Aktionspapier des Blockchain Bundesverband e.V.

zur Blockchain-Strategie der Bundesregierung vom 18.09.2019

Arbeitsgruppe :

Digitale Identität

Autoren:

Kai Wagner, Oliver Naegele, André Kudra,

Irene Adamski, Silvan Jongerius

BLOCKCHAIN BUNDESVERBAND

Digitale Identität

Digitale Identität

Vorwort:

Die Arbeitsgruppe zu Digitalen Identitäten innerhalb des Bundesverband Blockchain[1] hat die im September veröffentlichte Blockchain-Strategie der Bundesregierung insgesamt positiv aufgenommen. Das klare Bekenntnis der Bundesregierung zur Bedeutung interoperabler und technologieneutraler Digitaler Identitäten für die digitale Souveränität der Bundesrepublik ist dabei besonders hervorzuheben und wird ausdrücklich begrüßt. Die in Kapitel 4 der Strategie beschriebene Rolle des Staates bei der Etablierung von Vertrauen in Digitale Identitäten, insbesondere die hierfür vorgeschlagene Verknüpfung von staatlicher Vertrauens-infrastruktur (z.B. eIDAS) mit selbst-bestimmten Identitäten auf Blockchain-Basis, ist zukunftsweisend.

Die geplanten Pilotprojekte für solche blockchain-basierten, digitalen Identitäten in Schaufensterregionen wurde vom Blockchain Bundesverband bereits im Positionspapier zur Bundestagswahl 2017 gefordert. Zu sehen, dass mit der Ausschreibung zum Schaufenster Sichere Digitale Identitäten jetzt konkrete Schritte eingeleitet wurden wird vom Verband ausdrücklich begrüßt.

Um realwirtschaftliche Effizienzgewinne und damit volkswirtschaftlichen Nutzen, sowie erhöhte Benutzerfreundlichkeit zu ermöglichen, müssen jedoch weitere Schritte folgen. Bürger und Unternehmen sollen medienbruchfrei Verwaltungsinteraktionen tätigen können. Die notwendigen gesicherten Attribute und Nachweise sollten dabei zusätzlich zum elektronischen Personalausweis auch durch weitere Verifizierungsstellen kommen können. Die Nutzung des elektronischen Personalausweises ist statistisch zu gering um eine notwendige Abdeckung für Unternehmen zu ermöglichen.

Das mit Blockchain Technologie ermöglichte Identitätsmodell der Self-sovereign Identity [2](SSI) kann hier einen enormen Mehrwert bieten, da es die Ausstellung, Speicherung und Nutzung von digitalen Identitätsattributen und Nachweisen über ein modulares und interoperables Identitäts-Protokoll möglich macht. Mit Hilfe von SSI können Bürger so eine anbieterunabhängige Technologie nutzen, welche über Vetrauensniveaus hinweg eine hohe Sicherheit, Zuverlässigkeit und Benutzbarkeit bietet.

Zwar finden sich im Strategiepapier Hinweise auf die Bereitschaft im eGovernment auch dezentrale Datenhaltung bei Bürgern und Unternehmen zu ermöglichen, das Papier bleibt hier jedoch zu vage und sollte um konkrete Vorschläge ergänzt werden.
Das Bekenntnis zu offenen Standards und die Notwendigkeit der Abstimmung im europäischen digitalen Binnenmarkt ist von besonderer Bedeutung und sollte weiter vertieft werden. Nur wenn ein gemeinsames europäisches Rahmenwerk für Blockchain-basierte digitale Identitäten entsteht, werden wir die positiven Effekte dieser neuen Vertrauensinfrastruktur in Europa verwirklichen können. Das im Rahmen des European Blockchain Partnership Programms laufende Projekt für ein „European Self-sovereign Identity Framework“[3] (ESSIF) im European Blockchain Service Infrastructure Projekt (EBSI)[4] ist hier von großer Bedeutung. Modelle wie EBSI und ESSIF können dabei aber nur für die Schnittstelle zu öffentlichen Stellen (Registern, etc.) genutzt werden. Die begleitenden Blockchain Projekte für eine Beteiligung und Zugriffssteuerung der Bürger*innen und Unternehmen durch privatwirtschaftliche Lösungen sind dabei elementar und zukunftsweisend.

