Fraunhofer FOKUS

FRAUNHOFER-INSTITUT FÜR OFFENE KOMMUNIKATIONSSYSTEME FOKUS

DIGITALE IDENTITÄTEN IN DER BLOCKCHAIN
ERFAHRUNGEN AUS DER ENTWICKLUNG

Fabian Kirstein, Manuel Polzhofer, Klaus-Peter Eckert

IMPRESSUM

Digitale Identitäten in der Blockchain – Erfahrungen aus der Entwicklung

Autoren:
Fabian Kirstein, Manuel Polzhofer, Dr. Klaus-Peter Eckert

Herausgeber:
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Digital Public Services (DPS)
Kaiserin-Augusta-Allee 31, 10589 Berlin
www.fokus.fraunhofer.de
www.blockchain-werkstatt.de

Fotonachweise: Reiko Kammer

Aus Gründen der Vereinfachung und um einen besseren Lesefluss zu gewährleisten, wird in den folgenden Ausführungen auf die parallele Verwendung der männlichen und der weiblichen Form bzw. Schreibweise verzichtet. Es wird an dieser Stelle ausdrücklich betont, dass immer alle Geschlechter angesprochen und gemeint sind.

Soweit in diesem Werk direkt oder indirekt auf Gesetze, Vorschriften oder Richtlinien (z. B. DIN, VDI) Bezug genommen oder aus ihnen zitiert worden ist, kann das Institut keine Gewähr für Richtigkeit, Vollständigkeit oder Aktualität übernehmen.

INHALTSVERZEICHNIS

1 EINLEITUNG 4

2 ZIELSTELLUNG 6

3 EIGNUNG DER BLOCKCHAIN 7

4 ENTWURF UND UMSETZUNG 9

4.1 Was kommt in die Blockchain? 9
4.2 Smart Contracts 9
4.3 Die Webanwendung 11
4.4 Datenhaltung 11
4.5 Verifikationsprozess 12
4.6 Der Private Schlüssel 13
4.7 Zwischenfazit 13

5 ERGEBNISSE UND EVALUATION 15

5.1 Transaktionskosten 15
5.2 Latenz 16
5.3 Usability 16
5.4 Dezentralität 16
5.5 Datenschutz 16

6 AUSBLICK UND EMPFEHLUNGEN 17

7 WEITERE PROJEKTE 19

1 EINLEITUNG

Digitale Identitäten sind eine entscheidende Grundlage für das moderne World Wide Web und die digitale Vernetzung. Erst sie ermöglichen Kommunikation, Datenaustausch und Transaktionen. Jeder Mensch besitzt eine Vielzahl digitaler Identitäten, aufgrund der Nutzung verschiedener Dienstleistungen: Vom Onlinebanking-Account, über den Twitter-Zugang, bis zum Datenbankeintrag im Bürgeramt.

Die Welt der digitalen Identitäten ist höchst fragmentiert und redundant. Erschwerend kommt hinzu, dass die meistgenutzten digitalen Identitäten von wenigen amerikanischen Unternehmen zur Verfügung gestellt werden. Dazu zählen u.a. die Plattformen von Facebook und Google und ihre entsprechenden Single Sign-on Systeme. Diese Dienste sind geschlossen, proprietär und zentralisiert. Sie erzeugen »Daten-Silos«, verursachen Anbieterabhängigkeit, verhindern Wettbewerb und verringern Marktvielfalt. Hinzu kommen die bekannten Bedenken bezüglich Datenschutz und Datensouveränität.

Als ein Lösungsansatz gilt der Einsatz einer sogenannten »Self-Sovereign Identity«[1]. Damit sind digitale Identitäten gemeint, die vollständig unter der Kontrolle ihrer Nutzer liegen und von keiner zentralen Instanz verwaltet und kontrolliert werden. Der Nutzer hat entsprechend die ausschließliche Hoheit über die assoziierten Daten der Identität und ist zu jedem Zeitpunkt in der Lage diese Informationen zu ändern oder zu löschen. Im Idealfall wird man zukünftig alle digitalen Dienste mit einer solchen Identität nutzen können und somit der Fragmentierung und dem Kontrollverlust entgegenwirken.

Wie eine Self-Sovereign Identity technisch genau umgesetzt werden kann ist ungeklärt. Offene Single Sign-on Systeme, wie OpenID, haben bisher zu wenig Verbreitung gefunden und basieren weiterhin auf dem Prinzip, dass ein zentraler Anbieter die digitale Identität verwaltet. Um diese Zentralisierung zu umgehen, werden derzeit vielfältige Lösungsansätze auf Basis von dezentralen Technologien diskutiert und umgesetzt. Besondere Beachtung findet dabei die Blockchain-Technologie. Als sichere, dezentrale Datenbank scheint die Blockchain prädestiniert zu sein, die technologische Grundlage für digitale Identitäten der nächsten Generation zu sein. Tatsächlich wird Identitätsmanagement fast immer als typischer Anwendungsfall der aufstrebenden Technologie genannt. Das scheint in jedem Fall gerechtfertigt, da auch andere Anwendungsfälle der Blockchain als Grundlage ein Identitätsmanagement in der einen oder anderen Form benötigen.

[1] www.coindesk.com/path-self-sovereign-identity/

Fraunhofer FOKUS hat im Auftrag des Berliner Start-ups Jolocom (www.jolocom.com) die Eignung der Blockchain für das Management von digitalen Identitäten untersucht. Das 6-monatige Vorhaben wurde von der Investitionsbank Berlin (www.ibb.de) gefördert und praktisch an den Anforderungen des bestehenden Softwareprodukts von Jolocom umgesetzt. Das Start-up entwickelt ein dezentrales Kommunikationsnetzwerk, um Daten, Dateien, Informationen und Nachrichten auszutauschen. Daher scheint der Einsatz einer dezentralen digitalen Identität konsequent.

Aufgrund des begrenzten Zeitrahmes des Projektes wurde auf eine detaillierte Analyse und Evaluation der verschiedenen Blockchain-Technologien und Ausprägungen verzichtet. Als Grundlage wurde daher die öffentliche, permissionless Blockchain Ethereum (www.ethereum.org) festgelegt.

