Bayerisches Staatsministerium für Digitales

Bayerisches Landesamt für Steuern

Fraunhofer FIT
Projektgruppe Wirtschaftsinformatik

FAU

mgm

SSI@LfSt

Einsatz der Blockchain-Technologie in der Steuerverwaltung

EINSATZ DER BLOCKCHAIN-TECHNOLOGIE IN DER STEUERVERWALTUNG

Autoren

Bayerisches Landesamt für Steuern:

Dr. Daniela Kühne, Sabrina Schön

Fraunhofer FIT:

Tobias Guggenberger, Vincent Schlatt, Dr. Nils Urbach

Friedrich-Alexander-Universität Erlangen-Nürnberg:

Dr. Roland Ismer, Quirin Jackl

mgm technology partners:

Stefan Hauffe, Dr. Hans Huber, Ansgar Knipschild, Guido Wischrop

Die Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT vereint die Forschungsbereiche Finanz- und Informationsmanagement in Augsburg und Bayreuth. Die Expertise an der Schnittstelle von Finanzmanagement, Informationsmanagement und Wirtschaftsinformatik sowie die Fähigkeit, methodisches Know-how auf höchstem wissenschaftlichem Niveau mit einer kunden-, ziel- und lösungsorientierten Arbeitsweise zu verbinden, sind ihre besonderen Merkmale.

Fraunhofer-Institut für Angewandte Informationstechnik FIT
Projektgruppe Wirtschaftsinformatik
Wittelsbacherring 10
95444 Bayreuth

Das Bayerische Landesamt für Steuern (BayLfSt) ist eine Landesbehörde des Freistaats Bayern im Geschäftsbereich des Bayerischen Staatsministeriums der Finanzen und für Heimat.

Bayerisches Landesamt für Steuern
Sophienstr. 6
80333 München

Danksagungen

Die Autoren danken Lars Wolf und Jens Stoetzer von der Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT für die Unterstützung bei der Anfertigung des White Papers.

Haftungsausschluss

Dieses White Paper wurde vom Fraunhofer-Institut für Angewandte Informationstechnik FIT nach bestem Wissen und unter Einhaltung der nötigen Sorgfalt erstellt.

Fraunhofer FIT, seine gesetzlichen Vertreter und/oder Erfüllungsgehilfen übernehmen keinerlei Garantie dafür, dass die Inhalte dieses White Papers gesichert, vollständig für bestimmte Zwecke brauchbar oder in sonstiger Weise frei von Fehlern sind. Die Nutzung dieses White Papers geschieht ausschließlich auf eigene Verantwortung.

In keinem Fall haften das Fraunhofer FIT, seine gesetzlichen Vertreter und/oder Erfüllungsgehilfen für jegliche Schäden, seien sie mittelbar oder unmittelbar, die aus der Nutzung des White Papers resultieren.

Empfohlene Zitierweise

Guggenberger, T., Hauffe, S., Huber, H., Ismer, R., Jackl, Q., Knipschild, A., Kühne, D., Schlatt, V., Schön, S., Urbach, N., Wischrop, G. 2020. SSI@LfSt: Einsatz der Blockchain-Technologie in der Steuerverwaltung. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT.

Bildquellen

SSI@LfSt

Einsatz der Blockchain-Technologie in der Steuerverwaltung

White Paper der Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT

Bayerisches Landesamt für Steuern 2020

Kurzfassung

Das nachfolgend dargestellte Forschungsprojekt umfasste die Konzeptionierung, prototypische Umsetzung und Evaluation eines Blockchain-basierten Systems zur Vermeidung von Steuerausfällen auf Online-Marktplätzen. Dabei werden zunächst die bestehenden Prozesse analysiert und Verbesserungspotenziale identifiziert. Der aktuell genutzte, papierbasierte Prozess weist wesentliche Ineffizienzen durch Medienbrüche und Fälschungsmöglichkeiten auf.

Nach gründlicher Evaluation verschiedener Lösungsansätze wird abschließend auf eine SSI-basierte Steuer-ID gesetzt. Hierbei werden – ähnlich den papierbasierten Prozessabläufen – digitale Nachweise über die steuerliche Registrierung an Händler ausgegeben. Diese können dann mittels einer digitalen Geldbörse Beweise über ihre Registrierung und Stammdaten an die Marktplätze geben. Diese Beweise enthalten auch den Status der Gültigkeit ihrer Registrierung, der über einen Indikator auf einer öffentlichen Blockchain geprüft werden kann. Die Kommunikation findet größtenteils über eine bilaterale Verbindung zwischen den beteiligten Parteien (Finanzbehörden und Onlinehändler, Onlinehändler und Marktplätze) statt.

Aufbauend auf diesem Konzept ist ein entsprechender Prototyp entwickelt worden, der das System technisch umsetzt. Der Prototyp dient hierbei als Machbarkeitsbeweis der konzipierten Lösung und stellt weiterhin wichtige Erkenntnisse für die Evaluation und zur Umsetzung möglicher Produktivsysteme.

Die Evaluation der angedachten Lösung wird abschließend aus rechtlicher, ökonomischer und technischer Perspektive vorgenommen. Einige technische Hürden, zum Beispiel hinsichtlich der Skalierbarkeit, der eingeschränkten Funktionalitäten aktueller Infrastrukturen zur Verwaltung von Nachweisen, sowie die geringe Anzahl technischer Anbieter, scheinen sich hinsichtlich der fortschreitenden Entwicklung und Forschungsvorhaben auf dem Gebiet SSI potenziell lösen zu lassen. Es kann gezeigt werden, dass bereits der Prototyp aber zuletzt auch das Konzept weitreichende Vorteile in dem betrachteten Steuerprozess liefern können. Vor allem hinsichtlich der Erweiterungsmöglichkeit auf andere steuerliche und nicht-steuerliche Vorgänge könnte ein SSI-basiertes System große Synergien schaffen.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Motivation

1. Motivation

Die fortschreitende Digitalisierung stellt die Finanzverwaltung vor die Herausforderung, mit der technologischen Entwicklung Schritt zu halten und die sich hieraus ergebenden Chancen für eine weitere Modernisierung des Besteuerungsverfahrens effektiv und effizient zu nutzen. Eine Herausforderung bringt dabei die wachsende Bedeutung von Internetplattformen mit sich, die zur Anbahnung von Offline-Umsätzen genutzt werden. Händler bieten ihre Waren im Inland an, kommen aber unter Umständen ihren steuerlichen Pflichten nicht nach, wodurch von erheblichen Steuerausfällen auszugehen ist. Der Gesetzgeber hat auf diese Situation mit der Einführung von Aufzeichnungspflichten für Betreiber elektronischer Marktplätze reagiert. Betreiber werden dazu verpflichtet, eine Bescheinigung über die steuerliche Erfassung der Unternehmer einzuholen, die auf ihren Marktplätzen tätig werden. Die Bescheinigung muss vom Onlinehändler beim zuständigen Finanzamt beantragt werden. Gegenwärtig erfolgen Antragstellung und Ausstellung der Bescheinigung in Papierform. Mit Hilfe der Regelung sollen Marktteilnehmer im Bereich des E-Commerce zur steuerlichen Registrierung bewegt werden, um Kenntnis von ihnen und Informationen über ihre Identität zu erlangen sowie eine Überwachung zu ermöglichen. Es ist deshalb für die Steuerverwaltung von Interesse, ein Identifikationsmerkmal für Onlinehändler zu schaffen, mit dem diese ihre steuerliche Registrierung nachweisen und das sie an die Betreiber von Internetplattformen übergeben können.

Um die Grundlagen für eine Effizienzsteigerung im beschriebenen Prozess zu schaffen, wurde vom Bayerischen Landesamt für Steuern (BayLfSt) mit Unterstützung des Bayerischen Staatsministeriums für Digitales (StMD) und in Zusammenarbeit mit ausgewählten Forschungseinrichtungen und Technologiepartnern ein Forschungsprojekt initiiert, welches zum Ziel hatte, die Möglichkeiten der Entwicklung eines elektronischen Verfahrens unter Verwendung der Blockchain-Technologie zu eruieren. Es soll ausgelotet werden, ob ein Blockchain-basierter Ansatz Möglichkeiten zur Antragstellung, zur Ausstellung der Bescheinigung und zur Gültigkeits- bzw. Statusprüfung durch die Marktplatzbetreiber bieten kann. Übergeordnetes Ziel des Projekts ist es, durch eine umfassende Auseinandersetzung mit der Thematik qualifizierte Aussagen über Einsatzmöglichkeiten der Blockchain-Technologie auch in anderen Bereichen des Besteuerungsverfahrens bzw. in anderen Verwaltungsverfahren treffen zu können.

Abstrahiert vom Gesetzeswortlaut soll folgende Situation analysiert und ein Lösungskonzept erarbeitet werden: Beteiligt ist (1) die zuständige Finanzbehörde (bzw. ELSTER), die dem Steuerpflichtigen auf elektronischem Weg eine Bescheinigung ausstellt, die ein Merkmal oder eine Information enthält. Beteiligt ist weiterhin (2) ein Steuerpflichtiger bzw. Marktteilnehmer im E-Commerce, der die Bescheinigung über das Merkmal oder die Information beantragt, die dafür nötigen Voraussetzungen nachweist und die Bescheinigung nach Ausstellung entgegennimmt. Es ist davon auszugehen, dass es sich beim Inhalt der Bescheinigung um ein Merkmal oder eine Information handeln sollte, die den Steuerpflichtigen zu einer Handlung berechtigt bzw. dessen Nachweis dem Steuerpflichtigen einen Vorteil verschafft, da dieser die Erbringung des Nachweises möglicherweise selbst initiieren soll. Zuletzt ist (3) eine weitere Partei beteiligt, für die das Merkmal bzw. die Information von Interesse ist. Die Drittpartei muss ggf. im Nachhinein nachweisen können, dass und wann sie den Nachweis eingefordert und erhalten hat. Der Nachweis des Merkmals soll nicht mehr geführt werden können, wenn die Voraussetzungen beim Steuerpflichtigen bzw.

Marktteilnehmer nicht mehr vorliegen oder das Merkmal aus anderen Gründen nicht mehr vorhanden ist. In diesem Fall soll der Status der Bescheinigung auf „ungültig“ gesetzt werden können. Die Regeln, die bspw. durch Gesetz für die Gültigkeit bzw. Ungültigkeit der Bescheinigung gelten, müssen umgesetzt werden können.

Das Forschungsprojekt dient vornehmlich dem Sammeln von Erfahrungen mit der Blockchain-Technologie zur Abbildung von Prozessen und zur Effizienzsteigerung in der Steuerverwaltung. Insbesondere sollen Möglichkeiten des Identitätsmanagements mit Hilfe der Blockchain-Technologie untersucht und ein Ausblick auf weitreichendere Einsatzmöglichkeiten im Bereich Tax Compliance gegeben werden. Grundsätzliche rechtliche Fragestellungen im Zusammenhang mit dem Einsatz der Blockchain-Technologie in der öffentlichen Verwaltung sollen zudem adressiert werden. Dies umfasst die Klärung von Fragen rund um den Datenschutz sowie das Steuergeheimnis.

Dieses White Paper ist wie folgt aufgebaut. Zunächst wird die derzeitige umsatzsteuerliche Situation aufgezeigt, um anschließend die daran anknüpfenden Prozesse zu analysieren. Aufbauend auf diesen Informationen werden in den nächsten Kapiteln die technischen Grundlagen der Blockchain sowie des Konzepts der SSI erläutert und Anforderungen an mögliche Lösungsansätze erhoben. Daran anknüpfend werden verschiedene Lösungsideen vorgestellt und eine explizite Konzeption ausgearbeitet. In den darauffolgenden Kapiteln wird der dem Lösungskonzept zu Grunde liegende Prototyp beschrieben, bevor abschließend die Evaluation beschrieben und mit einem Fazit geschlossen wird.

2 Rechtliche Situation

2. Rechtliche Situation

Die Nutzung von Internetplattformen ermöglicht es Unternehmern unabhängig von ihrer Ansässigkeit, auf dem inländischen Markt aufzutreten und inländische bzw. in anderen EU-Mitgliedstaaten ansässige Endverbraucher als Kunden zu gewinnen. Dies verändert nicht nur die wirtschaftlichen Rahmenbedingungen für inländische und ausländische Unternehmen, es stellt auch die an das Territorialitätsprinzip gebundene nationale Steuerverwaltung vor neue Herausforderungen. Risiken für das Steueraufkommen ergeben sich unter anderem im Zusammenhang mit der Besteuerung der Umsätze von Unternehmen, die zur Anbahnung von Offline-Umsätzen die Vermittlungsdienste von Internetplattformen in Anspruch nehmen. Steuerausfälle in diesem Bereich sind auf mangelnde Möglichkeiten der Identifikation der Anbieter und auf mangelnde Zugriffsmöglichkeiten insbesondere auf Anbieter aus Drittstaaten zurückzuführen.

Kommt es zu einer Steuerpflicht im Inland, so ist der Drittlandsunternehmer nach derzeitiger Gesetzeslage verpflichtet, sich beim zuständigen Finanzamt registrieren zu lassen und Umsatzsteuererklärungen abzugeben. Risiken für das Steueraufkommen ergeben sich zum einen bei der Einfuhr in die Europäische Union, wenn Drittlandshändler Warenwerte bewusst zu niedrig deklarieren. Zum anderen ist davon auszugehen, dass eine Vielzahl von im Onlinehandel tätigen Drittlandsunternehmern ihrer Verpflichtung zur steuerlichen Erfassung im Inland nicht nachkommt. Das Risiko einer Entdeckung durch die Finanzverwaltung ist dabei bisher als gering einzustufen. Jedoch kann selbst bei Registrierung des Unternehmers eine Durchsetzung der Steueransprüche nicht immer gewährleistet werden. In der Konsequenz ist die Gleichmäßigkeit des Steuervollzugs gefährdet und es entstehen Wettbewerbsverzerrungen, durch die korrekt handelnde in- und ausländische Unternehmen benachteiligt werden.

Der Gesetzgeber hat auf diese Situation mit der Einführung von Aufzeichnungspflichten für Marktplatzbetreiber reagiert. Betreiber elektronischer Marktplätze werden verpflichtet, Informationen über die Identität der Unternehmer aufzuzeichnen, deren Lieferungen auf den von ihnen bereitgestellten Marktplätzen rechtlich begründet werden. Zur Erfüllung der Aufzeichnungspflichten ist von den Marktplatzbetreibern eine Bescheinigung über die steuerliche Erfassung der Unternehmer einzuholen, welche wiederum von diesen beim zuständigen Finanzamt beantragt werden muss. Es ist davon auszugehen, dass Onlinehändler einen Rechtsanspruch auf Erteilung der Bescheinigung haben, soweit sie steuerlich als Unternehmer registriert sind. Kann der Marktplatzbetreiber die Bescheinigung über die steuerliche Erfassung des Unternehmers nicht vorlegen, ist eine Exkulpation aus der Haftung für die nicht entrichtete Steuer aus Lieferungen des Unternehmers, die auf dem Marktplatz begründet worden sind, nicht möglich. Ebenfalls haftet der Marktplatzbetreiber, wenn zwar eine gültige Bescheinigung vorliegt, er aber Kenntnis davon hatte oder nach der Sorgfalt eines ordentlichen Kaufmanns hätte haben müssen, dass der Unternehmer seinen steuerlichen Verpflichtungen nicht oder nicht in vollem Umfang nachkommt. Zudem verfügt die Finanzverwaltung über das Instrument der Mitteilung über die steuerliche Unzuverlässigkeit. Bestehen Anhaltspunkte, dass der Onlinehändler seinen steuerlichen Pflichten nicht oder nicht im wesentlichen Umfang nachkommt, kann das zuständige Finanzamt den Marktplatzbetreiber darüber informieren, wenn andere Maßnahmen keinen unmittelbaren Erfolg versprechen. Der Marktplatz muss innerhalb der vom Finanzamt gesetzten Frist nachweisen, dass der Onlinehändler keine Waren mehr anbieten kann, andernfalls haftet er für die Steuer auf Umsätze, die nach Zugang der Mitteilung auf dem Marktplatz begründet worden sind. Im Falle von als Privatperson registrierten Händlern kann zudem eine Haftung eintreten, wenn der Marktplatzbetreiber

nach Art, Menge oder Höhe der erzielten Umsätze Kenntnis davon hatte oder hätte haben müssen, dass die Umsätze im Rahmen eines Unternehmens erbracht werden.

Durch die Einführung der Haftungsregelung sollen Marktplatzbetreiber dazu angehalten werden, nur mit Onlinehändlern zu kooperieren, die ihren Compliance-Verpflichtungen nachkommen. Von der Regelung wurde vor allem eine Präventivwirkung sowie eine Registrierungswelle erwartet, die der Finanzverwaltung einen Erkenntnisgewinn über die Identität der auf Marktplätzen handelnden Unternehmer liefert. Das Gesetz ist grundsätzlich geeignet, zur Sicherung des Steueraufkommens und der Gleichmäßigkeit der Besteuerung beizutragen und bestehende Wettbewerbsverzerrungen einzudämmen. Bei Ausgestaltung der Umsetzung ist jedoch besonderes Augenmerk darauf zu legen, dass es Onlinehändlern und Marktplätzen unbürokratisch ermöglicht wird, ihren Compliance-Verpflichtungen nachzukommen. Komplizierte, arbeitsaufwändige oder ineffiziente Verfahren dürfen einer beabsichtigten Steuerehrlichkeit nicht entgegenstehen.

3 Prozessanalyse

3. Prozessanalyse

Bevor ein innovatives System zur vorteilhaften Umsetzung des Bescheinigungsverfahrens erarbeitet werden kann, muss zunächst das bestehende Verfahren analysiert werden. Onlinehändler beantragen aktuell ein Papierdokument, das ihnen bescheinigt, als Unternehmer steuerlich erfasst zu sein. Der Antrag ist schriftlich, per Post oder E-Mail zu stellen, wozu ein Vordruckmuster verwendet werden kann. Der Antrag kann jedoch auch formlos gestellt werden. Im Antrag sind Angaben zur Identität des Onlinehändlers (Name, Anschrift, Telefonnummer, etc.) sowie verschiedene weitere Informationen (ggf. Name und Anschrift des steuerlichen Vertreters; ggf. Name und Anschrift des inländischen Empfangsbevollmächtigten; freiwillige Angabe zu den elektronischen Marktplätzen auf denen der Onlinehändler tätig werden will und Identifikationsmerkmal des Händlers auf diesen Marktplätzen) enthalten.