Während sich die generelle Haltung der Bundesregierung zum Thema Blockchain und DLT im Strategiepapier als zukunftsorientiert, weitsichtig und anwendungsbezogen präsentiert, wird es in erster Linie darum gehen, wie schnell, fachlich sauber und handwerklich gut gemacht die präsentierten Ideen umgesetzt werden.

1 https://bundesblock.de/de/groups/digital-identity/
2 https://www.bundesblock.de/wp-content/uploads/2019/01/ssi-paper.pdf
3 https://www.eesc.europa.eu/sites/default/files/files/1._panel_-_daniel_du_seuil.pdf
4 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi

Anreize zur Sicherstellung und Förderung von Interoperabilität

Im digitalen Binnenmarkt und internationalen Wettbewerb stellt Interoperabilität eine Grundvoraussetzung für erfolgreiches wirtschaftliches Handeln dar. Wie oben bereits dargelegt begrüßt der Blockchain Bundesverband das in der Blockchain-Strategie formulierte Bekenntnis zur Förderung und Nutzung offener Standards.
Bisher bleibt dieses Bekenntnis jedoch zu vage, da klare Ziele oder Regelungen für eine solche Förderung von Interoperabilität und offenem Wettbewerb auf Augenhöhe fehlen.

Konkrete Schritte hin zur Förderung von Wettbewerb und Innovation wäre in diesem Punkt die Änderung von Förderkriterien und Beschaffungsregelungen für den öffentlichen Dienst wie sie auch von der Kampagne Public Money Public Code[1] gefordert werden.
Die in der Ausschreibung zum Schaufenster Sichere Digitale Identität angemahnte Berücksichtigung offener Standards kann in diesem Verständnis nur ein erster Schritt sein in Zukunft starke Anreize für die Verwendung von offenen Standards und Open Source Software in der Beschaffung und Vergabe von Förderungen zu setzen.

Ein innovativer Wettbewerb für Digitale Lösungen (aus Deutschland) kann sich nur in einem fairen und offenen Markt entfalten, bei dem aktuelle Monopoltendenzen im Bereich Software und Cloud Computing durch ein radikales Bekenntnis zu Interoperabilität und Open Source eingehegt werden.[2] Wie wichtig dies gerade im Bereich digitaler Identitäten ist, kann hier nur einmal mehr betont werden.

Aufeinander aufbauende kurze Projektzyklen für Pilotprojekte und Proof of Concepts

Die Erprobung von Digitalen Identitäten auf Blockchain-Basis geht im öffentlichen Sektor bisher nur schleppend voran. Zwar gibt es mit Wettbewerb zum Schaufenster Sichere Digitale Identitäten einen aktuellen Förderaufruf der explizit auf die Themen der Arbeitsgruppe bezug nimmt, die Zeitplanung dieses Förderaufrufs steht aber im krassen Kontrast mit der Innovationsgeschwindigkeit im Markt Digitaler Identitäten auf Blockchain-Basis.

So wertvoll die Förderung von Projekten ist welche über einen längeren Zeitraum von zwei bis drei Jahren durchgeführt werden, so wenig können diese Projekte einen Einfluss auf die laufende Konsolidierung am Self-sovereign Identity Markt nehmen.
Durch eine aktive Erprobung von Self-sovereign Identity in kurzen und iterativen Projektzyklen wäre es möglich, eine klare Position zu erarbeiten und damit auch eine proaktive Rolle in der Regulierung von Self-sovereign Identity Konzepten einzunehmen. Ein erster Schritt hierfür kann die in der Strategie angesprochene Beteiligung am ESSIF-Projekt auf EU Ebene sein. Empfehlenswert wäre eine Erprobung von neuen Technologien wie sie in den Vereinigten Staaten von Amerika umgesetzt wurde.[3]
Dort wurde in einer kürzlichen Ausschreibung des Department of Homeland Security nach konkreten Technologien zur Prozessverbesserung gesucht, welche in einem iterativen 4 Phasen Modell umgesetzt werden.[4] Diese Art der Ausschreibung ermöglicht einen kontinuierlichen Lernprozess und damit einhergehend eine bessere Grundlage zur regulatorischen Einordnung der neuen Technologie, sowie deren Standardisierung.