Im Folgenden werden kompakt die Zielstellungen und Ergebnisse des Projektes vorgestellt.

2 ZIELSTELLUNG

Das genaue Verständnis der Anforderungen an das Management der digitalen Identität im Rahmen dieses Projektes wurde durch Zielstellungen eingegrenzt. Es ist hervorzuheben, dass es nicht der Anspruch war, ein vollständiges Identitätsmanagementsystem zu entwickeln. Vielmehr sollten grundlegende Funktionen abgebildet und prototypisch umgesetzt werden, um eine realistische Einschätzung der Eignung der Blockchain zu erhalten. Im Einzelnen waren die Ziele:

- Selbstregistrierung der Nutzer.
- Abbildung der Identität in der Ethereum-Blockchain.
- Umsetzung eines Authentisierungmechanismus für bereits registrierte Nutzer.
- Auffinden von anderen Nutzern.
- Hinterlegen von Identitätsmerkmalen (Attribute), z. B. das Geburtstadatum.
- Verfikation dieser Merkmale durch andere Nutzer des Systems, um das Vertrauen in die entsprechene Identität zu erhöhen.
- Umsetzung des gesamten Systems in Form einer Webanwendung.
- Beachtung der Konzepte einer Self-Sovereign Identity.

Darüber hinaus sollten auch nicht-funktionale Aspekte, wie eine hohe Nutzerfreundlichkeit und der Datenschutz Beachtung finden.

3 EIGNUNG DER BLOCKCHAIN

Im Rahmen des Projektes konnten grundlegende Erkenntnisse über den Einsatz der Blockchain-Technologie für die Umsetzung von digitalen Identitäten erarbeitet werden. Die Projektarbeit hat ergeben, dass die Blockchain und im speziellen Ethereum grundsätzlich dafür geeignet sind eine dezentrale digitale Identität umzusetzen.

Die offensichtlichen Eigenschaften der Blockchain-Technologie sind ihre Dezentralität, Offenheit, Sicherheit und Unveränderbarkeit. Dadurch werden grundlegende Anforderungen an eine digitale Identität erfüllt, ohne dass ein zentraler Dienstleister benötigt wird. Die eingebauten Sicherheitsmechanismen und kryptografischen Verfahren garantieren zudem die Integrität der Identität. Der Verzicht auf einen zentralen Dienstleister hat vielfältige Vorteile. Insbesondere entfallen datenschutzrechtliche Bedenken gegenüber genau diesen Dienstleistern. Das Vertrauen verlagert sich vom Dienstleister zur Technologie. Die Nutzer bekommen tatsächliche Kontrolle über ihre digitale Identität. Dadurch wird die Entwicklung einer Self-Sovereign Identity unterstützt.

Ethereum ist eine Blockchain der 2. Generation, also eine Weiterentwicklung des ursprünglichen Konzeptes, das durch die Kryptowährung Bitcoin etabliert wurde. Die Bitcoin-Blockchain ermöglicht in erster Linie die Speicherung von simplen Transaktionen, bei denen die virtuelle Währung von einem Nutzer A zu Nutzer B transferiert wird. Dahingegen ermöglicht Ethereum die Speicherung, Ausführung und Zustandsänderung von sogenannten Smart Contracts. Diese kleinen Softwareprogramme[2] können beliebige Datenstrukturen besitzen und Algorithmen ausführen und erlauben es dadurch vielfältige Funktionalitäten abzubilden. Die Ethereum-Blockchain kann folglich vereinfacht als ein verteilter Computer betrachtet werden.

Auf Basis von Smart Contracts ist es möglich eine digitale Identität zu definieren und in der Blockchain zur Verfügung zu stellen. Jeder Smart Contract verfügt über eine eindeutige Adresse, über die er gefunden und ausgeführt werden kann. Benötigte Attribute, Datenstrukturen und Funktionen können unproblematisch in einem Smart Contract definiert werden.

Alle Daten und Zustandsänderungen von Smart Contracts in Ethereum sind öffentlich einsehbar und werden an alle Knoten des Netzwerkes verteilt. Lediglich der Schreibzugriff kann im Rahmen eines Smart Contracts eingeschränkt werden. Eine Einschränkung des Lesezugriffs ist grundsätzlich nicht

[2] Die Programmiersprache der Ethereum-Smart Contracts heißt Solidity (www.solidity.readthedocs.io)

möglich. Dieser Umstand weist auf eine häufige Missdeutung der Blockchain-Technologie als Grundlage für ein Identitätsmanagementsystem hin:

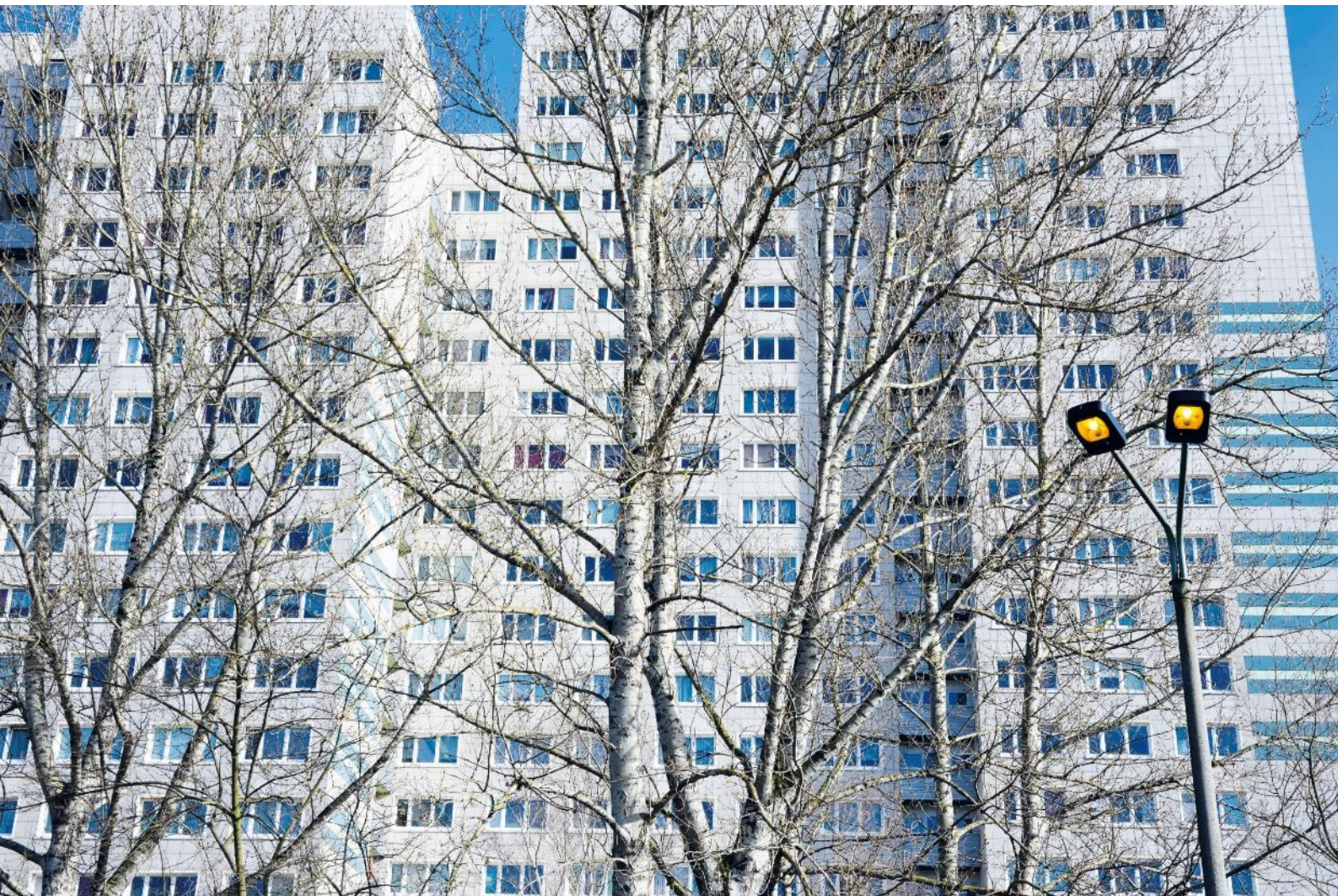
In einer öffentlichen Blockchain dürfen in keinem Fall sensible oder personen-bezogene Daten unmittelbar abgelegt werden.

Alle Daten, die in der Blockchain gespeichert werden, müssen entweder verschlüsselt oder absolut unsensibel sein. Hinzu kommt, dass von der Speicherung von größeren Datenmengen in der Blockchain grundsätzlich abzusehen ist. Die Blockchain ist ein verteiltes System und alle Daten werden über alle Knoten verteilt. Konzeptuell ist davon auszugehen, dass die Verteilung und Verarbeitung von größeren Datenmengen zu enormen Skalierungs- und Performanceproblemen führen wird. Im Fall von Ethereum treten diese Schwierigkeiten bereits auf.

Die eigentlichen Daten müssen daher auf einem gesonderten System gespeichert werden.

Die Zugriffskontrolle für dieses System muss dabei beim entsprechenden Besitzer der digitalen Identitäten liegen. Der Datenaustausch zwischen Nutzern muss entsprechend ebenfalls über dieses System abgewickelt werden.

Zusammengefasst bedeutet das, eine Blockchain kann nicht als alleiniges System zum Management von digitalen Identitäten eingesetzt werden. Vielmehr kann sie als dezentraler, nicht-manipulierbarer Einstiegspunkt zu einer digitalen Identität dienen. Zusätzlich können ganz bestimmte Informationen und Verweise dort hinterlegt werden. Im Rahmen dieses Projektes wurden die Ziele unter Berücksichtigung dieser Einschränkung umgesetzt. Im Folgenden wird die genaue Umsetzung erläutert.



4 ENTWURF UND UMSETZUNG

Der Entwurf und die Umsetzung waren grundsätzlich in zwei Teilaspekte untergliedert. Auf der einen Seite mussten die Smart Contracts zur Ausführung in der Ethereum-Blockchain entwickelt werden und zum anderen eine entsprechende Webanwendung, um den Nutzern Zugriff auf die Funktionalität zu geben und die persönlichen Daten zu verwalten.

4.1 WAS KOMMT IN DIE BLOCKCHAIN?

Die zentrale Funktionalität des Prototyps entsprechend der Zielstellung ist die Hinterlegung von persönlichen Attributen bzw. Merkmalen der digitalen Identität und die Verifikation dieser durch weitere Parteien. Typische Beispiele sind die Adresse, die Daten des Personalausweises oder Kreditkarteninformationen.

Wie bereits aufgeführt, ist es nicht möglich diese Daten unmittelbar in der Blockchain abzulegen. Stattdessen wird ein eindeutiger Hashwert, eine Art Fingerabdruck der Daten hinterlegt. Es ist nicht möglich aus diesem Wert die eigentlichen Daten wiederherzustellen. Dieser Wert kann dann von einer oder mehreren dritten Parteien verifiziert werden. Diese Verifikationen und die Zustimmung des Besitzers der digitalen Identität werden ebenfalls in der Blockchain abgelegt.

Konkret bedeutet das, dass in der Ethereum-Blockchain ausschließlich Bezeichner von Attributen, zugeordnete Hashwerte und Verifikationen dieser Hashwerte abgespeichert werden.

4.2 SMART CONTRACTS

Zunächst ist festzuhalten, dass die Nutzer der Ethereum-Blockchain für die Teilnahme im Netzwerk einen privaten und einen öffentlichen Schlüssel generieren. Es wird also ein asymmetrisches Verschlüsselungsverfahren zur Sicherung der Transaktionen eingesetzt. Zusätzlich werden den Teilnehmern persönliche Identifikationsnummern (Account-ID) zugeordnet, die von dem jeweiligen öffentlichen Schlüssel abgeleitet sind. Diese automatisch verfügbare Account-ID dient als eindeutiger Identifikator der digitalen Identität im Rahmen dieses Projektes.

