www.jusletter-it.eu

Raphaël Schwab

Blockchain als Lösung für eine effektive und fälschungssichere Speicherung von Diplomen

Der technologische Fortschritt und insbesondere die Blockchain-Technologie bringt unzählige neue Anwendungsmöglichkeiten mit sich. Die vorliegende Arbeit beschäftigt sich mit der rechtlichen Auseinandersetzung einer Blockchain-basierten Lösung zur Sicherung, Nutzung und Überprüfung von Hochschulzertifikaten. Dabei wurden insbesondere datenschutzrechtliche Aspekte, die Umsetzung und die Vereinbarkeit mit den heutigen Universitätsgesetzen untersucht.

Beitragsart: Next Generation
Region: Schweiz; EU
Rechtsgebiete: LegalTech

Zitiervorschlag: Raphaël Schwab, Blockchain als Lösung für eine effektive und fälschungssichere Speicherung von Diplomen, in: Jusletter IT 30. September 2021

Inhaltsübersicht

1. Einleitung

[1] In einem wettbewerbsintensiven Markt wie dem Arbeitsmarkt hat das Diplom einer Hochschule eine äusserst relevante Bedeutung.[1] Alleine in der Schweiz wurden im Jahr 2019 über 14'000 Eidgenössische Fachausweise, über 17'000 Bachelorabschlüsse von Fachhochschulen und mehr als 33'000 universitäre Abschlüsse erlangt.[2] Das Zertifikat wird als Zeichen einer Kompetenz angesehen, die das Bildungsniveau und die Fähigkeiten des Einzelnen bescheinigen.[3] Weiter bestätigen sie im Bildungsbereich das Erreichen bestimmter Lernergebnisse.[4]

[2] Gemäss einer Schätzung von Dr. George Brown im Rahmen einer UNESCO-Studie weisen weltweit 30 % aller leitenden Führungskräfte Qualifikationen aus, die sie nicht besitzen.[5] Alleine die Suche nach «fake Diploma» über Google generiert mehr als 27 Millionen Suchergebnisse, wobei die meisten vorgeschlagenen Webseiten allesamt gefälschte Zertifikate gegen Entgelt anbieten. Weiter können die in PDF-Format verschickten Hochschuldiplome mit nur wenigen Klicks verändert und so Noten oder Namen des Absolventen[6] auf Wunsch angepasst werden.[7] Hier soll diese Arbeit anknüpfen und eine mögliche Blockchain-Lösung für die Verhinderung von Fälschungen rechtlich analysieren.

[3] Bei der dafür eingesetzten Methodik handelt es sich ausschliesslich um eine Recherche und Analyse bereits bestehender Literatur. Der Aufbau ist so gestaltet, dass zuerst die Problemstellung erläutert wird. Anschliessend findet eine vertiefte Auseinandersetzung mit der Blockchain als Lösung statt, diese dient als Grundlage für die darauffolgende rechtliche Würdigung. Abschliessend werden die Resultate zusammengetragen und eine Erweiterungsmöglichkeit der rechtlichen Würdigung aufgegriffen.

---

1 Gresch et al., S. 1.

2 Bundesamt für Statistik, Ausgewählte Bildungsabschlüsse.

3 Gresch et al., S. 1.

4 Gräther et al., Introduction.

5 Ott, Mit Blockchain gegen Diplomfälschung.

6 Zugunsten der Leserlichkeit wird in dieser Arbeit ausschliesslich das generische Maskulinum verwendet, unter welchem alle Geschlechter inkludiert sind.