Zieht man in Betracht welche Rolle Self-sovereign Identity mittelfristig auf den gesamten Markt für Digitale Identitäten haben wird ist es wichtig, dass sich Deutschland bei dieser Konsolidierung durch ein Bekenntnis zu IT-Sicherheit, Interoperabilität und Datenschutz klar positioniert. Die Nutzung kurzer iterativer Projektzyklen und eine schnelle Umsetzung von Reallaboren sind dafür essentiell.

---

1 https://publiccode.eu/de/
2 Die relevanten Maßnahmen im Rahmen der European Blockchain Partnership (EBP), insbesondere unter dem zuvorgenannten ESSIF, sind dabei zu berücksichtigen bzw. entsprechende Beiträge sind dort zu leisten.
3 https://www.dhs.gov/science-and-technology/svip
4 https://www.dhs.gov/science-and-technology/news/2019/09/26/news-release-dhs-st-awards-143k-blockchain-interoperability

Digitale Identität

Anerkennung von abgeleiteten Digitalen Identitäten

Der Bundesverband Blockchain empfiehlt die Anerkennung von “abgeleiteten Digitalen Identitäten der Privatwirtschaft für Verwaltungsverfahren bzw. bestimmte Rechtsgeschäfts” wie es auch im §4.1 der Blockchain-Strategie gefordert wird. Interessant sind hier vor allem jene abgeleiteten Identitätsattribute und Dokumente für die es bisher kein digitales Äquivalent gibt.

Nur wenn es für diese Attribute und Dokumente eine rechtliche Anerkennung gibt, können Investitionen in diesen Bereich erfolgen.
Das Konzept von SSI basiert auf einer freien Wahl der Bürger von privatwirtschaftlich organisierten Identitäts-Dienstleistern. Privatwirtschaftlicher Wettbewerb führt zu höherer Innovation, wobei durch klare Vorgaben im Bereich Sicherheit, Datenschutz und Interoperabilität der notwendige Standard vorgegeben werden sollte.

In einem Workshop können die Mitglieder der Arbeitsgruppe Digitale Identitäten des Bundesverbandes Blockchain mit Vertretern des BSI einen Anforderungskatalog erstellen. Darauf aufbauend sollte ein offener Wettbewerb in Form einer Konzept-Vorstellung von unterschiedlichen Lösungsansätzen (Pitch-Event) mit Vertretern der Bundesregierung durchgeführt werden.

Diese Veranstaltung kann in Abstimmung vom Bundesverband Blockchain durchgeführt werden. Der Bundesverband Blockchain empfiehlt die Bereitstellung eines Budgets sowohl für die Ausarbeitung der Vorgaben in Form eines Arbeitspapiers als auch für die Durchführung der Veranstaltung. Darauf aufbauend sollte dann eine Weiterführung der besten Lösungen gefördert werden.

Kategorie	Digitale Identität
Forderung	Anerkennung von “abgeleiteten Digitalen Identitäten der Privatwirtschaft für Verwaltungsverfahren bzw. bestimmte Rechtsgeschäfts”
Blockchain Strategie	§4.1
Handlungsnotwendigkeit	hoch
Reifegrad der Lösungen	mittel
Förderbedarf	hoch
Call to Action	Offener Wettbewerb in Form einer Konzept-Vorstellung von unterschiedlichen Lösungsansätzen (Pitch-Event) mit Vertretern der Bundesregierung.
Ansprechpartner	Jolocom, esatus, AG, Blockchain HELIX u.a.

Blockchain und Datenschutz

In der Blockchain-Strategie der Bundesregierung fällt die Aussage, dass sich aus Sicht der Bundesregierung kein Änderungsbedarf bei der DSGVO ergibt, wenn es um die Anwendung von Blockchain-Technologie geht (Punkt 3a S.13). Vielmehr, heißt es, muss die Blockchain-Technologie datenschutzkonform ausgestaltet und angewendet werden. Wir stimmen dieser Aussage als Verband insoweit weitgehend zu, müssen aber darauf verweisen, dass diese datenschutzkonforme Ausgestaltung und Anwendung ohne Unterstützung der Regierung und der Datenschutzbeauftragten zum jetzigen Zeitpunkt unmöglich ist.

