NExT BiVD

Blockchain in der Verwaltung

Anwendungsbereiche und Herausforderungen

August 2019

BUNDESNOTARKAMMER
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

BLOCKCHAIN BUNDESVERBAND

Bundesamt für Migration und Flüchtlinge

regio IT

Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

Fraunhofer FIT
Projektgruppe Wirtschaftsinformatik

VITAKO

LEGAL TECH CENTER

Grußwort

Die Initiative "Blockchain in der Verwaltung Deutschland" (BiVD) und die "Community-of-Practice Blockchain" des NExT-Expertennetzwerkes haben Anfang des Jahres 2019 ein Whitepaper angekündigt, um die wichtigsten organisatorischen, technischen und juristischen Herausforderungen aufzuzeigen, die zur Entwicklung künftiger Blockchain-Lösungen für die öffentliche Verwaltung adressiert werden müssen. Das vorliegende Dokument soll als erstes in der Serie "Blockchain in der Verwaltung" mögliche Anwendungsbereiche der Blockchain-Technologie aufzeigen sowie die relevanten organisatorischen und technischen Fragestellungen darstellen und mögliche Lösungsrichtungen bewerten. Spätere Papiere sollen die hier ausgeführten Überlegungen erweitern und insbesondere aus dem juristischen Blickwinkel vertiefen sowie Erkenntnisse aus zukünftigen Projekten zur Erprobung und Validierung konkreter Lösungsansätze dokumentieren.

Wir wünschen Ihnen viel Vergnügen und eine aufschlussreiche Lektüre.

Dr. Hans-Günter Gaul

IT-Direktor der Bundesnotarkammer, Vorstand NExT e.V. und Werkstattleiter Neue Technologien des NExT-Expertennetzwerkes

Helmut Nehrenheim

Referent im Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie NRW, Gründer der Initiative Blockchain in der Verwaltung Deutschland (BiVD), Federführer des Koordinierungsprojekts Blockchain des IT-Planungsrates

Inhaltsverzeichnis

1. Werte- und Prinzipien-Rahmen

Die Sicherheit, Integrität und Authentizität von Daten bilden den Grundstein einer gelingenden digitalen Transformation in Deutschland und Europa. Gleichfalls zeigen uns die Lehren aus den bisherigen Bemühungen zur Digitalisierung, dass stets auch die Frage, wie IT-Infrastrukturen aufgebaut und betrieben werden, entscheidend ist. Das Werte- und Prinzipiengerüst, welches uns das Grundgesetz und gemeinsame europäische Verordnungen vorgeben, muss sich auch auf der technischen Ebene wiederfinden.

Deutschland ist geprägt von einer föderal betriebenen IT-Infrastruktur mit einer Vielzahl an klassischen Koordinierungs-herausforderungen. Gemeinsame Schnittstellen und behördenübergreifende Prozesskoordination sind schwer zu erreichen. Derzeit bedingen viele behördenübergreifend genutzte IT-Systeme einen Trend hin zur Zentralisierung geographisch fragmentierter Datenbanken. Dies birgt jedoch das Risiko einer großen Angriffsfläche gegenüber Hackern und eines zunehmenden Aufweichens des in der Verfassung verankerten Föderalismus. Die Blockchain-Technologie bricht mit diesem Muster. Sie ermöglicht den Aufbau und Betrieb einer dezentralen, föderal geprägten IT-Infrastruktur, in der Daten unter der Kontrolle der Bürgerinnen und Bürger bleiben und Behörden dennoch prozessübergreifend miteinander kooperieren können.

Wird das Once-Only-Prinzip mittels der Blockchain-Technologie korrekt umgesetzt, können bestimmte Stammdaten von Bürgern und Unternehmen behördenübergreifend nur einmal erhoben werden und verfügbar bleiben. Hierfür sind insbesondere selbstsouveräne Identitäten geeignet, welche dem jeweiligen Identitätsinhaber jederzeit die Ausübung vollständiger Kontrolle über seine personenbezogenen Daten ermöglichen, insbesondere Transparenz darüber, welche Daten an die Diensteanbieter digitaler Services übermittelt werden [16]. Darüber hinaus kann der Schutz personenbezogener Daten durch den Ansatz der Daten-minimierung gefördert werden, um jederzeit nur die absolut notwendige Menge an Daten, die für die Nutzung des jeweiligen Services erforderlich sind, preisgeben zu müssen.

2. Eigenschaften und Mehrwerte der Blockchain-Technologie

Blockchain-Lösungen können Vertrauen zwischen unterschiedlichen Akteuren, wie z.B. Behörden, Unternehmen und Bürgern, stärken. Sie ermöglichen ihren Nutzern eine einheitliche Sicht auf einen gemeinsamen Datenbestand zu erhalten, die weder von einzelnen Nutzern noch von Dritten nach eigenen Interessen manipuliert oder nachträglich geändert werden kann.

Den Kern einer jeden Blockchain-Anwendung stellt der sogenannte Konsens-Algorithmus dar. Dieser Algorithmus implementiert einen transparenten und verlässlichen Mechanismus für die Einigung der Nutzer über die Validität und Reihenfolge der auf der Blockchain durchzuführenden Transaktionen. Dies ermöglicht eine dezentrale Speicherung eines jederzeit identischen Informationsstandes auf den Systemen der jeweiligen Nutzer und bietet ihnen eine sichere Grundlage für die Überprüfung der Quelle und Unversehrtheit (d.h. Authentizität und Integrität) der abgelegten Informationen.

Die dezentrale Speicherung ermöglicht den Akteuren zudem die vollständige Kontrolle über die eigenen personenbezogenen Daten im Sinne selbstsouveräner Identitäten und lässt damit die durch die DSGVO definierten Ziele in den digitalen Prozessen der Zukunft leichter und besser realisieren. Dabei ist zu beachten, dass personenbezogene Daten (wie z.B. Registerdaten) gerade nicht auf der Blockchain gespeichert werden sollen, sondern lediglich deren pseudonymisierte Entsprechungen, wie z.B. Hashwerte.

Moderne Blockchain-Technologien können zudem Prozesslogiken in sogenannten Smart Contracts hinterlegen. Diese vordefinierten und für jeden einsehbaren Programmcode-Abschnitte werden bei Eintritt bestimmter Bedingungen automatisch ausgeführt und können dadurch die Effizienz, Transparenz und Manipulationsresistenz insbesondere organisationsübergreifender Prozesse steigern.

3. Anwendungsbereiche in der öffentlichen Verwaltung

3.1. Blockchain-basierte Identitätslösungen

Blockchain-basierte Identitätslösungen stärken die Kontrolle der Bürgerinnen und Bürger über ihre digitalen Identitäten und ermöglichen es, Identitätsnachweise ohne die Preisgabe identitätsbezogener Daten zu gestalten. Kernelement dieser Lösungen sind sog. selbstsouveräne Identitäten (engl. Self-Sovereign Identities oder kurz SSI). Diese unterscheiden sich wesentlich von herkömmlichen digitalen Identitäten, welche die Identität der Bürgerinnen und Bürger durch Profile auf Seiten eines Dienstes darstellen. So sammeln sich für jeden Dienst immer neue Profile an, die oftmals redundante personenbezogene Informationen enthalten und alle individuell durch Nutzernamen und Passwörter gesichert werden müssen. Bei selbstsouveränen Ansätzen pflegen die Bürgerinnen und Bürger ihr Profil dezentral in einem so genannten Identity Wallet. Informationen wie Name, Adresse, Steuernummer oder Führerschein liegen darin als bestätigte Kopie vor. In der Interaktion mit einem Dienst können die Bürger dann entscheiden, welche Informationen sie aus dem Profil teilen möchten, um sich zu authentifizieren und den Dienst in Anspruch zu nehmen. Die redundante Speicherung und Pflege von diensteabhängigen Identitäten entfällt. Besonders interessant an dieser Form der digitalen Identität ist, dass sie anbieterunabhängig auf Basis offener Standards und interoperabler Protokolle funktioniert und so keine Abhängigkeit von Identity Providern erzeugt [16].

Um die Vertrauenswürdigkeit selbstsouveräner Identitäten zu stärken, können sie durch eine vertrauenswürdige Instanz, wie z.B. Kommunen oder geeignete Zertifizierungsdiensteanbieter (ZDA), verifiziert bzw. bestätigt werden. Das Einsatzspektrum verifizierter selbstsouveräner Identitäten reicht dabei von der Anmeldung in Bürgerportalen bis hin zur digitalen Signatur. Über sie können Basisdaten im Bedarfsfall registerübergreifend zugeordnet und für die automatisierte Vorbefüllung von Antragsformularen abgefragt werden. Eine Blockchain-Identität kann entsprechend als gezielte Ergänzung zum elektronischen Personalausweis, zur elektronischen Gesundheitskarte und zur Steueridentifikationsnummer eingesetzt werden. Darüber hinaus kann eine Blockchain-Identität Bürgern Mitbestimmungsrechte bei der Weitergabe identitätsbezogener Informationen ermöglichen. So kann beispielsweise vor jeder Weitergabe von Daten, für die keine explizite rechtliche Grundlage besteht, die Erlaubnis des Bürgers abgefragt werden ("opt-in"). Diese Freigabe sowie eine Beschreibung der weitergegebenen Daten kann bei Bedarf zudem nachvollziehbar auf der Blockchain festgehalten werden.

Blockchain-basierte digitale Identitätslösungen können entsprechend deutliche Mehrwerte für den Aufbau funktionierender föderaler e-Government Dienste bieten. Sie eignen sich aber auch für viele weitere Identifizierungsvorgänge, wie z.B. den Online-Abschluss von Versicherungen.

3.2. Koordination behördenübergreifender Verwaltungsvorgänge

Blockchain-basierte Lösungen können einen wichtigen Beitrag zur Koordination behördenübergreifender Verwaltungsvorgänge leisten. Aktuell sind die Kommunikationswege zwischen Behörden oftmals aufwendig, mit Medienbrüchen verbunden und führen insgesamt zu Verzögerungen. Zudem erschweren abweichende Vorgangsvarianten auf Länder- und kommunaler Ebene die Zusammenarbeit. Blockchain-basierte Lösungen können an dieser Stelle helfen, den Informationsaustausch zu verbessern, sowie Gesamtprozesse effizienter und sicherer zu gestalten. Konkret ermöglichen Blockchain-Lösungen eine gesicherte und zeitnahe Verteilung neuer Vorgangsinformationen an alle Teilnehmer des Netzwerks. Einerseits können hierdurch Übertragungsfehler minimiert werden, anderseits lässt sich so sicherstellen, dass alle beteiligten Behörden den gleichen Informationsstand besitzen. Zudem können einmal auf die Blockchain geschriebene Sachstände als Auslöser für den Beginn von Folgeprozessen bei anderen Behörden genutzt werden. Hierdurch können Prozessdurchlaufzeiten und insbesondere Prozesszwischenzeiten reduziert werden. Durch den zielgerichteten Einsatz von Smart Contracts kann zudem eine automatisierte Prozesskontrolle und perspektivisch auch eine (Teil-) Automatisierung ausgewählter Prozessschritte erfolgen. Somit werden im Sinne der Integrität Prozessabweichungen vermieden bzw. vollständig dokumentiert und die Prozessqualität verbessert. Werden in der Blockchain zudem präzise Datenbankverweise gespeichert, können weiterführende Informationen bei Bedarf zielgerichtet angefragt werden. Gleichzeitig können sensible und personenbezogene Daten in den jeweiligen Bestandssystemen verbleiben. Eine Blockchain-Lösung kann somit die Informationsverfügbarkeit bei gleichzeitiger Wahrung der Datensouveränität, des Once-Only-Prinzips und des Datenschutzes stärken sowie einen unmittelbaren, medienbruchfreien Informationsaustausch ermöglichen. All diese Möglichkeiten macht sich beispielsweise aktuell das Bundesamt für Migration und Flüchtlinge (BAMF) im Rahmen eines Blockchain Pilotprojektes im Asylbereich zunutze. Die zentralen Herausforderungen hierbei liegen v.a. in der Umsetzung datenschutzrechtlicher Details unter Wahrung der geltenden Rechtslage.

3.3. Digitale Verwaltung von Dokumenten

Die Blockchain-Technologie ermöglicht eine digitale Verwaltung von Dokumenten. Sie macht es möglich, den Aussteller eines elektronischen Dokuments eindeutig zu identifizieren und die Integrität des Dokuments zu verifizieren. Gleichzeitig lässt sich über die Blockchain die Gültigkeit der Beweisfunktion des Dokuments überprüfen, indem auch eine etwaige Unwirksamkeit zu einem späteren Zeitpunkt auf der Blockchain vermerkt werden kann. Konkret können mit einer Blockchain-Lösung beispielsweise Zeugnisse oder Führerscheine digital nachgehalten werden.

Noch weitergehende Überlegungen gehen dahin, für jeden Bürger eine Art "zentrales" Postfach (mit dezentraler Datenhaltung) zu eröffnen. Darin könnten Behörden, Unternehmen oder auch der Bürger selbst verschiedene Dokumente hinterlegen und gleichzeitig anderen Stellen den selektiven Zugriff darauf ermöglichen. Derartige Projekte existieren derzeit schon, allerdings ohne Rückgriff auf die Blockchain-Technologie (vgl. etwa die BayernID bzw. das BayernPortal). Im Wettstreit mit herkömmlichen Technologien wird es daher entscheidend darauf ankommen, einen etwaigen Mehrwert einer Blockchain-Lösung herauszuarbeiten.

Insgesamt ist das Thema der digitalen Verwaltung von Dokumenten einerseits eng verknüpft mit der Koordination behördenübergreifender Vorgänge. Andererseits weist es enge Bezüge zur Registerlandschaft auf, da sich viele Dokumente letztlich als Auszug aus einem (weit verstandenen) Register begreifen lassen. So ist zum Beispiel das analoge Dokument Führerschein bei Lichte besehen ein Auszug aus dem digitalen Zentralen Fahrerlaubnisregister.

Die digitale Verwaltung von Dokumenten ist damit eines der Schlüsselthemen für den Einsatz der Blockchain in der Verwaltung.

3.4. Modernisierung der Registerlandschaft

Auch zur Modernisierung der Registerlandschaft kann die Blockchain-Technologie einen Beitrag leisten. Eine Erhebung des Statistischen Bundesamtes sowie ein darauf aufbauendes Register-Gutachten des Normenkontrollrats aus dem Jahr 2017 zählen deutschlandweit 214 Register und registerähnliche Strukturen. Gleichzeitig entstehen laufend neue Register. Beispielsweise sieht ein Gesetzesentwurf ein Implantateregister vor, ferner soll ein Transplantationsregister den Betrieb aufnehmen. Die Zahl von Registern und damit die Menge der dort gespeicherten Informationen wird also weiter zunehmen.

Aus der Vielzahl an Registern sind für einen Blockchain-Einsatz vor allem zwei Registertypen prädestiniert: zum einen gänzlich neue, also bisher noch nicht existente Register und zum anderen bereits bestehende, aber noch nicht elektronisch geführte Register. Denn ein neues bzw. bislang noch analog geführtes Register ist technologieoffen, d.h. zu seiner digitalen Umsetzung kommen grundsätzlich verschiedene Technologien in Frage. Dabei ist es denkbar, dass für verteilte Datenbanken neben klassischen Client-Server-Architekturen künftig auch blockchain-basierte Alternativen ins Auge gefasst werden. Besonders vielversprechend erscheint ein Blockchain-Einsatz, wenn andernfalls eine unabhängige Vertrauensstelle allein zum Zweck der Pseudonymisierung von Daten geschaffen werden müsste. Für das Implantateregister richtet etwa das Robert-Koch-Institut eine solche Vertrauensstelle ein. Auch für das Transplantationsregister existiert eine entsprechende Vertrauensstelle, die von einer Aktiengesellschaft mit Gewinnerzielungsabsicht betrieben wird. Vor diesem Hintergrund kann eine Blockchain-Lösung in bestimmten Bereichen eine sinnvolle Alternative sein, soweit das im konkreten Fall erforderliche Vertrauen vollständig durch Technik abgesichert werden kann. Dies wird zwar nicht bei jedem Register der Fall sein, doch sind z.B. mit dem Implantate- und dem Transplantationsregister erste Anwendungsfälle denkbar.

Ebenso zentral wie die Auswahl Blockchain-geeigneter Register wird in einem nächsten Schritt die konkrete Ausgestaltung der jeweiligen Blockchain sein. Besonderes Augenmerk verdienen dabei drei Aspekte: Wer darf Informationen zum Register einreichen? Wer kann die eingereichte Information sodann in den Datenbestand des Registers eintragen? Und wer kann schließlich Einsicht in das Register nehmen? Für einen konkreten Use Case wird daher eine wesentliche Aufgabe darin bestehen, die gesetzlichen Vorgaben zu diesen drei Fragen technisch umzusetzen und registerabhängige Weichenstellungen zwischen "private" und "public" Blockchains sowie "permissioned" und "permissionless" Blockchains vorzunehmen (näher hierzu unter Technische Herausforderungen – Netzwerktopologien).

Gleichzeitig müssen die rechtsstaatlichen Garantien gewahrt werden, wenn durch Registereintragungen in Rechte des Bürgers eingegriffen wird. Zur Veranschaulichung denke man etwa an eine Eintragung eines Fußballfans in eine Gewalttäterdatei des BKA

oder umgekehrt an die Versagung der Eintragung eines Handwerkers in die Handwerksrolle. Den Bürger belastende Entscheidungen müssen nachvollziehbar sein und individuell begründet werden. Gleichzeitig muss für den Bürger ersichtlich sein, wer für einen etwaigen Fehler verantwortlich ist, sodass er sich mit Rechtsmitteln gegen die Entscheidung zur Wehr setzen und ggf. Amtshaftungsansprüche geltend machen kann. All diese Rechte sind Ausfluss des Rechtsstaatsprinzips, des Justizgewährungsanspruchs und nicht zuletzt des Grundrechtsschutzes (in der EU-Grundrechtecharta zusammengefasst als "Recht auf eine gute Verwaltung"). Bei der technischen Ausgestaltung eines Blockchain-Registers wäre daher dafür Sorge zu tragen, dass diese verfassungsrechtlichen Garantien beachtet werden. Gleichzeitig betreffen aber nicht alle Register gleichermaßen grundrechtssensible Bereiche. Für eine Pilotierung der Blockchain-Technologie im Registerwesen bieten sich mithin vor allem verwaltungsinterne Register an, um etwa den Datenaustausch zwischen verschiedenen Behörden zu verbessern.

