NExT BiVD

ANKÜNDIGUNG WHITEPAPER

MÄRZ 2019

NExT

VITAKO

regio iT

BLOCKCHAIN BUNDESVERBAND

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

LEGAL TECH CENTER

Bundesamt für Migration und Flüchtlinge

Fraunhofer FIT

Projektgruppe Wirtschaftsinformatik

ZIEL

Ankündigung eines Blockchain-Whitepapers des BiVD

In einem zeitnah erscheinenden Whitepaper der Initiative „Blockchain in der Verwaltung Deutschland (BiVD)“ und des Next-Netzwerks sollen die wichtigsten **organisatorischen, technischen und juristischen Fragestellungen aufgezeigt werden**, die zur Entwicklung künftiger Blockchain-Lösungen für die öffentliche Verwaltung beantwortet werden müssen. Das Positionspapier folgt einem „Green Field"-Ansatz und stellt das erste Papier im Rahmen einer Blockchain-Whitepaper-Serie des BiVD dar.

INHALT DES POSITIONSPAPIERS

Zu Beginn skizziert das Whitepaper den generellen **Werte- und Prinzipien-Rahmen**, in welchen sich IT-Infrastrukturen für die deutsche Verwaltung einbetten müssen.

Anschließend werden die **technischen Besonderheiten** und für die öffentliche Verwaltung **Mehrwert stiftende Eigenschaften** der Blockchain-Technologie umrissen und vor dem Hintergrund des eingangs eingeführten Rahmens diskutiert.

Im dritten Abschnitt werden wichtige potentielle Anwendungsbereiche der Blockchain-Technologie in der öffentlichen Verwaltung vorgestellt. Diese Anwendungsbereiche orientieren sich an Erfahrungswerten der BiVD-Partner und an den Ergebnissen europäischer Arbeitsgruppen.

Im vierten Abschnitt spannt das Whitepaper **organisatorische, technische und juristischen Fragestellungen** auf, welche vor der Entstehung einer Blockchain-Infrastruktur in der deutschen Verwaltung adressiert werden müssen. Zudem werden aus diesen Fragestellungen spezifische Anforderungen abgeleitet.

Zum Abschluss skizziert das Papier einen Fahrplan für die vertiefte Untersuchung der Fragestellungen im Rahmen einer Whitepaper-Serie des BiVD.

WERTE- UND PRINZIPIEN-RAHMEN

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

Aktuell bedingen viele behördenübergreifend genutzte IT-Systeme eine Zentralisierung geographisch fragmentierter Datenbanken. Diese Zentralisierung birgt jedoch das Risiko einer Überwachungsmöglichkeit der Bürgerinnen und Bürger durch den Staat sowie einer großen Angriffsfläche gegenüber Hackern. Die Blockchain-Technologie bricht mit diesem Muster: Die Technologie 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. Die Entstehung eines parallelen digitalen Zentralstaats kann so verhindert werden.

Wird das **Once-Only-Prinzip** mittels der Blockchain-Technologie korrekt umgesetzt, können bestimmte Stammdaten von Bürgerinnen, Bürger 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 das freie Ermessen darüber, welche Daten an die Diensteanbieter digitaler Services übermittelt werden. Der europäische Rechtsraum ist von bürgerschützender Gesetzgebung wie dem **Datenschutz** geprägt. Der Schutz personenbezogener Daten kann unter anderem durch den Ansatz der Daten-Minimalisierung gefördert werden, um jederzeit nur die absolut notwendige Menge an Daten, die für die Nutzung des jeweiligen Services erforderlich sind, preisgeben zu müssen.

Eine richtig verstandene digitale Infrastruktur gibt die Möglichkeit, Verwaltung und Normadressaten zu helfen. Häufig wird sich das Recht, einmal in digitale Strukturen übersetzt, einbetten lassen. Das bedeutet, dass in einer staatlichen Blockchain-Infrastruktur Regeln und Institutionen des Staates als „Protokoll“ etabliert werden können. So kann der staatliche Rechtsrahmen teilweise als technisches Protokoll auf der Blockchain mitlaufen. Ebenso sind **Innovationsfreundlichkeit** in der Rechtsprechung und zeitgemäße, **agile Gesetzgebungsverfahren** notwendiger Kern des juristischen Umgangs mit neuen Technologien.

