SELF-SOVEREIGN IDENTITY UND BLOCKCHAIN

Jakob Zanol / Alexander Czadilek / Kaspar Lebloch

Mag., Wissenschaftlicher Projektmitarbeiter, Universität Wien, Arbeitsgruppe Rechtsinformatik
Schottenbastei 10-16/2/5, 1010 Wien, AT
jakob.zanol@univie.ac.at

Mag., Rechtsanwaltsanwärter, Scheucher Rechtsanwalt GmbH
Lindengasse 39 1070 Wien, AT
czadilek@scheucher.eu; www.scheucher.eu

BSc, Wissenschaftlicher Projektmitarbeiter, Universität Wien, Forschungsgruppe Cooperative Systems
Sensengasse 6, 1090 Wien, AT
kaspar.lebloch@univie.ac.at; https://informatik.univie.ac.at/cosy

Keywords: ***Self-Sovereign Identity, Blockchain, Identitätsmanagement, Datenschutz***

Abstract: *Konzepte zur Schaffung einer Self-Sovereign Identity, also einer durch die jeweils betroffene Person ausschließlich selbst kontrollierte digitale Identität, auf Basis der Distributed-Ledger (Blockchain)-Technologie werden immer konkreter. Der vorliegende Beitrag stellt die technischen Grundlagen der öffentlich zugänglichen Self-Sovereign-Identity-Konzepte dar und stellt diese der österreichischen Rechtslage im Bereich Datenschutzrecht und elektronische Identität (eID) gegenüber.*

1. Die Idee der Self-Sovereign Identity

In einem Self-Sovereign-Identity-Modell[1] kontrolliert und besitzt ein Benutzer die gesamte Menge seiner eigenen Daten. Die Idee einer Self-Sovereign Identity entstand nicht einfach aus dem Blauen heraus. Der Internet-Identity-Workshop etwa fand etwa bereits im Jahr 2005 zum ersten Mal statt und begann sich mit dem Thema «User-Centric-Identity» zu beschäftigen. Im Gegensatz zum Ansatz der «Enterprise-Centric-Identity» erlaubt die «User-Centric-Identity» den Nutzern die Kontrolle ihrer digitalen Identität. Sie selbst können bestimmen, welche Attribute (persönliche Daten) bei einem Authentifizierungsvorgang übermittelt werden. Die Nutzer erhalten somit mehr Rechte aber auch Verantwortlichkeit hinsichtlich ihrer persönlichen Informationen.

Die Distributed-Ledger-Technologie oder auch Blockchain war ein Meilenstein in der Entwicklung der gängigen Self-Sovereign-Identity-Konzepte. Im Rahmen der Entdeckung der Blockchain für andere Zwecke als der Transaktion von Kryptowährungen wie etwa Bitcoin brach ein regelrechter Hype um diese Technologie aus. Auch österreichische Medien berichteten über «die Blockchain», wobei der Fokus dabei auf Bitcoin lag.

2. Technische Grundlagen

2.1. Blockchain

Die Distributed-Ledger-Technologie soll Vertrauen (in den Transaktionspartner) durch gegenseitige Kontrolle ersetzen. Durch die Generierung eines jeden neuen Blocks in der Blockchain mit dem Inhalt, welchem die Mehrheit der Teilnehmer des Netzwerks zugestimmt hat, wird das Vertrauen von einer zentralen Autorität in die Mehrheit der Teilnehmer verlagert. Durch die Verknüpfung des Hash-Wertes des vorherigen Blocks in den jeweils folgenden, werden die Blöcke zu einer Kette (*chain*), welche die Integrität der darin enthaltenen Daten garantiert. Wollte man die Daten fälschen, müsste man über die jeweils durch das Skript vorgegebene Mehrheit der am Netzwerk teilnehmenden Server verfügen.

[1] Abraham, Whitepaper Self-Sovereign Identity (https://www.egiz.gv.at/files/download/Self-Sovereign-Identity-Whitepaper.pdf [alle Websites zuletzt abgerufen am 3. Januar 2018]).