Jede digitale Identität wird durch einen einzelnen Smart Contract (**Identity-Smart-Contract**) repräsentiert, der Variablen und Funktionen enthält, um die Zielstellung zu erfüllen. Die wichtigsten Variablen sind:

- Die Account-ID des Eigentümers, die den Smart Contract eindeutig einem Nutzer zuordnet. **(owner)**

- Eine Liste von Attributen, wo bei jedes Attribut über einen Schlüssel eindeutig identifiziert werden kann. Ein Attribut widerum ist eine Struktur und besteht u. a. aus Variablen für den Hashwert und Verifikationen für dieses Attribut. **(attributes)**

Die Anzahl an Variablen ist dementsprechend überschaubar und die Menge an Daten, die gespeichert werden entsprechend klein. Als eigentliche Schnittstelle zu dem Smart Contract dient eine Reihe von Funktionen. Diese ermöglichen es u. a. den schreibenden Zugriff auf die Variablen zu beschränken. Zum Beispiel dürfen bestimmte Operationen nur vom Eigentümer durchgeführt werden. Beispielhafte Funktionen sind:

- Hinzufügen eines neuen Attributes, das den Schlüssel (z. B. dateofbirth) und den Hashwert enthält. **(addAttribute)**
- Hinzufügen einer Verfikation für ein bestimmtes Attribut. Eine Verifikation muss vom Eigentümer der Indentität akzeptiert werden, bevor sie Gültigkeit hat. **(addVerification)**
- Bestätigung einer bestehenden Verifikation eines Attributes. **(acceptVerification)**
- Ein Attribut und alle assoziierten Verifikationen können gelöscht werden. Dabei ist festzuhalten, dass sich das nur auf den letzten Stand des Smart Contracts bezieht. Die Blockchain enthält auch alle zurückliegenden Stände. Ein echtes Löschen ist nicht möglich. **(removeAttribute)**

Jeder Smart Contract in der Ethereum-Blockchain hat eine eindeutige Adresse, analog zur Adresse eines Teilnehmers. Über diese Adresse kann der Smart Contract im Netzwerk gefunden und seine Funktionen aufgerufen werden. Sie könnte somit als zweite eindeutige Identifikationsnummer der digitalen Identität dienen. Jedoch müsste sie, wie schon das Schlüsselpaar, dafür vom Teilnehmer verwaltet werden. Daher wurde ein einzelner, globaler **Lookup-Smart-Contract** entwickelt, der eine Abbildung der Account-ID auf die entsprechende Adresse des Identity-Smart-Contract speichert. Der Lookup-Smart-Contract übernimmt die Funktion eines „zentralen" Registers aller Nutzer. Er ermöglicht die Umsetzung von weiteren Funktionalitäten, wie die Suche nach einem bestimmten Teilnehmer. Dafür enthält er zusätzlich zu der Account-ID einen frei wählbaren Nutzernamen. Auf Basis der Account-ID oder des Nutzernamens kann die digitale Identität eines Teilnehmers aus dem Ethereum-Netzwerk abgerufen werden.

Für die praktische Entwicklung und das Testen der Smart Contracts wurde ein eigenes, geschlossenes Testnetzwerk der Ethereum-Blockchain installiert. Eine Entwicklung auf dem Ethererum-Livesystem ist nicht ratsam, da dort echte Transaktionsgebühren anfallen. Zusätzlich wurde die Entwicklungs- und Testumgebung Truffle[3] zur Umsetzung eingesetzt.

Der Zugriff auf die Ethereum-Blockchain erfolgt über den direkten Zugriff auf einen Knoten des Netzwerkes. Grundsätzlich bestehen zwei Möglichkeiten auf einen solchen Knoten zuzugreifen. Entweder ein Teilnehmer installiert auf seinem System einen eigenen Knoten oder er greift auf einen entfernten, existierenden Knoten zu. Die erste Möglichkeit ist dabei die konsequentere, da es die Dezentralität und die Transparenz der Blockchain-Technologie widerspiegelt. Allerdings wird dabei die gesamte Blockchain auf das eigene System repliziert. Ende November 2017 betrug die Gesamtgröße der produktiven Ethereum-Blockchain über 400 GB.[4]

[3] www.truffleframework.com

[4] www.etherscan.io/chart/chaindatasizefull

4.3 DIE WEBANWENDUNG

Für die Erstellung und Nutzung der digitalen Identität in der Ethereum-Blockchain wurde im Rahmen des Projektes eine leichtgewichtige Webanwendung entwickelt. Sie erfüllt im Wesentlichen drei Aufgaben:

- Genereriung des Schlüsselpaars zur Teilnahme am Netzwerk.
- Nutzerfreundliche Abbildung, der durch die Smart Contracts zur Verfügung gestellten Funktionen, wie das Hinzufügen von Attributen und die Verfikation dieser.
- Sichere Speicherung der eigentlichen Daten der Identität.

Die Webanwendung wurde in Form eine Single-Page-Application auf Basis des Java Script Framework Vue.js[5] entwickelt. Der Zugriff auf die Ethereum-Blockchain erfolgt über eine fest definierte Schnittstelle[6], die jeder Knoten des Netzwerkes anbietet. Der Zugriff auf die Schnittstelle kann mit Hilfe verschiedener Softwarebibliotheken vereinfacht durchgeführt werden. Konkret wurde die web3.js[7] Bibliothek eingesetzt. Im Detail besitzt die Webanwendung folgende Funktionalitäten:

- Registrierung eines Nutzers mit Wahl eines Nutzernamens. Ber der Registrierung wird durch zufällige Bewegungen der Maus oder des Fingers hinreichend Entropie[8] generiert, um die Qualität der krypthografischen Schlüssel der Nutzer zu erhöhen.
- Der Registrierungsprozess führt zur Erstellung eines eindeutigen Schlüssels. Dieser Schlüssel muss vom Nutzer sicher verwahrt werden und wird zur erneuten Anmeldung bzw. Authentifizierung benötigt. Im Hintergrund wird für die Nutzer ein Identity-Smart-Contract der Blockchain hinzugefügt und seine Adresse und der Nutzername im Lookup-Smart-Contract hinterlegt. Die dezentrale digitale Identität wurde somit erfolgreich generiert.
- Nach der Registrierung haben die Nutzer die Möglichkeit ihrer Identität beliebige Attribute, wie das Geburtstdatum hinzufügen. Von diesen Attributen wird automatisch ein Hashwert erzeugt und dem Identity-Smart-Contract hinzugefügt. Damit liegt ein eindeutiger Fingerabdruck, unveränderbar in der Blockchain vor.
- Die zentrale Funktionalität des Prototyps ist die Verifikation von Attributen anderer Nutzer. Nutzer können auf Basis des Lookup-Smart-Contracts andere Nutzer finden und die jeweiligen Attribute und zugeordneten Hashwerte einsehen. Jedes Attribut kann dann individuell verifiziert werden. Jeder Verfikation kann dann widerum vom Eigentümer des Attributes angenommen oder abgelehnt werden.