Wir begrüßen aus diesem Grund den Vorschlag einer Round Table-Veranstaltung zu Datenschutz und Blockchain. Um die offenen Fragen jedoch wirksam anzugehen, empfehlen wir eine aufeinander aufbauende Reihe an Round Table Workshops, bei denen eine gleichbleibende Gruppe an Teilnehmer*innen aus Verbänden, Ministerien und weiteren Stakeholder-Gruppen gemeinsam an einem geteilten Verständnis der Problemlage und deren subsequenter Lösung arbeiten kann.

Die größten Hindernisse für eine datenschutzkonforme Anwendung von Blockchain-Technologie und somit Leitfragen für eine Round Table-Reihe ist hier zusammengefasst:

1. **Governance von Blockchain Netzwerken als Ausgangspunkt der datenschutzrechtlichen und Compliance Bewertung**

In ihrer Architektur können Blockchain- und DLT-Netzwerke vor allem in zwei Dimensionen unterschieden werden: Erstens, ob der Kreis der teilnehmenden / schreibenden Knotenpunkte (Nodes) eine Zugangsbeschränkung aufweist oder nicht (permissioned & permissionless). Zweitens kann danach unterschieden werden, ob das Netzwerk öffentlich ausgelesen werden kann oder nicht (public & private). Aus diesen Architekturen ergeben sich höchst unterschiedliche Governance- Anforderungen und damit einhergehende Rollen und Verantwortlichkeiten. Eine datenschutzrechtliche Bewertung von Blockchain-Lösungen muss diese fundamentalen Unterschiede anerkennen und entsprechend getrennt bewerten.

2. **Klärungsbedarf besteht des weiteren bei der Zuweisungen datenschutzrelevanter Rollen für die Bewertung von DLT- und Blockchain-Angeboten**

Es gibt eine Vielzahl an Interpretationen der DSGVO bei der Frage ob ein Blockchain basierter Dienst als Data Processor oder Data Controller eingestuft werden muss. Wie kann mit der unklaren und teilweise gleichzeitigen Zuweisung von Prozessor und Controller bei verteilten/nicht-hierarchischen Netzwerken und Peer to Peer (P2P)-Technologien umgegangen werden? Hier stellt sich zudem die drängende und auch über DLT und Blockchain hinausgehende Frage, ob die DSGVO mit dem Ziel der Datensouveränität und deren Erreichung durch P2P-Technologien in Einklang zu bringen ist?

3. Zur Anonymisierung und Hashing von Daten welche in DLT- und Blockchain-Netzwerken gespeichert werden wird eine klare Einordnung und Bewertung benötigt.

Anonymisierung ist eine Praktik des DSGVO, die nicht nur im Bereich der Blockchain-Technologie noch viele Fragen offen lässt (siehe Konsultation des Bundesdatenschutzbeauftragten). Eine erste Möglichkeiten einer DSGVO-konformen Anonymisierung wurde bereits durch die Artikel 29 Arbeitsgruppe diskutiert. Eine tragfähige Anerkennung der entsprechenden Auslegung im Kontext der DLT und Blockchain-Technologie durch verantwortliche Stellen in Deutschland blieb bisher jedoch aus. Im Oktober 2019 wurde ein gemeinsames Papier von der Spanischen Datenschutzbehörde und dem Europäischen Datenschutzbeauftragten veröffentlicht. Das Dokument untersucht die Verwendung von Hash Funktionen als Mittel der Pseudonymisierung.[1] Ob die darin gemachten Schlüsse auch für Deutschland übertragen werden können ist bisher nicht geklärt. Eine klare Einordnung ist entsprechend erforderlich.

4. Unklarheit darüber ob in der DSGVO genannte Ausnahmen für das Recht auf Löschung und Berichtigung in DLT- und Blockchain-Netzwerke angewendet werden können.

Zwar sind diese Punkte stark vom Anwendungsfall abhängig, es lässt sich aber heute keine sichere Bewertung vornehmen, da bei Fehleinschätzung eine nicht veränderbare Eintragung erfolgen könnte, welche für Unternehmen weitreichende Folgen nach sich ziehen könnte. Wie auch für die oben stehenden Punkte wäre es empfehlenswert, wenn konkrete “best practices” entsprechend der unterschiedlichen Governance-Architekturen entwickelt würden, um eine Umsetzung der Betroffenenrechte (Löschung/Berichtigung) zu gewährleisten.

1 https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf