BLOCKCHAIN-BASIERTE ATTESTIERUNG VON IDENTITÄTEN UND DOKUMENTEN

Felix Härer / Hans-Georg Fill

Felix Härer, Oberassistent, Universität Fribourg, Gruppe für Digitalisierung und Informationssysteme
Bd. de Pérolles 90, 1700 Fribourg, CH
felix.haerer@unifr.ch, https://www.unifr.ch/inf/digits/

Hans-Georg Fill, Ordentlicher Professor, Universität Fribourg, Gruppe für Digitalisierung und Informationssysteme
Bd. de Pérolles 90, 1700 Fribourg, CH
hans-georg.fill@unifr.ch, https://www.unifr.ch/inf/digits/

Schlagworte: ***Blockchain, Notar, Attestierung, Identität, Smart Contract***

Abstract: *Eine zunehmend diskutierte Anwendung von Blockchains ist die Attestierung von Identitäten und Dokumenten. Die Verteilung entsprechender Daten und deren manipulationssichere Speicherung eröffnet die Möglichkeit, die Überprüfung einmalig erhobener Identitäten sowie Dokumente Dritten zugänglich zu machen. Dieser Beitrag greift dieses Konzept der Blockchain-basierten Attestierung auf und zeigt eine mögliche Entwicklung hin zur Einbeziehung von Notaren. Ausgehend von einer Einführung zur Blockchain-basierten Attestierung diskutiert der Beitrag Beispiele des aktuellen technischen Standes sowie Szenarien einer von Notaren ausgehenden Identifikation und Beglaubigung von Identitäten und Dokumenten. Der Beitrag arbeitet hiermit komplementäre Einsatzmöglichkeiten heraus und relativiert die technisch geprägte Position einer möglichst weitreichenden Anwendung der Technologie.*

1. Einführung

Digitale Identitäten besitzen im Transformationsprozess der gesellschaftlichen und wirtschaftlichen Digitalisierung eine wesentliche Bedeutung. Sie sind einerseits eine Repräsentation natürlicher Personen sowie elementare Bezugspunkte von all denjenigen Interaktionen über digitale Kommunikationskanäle, die eine eindeutige Zuordnung von Identitäten zu natürlichen Personen erfordern. Die von diesem Thema berührten Anwendungen sind universell und betreffen beispielsweise über das Internet getätigte Finanztransaktionen sowie das Signieren von Dokumenten und das Abschließen digital vorliegender Verträge. Die hiermit einhergehende Identifikation über Webseiten und Webdienste wird derzeit im Kontext von Anmelde- und Authentifikationsverfahren wie FIDO2 diskutiert (FIDO Alliance, 2018), die Passwörter durch in Hardware-Modulen gespeicherte private Schlüssel ersetzen, sowie in Verbindung mit eID im Rahmen der eIDAS-Verordnung (Konzelmann, 2017) und daraus hervorgehenden Funktionen wie dem Identitätsmanagement (Piswanger et al., 2018). Bezogen auf die Hinterlegung von Identitäten werden zudem Blockchain-basierte Verfahren auf ihren Einsatz hin untersucht (Steinbrück, 2019). Hinzu kommen Blockchain-basierte Attestierungsverfahren, die insbesondere die Ablage von Dokumenteninformationen in einer Blockchain vorsehen, um die Existenz von Dokumenten sowie ggf. deren Urheber zu einem späteren Zeitpunkt durch Dritte nachzuweisen, c.f. (Härer und Fill, 2019b). Die Verbindlichkeit der Zuordnung von Identitäten und Dokumenten zu ihren digitalen Repräsentationen ist dabei eine wesentliche Herausforderung, die von entsprechenden Verfahren bislang nicht ausreichend betrachtet wird. Der vorliegende Beitrag diskutiert daher Beispiele bestehender Verfahren und mögliche Szenarien unter Einbeziehung von Notaren, wodurch eine höhere rechtliche und informationstechnische Sicherheit erwartet wird.

2. Grundlagen

Blockchain-Technologien erlauben eine global verteilte und konsistente Speicherung von Daten, die stets verbindlich auf Adresskennungen einzelner Benutzer zurückführbar sind. Der nachfolgende Abschnitt geht auf die Grundlagen von Blockchains ein, bespricht die pseudonyme Identifikation anhand von Adressen und beschreibt die wesentlichen Eigenschaften von Attestierungen.