BESONDERHEITEN DER BLOCKCHAIN-TECHNOLOGIE

Eigenschaften und Mehrwerte

Blockchain-Lösungen können **Vertrauen zwischen unterschiedlichen Akteuren stärken** (z.B. zwischen Behörden, Unternehmen, Bürgerinnen und Bürger). Sie ermöglichen ihren Nutzern eine **gemeinsame Sicht auf die "Wahrheit"** zu erhalten, die weder von einzelnen Nutzern noch von Dritten **gemäß der 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 (nachträgliche) **Überprüfung der Richtigkeit und Unversehrtheit** der abgelegten Informationen.

Die dezentrale Speicherung ermöglicht den Akteuren zudem die vollständige Kontrolle über die eigenen personenbezogenen Daten im Sinne **selbstsouveräner Identitäten** (SSI) und lässt damit die durch DSGVO definierten Ziele in den digitalen Prozessen der Zukunft leichter und besser realisieren.

Moderne Blockchain-Technologien können zudem **Prozesslogiken** in sogenannten Smart Contracts hinterlegen. Diese vordefinierten und für jeden einsehbaren Prozesslogiken werden bei Eintritt bestimmter Bedingungen automatisch ausgeführt und können dadurch die **Effizienz, Transparenz und Manipulationsresitenz von Prozessen steigern**.

ANWENDUNGSBEREICHE IN DER ÖFFENTLICHEN VERWALTUNG

Die Blockchain-Technologie kann die öffentliche Verwaltung in verschiedensten Bereichen unterstützen. Vereinfacht gesagt bietet Blockchain eine IT-Lösung für föderale Geschäfts- und Verwaltungsprozesse, in denen die Wahrung der digitalen Souveränität und das Once-Only-Prinzip eine wichtige Rolle spielen. Im Folgenden sind die vier vielversprechendsten aufgeführt.

Blockchain-basierte Identitätslösungen erlauben es, den Bürgerinnen und Bürgern die Kontrolle über ihre digitalen Identitäten zurückzugeben und Identitätsnachweise ohne die Preisgabe identitätsbezogener Informationen zu gestalten. Darüber hinaus können derartige Identitätslösungen Bürgerinnen und Bürgern Mitbestimmungsrechte bei der Weitergabe identitätsbezogener Informationen ermöglichen. Blockchain kann entsprechend deutliche Mehrwerte für den Aufbau funktionierender föderaler e-Government Dienste bieten.

Die Blockchain-Technologie kann zudem die **Koordination behördenübergreifender Verwaltungsvorgänge** unterstützen. Die zeitnahe Verteilung neuer Informationen an alle Teilnehmer und Teilnehmerinnen des Blockchain-Netzwerks ermöglicht eine organisationsübergreifende Orchestrierung von Prozessen. Im Netzwerk verteilte Sachstände können so beispielsweise als Auslöser für den Beginn von Folgeprozessen bei anderen Behörden genutzt und Prozesszwischenzeiten dadurch deutlich reduziert werden. Werden im Blockchain-Netzwerk zudem präzise Datenbankverweise gespeichert, können weiterführende Informationen bei Bedarf zielgerichtet angefragt werden. Blockchain kann somit die Informationsverfügbarkeit bei gleichzeitiger Wahrung des Once-Only-Prinzips signifikant verbessern.

Die Blockchain-Technologie ermöglicht außerdem eine **digitale Nachhaltung von Zeugnissen oder Ausweisdokumenten**. Blockchain-Lösungen ermöglichen dabei einerseits, den Aussteller zu identifizieren und die Echtheit zu verifizieren. Gleichzeitig garantiert die Blockchain-Lösung die Persistenz des Dokuments. Auch eine etwaige Unwirksamkeit kann zu einem späteren Zeitpunkt auf der Blockchain vermerkt werden. Konkret können mit einer Blockchain-Lösung beispielsweise Zeugnisse oder Führerscheine digital nachgehalten werden.

Zudem kann die Blockchain-Technologie einen Beitrag zur **Modernisierung der Registerlandschaft** leisten. Konkret ermöglicht die Blockchain-Technologie die Schaffung innovativer neuer Meta-Register, in welchen Daten (veränderungen) in fragmentierten Registern indiziert werden können. In bestimmten Fällen könnten aber auch bestehende Register von einer Abbildung auf einer Blockchain profitieren, wenn es sich dabei um Register handelt, die keinen öffentlichen Glauben begründen.

Daneben sind noch viele weitere Anwendungsfälle denkbar, wie beispielsweise eine Automatisierung des Steuereinzuges, eine Zweckbindung von Zuschüssen oder eine Zweckbindung von Zuschüssen.

FRAGESTELLUNGEN

Organisatorische Fragestellungen

Das Thema **Verantwortung & Governance** spielt in der öffentlichen Verwaltung eine wichtige Rolle. Hierfür müssen die Verantwortlichkeiten bzgl. der Implementierung, des Betriebs und der Wartung einer Blockchain-Infrastruktur geklärt werden. Dabei müssen klare Entscheidungsstrukturen, Handlungsbefugnisse und Kontrollmechanismen etabliert werden, welche die Bedürfnisse der öffentlichen Verwaltung widerspiegeln und gleichzeitig eine zielgerichtete Implementierung, einen stabilen Betrieb sowie eine effektive Wartung ermöglichen. Zudem gilt es zu klären, wie eine Blockchain-Infrastruktur der Verwaltung finanziert werden kann.

Auch das Thema **nachhaltige Weiterentwicklung** ist bei vielen Blockchain-Technologien noch nicht sichergestellt. Blockchain-Technologien müssen auch in Zukunft kontinuierlich an neue Erkenntnisse und Anforderungen anpassbar sein. Dies erfordert eine aktive Weiterentwicklung durch entsprechende Entwickler-Gruppen bzw. Organisationen ggf. unter staatlicher Beteiligung. Ohne diese Weiterentwicklungen können auch etwaige gesetzliche Neuerungen nicht umgesetzt werden. Aus Sicht der öffentlichen Verwaltung ist daher die Entwicklung eines entsprechenden Modells zur nachhaltigen Weiterentwicklung einer Blockchain-Infrastruktur essentiell.

Technische Fragestellungen

Passend zur organisatorischen Ausgestaltung müssen **alternative Netzwerk-Topologien** durch unterschiedliche Kombination öffentlicher und privater Blockchains zu einem Gesamtsystem beleuchtet werden. Insbesondere müssen dabei Anforderungen hinsichtlich der **Interoperabilität** der beteiligten Blockchain-Lösungen und Komponenten definiert werden.

Aufbauend auf der Netzwerk-Topologie und den Nutzungs-Charakteristika der durch die jeweiligen Blockchain-Lösungen zu realisierenden Anwendungsfälle müssen die genauen Anforderungen hinsichtlich der **Skalierbarkeit der Blockchain-Infrastruktur** und des notwendigen **Sicherheitsniveaus des Konsens-Algorithmus** und der Gesamtsoftware kritisch bewertet werden.

Die maximale Anzahl von Transaktionen pro Sekunde stellt dabei für viele klassische Blockchain-Technologien eine Herausforderung für deren breitflächige Anwendung durch die Bürgerinnen und Bürger dar. Moderne Ansätze adressieren diese Einschränkungen durch alternative Konsens-Mechanismen (wie Proof of Stake statt Proof of Work) oder durch vollkommen neue, vielversprechende Ansätze (wie z.B. gerichtete azyklische Graphen), welche aber noch in der Praxis erprobt werden müssen.

Zwar bietet die Blockchain-Technologie allgemein einen hohen Grad an Manipulationsresistenz, verschiedene Konsens-Algorithmen können sich jedoch hinsichtlich deren Schutzniveau gegen Angriffsszenarien verschiedener Art stark unterscheiden. Die Sicherheitsgarantien unterschiedlicher Technologien müssen daher unter Berücksichtigung der angestrebten Netzwerk-Topologie kritisch bewertet und miteinander verglichen werden.

Juristische Fragestellungen

Der Aufbau einer Blockchain-Infrastruktur für die deutsche Verwaltung birgt daneben eine Reihe **rechtlicher Herausforderungen**. Wird ein Blockchain-Netzwerk tatsächlich dezentral betrieben, gibt es per Definition keinen zentralen Intermediär, der klassisch reguliert oder von Anwenderseite adressiert werden könnte. Die bislang von vertrauenswürdigen Dritten gebotene Sicherheit wird durch eine Software bzw. Ausführungsumgebung in einem dezentralen Netzwerk ersetzt (Protokolle).

Es ist deshalb von entscheidender Bedeutung, neue regulatorische Möglichkeiten im Bereich der dezentralen Netzwerke durch **Soft Governance, zertifizierte Standards und intelligente Regulierung** zu entwickeln, die in das digitale Gefüge einer kollektiv betriebenen Verwaltungsinfrastruktur eingebettet sind (Embedded Law).

Zwar bringt die Blockchain-Technologie in Sachen selbstsouveräner Identitätsverwaltung große Vorteile mit sich, es gibt jedoch hinsichtlich der **Berichtigung und Löschung von Daten** (etwa das Recht auf Vergessen werden aus der DSGVO) auch große Herausforderungen, die adressiert werden müssen. Best-Practices unter anderem im Bereich der Daten-Minimalisierung müssen etabliert und gefördert, das Versprechen neuer technischer Lösungsansätze analysiert und getestet werden.

Hinsichtlich der **langfristigen Beweiswerterhaltung und des Integritätsschutzes** müssen zudem unterschiedliche Lösungsansätze zur Gewährleistung der eIDAS-Konformität überprüft und bewertet werden. Wichtige Themen sind dabei der Umgang mit kryptographischen Algorithmen, auf deren Sicherheit die Blockchain-Technologie ruht, die aber mit der Zeit ihre Sicherheitseignung verlieren können, die Erzeugung von vertrauenswürdigen Zeitstempeln durch qualifizierte Zeitstempeldienste oder Blockchain-eigene Mechanismen, sowie perspektivisch das Schutzniveau gegenüber Quantencomputern.

WER SIND WIR?

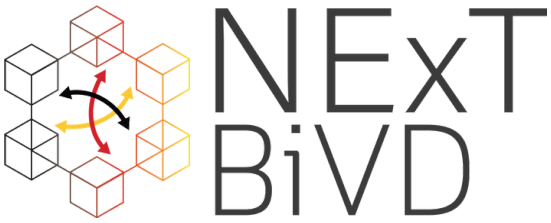
Der CIO des Landes Nordrhein-Westfalen hat im Jahr 2018 die Initiative „Blockchain in der Verwaltung Deutschland (BiVD)“ ins Leben gerufen. Neben der CIO-Abteilung des Nordrhein-Westfälischen Wirtschafts- und Digitalisierungsministeriums konnten VITAKO zusammen mit RegioIT Aachen, das Bundesamt für Migration und Flüchtlinge (BAMF), sowie der Bundesblock (Blockchain Bundesverband - Verband zur Förderung der Blockchain-Technologie in Deutschland) sowie die Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT als Initiativpartner gewonnen werden. Ebenfalls im Jahr 2018 hat sich BiVD mit dem NExT-Netzwerk zu „NExT-BiVD“ zusammengeschlossen.

ZEITPLAN

Die Arbeitsgruppe plant die Veröffentlichungen folgender Dokumente:

- Ein erstes Whitepaper mit Beschreibung der Anwendungsfälle, detaillierter Diskussion der organisatorischen, technischen und juristischen Fragestellungen und einer Ableitung entsprechender Anforderungen.

- Ein zweites Whitepaper mit Bewertung unterschiedlicher Technologien und Lösungsansätzen, einer Analyse relevanter Proof-of-Concept-Projekte und einer Skizzierung der weiteren Schritte des BiVD.



MÄRZ 2019