Für die bisher "zersplitterte" Registerlandschaft Deutschlands bietet die Blockchain damit erhebliches Verbesserungspotential.

3.5. Weitere Anwendungsmöglichkeiten

Das vielfältige Spektrum potentieller Einsatzmöglichkeiten der Blockchain-Technologie umfasst daneben eine Vielzahl weiterer Anwendungsfälle wie z.B. das (realtime) Micropayment, die Zweckbindung von Zuschüssen und den automatischen Einzug von Steuern. Daneben wird Blockchain auch immer wieder im Kontext korruptionsfreier und transparenter Wahlen sowie E-Votings (elektronische Wahlen) oder gar I-Votings (Wahlen über das Internet) diskutiert. Für den Bereich parlamentarischer Wahlen wird der Einsatz technologischer Hilfsmittel in Deutschland jedoch sehr kontrovers gesehen und ist bislang nur in Fachkreisen angekommen.

4. Herausforderungen im Bereich der Governance

In dezentralen, föderal geprägten IT-Infrastrukturen spielt das Thema Koordinierung auf vielerlei Ebenen eine wichtige Rolle. Dies beginnt bei der Definition von fachlichen Anforderungen und reicht bis zur Aufgabenverteilung im operativen Betrieb. Um die Komplexität der erforderlichen Koordinierungsprozesse zu minimieren, bedarf es entsprechender Steuerungs- und Reglungssysteme, mithin einer effektiven Governance.

Das Hauptaugenmerk der Governance-Strukturen sollte dabei insbesondere auf drei Bereichen liegen: Strategische Grundsätze und fachliche Anforderungen (organisatorische Governance), Gesetzgebung und Regulierung (juristische Governance) sowie Entwicklung und Betrieb (technische Governance). Die organisatorische Governance adressiert insbesondere Fragen der strategischen Richtlinienkompetenz und der Definition von fachlichen Anforderungen an eine Blockchain-Infrastruktur für die öffentliche Verwaltung in Deutschland. Die technische Governance wiederum adressiert Koordinierungsfragen der technischen Umsetzung und des Betriebs. Die juristische Governance beinhaltet einerseits die Einhaltung gesetzlicher Anforderungen wie des Rechtsstaatsprinzips, des Justizgewährungsanspruchs, des Rechts auf eine gute Verwaltung, des Datenschutzes, der Regeln über Identitäts- und Vertrauensdienste u.v.m. Andererseits betrifft juristische Governance die Frage, wie die Regeln und Institutionen des Rechtsstaats im Wege eines Blockchain Protokolls implementiert werden können, um rechtliche Compliance und Zugang zu staatlichen Dienstleistungen für Normadressaten zu vereinfachen.

In diesem Kapitel werden insbesondere Herausforderungen der organisatorischen und der technischen Governance diskutiert. Spezifische Herausforderungen der juristischen Governance werden in einem späteren Whitepaper mit Fokus auf den juristischen Herausforderungen beleuchtet.

4.1. Organisatorische Governance

Insbesondere im Bereich der Definition strategischer Grundsätze und fachlicher Anforderungen ist eine effektive organisatorische Governance unerlässlich. Ein wichtiger Schritt in diese Richtung ist auf gesamteuropäischer Ebene bereits mit den Organen der European Blockchain Partnership erfolgt. Diese Organe sollen gesamteuropäische Grundsätze und Leitlinien definieren sowie eine Blockchain-Infrastruktur auf europäischer Ebene aufbauen. Darunter bedarf es allerdings auch einer starken deutschen Blockchain-Infrastruktur mit einer ebenso effektiven Governance-Struktur. Diese Governance-Struktur muss zwei wesentliche Vermittlungsaufgaben erfüllen. Einerseits muss sie die gesamteuropäischen Grundsätze in passende Leitlinien und Referenz-architekturen für die deutsche Verwaltung übersetzen. Andererseits muss sie die Anforderungen des Bundes, der Länder und der Kommunen in die europäischen Gremien transportieren.

Obgleich mit dem Koordinierungsprojekt "Blockchain" des IT-Planungsrates bereits erste Ansätze einer deutschen Governance-Struktur bestehen, sind noch einige

Herausforderungen zu adressieren. So fehlt bisher noch eine nachhaltig tragfähige Verteilung strategischer Entscheidungskompetenzen. Diese Verteilung sollte sowohl zum Werte- und Prinzipienrahmen als auch zum Grad der Dezentralisierung der deutschen Blockchain-Infrastruktur passen. So widerspricht z.B. eine zu starke Bündelung von Entscheidungskompetenzen der föderalen Struktur der deutschen Verwaltung. Aber auch eine zu starke Dezentralisierung birgt Risiken, wie z.B. langsame Entscheidungsprozesse.

Neben Entscheidungsstrukturen spielen auch Kontrollmechanismen eine wichtige Rolle. Konkret müssen Kontrollstrukturen sicherstellen, dass die entwickelte Blockchain-Infrastruktur stets gemäß den gesamteuropäischen Vorgaben sowie den Anforderungen der deutschen Verwaltung weiterentwickelt wird. Entsprechend sollten frühzeitig verschiedene Kontrollansätze mit potentiellen Betreibern einer Blockchain-Infrastruktur auf Bundes-, Landes und Kommunalebene diskutiert werden. Gerade bei öffentlichen Blockchain-Infrastrukturen spielt zudem das Thema Standardisierung und die damit verbundene Koordinierung mit internationalen Standardisierungsgremien und Foren eine wichtige Rolle.

Schlussendlich gilt es, ein passendes Finanzierungs - und Bezahlmodell für die Entwicklung und Nutzung der Blockchain-Infrastruktur zu schaffen. Diese Modelle müssen sowohl die initiale Entwicklung abdecken, als auch den Betrieb, die Wartung und die Weiterentwicklung. Insbesondere das Thema Weiterentwicklungsfinanzierung spielt eine hervorgehobene Rolle. Aus Sicht der öffentlichen Verwaltung ist daher ein entsprechendes Finanzierungs- und Bezahlmodell essentiell.

4.2. Technische Governance

Neben der organisatorischen Governance spielt bei Blockchain-Infrastrukturen und Blockchain-Lösungen insbesondere die technische Governance eine wichtige Rolle. Diese muss effektive Steuerungs- und Reglungsstrukturen bieten, um sowohl eine zuverlässige (Weiter-)Entwicklung als auch einen reibungslosen Betrieb zu gewährleisten. Konkret erstrecken sich Fragen der technischen Governance sowohl auf die Blockchain-Schicht als auch die darunterliegenden Hard- und Softwareschichten, die für den Betrieb der Blockchain-Knoten benötigt werden. Grundsätzlich empfiehlt es sich, im Rahmen der technischen Governance eine bewusste Differenzierung der Blockchain-Schicht in eine Protokoll-Schicht (d.h. die eingesetzte Blockchain-Technologie) und eine DApp-Schicht (d.h. dezentrale Anwendungen inkl. Smart Contracts und weiterer Anwendungskomponenten) vorzunehmen.

Eine Blockchain-Infrastruktur für die deutsche Verwaltung muss auch in Zukunft kontinuierlich an neue Erkenntnisse und Anforderungen anpassbar sein. Dies erfordert eine aktive Weiterentwicklung durch entsprechende Entwicklergruppen bzw. Organisationen. Ohne diese Weiterentwicklungen können auch etwaige gesetzliche Neuerungen nicht umgesetzt werden. Hier gilt es, durch technische Governance-Strukturen eine nachhaltig tragfähige Verteilung von technischen Entscheidungs- und Umsetzungskompetenzen zu definieren. Je nach gewünschter Ausgestaltung der Protokoll- und DApp-Schichten (näheres hierzu im Kapitel Technische Herausforderungen), gilt es diese Verteilung in einem entsprechenden Entwicklungsmodell zu konkretisieren (z.B. durch Open-Source Communities und / oder durch eine Gruppe von Entwicklungspartnern – diese können sowohl kommunale Dienstleister, IT-Dienstleister des Bundes oder internationale IT-Dienstleister mit

einschlägiger Blockchain-Erfahrung sein). Das Entwicklungsmodell muss zwei wesentliche Aspekte gewährleisten. Einerseits muss das Blockchain-Protokoll gemäß den strategischen Vorgaben, z.B. hinsichtlich der Stabilität, weiterentwickelt und vor ungewollten Forks geschützt werden. Forks bewirken dabei eine Aufsplittung des Konsenses über den einheitlichen Systemzustand in miteinander konkurrierende Sichten. Forks stellen dadurch ein großes Problem vieler Open Source Blockchain-Projekte mit schwacher Governance bzw. uneinigen Entwickler-Communities dar und wirken der Massenadoption der Technologie, zumindest beim Einsatz von öffentlichen Ledgers, stark entgegen. Das Vorhandensein von technischen und ggf. rechtlichen "no-fork" Garantien sollte daher als wichtiges Erfolgskriterium für die Akzeptanz von breitflächigen Blockchain-Lösungen diskutiert werden. Andererseits muss neben dem Blockchain-Protokoll auch die Umsetzung, das Auditing und das Deployment etwaiger Komponenten der DApp-Schicht gewährleistet werden. Eine weiterführende Diskussion der Herausforderungen, welche sich aus der Anpassung des Programm-Codes z.B. zur Berücksichtigung einer geänderten Gesetzeslage ergeben, finden sich im Kapitel Technische Herausforderungen.

