

BLOCKCHAINS EROBERN DIE ÖFFENTLICHE VERWALTUNG



Bitcoin, Blockchain, Ethereum und Distributed-Ledger-Technologien (DLT) sind keine Begriffe aus den Kellern und Garagen passionierter Entwickler und IT-Spezialisten. Diese Technologien haben – nach einem anfänglichen Hype – einen hohen Reifegrad erreicht und sind dabei, sich zu etablieren. Unternehmen und Regierungen können damit neue vertrauenswürdige und zukunftsweisende digitale Ökosysteme und Geschäftsmodelle entwickeln. Der Markt entwickelt sich zunehmend zu einem Partnernetzwerk.

| von STEFFEN SCHWALM

Kerneigenschaften der Blockchain, wie Dezentralität, Diversifizierung der Daten und Knoten zwischen den Nutzern oder grundlegende Fälschungssicherheit und Zuverlässigkeit, ermöglichen potenzielle neue Geschäftsmodelle und bieten Chancen für eine effizientere Digitalisierung in Verwaltung und Wirtschaft. Als besonderes Merkmal der Blockchain wird gern ein spezielles Vertrauensmodell genannt. Hierbei erhofft man sich durch den Verzicht auf eine zentrale Instanz,

die die Kommunikation steuert, verwaltet und das Netzwerk betreibt und der im Grunde alle Nutzer vertrauen, eine schnelle Abwicklung komplexer Prozesse beispielsweise der Automatisierung öffentlicher Register, Beglaubigungen bis hin zur Vereinfachung von Nachweispflichten. Die Einsparung von sogenannten Intermediären, also zum Beispiel Notaren, Banken oder staatlichen Stellen, in digitalen Transaktionen soll die digitale Transformation erleichtern.

Andererseits impliziert die Nutzung zumindest einiger Formen der Blockchain-technologie einen hohen Energieverbrauch, was angesichts laufender Klimaschutzbemühungen kritisch zu bewerten ist. Die der Blockchain immanente Manipulationsunsicherheit birgt zudem Nachteile im Hinblick auf die Vorgaben des Datenschutzes. Zudem unterliegt vor allem die öffentliche Verwaltung – wie auch andere hochregulierte Branchen, wie Luftfahrt, Pharma- und Finanzindus-

trie, Automotive, Gesundheitswesen – umfassenden regulatorischen Vorgaben zur Digitalisierung sowie zur Dokumentation und langfristigen Vorgaben, wie verlustfreien Nachweisen ihrer Prozesse und Aufzeichnungen gegenüber Gerichten, Prüfbehörden und anderen vertrauenswürdigen Dritten.

Konkrete Umsetzungstermine erzeugen in Bund, Land und Kommunen einen zusätzlichen Druck, praktische Lösungen zeitnah wie wirtschaftlich zu etablieren und dabei gegebenenfalls auch neue Wege zu gehen. Dazu gehören beispielsweise die elektronische Bereitstellung aller digitalisierbaren Verwaltungsleistungen bis 2022 und hieraus abgeleitete Verpflichtungen zur Automatisierung öffentlicher Register, um diese Leistungen auch verwaltebeneübergreifend abbilden zu können,

Dieses Spannungsfeld aus Chancen einer neuen Technologie einerseits sowie geltenden regulatorischen Vorgaben und Nachweispflichten andererseits greift die Bundesregierung mit ihrer Blockchainstrategie auf.¹ Mehr als 150 Experten aus Wirtschaft, Wissenschaft und Forschung wurden in die Onlinekonsultation eingebunden, um ein ganzheitliches, branchenübergreifendes Bild der Chancen, Risiken und möglichen Anwendungsfälle der Blockchaintechnologie zu erhalten.² Im Ergebnis liegt eine kohärente Strategie vor, die die Möglichkeiten zur Nutzung von Blockchain in den verschiedenen Branchen ebenso aufzeigt wie mögliche Regulierungs- und vor allem Standardisierungsbedarfe.

Wie lassen sich DLT/Blockchain im Allgemeinen sowie die Blockchainstrategie im Besonderen aus Sicht der öffentlichen Verwaltung beurteilen? Wie integriert sich die neue Technologie in den regulatorischen Rahmen und Stand der Technik? Welche Anwendungsfälle kommen infrage?

BLOCKCHAINTECHNOLOGIE – EIN ÜBERBLICK

Blockchain ist eine spezielle Kategorie der weitaus umfangreicheren Distributed-Ledger-Technologie (DLT). Bei DLT handelt es sich im Wesentlichen um ein dezentrales, verteiltes Peer-to-Peer-Netzwerk technischer Knoten zum gemeinsamen Austausch von Daten und Transaktionen. Faktisch realisiert die DLT ein verteiltes Register oder Journal zwischen den beteiligten Parteien. Sofern die Daten in sequenziellen Blöcken organisiert sind, deren Integrität über Hashketten abgesichert ist, handelt es sich um eine Blockchain. Bei anderen Distributed-Ledger-Technologien sind die Datenstrukturen einfacher aufgebaut – die Integritätssicherung über entsprechende Hashfunktionen ist allen DLT gleich.³

Der Konsensmechanismus stellt eine Kernkomponente von DLT dar und stellt die übereinstimmende Speicherung der Daten in der Blockchain auf den verschiedenen Netzwerkknoten sicher. Der bekannteste ist dabei „Proof of Work“, wie er insbesondere bei Bitcoin zum Einsatz kommt, der jedoch aufgrund der Komplexität des Verfahrens einen immens hohen Energiebedarf hat. Andere Konsensverfahren wie beispielsweise „Proof of Authority“ oder „Notary“ sind aufgrund effizienterer Konsensfindung deutlich ressourcenschonender [Ko18], [CGR11], [BSI19]. Jede Transaktion wird eindeutig in der DLT dokumentiert. Über regelbasierte Programme (sogenannte Smart Contracts) können Prozessregeln für eine Transaktion entsprechend den definierten Voraussetzungen abgewickelt werden. [BSI19], [Ko18], [DINTS31648], [Na08], [WEKJ17].