2.1. Blockchains und pseudonyme Identitätskennungen

Eine Blockchain ist eine Datenstruktur, die aus rückwärts miteinander verketteten Blöcken durch einen Konsensalgorithmus konstruiert wird (Fill und Meier, 2020). Dieses iterativ ausgeführte Verfahren validiert die Datenstruktur hinsichtlich ihrer Konsistenz und stellt eine unveränderliche Speicherung sowie ein identisches Vorliegen der Daten bei allen verteilten Beteiligten sicher. Dabei akzeptiert das System ausschließlich Daten in Form von Transaktionen, welche eine überprüfbare digitale Signatur des Absenders sowie eine Adresskennung besitzen, wobei die Adresse bei gängigen technischen Plattformen, wie z.B. Bitcoin oder Ethereum, lokal als pseudonyme Kennung generiert wird. Die häufige Anwendung des Transfers von digitalen Währungseinheiten und Tokens setzt weitere Angaben wie einen Betrag sowie eine Adresskennung eines Empfängers voraus. Unabhängig von digitalen Währungen sind auch beliebige in Blockchains abgelegte Daten stets mit einer sendenden Adresse verknüpft. Diese Daten können jederzeit aus der Blockchain abgerufen und nachvollzogen werden, cf. (Härer und Fill, 2019a). Eine Blockchain-basierte Attestierung baut auf dieser Infrastruktur zur Verwaltung von Identitäten anhand entsprechender Kennungen auf. Transaktionen dienen hier der Hinterlegung von Informationen über Dokumente.

2.2. Blockchain-basierte Attestierung

Eine Blockchain-basierte Attestierung belegt die Existenz eines digitalen Dokuments, oder beliebiger Daten, zu einem annähernd bestimmbaren Zeitpunkt. Die hierfür ursprünglich verwendete Datenstruktur stellt einen Vorgänger der Blockchain dar (Haber und Stornetta, 1990) und gewinnt seit dem Aufkommen öffentlich verfügbarer Blockchains an Bedeutung c.f. (Swan, 2015), (Härer und Fill, 2019b).

Das in Abbildung 1 dargestellte Vorgehen beschreibt die Attestierung in mehreren Schritten: die Berechnung und Hinterlegung eines Prüfwertes in der Blockchain, zusammen mit einem Zeitstempel des Blocks, sowie die Validierung des Wertes durch einen Dritten zu einem späteren Zeitpunkt. Zunächst erfolgt (1) die Berechnung durch Anwendung einer Hash-Funktion auf das Dokument und (2) das Speichern des Hash-Wertes in einer signierten Transaktion, die in einen Block mit weiteren Metadaten wie einem Zeitstempel eingeht. Der Konsensalgorithmus führt an dieser Stelle eine Validierung der Signatur und des Zeitstempels durch.

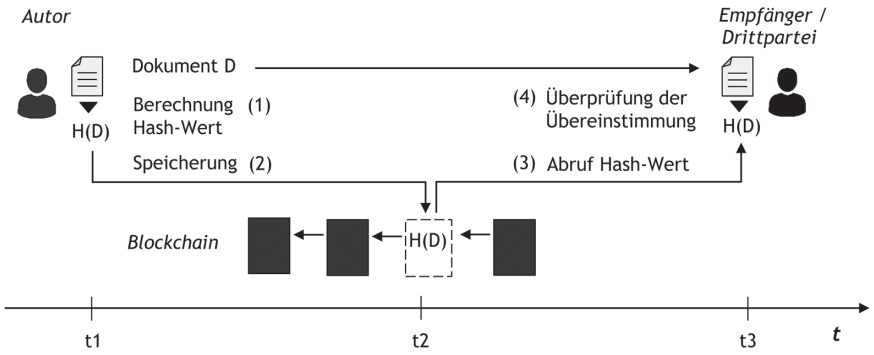

Abbildung 1: Prinzip der Blockchain-basierten Attestierung von Dokumenten

Um eine vorhergehende Existenz des Dokuments zu überprüfen, erfolgt (3) ein Abruf des gespeicherten Hash-Wertes und die (4) die Überprüfung der Übereinstimmung mit einem erneut aus dem Dokument berechneten Hash-Wert. Aufgrund der Eigenschaften von Hash-Funktionen, c.f. (Fill und Meier, 2020), belegt das Auffinden eines übereinstimmenden Hash-Wertes die Existent des Dokuments zum Zeitpunkt t2. Kommt das Verfahren in dieser Form in der Bitcoin-Blockchain zur Anwendung, besteht für den aus den Metadaten eines Blocks ermittelten Zeitstempel eine Genauigkeit in der Größenordnung von Stunden (Bitcoin, 2019). Ansätze zur Attestierung unter Einbeziehung weiterer Metadaten und Datenstrukturen in Smart Contracts existieren u.a. für die Ethereum-Blockchain (Antonopoulos und Wood, 2019).

3. State of the Art – Nutzung von Attestation-Services am Beispiel von OpenTimestamps.org

Die Attestierung von Dokumenten kommt heute nach dem beschriebenen Verfahren in der Bitcoin- und der Ethereum-Blockchain zum Einsatz. Verschiedene Services kommerzieller und nicht-kommerzieller Dienstleister bieten hierfür Lösungen an.

Ein Beispiel verbreiteter Attestierungs-Services wie OpenTimestamps.org und Stampery.com zeigt die in der Praxis vorzufindende Anwendung des Verfahrens. Ein Dienst wie OpenTimestamps.org erlaubt die Vergabe von Zeitstempeln unter Nutzung eines standardisierten Formats, das die Hash-Werte mehrerer Dokumente aggregiert und in einem Block der Bitcoin-Blockchain hinterlegt. Ein Nutzer folgt dabei dem in Abbildung 2 gezeigten Schema. Die zur Verfügung stehende Software[1] speichert für eine gegebene Datei im Zuge der zuvor genannten Verfahrensschritte (1) und (2) einen Hash-Wert in der Bitcoin-Blockchain und erstellt eine Attestierungsdatei im Dateiformat OTS. Diese Datei umfasst den Hash-Wert des Dokuments sowie zur Überprüfung erforderliche Operationen, mit denen der Hash-Wert innerhalb eines Blocks unter Nutzung einer Baumstruktur aufgefunden werden kann. Eine Überprüfung der Attestierung durch Dritte wird durch die Weitergabe des Dokuments zusammen mit der OTS-Datei ermöglicht. Hierfür ruft die Software einen Block der Bitcoin-Blockchain ab (3) und rekonstruiert unter Anwendung des Hash-Wertes und der innerhalb der OTS-Datei abgelegten Operationen einen innerhalb des Blocks enthaltenen Hash-Wert (4). Diese Validierung belegt die Existenz des Dokuments zum Zeitpunkt der Attestierung, sofern der Wert aufgefunden wird.

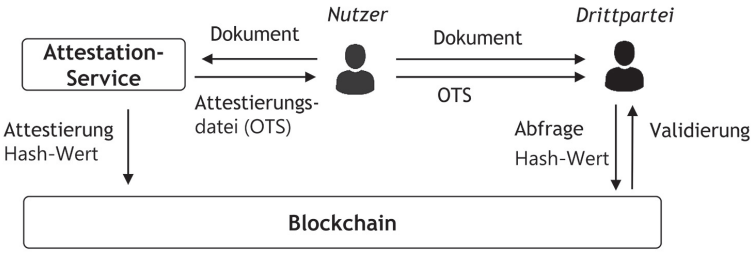

Abbildung 2: Attestierung unter Nutzung eines Attestation-Service

Die Services verschiedener Anbieter unterscheiden sich in der Praxis geringfügig in der von ihnen unterstützten Integration mit weiteren Software-Produkten und Schnittstellen. Darüber hinaus verfolgen Anbieter wie Stampery.com die Einbindung von elektronischen Identitätsdokumenten. Für den estländischen «E-Residency»-Ausweis[2] kann die Attestierung und Überprüfung bereits an die Identität einer entsprechend identi-

[1] Opentimestamps, https://github.com/opentimestamps/opentimestamps-client/releases (Abruf am 16. Dezember 2019).
[2] Stampery, https://stampery.com/estonia (Abruf am 16. Dezember 2019).

fizierten Person gebunden werden. Die Limitationen heute verfügbarer Services zeigen sich im Hinblick auf Rechtsgeschäfte und die Rechtssicherheit. So sieht etwa die Beglaubigung eines Dokuments eine Begleitung des gesamten Verfahrens durch einen Notar vor, die über die rein technische Feststellung der Existenz eines Dokuments hinausgeht.

4. Mögliche Entwicklung – Szenarien unter Einbeziehung von Notaren

Eine aus technischer Sicht sichere und unveränderliche Speicherung bietet Chancen für die Digitalisierung von Prozessen in denjenigen Bereichen, die eine verbindliche Zuordnung von natürlichen Personen sowie verbindliche Dokumentensignaturen erfordern. Dabei sind die nunmehr bestehenden und umfassenden technischen Möglichkeiten ohne Berücksichtigung der beteiligten Personen und der zugrundeliegenden Prozesse nicht hinreichend. Die Einbindung von Notaren kann für die Attestierung von Identitäten und Dokumenten vor diesem Hintergrund ein etabliertes Vorgehen gewährleisten und Rechtssicherheit schaffen. Hierzu tragen die von Notaren ausgeübte Aufgaben wie etwa Rechtskontrolle und Aufklärung bei, die beispielsweise die Geschäftsfähigkeit betreffen und Beteiligte vor Übereilung und rechtlicher Benachteiligung schützen – siehe zu Details (Fill und Härer, 2020).

4.1. Szenario 1: Attestierung von anonymen Identitäten

Die Attestierung von Identitäten umfasst die Feststellung der Identität einer natürlichen Person sowie die Vergabe einer digitalen Identitätskennung, die beispielsweise für Rechtsgeschäfte im Internet einsetzbar ist. Eine Überprüfung der Attestierung zu einem späteren Zeitpunkt geht in diesem Fall von einem potenziell unbeteiligten Dritten in Form eines Internet-Dienstes aus. Das Prinzip des Szenarios besteht daher darin, eine verbindliche und von Notaren durchgeführte Identitätsfeststellung mit anonymen digitalen Identitätskennungen inkl. der dabei von Notaren zu prüfenden Eigenschaften in einer Blockchain zu verknüpfen, um die Informationssicherheit und Rechtssicherheit zu stärken. Abbildung 3 stellt das Szenario dar.

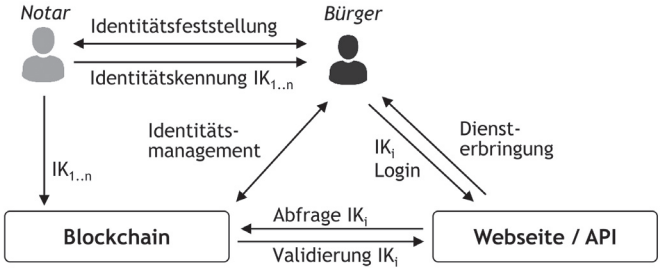

Abbildung 3: Attestierung von Identitäten

Eine zunächst erfolgende Identitätsfeststellung ist die Voraussetzung für die Generierung einer Menge von n anonymen Identitätskennungen $IK_{1..n}$ durch einen Notar. Dabei liegt die Kenntnis der Zuordnung aufseiten des Notars, so dass $IK_{1..n}$ zur Wahrung des Datenschutzes gegenüber Dritten keinen Rückschluss auf eine Identität zulässt und in einer öffentlichen Blockchain registriert werden kann. Die Registrierung greift auf die Blockchain durch einen Smart Contract zu, der per Bekanntmachung des Notars öffentlich abrufbar ist. Wird eine Identität IK_i für den Login und die Nutzung eines Dienstes bei einer Webseite oder einer Programmierschnittstelle (Application Programming Interface, API) angegeben, kann diese ohne weitere Abhängigkeiten überprüft werden. Kann durch eine Abfrage von IK_i eine entsprechende Kennung in der Blockchain aufgefunden werden, so ist diese analog zu dem zuvor beschriebenen Verfahren der Attestierung valide. Zur Dienst-

erbringung wird damit die Verbindlichkeit der Zuordnung zu einer natürlichen Person unabhängig von deren Offenlegung gewährleistet. Ein gesetzlich zu Neutralität und Verschwiegenheit verpflichteter Notar verwahrt die Zuordnung. Die beschriebene Herangehensweise bietet damit als Identifikations- und Login-Verfahren einen höheren Datenschutz, ist nicht von einer zentralisierten Public-Key-Infrastruktur zur Verwaltung von Schlüsseln abhängig und ermöglicht verbindliche Zuordnungen von digitalen Identitäten zu Personen. Das Prinzip ist um die Einbindung von eIDs erweiterbar, c.f. (Fill und Härer, 2020).