7 Ott, Mit Blockchain gegen Diplomfälschung.

2. Problemstellung

[4] Gegenwärtig wird die Mehrheit der Diplome in einem papierbasierten Format ausgestellt.[8] Die Papierzertifikate gelten in vielen Kreisen immer noch als die sicherste und einfachste Form der Zertifizierung.[9] Dies aufgrund der in den Zertifikaten selbst eingebauten und schwer zu fälschenden Sicherheitsmerkmalen und den relativ unkomplizierten Aufbewahrungsmöglichkeiten. Allerdings haben sie auch erhebliche Nachteile. So bleibt stets ein Restrisiko, da in der Realität nicht das Originalzertifikat geteilt wird, sondern eine Kopie oder ein Scan, auf welchem die Sicherheitsmerkmale nicht erkennbar sind und demnach einfach zu fälschen sind. Diese Fälschungen können die Glaubwürdigkeit der Institutionen erheblich schädigen.[10] Zusätzlich führt dies zur Pflicht des Ausstellers, ein zentrales Register zu führen, um die Überprüfung auf Echtheit zu ermöglichen. Dieses zentrale Register ist ein «single point of failure»; während die Gültigkeit des Zertifikates bestehen bleibt, kann durch den Untergang des Ausstellers die Fähigkeit zur Verifizierung untergehen.[11] Der Untergang ist bei staatlich geführten Bildungsinstitutionen unwahrscheinlich, bei privaten Weiterbildungsveranstaltern aber durchaus denkbar. Weiter ist die Führung und die Beantwortung von Gültigkeitsanfragen Dritter mit einem zentralen Register ein zeitaufwändiger Prozess, der erhebliche personelle Ressourcen erfordert.[12] So dauert es unter heutigen Bedingungen meist mehrere Tage, bis eine Verifizierung abgeschlossen ist.[13] Zuletzt ist die Widerrufbarkeit des Diploms bei der Aushändigung in Papierformat erschwert. Der Eigentümer muss für eine vollständige Rücknahme die Verfügungsmacht über das Zertifikat aufgeben.[14]

[5] Es gilt zu beachten, dass es kein perfektes Format für Zertifikate gibt.[15] Die erheblichen Einschränkungen des jetzigen Systems zeigen jedoch deutlich die Notwendigkeit einer besseren, robusteren Zertifizierungstechnologie auf.[16] Insbesondere der Realitätscheck zeigt, dass ein Zertifikat von der entsprechenden Institution in Papierform ausgestellt wird und der Empfänger dieses der Einfachheit halber einscannt oder kopiert und einzig die Kopie ohne Sicherheitsmerkmale mit Dritten geteilt wird.

3. Digitale Zertifikate mittels Blockchain

[6] Die Blockchain-Technologie eignet sich ideal als neue Infrastruktur zur Sicherung, gemeinsamer Nutzung und Überprüfung von Lernleistungen.[17] Zu dieser Erkenntnis kamen auch die unterschiedlichsten Bildungsstätten auf der Welt. So entwickelten im Ausland die Universität Nikosia auf Zypern oder das Massachusetts-Institut für Technologie (MIT) aus den Vereinigten

8 Gresch et al., S. 2.

9 Grech/Camilleri, S. 30.

10 Ott, Mit Blockchain gegen Diplomfälschung.

11 Grech/Camilleri, S. 30.

12 Grech/Camilleri, S. 30.

13 Rau, Universität von St. Gallen bekämpft Fälschungen mithilfe der Blockchain.

14 Grech/Camilleri, S. 30.

15 Grech/Camilleri, S. 30.

16 Grech/Camilleri, S. 30.

17 Smolenski, S. 45.

Staaten schon früh erste taugliche Anwendungen.[18] Auch in der Schweiz werden unterschiedliche Projekte der Blockchain-basierten Speicher- und Verifizierungsmethoden geprüft. Dies unter anderem in Zusammenarbeit mit den Schweizer Unternehmen BlockFactory, Certification oder Switch an den Universitäten Basel und St. Gallen.[19] Ein ähnlicher Ansatz verfolgt auch Weblaw Memory. Der Dienst von Weblaw ermöglicht es, Dokumente in einer Blockchain abzuspeichern und deren Authentizität zu jedem Zeitpunkt mit wenigen Klicks selbständig zu überprüfen.[20]

3.1. Funktionsweise der Blockchain-Zertifikate

[7] Obwohl die verschiedenen Projekte teils unterschiedlich funktionieren oder auf einer unterschiedlichen Blockchain laufen, haben sie alle einige Gemeinsamkeiten. Die Nutzung der Blockchain ermöglicht eine dezentrale Speicherung der Daten und eliminiert so den «single point of failure». Ein solch verteiltes, dezentrales Netzwerk fällt nur dann aus, wenn jeder einzelne Teilnehmer ausfällt, so dass es praktisch immer verfügbar ist.[21] Dies wird erreicht, indem mehrere Teilnehmer eine Kopie des gesamten Registers (sogenannter «Ledger») halten. Das Schreiben oder Ändern des «Ledgers» erfordert somit den Konsens aller Teilnehmer, die eine Kopie davon halten. Dadurch wird eine Fälschung, namentlich die nachträgliche Manipulation des Zertifikates in einem Block, verunmöglicht.[22] Weiter bedarf es durch die dezentrale Speicherung keine zwischengeschaltete Partei mehr zur Verifizierung der Zertifikate.[23] Jeder, der Zugang zur Blockchain hat, kann eigenständig und zeitnah die Echtheit der Diplome kontrollieren. Damit ist die Validierung des Zertifikates auch dann noch möglich, wenn die Organisation, die es ausgestellt hat, selbst nicht mehr existiert.[24] Diese Möglichkeit bestärkt die Beständigkeit der Diplome. Zuletzt wird die Widerrufbarkeit der Zertifikate vereinfacht. Sie bedarf nicht mehr der Eigentumsübertragung des Diploms zurück an den Aussteller, sondern kann durch einen neuen Eintrag auf der Blockchain für ungültig erklärt werden.[25]

3.2. Inhalt der Blockchain

[8] Auf der Blockchain können beliebig unterschiedliche Informationen gespeichert werden.[26] Zertifikate beinhalten sensible Daten, wodurch die Speicherung der gesamten Informationen oft nicht wünschenswert ist.[27] Zum Schutz der Daten kommt daher eine doppelte Verschlüsselung zum Einsatz. Auf der Blockchain wird einzig ein zum Original-Zeugnis passend erzeugter «Fin-

18 Gräther et al., Related Work.

19 Rau, Universität von St. Gallen bekämpft Fälschungen mithilfe der Blockchain; Ott, Mit Blockchain gegen Diplomfälschung; Siehe weiterführend: https://cif.unibas.ch/de/events-projekte/zertifikate/; https://www.switch.ch/de/verify/; https://www.switch.ch/de/stories/why-University-StGallen-is-using-SWITCHverify/.

20 Siehe https://memory.weblaw.ch/memory.

21 Grech/Camilleri, S. 36.

22 Grech/Camilleri, S. 31.

23 Grech/Camilleri, S. 32.

24 Grech/Camilleri, S. 32.

25 Gräther et al., Discussion.

26 Rauschenbach/Stuck, S. 7.

27 Schmid, Mit Blockchain gefälschte Diplome entlarven.

gerabdruck» (sogenannter «Hashwert») abgelegt. Somit wird das Dokument selbst nicht auf der Blockchain hinterlegt und dessen Inhalt auch nicht veröffentlicht.[28] Wird das Original-Zeugnis nachträglich manipuliert, passt es nicht mehr zum hinterlegten Referenzwert. Gleiches gilt, wenn kein echtes Zeugnis vorliegt.[29]

4. Rechtliche Würdigung

[9] Trotz namhafter Vorteile durch die Blockchain-basierte Lösung bedarf die Implementierung derer die Berücksichtigung des rechtlichen Rahmenwerkes. Die Tauglichkeit der Technologie ist nur bei rechtskonformer Verwendung, welche sich aus dem geltenden Recht ableiten lässt, gegeben.

[10] Die explizite Ausgestaltung der Blockchain-basierten Lösung als Speicherungsmedium von Zertifikaten ist entscheidend für die rechtliche Würdigung. Es sind hierbei verschiedene Ansätze denkbar. Diese Arbeit beschränkt sich auf die Anwendungsfälle eines ausschliesslich digitalen Zertifikates und einer Kombination aus physischem und digitalem Zertifikat. Weiter ist der Inhalt der zu speichernden Daten entscheidend. Oft dient die Blockchain nicht als Speicher für den Inhalt des ganzen Zertifikates, sondern einzig für dessen «Hashwert».[30]

4.1. Ausstellungskompetenz

[11] Die im Hochschulförderungs- und Koordinationsgesetz namentlich erwähnten universitären Hochschulen verleihen gemäss ihrem jeweiligen Universitätsgesetz akademische Grade sowie Diplome.[31] Die Kompetenz zur Verleihung der Diplome obliegt somit einzig der von der jeweiligen Universität zuständigen Organisationseinheit.[32] Um dieser Vorschrift gerecht zu werden, muss die Kompetenz zur Schreibberechtigung auf den Aussteller der Diplome beschränkt werden. Diese Kompetenzbeschränkung ist durch die Verwendung einer «permissioned Blockchain» möglich.[33] Somit wäre hinsichtlich der Kompetenzverteilung sowohl eine ausschliesslich digitale als auch eine Kombinationslösung des Zertifikates möglich.