DLT werden typischerweise hinsichtlich Zugriff, Beteiligung der Nutzer und Berechtigungen wie folgt unterschieden:

- Öffentliche DLT/Blockchain: Alle Nutzer haben Einsicht in alle Transaktionen.
- Private DLT/Blockchain: Einsicht nur für berechnete Nutzergruppen.
- Genehmigungsfreie DLT/Blockchain: Alle Netzwerkknoten (Nutzer) dürfen Transaktionen durchführen und validieren.
- Private DLT/Blockchain: Nur berechnete Netzwerkknoten (Nutzer) dürfen Transaktionen durchführen und validieren.

Öffentliche, genehmigungsfreie DLT/Blockchains entsprechen dem gern verwendeten Idealbild, bei dem das Vertrauen in die Korrektheit der Daten faktisch ausschließlich durch die Community erzeugt wird, die die Blockchain als quasi gemeinsames Netzwerk „betreibt“. Unabhängig von weiteren Angriffsszenarien würde nur eine Übernahme von 51 % des Netzwerks eine Kompromittierung ermöglichen, was technisch zwar aufwendig, aber nicht ausgeschlossen ist.

Private genehmigungspflichtige DLT/Blockchains werden von einer oder mehreren Institutionen (beispielsweise in einem Konsortium) betrieben. Hier werden die Kerneigenschaften der DLT, wie dezentrale, verteilte, unveränderliche Speicherung in einem verteilten Netzwerk für übergreifende Prozesse zwischen den Beteiligten, mit den bestehenden Maßgaben hinsichtlich Dokumentation und Nachweisfähigkeit gegenüber vertrauenswürdigen Dritten sowie dem Vorteil klarer Verantwortlichkeiten im Fehlerfall verbunden. Daher ist dieser erst später entstandene DLT-Typ besonders in regulierten Branchen deutlich umfangreicher im Einsatz als die „klassische Blockchain“.

Von On-Chain-Speicherung spricht man, wenn Daten auf der DLT/Blockchain abgelegt werden. Werden nur deren Hashwerte abgelegt, spricht man von Off-Chain-Speicherung. Im Gegensatz zu anderen verteilten Systemen können ein-

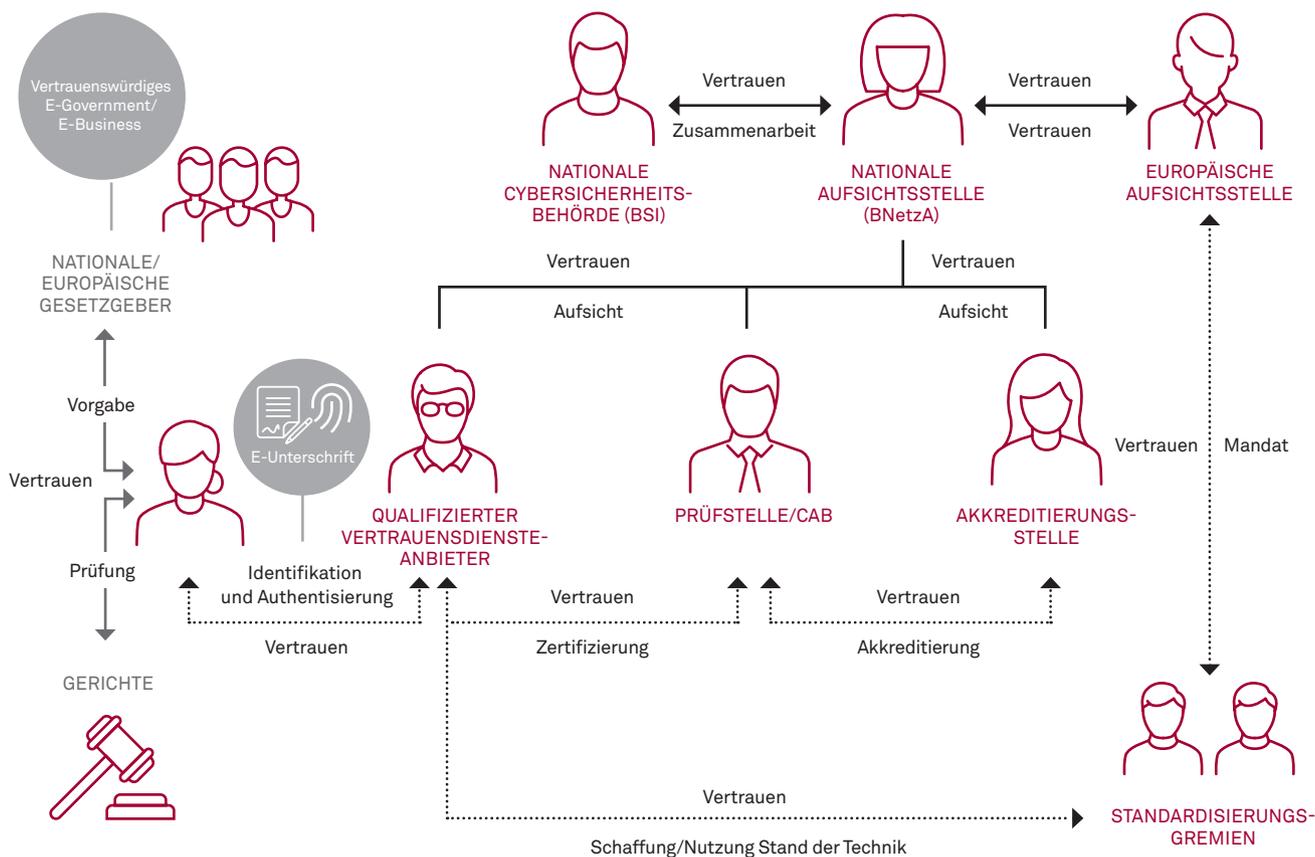


Abbildung 1: Vertrauenskette am Beispiel der eIDAS-Verordnung

mal auf der DLT/Blockchain gespeicherte Daten nicht gelöscht oder verändert werden. Ebenso bestehen aktuell keine standardisierten Möglichkeiten zum Datenexport [Ko18], [BSI19]. Dies ist insbesondere aus Sicht des Datenschutzes kritisch zu bewerten. Die Performance, wie Skalierbarkeit der DLT/Blockchain, ist im Vergleich zu anderen verteilten Systemen begrenzt, was vor allem für die On-Chain-Speicherung nachteilig ist.

Diese technologischen Unterschiede greift auch die Blockchainstrategie der Bundesregierung zu Recht auf, zumal die Eigenschaften der verschiedenen DLT in der Praxis eine entscheidende Auswirkung auf die möglichen An-

wendungsfälle besitzen, was vor allem in hochregulierten Branchen wie der öffentlichen Verwaltung gilt. Die Umsetzung der regulatorischen Vorgaben nach dem Stand der Technik, das Etablieren klarer Verantwortlichkeiten und Richtlinien für die Prozessabwicklung sowie der Nachweis behördlicher Entscheidungsprozesse gegenüber Dritten ist eine wesentliche Rahmenbedingung des vertrauenswürdigen E-Governments. Dies schließt die Nutzung von DLT/Blockchain für die digitale Verwaltung nicht aus, wie die Blockchainstrategie zu Recht ausführt. Vielmehr muss DLT/Blockchain, wie jede neue Technologie, in den bestehenden regulatorischen wie technischen Rahmen integriert werden.

Es gilt, dass die Technologie den Branchenvorgaben folgt, nicht umgekehrt. Insofern müssen regulatorische Anpassungen kritisch auf ihre tatsächliche Notwendigkeit geprüft werden.

VERTRAUENSWÜRDIGE DIGITALE TRANSAKTIONEN IM E-GOVERNMENT UND DLT/BLOCKCHAIN

Vertrauenswürdige digitale Prozesse ermöglichen den eindeutigen und verlustfreien Nachweis der Authentizität, Integrität und Zuverlässigkeit der bei der Transaktionsabwicklung entstehenden oder empfangenen geschäftsrelevanten Aufzeichnungen bis zum Ablauf der geltenden Aufbewahrungsfristen zwischen

2 und 100 Jahren gegenüber Gerichten, Prüfbehörden, Dritten. Vertrauenswürdigkeit wird grundsätzlich durch den Nachweis von

- Authentizität (eindeutige Zuweisbarkeit von Aufzeichnungen und Transaktionen zum Aussteller/Absender),
- Integrität (Unverändertheit) und
- Zuverlässigkeit (Nachvollziehbarkeit)

geschäftsrelevanter Aufzeichnungen und Transaktionen erreicht. Wesentlich hierfür ist einerseits die eindeutige Identifizierung der am Prozess beteiligten natürlichen wie juristischen Personen und andererseits die nicht abstreitbare Zuweisbarkeit von Transaktionen und Unterlagen zum

Aussteller/Absender. Der Nachweis wird gegenüber vertrauenswürdigen Dritten anhand der Aufzeichnungen erbracht, wozu deren Verkehrsfähigkeit, also Portabilität beziehungsweise Datenexport in interoperabler Form, erforderlich ist. Hinzu kommt die Gewährleistung der Verfügbarkeit behördlicher Unterlagen, bei Aufbewahrungsfristen zwischen 2 und 100 Jahren oder dauernd, sowie deren Interpretierbarkeit und die Erhaltung von deren Beweiswert.

Nicht vergessen werden darf der Schutz sensibler und personenbezogener Daten durch Wahrung der Vertraulichkeit, auch zur Erfüllung bestehender Datenschutzvorgaben. Organisatorisch wird dies unter anderem durch klare Verant-

wortlichkeiten, Richtlinien und Prozesse, technisch durch die nachweisbare Umsetzung des Stands der Technik, also anerkannte Standards und Normen etablierter Standardisierungsgremien zum Beispiel DIN, ISO, ETSI, BSI etc., erreicht.

Eine Vertrauenswürdigkeit eines Systems oder einer Community besteht nicht per definitionem. Es muss stets der Nachweis gegenüber vertrauenswürdigen Dritten erbracht werden [He18], [KoScKu18]. Abbildung 1 zeigt diese faktischen Vertrauensketten am Beispiel der eIDAS-Verordnung. DLT/Blockchain erfüllt diese Anforderungen derzeit nur bedingt, wie Tabelle 1 zeigt [DIN TS 31648]:

KERNANFORDERUNG	ERFÜLLUNG	BEGRÜNDUNG
Integrität	Bedingt	Unveränderlichkeit wird durch die kryptografische Sicherung der Blöcke (Blockchain) respektive der Transaktionen (DLT) erreicht. Keine Langzeitstabilität aufgrund von fehlendem Rehashing und Proof of Existence
Authentizität	Nein	Keine standardisierten Werkzeuge zur eindeutigen Zuweisbarkeit von Transaktionen und Daten; zum Ergänzen bedarf es eindeutiger Identifizierung der Aussteller/Absender; ist nur in Permissioned DLT/Blockchain möglich.
Vertraulichkeit	Bedingt	Nur in Private Permissioned DLT/Blockchain möglich Erfüllung der Rechte des Betroffenen (Löschung, Datenübermittlung, Berichtigung etc.) nur bei Off-Chain-Speicherung der Inhaltsdaten möglich Nachweisführung (Informationspflicht, Einwilligung) bedarf zusätzlicher Maßnahmen
Verfügbarkeit	Bedingt	Effektive Skalierbarkeit nur bei Off-Chain-Speicherung der Inhaltsdaten möglich Zugriff nur in DLT/Blockchain Keine standardisierten Mechanismen zum Langzeiterhalt der in DLT/Blockchain abgelegten Daten
Zuverlässigkeit	Bedingt	Nur in Private Permissioned DLT/Blockchain; vollständige Dokumentation bedarf zusätzlicher Maßnahmen durch Metadaten, Protokollinformationen etc., die in DLT/Blockchain nicht vorhanden sind.
Verkehrsfähigkeit	Nein	Keine standardisierten Werkzeuge zum Datenexport aus DLT/Blockchain vorhanden

Tabelle 1: Anforderungen an DLT/Blockchain und deren Erfüllung

Im Ergebnis lässt sich feststellen, dass DLT/Blockchain für nachweispflichtige Prozesse, wie sie in der öffentlichen Verwaltung üblich sind, derzeit nur als Private Permissioned, also private genehmigungspflichtige DLT/Blockchain, die beispielsweise von einem behördlichen Konsortium betrieben wird, mit einer Off-Chain-Speicherung der geschäftsrelevanten Aufzeichnungen empfehlenswert ist. Die eigentlichen Nutzdaten werden dabei wie bislang in der vorhandenen Geschäftsanwendung abgelegt und im DLT-Netzwerk nur deren Hashwerte [BSI19], [Ko18], [Lem16]. Dies ist für die breite Anwendung der DLT/Blockchain nicht hinderlich, sondern verbessert zum einen deren Performance und Skalierbarkeit und erweitert zum anderen den Blick für die eigentlichen Vorteile der Technologie – so zum einen für die Abbildung eines verteilten Netzwerks zur erleichterten wie dokumentierten Umsetzung behörden- und unternehmensübergreifender Transaktionen für beliebig viele Beteiligte. Zum anderen lässt sich DLT/Blockchain um fehlende Punkte, wie eine eindeutige Identifizierung und Zuweisbarkeit von Transaktionen oder der Vertraulichkeit einfach ergänzen, indem bekannte Lösungen integriert werden.

Dass das Rad nicht immer neu erfunden werden muss, spiegelt sich auch in der aktuellen Standardisierung wider [SSI], [DINSPEC 3104], [DINSPEC 4997]. Mithilfe sogenannter Selbst-Souveräner-Identitäten (SSI) liefert DLT/Blockchain dabei einen signifikanten Mehrwert gegenüber bestehenden Technologien für die Verbreitung digitaler Verwaltungsleistungen durch Schaffung der Datensouveränität von Bürgern und Unternehmen über ihre sicheren digitalen Identitäten.

Vergleichbare Effekte lassen sich mit (qualifizierten) Signaturen und Siegeln gemäß eIDAS erzeugen. Diese Nutzung

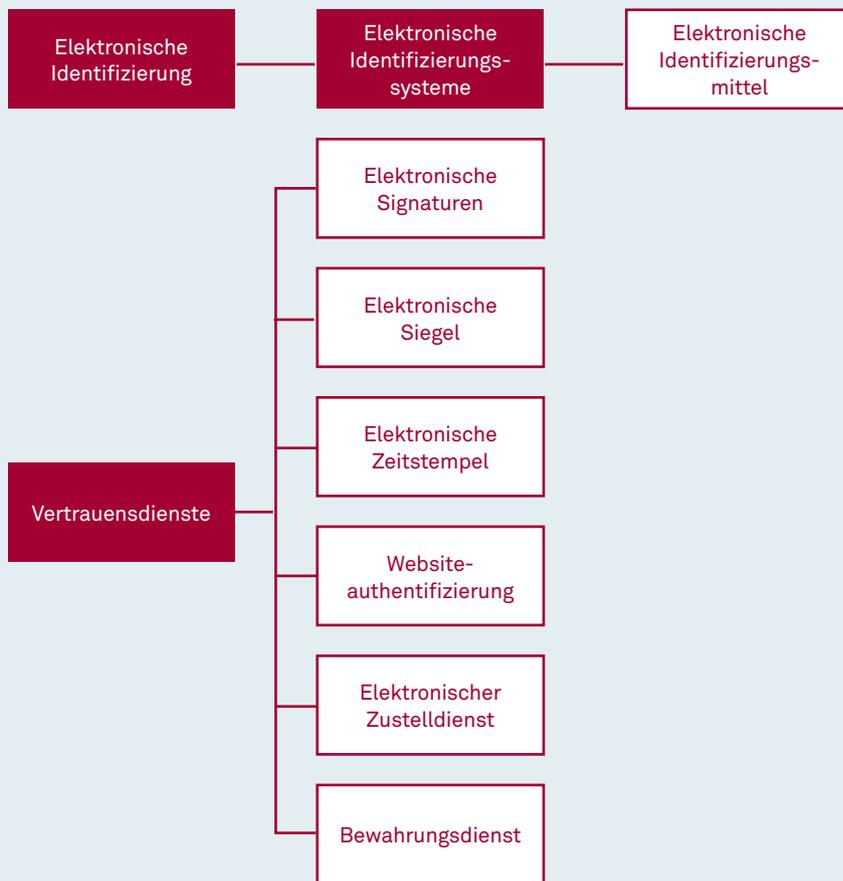


Abbildung 2: Kernbestandteile der eIDAS-Verordnung

von Synergien zwischen vorhandener Technologie und DLT/Blockchain unterstützt die Absicht der Bundesregierung, konkrete, weil praktisch nutzbare Innovationen zu fördern und nachhaltige Investitionen vorzunehmen. Unter anderem wird dies in Kapitel 4 der Blockchainstrategie hinsichtlich sicherer digitaler Identitäten aufgegriffen. Auch das BSI weist in seinen Empfehlungen zur Informationssicherheit in DLT/Blockchain zu Recht auf diesen wirtschaftlich wie technisch wesentlichen Aspekt hin [BSI19].

Die Anpassung oder besser Ergänzung von DLT/Blockchain sollte sich angesichts umfassender wie langfristiger Dokumentations- und Nachweispflichten, eines hohen Zeitdrucks aufgrund klarer wie zeitlich verbindlicher Umsetzungsvorgaben so-

wie umfangreicher Anforderungen an den Schutz personenbezogener wie anderer behördlicher Daten, wie sie für Bund, Länder und Kommunen typisch sind, auf folgende elementare Punkte konzentrieren:

- Digitale Identitäten und Vertrauensdienste (Nachweisfähigkeit)
- Datenschutz
- Informationssicherheit und Langzeitstabilität

Diese Aspekte werden weitaus umfassender durch die aktuelle Standardisierung, unter anderem DIN [DINSPEC 31648] und ISO [ISO TR 24332], aufgegriffen, in denen aktuell dezidierte, prüfbare Standards zur Nutzung von DLT/Blockchain wie vertrauenswürdige digitale Transaktionen geschaffen werden.

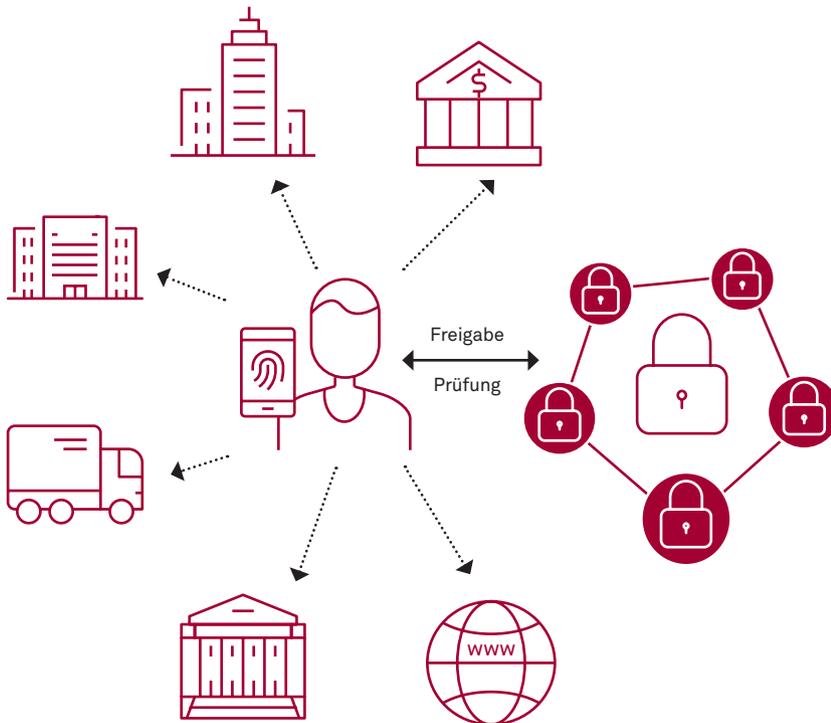


Abbildung 3: Effizienter Umgang mit sicheren digitalen Identitäten durch Self-Sovereign-Identity

DIGITALE IDENTITÄTEN UND NACHWEISFÄHIGKEIT

Die seit 2016 vollständig anwendbare eIDAS-Verordnung schafft für den gesamten europäischen Wirtschaftsraum verbindliche Grundlagen für die vertrauenswürdige elektronische Interaktion zwischen Bürgern, Unternehmen und öffentlichen Verwaltungen durch einheitliche Vorgaben für elektronische Identitäten sowie Vertrauensdienste. Die eIDAS ist technologieoffen und kann damit auch für DLT/Blockchain leicht angewendet werden.

Die zur Nachweisführung wichtige Identifizierung natürlicher oder juristischer Personen muss dabei auf einem sicheren und zugelassenen Weg unter Verwendung eines anerkannten Identifizierungssystems, wie dem elektronischen Personalausweis oder einer anderen europäischen eID, erfolgen sowie ein an-

gemessenes Vertrauensniveau (in der Regel substanziiell oder hoch) nach eIDAS umfassen. Damit wird ein hinreichendes Maß an Sicherheit für digitale Identitäten zum Schutz aller Beteiligten erreicht. Darüber hinaus ist zu beachten, dass alle notifizierten eID durch alle öffentlichen Stellen im EWR anzuerkennen sind [KokuSt18], [BSI19].

Die Integration sicherer digitaler Identitäten erfolgt in DLT/Blockchain typischerweise als sogenannte Self-Sovereign-Identity, kurz SSI. Hierbei werden sichere digitale Identitäten der DLT/Blockchain mithilfe der W3C-DID-Spezifikation vergleichsweise einfach hinzugefügt. Aus Datenschutzgründen werden auf der DLT/Blockchain nur anonymisierte/pseudonymisierte Informationen abgelegt. Die eigentlichen Identitätsdaten befinden sich sicher gespeichert bei der verantwortlichen Institution. Der Nutzer kann zum Beispiel

über Token der DLT/Blockchain seine Identitätsdaten unterschiedlichen Diensten zeitlich begrenzt oder unlimitiert freigeben. Der Ablauf der Berechtigung wird durch die DLT/Blockchain ebenso überwacht und dokumentiert wie jeder Zugriff selbst. Die Bestätigung, dass anonymisierte Informationen und Identität zusammengehören, erfolgt automatisiert. Im Ergebnis gewinnen Bürger und Unternehmen die Souveränität über ihre Identitätsdaten und können diese sogenannte Selbst-Souveränen-Identitäten für verschiedene behördliche Dienste auf allen Verwaltungsebenen sowie für private Services einsetzen: eine Lösung für das bekannte Henne-Ei-Problem bei der Umsetzung des Onlinezugangsgesetzes.

So bleiben Datensouveränität und Smart City keine Schlagwort mehr. Zudem wird damit die aufwendige wie nutzerunfreundliche permanente Re-Identifizierung an Onlinediensten vermieden. Es wird jeweils auf die konkreten Identitätsdaten eines Bürgers oder Unternehmens, per vorheriger Freigabe durch den Bürger/das Unternehmen, dokumentiert zugegriffen. Einzige Bedingung: Die SSI muss auf einem anerkannten Identifizierungsmittel mit notwendigem Vertrauensniveau gemäß eIDAS beruhen. Angesichts dessen, dass die Umsetzung des OZG unmittelbar auf die Nutzung des notifizierten elektronischen Personalausweises respektive dessen europäischer Pendanten setzt, ist die Nutzung der Synergie für DLT/Blockchain offensichtlich. Abbildung 3 zeigt das Prinzip.

Dieses Konzept wird auf europäischer Ebene in den Initiativen ESSIF und EBSI derzeit aufgegriffen, erste Anwendungsfälle werden erprobt.

Das Erzeugen und die Validierung (qualifizierter) elektronischer Signaturen und Siegel ermöglichen den einfachen wie verkehrsfähigen Nachweis der Authen-

tizität und Integrität an den geschäftsrelevanten Aufzeichnungen selbst. Qualifizierte elektronische Zeitstempel unterstützen dies und gewährleisten zudem den Nachweis des Zeitpunkts einer Transaktion. Mit den (qualifizierten) Vertrauensdiensten schuf die eIDAS-Verordnung auch hierfür in der EU und EFTA einheitliche wie verbindliche regulatorische und technische Vorgaben. So sind alle mindestens fortgeschrittenen elektronischen Signaturen, Siegel und Zeitstempel durch jede Behörde anzuerkennen. Gemäß „E-Government-Gesetz des Bundes“ ist zudem ohnehin ein Zugang für qualifizierte elektronische Signaturen durch alle Behörden einzurichten [KSDV15], [Ko18].

Dank mobiler Signaturen und Siegel, die von jedem (qualifizierten) Anbieter verwendet werden können, ist die Anwendung jedoch denkbar einfach geworden, wie die Verbreitung in der Privatwirtschaft und dem europäischen Ausland zeigt [FOKUS]. Wesentlich ist, dass das Erzeugen und, soweit notwendig, die Validierung, egal in welchem Verfahren, also auch bei DLT/Blockchain, durch einen (qualifizierten) Vertrauensdienst gemäß eIDAS erfolgt. Entscheidender Vorteil, neben technischer Interoperabilität und Sicherheit, ist die Klarheit der Verantwortung im Fehlerfall. Hier liegt die Nachweispflicht beim Anbieter und nicht bei der Behörde [KSDV15].

(Qualifizierte) elektronische Signaturen, Siegel, Zeitstempel gemäß eIDAS lassen sich auf ebenso einfache wie effiziente Weise in DLT/Blockchain integrieren. Dies kann sowohl auf Basis bekannter Technologie als auch durch native DLT/Blockchain-Technologie erfolgen – beide Varianten sind bereits europaweit im praktischen Einsatz. Entsprechende Onlinedienste, die quasi als eine Art „Gatekeeper“ fungieren und sowohl Identifizierungsdienste als auch Vertrauensdienst integrieren oder diese selbst anbieten, können so eine staatliche oder private DLT/Blockchaininfrastruktur oder ganze digitale Ökosysteme effizient für vertrauenswürdige digitale Transaktionen ermöglichen.

Das Rad hier in DLT/Blockchain neu zu erfinden, birgt nur hohe Kosten ohne praktischen Mehrwert, denn vertrauenswürdige Lösungen sind im eIDAS-Vertrauensraum vorhanden. Auch die aktuelle Evaluation der eIDAS-Verordnung weist auf eine Integration von DLT/Blockchain in die bestehenden Vertrauensdienste sowie sicheren digitalen Identitäten hin (siehe zum Beispiel Initiativen wie ESSIF, EBSI etc.), nicht auf die Schaffung einer Parallelwelt.

Die Blockchainstrategie der Bundesregierung greift diesen Umstand in Kapitel 4 richtigerweise auf und fokussiert konsequent auf die Umsetzung der Maßgaben

in DLT/Blockchain. Nur so kann auch die angestrebte Stärkung des (europäischen) Binnenmarkts erreicht werden.

DATENSCHUTZ

In behördlichen Prozessen werden umfassend personenbezogene Daten verarbeitet. Der Datenschutz und hier insbesondere die Rechte des Betroffenen, wie zum Beispiel das Recht auf Berichtigung (Art 16), das Recht auf Datenübertragbarkeit in einem strukturierten, gängigen, maschinenlesbaren Format (Art. 20) und das Recht auf Löschung beziehungsweise das Recht auf „Vergessen werden“ (Art. 17), sind für den Einsatz von DLT/Blockchain aufgrund mangelnder Funktionen zur Veränderung und Löschung von Daten kritisch zu bewerten. Derzeit bestehen keine standardisierten Wege, um innerhalb einer DLT/Blockchain gespeicherte Daten zu berichtigen, zu löschen oder in maschinenlesbarer Form zu exportieren, weshalb personenbezogene Daten grundsätzlich „off chain“, also in einer parallelen Geschäftsanwendung, geführt werden müssen. Diese zusätzliche Komplexität bei der Nutzung von DLT/Blockchain betrachtet auch die Blockchainstrategie der Bundesregierung zu Recht als kritischen Erfolgsfaktor. Der geplante Roundtable ist hier sicher ein erster Schritt. Weitaus dringender sind jedoch konkrete technische Standards, um DLT/Blockchain datenschutzgerecht effizienter einsetzen und gegebenenfalls auf parallele Geschäftsanwendung verzichten zu können. Die [DINSPEC 4997] sowie [ISOTR23244] sind erste konkrete Schritte, auf die aufgebaut werden sollte.

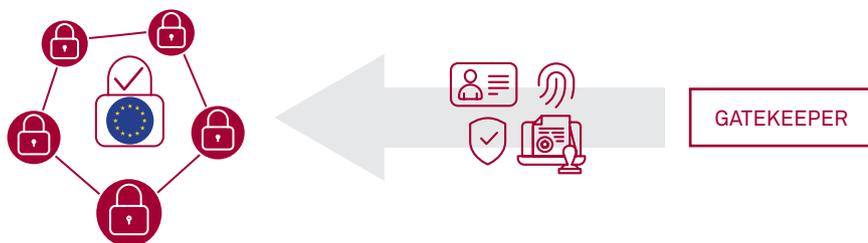


Abbildung 4: Befähigung der DLT/Blockchain für vertrauenswürdige Transaktionen durch eIDAS

INFORMATIONSSICHERHEIT UND LANGZEITSTABILITÄT

Wie das BSI in seiner Veröffentlichung „Blockchain sicher gestalten“ [BSI19] feststellt, bestehen für DLT/Blockchain

bereits verschiedene nicht unkritische Angriffsszenarien. Zur Gewährleistung der Informationssicherheit muss, wie für jede IT, die in Behörden verwendet wird, ein verfahrensbezogenes Sicherheitskonzept erstellt werden. Neben klaren Richtlinien, Rollen und Verantwortlichkeiten gilt es, anhand der Methodik des BSI-Grundschutzes konkrete Sicherheitsmaßnahmen zu definieren, wozu neben der Begegnung unmittelbarer Bedrohungen beispielsweise ein klares Berechtigungsmanagement, ein sicherer Konsensmechanismus oder kryptografische Verfahren nach dem Stand der Technik zählen. Dies erfordert im Kern eine Private Permissioned DLT/Blockchain, um auch die Verantwortlichkeit für die Datenverarbeitung eindeutig zu definieren.

Ein wesentlicher Schwachpunkt der DLT/Blockchain sind fehlende Maßnahmen zur Langzeitstabilität der eingesetzten kryptografischen Verfahren.⁴ Ohne eine periodische Erneuerung der Hashabsicherung der DLT/Blockchain sind Manipulationsmöglichkeiten absehbar. Doch auch hier lassen sich bestehende Verfahren leicht mit DLT/Blockchain kombinieren. So kann das aus der TR-ESOR des BSI bekannte Verfahren zur Beweiserhaltung auch bei DLT/Blockchain zur Erneuerung der Integritätssicherung der Kette (Chain) einschließlich des obligatorischen Archivzeitstempels verwendet werden. Erste Lösungen hierzu sind ebenso wie konkrete Standards im Aufbau.

ZUSAMMENFASSUNG UND WESENTLICHE ANWENDUNGSFÄLLE VON DLT/BLOCKCHAIN IM E-GOVERNMENT

Die wesentlichen Vorteile der DLT/Blockchain gegenüber bestehenden verteilten Systemen sind:

- Dezentralität und Verteiltheit
- Systemimmanente grundlegende Manipulationssicherheit

- Leichtere Abbildung übergreifender Transaktionen, da nur ein Knoten im Netzwerk notwendig ist statt aufwendiger gemeinsamer Verfahren, Integrationen, Schnittstellen, Datenübertragungen zwischen Verfahren
- Gemeinsame Verfahrensregeln und Abhängigkeiten, die beispielsweise über Smart Contracts automatisiert werden können
- Gewinnung der Datensouveränität für Bürger und Unternehmen durch SSI
- Vermeidung aufwendiger Re-Identifizierungen an Onlinediensten
- In Verbindung mit Beweiserhaltung gemäß eIDAS und TR-ESOR effiziente Integritätssicherung, -verifikation und Nachweis
- Hohe Performance, vor allem bei Off-Chain-Speicherung der Nutzdaten

Sie lassen sich vor allem bei hoher Komplexität der betroffenen Prozesse ausspielen. Je mehr beteiligte Institutionen in unterschiedlichen Verwaltungsebenen, je mehr Regeln und Abhängigkeiten und je weniger sich die eigentlichen Nutzdaten in der DLT/Blockchain befinden, desto eher unterstützt die dezentrale wie verteilte Struktur der DLT/Blockchain die konkrete Umsetzung absehbar effizienter als andere Lösungsoptionen. Besonders die bereits unter anderem seitens des Normenkontrollrats geforderte Registerautomatisierung kann hiervon profitieren. Dabei werden zum einen meist hochstandardisierte Prozesse durchlaufen, bei denen vielfach nicht Daten ausgetauscht, sondern nur Einträge in Registern geändert werden. Dies kann durch Smart Contracts wirksam unterstützt werden. Die DLT/Blockchain dient hier nur zur Prozessabwicklung/-kontrolle und Gewährung eines übergreifenden Zugriffs anhand dezidiert, zeitlich begrenzter Zugriffsrechte. Die eigentlichen Nutzdaten verbleiben im jeweiligen Register. Die für vertrauenswürdige digitale Transaktionen

fehlenden, sicheren digitalen Identitäten und Vertrauensdienste lassen sich mit den eIDAS-Werkzeugen effizient in DLT/Blockchain integrieren.

Praktisch würde dies am Beispiel des Umzugs einer Firma von Berlin nach München bedeuten, dass die DLT/Blockchain als regelbasiertes Transaktionsmanagement den Prozess steuert, abarbeitet und die notwendigen Eintragungen in den Registern vornimmt. Ein, wie bislang erforderlich, aufwendiger Datenaustausch über mehr als sechs Behörden in Bund, Land, Kommunen würde entfallen. Notwendig hierzu ist die Identifikation von Unternehmen und handelnden Mitarbeitern sowie der eindeutige Zeitpunkt des Prozessbeginns. Im Ergebnis wird der immer gleich ablaufende, in einem Smart Contract hinterlegte Prozess durch die Blockchain koordiniert, also Änderungen der Einträge im Handelsregister, Kfz-Register, Gewerberegister, Sozialversicherung etc. Für Authentisierung und Nachweis kommen die Vertrauensdienste der eIDAS-Verordnung zum Einsatz. Im Ergebnis kann ein Kostenbescheid mit einem qualifizierten elektronischen Siegel als Herkunftsnachweis der zuständigen Behörde ausgestellt und dem Unternehmen zugestellt werden. Selbst die Zahlungsfrist für die Gebühren des Verwaltungsakts kann durch die DLT/Blockchain überwacht werden. Für den langfristigen Nachweis des Prozesses werden qualifizierte Bewahrungsdienste auf Basis der Produkte zur Beweiserhaltung gemäß BSI TR-ESOR verwendet. Durch die Kombination von DLT/Blockchain sowie den Werkzeugen der eIDAS-Verordnung kann so eine ebenso vertrauenswürdige wie voll-digitale Registerautomatisierung effizient realisiert werden [Ko19]. Selbstsouveräne Identitäten auf Basis von eIDAS und DLT/Blockchain erleichtern die OZG-Umsetzung bis hin zur Smart City und IoT. Sowohl eine Harmonisierung der technischen Lösun-

gen durch die nationale wie internationale Standardisierung als auch die weitere Umsetzung in konkreten behördlichen Projekten sind empfehlenswert.

Darüber hinaus kann DLT/Blockchain in Verbindung mit den eIDAS-Werkzeugen digitale Herkunftsnachweise und Datenvalidierungen, zum Beispiel Zeugnisvalidierungen, wie es in NRW bereits erprobt wird, unterstützen. In Sachen Archivierung könnte DLT/Blockchain als Integritätssicherung dienen und so die teure WORM-Technologie ablösen – in Verbindung mit der Beweiswelterhaltung nach TR-ESOR und eIDAS entstünde so eine langfristige sichere wie stabile und vor allem wirtschaftliche E-Government-Dateninfrastruktur. In anderen regulierten Industrien, wie Versicherungen und Banken, wird dies bereits technisch umgesetzt.

Wesentliche Herausforderungen bei der Nutzung von DLT/Blockchain bleiben die Themen Datenschutz, Interoperabilität und Langzeitstabilität, hier sind nationale wie internationale technische Standards dringend notwendig. Diese Themen sollten einen Schwerpunkt in der Innovationsförderung der Bundesregierung zur Blockchainstrategie bilden – stellen sie doch elementare Grundlagen einer sicheren wie langfristig vertrauenswürdigen DLT/Blockchaininfrastruktur nicht nur in Deutschland dar. Die Korrelierung mit europäischen Initiativen wie ESSIF, EBSI, ETSI, CEN etc. kann dabei nur vorteilhaft sein. ●

1 <https://www.bundesregierung.de/breg-de/themen/digital-made-in-de/blockchain-strategie-1546662> (abgerufen am 05.03.2020).
 2 Vgl. ebenda.
 3 https://www.bsi.bund.de/DE/Themen/Kryptografie_Kryptotechnologie/Kryptografie/Blockchain/blockchain_node.html.
 4 Vgl. Kapitel 3.2 der Blockchainstrategie sowie [BSI19].



[BSI19] Blockchain sicher gestalten. Bundesamt für Sicherheit in der Informationstechnik. Bonn 2019.

[BITKOM19] eIDAS und der ECM-Markt Elektronische Identifizierung und Vertrauensdienste als Chance für die Digitalisierung. BITKOM (Hrsg.), Berlin 2019.

[DINSPEC3104] DIN SPEC 3104. Blockchain-basierte Datenvalidierung.

[DIN TS 31648] DIN TS 31648. Criteria for Trusted Transactions — Records Management and Preservation of Evidence in DLT/Blockchain.

[DINSPEC4997] DIN SPEC 4997. Privacy by Blockchain Design: Ein standardisiertes Verfahren für die Verarbeitung personenbezogener Daten mittels Blockchain-Technologie.

[eIDAS] VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“ vom 23.07.2014.

[EUDSGVO] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[He18] T. Henne: Juristische Anforderungen an die Beweiserhaltung bei digitaler Archivierung. 23. Archivwissenschaftliches Kolloquium. Marburg 2018.

[ISOTR23244] ISO PRF TR 23244: Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations.

[ISOTR24332] ISO TR 24332: Information and documentation – Blockchain and DLT and records management: Issues and considerations.

[Ko18] U. Korte, C. Berghoff, T. Kusber, S. Schwalm: Langfristige Beweiserhaltung und Datenschutz in der Blockchain. DACH-Security 2018. S. 177-191 Frechen 2018.

[Ko19] U. Korte, S. Schwalm, R. Schmidt, F. Boldt: Vertrauenswürdige digitale Transaktionen – Records Management und Beweiserhaltung mit Blockchain. eIDAS-Summit 2019.

[Ko20] Criteria for trustworthy digital transactions Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation. OpenIdentitySummit 2020. Kopenhagen 2020.

[KSDV15] T. Kusber, S. Schwalm, A. Dörner, T. Vogt, Die Bedeutung der eIDAS-Verordnung für Unternehmen und Behörden. Neue Chancen und Herausforderungen für vertrauenswürdige elektronische Geschäftsprozesse in Europa, Berlin, 2015.

[KoScKu18] U. Korte, S. Schwalm, T. Kusber: Vertrauenswürdige E-Government – Anforderungen und Lösungen zur beweiserhaltenden Langzeitspeicherung. 23. Archivwissenschaftliches Kolloquium. Marburg 2018.

[Lem16] V. L. Lemieux: „Trusting Records: Is Blockchain Technology the Answer?“, Records Management Journal 26.2.2016.

[Sc19] S. Schwalm Neue Besen im Spannungsfeld eIDAS und DSGVO-Blockchain für (dauerhafte) Verzeichnisdienste?. CAST Workshop „PKI – Elektronische Vertrauensdienste“. Darmstadt 2019.

[TR03125] BSI: Beweiserhaltung kryptographisch signierter Dokumente (TR-ESOR), TR 03125, V1.2.2, 2019.

[VDG] Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist.

[W3CDID] W3C. Decentralized Identifiers (DIDs) v1.0.

[We18] M. Weber, T. Vogt, W. Krogel, S. Schwalm: Records Management nach ISO 15489. Einführung und Anleitung. Berlin 2018.