Neben der Blockchain-Schicht sollte die technische Governance auch Aspekte rund um das Entwicklungsökosystem adressieren, welches für die effiziente Bereitstellung der Blockchain-Schicht erforderlich ist. Hierzu gehört insbesondere die Bereitstellung einer Entwicklungsumgebung für Komponenten der DApp-Schicht. Diese Entwicklungs-umgebung sollte flexibel einsetzbar und mit weit verbreiteten Programmiersprachen (z.B. Java, Python, Go anstatt nur exotischer Sprachen wie Solidity) kompatibel sein. Konkret sollte sie z.B. Tools für die Erstellung, für das Testen und für das Deployment von Prozesslogiken (Smart Contracts) zur Verfügung stellen. Selbstverständlich sollte neben dem Blockchain-Protokoll und den Komponenten der DApp-Schicht auch über die Entwicklungsumgebung vollständige Transparenz durch Open Source bzw. Open Review Quellcode gewährleistet werden.

Der zweite Kernbereich der technischen Governance erstreckt sich auf die Aufrechterhaltung des Betriebs. Hierzu gehören je nach Erfordernissen des Anwendungsfalls der Betrieb der Blockchain-Schicht und ggf. eigener Knoten für das eingesetzte Blockchain-Protokoll. Erfordert ein Anwendungsfall den Betrieb einer eigenen Blockchain-Schicht, so müssen insbesondere klare Rollen und Rechte einzelner Knoten im Netzwerk (z.B. zur Validierung von neuen Transaktionen) definiert werden. Diese Rollen- und Rechtestruktur muss insbesondere an die gewünschte Ausgestaltung der Blockchain-Schicht und an das ausgewählte Blockchain-Protokoll angepasst werden. Sollen zudem dezidierte Hard- und Softwareschichten für eigene Knoten betrieben werden, so sind diese zu definieren und an das gewünschte Betriebsmodell anzupassen. So erfordert z.B. ein selbständiges Hosting einer kompletten Instanz des Blockchain Technology-Stacks eines permissioned Ledgers auf proprietären Servern andere Governance-Strukturen als die Nutzung einer mandantenfähigen Cloud-Umgebung eines Drittanbieters.

5. Technische Herausforderungen

Für den Einsatz von Blockchain-Technologien in ökonomisch oder politisch bedeutsamen Anwendungsbereichen, wie beispielsweise in der deutschen oder europäischen Verwaltung, müssen die in Frage kommenden Technologien die heute bestehenden Herausforderungen in Bezug auf Skalierbarkeit, Sicherheit und Gesetzeskonformität erfolgreich adressieren. Da die diesbezüglich festzulegenden Anforderungen oft von der Art und Topologie eines oder von mehreren miteinander verbundenen Blockchain-Netzwerken abhängig sind, möchten wir zunächst einen Überblick der verschiedenen Blockchain-Varianten hinsichtlich deren Zugänglichkeit und Offenheit geben sowie deren Eignung zu unterschiedlichen Anwendungsbereichen bewerten.

Da Blockchain zwar die meist bekannte aber nur eine mögliche Form einer Distributed Ledger Technology (kurz DLT) ist und modernere, alternative DLT vergleichsweise deutlich bessere Eigenschaften bzgl. Skalierbarkeit, Sicherheit und Gesetzeskonformität aufweisen können, wird im technischen Kapitel der Wortgebrauch zwischen Blockchain und DLT bewusst differenziert, um Blockchain- und nicht Blockchain-basierte DLT miteinander vergleichen zu können.

5.1. Netzwerktopologien

Bei der Topologie eines Ledgers wird zum einen zwischen "public" vs. "private" und zum anderen zwischen "permissioned" vs. "permissionless" unterschieden. Während ersteres die öffentliche Zugänglichkeit und den uneingeschränkten Nutzerkreis des Systems zulässt (public) oder eben untersagt (private), regelt der zweite Aspekt die Möglichkeit zur freien Teilnahme am Netzwerk durch den Betrieb von eigenen Knoten sowie ggf. durch die Teilhabe in der damit verbundenen Governance-Struktur für die Steuerung und Zukunftsgestaltung der verwendeten Technologie.

Für Anwendungsszenarien mit einem eingeschränkten Nutzerkreis innerhalb der deutschen Verwaltung können "private permissioned" Ledgers als möglicherweise gut geeigneter Ansatz angesehen werden. Durch die Eigenschaft "private" lassen diese Lösungen mehr Kompromisse in Sachen Skalierbarkeit zu, während die "permissioned" Natur durch die Implementierung von infrastrukturellen Schutzmechanismen außerhalb des Ledgers mehr Flexibilität hinsichtlich der Sicherheitsanforderungen an den Ledger selbst bietet.

Für die Unterstützung bürgergerichteter Anwendungsszenarien sind dahingegen die Anforderungen an die dort zu verwendenden "public" Ledgers sowohl bzgl. deren Skalierbarkeit als auch deren Sicherheit deutlich höher anzusetzen. Hinsichtlich der Frage, ob die zur Anwendung kommenden "public" Ledgers "permissioned" oder "permissionless" sein sollten, müssen die Für- und Wider-Argumente unter Betrachtung der Spezifika der jeweiligen Technologien kritisch bewertet werden. Obwohl in erster Annäherung ein "permissioned public" Ledger mit wohl definierten Knotenbetreibern in der Verwaltung als besser geeignete Lösung erscheinen mag (nicht zuletzt wegen einer einfacheren Umsetzung von Governance-Strukturen), könnten unter gewissen Voraussetzungen an das Governance-Modell (z.B. Vertrauenswürdigkeit durch technische und regulatorische Expertise, durch

geographische und organisatorische Verteilung und durch Kontinuität) sowie an die technisch-juristischen Eigenschaften des Systems (z.B. KYC-, AML-, DSGVO- und eIDAS-Konformität sowie "no-fork" Garantien) die Vorteile eines entsprechenden "permissionless public" Ledgers überwiegen. So wären z.B. unterschiedliche Prozesse und Anwendungsszenarien aus der freien Wirtschaft und aus der Verwaltung von der kommunalen, über die nationalen bis hin zur europäischen und globalen Ebene leichter integrierbar, so dass keine Medienbrüche für die Bürgerinnen und Bürger sowie für die staatlichen Instanzen bei fachübergreifender, transnationaler Nutzung entstünden. Zudem würde der höhere Grad an Dezentralität mit deutlich mehr Netzwerkknoten, als es in einem "permissioned public" Ledger wirtschaftlich abbildbar wäre, ein besseres Sicherheitsniveau mit erhöhter Manipulationsresistenz ermöglichen. Durch die Mitnutzung einer bestehenden dezentralen Infrastruktur und Governance-Struktur wäre zudem der Betrieb und die kontinuierliche Weiterentwicklung des Systems deutlich kosteneffizienter gewährleistet.

Aufgrund unterschiedlicher Anforderungen für "public" und "private" Ledgers können natürlich auch DLT-Lösungen mit unterschiedlichem Fokus (z.B. Geschwindigkeit vs. Sicherheit) eingesetzt und diese miteinander, falls interoperabel, kombiniert werden. Grundsätzlich gilt aber immer, dass nicht skalierbare bzw. nicht sichere Einzelkomponenten durch deren Kombination auch nicht schneller und sicherer werden. Optimalerweise sollte daher das Gesamtsystem aus in sich performanten und möglichst sicheren Teilkomponenten aufgebaut werden, um unnötige Kompromisse auf allen Ebenen zu vermeiden.

5.2. Skalierbarkeit

Klassische Blockchain-Technologien mit Proof of Work (PoW) Konsens-Algorithmen haben im Kern ein Skalierungsproblem. Einige Dutzend oder Hundert Transaktionen pro Sekunde lassen keine Anwendungsszenarien mit aktiver Beteiligung der Bürgerinnen und Bürger zu. Eine langsame Geschwindigkeit bei der Blockgenerierung kombiniert mit der fehlenden Finalität bedeutet, dass schreibende Transaktionen Minuten oder Stunden für ihre Bestätigung mit einer als hinreichend erachteten Zuverlässigkeit nach einer gewissen Anzahl von weiteren Blöcken benötigen. Entscheidend dabei ist, dass zwar die Wahrscheinlichkeit für die Unveränderlichkeit des Konsenses mit jedem neuen Block weiter gegen 100% konvergiert, eine 100%ige Sicherheit wird allerdings darüber formal betrachtet nie erreicht (d.h. "eventual consistency") [1].

Der Durchsatz klassischer Blockchain-Technologien mit PoW Konsens-Algorithmen wird oft auf Kosten der Sicherheit und Vertrauenswürdigkeit durch unterschiedliche Ansätze und Workarounds verbessert. "Economy based" Konsens-Mechanismen wie Proof of Stake (PoS) sind oft bzgl. ihrer Sicherheitsgarantien mathematisch nicht klassifizierbar, da diese die nicht vorhersagbaren stochastischen Verhaltensmuster der Netzwerkteilnehmer nicht formal beschreiben können [1]. "Leader based" Konsens-Algorithmen wie Paxos [2], Raft [3], PBFT [4], Tendermint [5] oder HotStuff [6] senken den Grad der Dezentralisierung enorm und machen das System dadurch gegen bestimmten Angriffsszenarien (DDoS-Attacke, Netzwerk Partitionierung durch Firewall-Attacke) anfällig. Ebenso sind zwar side-chains und off-chain Transaktionen deutlich schneller, spielen sich aber außerhalb des netzwerkeigenen bzw. netzwerk-übergreifenden Konsens-Mechanismus ab und können daher nicht das gleiche Maß an Sicherheit, Vertrauenswürdigkeit und Transparenz für die Beteiligten gewährleisten.

Da diese genannten Ansätze immer in einen oft nicht hinnehmbaren Kompromiss zwischen Geschwindigkeit, Sicherheit und Vertrauenswürdigkeit der Blockchain-Lösungen resultieren, müssen moderne Ansätze aus dem breiteren DLT-Spektrum betrachtet bzw. in der Praxis unter Beweis gestellt werden, welche das Problem der Skalierbarkeit mit gleichzeitiger Gewährleistung von höchstmöglicher Sicherheit zu bewältigen versprechen. Der Hashgraph Konsens-Algorithmus erreicht z.B. eine theoretisch höchstmögliche Geschwindigkeit von 100.000 Tx/s pro Shard (limitiert allein durch die Bandbreite des Internets) und weist gleichzeitig die mathematisch höchstmögliche Sicherheitsstufe eines dezentralen Systems, die Asynchronous Byzantine Fault Tolerance (ABFT), auf [7]. Diese Kombination von Skalierbarkeit und Sicherheit kann momentan keine andere DLT bzw. Blockchain-Technologie ihre Eigen nennen, geschweige denn ihre Sicherheitsgarantien von ABFT formal-mathematisch beweisen [8].

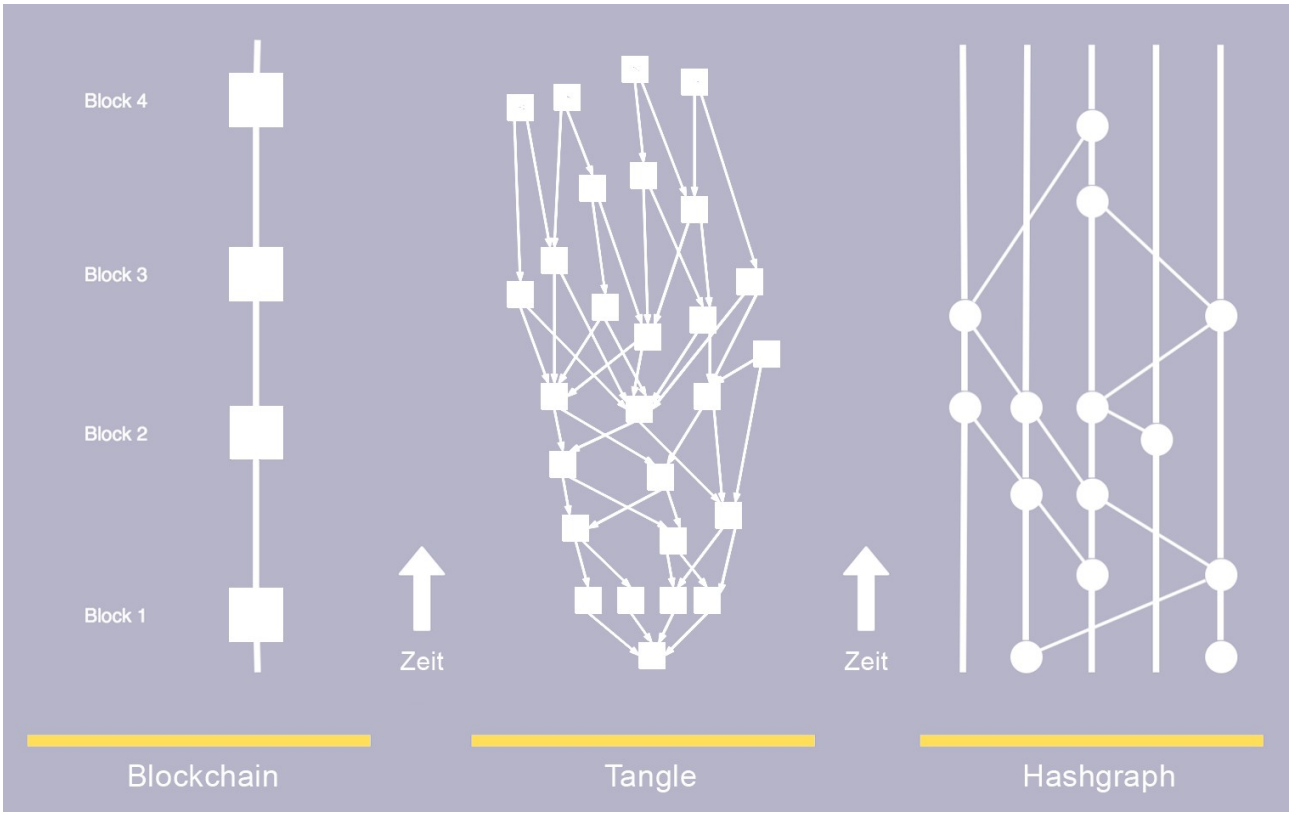


Abbildung 1: Schematische Darstellung der Datenstrukturen einiger unterschiedlicher Ledger-Arten ohne Anspruch auf Vollständigkeit – von links nach rechts: eine Blockchain, der Tangle von IOTA und Hashgraph. Die Zeit vergeht von unten nach oben.

5.3. Sicherheit

5.3.1. Sicherheit von Konsens-Mechanismen

Das Versprechen der Blockchain-Technologien bzgl. deren Manipulationsresistenz und Schutz gegen unterschiedliche Angriffsszenarien wird in der Regel wenig differenziert betrachtet. Konkret wird Manipulationsschutz oft als Blockchain-inhärente Eigenschaft unkritisch und pauschal postuliert, obgleich verschiedenen Konsens-Algorithmen ganz unterschiedliche Schutzniveaus gegenüber verschiedenen Angriffsszenarien erreichen können. Die unterschiedlichen Services eines Ledgers, welche auf Basis eines Konsens-Algorithmus realisiert werden (z.B. Smart Contract Ausführung, Geldtransfer, usw.), können zudem je nach Implementierung auch sehr unterschiedliche Qualitäten aufweisen. Für sicherheitskritische Anwendungsfälle sollten daher auf alle Fälle die versprochenen Performance- und Sicherheitseigenschaften sowie die Erfüllung bestimmter gesetzlichen Normen (z.B. DSGVO- und eIDAS-Konformität) durch anerkannte Akteure zertifiziert werden.

Die Manipulationssicherheit einer DLT beginnt im Regelbetrieb (d.h. noch ohne den Versuch einer bewussten Manipulation) mit der Gewährleistung einer fairen und nicht durch einzelne Netzwerkteilnehmer manipulierbaren Konsens-Reihenfolge der in den Ledger einfließenden Transaktionen. In klassischen Blockchain-Technologien können die Miner/Leader/Delegates (je nach Konsensverfahren) die Reihenfolge oder gar die Inklusion der Transaktionen innerhalb der von ihnen erstellten Blöcke alleine bestimmen und den Konsens bzw. den Zustand des Systems durch das Auslassen oder die Verzögerung von Transaktionen auch ungewollt beeinflussen [1]. Diese fehlende Fairness ist für viele Anwendungsfälle höchst problematisch (z.B. bei Marktplätzen wie bei einem Donor-Empfänger Matching in einer möglichen Vorstufe eines Transplantationsregisters). Moderne DLT-Konsensverfahren, wie beispielsweise Hashgraph, bieten hier ebenfalls neuartige Lösungsansätze. Durch Consensus Timestamps, welche im Konsens aller Knoten des Netzwerks ermittelt werden und die Reihenfolge der Transaktionen durch die Sortierung ihrer Konsens-Zeitstempel festlegen, wird Fairness auf Transaktionsebene (in Kontrast zu Blockebene im Falle einer Blockchain) für alle Teilnehmer des Netzwerks gewährleistet. Dieser Konsens wird sogar mit 100%iger Sicherheit innerhalb weniger Sekunden erzielt [7]. Eine spätere Veränderung des Konsenses ist dadurch ausgeschlossen. Diese Finalität lässt Angriffsszenarien für eine rückwirkende Manipulation des Konsenses (wie z.B. durch eine 51% Hashrate-Attacke für PoW-Systeme) effektiv unterbinden und eröffnet neuartige Möglichkeiten zur Gewährleistung von DSGVO- und eIDAS-Konformität.

Bei bewusster Manipulation eines Netzwerks durch bösartige Akteure wird zwischen 51%- und 34%-Angriffsszenarien unterschieden. Diese Prozentangabe besagt, welchen Anteil der für die Konsensfindung erforderlichen Ressourcen ein Angreifer kontrollieren muss, um den Konsens in seinem Sinne zu manipulieren (Gefährdung der Sicherheit - d.h. "safety" oder "consistency") oder das Netzwerk gar zum Erliegen zu bringen (Gefährdung der Lebendigkeit - d.h. "liveness"). So kann z.B. ein PoW-Konsensalgorithmus mit der Kontrolle über mehr als 50% der Knoten bzw. Rechenkapazität im Netzwerk manipuliert werden, oder ein PoS-System durch den Besitz von mehr als 33% des Stakes ausgehebelt werden. Darüber hinaus können Ledgers auch durch die Manipulation von außerhalb der Ledger-Infrastruktur befindlichen Komponenten angegriffen werden. Bei einer Distributed Denial of Service (DDoS) Attacke können z.B. wichtige Einzelknoten des Netzwerks (Leader/Delegates/Coordinators) durch Verhinderung

derer Kommunikation quasi "ausgeschaltet" und dadurch ggf. das gesamte Netzwerk lahmgelegt werden. Bei einem Firewall-Angriff können zudem bestimmte Teile des Netzwerks selektiv abgetrennt werden, sodass durch den manipulativ erzeugten Fork (d.h. Verzweigung der Wahrheit) eine Double Spending Attacke (z.B. zweimaliges Verkaufen eines Wertgegenstandes) durchgeführt werden kann. Diese Manipulationen fallen alle in die Kategorie der 34%-Angriffs-szenarien. 33% (genau gesagt ein Drittel) ist dabei eine magische Grenze, welche mathematisch festgelegt ist und die theoretisch höchstmögliche Widerstands-fähigkeit einer beliebigen DLT oder Blockchain-Lösung gegen sog. byzantinischen Fehler darstellt [9][11], deren Vorhandensein im Internet aufgrund üblicher Angriffs-szenarien leider angenommen werden muss.

In der Praxis können allerdings nicht alle Konsens-Verfahren diese höchstmögliche Stufe an Widerstandsfähigkeit erreichen. Hinsichtlich der realen Fehlertoleranz können Konsens-Mechanismen in vier Kategorien unterteilt werden: Crash Fault Tolerant (CFT), Byzantine Fault Tolerant (BFT), Asynchronous Byzantine Fault Tolerant (ABFT) und "undefiniert". CFT-Systeme garantieren dabei eine Sicherheit über das Erreichen des korrekten Konsenses (d.h. Konsistenz und Lebendigkeit des Ledgers), solange weniger als max. 50% der Knoten im System ausfallen, wobei dies die einzige tolerierte Fehlerart eines Knotens darstellt [1] [9]. Je nach Konsens-Verfahren können allerdings solche Systeme sogar durch die gezielte Manipulation eines einzigen Leader-Knotens ihre Lebendigkeit verlieren [10]. BFT-Systeme können die Konsistenz und Lebendigkeit des Ledgers gewährleisten, solange weniger als max. 33% (je nach Algorithmus kann die Grenze auch hier deutlich niedriger sein) der Knoten oder des Stakes im System auf beliebiger Weise fehlerhaft oder manipuliert sind – allerdings nur unter der Annahme, dass die Knoten innerhalb einer bekannten Zeitspanne miteinander kommunizieren können (Synchronität im Netzwerk) [4][9]. Gerade bei "public" Ledgers stellt diese Annahme wegen der oben beschriebenen DDoS- und Firewall-Angriffsszenarien ein großes Risikopotential dar. ABFT-Systeme brauchen hingegen keine zeitliche Annahme über die Synchronität der Kommunikation zwischen ehrlichen Knoten zu treffen, um die Widerstandsfähigkeit des Netzwerks bis zur theoretisch höchst-möglichen Grenze gewährleisten zu können [11]. ABFT-Algorithmen, wie beispielsweise Hashgraph, können daher auch unter realen Bedingungen im Internet mit DDoS- und Firewall-Attacken die Unaufhaltsamkeit und die Korrektheit des Konsenses bis zur theoretischen Grenze (d.h. bis zur beliebigen Manipulation von einem Drittel der Knoten oder des Stakes im Netzwerk) garantieren [7]. Zu guter Letzt gehören alle Konsens-Algorithmen, die die Eigenschaften eines CFT-, BFT- oder ABFT-Systems nicht aufweisen können, zur Kategorie "undefiniert". Diese Algorithmen erlauben leider aufgrund ihrer auf Wahrscheinlich-keiten und spieltheoretischen Mechanismen basierender Natur keine formale Einstufung oder gar Beweisführung über deren Sicherheitsniveau [1]. Beispiele für diese Kategorie sind PoW-Algorithmen, unterschiedliche Economy Based Mechanismen mit Proof of Stake (PoS) oder Proof of Importance (PoI), aber auch einige auf Directed Acyclic Graphs (DAG) basierende neue Ansätze wie der Tangle von IOTA.

Je nach Ledger-Topologie birgt eine unklare oder suboptimale Sicherheitseinstufung des verwendeten Konsens-Algorithmus unterschiedliche Risiken. Im Falle von "private permissioned" Ledgers kann zwar z.B. die Kritikalität der aus der fehlenden ABFT-Eigenschaft folgenden Sicherheits-risiken (Anfälligkeit gegen DDoS- oder Firewall-Angriffe) durch Schutz der Infrastruktur kompensiert werden, die vergleichsweise niedrige Anzahl von Knoten lässt allerdings die maximale 33%-Grenze für

Angreifer leichter erreichen. Aber auch "public permissionless" Netzwerke, welche die Konsensfindung durch Beteiligung einer eingeschränkten Auswahl von Knoten performant zu bewerkstelligen versuchen (Leader bei Leader based Systemen, Validatoren bei PoS-Systemen oder Delegates bei DPoS-Verfahren), sind gegen solche Angriffe wegen leichterer Erreichbarkeit der theoretischen 33%-Grenze deutlich anfälliger. Insbesondere bei der Nutzung solcher Konsens-Mechanismen sollte daher eine Zentralisierung des Netzes auf geographischer und organisatorischer Ebene sorgsam vermieden werden, damit die Funktionsfähigkeit des Ledgers trotz eines Katastrophenfalls, eines technischen Fehlers oder eines gezielten Angriffs einer Region, eines Rechenzentrums oder eines Cloud-Anbieters gewährleistet bleibt.

Eine Übersicht über die Eigenschaften der wichtigsten Arten von Konsens-Verfahren findet sich in der nachfolgenden Tabelle.

Kategorie	**Message Based Algorithmen (Nachrichtenbasierte)**		**Proof Based Algorithmen (Nachweisbasierte)**		**Voting Based Algorithmen**
Untergruppe	**Leader Based CFT**	**Leader Based BFT**	**PoW**	**Economy Based (PoS, PoI, usw.)**	**Gossip mit Virtual Voting**
Konsens-Algorithmus Beispiele (Ledger)	Paxos Raft	PBFT Tendermint (Cosmos) HotStuff (Facebook Libra)	(Bitcoin) (Ethereum)	Casper (Ethereum 2.0) Ouroboros (Cardano)	Hashgraph (Hedera)
Fehlertoleranz	CFT	BFT	Undefiniert	Undefiniert	ABFT
Sicherheit Konsistenz Finalität	Ja	Ja	Nein - "eventual consistency" bei Synchronität kurzfristig & Gefahr Hashrate-Attacke langfristig	Undefiniert (implementie-rungsabhängig)	Ja
Lebendigkeit	Nur bei Synchronität im Netzwerk	Nur bei Synchronität im Netzwerk	Ja	Undefiniert (implementie-rungsabhängig)	Ja - bis 33% byzantinischem Fehler auch mit Asynchronität im Netzwerk (d.h. z.B. bei DDoS-Attacke)
Formale Sicherheits-beweise	Ja	Ja	Nein	Nein	Ja - inkl. maschinen-gestütztem Coq-Beweis [8]
Durchsatz	Hoch - ca. 50.000 Tx/s mit max. 3 Fehlern (sinkt rapide mit fehlerhaften Knoten) [1]	Mittel hoch - ca. 1.000 - 20.000 Tx/s mit max. 3 Fehlern [1][6] (sinkt mit fehlerhaften Knoten je nach Algorithmus stark oder moderat [12])	Niedrig - ca. 10-100 Tx/s	Mittel hoch - ca. 1.000 - 10.000 Tx/s	Sehr hoch - ca. 100.000 Tx/s (keine wesentliche Degradation durch Fehler) [7]

Kategorie	Message Based Algorithmen (Nachrichtenbasierte)		Proof Based Algorithmen (Nachweisbasierte)		Voting Based Algorithmen
Untergruppe	**Leader Based CFT**	**Leader Based BFT**	**PoW**	**Economy Based (PoS, PoI, usw.)**	**Gossip mit Virtual Voting**
Skalierbarkeit auf n Knoten – Cummunication Time(!) Complexity	Mittelmäßig - $O(n)$ [6]	Mittelmäßig bis schlecht - $O(n)$ - $O(n^2)$ [6]	An sich sehr gut - $O(\log n)$, aber riesige lokale Computational Cost wegen PoW	Mglw. gut - $O(m + \log n)$, wo m die Anzahl der Validatoren darstellt und m<n	An sich sehr gut - $O(\log n)$, aber $O(n^2)$ lokale Computational Complexity wg. Virtual Voting
Fairness	Nein - Leader bestimmen im Alleingang den neuen Block	Nein - Leader bestimmen im Alleingang den neuen Block	Nein - Miner bestimmen im Alleingang den gefundenen Block	Nein - Validatoren bestimmen im Alleingang den neuen Block	Ja - durch Consensus Timestamps auf Transaktions-Ebene
Eignung für "private permissioned" Ledger	Bedingt - Skalierung weniger notwendig, Anfälligkeit gegen byzantinische Attacke durch Schutz der Infrastruktur kompensierbar	Bedingt - Skalierung weniger notwendig, Anfälligkeit gegen DDoS-Attacke durch Schutz der Infrastruktur und Optimierung der Algorithmen [12] kompensierbar	Nein - niedrige Geschwindigkeit	Bedingt - fehlende ABFT-Eigenschaft durch Schutz der Infrastruktur kompensierbar	Ja
Eignung für "public permission-less" Ledger	Nein - mittelmäßige Skalierung, hohe Anfälligkeit gegen byzantinische Fehler und Attacke	Nein - mittelmäßige Skalierung, hohe Anfälligkeit gegen DDoS-Attacke	Langfristig nicht - Energiebedarf	Bedingt - keine formalen Sicher-heitsgarantien, fehlende ABFT-Eigenschaft birgt hohe Risiken	Ja - sharding und / oder Optimierung der Computational Complexity vorausgesetzt

Tabelle 1: Übersicht über die Eigenschaften der wichtigsten Kategorien von Konsens-Verfahren. ACHTUNG: Die Auswahl der Algorithmen-Arten geschah ohne Anspruch auf Vollständigkeit. Die Angaben zu deren technischen Eigenschaften spiegeln den den Autoren bekannten Stand der wissenschaftlichen Forschung zum Zeitpunkt der Erstellung des Papiers (August 2019) wieder. Spätere Entwicklungen und Erkenntnisse in dem dynamischen Umfeld der DLT könnten die Berücksichtigung weiterer Algorithmen und mglw. die Anpassung einiger oben beschriebener Angaben erforderlich machen.

5.3.2. Sicherheit der Krypto-Algorithmen

Auf der untersten Ebene ist die Public Key Infrastructure (PKI) ein Grundstein für die Sicherheit von sämtlichen DLT, da die Transaktionen durch kryptographische Methoden wie Hashbildung und Signatur abgesichert werden. Es muss daher sichergestellt werden, dass die eingesetzten DLT auch mit unsicher werdenden Algorithmen bzw. mit neuen Algorithmen umgehen können, um die Vertraulichkeit, Integrität und Beweiswerterhaltung der on-ledger gespeicherten Daten langfristig zu gewährleisten. Aufgrund der perspektivisch zu erwartenden Weiterentwicklung der Quantencomputer (Schätzungen zufolge könnten in ca. 7-10 Jahren Quantencomputer existieren, die die heute üblichen PKI-Sicherheitsmechanismen kurzerhand umgehen können) müssen zudem die bereits heute eingesetzten DLT-Lösungen kritisch

bewertet werden, ob diese später durch den Einsatz von resistenten Algorithmen (z.B. Einmal-Signatur Schemes wie LD-OTS) gegen Quantencomputer gewappnet sein können – auch was die rückwirkende Absicherung bereits existierender Daten betrifft.

Als weitere wichtige Anforderung kann die Multisignatur-Fähigkeit der eingesetzten DLT angesehen werden. Durch hierarchische Multisignatur-Schemata mit geschachtelten Signaturmuster können komplexe Entscheidungswege organisationsübergreifend abgebildet werden, um die notwendigen Erlaubnisse für das Auslösen eines Prozessschrittes mit gleichzeitiger Gewährleistung der notwendigen Flexibilität bei Nichtverfügbarkeit einzelner Akteure bzw. deren Schlüssel anzubieten. Die Multisignatur-Funktion bietet zudem auch die Möglichkeit, Geheimnisse (wie private Schlüssel) mittels Secret Sharing im Ledger zu hinterlegen und im Verlustfall durch die notwendige Anzahl und Kombination von Signaturen wiederherzustellen, um die Handlungsfähigkeit der Akteure langfristig sicherzustellen.

5.4. Rechtliche Aspekte

In einer klassischen Blockchain müssen zwecks Integritätssicherung sämtliche Transaktionshistorien und die dadurch erzeugten on-chain gespeicherten Zustandsdaten in Form von immer länger werdenden Blockketten dauerhaft und unverändert aufbewahrt werden. Diese Unveränderlichkeit einer Blockchain ist zwar eine der wichtigsten Eigenschaften zur Gewährleistung ihrer Vertrauenswürdigkeit, es macht allerdings die Erfüllung bestimmter gesetzlichen Anforderungen äußerst schwierig.

Die von der DSGVO geforderte Notwendigkeit zur Berichtigung und Löschung der Daten durch berechtigte Instanzen oder das Recht auf Vergessenwerden eines Individuums ist mit einer Blockchain gerade aufgrund seiner Unveränderlichkeit schwer realisierbar [13]. Gemeinhin werden deshalb personenbezogene Daten iSd. DSGVO nicht direkt auf einer Blockchain gespeichert, sondern lediglich in Form von pseudonymisierten Daten (wie z.B. Hashwerte) hinterlegt. Allerdings kann je nach Konstruktion der pseudonymisierten Daten, insbesondere dem darin enthaltenen Maß an Entropie, auch dieser als personenbezogenes Datum angesehen werden, z.B. wenn der Hashwert durch Brute-Force-Methoden leicht zu erraten ist und dadurch Rückschlüsse auf die Rohdaten gezogen werden können (z.B. Hash(Vorname, Nachname) wäre ein einfach zu erratender Wert und gälte daher auch als personenbezogenes Datum). Während auf der Blockchain nur pseudonymisierte Daten abgelegt werden, können die Rohdaten mit Personenbezug auf klassischen Datenbanksystemen oder in geeigneten dezentralen Datenbanken vorgehalten werden, mit der Fähigkeit diese nach Bedarf zu löschen, wodurch der auf der Blockchain hinterlegte Referenzwert bedeutungslos wird. Da der Betrieb klassischer Datenbanksysteme das Risiko der Zentralisierung in sich trägt, sollte die Nutzung geeigneter dezentraler Speicherlösungen mit gleichzeitiger Anwendung der notwendigen Verschlüsselungsmechanismen und kryptographischen Zugriffsrechtemanagement-Verfahren bevorzugt werden, oder die Daten idealerweise beim Datensubjekt selbst im Sinne von SSI gehalten werden. Im letzteren Fall ist das Vorhandensein standardisierter Schnittstellen von wichtiger Bedeutung. Einerseits ermöglicht dies die Portabilität der Daten zwischen interoperablen, standardkonformen Wallet-Lösungen, anderseits kann dadurch ggf. die Zugänglichkeit der Daten gewährleistet werden, wenn z.B. Datenabfragen über mehrere Speicherorte hinweg (mit Zustimmung und expliziter Berechtigung der beteiligten Subjekte) automatisiert abgebildet werden sollten.

Die langfristige Integritätssicherung bzw. Beweiswerterhaltung einer Blockchain beruht u.a. auf den eingesetzten Hash- und Verschlüsselungsalgorithmen. Sobald diese ihre Sicherheitseignung verlieren (z.B. durch einen gebrochenen Hash-Algorithmus, mit dem Angreifer gezielt Hash-Kollisionen erzeugen können, um den Beweiswert eines damit gesicherten Datensatzes zu schwächen), müssen die on-chain gelagerten Transaktions- und Zustandsdaten, wie von eIDAS gefordert, neu verhasht bzw. inklusive eines qualifizierten Zeitstempels übersigniert werden. Dies stellt vor dem Hintergrund der Unveränderlichkeit der Daten ebenfalls eine große Herausforderung dar [13].

Andererseits entstehen derzeit alternative DLT-Systeme, welche mit gewissen Grundannahmen, was eine Blockchain technisch zwingend voraussetzt, brechen. Alternative DLT basierend auf Konsens-Mechanismen mit 100%iger Finalität, wie Hedera Hashgraph, können neuartige Möglichkeiten anbieten, um den beschriebenen Herausforderungen effektiv zu begegnen. Im Gegensatz zu Blockchain-Systemen muss diese neue Art von Ledger allein wegen der Integritätssicherung keine Transaktionshistorie mehr aufbewahren. Nachdem ein Konsens über eine Transaktion unumkehrbar erzielt worden ist bzw. nachdem diese Transaktion entsprechend ihrer Konsens-Reihenfolge ausgeführt worden ist, kann diese auf Wunsch auch weggeworfen werden. Der Zustand des Systems, welcher durch die Ausführung der Transaktionen in Konsens-Reihenfolge fortgeschrieben wird, kann wiederum in einer dezentralen Datenbank on-ledger festgehalten werden, welches die Bearbeitung und Löschung der Daten sowie eine kryptographische Beweisführung über deren Unversehrtheit (in Form von State Proofs) ermöglicht [14]. Auf funktionaler Ebene kann dadurch auch die Option zur Controlled Mutability (d.h. kontrollierte Veränderung) des Ledgers ermöglicht werden. Smart Contracts können dabei optional und transparent mit der Fähigkeit angelegt werden, durch die notwendige Anzahl und Kombination von Signaturen in einem vordefinierten Multisignatur-Schema "aufgeschlossen" zu werden, um beliebige Änderungen des Systemzustandes ebenfalls transparent und nachvollziehbar durch berechtigte Akteure vornehmen zu können [15]. Auf diesem Wege könnten fehlerhafte Transaktionen oder Folgen eines Betrugsfalls in geregelter Weise durch die berechtigten Akteure in der Verwaltung rückgängig gemacht werden, ohne sich mit dem Blockchain-üblichen Dilemma eines ggf. notwendigen rückwirkenden Forks befassen zu müssen. Durch die Änderung von Smart Contract Code im gleichartigen geregelten und transparenten Verfahren kann zudem die technische Lösung an geänderte gesetzliche Rahmenbedingungen angepasst werden und dem Embedded Law Ansatz mit Kontinuität Rechnung tragen.

Eine auf Merkle-Bäumen basierende dezentrale Datenbank für die Abbildung des Systemzustandes kann zudem, wie von eIDAS gefordert, im Falle eines aus Sicherheitsgründen notwendigen Algorithmus-Tauschs durch die simultane Anwendung des neuen Hash-Algorithmus auf allen Knoten die Neuverhashung des aktuellen Standes leicht bewältigen. Anstelle des von eIDAS aktuell vorgeschriebenen qualifizierten Zeitstempels eines zentralisierten und zertifizierten Zertifizierungsdiensteanbieters könnten dabei z.B. Consensus Timestamps als Nebenprodukt eines geeigneten Konsens-Mechanismus als offizieller Zeitstempel für jede Transaktion verwendet werden. Aus technischer Sicht könnte dieser Zeitstempel zwar als gleichwertige oder sogar zur DLT-Architektur besser passende Alternative angesehen werden, das juristische Rahmenwerk müsste jedoch noch erweitert werden, um geeignete DLT-basierte oder DLT-taugliche Lösungsansätze auch gesetzlich zu verankern und die für deren Zertifizierung notwendigen Sicherheitsmerkmale festzulegen.

6. Ausblick - Juristische Herausforderungen

Im nächsten Whitepaper werden die Initiative "Blockchain in der Verwaltung Deutschland" (BiVD) und die Community of Practice Blockchain des NExT-Expertennetzwerkes die beschriebenen rechtlichen Herausforderungen weiter beleuchten und Wege zur Harmonisierung von Recht und Distributed Ledger Technologien aufzeigen. Ein besonderer Fokus wird dabei auf eIDAS sowie der DSGVO liegen.

7. Abkürzungen

Abkürzung	Bedeutung
ABFT	Asynchronous Byzantine Fault Tolerance
AML	Anti Money Laundering (Geldwäschegesetz)
BFT	Byzantine Fault Tolerance
BiVD	Blockchain in der Verwaltung Deutschland (http://bivd-initiative.de)
CFT	Crash Fault Tolerance
DAG	Directed Acyclic Graph
DApp	Decentralized Application
DLT	Distributed Ledger Technology
DDoS	Distributed Denial of Service
DPoS	Delegated Proof of Stake
DSGVO	Datenschutz-Grundverordnung
eIDAS	electronic IDentification, Authentication and trust Services
KYC	Know Your Customer
LD-OTS	Lamport-Diffie One-Time Signature Scheme
NExT	Netzwerk Experten digitale Transformation der Verwaltung (http://next-netz.de)
PBFT	Practical Byzantine Fault Tolerance
PKI	Public Key Infrastructure
PoI	Proof of Importance
PoS	Proof of Stake
PoW	Proof of Work
SSI	Self Sovereign Identity
ZDA	Zertifizierungsdiensteanbieter

8. Literatur

[1] BSI, *Blockchain sicher gestalten - Konzepte, Anforderungen, Bewertungen*, 2019. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf

[2] Leslie Lamport, *The Part-Time Parliament*, ACM Trans. Comput. Syst., 16, Nr. 2, S. 133–169, 1998. https://lamport.azurewebsites.net/pubs/lamport-paxos.pdf

[3] Diego Ongaro und John Ousterhout, *In Search of an Understandable Consensus Algorithm*, 2014 USENIX Annual Technical Conference, USENIX ATC '14, Philadelphia, PA, USA, June 19–20, 2014, S. 305–319. https://raft.github.io/raft.pdf

[4] Migual Castro und Barbara Liskov, *Practical byzantine fault tolerance and proactive recovery*, 2002. http://www.pmg.csail.mit.edu/papers/bft-tocs.pdf

[5] Ethan Buchman, *Tendermint: Byzantine Fault Tolerance in the Age of Blockchains*, 2016. https://allquantor.at/blockchainbib/pdf/buchman2016tendermint.pdf

[6] Maofan Yin, Dahlia Malkhi, Michael K. Reiter et al., *HotStuff: BFT Consensus in the Lens of Blockchain*, 2019. https://arxiv.org/pdf/1803.05069.pdf

[7] Leemon Baird, *The Swirlds Hashgraph Consensus Algorithm*, 2016. https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

[8] Hedera Hashgraph, *Formal Methods: The Importance of Being ABFT in a World with Bad Actors*, 2018. https://www.hedera.com/blog/formal-methods-the-importance-of-being-abft-in-a-world-with-bad-actors

[9] Cynthia Dwork, Nancy Lynch und Larry Stockmeyer, *Consensus in the presence of partial synchrony*, J. ACM, 35, Nr. 2, S. 288–323, 1988. https://groups.csail.mit.edu/tds/papers/Lynch/podc84-DLS.pdf

[10] Michael J. Fischer, Nancy A. Lynch und Michael S. Paterson, *Impossibility of Distributed Consensus with One Faulty Process*, J. ACM, 32, Nr. 2, S. 374–382, 1985. https://groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf

[11] Leslie Lamport, Robert Shostak und Marshall Pease, *The Byzantine Generals Problem*, ACM Trans. Program. Lang. Syst., 4, Nr. 3, S. 382–401, 1982. https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf

[12] Zachary Amsden, Ramnik Arora, Shehar Bano et al., *The Libra Blockchain*, 2019. https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf

[13] Tomasz Kusber, Steffen Schwalm, Christian Berghoff, Ulrike Korte, *Langfristige Beweiswerterhaltung und Datenschutz in der Blockchain*, 2018. https://www.researchgate.net/publication/327467430_Langfristige_Beweiswerterhaltung_und_Datenschutz_in_der_Blockchain

[14] Leemon Baird, *Hedera Hashgraph Webinar: A stable ledger in an unstable forking world*, 2019. https://www.youtube.com/watch?v=mYrTBxfanPU

[15] Paul Madsen, *Hedera Technical Insights: Code is law, but what if the law needs to change?*, 2018. https://www.hedera.com/blog/code-is-law-but-what-if-the-law-needs-to-change

[16] Identity Working Group of the German Blockchain Association, *Self-sovereign Identity - A position paper on blockchain enabled identity and the road ahead*, 2018. https://www.bundesblock.de/wp-content/uploads/2019/01/ssi-paper.pdf

9. Impressum

Herausgeber

NExT e.V. in Zusammenarbeit mit der
Initiative "Blockchain in der Verwaltung Deutschland" (BiVD) und der
Community of Practice Blockchain des NExT-Expertennetzwerks

Bezugsquelle und Kontakt

Elektronisch zum Herunterladen
http://bivd-initiative.de
http://next-netz.de

Anfragen zur gedruckten Ausgabe oder zu sonstigen Themen
whitepaper@bivd-initiative.de
blockchain@next-netz.de

Autoren und Redaktion

Einleitende Kapitel

Helmut Nehrenheim (Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie NRW, BiVD), Florian Glatz (Bundesblock, Legal Tech Center), Alexander Rieger (Fraunhofer FIT), Laszlo Papp (Bundesnotarkammer)

Anwendungsbereiche und organisatorische Herausforderungen

Alexander Rieger (Fraunhofer FIT), Nadja Danninger (Bundesnotarkammer), Florian Glatz (Bundesblock, Legal Tech Center), Kai Wagner (Bundesblock, Jolocom, INATBA), Laszlo Papp (Bundesnotarkammer)

Technische Herausforderungen

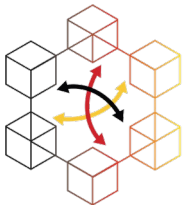
Laszlo Papp (Bundesnotarkammer), Florian Glatz (Bundesblock, Legal Tech Center), Alexander Rieger (Fraunhofer FIT)

Inhaltliches und formales Lektorat

Annette Wenninger (Fraunhofer FIT), Ralf Resch (VITAKO), Martin Fuhrmann (VITAKO), Nadja Danninger (Bundesnotarkammer), Helmut Nehrenheim (Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie NRW, BiVD), Dr. Hans-Günter Gaul (Bundesnotarkammer, NExT)

Gestaltung

Laszlo Papp (Bundesnotarkammer)



NExT
BiVD