4.2. Szenario 2: Attestierung von Dokumenten

Die Blockchain-basierte Attestierung eines Dokuments entspricht einer Bestätigung der Existenz des Dokuments zu einem definierten Zeitpunkt. In Kombination mit dem zuvor beschriebenen Verfahren wird dieses Prinzip um die verbindliche Zuordnung einer Signatur des Dokuments unter Aufsicht eines Notars erweitert. Damit besteht die Möglichkeit, die Existenz analog vorliegender Dokumente, die Authentizität von Signaturen und die exakte Erstellungszeit digital und rechtssicher zu gewährleisten. Abbildung 4 zeigt das Szenario.

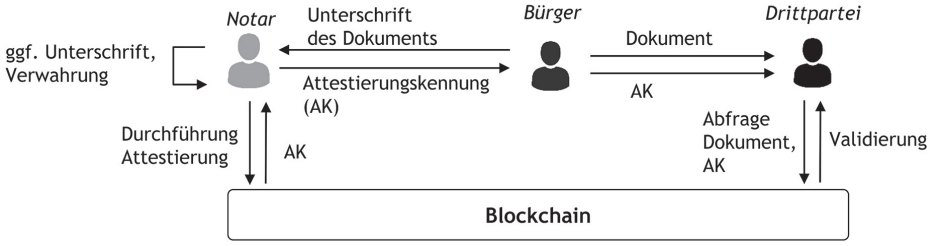

Abbildung 4: Attestierung von Dokumenten

Die Feststellung der Existenz sowie die Unterschrift des Dokuments erfolgen unter Aufsicht eines Notars. In Abhängigkeit des Dokuments kann zudem eine inhaltliche Überprüfung, eine Unterschrift durch den Notar, sowie ggf. eine anschließende Verwahrung des Dokuments vorgenommen werden. Die Durchführung der Blockchain-basierten Attestierung ist nachfolgend Aufgabe des Notars, der anhand des zuvor beschrieben Prinzips einen Hash-Wert des Dokuments erstellt und diesen zusammen mit einer eindeutigen Kennung AK in der Blockchain ablegt. Diese Werte werden per Smart Contract in der Blockchain gespeichert und lassen keinen Rückschluss auf den Inhalt eines Dokuments zu. Zur Überprüfung eines Dokuments durch Dritte muss lediglich der Ablageort in Form des Smart Contracts bekannt sein, der durch den Notar veröffentlicht wird. Eine dritte Person ist anschließend in der Lage, die Attestierungskennung eines Dokuments analog zum regulären Verfahren der Blockchain-Attestierung zu überprüfen. Zudem überprüfbar sind somit der Zeitpunkt der Attestierung und eine optional ebenfalls abgelegte Identitätskennung. Das Szenario zeigt die prinzipielle Möglichkeit einer weitergehenden rechtlichen und technischen Absicherung gegenüber Dokumentensignaturen. Dabei kann eine Vergabe von Zertifikaten zur Erstellung und Überprüfung von Signaturen durch eine zentrale Stelle wie die Bundesnotarkammer in Deutschland erfolgen, c.f. (Fill und Härer, 2020).

5. Ergebnisdiskussion

Die Digitalisierung von Prozessen in Wirtschaft und Verwaltung kann Stand heute auf etablierte technische Verfahren digitaler Signaturen in Verbindung mit eID sowie Attestierungsverfahren für Dokumente und deren Urheber zurückgreifen. Ausstehend ist dabei einerseits die Verknüpfung entsprechender Verfahren auf technischer Ebene, etwa um den Einsatz von eID-Signaturen mit Anmeldeverfahren wie FIDO2 und in der Blockchain attestierten Dokumenten zu verknüpfen, sowie auch die Sicherstellung der Verbindlichkeit einer Attes-

tierung über technische Aspekte hinaus. Im Diskurs um digitale Identitäten weisen die gezeigten Szenarien auf die Möglichkeit einer expliziten Einbindung von Notaren hin. Diese setzt an der Schnittstelle digitaler und analoger Artefakte an, die aufgrund der Notwendigkeit von Konsistenz stets mit Rechtsunsicherheit behaftet ist. In der Konsequenz ergibt sich eine höhere Rechtssicherheit hinsichtlich des Ablaufs der Attestierung und des Vorliegens involvierter Dokumente, sowie perspektivisch die Option zur weitergehenden Einbeziehung und Nutzung von Verfahren wie FIDO2 und eID-Signaturen.