Nach Eingang des Antrags werden im zuständigen Finanzamt die Voraussetzungen für die Erteilung einer Bescheinigung geprüft. Der Antragsteller muss zum einen für Zwecke der Umsatzsteuer steuerlich erfasst sein. Verfügt der Antragsteller nicht über einen Wohnsitz oder gewöhnlichen Aufenthalt, Sitz oder Geschäftsleitung im Inland oder in einem anderen Mitgliedstaat der Europäischen Union oder einem Staat, auf den das Abkommen über den Europäischen Wirtschaftsraum anwendbar ist (derzeit: Norwegen), muss zum anderen spätestens bei Antragstellung ein inländischer Empfangsbevollmächtigter benannt werden. Liegen die Voraussetzungen vor, wird die Bescheinigung in Papierform erteilt.

Für alle Bescheinigungen, die derzeit ausgestellt werden, wird das Ende der Gültigkeit regelmäßig einheitlich auf den 31.12.2021 festgelegt. Die Papierbescheinigung wird vom Onlinehändler an den Marktplatz übermittelt (im Original, in Kopie oder in gescannter digitaler Form) und von diesem aufbewahrt. Handelt es sich nicht um eine gültige Bescheinigung und unterlässt der Marktplatzbetreiber die Nachfrage beim zuständigen Finanzamt, besteht potenziell ein Haftungsrisiko. Der Marktplatz muss jedoch nur offensichtliche Fälschungen erkennen.

Neben dem grundsätzlichen Problem der Fälschungsanfälligkeit von Papierbescheinigungen ist die fehlende Möglichkeit einer regelmäßigen Gültigkeitsabfrage eines der gewichtigsten Probleme des Papierverfahrens. Nach Ausstellung der Bescheinigung ist es dem Onlinehändler möglich, sich beim zuständigen Finanzamt abzumelden, und sich so der Überwachung zu entziehen. Dennoch kann er Marktplatzbetreibern weiterhin eine gültige Papierbescheinigung vorlegen. Unter anderem aus diesem Grund wurde die Gültigkeit der Papierbescheinigungen einheitlich beschränkt.

Abbildung 1 zeigt den Prozess der Beantragung und Ausstellung der Bescheinigung und der Gültigkeitsabfrage durch die involvierten Marktplatzbetreiber im aktuellen Papierverfahren auf. Das Flussdiagramm ist hierbei als Abstraktion zu verstehen und erhebt nicht den Anspruch der Vollständigkeit. OH steht in dem Diagramm für Onlinehändler, während MP Marktplätze kennzeichnen.

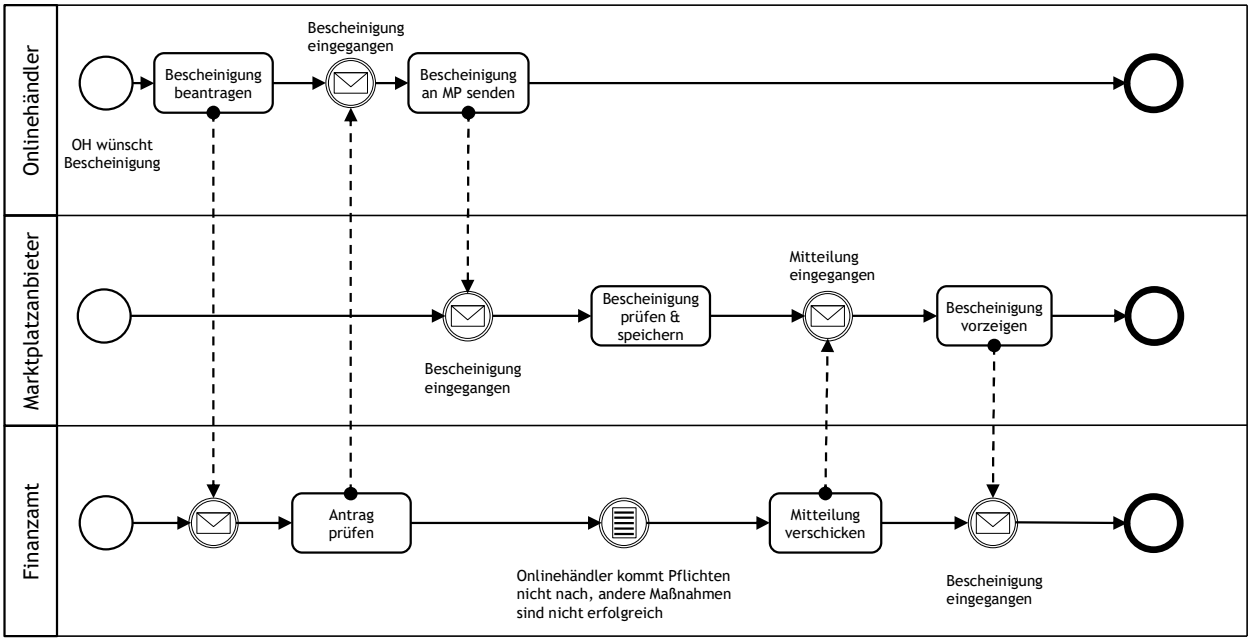


Abbildung 1: Prozessdiagramm Papierverfahren

Obwohl die Finanzverwaltung sowie viele der betroffenen Händler und Marktplätze auf ein digitales Verwaltungssystem zurückgreifen, setzt das aktuelle Verfahren noch immer auf die Papierform. Dem sich hieraus ergebenden Medienbruch folgen eine Reihung von inhärenten Problemen. Der gesamte Prozessablauf ist durch manuelle Tätigkeiten geprägt. Dies führt gerade seitens der Marktplätze zu vergleichsweise hohen Aufwendungen, da die jeweiligen Papierbescheinigungen händisch geprüft werden müssen. Hierbei ist die Authentizität des Dokumentes schwer nachvollziehbar, da für das Dokument abseits eines Dienststempels des Finanzamtes und der Unterschrift des Ausstellenden keine weiteren Maßnahmen zum Schutz vor Fälschung getroffen werden. Somit ist im papierbasierten Prozess eine Manipulation des Nachweises ohne große Hürden möglich. Dies wird auch durch den Fakt bestärkt, dass der Händler dem Marktplatz das Dokument nicht im Original, sondern beispielsweise in Form eines digitalen Scans vorzeigen kann.

Auch ist eine Aktualisierung des via Papierbescheinigung abgebildeten Status nicht möglich. Sobald sich beispielsweise ein Händler beim zuständigen Finanzamt abmeldet, erlischt die steuerliche Erfassung, was sich auch auf den Nachweis auswirken müsste. Hierzu wäre beispielsweise ein Einzug der ausgegebenen Papierbescheinigungen nötig. Dies ist jedoch weder angedacht noch praktikabel, da der Onlinehändler vergleichsweise einfach das Dokument selbst vervielfältigen kann. Darüber hinaus ist dem Finanzamt nicht zwingend bekannt auf welchen Marktplätzen der Onlinehändler agiert, was auch eine Mitteilung an die Marktplätze ausschließt.

4 Technologische Grundlagen

4. Technologische Grundlagen

4.1. Blockchain und DLT

Die erste umfassende Idee der Blockchain-Technologie wurde von Satoshi Nakamoto entwickelt. Obwohl der Autor den Begriff Blockchain noch nicht verwendete, hat er dessen Struktur und die für die Technologie erforderliche Funktionalität bereits im White Paper von Bitcoin beschrieben (Nakamoto 2008). Das Grundkonzept hinter der Entwicklung von Bitcoin bestand darin, ein System bereitzustellen, das sichere Finanztransaktionen mit geringen Transaktionskosten in einem unsicheren Umfeld ermöglicht. Dadurch verspricht die Technologie u.a. in der Logistik, dem Dienstleistungssektor und in der Industrie weitreichende Verbesserungen gegenüber zentralistischen Systemen (Zheng et al. 2018).

Eine Blockchain kann als eine Art Datenbank definiert werden, in der Transaktionen in Blöcken gruppiert werden. Diese Blöcke sind in chronologischer Reihenfolge durch kryptographische Fingerabdrücke miteinander verbunden. Die Verwendung digitaler Signaturen und eines Konsensverfahrens gewährleistet die Authentizität der Transaktionen und die Integrität der Blöcke. Terminologisch ist der Begriff Blockchain von der Distributed-Ledger-Technologie (DLT) abzugrenzen, indem Blockchain eine spezielle Form der DLT ist, in der die Transaktionen geblockt verarbeitet und gespeichert werden (siehe Abbildung 2).

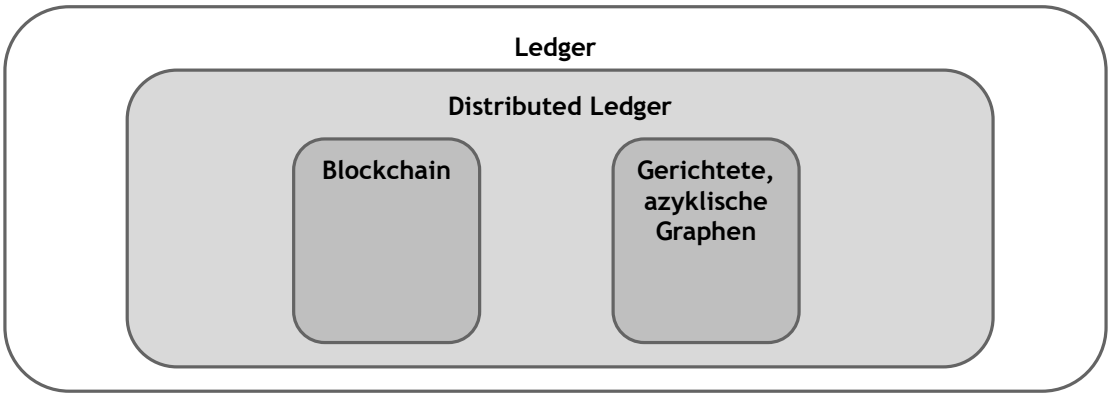


Abbildung 2: Abgrenzung Blockchain und DLT

Auf der Grundlage dieser Definitionen beschreibt Blockchain eine Technologie, welche Transaktionen fortlaufend speichert, wobei miteinander verknüpfte Blöcke verwendet werden, Peer-to-Peer-Technologie nutzt, um verteilte Datenspeicherung und -verarbeitung zu ermöglichen, Mechanismen zur Gewährleistung eines Konsenses zwischen den Knoten des Netzwerks besitzt und kryptographische Techniken einsetzt, um die Integrität, Authentifizierung und Gültigkeit der Daten zu gewährleisten.

Das große Interesse an der Technologie ist auch auf die Einführung sogenannter Smart Contracts zurückzuführen. Smart Contracts sind Computerprogramme, welche direkt auf den teilnehmenden Netzknoten eines Blockchain-Systems ausgeführt werden und dadurch alle Eigenschaften der Infrastruktur, wie Unveränderlichkeit und durchgehende Protokollierung, erben. Smart Contracts sind keine Verträge im juristischen Sinne, sondern erlauben durch die Nutzung von Programmcodes eine flexible Implementierung von Geschäftslogik. Somit können durch den Ein-

satz von Wenn-Dann-Funktionen beliebige Prozesse automatisiert werden, ohne, dass die beteiligten Personen einer dritten Partei vertrauen müssen.

Je nach Anwendungsbereich folgen Blockchains in der Regel zwei Dimensionen hinsichtlich Öffentlichkeit und Nutzungsbeschränkung. Erstens kann eine Blockchain entweder öffentlich oder privat ausgestaltet sein. In einer öffentlichen Blockchain gibt es keine Einschränkungen für den Zugriff auf die Blockchain und schließlich für das Lesen ihrer Daten, während in einer privaten Blockchain nur vordefinierte Benutzer auf die Blockchain zugreifen können. Zweitens kann eine Blockchain zusätzlich nutzungsbeschränkt oder -unbeschränkt sein. Wenn eine Blockchain nutzungsbeschränkt ist, können verschiedene Entitäten unterschiedliche Rechte besitzen. Beispielsweise können nur bestimmte Peers Transaktionen validieren. Diese Einschränkung besteht nicht in einer nutzungsunbeschränkten Blockchain, in der jeder beliebige Benutzer Transaktionen erstellen und validieren kann (Peters und Panayi 2016).

4.2. Digitale Identitäten

Identitäten spielen seit jeher eine wichtige Rolle in der zwischenmenschlichen Kommunikation und dem Gesellschaftsleben generell. Eine Identität setzt sich aus Attributen zusammen, die den Identitätsinhaber beschreiben. Während einige Attribute, wie beispielsweise biometrische Merkmale von Menschen, statisch sind, treten andere Attribute dynamisch auf und können sich mit dem Identitätsinhaber verändern (z.B. persönliche Interessen). Wie in Abbildung 3 dargestellt, kann ein Identitätsinhaber verschiedene partielle Identitäten besitzen (Clauß und Köhntopp 2001). Eine Teilidentität kann zum Beispiel nur die professionellen, berufsbezogenen Attribute eines Identitätsinhabers beschreiben, wohingegen andere partielle Identitäten Attribute aus dem persönlichen Umfeld beschreiben. Traditionelle Identitätsnachweise umfassen zumeist statische Dokumente, die eindeutig zuordnungsfähige Attribute eines Identitätsinhabers beschreiben. Hierzu gehören zum Beispiel der Führerschein und staatlich ausgestellte Ausweisdokumente.

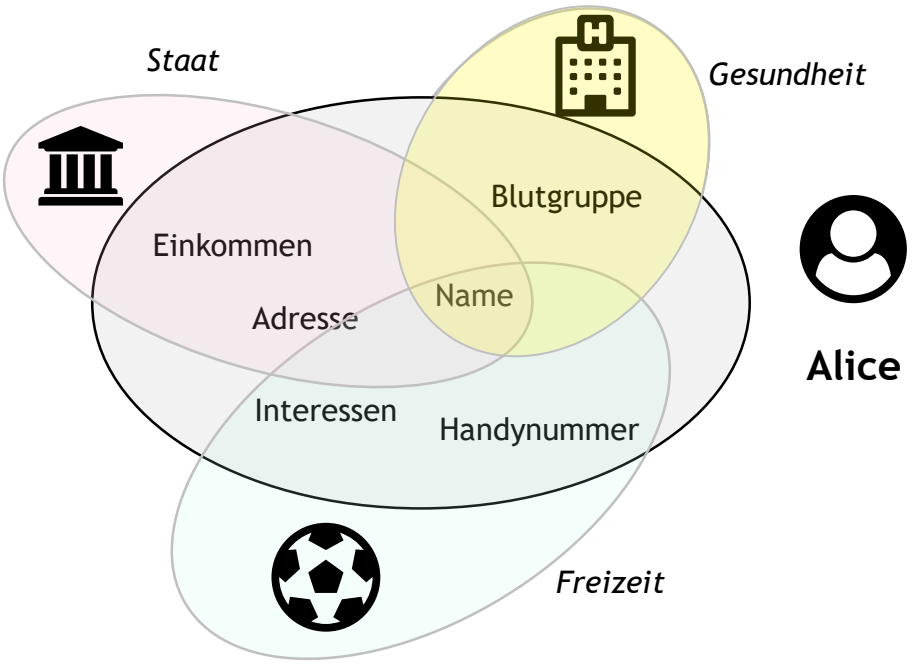


Abbildung 3: Partielle Identitäten

Digitale Identitäten gewinnen dabei in einer zunehmend digitalisierten Umgebung vermehrt an Relevanz. Dort treten jedoch besondere Herausforderungen auf: Da physische Interaktionen stetig geringer werden, wird es auch schwieriger, Identitäten und somit Interaktionspartner eindeutig festzustellen. Zudem lassen sich Attribute bzw. Bescheinigungen darüber in der digitalen Welt nahezu beliebig oft vervielfältigen. Das zunehmende Auftreten nichtmenschlicher Entitäten im digitalen Umfeld, beispielsweise im Rahmen des Internet der Dinge, erschwert die Thematik überdies. In der Folge bedarf es umfassender Identitätsmanagementsysteme, die es ermöglichen, digitale Identitäten kontextabhängig und dynamisch zu verwalten. Dabei muss auf die speziellen Herausforderungen, die in digitalen Umgebungen auftreten, sowie auf allgemeine Anforderungen an Identitäten eingegangen werden.

In der Schlussfolgerung besteht ein Bedürfnis nach einem Identitätsmanagementsystem, das die Verwaltung der Identität wieder dem Nutzer selbst übergibt, die Daten nicht einem einzelnen Anbieter überlässt und dabei bequem zu benutzen ist. Sogenannte SSIs stellen hierfür potenziell eine Lösung dar.

4.3. Self-Sovereign Identity

Das Konzept der SSI lässt sich mit einem Geldbeutel vergleichen (siehe Abbildung 4). Einzelne Nachweise über Attribute (Ausweise wie Führerscheine oder Personalausweise) werden gesammelt in einer Infrastruktur, die der Identitätsinhaber kontrolliert und besitzt, aufbewahrt. Diese Ausweise werden von verschiedenen vertrauenswürdigen Institutionen ausgestellt und durch diese fälschungssicher gestaltet. Jeder Ausweis stellt nur die für einen spezifischen Teilbereich relevanten Attribute dar. In unterschiedlichen Kontexten kann durch die Kombination verschiedener Ausweise ein Eigenschaftsnachweis für den Anwendungsfall erstellt werden.

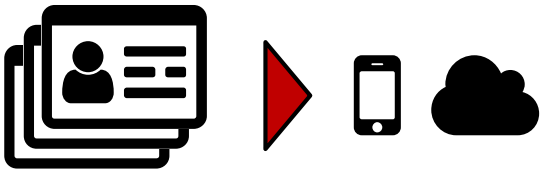


Abbildung 4*:* Digitale Eigenschaftsnachweise in einem SSI-System

Ein SSI-System besteht aus verschiedenen einzelnen Bestandteilen. Zentral ist dabei, dass Nutzer unabhängig von den jeweiligen Services, in denen sie ihre Identität partiell preisgeben, existieren. Interaktionen sind per Definition bilateral und involvieren keinen Umweg über zentrale Drittparteien. Entsprechend lassen sich vier Hauptelemente unterscheiden, die im Nachfolgenden jeweils detailliert ausgeführt werden. Abgesehen von technologischen Komponenten wie Public-Key-Systemen, handelt es sich hierbei um dezentrale Netzwerke (wie Blockchain-Netzwerke), dezentrale Identifier (DIDs), Verifiable Credentials (VCs) sowie Wallets zur Speicherung und Verwaltung der VCs.

DIDs sind Verlinkungen, die eine Entität mit Mitteln für die vertrauenswürdige Interaktion ausstatten. Sie müssen dabei einzigartig (bzw. kollisionsresistent) sein und dürfen nicht zentral vergeben werden, um Korrelationen zu vermeiden. Zugleich muss der Besitz über eine DID dezentral und kryptographisch sicher nachweisbar sein. Zur Erstellung sowie Nutzung von DIDs besteht ein weltweiter Standard, der durch das W3C-Konsortium (einem Gremium zur Standardisierung der Techniken im World Wide Web), spezifiziert wird und auch namensgebend für das Konzept ist (das auch darüber hinaus existiert). DIDs bestehen demnach aus einem Schema, einer Methode,

die spezifiziert, auf welchem DLT-System gearbeitet wird und wie mit der DID assoziierte Operationen stattfinden sowie einem methodenabhängigen Identifier. DIDs lösen sich zu DID-Dokumenten auf, die auch kryptographische Details (wie Schlüsselsysteme) beschreiben, die mit der DID zusammenhängen (Hyperledger 2020). Die folgende Abbildung zeigt eine beispielhafte DID auf:

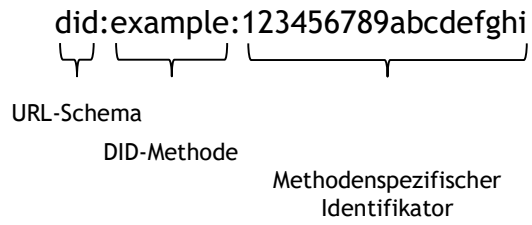


Abbildung 5: Beispielhafte Darstellung einer DID (basierend auf (Reed et al. 2020)))

Bezüglich der Credentials, also den Eigenschaftsnachweisen, wird zwischen zwei grundlegenden Typen unterschieden. Zum einen bestehen Credentials, die selbst ausgestellt werden können, möglicherweise über Hobbies eines Identitätsinhabers. Zum anderen gibt es Credentials, die Eigenschaften beinhalten, die durch offizielle Stellen verifiziert werden, sog. VCs (Reed et al. 2020). Im Wesentlichen sind VCs digitale Dokumente, die durch vertrauenswürdige Einrichtungen an einzelne Subjekte gegeben werden. Um die Herkunft von einer entsprechenden Institution zu beweisen, sind die Dokumente durch die jeweiligen Institutionen digital signiert. Zudem enthalten sie Metadaten, wie die kryptographischen Details des jeweiligen VCs.

Die VCs werden in einer Wallet auf einer durch den Inhaber der VCs kontrollierten Infrastruktur (zum Beispiel einem Smartphone) gespeichert. Hier werden auch vermehrt Cloud-basierte Infrastrukturen diskutiert. Dies hat zum Hintergrund, dass Nutzer möglicherweise VCs nachweisen wollen, aber nicht permanent verfügbar sind und ihre Verwaltungsinfrastruktur nutzen. Deshalb gibt es in letzter Zeit Standardisierungsversuche, um Nutzern zu ermöglichen, die Verwaltung bestimmter VCs an externe technische Infrastrukturen (sog. Agents) abzugeben (z. B. bei Anfragen, einen Altersnachweis zu geben). Abbildung 6 fasst die Prozesse in einer Übersicht zusammen.

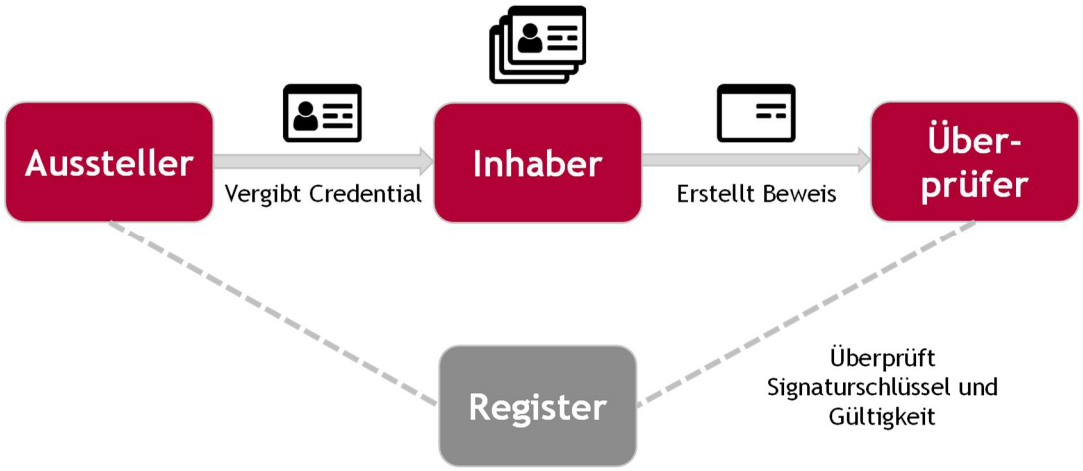


Abbildung 6: Prozesse in einem SSI-System

Um den Schutz der Privatsphäre zu erhöhen, existieren zudem Konzepte, die eine selektive Informationsweitergabe aus den Credentials erlauben. Generell werden keine Credentials direkt übertragen. Vielmehr werden kryptographische Beweise über Eigenschaften durch die Inhaber erstellt. Diese können entweder durch Klartext Informationen offenlegen oder auch nur "Aussagen" darstellen (z.B. „Ich bin über 18 Jahre alt“). Durch den Einsatz von kryptographischen Verfahren wie Zero-Knowledge-Proofs lassen sich bestimmte Eigenschaften eines zu Grunde liegenden Credentials beweisen. Beispielsweise bedeutet dies, dass man mittels eines Proofs den Besitz eines Credentials beweisen kann, welches den Besitzer als über 18 Jahre ausweist. Weitere Informationen aus dem Credential, wie beispielsweise Namen und Wohnort, werden so nicht mit vorgewiesen.

Da es erforderlich sein kann, dass Nachweise entzogen werden können, muss diese Funktionalität für ein umfassendes digitales Identitätsmanagement abzubilden sein. Als illustratives Beispiel dient ein entzogener Führerschein. Da im SSI-Umfeld Credentials jedoch jeweils dezentral bei den Nutzern liegen, muss eine zentrale Stelle existieren, die zum Nachweis eines durch den Aussteller zurückgezogenen Credentials dient. Gleichzeitig darf diese allerdings wiederum keinen Rückschluss auf die Inhaberidentität geben. Zu diesem Zweck werden häufig kryptographische Verzeichnisse, die auf einer Blockchain abgelegt sind, verwendet. Dabei muss bereits bei Ausstellung des Credentials eine Referenz abgelegt werden. Zur Wahrung der Anonymität werden z.B. kryptographische Akkumulatoren verwendet, um entsprechende Verzeichnisse abzubilden, obwohl auch alternative Ansätze existieren. Aktuell ist das Konzept der kryptographischen Akkumulatoren jedoch der am häufigsten genutzte Ansatz. Die Blockchain, auf der die entsprechenden Verzeichnisse gespeichert werden, muss zur Erstellung von Proofs öffentlich einsehbar sein (Reed et al. 2016).

Zur Kommunikation von Faktoren werden Tails-Files oder alternative Infrastrukturen verwendet. Ein Tails-File ist mit einem Akkumulator und seinen Faktoren verknüpft. Jeder Akkumulator besitzt ein Tails-File, welche die Faktoren in Form von Zahlen enthält, die zu dem auf der Blockchain gespeicherten Akkumulator führen. Ein Tails-File ist dabei jedoch nicht geheim, sondern wird für die Nutzer des Systems einsehbar veröffentlicht.

Bei der Ausstellung eines Credentials, wird auf dem Credential ein Index vermerkt, welcher direkt auf einen bestimmten Faktor im Tails-File referenziert. Um nun zu beweisen, dass ein Credential gültig ist, muss gezeigt werden, dass der mit dem Credential verknüpfte Faktor noch immer im Akkumulator hinterlegt ist. Die geschieht, indem ein Zero-Knowledge-Proof erstellt wird, welcher beweist, dass man einen Faktor a kennt, der multipliziert mit dem Witness (dem Produkt b*c*d) den Akkumulator e ergibt. Hierbei werden weder der Faktor a noch das Witness im Klartext vorgezeigt. Wenn ein Credential anschließend auf ungültig gesetzt wird, wird der entsprechende Faktor aus der Berechnung für den Akkumulator entfernt. Der Aussteller des Credentials passt entsprechend den korrespondierenden Akkumulator an und veröffentlicht einen Faktor, mittels dessen Besitzer korrespondierender Credentials Beweise über die Gültigkeit ihres Credentials mit dem neuen Akkumulator führen können. Nachfolgend ist der obenstehende Beweis nicht mehr möglich und die Gültigkeit des Credentials kann nicht mehr bewiesen werden. Da der Faktor a für andere Credentials jedoch auch einen Teil deren Witness ausgemacht hat, wird zeitgleich ein Witness-Delta über die Blockchain kommuniziert, so dass andere Nutzer ihr Witness entsprechend anpassen können, um in Zukunft auf den richtigen Akkumulator zu kommen.

Darüber hinaus gibt es verschiedene weitere Anwendungen der Blockchain im SSI-Umfeld, illustriert in der nachfolgenden Darstellung. Zum Beispiel können neben Revokationslisten auch Schemata über die jeweiligen Felder und Metadaten, die in einem Credential eines bestimmten Typs vorgesehen sind, auf der Blockchain liegen. Außerdem wird die Blockchain dazu genutzt,

öffentliche Identitäten zu veröffentlichen. Hierbei handelt es sich um ein Profil über Credential-ausstellende Institutionen, welche allgemeine Informationen, wie bspw. Name, Public-Key des Signatur-Schlüsselpaares und eine öffentliche DID enthalten. Somit kann bei Erhalt eines Proofs geprüft werden, ob die zugrundeliegende Signatur tatsächlich der gewünschten Institution gehört.

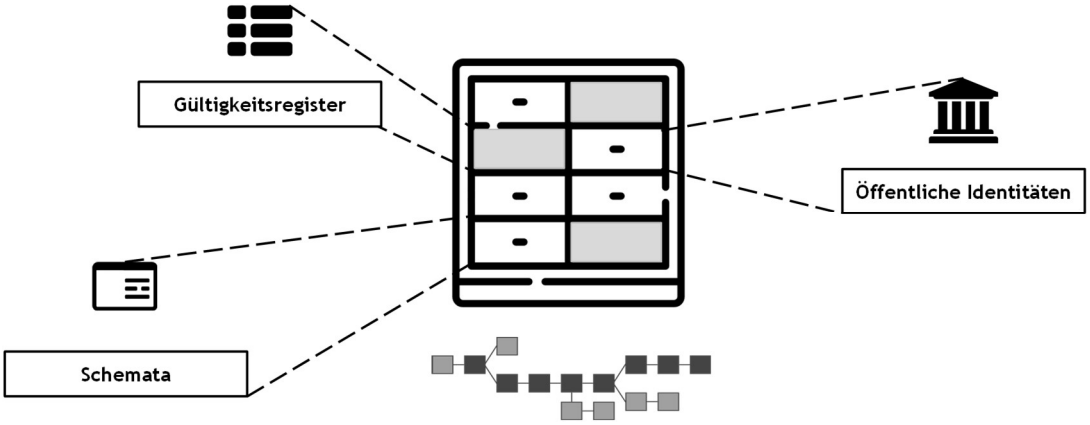


Abbildung 7: Rolle der Blockchain im SSI-Kontext

Im Kontext von SSI spielen zudem Wallets eine herausragende Rolle. Wallets bezeichnen eine Software, mit der Interaktionen mit der Blockchain ausgelöst werden können. Beispielsweise kann man Transaktionen auslösen, ansehen oder validieren. Eine Wallet ist immer vom Kontext abhängig und stammt aus der Welt der Kryptowährungen.

Im Umfeld der SSI bezeichnet eine Wallet eine Software, mit der Informationen wie Identitäts-nachweise (Credentials) und Verbindungsdaten (Connections) digital verwaltet werden können. Die Wallet kann auch Interaktionen abbilden, so zum Beispiel die Anforderung eines Nachweises (Proof) oder die Beantwortung eines solchen. Mit der Wallet kann der Nachweis über den Besitz eines Credentials geführt werden (Proof-Presentation).

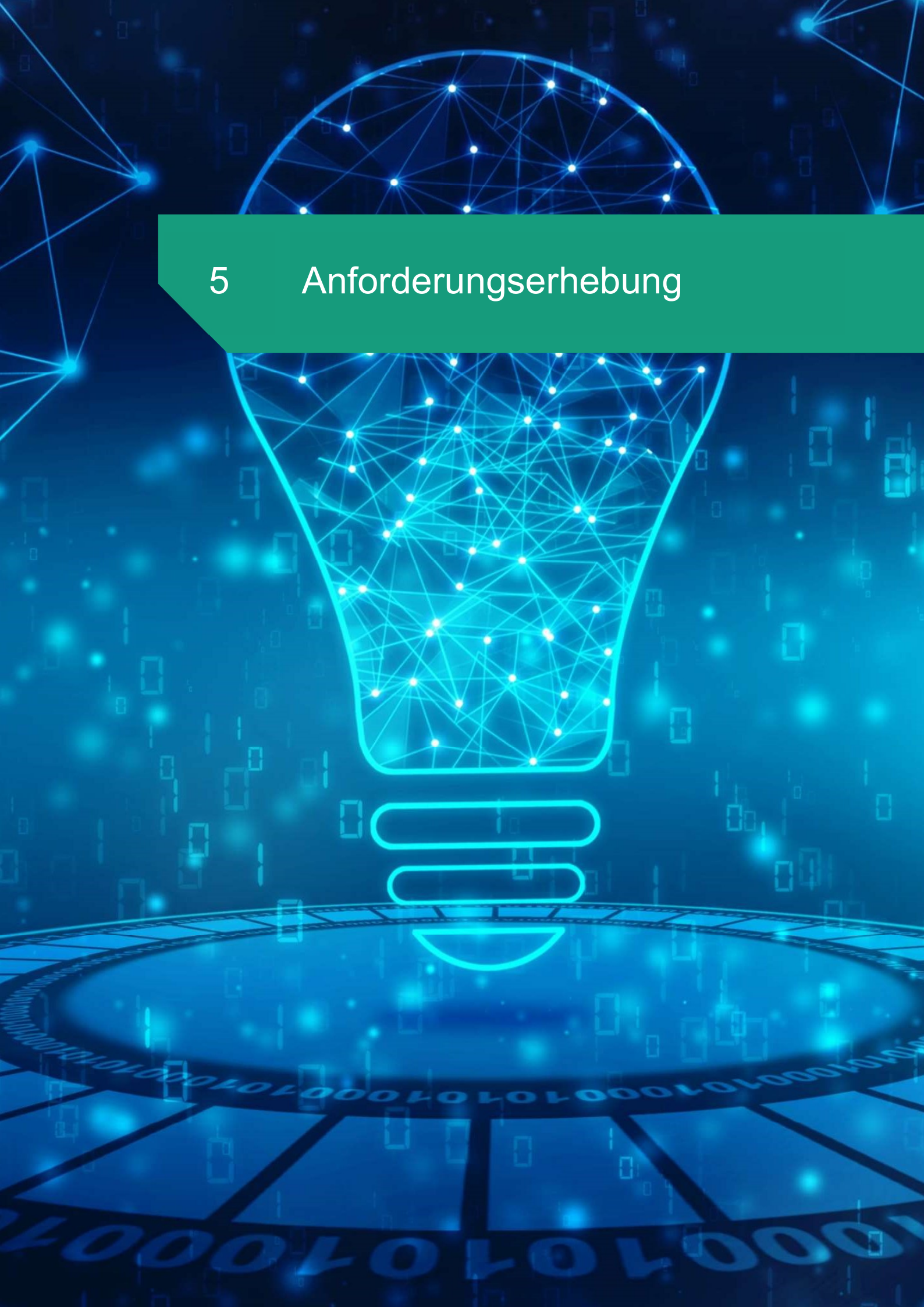
In einer SSI gehört zu einer Wallet optional auch ein Agent. Diese Software wird potenziell in einer Cloud oder anderen durchgängig verfügbaren Infrastruktur betrieben. Sie steht dementsprechend in dieser Ausprägung dauerhaft für die Adressierung von Nachrichten bereit. Eine Wallet holt sich von dort die Nachrichten ab und verarbeitet sie. Konkrete Implementierungen von Wallets/Agents treten in verschiedenen Varianten auf:

- Als Wallet-Applikation, z.B. als Handy-App, die ein Anwender für seine persönliche Teilnahme am System benötigt. Hier gibt es meist eine Benutzerschnittstelle, mit der Anwender Eingaben, wie z.B. Freigaben, durchführen können. Der Agent ist oftmals cloudbasiert und wird als Service genutzt, obwohl auch andere Umsetzungen existieren.
- Als Server-Applikationen: Die beiden Teile Wallet/Agent können zusammen auf einem Server betrieben werden. Hier muss es keine direkte Benutzerschnittstelle geben, das Programm kann Teil einer komplexen Anwendungslandschaft sein. Diese Umsetzung wird häufig in Unternehmensumfeldern diskutiert.

Sie erfüllt unter anderem folgende Aufgaben:

- Verschlüsselte Kommunikation (Austausch und Speicherung der DIDs) zwischen Teilnehmern (hier Händler) und den Institutionen.
- Kommunikation mit der Blockchain zur Verifizierung und Invalidierung von Credentials.

- Ausstellen von Credentials anhand der vom Benutzer übermittelten Daten und der als Proof erforderlichen Credentials (ggf. nach Prüfung der Gültigkeit der eingereichten Credentials/Proofs in der Blockchain).



5 Anforderungserhebung

5. Anforderungserhebung

Die Anforderungen an die Entwicklung einer technologischen Lösung wurden im Laufe des Projektes gemeinsam mit Mitarbeitern des Bayerischen Landesamt für Steuern erhoben. Die Anforderungen lassen sich dabei in rechtliche, technische sowie organisatorische Anforderungen untergliedern. Zur Erhebung wurden dabei mit unterschiedlichen Stakeholdern aus dem Bayerischen Landesamt für Steuern Interviews geführt. Die insgesamt acht Interviewpartner waren dabei in verschiedenen Rollen fachlich in die Entwicklung technischer Lösungen zur Umsetzung der Marktplatzhaftung involviert. Als Einführung in die Interviews wurden kurze Überblicke zum aktuellen Status der verfügbaren Umsetzungen sowie eine Grundidee des Projektvorhabens gegeben. Alle Interviews dauerten zwischen zwei und vier Stunden.

5.1. Wirtschaftlich / Organisationale Anforderungen

Innovationspotenzial

Eine Innovation resultiert im wirtschaftlichen Sinn aus Ideen bzw. Erfindungen, die in neue Produkte oder Dienstleistungen umgesetzt werden. Da das vorliegende Projekt bewusst als Forschungsprojekt mit starkem Innovationscharakter definiert wurde, ist das Innovationspotenzial des Prototyps und grundlegenden Konzepts ein Evaluationskriterium. Dabei ist besonders relevant, wie der Prototyp in die Praxis umgesetzt werden kann und welche weiterführenden Anwendungen außerhalb des definierten Falles damit möglich sind.

Flexibilität

Flexibilität bezeichnet die Fähigkeit, sich unter Wahrung der bisherigen Effektivität und Effizienz an verändernde Gegebenheiten anzupassen. Darunter zählen insbesondere Anpassungen an veränderte Umweltbedingungen, neue Entwicklungen in der Legislative oder angeschlossene Partnersysteme, die die bisherigen Prozesse beeinflussen können. Zudem versteht man unter Flexibilität häufig auch die Fähigkeit, Besonderheiten eines Anwendungsbereichs abbilden zu können.

Skalierbarkeit

Skalierbarkeit beschreibt die Fähigkeit eines Systems, sich in Größe und Umfang anforderungsbedingt anzupassen. Im konkreten Anwendungskontext definiert Skalierbarkeit die Fähigkeit, alle potenziell fachlich erforderlichen Anfragen an das Gesamtsystem in allen Komponenten des Systems so abzubilden, dass die fachlichen Anforderungen rechtskonform umgesetzt wurden. So soll die Masse an Stakeholdern (Händler, Marktplätze) Zugriff auf die Ressourcen der Anwendung haben, um ihren rechtlichen Pflichten nachkommen zu können.

Auf Basis einer Studie von ecom wird von 135 Marktplätzen ausgegangen, welche im deutschsprachigem Raum Produkte anbieten (ecom 2020). Die Anzahl der Onlinehändler ist vergleichsweise schwer abzuschätzen. Laut Meldungen des Blogs *Wortfilter* bieten ca. 125.000 Onlinehändler aktiv Waren auf ebay.de an (Wortfilter 2016b). Bei Amazon wird von etwa 55.000 Händlern ausgegangen (Wortfilter 2016a). Mit Einrechnung großer Schätzfehler und der Berechnung einer oberen Schätzgrenze wird von ca. 843.500 auszustellenden Proofs ausgegangen. Dies berechnet sich durch die bestätigten Händlerzahlen der oben aufgezeigten Marktplätze sowie der Annahme, dass die weiteren 130 Marktplätzen jeweils 5.000 Onlinehändler besitzen.

Benutzerfreundlichkeit

Die Dimension Benutzerfreundlichkeit beschreibt, wie einfach und intuitiv das System durch den Endanwender genutzt werden kann. Komplexe grafische Benutzeroberflächen und Abläufe können zu einer starken Unzufriedenheit der Nutzer führen und letztendlich die Effektivität und Effizienz der Nutzung beeinflussen. Selbst wenn das System alle fachlichen Anforderungen erfüllt, können hohe Hürden bei der Nutzung zu gravierenden Problemen führen. Im Hinblick auf den vorliegenden Anwendungsfall sollte die Beantragung und das Handling eines Credentials möglichst intuitiv ausgestaltet sein.

5.2. Technische Anforderungen

Datenintegrität

Die Datenintegrität stellt eines der drei Schutzziele der IT-Sicherheit dar. Dieses Schutzziel bezeichnet die Korrektheit (Unversehrtheit) von Daten und die korrekte Funktionsweise von Systemen. Insbesondere im steuerlichen Kontext ist die Datenintegrität von höchster Relevanz. Die Nachweise über die steuerliche Erfassung und deren Protokollierung sollten sich nicht verändern und fälschen lassen.

Datenvertraulichkeit

Vertraulichkeit definiert die Eigenschaft von Daten bzw. Informationen, nur für einen begrenzten Kreis von Empfängern bestimmt zu sein. Die Vertraulichkeit kann hierbei durch technische Mittel gefördert oder durchgesetzt werden. Mit Bezug auf die zu evaluierende Anwendung muss sichergestellt werden, dass Daten über einzelne Parteien ausschließlich ihnen und den zur Wahrung der Prozesse notwendigen Beteiligten zugänglich sind. Die zu erfassenden steuerlichen Informationen könnten beispielsweise durch Dritte ausgenutzt werden, weshalb eine Geheimhaltung der relevanten Daten sichergestellt werden muss.

Datenverfügbarkeit

Verfügbarkeit beschreibt die Wahrscheinlichkeit, dass ein System zu einem bestimmten Zeitpunkt in der Lage ist, den angedachten Dienst zur Verfügung zu stellen. Die Verfügbarkeit eines Systems wird typischerweise über seine Zuverlässigkeit, Wartbarkeit und seine Redundanz betrachtet. Mit zunehmender Zuverlässigkeit und Redundanz nimmt auch die Verfügbarkeit zu. Mit abnehmender Wartungsausfallzeit nimmt die Verfügbarkeit ebenfalls zu. Da eine große Zahl an Onlinehändlern und Marktplätzen direkt auf die Nutzung des Systems angewiesen sind, bedarf es eines hohen Maßes an Verfügbarkeit, um die Geschäftsvorgänge aller Beteiligten nicht zu gefährden.

Entwicklungs-/Betriebsaufwand

Während der Entwicklungsaufwand die Aufwendungen zur initialen Einführung beschreibt, beinhaltet der Betriebsaufwand alle Aufwendungen zur Nutzung und Sicherstellung des Betriebes. Die Einführung neuer Systeme und Prozesse sind zumeist mit hohen initialen Kosten verbunden, welche gerade bei innovativen Systemen vergleichsweise hoch ausfallen können. Weiterhin fallen auch nach der Fertigstellung zusätzliche Kosten an, welche sich beispielsweise durch Weiterentwicklung, Wartung und Nutzung von Drittanbieterdiensten äußern.

5.3. Rechtliche Anforderungen

Bei den rechtlichen Anforderungen sind zwei Dimensionen zu bewerten. Zum einen sollen die §§ 22f, 25e UStG in der Form des Gesetzes zur Vermeidung von Umsatzsteuerausfällen beim Handel mit Waren im Internet und zur Änderung weiterer steuerlicher Vorschriften vom 11.12.2018 umgesetzt werden. Es ist also sicherzustellen, dass die gesetzlichen Vorgaben abgebildet und die dafür notwendigen Prozesse umgesetzt werden können. Dabei ist allerdings zu beachten, dass § 22f Abs. 4 UStG das Bundesministerium der Finanzen dazu ermächtigt, das Verfahren des Abrufs, der Verarbeitung und der Übermittlung der Daten durch eine Rechtsverordnung zu gestalten. Von dieser Ermächtigung wurde bisher noch kein Gebrauch gemacht. Auch hat sich schon während des Projektes abgezeichnet, dass die Gesetzesgrundlage sich in Zukunft mit großer Wahrscheinlichkeit ändern würde. Zugunsten des Innovationspotenzials des vorgeschlagenen Lösungsansatzes wird deshalb teilweise vom aktuellen Gesetzeswortlaut abstrahiert und einer allgemeineren Lösung der Vorzug gegeben.

Zum anderen muss die Umsetzung des Konzeptes auch mit den übrigen rechtlichen Vorgaben vereinbar sein. Gerade weil Blockchain Technologie zum Einsatz kommt, ist ein besonderer Fokus auf datenschutzrechtliche Problematiken zu legen. Zentral und in der Anwendung vorrangig sind hierbei die Vorgaben der europäischen Datenschutz-Grundverordnung. Da es sich um Daten in der Verwaltung der Umsatzsteuer handelt, ist darüber hinaus der Anwendungsbereich der Abgabenordnung eröffnet. Daraus ergeben sich Vorgaben, die über diejenigen der Datenschutz-Grundverordnung hinausgehen.

Umsatzsteuerliche Vorgaben

Es ist dementsprechend sicherzustellen, dass bei einer Umsetzung des Konzeptes die Vorgaben des Umsatzsteuergesetzes eingehalten wurden. Alternativ könnte von der Ermächtigungsbefugnis Gebrauch gemacht werden oder gar eine gezielte Gesetzesänderung notwendig werden. Gleichzeitig sollte das Konzept auch nach der geplanten Gesetzesänderung hin zur Nutzung der Umsatzsteuer-Identifikationsnummer noch umsetzbar sein.

Anforderungen der Datenschutz-Grundverordnung

Im Anwendungsbereich der Datenschutz-Grundverordnung muss es eine Grundlage für die Verarbeitung der personenbezogenen Daten geben; auch für solche, die durch den SSI-Ansatz zusätzlich entstanden sind. Außerdem müssen die Grundsätze der Datenverarbeitung sowohl auf, als auch abseits der Blockchain eingehalten werden.

Vorgaben der Abgabenordnung

Im Anwendungsbereich der Abgabenordnung unterliegen auch Daten von Unternehmen dem Schutz der Datenschutz-Grundverordnung. Hier müssen ebenso die oben genannten Kriterien erfüllt sein. Das Steuergeheimnis muss gewahrt werden und alle Daten, die diesem unterliegen, genießen das erhöhte Schutzniveau, wie es für personenbezogene Daten besonderer Kategorie normiert ist.

6 Lösungskonzeptionierung

6. Lösungskonzeptionierung

In diesem Abschnitt soll vor allem das abschließend ausgewählte Lösungskonzept beschrieben und erklärt werden. Dabei wurden technische, rechtliche und wirtschaftlich / organisationale Anforderungen an die Lösung zusammenfassend berücksichtigt. Zunächst werden zwei initial betrachtete Konzeptausgestaltungen vorgestellt, die für den Prototyp nicht berücksichtigt wurden und deren Vor- und Nachteile gegenüber dem Lösungsansatz diskutiert. Anschließend wird das in dem Projekt umgesetzte Lösungskonzept vorgestellt.

Der erste alternative Lösungsansatz, ein Blockchain-basierter Steuer-Token, entspricht der Verwendung klassischer Tokenization-Strukturen. Entsprechend wird eine öffentliche Blockchain dazu genutzt, die Repräsentanz einer realen Eigenschaft durch einen Eintrag in dem Blockchain-System abzubilden. In dem Fall repräsentiert ein Token, welcher einem Onlinehändler zugeordnet wird, dessen steuerliche Erfassung.

Als zweite Alternative, ein Blockchain-basiertes Gültigkeitsregister, wurde die Verwendung einer privaten Blockchain, welche die Gültigkeit von Zertifikaten in einer Datenstruktur vorhält, diskutiert. Anders als in der ersten Lösungsskizze, ist die Blockchain dabei verwaltungsintern und es wird nicht mehr auf eine öffentlich zugängliche, bereits bestehende Infrastruktur zurückgegriffen.

Das schlussendlich verwendete SSI-basierte Lösungskonzept weist verschiedene Vorteile sowie Herausforderungen auf. Durch die Möglichkeit, auf eine bereits bestehende, öffentliche Blockchain zurückzugreifen, muss hier keine eigens initiierte Infrastruktur aufgebaut werden. Zugleich schwinden so die Einstiegsbarrieren für etwaige Nutzer sowie Entwickler, die Lösungen zum Zugriff auf die Blockchain entwickeln (z.B. Marktplätze), da der Umgang mit dem entsprechenden System bekannt sein sollte. Das System weist überdies eine hohe technische Skalierbarkeit auf, die durch die dezentrale Datenhaltung und geringe Anzahl an Schreibvorgängen auf der Blockchain entsteht. Ersterer Punkt bedingt auch einen hohen Datenschutz, da Beweise nur durch den Besitzer erbracht werden können und Gültigkeitsabfragen nicht korrelierbar für Prozessunbeteiligte ausfallen. Ein zusätzlicher Gesichtspunkt ist die große Erweiterbarkeit des Anwendungsfalls im Steuerkontext und darüber hinaus. Das System lässt sich gut in die übergeordnete Vision der SSI einbetten und stellt somit potenziell einen wichtigen Baustein für die Einbettung einer übergeordneten (staatlichen) Infrastruktur dar.

Nachteile, die das System mit sich bringt, umfassen zum einen die Notwendigkeit für die Onlinehändler, stetig Beweise zu erstellen und somit aktiv zu werden, sowie zum anderen das Fehlen einer inhärenten Protokollierung der Gültigkeitsabfragen der Marktplatzbetreiber. Zudem zieht die Verwendung einer öffentlichen Blockchain auch eine gewisse Abhängigkeit nach sich, wobei diese durch Verwendung offener Standards weitgehend umgangen werden können.

Obwohl alle drei Lösungsansätze zunächst valide Optionen darstellen, zeigt sich bei einer genaueren Betrachtung der Vor- und Nachteile, dass die SSI-basierte Lösung den größten Mehrwert verspricht. Durch den Einsatz moderner kryptographischer Verfahren, erlaubt es die SSI-basierte Lösung die Vorteile der beiden alternativen Konzepte zu vereinen, ohne dabei ihre Nachteile mitzunehmen.

6.1. Das finale Lösungskonzept

Das Lösungsdesign der Studie baut auf dem Konzept der SSI und der Blockchain-Technologie auf. Dabei wird auf Anfrage eines Onlinehändlers nach positiver Prüfung der vorausgesetzten Händlereigenschaften durch Abgleich mit den hinterlegten Stammdaten im ELSTER-System ein VC ausgestellt, welches die steuerliche Erfassung des Onlinehändlers – ähnlich zum aktuellen papierbasierten Dokument – nachweist. Das VC, welches z.B. ein JavaScript Object Notation (JSON)-Dokument (ein Standardformat für den Austausch von Daten im Web) sein kann, kann dabei nach einem Schema erstellt werden, das auf einer öffentlichen Blockchain publiziert wurde und standardisiert verarbeitungsfähig ist. Zudem wird in dem angedachten Konzept ein weiteres VC ausgestellt, welches die steuerlichen Informationen des Händlers beinhaltet und somit auch in weiteren Szenarien über den Anwendungsfall hinaus nutzbar ist.

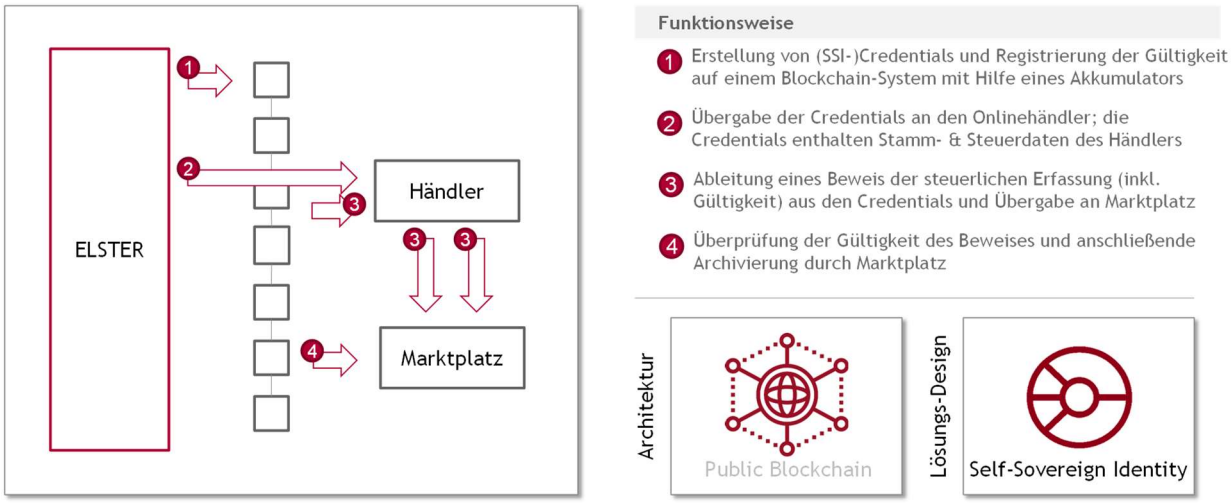


Abbildung 8: SSI-basiertes Steuernachweissystem

Ausstellung der Credentials

Zunächst meldet sich der Onlinehändler in dem gegebenen Szenario durch ein bereits bestehendes Interface, wie zum Beispiel via dem ELSTER-Portal (1), an. Voraussetzung für die Beantragung ist daher der Besitz eines ELSTER-Zertifikats. Hier beantragt der Onlinehändler ein SSI-Credential seiner Stammdaten, das sog. ELSTER-Credential. Im Backend von ELSTER wird darauffolgend ein Invitation-Link generiert, um eine sichere SSI-Verbindung zum Onlinehändler herzustellen (2). Dies ist die Voraussetzung, damit die SSI-Wallets des Onlinehändlers und von ELSTER direkt miteinander kommunizieren können, womit nicht nur die Sicherheit erhöht, sondern auch das ELSTER-Portal nicht zusätzlich belastet wird. Der generierte Link wird dem Onlinehändler als QR-Code angezeigt, könnte allerdings auch anders verarbeitet werden (bspw. als Reintext). Der Onlinehändler scannt diesen QR-Code mithilfe seiner SSI-Wallet (3). Diese Wallet stellt daraufhin eine sichere Verbindung mit der SSI-Wallet von ELSTER her (4) und bestätigt die erfolgreiche Verbindungserstellung. Das ELSTER-System schickt daraufhin ein Credential-Angebot mit den intendierten Informationen, die darin enthalten sein sollen, an die Wallet des Onlinehändlers (5). Wenn der Onlinehändler das Credential in der vorgeschlagenen Ausgestaltung akzeptiert, sendet er einen Credential-Request über die SSI-Verbindung zurück (6). Im darauffolgenden Schritt sendet ELSTER schließlich das entsprechende Credential an den Onlinehändler

zurück (7). Für die reine Ausstellung ist noch keine Kommunikation mit der Blockchain erforderlich. Sollten sich die Stammdaten eines Onlinehändlers ändern, so müsste das Credential als ungültig markiert und ein neues Credential ausgestellt werden.

Aufzeichnungspflichten über die Identität des Anbieters bestehen grundsätzlich für alle Händler, die mit Hilfe des Marktplatzes Umsätze ausführen, deren Warenbewegungen im Inland beginnen oder enden. Dieses Credential könnte daher nicht nur Unternehmern, sondern allen auf den Plattformen handelnden Anbietern ausgestellt werden, um ihnen damit einen durch die Steuerverwaltung bestätigten Nachweis ihrer Stammdaten zu ermöglichen. Für die Marktplatzbetreiber bestünde die Möglichkeit, mit Erhalt dieses Credentials ihre Aufzeichnungspflichten zu erfüllen.

Abstrahiert vom Anwendungsfall der Marktplatzhaftung könnte das Credential grundsätzlich ausgestellt werden, um Steuerpflichtigen auch zu anderen Zwecken den Nachweis ihrer von der Steuerverwaltung bestätigten Grunddaten zu ermöglichen.

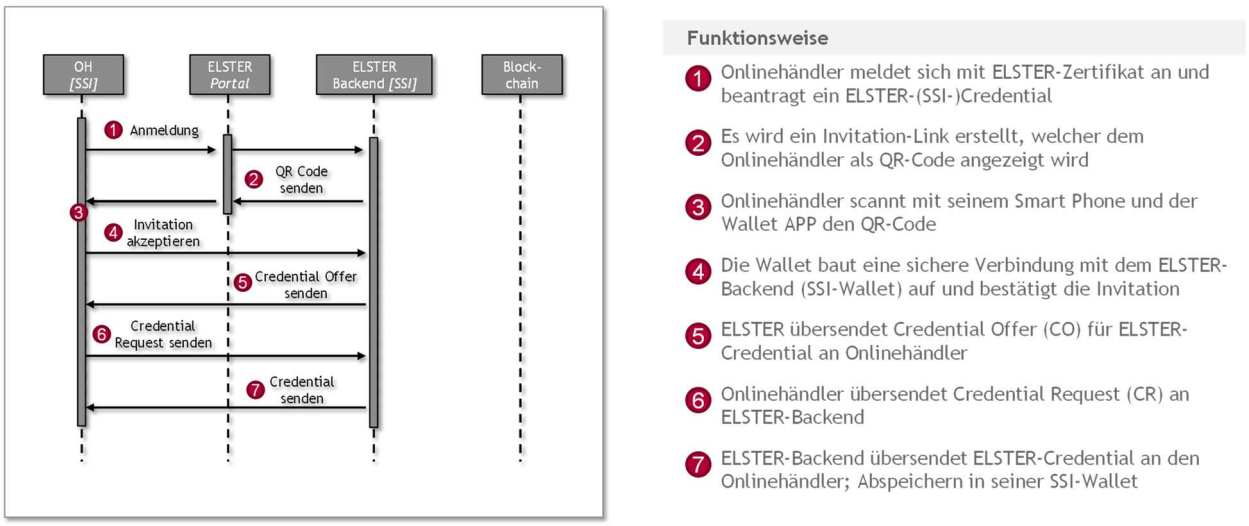


Abbildung 9: Ausstellung des SSI-Credentials

Um die steuerliche Erfassung zu bestätigen, wird dem Onlinehändler auf Antrag ein weiteres VC ausgestellt. Dieses sog. Tax-Credential soll nun nicht die Stammdaten, sondern die steuerliche Erfassung repräsentieren. Dies erlaubt, dass das ELSTER-Credential ungültig gesetzt und mit neuen Daten (bspw. einer neuen Adresse) ausgestellt werden kann, ohne, dass das zweite Credential davon betroffen ist und der Onlinehändler keinen Nachweis über seine steuerliche Erfassung mehr erbringen kann.

Über das Interface des ELSTER-Portals beantragt ein Onlinehändler das passende Credential. Im Backend von ELSTER werden die Voraussetzungen für die Ausstellung des entsprechenden Zertifikates geprüft. Dies geschieht automatisch durch Abgleich der beim Finanzamt hinterlegten Daten. Sind diese erfüllt, beginnt der Prozess zur Übermittlung eines Credentials erneut. Die Schritte (2) - (4) sind analog zur Ausstellung des ELSTER-Credentials. Um die Identität des Onlinehändler sicher zu bestätigen, erwartet das ELSTER-Backend nun einen Beweis durch den Onlinehändler über die Stammdaten aus seinem ELSTER-Credential (5). Obwohl dieser Schritt nun nicht zwingend erforderlich ist, soll somit die Identifikation durch bereits zuvor ausgestellte Stammdaten-Credentials, die z.B. auch in Form eines Personalausweis-Credentials vorliegen könnten, simuliert werden. Der Onlinehändler erstellt nun einen entsprechenden Beweis (6). Dieser Proof wird daraufhin an ELSTER zurückgesendet. Das Backend prüft die Inhalte des Beweises und ob der Beweis über die Identität zu dem auszustellenden Credential passt (7). Wenn der

Onlinehändler sich mit seinem ELSTER-Credential authentifizieren konnte, wird das Tax-Credential über denselben Vorgang wie beim ELSTER-Credential ausgestellt. Der Onlinehändler speichert das Credential schlussendlich in seiner Wallet (8).

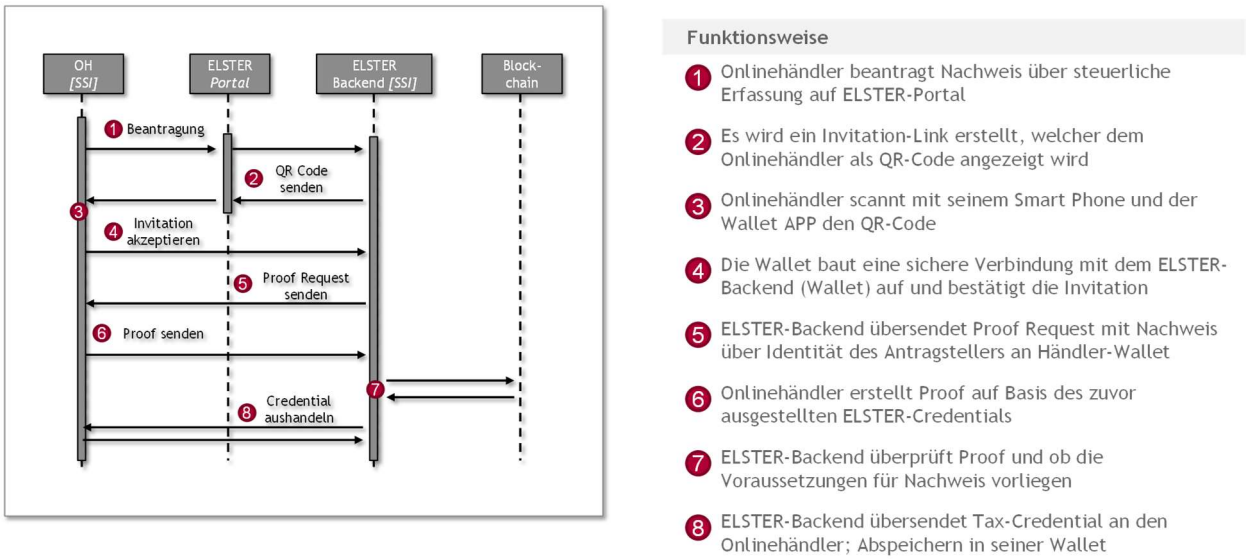
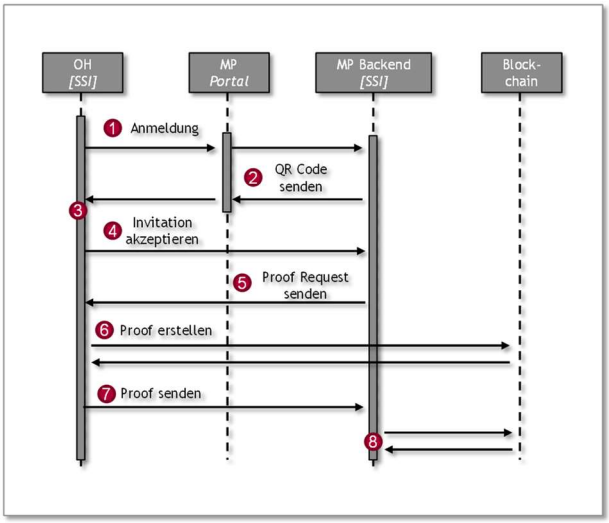


Abbildung 10: Ausstellung des zweiten SSI-Credentials

Nutzung der Credentials

Der Onlinehändler meldet sich weiterhin regulär auf dem Marktplatz an, auf dem er seine Produkte zu verkaufen wünscht (1). Um seinen Aufzeichnungspflichten gem. § 22f UStG nachzukommen, muss der Marktplatz einen entsprechenden Nachweis über die steuerliche Erfassung des Onlinehändlers einholen. Bevor der Onlinehändler jedoch die von ELSTER ausgegebenen Credentials zur Erstellung eines Proofs nutzen kann, muss auch hier zunächst eine sichere Verbindung zwischen den Wallets der jeweiligen Teilnehmer aufgebaut werden. Das SSI-System/Wallet des Marktplatzes erstellt hierzu einen Invitation-Link, welcher dem Onlinehändler auf dem Web-Portal des Marktplatzes nach Anmeldung angezeigt wird. Der Link kann hierbei entweder in Form einer URL oder auch als QR-Code vorliegen (2). Abhängig vom Typ der Wallet, die ein Onlinehändler nutzt, kann er diesen Link direkt aufrufen oder den QR-Code mit seinem Smart Phone einscannen (3). Durch Aufruf des Links wird die Einladung akzeptiert und eine gesicherte Verbindung zwischen den Wallets des Onlinehändler und des Marktplatzes aufgebaut (4). Ab diesem Schritt findet jede weitere Kommunikation direkt zwischen den Wallets statt. Im nächsten Schritt erstellt der Marktplatz einen sog. Proof-Request und übersendet ihn an den Onlinehändler (5). Der Proof-Request beinhaltet eine genaue Aufstellung der benötigten nachgewiesenen Attribute sowie die Vorgabe, um welche Art von Credential es sich handelt und von wem diese Attribute bescheinigt sein sollten. In dem hier vorliegenden Fall entsprechen die Attribute den gesetzlichen Vorgaben des § 22f UStG und müssen von der Finanzverwaltung bescheinigt worden sein. Mit Erhalt des Proof-Requests kann der Onlinehändler die entsprechende Anfrage verarbeiten. Hierzu erstellt er auf Basis der Vorgabe des Marktplatzes und den ihm zur Verfügung stehenden Credentials einen entsprechenden Proof. Die Wallet des Onlinehändlers erstellt dazu zunächst einen primären Proof zum Nachweis der geforderten Eigenschaften. Dieses Vorgehen erlaubt

letztendlich den Nachweis über den Besitz eines Credentials, inklusive der attestierten Eigenschaften, ohne dass das eigentliche Credential vorgezeigt werden muss. Neben dem primären Proof wird zusätzlich auch ein sekundärer Proof erstellt. Dieser Proof of Non-Revocation soll beweisen, dass zum Zeitpunkt der Proof-Erstellung das zu Grunde liegende Zertifikat gültig war. Während es bei der Erstellung des primären Proofs zu keiner Interaktion mit der Blockchain kommt, bedarf es für die Ableitung des Proof of Non-Revocation eines Abgleiches mit dem Witness-Delta und dem Akkumulator oder alternativer potenziell verwendeter Technologien auf der Blockchain. Um die Gültigkeit der zwei zugrunde liegenden Credentials zu beweisen, benötigt es entsprechend zwei Proofs of Non-Revocation. Die sich ergebenden Proofs werden nun an die Wallet des Marktplatzes geschickt (6). Der Marktplatz kann nun mit Hilfe von kryptographischen Methoden die Proofs validieren und somit die Identität des Onlinehändlers als auch die Gültigkeit der steuerlichen Erfassung bestätigen.



Funktionsweise

1. Onlinehändler meldet sich auf Marktplatz-Portal an und meldet die Erbringung eines Nachweises an
2. Es wird ein Invitation-Link erstellt, welcher als QR-Code dem Onlinehändler angezeigt wird
3. Onlinehändler scannt mit seinem Smart Phone und der Wallet APP den QR-Code
4. Die Wallet baut eine sichere Verbindung mit dem Marktplatz-Wallet auf und bestätigt die Invitation
5. Marktplatz-Wallet übersendet Proof Request mit Nachweis über Identität, Erfassung und Gültigkeit
6. Onlinehändler erstellt Proof auf Basis des zuvor ausgestellten ELSTER- und Tax-Credentials
7. Onlinehändler schickt den erstellten Proof an das SSI-System des Marktplatzes

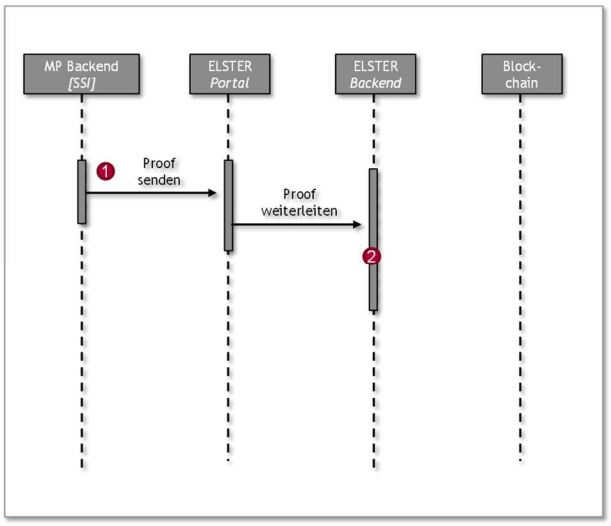
Marktplatz-Wallet überprüft Proof und gleicht die Gültigkeit ab; Vorhalten der Proofs

Abbildung 11: Eigenschaftsnachweis gegenüber einem Marktplatz

Nachweis an das Finanzamt

Zur Beweissicherung sieht das Konzept vor, dass erhaltene Proofs beim Marktplatzbetreiber grundsätzlich abgespeichert werden können. In diesem Zusammenhang ist jedoch anzumerken, dass der auf dem Proof beschriebene Zeitstempel durch den Onlinehändler gesetzt wird. Unter der Annahme, dass sowohl Onlinehändler als auch Marktplatzbetreiber unehrlich wären und sich absprächen, wäre es möglich, dass sie das Erstellen von vergangen Proofs zu einem bestimmten Zeitpunkt nachholen. Zu einem Zeitpunkt, zu dem das Credential ungültig ist, ist das nachträgliche Erstellen aber nicht mehr möglich. Proofs sind also manipulationssicher in dem Sinne, dass zu einem Zeitpunkt, zu dem das zugrundeliegende Credential ungültig ist, keine gültigen Proofs erstellt und ggf. abgespeichert werden können.

Es wird daher vorgeschlagen, Marktplatzbetreiber dazu zu verpflichten, den ersten, bei der Registrierung des Händlers auf der Plattform eingeforderten Proof über die Gültigkeit des zweiten SSI-Credentials an die Finanzbehörde zu übermitteln. Zum einen kann der Marktplatz dadurch beweisen, dass eine Nachweiserbringung stattgefunden hat. Zum anderen erlangt die Finanzbehörde Kenntnis davon, auf welchen Marktplätzen der Onlinehändler tätig ist. Ab diesem Zeitpunkt sollte es dem Marktplatz überlassen sein, in welchen Abständen die Gültigkeit des zweiten SSI-Credentials erneut überprüft wird. Eine Haftung könnte beispielsweise ab dem Zeitpunkt eintreten, zu dem das Credential seit einem Monat ungültig ist, wenn der Marktplatzbetreiber den Onlinehändler weiterhin zum Handel zulässt.



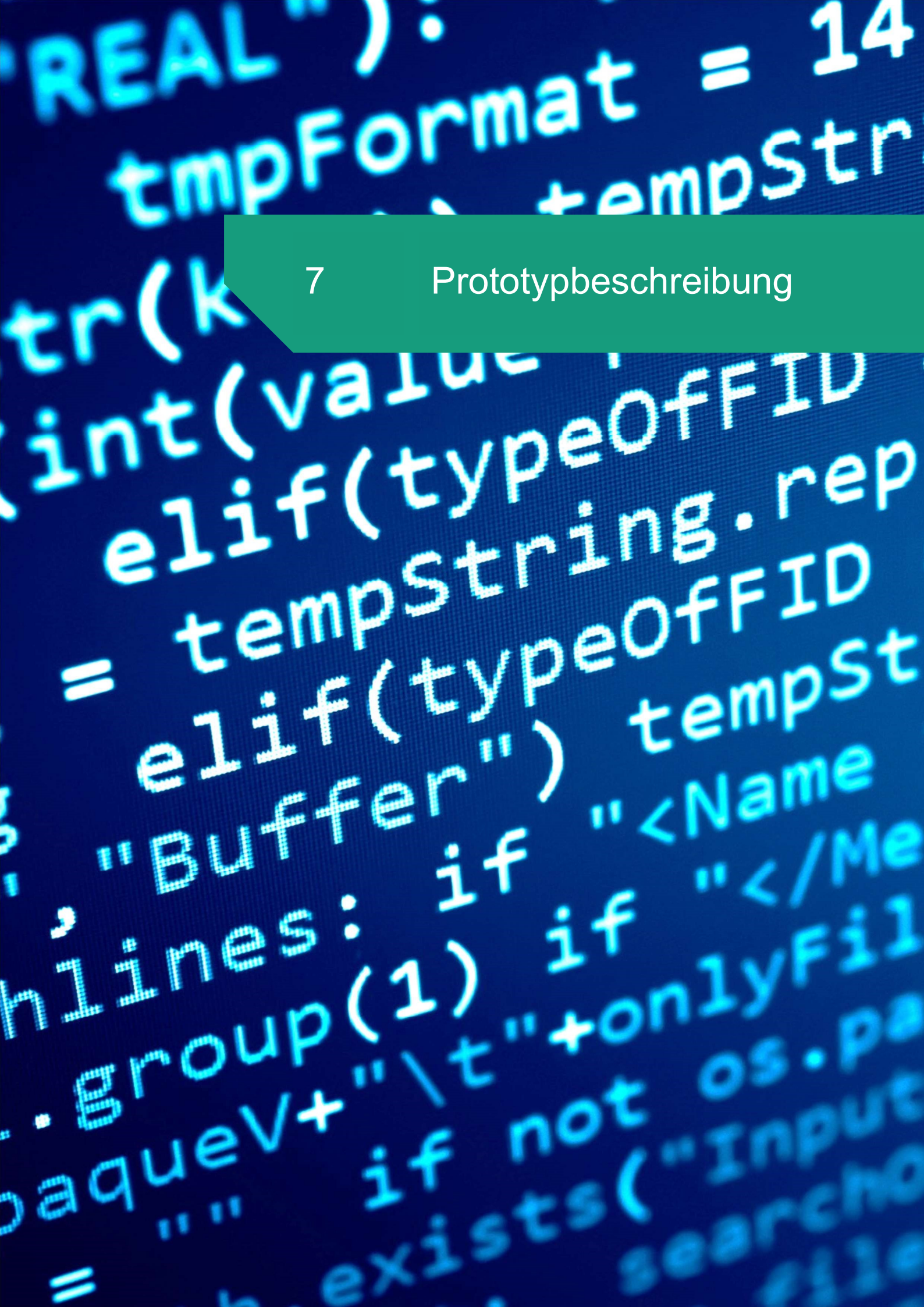
Funktionsweise

1. Marktplatz übersendet ersten Proof eines neuen Händlers an ELSTER (und nutzt hierzu ELSTER-Portal oder API)
2. ELSTER speichert den Proof

Abbildung 12: Informationsweitergabe an die Finanzbehörden

Deaktivierung eines Credentials

Es kann in einzelnen Fällen vorkommen, dass die im Credential hinterlegten Daten nicht mehr aktuell sind oder auch die steuerliche Erfassung eines Händlers nicht mehr gegeben ist. Hierzu bedarf es der Möglichkeit, einzelne Credentials auf ungültig zu setzen. Zu diesem Zweck passt ELSTER den auf der Blockchain gespeicherten Akkumulator so an, dass der Faktor, welcher das Credential repräsentiert, nicht mehr in dem Akkumulator beinhaltet ist. Ab diesem Moment ist es nicht mehr möglich einen gültigen Proof of Non-Revocation zu erstellen. Falls erforderlich, kann anschließend ein Credential mit den neuen Daten ausgestellt werden.



7 Prototypbeschreibung

7. Prototypbeschreibung

Im Bereich SSI existieren zahlreiche Initiativen, welche entsprechende Konzepte, Technologien und Lösungen entwickeln. Im Rahmen der Prototypentwicklung wurde der Ansatz verfolgt, Lösungsbausteine zu identifizieren, die weit verbreitet und im Rahmen einer Prototypentwicklung schnell zu realisieren sind. Generell lässt sich der vorgeschlagene Lösungsansatz aber auch auf anderen SSI-Lösungen umsetzen. Die Komponentenauswahl für den Prototypen legt also nicht zwingend die späteren produktiven Komponenten fest.

7.1. Entwicklungs-Framework Hyperledger Indy

Als grundlegendes Framework wurde für den Prototyp auf Hyperledger Indy gesetzt. Das Projekt ist Open Source und stellt einen Defacto-Standard für eine Vielzahl verschiedener SSI-Projekte dar. Durch die starke Hyperledger-Blockchain-Community sind auch kommerzielle Indy-Projekte entstanden, so z. B. das Sovrin Network (Öffentliche Blockchain auf Indy-Basis) und Evernym (Kommerzielle Produkte auf Sovrin-/Indy-Basis). Damit wird auf der einen Seite eine Weiterentwicklung durch die Open-Source Community erreicht. Auf der anderen Seite ist auch die Einbindung professioneller Lösungen möglich.

Für die Umsetzung des Prototyps wurde aus zwei Gründen auf ein öffentliches Netzwerk zurückgegriffen. Zum einem erlaubt das SSI-Konzept, dass keinerlei "Netto-Daten" auf der Blockchain gespeichert werden. Somit ist die Nutzung datenschutztechnisch vergleichsweise unbedenklich. Dies unterstreicht einen wichtigen Vorteil des SSI-Ansatzes. Zum anderen spiegelt die Nutzung einer vorhandenen Blockchain das mittelfristig angestrebte Nutzungsszenario wider: Behörden und Unternehmen stellen immer mehr SSI-Zertifikate bzw. Proofs aus und werden dafür nicht immer eine eigene Blockchain betreiben, sondern auf eine oder mehrere öffentliche Blockchain-Infrastrukturen zurückgreifen. Dies soll entsprechend zu mehr Komfort für den Nutzer sowie zur Senkung von Betriebskosten führen. Zudem kann so eine Vermeidung von Insellösungen und sog. Vendor-Lock-Ins erreicht werden. Geringere Entwicklungskosten sind bei der Verwendung bereits bestehender Infrastrukturen zudem zu erwarten und das Vertrauen von Anwendern zu bereits bestehenden Lösungen steigt. Überdies können neue Nutzungsszenarien mit geringem Entwicklungsaufwand erschlossen werden.

7.2. Architektur

Komponentenübersicht

Während serverseitig folgende Komponenten zum Einsatz kommen

Komponente	Zweck / Verantwortlichkeit	Betrieb bei
Java-Applikation "SSI-POC"	• Bereitstellung der sichtbaren Anteile des POC (Mein ELSTER, Marktplatz, Admin-Bereiche, Startseite, Webwallet) • Business-Logik • Datenhaltung • Aufrufpunkt für die Webhooks von Trinsic	Amazon AWS Cloud
Trinsic	• Hosting und Konfiguration der Wallets/Agents • Schnittstelle zur Blockchain (Sovrin-Ledger "BCGov Test Ledger") • Bereitstellung definierter REST-Schnittstellen für den "SSI-POC" Teil	Trinsic, Verifiable Organizations Network (VON)

sind clientseitig (seitens des Onlinehändlers) die folgenden Komponenten erforderlich:

Komponente	Zweck	Beispiel
Browser	Mit dem Browser navigiert der Onlinehändler zwischen den simulierten Portalen des POC.	Firefox, Chrome, Edge, Safari...
Wallet	Die persönlichen Wallet Applikation ermöglicht dem Onlinehändler die Teilnahme am SSI-System für den POC	Esatus Wallet, POC-Webwallet

Der in diesem Projekt entstandene Prototyp gliedert sich in zwei wesentliche Server-Komponenten. Die Java-Applikation "SSI-POC" beinhaltet in diesen Prototypen sämtliche Abläufe, die im Browser zu sehen sind. Sie bündelt die gesamte Business-Logik und die Datenhaltung für Mein ELSTER und den Marktplatz. Die Komponente "Trinsic" ist das Verbindungsglied zur Blockchain. Hier werden drei Wallets und Agents implementiert und aufrufbar vorgehalten. Beide Teile sind eng miteinander verknüpft, der Betrieb ist nur mit beiden Teilen gemeinsam möglich: Alle fachlichen Abläufe sind in der SSI-POC-Applikation gebündelt, die Blockchain-Operationen werden immer an Trinsic per REST-Schnittstelle weitergegeben. Trinsic verwaltet die Wallets und die Kommunikation mit der Blockchain, hat aber selbst kein fachliches Frontend, das komplexe Abläufe darstellt.

Kollaborations-Diagramm

Das folgende Kollaborationsdiagramm zeigt alle Akteure und Dienste, die in den Kommunikationsbeziehungen des Onlinehändlers erforderlich sind.

Auf der linken Seite ist in blau die "SSI-POC Server Applikation" eingezeichnet, die die Simulationen für Mein ELSTER und den Marktplatz enthält. Auf der rechten Seite ist in lila der vom Prototypen genutzte Blockchain-Anteil bei Trinsic zu sehen. Das Subjekt, ein Onlinehändler, der auf dem Marktplatz Handel treiben will, ist mittig eingezeichnet. Er hat vielfältige Kommunikationsbeziehungen zu den Applikationen:

Mit seinem Browser greift er auf die Webseiten (bzw. deren Simulationen) von Mein ELSTER und Marktplatz zu. Mit seiner Wallet-Applikation, hier ist die Handy-App eingezeichnet, erzeugt er Verbindungsanfragen, erhält Credentials und bestätigt Proof-Requests.

Aktionen beeinflussen aufgrund der engen Kopplung der beiden Komponenten immer beide und bilden eine Aufrufkette. Sie werden immer vom Händler ausgelöst.

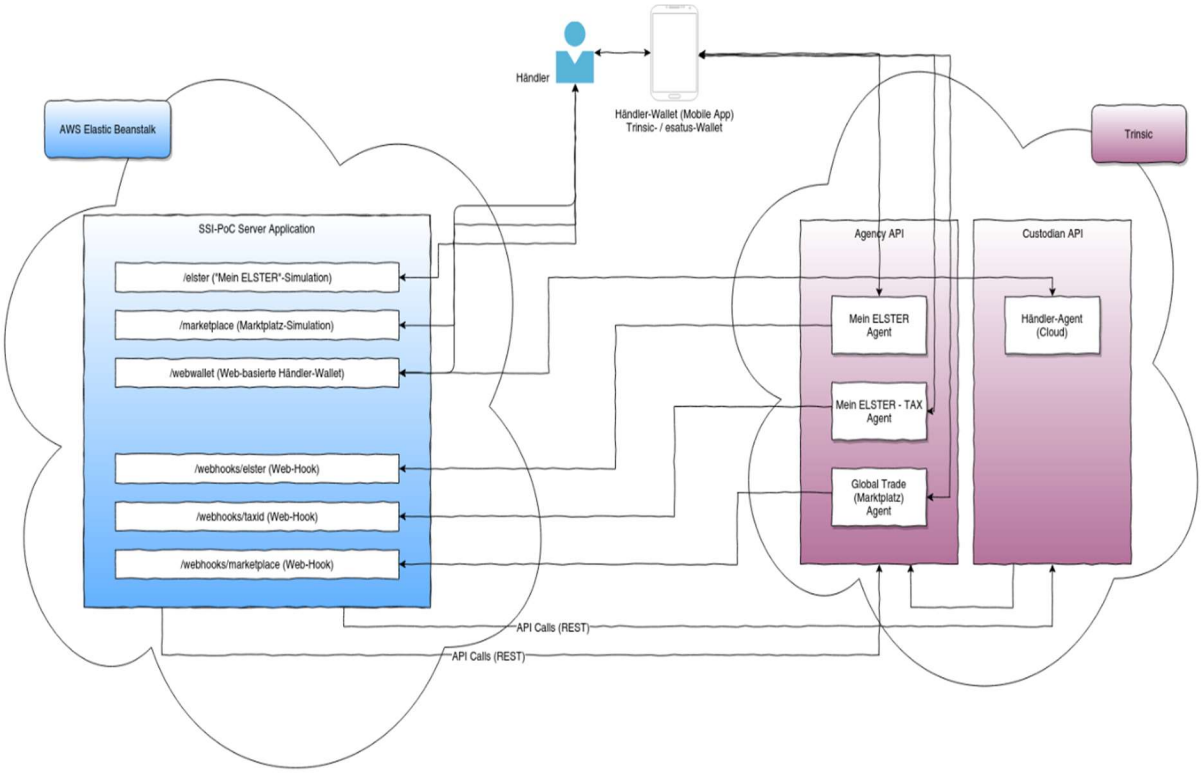


Abbildung 13: Architektur des Prototyps

7.3. Software-Entwicklung

Der Prototyp wurde mit Hilfe der folgenden Infrastruktur entwickelt:

Der SSI-POC Prototyp wurde mit Hilfe zweier Instanzen der AWS Elastic Beanstalk Umgebungen entwickelt. Beide Instanzen verwenden einen voneinander getrennten, persistenten Datenspeicher in einer Amazon S3 Storage. Dort wird die SQLite Datenbank abgelegt, in der der Prototyp zustandsbehaftete Informationen persistiert.

Zur Umsetzung der „Self Sovereign Identity“-spezifischen Anteile des Prototyps wurde die SSI-Plattform von Trinsic benutzt. Mit Trinsic Studio, der Administrationsoberfläche, steht ein Baukasten für diese Art von Anwendungen bereit. Zunächst muss der sogenannte Ledger festgelegt werden - das ist die Blockchain, auf der die öffentlichen Informationen des Prototyps hinterlegt sind. Dann werden sogenannte Organizations angelegt: Dies sind alle Unternehmen und Institutionen, die Credentials erstellen bzw. überprüfen wollen.

Onlinehändler sind Personen, die mit diesen Organizations im definierten Use-Case Daten austauschen. Sie besitzen keine Enterprise-Wallets, sondern eine persönliche, private Wallet, für die sie selbst verantwortlich sind.

7.4. Prozessübersicht

Der Prototyp bildet die folgenden Prozesse / Use-Cases ab:

Der Händler erhält eine dezentral beweisbare Bestätigung seiner Identität, mit der er sich ausweisen kann (ELSTER-Credential). Ergänzend erhält er das Tax-Credential, ein Nachweis darüber, dass er steuerlich erfasst, das heißt, zur Entrichtung von Umsatzsteuer angemeldet ist.

Der Händler beweist dem Marktplatz seine Identität und seine steuerliche Erfassung mit seinen beiden Credentials "ELSTER-Credential" und "Tax-Credential".

Der Marktplatzbetreiber überprüft regelmäßig, ob der Händler noch ein gültiges Tax-Credential besitzt. Hier Regelfall: Das Tax-Credential des Händlers ist noch gültig.

Der Marktplatzbetreiber überprüft regelmäßig, ob der Händler noch ein gültiges Tax-Credential besitzt. Hier Sonderfall: Das Tax-Credential des Händlers ist nicht mehr gültig.

Ausführliche Darstellungen dieser Prozesse wurden im Rahmen der Projektdokumentation erstellt und können bei den Autoren nachgefragt werden. Im Folgenden werden diese Use-Cases grob skizziert.

Zu Beginn will der Händler eine Bestätigung über sich und sein Tax-Credential einfordern, damit er eine dezentrale beweisbare Bestätigung seiner Identität besitzt, mit welcher er sich ausweisen kann (siehe Abbildung 14: Teilprozess A). Dafür meldet er sich bei Mein ELSTER an und wählt den Bereich „ELSTER-Credential beantragen“, dadurch stellt der Händler eine Vertrauensbeziehung mit dem „Mein ELSTER“-Agenten her. Darauffolgend erhält der Händler auch schon die Bestätigung, das „ELSTER-Credential“ (VC).

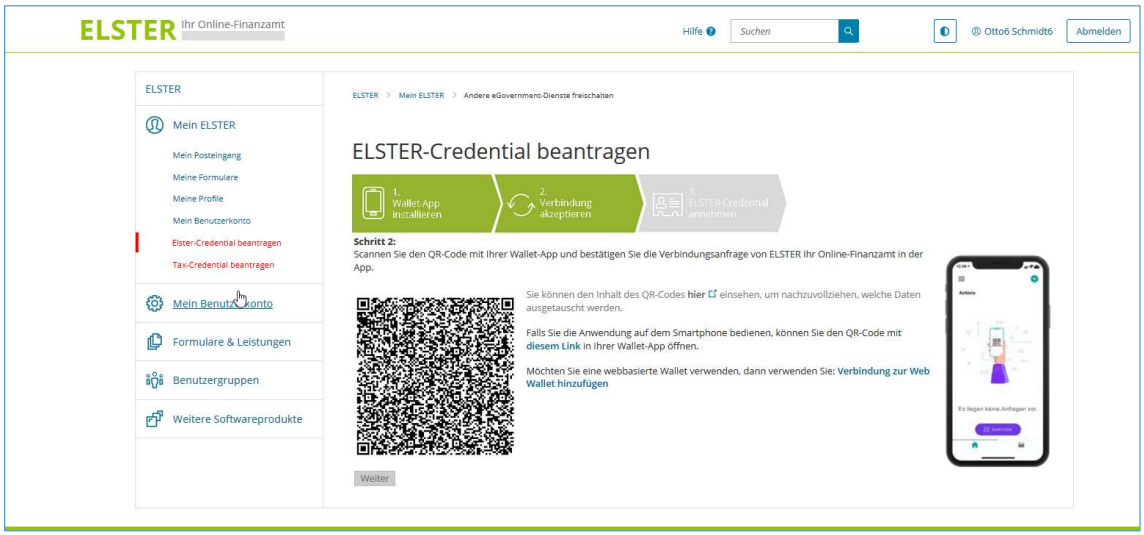


Abbildung 14: Teilprozess A

Im nächsten Schritt kümmert er sich um sein Tax-Credential, also den Nachweis, dass er steuerlich erfasst ist (siehe Abbildung 15). Dafür meldet er sich wieder bei Mein ELSTER an und wählt dieses Mal den Bereich „Tax-Credential beantragen“. Nun stellt die Website eine Vertrauensbeziehung zum „Mein ELSTER – TAX“-Agent her und der Händler erhält kurz danach seinen Tax-Credential.

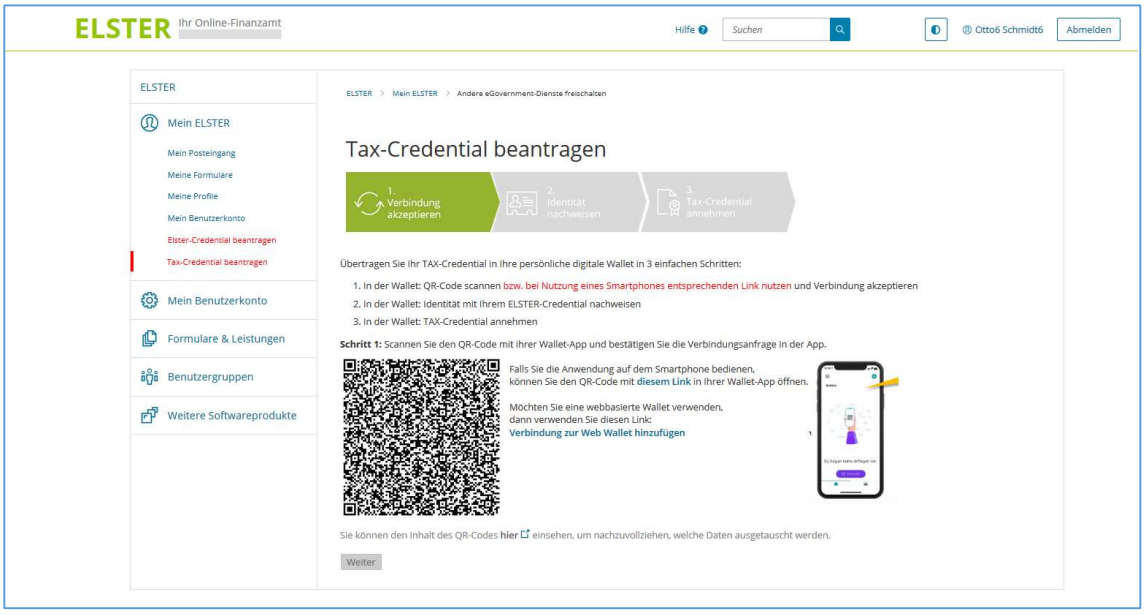


Abbildung 15: Teilprozess B

Mit dem ELSTER-Credential und dem Tax-Credential ist der Onlinehändler in der Lage, sowohl seine Identität als auch seine steuerliche Erfassung nachzuweisen. Er meldet er sich nun bei „Global Trade“ (dem Online-Marktplatz seiner Wahl) an und startet den Prozess „Tax-Credential nachweisen“ (siehe Abbildung 16). Daraufhin muss der Händler sein ELSTER-Credential und sein Tax-Credential vorzeigen. Der Marktplatzbetreiber kann auf diese Weise die Identität des Händlers überprüfen und sicher sein, dass der Händler steuerlich erfasst ist. Er stellt dem Händler ein Marktplatz-Credential aus, welches dem Händler als Nachweis dient, dass er auf diesem Marktplatz Handel treiben darf.

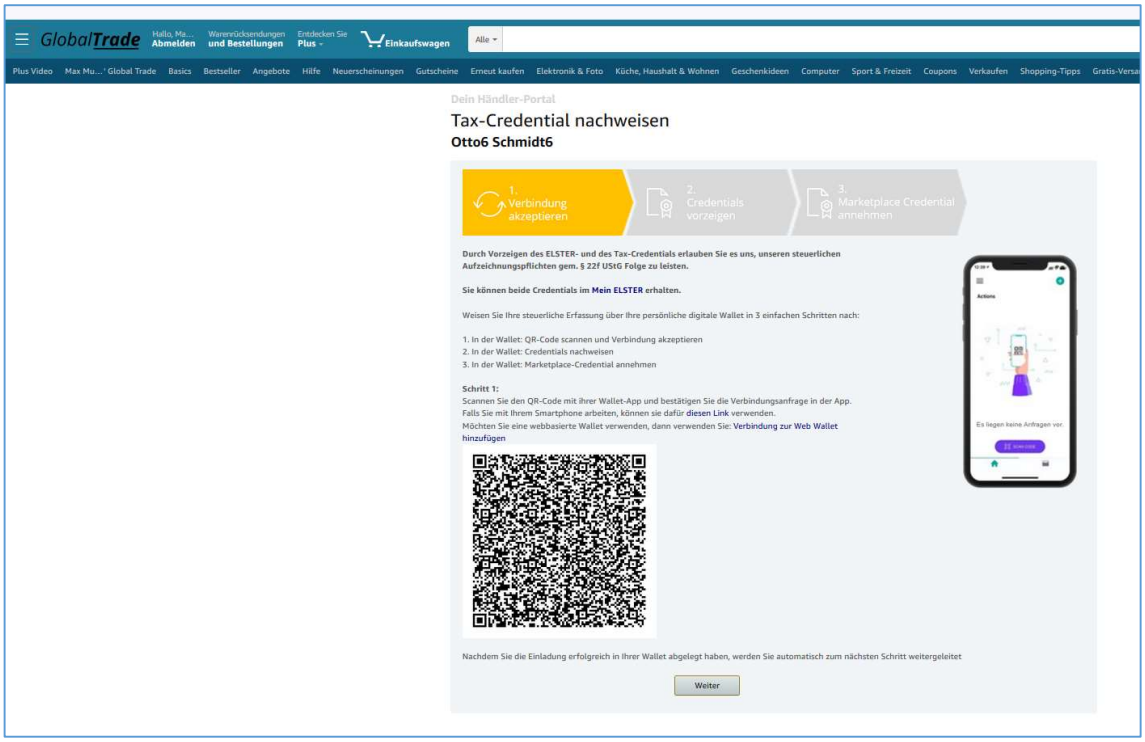


Abbildung 16: Teilprozess C

Da der Marktplatz in der Verantwortung steht, nur Händler zuzulassen, die auch ein gültiges Tax-Credential haben, sollte davon ausgegangen werden, dass er die Gültigkeit der Tax-Credentials in regelmäßigen Abständen erneut bewiesen haben will. Dafür veranlasst der Markplatzbetreiber die erneute Prüfung des Tax-Credentials des Händlers, indem er dem Händler einen Proof-Request zukommen lässt, um ihn aufzufordern einen gültigen Proof (in diesem Fall das gültige Tax-Credential) vorzuzeigen (siehe Abbildung 17).

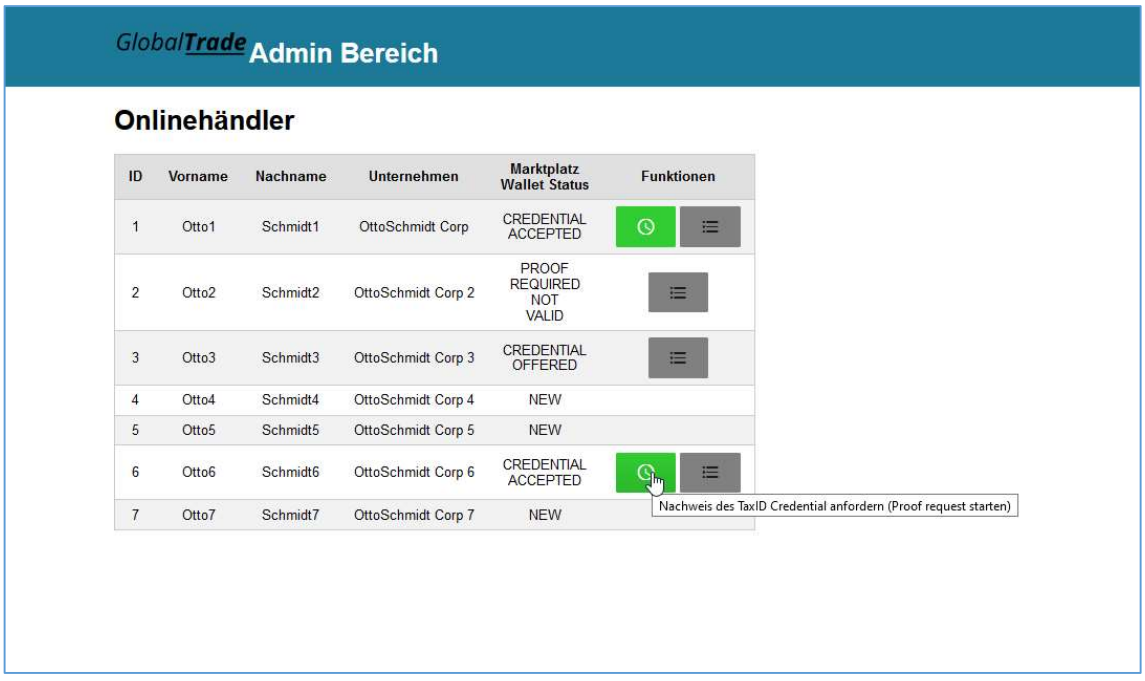
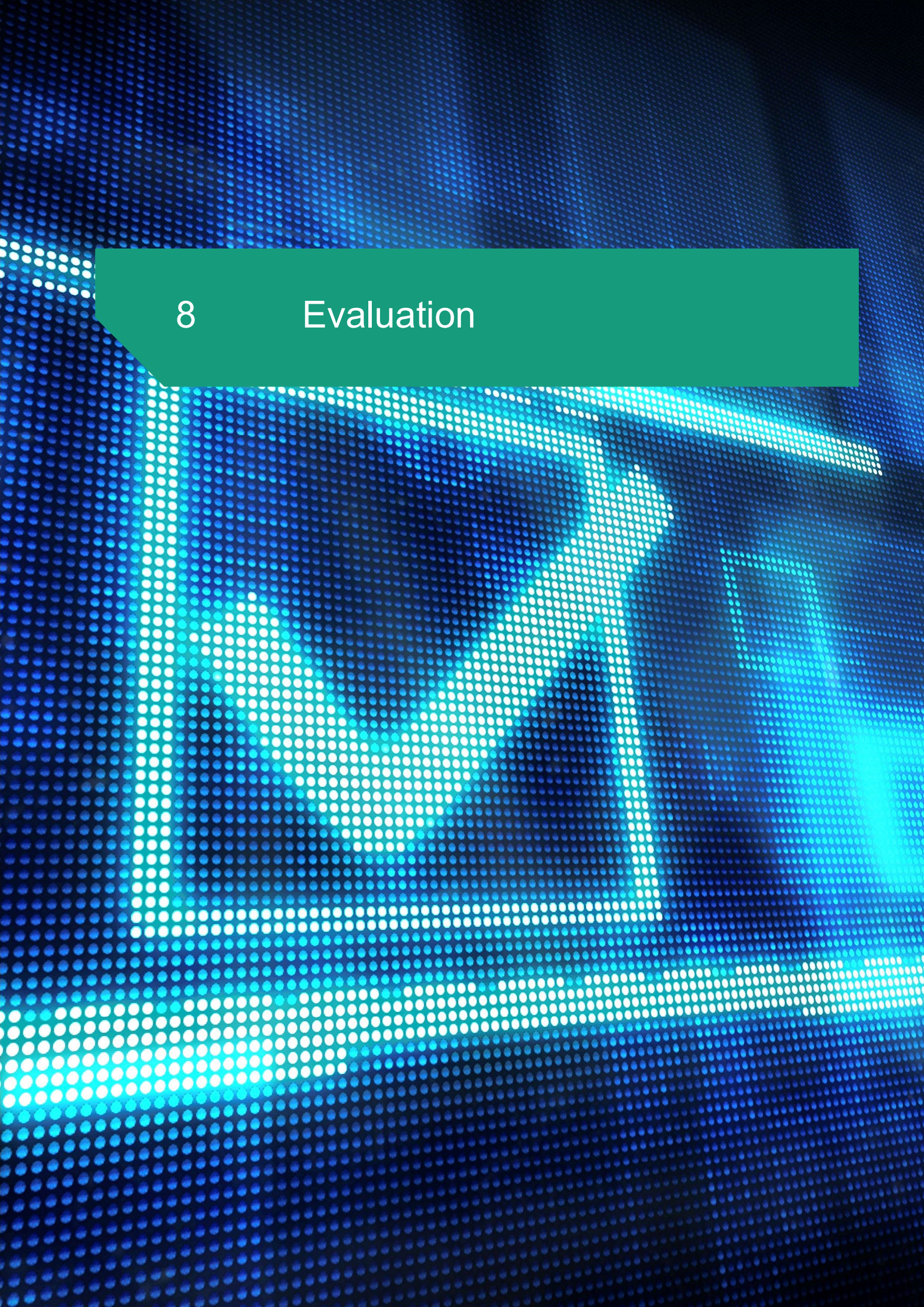


Abbildung 17: Teilprozess D



8 Evaluation

8. Evaluation

Für die Evaluation des Prototyps und die Evaluation des theoretischen Lösungsvorschlags wurde eine dreigeteilte Struktur ausgewählt. Anhand der Anforderungen, die im Kapitel 5 definiert wurden, findet die Evaluation sowohl unter rechtlichen, technischen als auch organisatorischen Blickwinkeln statt. In den jeweiligen Unterteilen der Evaluation werden sowohl die diversen Stakeholder des Systems als auch die Komponenten des Systems berücksichtigt. Dabei werden in der Evaluation der Prototyp sowie das grundlegende Basiskonzept des Systems unterschieden. Somit wird zum einen eine Evaluation des Projektfortschritts, zum anderen der entworfenen Gesamtidee ermöglicht.

Insgesamt wird die Evaluation auf drei unterschiedlichen Ebenen durchgeführt (siehe Tabelle 1). Pro Anforderung in den jeweiligen Ebenen wurden überdies Indikatoren definiert, die Aufschluss geben, ob einzelne Anforderungen umsetzbar sind oder sich Hindernisse während des Projekts gezeigt haben. Die Evaluation findet sowohl für den Prototyp als auch das Gesamtkonzept statt.

Tabelle 1: Evaluation des entwickelten Systems

Kategorie	Anforderung	Zusammenfassung	Bewertung
Wirtschaftlich / Organisational	Innovationspotenzial	Der Prototyp und das Konzept weisen durch den Einsatz vielversprechender Technologien und einer Erweiterbarkeit über den definierten Anwendungsfall hinaus, eine hohes Innovationspotenzial auf.	
	Flexibilität	Das System weist eine hohe Flexibilität auf, ist dabei allerdings durch die grundsätzlichen Eigenschaften von SSI limitiert.	
	Skalierbarkeit	Das System weist eine gute Skalierbarkeit auf, wenngleich Referenzen zu Zahlen im Produktivbetrieb fehlen.	
	Benutzerfreundlichkeit	Die Benutzerfreundlichkeit ist durch die Einbettung in bestehende Nutzeroberflächen gegeben, weist jedoch auch neue SSI-bedingte Oberflächen und Prozesse auf. Der hohe Interaktionsumfang lässt sich in einem Produktivsystem gut adressieren.	

	Entwicklungs-/Betriebsaufwand	Die Entwicklungs-/ und vor allem die Betriebskosten fallen im Vergleich zu einem bei ELSTER zentralistisch betriebenem System höher aus.	
Technisch	Datenintegrität	Das System weist eine hohe Datenintegrität über die gesamte Prozesskette auf.	
	Datenvertraulichkeit	Das System weist einen hohen Grad an Datenvertraulichkeit auf, wobei ein gewisses Restrisiko an einigen Komponenten bestehen bleibt.	
	Datenverfügbarkeit	Durch die Blockchain-Komponente wird stellenweise eine bessere Verfügbarkeit des Systems gewährgeleistet. Jedoch fordern die zum Einsatz kommenden kryptographischen Maßnahmen eine höhere Komplexität bei der Wiederinbetriebnahme.	
Rechtlich	Rechtssicherheit und -konformität	Der Prototyp ist flexibel und kann an die sich im Wandel befindenden gesetzlichen Vorgaben des Umsatzsteuergesetzes in einem Rahmen angepasst werden, der es ermöglicht, die zentralen Elemente umzusetzen. Datenschutzrechtlich ist vor allem der Einsatz der Blockchain-Technologie ein Risikofaktor. Durch den SSI-Ansatz und bei einer entsprechenden Gestaltung werden diese Risiken minimiert. Solange aber keine gesetzliche Klarheit herrscht, wird jedoch ein Restrisiko bestehen bleiben.	

Im Folgenden wurden für die Kategorien verschiedene Indikatoren aufgestellt, welche Zwischenziele zur Erreichung des jeweiligen Hauptzieles darstellen und so eine differenzierte Evaluation ermöglichen.

Innovationspotenzial

Der Prototyp und das Konzept weisen durch den Einsatz vielversprechender Technologien und einer hohen Erweiterbarkeit über den definierten Anwendungsfall hinaus eine hohes Innovationspotenzial auf.

Indikator 1: Das Konzept sowie der Prototyp des Systems sollten in ein vorteilhaftes Produktivsystem überführbar sein

Während der Prototyp aufzeigt, dass eine Umsetzung prinzipiell möglich ist, ist die Vorteilhaftigkeit zusätzlich mit zukünftigen Nutzern eines Produktivsystems zu evaluieren.

Indikator 2: Das System sollte sich technisch und prozessual für Anwendungen außerhalb des Steuerumfelds weiterentwickeln lassen

Das SSI-System steht prinzipiell auch Institutionen außerhalb des Steuerumfeldes zur Verfügung und weist keine steuer-spezifischen Komponenten abseits des ELSTER-Portals auf, womit auch Anwendungen außerhalb des Steuerumfeldes möglich sind.

Indikator 3: Das System sollte neue technologische Ansätze benutzen und somit einen Wissenszuwachs in der Finanzverwaltung ermöglichen

Das SSI-Konzept wird als vielversprechend wahrgenommen und wird auf verschiedenen politischen Ebenen untersucht. Im Rahmen des Projektes wurden hierzu unterschiedliche Technologien im Steuerkontext aufgearbeitet und ihre Einsatzmöglichkeiten erforscht.

Flexibilität

Das System weist eine hohe Flexibilität auf, ist dabei allerdings durch die grundsätzlichen Eigenschaften von SSI limitiert.

Indikator 1: Das System sollte Anpassungen an rechtl. Rahmenbedingung umsetzen können

Anpassungen an rechtliche Rahmenbedingungen sind flexibel umsetzbar, solange sich diese an dem Grundkonzept von SSI (Beweis von Eigenschaften durch Eigenschaftsbesitzer) ausrichten lassen.

Indikator 2: Das System sollte erweiterbar für andere Anwendungsbereiche im Steuerumfeld sein

Erweiterbarkeit für andere steuerliche Anwendungen ist gegeben, sofern es sich um Eigenschaftsnachweise handelt und technische Limitationen (Anzahl Credentials, bilaterale Interaktionen) berücksichtigt wurden.

Indikator 3: Das System sollte Interoperabilität zu anderen Systemen gewährleisten

Durch die Nutzung offener Standards und plattformunabhängiger Komponenten ist eine hohe Interoperabilität des Systems gegeben.

Skalierbarkeit

Das System weist eine gute Skalierbarkeit auf, wenngleich Referenzen zu Zahlen im Produktivbetrieb fehlen. Ggf. sind organisatorische Beschränkungen aufzuerlegen.

Indikator 1: Das System sollte technisch skalierbar sein, um alle fachlichen Anforderungen zu erfüllen

Das System ist grundsätzlich technisch skalierbar, wobei Rückschlüsse auf Zahlen im Produktivbetrieb schwierig sind. Gegebenenfalls müssen organisatorisch veranlasste Einschränkungen gegen die Systembelastung durchgeführt werden.

Indikator 2: Das System sollte Automatisierung von Vorgängen erlauben

Während der Prototyp noch diverse manuelle Interaktionen beinhaltet, ist eine Automatisierung der Vorgänge durch die Nutzung von maßgeschneiderten Softwarekomponenten grundsätzlich möglich.

Indikator 3: Das System sollte dynamisch und mit überschaubarem Aufwand skalierbar sein

Alle zentralen Elemente skalieren ähnlich wie existierende zentrale Lösungen. Alles was dezentral ist, bringt neue Herausforderungen mit sich.

Datenintegrität

Das System weist hohe Datenintegrität auf, jedoch bedarf es der Beachtung entsprechender Prozesse, um eine Korrektheit der in das System aufzunehmenden Daten zu erreichen.

Indikator 1: Das System sollte gewährleisten, dass Daten korrekt sind und den zugrunde liegenden Sachverhalt widerspiegeln

Sobald die Daten innerhalb des Systems (digitalisiert) sind, ist eine hohe Datenkorrektheit durch technische Gegebenheiten gegeben. Der Onboarding-Prozess muss jedoch zunächst entsprechend ausgestaltet werden.

Indikator 2: Das System sollte gewährleisten, dass Daten nicht unerlaubterweise modifiziert werden

Verschiedene kryptographische Maßnahmen sowie der Einsatz von DLT verhindern unerlaubte Datenmodifikation.

Indikator 3: Das System sollte eine temporale Korrektheit vorliegender Daten ermöglichen

Für die Daten, die auf der Blockchain abgewickelt werden, lässt sich eine hohe temporale Korrektheit attestieren, während die übrigen Prozesse einem bilateral definierten Zeitverständnis unterliegen.

Datenvertraulichkeit

Das System weist einen hohen Grad an Datenvertraulichkeit auf, wobei ein gewisses Restrisiko an einigen Komponenten bestehen bleibt.

Indikator 1: Das System sollte gewährleisten, dass Parteien nur Zugriff auf die für sie fachlich relevanten Daten erhalten

Bis auf die auf der Blockchain abgespeicherten Daten sowie die Tails-Files liegen alle relevanten Daten nur bei den jeweiligen Prozessbeteiligten.