4.4 DATENHALTUNG

Wie eingangs erläutert dient die Blockchain nicht der Speicherung und Übertragung der eigentlichen, unverschlüsselten Daten der digitalen Identität. Für diese Aufgabe muss ein weiteres System eingesetzt werden. Im Sinne einer Self-Sovereign Identity müssten die persönlichen Daten auf diesem System ebenfalls unter der vollen Kontrolle des Nutzers stehen. Die Erarbeitung von Lösungsansätzen für dieses Problem stellt eine separate Herausforderung dar. Häufig genannte Ansätze sind:

[5] www.vuejs.org
[6] www.github.com/ethereum/wiki/wiki/JSON-RPC
[7] www.github.com/ethereum/web3.js/
[8] www.de.wikipedia.org/wiki/Entropie_(Kryptologie)

- Eine ausschließlich lokale Speicherung der Daten auf dem Computer oder Smartphone des Nutzers.
- Die (verschlüsselte) Speicherung durch gängige Hosting- und Cloudanbieter.
- Einrichtung eines persönlichen Servers, zum Beispiel im eigenen Heimnetz.

Im Rahmen dieses Projektes wurde für diesen Zweck ein simpler Dienst zur Speicherung der Daten entwickelt, den die Nutzer bei der Registrierung auswählen kann. Das Vorhandensein einer sicheren Umgebung für die eigentlichen Daten (Datencloud) wird entsprechend nur simuliert.

4.5 VERIFIKATIONSPROZESS

Hervorzuheben ist, dass der eigentliche Prozess der Verifikation, also die tatsächliche Überprüfung, dass der Wert eines Attributes Gültigkeit hat, nicht Teil der Anwendung ist. Abbildung 1 illustriert wie der Verifikationsprozess abläuft, wobei nur die grauen Schritte die Blockchain involvieren. Will ein Nutzer beispielsweise sein Geburtsdatum verifizieren lassen, muss er zunächst diese Information im System abspeichern. Für dieses Projekt wird dafür die simulierte Datencloud verwendet.

Von dem Geburtsdatum wird dann ein eindeutiger Hashwert generiert und in der Blockchain gespeichert.

Für eine Verifikation muss dieser Hashwert nun überprüft werden. Diese Überprüfung findet unabhängig von der Anwendung und der Blockchain statt. Dafür muss einem anderen Nutzer des Systems der tatsächliche Nachweis über das Geburtsdatum vorgelegt werden. Im Idealfall ist dieser Nutzer dazu berechtigt Auskunft über die Richtigkeit des Geburtsdatums zu geben. Denkbar ist zum Beispiel, dass der Nutzer mit seinem Personalausweis zum Bürgeramt geht. Dort wird ebenfalls der Hashwert des Geburtsdatums ermittelt und mit dem bereits in der Blockchain abgespeicherten Wert verglichen. Sind die Hashwerte identisch, wird eine Verifikation dieses Attributes durch das Bürgeramt in der Blockchain hinterlegt. Das Bürgeramt ist dabei ebenfalls ein Nutzer des Systems.

Ein wichtiger Aspekt dabei ist, dass dem Bürgeramt-Nutzer Vertrauen entgegengebracht werden muss, damit die Verifikation einen Wert hat. Wie dieses Vertrauen entsteht, muss gesondert betrachtet werden. Eine einfache Lösung ist die Veröffentlichung des öffentlichen Schlüssels des Bürgeramt-Nutzers auf der offiziellen Webpräsenz des Bürgeramtes.