6. Literatur

Antonopoulos, Andreas, Wood, Gavin, Mastering Ethereum, Second Edition, O'Reilly Media Inc., Sebastopol, California 2019, S. 222, 258.

Bitcoin, Bitcoin Entwicklerreferenzen. https://bitcoin.org/de/entwickler-referenzen#block-headers (Abruf am 16. Dezember 2019), 2019.

Fido Alliance, FIDO Authentication and the General Data Protection Regulation (GDPR). https://fidoalliance.org/wp-content/uploads/FIDO_Authentication_and_GDPR_White_Paper_May2018-1.pdf (Abruf am 16. Dezember 2019), 2018.

Fill, Hans-Georg, Härer, Felix, Usage Scenarios for Blockchain Technologies in the Domain of Civil Law Notaries, In: Hötzendorfer, Walter/Tschohl, Christof/Kummer, Franz (Hrsg.): International Trends of Legal Informatics, Festschrift für Erich Schweighofer, Editions Weblaw, Bern 2020.

Fill, Hans-Georg, Meier, Andreas, Blockchain kompakt. Grundlagen, Anwendungsoptionen und kritische Bewertung. Springer Vieweg, Wiesbaden 2020.

Haber, Stuart, Stornetta, Scott W., How to Time-Stamp a Digital Document. In: Menezes, J., Vanstone, S. (Eds.), Advances in Cryptology-CRYPTO' 90. CRYPTO 1990. Lecture Notes in Computer Science, vol 537. Springer, Berlin, Heidelberg 1991.

Härer, Felix, Fill, Hans-Georg, A Comparison of Approaches for Visualizing Blockchains and Smart Contracts. In: Schweighofer, Erich/Kummer, Franz/Saarenpää, Ahti (Hrsg.), Internet of Things. Tagungsband des 22. Internationalen Rechtsinformatik Symposion IRIS 2019, Editions Weblaw, Bern 2019a, S. 527–537.

Härer, Felix, Fill, Hans-Georg, Decentralized Attestation of Conceptual Models Using the Ethereum Blockchain, 21st IEEE International Conference on Business Informatics CBI 2019, Moskau 2019b. DOI 10.1109/CBI.2019.00019.

Konzelmann, Alexander, eIDAS: Innerstaatliche Umsetzung eines nicht umsetzungsbedürftigen EU-Rechtsaktes. In: Schweighofer, Erich/Kummer, Franz/Hötzendorfer, Walter/Sorge, Christoph (Hrsg.), Trends und Communities der Rechtsinformatik. Tagungsband des 20. Internationalen Rechtsinformatik Symposions IRIS 2017, Österreichische Computer Gesellschaft, Wien 2017, S. 241–249.

Piswanger, Carl-Markus/Hühnlein, Detlef/Ponte, Nuno/Zehetner, Christoph/Hermanns, Christina/Kapanadze, Mikheil/Stojicic, Snezana/Dean, Roger, EU Project «FutureTrust»: Applications, Pilot, and Demonstrator. In: Schweighofer, Erich/Kummer, Franz/Saarenpää, Ahti/Schafer, Burkhard (Eds.), Data Protection / LegalTech. Proceedings of the 21th International Legal Informatics Symposium IRIS 2018, Editions Weblaw, Bern 2018, S. 369–375.

Steinbrück, Anne, Identitätsverwaltung über die Blockchain? Rechtliche Betrachtungen am Beispiel des Internets der Dinge. In: Schweighofer, Erich/Kummer, Franz/Saarenpää, Ahti (Hrsg.), Internet of Things. Tagungsband des 22. Internationalen Rechtsinformatik Symposion IRIS 2019, Editions Weblaw, Bern 2019, S. 283–289.

Swan, Melanie, Blockchain: Blueprint for a New Economy, O'Reilly Media Inc., Sebastopol, California 2015, S. 37–44.