt. Würde ein zentraler Server in Europa für alle Zeugnisse installiert werden, müssten unzählige VPN-Tunnel zu tausenden Hochschulen eingerichtet werden. Bei der Blockchain bleibt die Implementierung jedoch hoheitlich in den Händen der einzelnen Institutionen. Nur das Austauschformat muss vereinheitlicht werden. Dies bedeutet eine viel höhere Flexibilität für jede Hochschule, aber auch eine lokale Verwaltung der Daten ist nach Datenschutzvorgaben möglich. Zusätzlich erhalten auch externe Anwender, z.B. Partnerhochschulen aus Asien, ganz einfach Zugriff, um Zertifikate sekundenschnell zu überprüfen.

Die DigiCerts Allianz wird sich jedoch weiterentwickeln müssen. Es warten zukünftig viele Aufgaben auf uns, die das Netzwerk betreffen. So muss u.a. beschlossen werden, welche Technologie eingesetzt und weiterentwickelt wird, es muss eine Finanzierung gefunden werden, die Zusammensetzung und die Aufgaben der Allianz selbst müssen beschrieben werden. Auch die Verteilung und der Betrieb der Knoten muss koordiniert werden und vor allem, wer eine Zertifizierungsstelle sein darf und damit Schreibrechte in der Blockchain hat. Die Blockchain selbst hat „nur" die Aufgabe sicherzustellen, dass die Daten auf den Zertifikaten korrekt sind, ohne Aussage über deren inhaltliche Qualität. Ob die Noten der Zertifikate wahr sind, kann nur über die Qualitätssicherungsmaßnahmen der

[11] DigiCerts Allianz Mitglieder aufgrufen am 15.07.2019 https://www.digicerts.de/?page_id=44
[12] Blockchain Smart Contracts Positionspapier aufgrufen am 15.07.2019 https://www.fraunhofer.de/content/dam/zv/de/forschung/artikel/2017/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts_v151.pdf

Zertifizierungsstellen erfolgen und dies wird sicherlich auch ein entscheidender Aspekt bei der Diskussion über die gesellschaftliche Bedeutung von Bildungsabschlüssen sein.

4 Quorum Blockchain für Communities ohne Energiebedarf

Die Nutzung von Blockchains sollte wohlüberlegt sein. Es gibt etliche Aspekte, die später zu Diskussionen führen oder eventuell eine komplette Überarbeitung der gesamten Entwicklung erfordern könnten. Eine Grundsatzentscheidung ist, ob eine öffentliche oder eine private bzw. Community Blockchain betrieben werden soll. Hierbei spielen die anfallenden Mining-/Transaktionskosten eine große Rolle. So kann z.B. die Entscheidung für eine Bitcoin Blockchain Transaktionskosten von bis zu 50 Dollar erzeugen[13], was bei einem größeren Weiterbildungsanbieter schnell zu sechsstelligen Summen führen kann. Außerdem kann es technisch erforderlich sein, dass man einen bestimmten Code auf der Blockchain ausführen muss, dafür braucht man dann sogenannte Smart Contracts[14]. Bei DigiCerts wurden zwei Contracts entwickelt, damit Zertifizierungsstellen die Zertifizierungsaussteller berechtigen können, Zertifikate auszustellen und damit diese Zertifikate auch verwaltet werden können. Erst mit Smart Contracts sind bestimmte Rollenkonzepte auf der Blockchain möglich und damit wird die Wahl der Blockchain-Technologie eingegrenzt auf z.B. Ethereum oder Quorum.

[13] Bitcoin Transaktionskosten aufgrufen am 15.07.2019 https://coin-hero.de/wie-sich-die-hoehe-von-bitcoin-transaktionskosten-bestimmt/

[14] Smart Contracts aufgrufen am 15.07.2019 https://www.coindesk.com/information/ethereum-smart-contracts-work

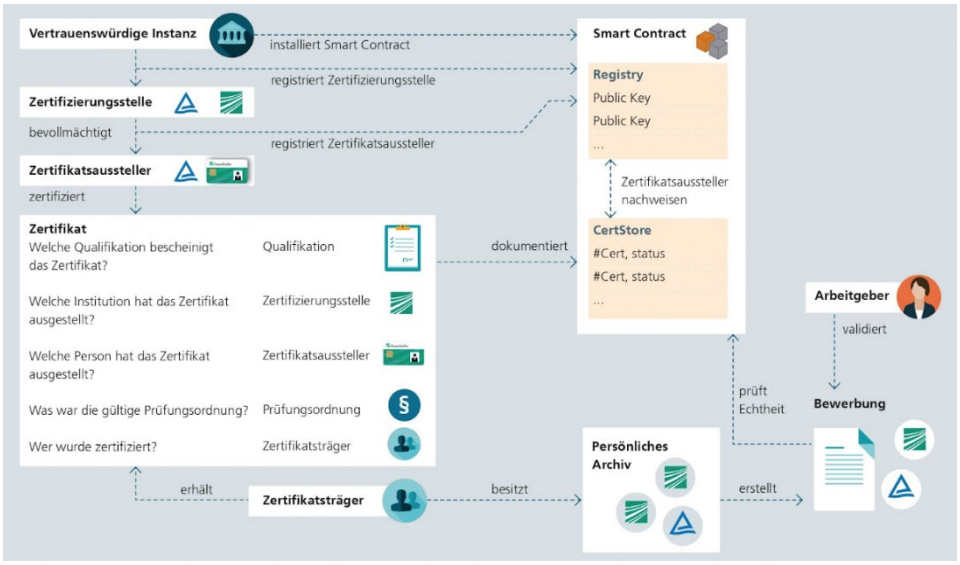

Abbildung 2 DigiCerts Funktionsweise (Quelle Fraunhofer[15])

Bei Quorum[16] fällt noch ein weiterer Kritikpunkt der Blockchain weg, nämlich der Energieverbrauch. Quorum ist eine Open Source Blockchain von JP Morgan und Microsoft, die auf einem Trust-Rollenkonzept basiert. Das bedeutet, dass jeder, der über bestimmte Rechte verfügt, ohne großen Energieaufwand bzw. Miningkosten Transaktionen durchführen kann und das auch relativ performant, ohne große Hardware.

Da die Blockchain als unveränderbar gilt, d.h. im Grunde ewig laufen könnte, ist bei der Implementierung auch der Nachhaltigkeitsaspekt der eingesetzten Software wichtig. Bei kommerzieller Software kann ein Lizenzmodell für „ewig“ mit einem Software-Unternehmen schnell Grenzen aufzeigen. Ideal sind hier Open Source Lösungen, die eine große Unabhängigkeit, Nachhaltigkeit und Flexibilität ermöglichen, jedoch das Problem der Aktualisierung und damit auch der Finanzierung nicht lösen.

Bei der Implementierung sollte auf bewährte Standards gesetzt werden. So nutzt DigiCerts den anerkannten Open Badge Standard, aber der sehr verbreitete Blockcerts Standard wird nicht unterstützt. An der TH Lübeck führte dies zu einer langen Design-Entscheidung, die zwei entscheidende Aspekte hatte. Zum einen unterstützte Blockcerts anfangs nur Bitcoin, was sich inzwischen geändert hat, zum anderen setzt Blockcerts einen Private Key beim Anwendenden voraus. Kryptografie ist heute immer noch eine komplexe Technologie, die sowohl eine hohe Medienkompetenz als auch eine Datensensibilität beim Anwender erfordert. Viele Nutzende sind jedoch mit der Bedeutung, der Nutzung wie auch der

[15] Grafik DigiCerts Funktionsweise aufgrufen am 15.07.2019 https://myotis.fit.fraunhofer.de/b4e/funktionsweise.html
[16] Quorum aufgrufen am 15.07.2019 https://www.goquorum.com/

Verwaltung von Private Keys überfordert. Die Schlüssel werden nicht sicher in einer Wallet oder einem Passwort Manager verwaltet und gehen ggf. verloren.

DigiCerts verzichtet auf die Versendung von Private Keys und verwaltet die Zertifikate über ein Rollenkonzept mittels Zertifizierungsstellen und Zertifizierungsaussteller. Diese sollen zukünftig über ein Gremium der DigiCerts Allianz vergeben und qualitätsgesichert verwaltet werden. Dies sind jedoch nur erste Pläne und sowohl die Allianz als auch das Gremium müssen sich noch formell gründen. Im Mittelpunkt der bisherigen Arbeiten stehen die Entwicklung und der Betrieb des Prototyps.