4.2. Datenschutzrechtliche Aspekte

[12] Weiter ist die dauerhafte Speicherung der Daten in der Blockchain aus datenschutzrechtlichen Aspekten genauer zu betrachten. Es ist offensichtlich, dass die dauerhafte Speicherung mit dem Recht auf Vergessen, Einschränkungs- und Berichtigungspflichten aus dem Datenschutzgesetz kollidieren kann.[34] Wichtig zu verstehen ist, dass aber je nach Ausgestaltung der Speicherung

28 Grech/Camilleri, S. 34.

29 Schmid, Mit Blockchain gefälschte Diplome entlarven.

30 Grech/Camilleri, S. 34.

31 Vgl. Art. 4 UG; § 34 UniG; Art. 4 i.V.m. Art. 44 UniGe.

32 Siehe bspw. Art. 3 FakR WISO.

33 Möri, Rz. 29.

34 Kunde et al., S. 20.

keine Personendaten auf der Blockchain selbst gespeichert werden. Gerade bei der Umsetzung der beiden Universitäten Basel und St. Gallen wird der Inhalt der Zertifikate einzig als «Hash» auf der Blockchain abgelegt.[35] Der «Hashwert» ist mit einem Fingerabdruck vergleichbar, der den ursprünglichen Inhalt charakterisiert.[36] Aus dem «Hashwert» alleine kann nicht direkt auf den Inhalt des darunterliegenden Zertifikates geschlossen werden. Die Speicherung des «Hashwertes» erlaubt eine private, vertrauliche und datenschutzkonforme Verarbeitung, da persönliche Daten wie bspw. einzelne Noten nicht geteilt werden.[37] Somit wären bei der gegebenen Ausgestaltung beide Anwendungsfälle mit den Datenschutzbestimmungen vereinbar.

4.3. Formerfordernis der Zertifikate

[13] Zuletzt muss eine ausschliesslich digitale Vergabe näher betrachtet werden. Bei der Vergabe einer Kombination wird die heute verbreitete Papierurkunde nicht ersetzt. Vielmehr wird das elektronisch verifizierbare PDF-Dokument als mehrwertstiftender Zusatz eingesetzt. Somit bedarf die Kombinationslösung einzig die Berücksichtigung der bereits behandelten datenschutzrechtlichen Aspekte. Nicht so bei der ausschliesslich digitalen Vergabe. Diese muss gerade bei staatlichen Bildungsstätten mit den jeweiligen Universitätsgesetzen vereinbar sein. Die verschiedenen Bestimmungen der jeweiligen Universität geben keine explizite Auskunft über das Format der Zertifikate.[38] Durch eine grammatikalische Auslegung der Gesetzesnormen ergeben sich einzelne Indizien, die für ein Zertifikat in Papierform sprechen. So steht bspw. in Art. 38 des Studienreglements der ETH Zürich, dass Absolventen, die den Studiengang erfolgreich absolvieren, drei Dokumente erhalten.[39] Namentlich sind dies ein Zeugnis, eine Urkunde und ein Diplom Supplement.[40] Weiter erteilt nach Art. 39 Abs. 4 des Studienreglements der ETH Zürich das zuständige Departement den Auftrag für den Druck des Zeugnisses. Auch die Ordnung und die Wegleitung der Universität Basel enthalten Indizien, die für ein Zertifikat in Papierform sprechen. Wer demnach an der Universität Basel das Bachelorstudium erfolgreich abgeschlossen hat, erhält an der Promotionsfeier nebst dem Zeugnis auch eine Promotionsurkunde.[41]

[14] Nach der herrschenden Lehre kann an Daten *de lege lata* kein dingliches Recht bestehen.[42] Dies ergibt sich vor allem aus dem fehlenden Element der Körperlichkeit, welche für das Sachenrecht zentral ist.[43] So können ausschliesslich digitale Zertifikate auch nie – im wahren Sinne des Wortes – ausgehändigt werden.[44] Somit ist der tatsächliche Erhalt der Dokumente, wie er bspw. in Art. 38 des Studienreglements der ETH Zürich oder in Art. 19 der Wegleitung der Universität Basel vorgesehen ist, in einer ausschliesslich Blockchain-basierten Lösung unmöglich.