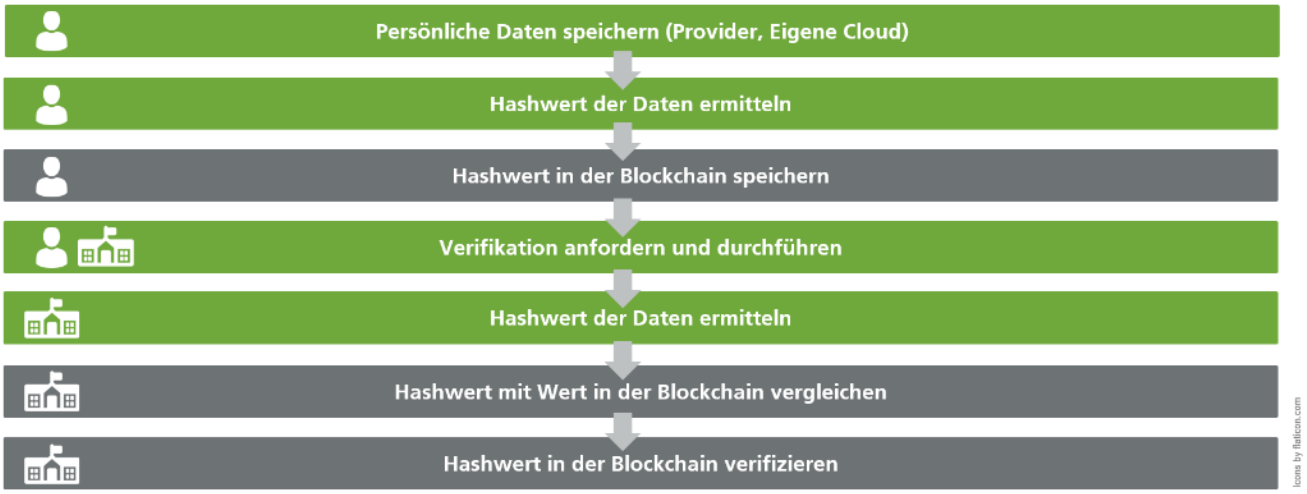


Abbildung 1 – Der Verifikationsprozess

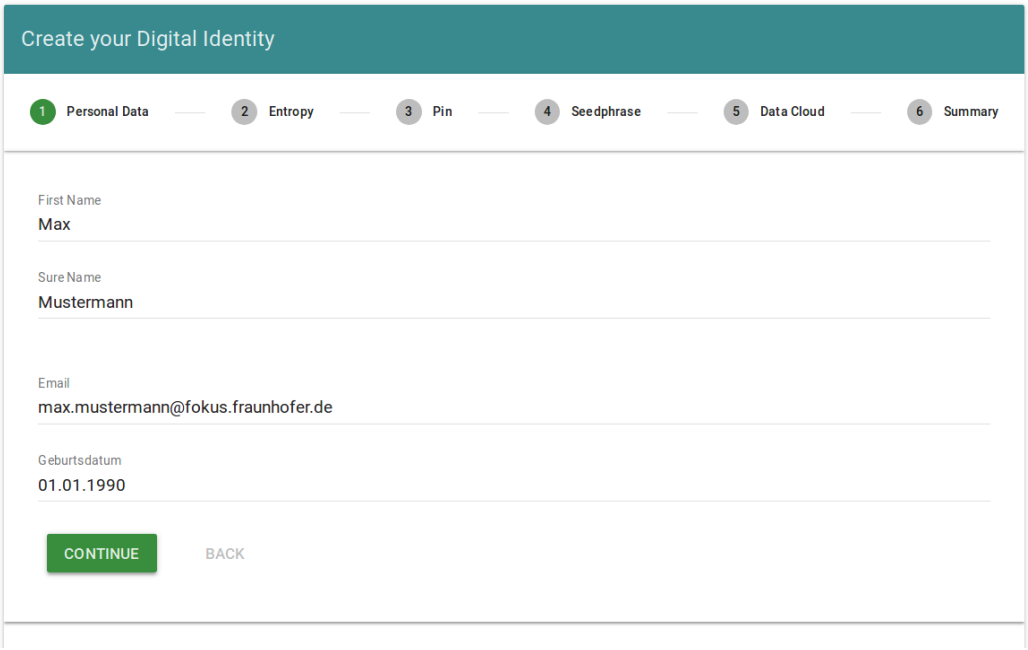


Abbildung 2 – Registrierungsprozess für eine digitale Identität

Zusammengefasst bedeutet das, dass die Blockchain in diesem Projekt lediglich als Vertrauensanker fungiert. Datenübertragung, Verifikation und Vertrauensbildung erfolgen unabhängig davon.

4.6 DER PRIVATE SCHLÜSSEL

Wie bereits angeführt verfügt jeder Teilnehmer der Ethereum Blockchain über ein Schlüsselpaar, bestehend aus privatem und öffentlichem Schlüssel. Dieser Aspekt ist eine zentrale Eigenschaft der Blockchain-Technologie und stellt eine Grundlage ihrer Sicherheit und Integrität dar. Das Schlüsselpaar dient der Authentisierung und der Authentifizierung des Nutzers.

Der öffentliche Schlüssel eines Teilnehmers ist allen anderen Nutzern bekannt, der private Schlüssel darf nur dem Nutzer selbst bekannt sein. Gerät der private Schlüssel in Besitz eines anderen Nutzers, ist die digitale Identität kompromittiert. Darüber hinaus ist es nicht mögliche die digitale Identität weiter zu nutzen, falls der private Schlüssel verloren geht. Der aktuelle Stand der Technik ermöglicht keine Wiederherstellung des Schlüssels. Es ist daher unabdingbar, dass der Nutzer seinen Schlüssel sicher verwahrt oder sich sogar einprägt. Der Schlüssel ist üblicherweise eine lange, kryptische Zeichenfolge. Allerdings gibt es kryptografische Verfahren, die eine Vereinfachung auf eine Wortkette, bestehend aus 12 englischen Wörtern ermöglichen: der sogenannte Seedphrase. Aus dieser Seedphrase kann jederzeit der eigentliche private Schlüssel wiederhergestellt werden. Ein beispielhafter Seedphrase folgt:

```
hint motion see hint honey ocean
start house car rain race cause
```

Im Rahmen dieses Projektes wurde dieses Verfahren angewendet und dem Nutzer wird seine Seedphrase nach der Registrierung präsentiert. Die sichere Speicherung wird dem Nutzer überlassen.

4.7 ZWISCHENFAZIT

Insgesamt bildet der Prototyp bestehend aus Smart Contracts, einer Webanwendung und einer Datencloud ein einfaches Nutzungsszenario für digitale Identitäten in der Blockchain ab und dient somit als

Vorlage, um mögliche Einsatzzwecke effektiv zu demonstrieren und Vor- und Nachteile der Blockchain im Kontext von digitalen Identitäten aufzuzeigen. Der Fokus liegt dabei auf einer pragmatischen Umsetzung und der Verifikation von persönlichen Daten.

Bei der Entwicklung wurde auf hohe Wiederverwendbarkeit und Interoperabilität geachtet, um eine Verbreitung der Lösung für andere Anwendungsfälle zu ermöglichen. Die Smart Contracts sind grundsätzlich unabhängig und ihre Funktionalitäten existieren unabhängig von einer bestimmten Clientimplementierung. Im Rahmen der Umsetzung der Webanwendung wurde eine JavaScript-Bibliothek für die Kommunikation mit den konkreten Smart Contracts entwickelt. Diese Bibliothek kann unabhängig von der Webanwendung eingesetzt werden. Somit ist es möglich weitere Webanwendungen, zum Beispiel zur Abbildung weiterer Anwendungsfälle, zu entwickeln.

Die beschriebene Anwendung wurde im Laufe des Projektes ausschließlich mit dem Ethereum Testnetzwerk (www.testnet.etherscan.io/) betrieben. In diesem Netzwerk fallen keine Transaktionskosten an. Teilnehmer können sich die zugrundeliegende Kryptowährung Ether umsonst gutschreiben lassen. Die Schnittstellen unterscheiden sich nicht von denen des Produktivnetzwerkes, daher ist eine Migration dorthin problemlos möglich.