Indikator 2: Parteien ohne berechtigtes Interesse sollten über die Eigenschaft einzelner Personen oder Unternehmen sowie deren Handeln keine Informationen erlangen können

Generell sind alle bilateralen Vorgänge für Drittparteien nicht nachvollziehbar. Dennoch gibt es bspw. für Betreiber d. Netzknoten grundsätzlich die Möglichkeit, Vorgänge nachzuvollziehen.

Indikator 3: Das System sollte unerlaubten Datenzugriff erkennbar machen

Die zum Einsatz kommenden SSI-Komponenten weisen keine Protokollierung von Datenzugriffen auf, sind aber prinzipiell erweiterbar.

Datenverfügbarkeit

Durch die Blockchain-Komponente wird stellenweise eine bessere Verfügbarkeit des Systems gewährgeleistet. Jedoch fordern die zum Einsatz kommenden kryptographische Maßnahmen eine höhere Komplexität bei der Wiederinbetriebnahme.

Indikator 1: Die Dienstbereitstellung des Systems sollte für alle Beteiligten durchgängig gewährleistet sein

Während die Blockchain als dezentrales System inhärent eine hohe Ausfallsicherheit aufweist, sind die ELSTER-Komponente und die Bereitstellung der Tails-File zentralistisch konzipiert und müssen auf zusätzliche Maßnahmen zur Ausfallsicherung zurückgreifen. Für die Wallets sind die jeweiligen Besitzer selbst verantwortlich.

Indikator 2: Das System sollte im Falle von Störungen schnell wieder zu einem Betriebsstand gebracht werden können

Das System weist keine Auffälligkeiten bezüglich der Wiederinbetriebnahme von Komponenten auf. Es sind jedoch Backup- und Restore-Konzepte für bestimmte Daten (Keys etc.) zu beachten.

Benutzerfreundlichkeit

Die Benutzerfreundlichkeit ist durch die Einbettung in bestehende Nutzeroberflächen gegeben, weist jedoch auch neue Oberflächen und Prozesse seitens SSI auf. Der hohe Interaktionsumfang lässt sich in einem Produktivsystem gut adressieren.

Indikator 1: Das System sollte in bestehenden und vertrauten Umgebungen eingebettet sein

Das System erlaubt eine Integration in die bestehenden Benutzeroberflächen sowohl von ELSTER als auch potenzieller Marktplätze.

Indikator 2: Das System sollte keine neuen und/oder ungewöhnlichen Oberflächen oder Geräte benötigen

Während der Prototyp noch auf eine ungewöhnliche Nutzung des Smartphones als Zweitgerät setzt, ist für ein Produktivsystem eine integrierte Lösung möglich.

Indikator 3: Die Komplexität der Interaktion soll in Umfang und Tiefe möglichst gering sein

Die hohe Nutzungskomplexität ergibt sich aktuell hauptsächlich aus der hohen Anzahl an Interaktionen, welche in einem Produktivsystem jedoch adressierbar wäre.

Entwicklungs-/Betriebsaufwand

Die Entwicklungs-/ und vor allem die Betriebskosten fallen im Vergleich zu einem bei ELSTER zentralistisch gehosteten System höher aus.

Indikator 1: Die Aufwendungen für die Implementierung des Systems sollten möglichst gering sein

Das System kann auf eine Vielzahl existierender Open-Source Lösungen zurückgreifen, was einen Entwicklungsaufwand potenziell verringert. Vereinzelt müssen spezielle Anpassungen getroffen werden, um spezifische Anforderungen an ein Produktivsystem zu erfüllen.

Indikator 2: Die Aufwendungen für den laufenden Betrieb des Systems sollte möglichst gering sein

Während die Lösung für ELSTER lediglich zusätzliche Kosten durch Gebühren der Schreibvorgänge aufweisen könnte, entstehen für die Onlinehändler und Marktplätze potenziell zusätzliche Kosten durch die Verwaltung ihrer Wallets.

Rechtssicherheit und -konformität

Eine rechtskonforme Gestaltung scheint durchaus möglich. Datenschutzrechtlich ist vor allem der Einsatz der Blockchain Technologie zu beachten. Durch den SSI-Ansatz und bei einer entsprechenden Gestaltung können Risiken aber weitgehend minimiert werden.

Umsatzsteuerliche Vorgaben

Das vorgeschlagene Konzept weicht zwar an manchen Stellen von den umsatzsteuerlichen Vorgaben ab, für die Umsetzung sollte aber eine entsprechende Gestaltung der Rechtsverordnung ausreichen. Eine Gesetzesänderung könnte mehr Sicherheit geben, ist im Grunde jedoch nicht nötig.

Sollte es zu einer Änderung der gesetzlichen Grundlage, z.B. zu einer Verpflichtung zur Verwendung der Umsatzsteuer-Identifikationsnummer, kommen, kann das System flexibel angepasst werden.

Anforderungen der Datenschutz-Grundverordnung

Wenn die umsatzsteuerlichen Vorgaben eingehalten werden, kann das Umsatzsteuergesetz als Grundlage für die Datenverarbeitung dienen. Abseits der Blockchain kann der Prozess dann ohne Weiteres so gestaltet werden, dass er der Datenschutz-Grundverordnung entspricht. Für die Daten auf der Blockchain ist die Einschätzung schwieriger. Nach hier vertretener Auffassung können aber auch hier Gestaltungen gewählt werden, die eine Umsetzung gemäß der Datenschutz-Grundverordnung ermöglichen. Allerdings können nicht alle Risiken eliminiert werden, zumal gerade im Bereich der Blockchain Technologie noch allgemein Klärungsbedarf von Seiten der Gesetzgebung und der Rechtsprechung besteht.

Im Prototyp werden keine personenbezogenen Daten verarbeitet. Damit ist der Anwendungsbereich der Datenschutz-Grundverordnung nicht eröffnet. An den Stellen, an denen auf externe Anbieter zurückgegriffen wird, wird davon ausgegangen, dass diese ebenso wenig personenbezogene Daten verarbeiten oder andernfalls dies entsprechend der Datenschutz-Grundverordnung tun.

Vorgaben der Abgabenordnung

Ein hohes Niveau an Datensicherheit ermöglicht es, die speziellen Vorschriften der Abgabenordnung zu erfüllen. Bei richtiger Nutzung des Konzepts werden keine Daten, die für einen Außenstehenden verständlich wären, auf die Blockchain geschrieben oder anderweitig offenbart.

Eine abschließende und umfassende Bewertung der rechtlichen Aspekte findet sich in einem gesonderten Rechtsgutachten.

9 Diskussion und Fazit

9. Diskussion und Fazit

9.1. Weitere Einsatzmöglichkeiten im Steuerbereich

Um den Nutzen der entwickelten Lösung zu erhöhen, soll die Lösung in weiteren Bereichen des Steuerfeldes und darüber hinaus nutzbar sein. Im Folgenden werden verschiedene weitere Anwendungsmöglichkeiten im Steuerkontext aufgezeigt:

Aufgrund der Ausgestaltung des Lösungskonzepts als ein generisches SSI-System, bestehend aus Aussteller, VC-Besitzer und Überprüfer, ist eine Übertragbarkeit auf zahlreiche Verfahren im Steuerbereich denkbar, in denen Nachweise von einer Finanzbehörde ausgestellt werden, ein Steuerpflichtiger als Dateninhaber auftritt und im Nachweis enthaltene Eigenschaften einer interessierten Drittpartei bewiesen werden müssen. Dies könnte beispielsweise den Nachweis einzelner Beträge oder Besteuerungsgrundlagen aus einem Steuerbescheid umfassen. Denkbar wäre bspw. der Nachweis einer bestimmten Einkommenshöhe als Klartext oder per Zero-Knowledge-Proof gegenüber Kreditinstituten. Auch andere Behörden oder juristische Personen des öffentlichen Rechts können als Überprüfer der von der Finanzverwaltung ausgestellten Credentials fungieren. Beispielsweise werden bei der Beantragung von BAföG Vermögensnachweise benötigt, die beim zuständigen Studentenwerk aktuell durch Einreichen des jeweiligen Einkommensteuerbescheids der Eltern oder des Ehegatten des Antragstellers erbracht werden. Dabei werden jedoch nicht nur Einkommensverhältnisse offengelegt, sondern auch sensible Daten wie bspw. der Sonderausgabenabzug oder die Höhe der außergewöhnlichen Belastungen. Durch selektiven Nachweis lediglich der notwendigen Information aus dem Einkommensteuerbescheid mit Hilfe eines entsprechenden Credentials könnte dieser Nachteil vermieden werden. Gleiches gilt für Nachweise über Einkommensverhältnisse im Sozialrecht.

Für Steuerpflichtige wäre ferner der Nachweis einer Freistellungsbescheinigung im Zusammenhang mit der Bauabzugsteuer oder Freistellungen im Bereich der Kapitalertragsteuer (z.B. Nichtveranlagungsbescheinigungen) denkbar. Derzeit werden diese Bescheinigungen mit einem Ablaufzeitraum von drei Jahren papierbasiert ausgestellt, was Probleme bei einem möglichen Widerruf während dieses Zeitraums mit sich bringt. Insbesondere ist im SSI-Kontext vorteilhaft, ein Credential jederzeit zurücknehmen zu können, wenn die Voraussetzungen bspw. für die Nichtveranlagung wegfallen. Fälschungen kann effektiver entgegengewirkt werden.

Die Finanzbehörde ist gleichermaßen als Überprüfer für von anderen Behörden ausgestellte Nachweise vorstellbar, bspw. bei Einholung des Nachweises über den Grad der Behinderung im Zusammenhang mit der Prüfung von außergewöhnlichen Belastungen.

9.2. Fazit und weiteres Vorgehen

Das vorliegende Forschungsprojekt umfasst die Konzeptionierung, prototypische Umsetzung und Evaluation eines Blockchain-basierten Systems zur Bekämpfung von Steuerausfällen auf Online-Marktplätzen. Dabei wurden zunächst die bestehenden Prozesse analysiert und Verbesserungspotenziale identifiziert. Der aktuell genutzte, papierbasierte Prozess zeigt dabei wesentliche Ineffizienzen durch Medienbrüche und diverse Fälschungsmöglichkeiten auf.

Zur Lösung der bestehenden Herausforderungen und um Erfahrungen mit den Potenzialen der Blockchain-Technologie in der Steuerverwaltung zu sammeln, wurden deshalb verschiedene Blockchain-basierte Ansätze konzipiert. Dabei wurden drei Vorschläge erarbeitet: im ersten Vorschlag wurde ein Steuer-Token in Erwägung gezogen. In dem Fall repräsentiert ein Token, welcher einem Onlinehändler zugeordnet wird, dessen steuerliche Erfassung. Dieser ist auf einer öffentlichen Blockchain gespeichert. Dadurch ergeben sich jedoch datenschutzrechtliche Risiken sowie einschränkende Abhängigkeiten zu der technischen Infrastruktur. Deshalb wurde ein zweiter Ansatz entworfen, der ein Blockchain-basiertes Gültigkeitsregister darstellt, das auf einem privaten Blockchain-System aufbaut. Dabei stehen allerdings technische Skalierbarkeitsprobleme und hoher Wartungsaufwand im Vordergrund. Aus diesen und weiteren Gründen wurde ein drittes Konzept entwickelt, das auf dem Paradigma der SSI aufbaut.

Hierbei werden – ähnlich der papierbasierten Prozessabläufe – digitale Nachweise über die steuerliche Registrierung an Händler ausgegeben. Diese können dann mittels einer digitalen Geldbörse Beweise über ihre Registrierung und Stammdaten an die Marktplätze geben. Diese Beweise enthalten auch den Status der Gültigkeit ihrer Registrierung, der über einen Indikator auf einer öffentlichen Blockchain geprüft werden kann. Kommunikation findet größtenteils über eine bilaterale Verbindung zwischen den beteiligten Parteien (Finanzbehörden und Onlinehändler, Onlinehändler und Marktplätze) statt, wobei für gelegentliche lesende und schreibende Zugriffe zusätzlich Kommunikation mit einem öffentlichen Blockchain-System stattfindet.

Ein Prototyp, der das System technisch umsetzt, ist aufbauend auf diesem Konzept entwickelt worden. Der Prototyp demonstriert im Besonderen die Prozessabläufe für die einzelnen Prozessbeteiligten. Dabei wurden vor allem die notwendigen Interaktionen ausdetailliert, während für die Umsetzung hauptsächlich auf bestehende Infrastruktur und Komponenten gesetzt wurde. So konnte der gesamte Ablauf von der Ausstellung bis zur Überprüfung von Steuernachweisen erfolgreich simuliert werden.

Eine Evaluation des Gesamtkonzepts hinsichtlich rechtlicher, ökonomischer und technischer Aspekte sowohl des Prototyps als auch des Gesamtkonzepts wurden im nächsten Schritt durchgeführt. Aus rechtlicher Sicht ist festzuhalten, dass die auf andere Technologien ausgelegten gesetzlichen Rahmenbedingungen mitunter eine Hürde für die Konzeptionierung und geplante Umsetzung bedeuten. Hier ist grundsätzlich an den Gesetzgeber zu appellieren, neue Technologiekonzepte in die Überlegungen miteinzubeziehen, um eine rechtskonforme Gestaltung zu erleichtern. Aus datenschutzrechtlicher Sicht bergen gerade die Permanenz und die öffentliche Zugänglichkeit der verwendeten Blockchain-Technologie auch bei einer Umsetzung eines SSI-Systems noch diverse Risiken. Diese können zwar minimiert, aufgrund des Mangels an klaren, etablierten Standards aber nicht vollständig eliminiert werden. Die Evaluation des Prototyps stellte heraus, dass sich der Grundgedanke des Lösungsansatzes technisch umsetzen lässt. Einige technische Hürden, zum Beispiel hinsichtlich der Skalierbarkeit, der eingeschränkten Funktionalitäten aktueller Infrastrukturen zur Verwaltung von Nachweisen, sowie die geringe Anzahl technischer Anbieter, scheinen sich hinsichtlich der fortschreitenden Entwicklung und Forschungsvorhaben auf dem Gebiet SSI potenziell lösen zu lassen. Der Prototyp zeigt, dass generische Komponenten genutzt werden können, um auch Anwendungsfälle über den spezifischen Anwendungsfall hinaus umzusetzen und durch eine gemeinsam genutzte, standardisierte technische Infrastruktur realisierbar sind.

Das vorliegende Forschungsprojekt weist trotz umfassender Analysen und strukturierter Vorge-

hensweisen Limitationen auf. Das Konzept betrachtet zunächst einen Anwendungsfall mit eingeschränkter Zahl teilnehmender Parteien, wobei das SSI-Konzept erst mit einer großen Anzahl teilnehmender Partner sein volles Potenzial entwickelt. Zudem wurden für den Prototyp teilweise Komponenten verwendet, die in einer tatsächlichen Umsetzung in dem Umfang nicht ausreichend wären (z.B. Smartphone-Anwendungen mit hohem Interaktionsgrad). Überdies wurden keine ausführlichen Analysen hinsichtlich der Performance oder tatsächlichen technischen Skalierbarkeit des Systems durchgeführt. Diese Limitationen sollten in weiterführenden Forschungsvorhaben ausführlich adressiert werden.

Zukünftige Forschungsprojekte sollten zusätzlich verschiedene Stakeholder aus der Praxis in Pilottests miteinbeziehen. Dies umfasst insbesondere Onlinehändler und Marktplätze, wodurch sowohl technische Aspekte als auch soziotechnische und -ökonomische Aspekte in realen Bedingungen abgewogen werden können. Umfassende Pilottests über den Anwendungsfall hinaus und damit in größeren SSI-Ökosystemen, sind zudem erstrebenswert. So kann die Kombination von ausgestellten Nachweisen verschiedenster Parteien und interorganisationale Zusammenarbeit erprobt werden. In dem Zug sollten überdies Ansätze wie die Verwendung der Steuer-Identifikationsnummer zum anwendungsübergreifenden Identitätsnachweis erforscht werden, wie in aktuellen Vorschlägen zur Registermodernisierung vorgeschlagen wird. Dazu können die in diesem Projekt gewonnen Erkenntnisse einen wertvollen ersten Schritt darstellen.

10. Literaturverzeichnis

- Clauß, Sebastian; Köhntopp, Marit (2001): Identity management and its support of multilateral security. In: *Computer Networks* 37 (2), S. 205–219. DOI: 10.1016/S1389-1286(01)00217-1.
- ecom (2020): Die Marktplatzwelt 2020 inkl. Landscape Poster Global und DACH. Online verfügbar unter https://www.ecom-consulting.de/marketplace-landscapes/, zuletzt aktualisiert am 27.05.2020+00:00, zuletzt geprüft am 21.07.2020.
- Hyperledger (2020): Aries OpenAPI Demo. Online verfügbar unter https://github.com/hyperledger/aries-cloudagent-python/blob/master/demo/AriesOpenAPIDemo.md.
- Nakamoto, Satoshi (2008): Bitcoin: A peer-to-peer electronic cash system. Manubot.
- Peters, Gareth W.; Panayi, Efstathios (2016): Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. In: Paolo. Tasca, Tomaso. Aste, Loriana. Pelizzon und Nicolas. Perony (Hg.): Banking Beyond Banks and Money. A Guide to Banking Services in the Twenty-First Century. Cham: Springer International Publishing; Imprint: Springer (New Economic Windows), S. 239–278. Online verfügbar unter https://doi.org/10.1007/978-3-319-42448-4_13.
- Reed, Drummond; Law, Jason; Hardman, Daniel (2016): The technical foundations of sovrin. In: *The Technical Foundations of Sovrin*.
- Reed, Drummond; Sporny, Manu; Longley, Dave; Allen, Christopher; Grant, Ryan; Sabadello, Markus; Holth, Jonathan (2020): Decentralized Identifiers (DIDs) v1.0. Core architecture, data model, and representations. Hg. v. W3 Consortium. Online verfügbar unter https://www.w3.org/TR/did-core/.
- Wortfilter (2016a): Amazon Marketplace in Zahlen. Online verfügbar unter https://www.wortfilter.de/news15Q1/5178-Aktuelle-Haendlerzahlen-von-Amazon.php, zuletzt aktualisiert am 21.07.2020.000Z, zuletzt geprüft am 21.07.2020.
- Wortfilter (2016b): eBay_DE Marktplatz in Zahlen. Online verfügbar unter https://www.wortfilter.de/news15Q1/5190-eBay-Zahlen-Haendlerverteilung-nach-Laendern.php, zuletzt aktualisiert am 21.07.2020.000Z, zuletzt geprüft am 21.07.2020.
- Zheng, Zibin; Xie, Shaoan; Dai, Hong Ning; Chen, Xiangping; Wang, Huaimin (2018): Blockchain challenges and opportunities: a survey. In: *IJWGS* 14 (4), S. 352. DOI: 10.1504/IJWGS.2018.095647.