Ledger können *permissioned* oder *permissionless* konzeptioniert sein. Im Kern bedeutet dies, dass das Betreiben von Knoten entweder nur mit Zugriffskontrollen oder für jeden möglich ist. Weiters kann ein Ledger öffentlich (*public*), oder nur für ausgewählte Entitäten ersichtlich sein (*private*). Die zum Zeitpunkt des Verfassens dieses Beitrags angedachte Sovrin[2]-Blockchain-Architektur sieht einen Public-Permissioned Ledger vor, der nur von bestimmten Mitgliedern (sogenannte *stewards*[3]) der Sovrin Foundation bearbeitet werden darf, aber öffentlich einsehbar ist.

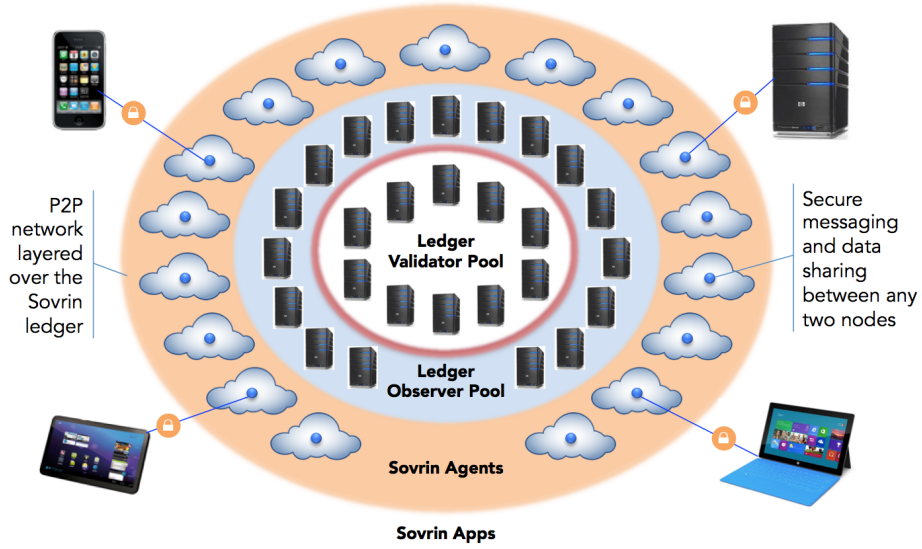

Abbildung 1: Übersicht Sovrin-Network[4]

Zusammenfassend: die Daten auf der Blockchain sind unabänderlich und verteilt gespeichert.

Aufgrund dieser Eigenheit der Blockchain wird auch in den verschiedenen Self-Sovereign-Identiy-Konzepten weitgehend auf die Speicherung von «echten» Datensätzen (auch in verschlüsselter oder gehashter Form) verzichtet. Denn auch wenn etwa das Hashing-Verfahren nach SHA256 eine «Rückführung» (bzw. Rekonstruktion) des Datensatzes aus dem Hashwert so gut wie unmöglich macht, so ist nicht abzusehen, ob dies durch zukünftige Technologien nicht etwa doch möglich sein wird.

Daher geht der Trend derzeit eher dahin, sogenannte Metadaten in die Blockchain zu integrieren, etwa durch Decentralized Identifiers (DIDs) und zugehörige DID-Dokumente.

2.2. DID und DID-Dokument

Um Einträge auf dem Sovrin-Ledger zu verankern, wird ein Decentralized Identifier gemeinsam mit den Daten, aus welchen das ihm zugeordnete DID-Dokument generiert werden kann, abgelegt. Ein DID ist eine in ihrer Anwendungsdomäne einzigartige, und somit eindeutig identifizierbare Zeichenkette, bestehend aus einem

2 Sovrin (https://sovrin.org).
3 Sovrin Trust Framework (https://sovrin.org/library/trust-framework/).
4 How Sovrin Works (https://sovrin.org/library/how-sovrin-works/).

führenden «did:» gefolgt von einer Methode, und einem spezifischen *idString*. Als Beispiel soll hier eine gültige Sovrin-DID wie aus dem DID-Implementer's-Draft[5] dienen:

did:sov:21tDAKCERh95uGgKbJNHYp

wobei sov die Methode (Sovrin) und 21tDAKCERh95uGgKbJNHYp der spezifische *idString* ist. Der DID ist im Weiteren als *key* des *key-value*-Paares *(*DID und DID-Dokument*)* zu interpretieren.

Ein DID-Dokument ist eine JSON-Datenstruktur, die den Identitätseigentümer beschreibt. Um Privacy by Design sicherstellen zu können, beschränkt sich diese Beschreibung auf die Metadaten, *public keys* (öffentliche Schlüssel) und sogenannte Service-Endpoints, an welchen mit Services des Identitätseigentümers in Kontakt getreten werden kann. Es gibt jedoch auch Konzepte, die ein erweiterbares DID-Dokument vorsehen, und somit das tatsächliche Ablegen von persönlichen Daten auf dem öffentlichen Ledger erlauben sollen.

Ein Beispiel für ein mögliches dem oben genannten DID zugehöriges DID-Dokument:

```
{
        ”@context”: ”https://w3id.org/did/v1”,
        ”id”: ”did:sov:21tDAKCERh95uGgKbJNHYp”,
        ”keys”: [{
        ”id”: ”#key1”,
        ”type”: ”rsa-2017-pem”,
        ”value”: ”——BEGIN KEY...END KEY——{\}r{\}n”
        }],
        ”services”: [{
        ”id”: ”#srv1”,
        ”type”: ”agent”,
        ”name”: ”agent”,
        ”keyref”: ”#key1”,
        ”endpoint”: ”https://agent.example.com/”
        }]
}
```

2.3. Agents und Verifiable Claims

Für den Zweck des Identitäts- oder Attributsnachweises ist als solcher Service-Endpoint in der Sovrin-Architektur ein *agent*[6] zuständig. *Agents* können Dienstleister sein, es steht allerdings auch jedem Sovrin-Identity-Owner (Identitätseigentümer) frei, selbst einen *agent* zu betreiben. Ein agent speichert sogenannte *verifiable claims* über den Identitätseigentümer. Unter einem *verifiable claim* versteht man eine Aussage über ein Subjekt (z.B. Geburtsdatum, Universitätsabschluss oder eine bestimmte Eigenschaft etc.), die digital durch Dritte verifizierbar ist, indem ihr Ursprung kryptographisch mittels Signaturen nachgewiesen wird[7]. Diese *claims* können gegenüber anfragenden Entitäten nachgewiesen werden.

Die Glaubwürdigkeit eines *verifiable claims* steht somit in direkter Abhängigkeit von der Glaubwürdigkeit der signierenden Autorität (z.B. eine Behörde). Zielführend ist somit die Ausarbeitung eines «Trust-Frameworks»

---

5 DID (Decentralized Identifier) Data Model and Generic Syntax 1.0 Implementer's Draft 01 (https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/draft-documents/did-implementer-draft-10.md).

6 Sovrin Provisional Trust Framework (https://sovrin.org/wp-content/uploads/2017/07/Sovrin-Provisional-Trust-Framework-2017-06-28.pdf).

7 Sporny/Longley, Verifiable Claims Data Model and Representations (Work in Progress!) (https://www.w3.org/TR/verifiable-claims-data-model/).

auf rechtlicher und geschäftlicher Ebene, um die Vertrauenswürdigkeit in *verifiable claims* sicherzustellen, da Glaubwürdigkeit nicht alleine durch Technik garantiert wird.

2.4. Zero-Knowledge-Proof und Korrelierbarkeit

Um so wenige Daten wie notwendig preiszugeben, werden statt des Inhalts eines *claims* lediglich Beweise für die Erfüllung von Voraussetzungen (z.B. Geschäftsfähigkeit) oder Attributen, sogenannte *proofs*, berechnet und an den Kommunikationspartner gesendet. Der Kommunikationspartner soll dadurch ohne das Wissen über das Attribut selbst (etwa ein Geburtsdatum) einen Beweis erhalten, dass die von ihm gesetzten Voraussetzungen (etwa: Volljährigkeit) erfüllt sind. Dafür werden spezielle Zero-Knowledge-Proof-Algorithmen eingesetzt[8].

Um der Korrelierbarkeit der eigenen Daten entgegenzuwirken, bietet Sovrin an, für jede Verbindung paarweise unterschiedliche (*pairwise unique*) DIDs mit eigenen Schlüsselpaaren und eigenen Service-Endpoints zu generieren. Unterschiedliche DIDs sollen dennoch auf dieselben *claims* verweisen können, sodass Daten nicht mehrfach bestätigt werden müssen. Ziel dieser Vorgehensweise ist es, zu verhindern, über einen einzigen, der eigenen Person zugeordneten DID identifizierbar zu sein. Einige der angelaufenen Pilotprojekte (*proof of concepts*) auf Basis von Sovrin haben sich allerdings vorerst gegen die Verwendung von multiplen DIDs pro Person entschieden.

Für eine vertiefende technische Analyse sowie den Vergleich von Sovrin mit anderen Anbietern von Self-Sovereign-Identity-Services, wird auf die Arbeit von Andreas Abraham[9] verwiesen.

3. Rechtsgrundlagen

3.1. Datenschutz

In Hinblick auf die Unabänderlichkeit der Blockchain ist die Anwendbarkeit des Datenschutzrechts auf in ihr gespeicherte Daten ein besonders kritischer Aspekt. Die Anwendbarkeit des Datenschutzrechts ist vom Personenbezug der Daten abhängig. Personenbezogene Daten, deren Verarbeitung nicht oder nicht mehr rechtmäßig ist, sind vom Verantwortlichen zu löschen.

Derzeit zeichnen sich zwei Ansätze ab, wie die Blockchain in Hinblick auf Self-Sovereign Identity verwendet werden soll.

Ein Ansatz ist die Speicherung von Hashwerten der jeweiligen Identitätsattribute. Ein anderer, der sich durchzusetzen scheint, ist die Speicherung von sogenannten Metadaten (siehe oben DID/DID-Dokument), welche ausschließlich die Kommunikation mit dem *agent* ermöglichen sollen.

Gemäß Art. 4 Z 1 DSGVO[10] sind Informationen, die sich auf eine identifizierte oder identifizierbare (natürliche) Person beziehen, personenbezogen. Nach (noch) geltender Rechtslage können Betroffene gemäß § 4 Z 3 DSG 2000 natürliche oder juristische Personen sein[11].

Ob ein Datum einer identifizierten oder identifizierbaren Person zuzuordnen ist, führt datenschutzrechtlich zum gleichen Ergebnis. Entscheidend ist allein die Frage, ob im konkreten Fall nicht einmal Identifizierbarkeit gegeben ist[12].

---

8 Sovrin Provisional Trust Framework (https://sovrin.org/wp-content/uploads/2017/07/Sovrin-Provisional-Trust-Framework-2017-06-28.pdf).

9 Abraham (Fn. 1).

10 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung; kurz: DSGVO).

11 Hötzendorfer, Datenschutz und Privacy by Design im Identitätsmanagement (2016), 126.

12 Ernst in: Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung[1] (2017) Art. 4 Rz 9.

Der diesbezügliche Meinungsstreit zwischen dem absoluten/objektiven und dem relativen/subjektiven Ansatz[13] wurde durch die Entscheidung des EuGHs in der Rechtssache Breyer[14] zugunsten einer Spielart des relativen Ansatzes entschieden[15].

Danach ist der Personenbezug von Daten davon abhängig, ob die Möglichkeit, diese mit den Zusatzinformationen zu verknüpfen, über die ein Dritter verfügt, ein Mittel darstellt, das vernünftigerweise zur Bestimmung der betreffenden Person eingesetzt werden kann. Dies wäre, so der EuGH, nicht der Fall, wenn die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar wäre, z.B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung de facto vernachlässigbar erschiene[16].

Die Ähnlichkeit von DIDs zu IP-Adressen drängt sich bei deren näherer Betrachtung (siehe oben) auf. DIDs verweisen auf den jeweiligen a*gent*, welcher entweder durch den User selbst betrieben wird, oder durch einen Dritten, der das Betreiben eines *agent*s als Service anbietet. Der DID ermöglicht die Kommunikation zwischen dem Identitätseigentümer und der anfragenden Entität und die Anfrage nach verschiedenen *claims*. Die in den DID-Dokumenten enthaltene URL des Service-Endpoints verweist auf die IP-Adresse des Servers, auf dem der *agent*, über welchen die Attribute und *claims* gehandhabt werden, gespeichert ist. Auch die Verarbeitung eines DIDs kann daher eine Verarbeitung personenbezogener Daten darstellen, sofern der Verantwortliche etwa über rechtliche Mittel verfügt, um die dahinter stehende Person bestimmen zu lassen. Dies wird auch dann gelten, wenn der Service-Endpoint auf einen Server verweist, der durch eine juristische Person[17] betrieben wird, sofern der Personenbezug zu einem User als natürlicher Person hergestellt werden kann. Abhängig von der technischen Umsetzung eines *agents*, der von einem Dritten betrieben wird, kann der Personenbezug eines DID durch das Zusatzwissen jenes Dritten hergestellt werden.

Werden aus personenbezogenen Daten mithilfe einer Hash-Funktion Hash-Werte gebildet, ist zu differenzieren. Einerseits werden jene Hash-Werte die durch eine unsichere Hash-Funktion[18] gebildet werden, als rückführbar zu bezeichnen sein. Hash-Werte, welche mittels einer sicheren Hash-Funktion gebildet werden, sind derzeit nicht rückführbar und zwar in dem Sinne, dass aus dem Hash-Wert nicht auf das Ursprungsdatum geschlossen werden kann[19]. Der Personenbezug kann sich diesfalls jedoch durch die Möglichkeit der Erstellung sogenannter «Rainbow-Tables»[20] ergeben. Da die Hash-Funktion in der Regel öffentlich ist (wie etwa SHA256) und der Input in einem bestimmten Format vorgegeben ist (Geburtsdatum wird bspw. im Format DD.MM.YYYY eingegeben) können Angreifer mit einem Minimum an Rechenleistung die Hash-Werte z.B. aller in Frage kommenden Geburtsdaten im Voraus berechnen, in einer Datenbank speichern und schließlich diese Datenbank mit den Hash-Werten vergleichen[21]. Unter Berücksichtigung der Entscheidung des EuGHs in der Rechtssache *Breyer*[22], ist der Personenbezug der Daten für jeden Verantwortlichen im Rahmen seiner Möglichkeiten zu beurteilen. Nicht jeder Verantwortliche kann aus einzelnen Attributen einen Rückschluss auf die Person vornehmen. Es wird daher auch bei Rückführbarkeit einzelner Daten mittels Rainbow-Tables

13 Für eine Darstellung des Meinungsstreites unter Einbeziehung der österreichischen Literatur siehe Hötzendorfer (Fn. 11), 132.

14 EuGH 19. Oktober 2016, Rs C-582/14, *Breyer/Deutschland*.

15 Hötzendorfer (Fn. 11), 137.

16 EuGH 19. Oktober 2016, Rs C-582/14, *Breyer/Deutschland*, Rz 45–48.

17 Daten juristischer Personen sind von der ab 25. Mai 2018 in Geltung stehenden DSGVO nicht umfasst. Zu beachten ist allerdings, dass § 1 DSG 2000 auch nach Erlassung des Datenschutz-Anpassungsgesetzes 2018 weiterhin in Geltung steht; die Frage des Schutzes juristischer Personen ist sohin – zumindest in Österreich – weiterhin strittig. Gegen einen Datenschutz für juristische Personen etwa Leissler, Datenschutz für juristische Personen – ein Blick in die Zukunft, ecolex 2017, 1222.

18 Etwa MD-4 oder MD-5.

19 Lässt man allfälliges Zusatzwissen des Verantwortlichen außer Betracht.

20 Datenbanken, welche die Hashwerte einer Vielzahl von in Frage kommenden Eintragungen enthalten, vgl. hierzu auch Voitel, Sind Hash-Werte personenbezogene Daten?, DuD Datenschutz und Datensicherheit 11/2017, 686.

21 Voitel (Fn. 20), 686.

22 EuGH 19. Oktober 2016, Rs C-582/14, *Breyer/Deutschland*.

darauf ankommen, ob die jeweiligen Daten (mit vertretbarem Aufwand) die dahinterstehenden Personen identifizierbar machen. Bei der Feststellung, ob Mittel i.S.d. Erwägungsgrundes 26 DSGVO nach allgemeinem Ermessen wahrscheinlich zur Identifizierung einer natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Identifizierung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Nun hat die Geschichte gezeigt, dass Hash-Funktion mit der Zeit veraltern[23]. Doch auch unter Berücksichtigung der Unabänderlichkeit der Blockchain, wird Erwägungsgrund 26 DSGVO wohl nicht so zu verstehen sein, dass auch Entwicklungen die sich noch gar nicht abzeichnen (lassen), zu berücksichtigen sind und sich der Personenbezug eines Datums bereits davor ergibt.

Hinzu kommt, dass der Nutzung von Rainbow-Tables auch bei unsicheren Hash-Funktionen durch die Verwendung eines sogenannten Salts[24] entgegengewirkt werden kann. Dabei werden, vor der Anwendung der (öffentlich zugänglichen) Hash-Funktion auf die betreffenden Daten, diese Daten noch mit einer (geheimen) Funktion – dem Salt – verändert, wodurch sich auch die errechneten Hash-Werte grundlegend ändern und ein Rainbow-Table ohne Kenntnis des Salt[25] nicht erstellt werden kann. Die Kenntnis des Salt könnte dazu führen, dass der Verantwortliche personenbezogene Daten verarbeitet. In jedem Fall, ist die Speicherung von, wenn auch kryptographisch verschlüsselten, Daten in einem *public ledger* aufgrund dessen Unabänderlichkeit problematisch, da sich die Rückführbarkeit mitunter in naher Zukunft, durch neue Technologien ergeben kann, die Daten jedoch bereits *distributed* sind.

Sind also die in der Blockchain gespeicherten Daten personenbezogen, unterliegen sie dem Datenschutz. Dies bedeutet, dass die Verarbeitung nicht mehr uneingeschränkt, sondern nur im rechtlichen Rahmen zulässig ist.

Es stellt sich zunächst die Frage, wer bei einem System, das auf einer Blockchain basiert, die Daten verarbeitet, wer also nach der Diktion der DSGVO Verantwortlicher ist. Wie bereits oben beschrieben, ist die Blockchain eine Distributed-Ledger-Technologie und wird auf jeden Netzwerkknoten (*node*) verteilt.

Verarbeitung i.S.d. Art. 4 Z 1 DSGVO ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie etwa das Erheben, das Erfassen, das Speichern, das Auslesen, das Abfragen von Daten etc. Verantwortlicher i.S.d. Art. 4 Z 7 DSGVO ist jene natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Daher ist grundsätzlich jeder *node*, und sei er auch bloß zum Beobachten und nicht zum Schreiben auf die Blockchain berechtigt (bloßer *observer node*), ein Verantwortlicher i.S.d. Art. 4 Z 7 DSGVO[26].

Eine rechtmäßige Verarbeitung i.S.d. Art. 6 DSGVO erfordert die Einwilligung oder eine sonstige zulässige Rechtsgrundlage[27]. Unabhängig davon, wie der Ablauf der Registrierung zu einer Self-Sovereign-Identity-Anwendung auf Blockchain-Basis ausgestaltet ist, steht die Einwilligung zu einer Speicherung in der Blockchain vor diversen Schwierigkeiten. Es ist etwa eine Einwilligung auch hinsichtlich der zukünftig dem

---

23 Zu MD4 und MD5 und SHA-1 siehe etwa bereits Lucks, Zur Sicherheit kryptographischer Hashfunktionen, http://www.cryptolabs.org/hash/LucksWeisSicherheitHash0305.pdf (veröffentlicht am 16. März 2005).

24 Also eines Initialisierungswertes, welcher den Grunddatensatz vor der Anwendung der Hash-Funktion adaptiert, wodurch auch bei Kenntnis der Hash-Funktion nicht auf den Grunddatensatz geschlossen werden kann, zum Begriff «Salt» siehe etwa http://www.aspheute.com/english/20040105.asp.

25 Die Kenntnis eines solchen verwendeten Salts, wäre diesfalls ein solches oben erwähntes «Zusatzwissen», welches den Personenbezug für den jeweiligen Verantwortlichen herzustellen vermag.

26 So etwa auch (allerdings bezogen insbesondere auf die Bitcoin-Blockchain): Schrey/Thalhofer, Rechtliche Aspekte der Blockchain, NJW 2017, 1433.

27 Vgl. Erwägungsgrund 40 DSGVO.

Netzwerk Beitretenden (zukünftige Verantwortliche) erforderlich[28]. Eine solche pauschale Einwilligung ist jedoch, aufgrund der strikten Zweckbindung der Einwilligung wohl nicht möglich[29].

Fraglich ist zudem, ob eine rechtsgültige Einwilligung in Hinblick auf die unbegrenzte Speicherung in der Blockchain überhaupt abgegeben werden kann. Schließlich ist eine Einwilligung in die Verarbeitung grundsätzlich jederzeit widerrufbar[30]. Würde man daher die Zulässigkeit einer Einwilligung in eine (weitgehend) unwiderrufliche Speicherung bejahen, könnte durch Verwendung einer entsprechenden Technologie die grundsätzliche Widerrufbarkeit der Einwilligung umgangen werden.

Als weitere Möglichkeit einer zulässigen Datenverarbeitung findet sich in Art. 9 Abs. 2 lit. e DSGVO noch der Fall, dass sich die Verarbeitung auf personenbezogene Daten bezieht, die «die betroffene Person offensichtlich öffentlich gemacht hat»[31]. Art. 9 DSGVO bezieht sich zwar auf die Verarbeitung besonderer Kategorien personenbezogener Daten (nach dem DSG 2000 weitestgehend sensible Daten). Wenn aber eine Veröffentlichung sogar besonderer Kategorien personenbezogener Daten durch den Betroffenen selbst deren Verarbeitung zulässig macht, so muss dies umso mehr kraft Größenschluss *(argumentum a maiore ad minus)* für nicht-sensible Daten gelten.

Es kann somit argumentiert werden, dass bei einem *public distributed ledger*, der grundsätzlich frei zugänglich ist, Daten durch den User selbst veröffentlicht werden können[32] und die Verarbeitung (also insbesondere die Speicherung dieser Daten auf den jeweiligen *nodes*) durch jeden Teilnehmer des Netzwerks daher rechtmäßig erfolgt.

Auch die Veröffentlichung i.S.d. Art. 9 Abs. 2 lit. e DSGVO hat diesfalls jedoch rechtmäßig zu erfolgen. Dies scheint bei der Veröffentlichung durch den Betroffenen selbst grundsätzlich unproblematisch zu sein. Allerdings gilt es hier zu bedenken, dass der Zugang zu einem Dienst mitunter an die Veröffentlichung von personenbezogenen Daten geknüpft wird. Es liegt daher nahe, die diesbezüglich bereits zu § 1 DSG 2000 («allgemein verfügbar») in der Lehre und Rechtsprechung entwickelten Grundsätze[33] auch in diesem Fall anzuwenden. Insbesondere Art. 1 i.V.m. Erwägungsgrund 1 der DSGVO, wonach der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ein Grundrecht ist, deutet darauf hin.

Daher ist bei der Veröffentlichung auf einem Distributed Ledger zu beachten, dass die Täuschung über die Konsequenzen der Veröffentlichung der Daten (etwa, dass die Hashwerte der Daten nicht rückführbar sind, ohne auch vor möglichen disruptiven Entwicklungen in diesem Bereich zu warnen) mitunter eine rechtmäßige Veröffentlichung verhindert.

Die schwer vorhersehbaren Entwicklungen in technischer Hinsicht, insbesondere betreffend Verschlüsselungstechniken, sind bei der Auswahl eines Self-Sovereign-Identity-Dienstes im öffentlichen wie im privaten Bereich zu berücksichtigen, wobei auch bei den einzelnen Diensten jeweils der volle Umfang datenschutzfördernder Maßnahmen implementiert werden sollte[34].

3.2. eIDAS Verordnung und E-GovG

Die eIDAS Verordnung (EU) 910/2014 schafft den Rechtsrahmen zur gegenseitigen Anerkennung der verschiedenen elektronischen Identifizierungsmittel in den Mitgliedstaaten der EU unter bestimmten normierten Voraussetzungen. Grundsätzlich wäre es möglich, Identitätsdaten einer existierenden eID Infrastruktur, wie dem eIDAS-Netzwerk in ein Self-Sovereign-Identity-Format umzuwandeln. Eine Self-Sovereign Identity, die