5 ERGEBNISSE UND EVALUATION

Im Rahmen des Projektes konnten wertvolle theoretische und praktische Erkenntnisse über digitale Identitäten in der Blockchain, im Speziellen in der Ethereum-Blockchain gesammelt werden. Grundsätzlich ist festzuhalten, dass Blockchain-Technologie im Aufbau von dezentralen, sicheren Identitätsmanagementsystemen, insbesondere im Hinblick auf das Konzept der Self-Sovereign Identity, eine zentrale Rolle spielen kann.

Das beschriebene Verfahren kann als vielversprechender Ansatz für die sichere Bestätigung von Merkmalen einer dezentralen digitalen Identität gesehen werden. Domänen- und systemübergreifende Prozesse können deutlich vereinfacht und effektiver gestaltet werden. Beispielsweise ist es denkbar, ein und dieselbe digitale Identität bei verschiedenen Diensten einzusetzen. Verifikationsprozesse (z. B. von Ausweisdokumenten) müssen im Idealfall nur noch einmalig durchgeführt werden. Das setzt voraus, dass sich Prozesse für den eigentlichen Beweis der Richtigkeit etablieren. Diese Prozesse sind zunächst unabhängig von der Blockchain und das Vertrauen in diese Prozesse entsteht durch das Vertrauen in die beteiligten Parteien als solche. Das bedeutet, dass der Verzicht auf zentrale Instanzen, die Vertrauen schaffen, nicht möglich ist.

Es zeigt aber auch, die Blockchain kann ihre Stärken und einzigartigen Eigenschaften nur im Zusammenwirken mit anderen Technologien und Verfahren ausspielen. Dazu zählen u. a. Methoden zum sicheren Austausch der eigentlichen Daten und standardisierte Prozesse zur Generierung von Hashwerten. Die Blockchain agiert nur als eine vertrauensschaffende Schicht – ein Single-Point-of-Truth.

Im Folgenden werden konkrete Hürden und Schwierigkeiten detailliert erläutert.

5.1 TRANSAKTIONSKOSTEN

Schreibende Operationen in der Ethereum-Blockchain verursachen Kosten für den Nutzer. Diese entstehen durch die rechenintensive Erstellung neuer Blöcke, verursacht durch den Mechanismus zur Konsensbildung Proof-of-Work, der durch die sogenannten Miner durchgeführt wird. Zusätzlich hat sich die zugrundeliegende Kryptowährung Ether durch die steigende Verbreitung und Nutzung der Ethereum-Blockchain zu einem Spekulationsobjekt entwickelt, was die Kosten der Nutzung weiter nach oben treibt. Hier greifen klassische Angebot und Nachfrage-Mechanismen. Diese Transaktionskosten wurden im Rahmen des Projektes untersucht und für die Erstellung der digitalen Identität konkret beziffert. Dabei ergab sich zunächst eine starke Schwankung der

Kosten, verursacht durch die täglichen Kursschwankungen des Ethers. Die Kosten für die Erstellung der digitalen Identität inklusive Hinzufügen eines Hashwertes und einer Verifikation schwankte im Laufe des Projektes zwischen 1 und 60 Euro. Zum Zeitpunkt November 2017 lagen die Kosten dafür bei ca. 15 Euro. Das Hinzufügen eines weiteren Hashwertes und einer Verifikation liegt bei ca. 2 Euro. Es ist davon auszugehen, dass der durchschnittliche Nutzer diese Preise als zu hoch empfinden wird. Zudem ist eine Stabilität der Preise nicht gewährleistet.

5.2 LATENZ

Die Blockchain ist ein verteiltes System. Die Daten müssen in Blöcke geschrieben und über das Netzwerk verteilt werden. In der Ethereum-Blockchain wird ca. alle 30 Sekunden ein neuer Block erstellt. Bis zur Bestätigung einer Transaktion an einem konkreten Knoten können mehrere Minuten vergehen. Das bedeutet, dass die Nutzer bei schreibenden Operationen, mit Verzögerungen und Wartezeiten rechnen müssen. Das widerspricht der gängigen Erwartungshaltung an moderne Anwendungen und wird die Akzeptanz eines solchen Systems verringern. Zudem existieren bisher noch Skalierungsprobleme von öffentlichen Blockchains. Die Latenz wird sich entsprechend erhöhen, umso mehr Teilnehmer das Netzwerk hat.

5.3 USABILITY

Die Identifikation innerhalb der Blockchain erfolgt auf Basis eines privaten-öffentlichen Schlüsselpaars. Wie bereits erläutert ist es notwendig, dass die Nutzer den privaten Schlüssel bzw. die Seedphrase sicher verwahren. Es ist davon auszugehen, dass der Umgang damit für die meisten Nutzer schwer zu bewältigen ist bzw. etablierte Lösungen (Email/Passwort) deutlich verständlicher sind. Darüber hinaus erhöht sich die Komplexität des gesamten Identitätsmanagementsystems durch den Einsatz der Blockchain. Waren die Nutzer bisher mit einem einheitlichen zentralen Dienst konfrontiert, muss nun ein Verständnis für die Dezentralität und die Aufgaben der Teilsysteme aufgebaut werden.

5.4 DEZENTRALITÄT

Das umgesetzte System setzt an vielen Stellen weiterhin auf zentrale Dienste auf. Die Webanwendung und Datencloud werden zentral betrieben. Die Größe der Ethereum-Blockchain ermöglicht in den meisten Fällen keine Installation eines vollständigen Knotens. Daher muss auch hier auf einen zentral verfügbaren Knoten ausgewichen werden. Für die Speicherung der Seedphrase bieten sich zentrale Dienste, wie Dropbox etc. an. Eine echte Dezentralität ist derzeit technisch noch nicht umsetzbar. Weiterhin ermöglicht der Einsatz zentraler Dienste und Systeme eine Vereinfachung in der Umsetzung und eine substantielle Erhöhung der Nutzerfreundlichkeit.

5.5 DATENSCHUTZ

Datenschutzrechtliche Bedenken spielen ebenfalls eine Rolle. Im Rahmen der Europäischen Datenschutzgrundverordnung wurde das „Recht auf Vergessen“ festgesetzt. Dieses Recht ist in der Blockchain nicht unmittelbar umsetzbar. Daten in der Blockchain können nicht gelöscht werden. Inwieweit zum Beispiel Hashwerte davon betroffen sind, muss weiter untersucht werden. Darüber hinaus müssen weitere datenschutzrechtliche Überlegungen auf das gesamte System angewendet werden, die weitere Forschung erfordern.