35 Rau, Universität von St. Gallen bekämpft Fälschungen mithilfe der Blockchain.

36 Möri, Rz. 41.

37 Möri, Rz. 42.

38 Siehe bspw. Art. 4 UniGe; Art. 38 Studienreglement ETH.

39 Siehe auch Art. 25 RSL WISO; § 37 Studienordnung Unibas; § 15 Studienordnung Unilu.

40 Art. 38 Studienreglement ETH.

41 § 37 Studienordnung Unibas i.V.m. Art. 19 Wegleitung zur Ordnung für das Bachelorstudium an der Juristischen Fakultät der Universität Basel.

42 Bericht des Bundesrates, S. 48.

43 Bericht des Bundesrates, S. 47.

44 Bericht des Bundesrates, S. 48.

Ohne Anpassung wäre ein ausschliesslich digitales Zertifikat nicht mit den oben genannten Bestimmungen vereinbar. Beispielhaft hervorzuheben ist in diesem Zusammenhang die Universität St. Gallen, welche mit Art. 104 ihrer Ausführungsbestimmungen zu den Prüfungsordnungen für die Bachelor- und Masterstufe bereits eine Grundlage geschaffen hat, um eine digitale Lösung anbieten zu können.

[15] Private Weiterbildungsveranstalter haben den Vorteil, dass sie keinen staatlichen Bildungsaufträgen unterstehen und daher nicht an bspw. Universitätsgesetze gebunden sind. Dies ermöglicht eine ausschliesslich digitale Form der Diplome bei privaten Weiterbildungsveranstaltern, insofern sie die datenschutzrechtlichen Bestimmungen einhalten.

5. Fazit

[16] Zusammenfassend kann festgehalten werden, dass heute aufgrund der Vielzahl an sowohl legitimen wie auch widerrechtlich erworbenen Diplomen ein Handlungsbedarf für eine sichere und einfache Ausstellungs-, Speicherungs- und Verifizierungslösung besteht. Wie aufgezeigt wurde, eignet sich die Blockchain als optimale Lösung, um die Nachteile, die sich aus der konventionellen Diplomvergabe ergeben, einfach und effektiv zu eliminieren.

[17] Dabei ist die Implementierung einer Kombinationslösung aus Blockchain-Speicherung und physischer Urkunde durchaus mit den gegebenen Rechtsbestimmungen vereinbar. Auch eine ausschliesslich digitale Lösung ist bei der Anpassung des bestehenden Regelwerks denkbar. Letzteres wäre bspw. bei privaten Weiterbildungsveranstaltern, die keinen Hochschulgesetzen oder Ähnlichem unterliegen, bereits heute möglich. Dies vor allem dann, wenn durch die korrekte Ausgestaltung der Lösung die Bestimmungen des Datenschutzgesetzes eingehalten werden. Zu beachten ist, dass eine physische Urkunde auch einen symbolischen Wert besitzt, der bei einer ausschliesslich digitalen Lösung vernachlässigt wird.

[18] Die Methodenwahl und der Rahmen dieser Arbeit ermöglichten einen Überblick über den Einsatz der Blockchain als Lösung für eine effektive und fälschungssichere Speicherung von Diplomen. Diese Arbeit ist aber insofern limitiert, da sie sich auf eine gezielte Auswahl an rechtlichen Hürden beschränkt und diese keineswegs abschliessend sind. Es bleibt hervorzuheben, dass die explizite Implementierung immer einer Einzelfallbeurteilung bedarf. Auch müssten in einem umfangreicheren Rahmen einzelne Zertifikatsinhalte wie bspw. die Signatur und das Siegel der Bildungsinstitution auf ihren digitalen Einsatz und dessen Gültigkeit rechtlich überprüft werden.

Raphaël Schwab, Student der Rechtswissenschaft mit Wirtschaftswissenschaften (BLE) an der Universität St. Gallen (HSG).