28 Schrey/Thalhofer (Fn. 26), 1434.
29 Ernst in: Paal/Pauly (Fn. 12), Art. 4 Rz 78.
30 Art. 7 Abs. 3 DSGVO.
31 Art. 9 Abs. 2 lit. e) DSGVO.
32 Auch wenn die Berechtigung, neue Blöcke anzuhängen, bei ausgewählten *nodes* liegt (*permissioned*).
33 Dohr/Pollirer/Weiss/Knyrim, DSG² § 1 (Stand 26. November 2015, rdb.at) Rz 7.
34 I.S.d. Grundsatzes des Datenschutzes durch Technikgestaltung (Art. 25 DSGVO).

den Anforderungen des Art. 26 eIDAS Verordnung entspricht, könnte als qualifizierte Self-Sovereign Identity auch als rein privatwirtschaftlich organisiertes Identifizierungssystem gemäß Art. 7 lit. a eIDAS Verordnung notifiziert und implementiert werden, sofern es vom jeweiligen bzw. den jeweiligen Mitgliedstaaten anerkannt wird. Solch ein Identifizierungssystem hätte auch ein hohes Sicherheitsniveau i.S.d. Art. 8 Abs. 2 lit. c eIDAS Verordnung[35]. Nach dem österreichischen EGovG i.d.F. BGBl. I 121/2017 ist die eID als ein technologieunabhängiges Identifizierungsmittel ausgestaltet. Das derzeitige österreichische Konzept lässt sich jedoch aufgrund der verpflichtenden hoheitlichen Registrierung der Nutzer bei bestimmten inländischen Behörden (§ 4 Abs. 3 und § 4a EGovG) mit den oben dargestellten Self-Sovereign-Identity-Konzepten nur schwer in Einklang bringen. Jedenfalls aber legen die Architekten verschiedener Self-Sovereign-Identity-Modelle Wert darauf, dass Self-Sovereign Identity nicht in Konkurrenz oder Wettbewerb zu nationalen, staatlichen eIDs stehen, sondern zu diesen sogar komplementär sind[36].

4. Fazit

Im Identitätsmanagement gibt es verschiedenste Ansätze, digitale Identitäten und die entsprechenden Daten zu verwalten. Viele dieser Modelle sind mit unterschiedlichsten Problemen behaftet, seien es Unzulänglichkeiten im Datenschutz, der Integrität der Daten oder der Datensicherheit. Mit dem Modell einer Self-Sovereign Identity, die auf der Blockchain-Technologie basiert, entwickelt sich die digitale Identität von einem nichtbenutzergesteuerten und zentralisierten Modell zu einem vollständig benutzergesteuerten und dezentralisierten Modell. Ein Self-Sovereign-Identity-Modell soll drei grundlegende Anforderungen erfüllen:

- Kontrolle der Nutzer über ihre Daten
- Sicherheit und Integrität der Daten
- Portabilität der Daten und Souveränität (in dem Sinne, dass dem Nutzer die Kontrolle über seine Daten nicht genommen werden kann)

Das Self-Sovereign-Identity-Modell bietet die Möglichkeit, in der DSGVO verankerte datenschutzrechtliche Grundsätze im Bereich des Identitätsmanagements zu verwirklichen. Besonders zu nennen ist an dieser Stelle der Grundsatz der Datenminimierung sowie der Grundsatz des Datenschutzes durch Technikgestaltung (Privacy by Design[37]).

Die europäische eIDAS Verordnung, die den Rechtsrahmen für eine Anerkennung verschiedener digitaler Identitätsmodelle unter den Mitgliedstaaten regelt, steht einer Implementierung eines auf der Blockchain basierenden Self-Sovereign-Identity-Modells nicht entgegen. Das österreichische eID-Modell, das im E-Governmentgesetz geregelt und grundsätzlich technologieunabhängig ist, ist hingegen so konzeptioniert, dass sich der Nutzer verpflichtend bei einer inländischen Behörde registrieren muss, um die digitale Identität nutzen zu können. Somit ist das österreichische eID-Modell nur schwer mit dem Modell der hier vorgestellten Self-Sovereign Identiy in Einklang zu bringen.

---

35 Die Festlegung der Mindestanforderungen an die technischen Spezifikationen erfolgt in der Durchführungsverordnung der EU-Kommission 2015/1502.

36 Cutler/Ho, Self-Sovereign Identity and Distributed Ledger Technology: Framing the Legal Issues (https://www.perkinscoie.com/en/news-insights/self-sovereign-identity-and-distributed-ledger-technology.html) .

37 Vgl. Art. 25 DSGVO.