6 AUSBLICK UND EMPFEHLUNGEN

Die aufgezeigten Ergebnisse stellen nur einen Ausschnitt der vielen Möglichkeiten und Hürden der Nutzung der Blockchain für digitale Identitäten dar. Durch die Komplexität und der Verfügbarkeit weiterer Blockchain-Systeme und verteilter Datenmanagementsysteme können vielfältigste Charakteristiken auftreten. Grundsätzlich ist aber festzuhalten, dass die Blockchain einen zentralen Eckpfeiler bei der Umsetzung von zukünftigen digitalen Identitäten einnehmen kann. Insbesondere die Möglichkeit auf zentrale Instanzen zu verzichten, stellt einen wichtigen Schritt in Richtung echter Datensouveränität dar. Festzuhalten ist aber, dass ein sofortiger, weitreichender Einsatz kurzfristig noch unwahrscheinlich ist.

Dabei muss die Arbeit auf vielfältigen Ebenen fortgesetzt werden. Dafür ist die Einbeziehung aller potentiellen Akteure, wie der Endnutzer, die Technologieentwickler und vertrauensbildende Organisationen notwendig. Sie alle müssen aktiv bei der Ausgestaltung und Untersuchung von Einsatzmöglichkeiten beteiligt sein. Unmittelbare Handlungsempfehlungen folgen:

- Für einen nachhaltigen und weitreichenden Einsatz einer öffentlichen Blockchain müssen sich diese Kosten stabilisieren. Entsprechende Lösungen werden bspw. von der Ethereum Community bereits erprobt. Alternative Konsensmechanismen wie Proof-of-Stake befinden sich in der Entwicklungs- und Testphase.
- Die grundlegenden Perfomance- und Skalierungsprobleme müssen gelöst werden. Auch hier befinden sich neue Konzepte bereits in der Entwicklung. Zum Beispiel die Verteilung auf mehrere parallele Blockchains.
- Die Usabiltiy, insbesondere die Verwaltung des privaten Schlüsselns muss optimiert und vereinfacht werden, um eine weitreichende Akzeptanz zu ermöglichen. Auch hier befinden sich Konzepte in der Entwicklung. Vom Speichern des Schlüssels auf spezieller Hardware bis zur Verteilung des Schlüssels auf weitere vertrauenswürdige Instanzen.
- Für die Speicherung und den Austausch der eigentlichen Daten müssen vertrauenswürdge Verfahren und Systeme etabliert werden, die dem Anspruch an Datensouveränität und Sicherheit gerecht werden.
- Um eine Nutzung der digitalen Identität von verschiedenen Parteien zu ermöglichen, ist die Entwicklung von standardisierten Prozessen und Methoden notwendig. Beispielsweise um den

Verifikationsprozess über Domänengrenzen hinweg einzusetzen. Die Ethereum Community arbeitet bspw. an entsprechenden Standardisierungen (www.github.com/ethereum/EIPs).

- Der grundsätzliche Reifegrad der Blockchain-Technologie und des dazugehörigen Softwareökosystems muss sich erhöhen, um für einen echten Produktiveinsatz verwendbar zu sein.
- Der unmittelbare nächste Schritt sollte die Förderung und Durchführung von konkreten Pilotprojekten unter Einbeziehung aller Akteure sein, um die technologische und institutionelle Entwicklung der digitalen Identität in der Blockchain zu unterstützen. Insbesondere etablierte, vertrauenswürdige Identitätsprovider, wie der Staat, müssen ihre Rolle als zukünftiger Verifikationsanbieter prüfen.

7 WEITERE PROJEKTE

Die in diesem Projekt angewendeten Konzepte und Verfahren, werden von zahlreichen weiteren Projekten angewendet und erprobt. Verbreitete Lösungen folgen:

- **uPort** ist eine dezentrales Identitätsmanagementsystem auf Basis der Ethereum-Blockchain. Das zentrale Konzept ist, dass der private Schlüssel auf dem Smartphone des Nutzers hinterlegt wird. Der private Schlüssel verbleibt auf dem Smartphone und ist nicht sichtbar für den Nutzer. Für Login-Prozesse in Webanwendungen werden QR-Codes verwendet. Für die Speicherung der eigentlichen Daten kann Amazon Web Services oder Microsoft Azure eingesetzt werden. (www.uport.me)

- **Blockstack** ist eine Sammlung von Open Source Komponenten, um dezentrale Anwendungen zu entwickeln und zu betreiben. Das System besteht aus verschienden Schichten und Diensten u. a. auch für digitale Identitäten. Es baut momentan auf Bitcoin auf und bietet persönliche Profile mit privaten und öffentlichen Informationen und einem eindeutigen Namen. Blockstack ist das populärste Identitätsmanagementsystem auf Basis von Blockchain mit mehr als 50.000 Registrierungen. (www.blockstack.org)

- **Sovrin** ist ein Identitätsnetzwerk auf Basis einer geschlossenen, öffentlichen Blockchain. Der Konsensmechanismus wird von der Non-Profit-Organisation Sovrin kontrolliert und als Plenum Consensus Protocol bezeichnet. Teilnehmer haben in der Regel mehrere Identitäten, um Korrelationen von persönlichen Daten zu vermeiden. Eine digitale Identiät wird über einen krypthografischen Schlüssel definiert. Das System ermöglicht die Verfikation von Attributen und Beziehungen. (www.sovrin.org)

- **Aevatar** ist eine Self-Sovereign Identity auf Basis verschiedener Blockchains, u. a. Bitcoin und Ethereum. Das Projekt gibt an den Richtlinien der Datenschutzgrundverordnung zu entsprechen. Der praktische Einsatz erfolgt auf Basis einer mobilen Anwendung. Es unterstützt Verifikationen und verfügt über eine Wiederherstellungsfunktion. (www.aevatar.com)

KONTAKT

Fabian Kirstein
Digital Public Services (DPS)
Tel.: +49 30 3463-7718

Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de/de/dps/themen/digitaleidentitaeten
www.blockchain-werkstatt.de
Twitter: @fraunhoferfokus, @fokuspublic