5 Moodle Plugin

Damit die DigiCerts Lösung eine große Verbreitung finden kann, wird Moodle, das führende Learning Management System Europas[17], als Nutzungsplattform genutzt. Die TH Lübeck entwickelt ein Plugin, das die Anbindung von Moodle an die Blockchain konfiguriert, die Private Keys verwaltet, die verschiedenen Rollen zuordnet und vor allem die Zertifikate erstellt und verwaltet. Das Plugin erzeugt eine Moodle Aktivität, die dann in jedem Kurs individuell nach Bedarf eingefügt werden kann. Jeder Moodle Betreiber selbst kann dann bestimmen, ob z.B. jeder Teacher Zertifikate in die Blockchain schreiben kann oder vielleicht nur jemand mit der Rolle „Zulassungsstelle“ dies darf. Außerdem muss jede Institution für sich entscheiden, wie das Zertifikat designed ist und welche Metadaten genutzt werden. Das Plugin muss dabei viele Freiheitsgrade haben, aber trotzdem die Komplexität des Prozesses vereinfachen, was viel Aufwand bei der Entwicklung der Usability erfordert.

Wenn die Zertifikate einmal in der Blockchain geschrieben sind, sind die Daten nicht mehr veränderbar. Das bedeutet, Schreibfehler sind nicht mehr korrigierbar. Aber auch die nachträgliche Aberkennung des Zertifikats, z.B. bei einem Betrugsversuch oder bei Plagiaten, muss berücksichtigt werden. Die DigiCerts Zertifikate haben daher Zeitstempel und Gültigkeitsflags mittels Smart Contracts, die diese Nutzungsszenarien berücksichtigen, und deren Einsatz wird wieder über die Rollen definiert.

Der gesamte Prozess kann auch automatisiert werden, so dass kein Mensch mehr den Schreibprozess des Zertifikats in die Blockchain anstoßen muss. Das ist vor allem für Selbstlernkurse mit Badges sinnvoll, wo es kleine Lernfortschritte gibt, und in denen mit automatisierten Tests Teilzertifikate vergeben werden. Hier wäre eine menschliche Qualitätssicherung meist zu aufwendig, daher könnte eine Schnittstelle dies automatisiert erledigen.

[17] LMS Market Share Europe aufgrufen am 15.07.2019 http://eliterate.us/wp-content/uploads/2017/10/European_LMS_Market_Dynamics_Fall_2016_Early_Access.pdf

6 Ausblick

Digitale Zertifikate und damit auch die Anerkennung und der Austausch von Studienleistungen sind immer ein Netzwerkproblem. Keine einzelne Institution, Behörde und auch kein Land kann das für sich alleine lösen. Daher braucht es Allianzen, die offen und vertrauensvoll arbeiten. DigiCerts ist ein guter Anfang, aber es bleibt noch sehr viel Arbeit.

Das DigiCerts Projekt zeigt schon heute die Komplexität der digitalen Zertifikate. Zum einen ist die Technologie hinter der Zertifizierung sehr komplex. Die Blockchain bietet sich für die Verwaltung von Zertifikaten an, jedoch sind viele Entscheidungen und Entwicklungen zu berücksichtigen.

Auf der anderen Seite sind die internen Verwaltungsprozesse für die Vergabe und Verwaltung von Zertifikaten in jeder teilnehmenden Institution zu digitalisieren und damit neu zu entwickeln. Hierzu müssen interne Strukturen verändert und es muss national und international kooperiert werden. Zertifikate sind nicht für den internen Gebrauch gedacht, sondern müssen weltweit lesbar und überprüfbar sein.

Dabei sind Zertifikate nur ein Aspekt, denn schnell ist das Potential dieser Lösung erkennbar. So sind sicherlich zukünftig auch andere Szenarien möglich, z.B. Führerscheine, Impfbücher, Organspende Ausweise, aber auch Sicherheitsschulungen, Zutrittskontrollsysteme und natürlich das Identity Management. Das zukünftige Bürgerkonto wird diese Daten vielleicht vereinen und evtl. auch mit einer Blockchain arbeiten. Es wird unser Leben verändern, sowohl positiv als auch negativ.

Blockchains legen das Fundament für zukünftige Kooperationen und schaffen so ein Netzwerk der Zusammenarbeit und des Austauschs und zeigen Lösungen, für Probleme, die eine einzelne Hochschule meist gar nicht sieht. Der Austausch von digitalen Zertifikaten ist nur ein Aspekt der digitalen globalisierten Bildung, es werden noch viele weitere folgen.