FZI

FZI FORSCHUNGSZENTRUM INFORMATIK

BLOCKCHAIN-TECHNOLOGIE

Positionspapier

Kompetenzzentrum
IT-Sicherheit

FZI-Positionspapier | Veröffentlichung 31.05.2019 | Version 1.0

Herausgeber

FZI Forschungszentrum Informatik
Haid-und-Neu-Str. 10–14
76131 Karlsruhe
Tel: +49 721 9654-0
Fax: +49 721 9654-909
Stiftung des bürgerlichen Rechts
Stiftung Az: 14-0563.1

ISSN 0930-3014

INHALTSVERZEICHNIS

Die Blockchain wird derzeit von vielen als mögliche Basistechnologie zur Lösung verschiedenster Problemstellungen diskutiert. Großunternehmen wie auch Startups evaluieren, wie effiziente Lösungen in einem weiten Spektrum von Themenfeldern mithilfe der Blockchain erarbeitet werden können. In diesem Kontext hat sich die Bundesregierung das Ziel gesetzt, eine umfassende Blockchain-Strategie zu erarbeiten und dafür Expertenmeinungen im Rahmen einer Online-Konsultation[1] eingeholt. Auch das FZI Forschungszentrum Informatik hat sich an diesem Konsultationsaufruf sowohl direkt, als auch im Rahmen einer gemeinsamen Erklärung des Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom), beteiligt. Im Folgenden stellen wir die Position des FZI im Bezug auf ausgewählte Fragen der Bundesregierung dar. Der Fokus lag dabei insbesondere auf dem Thema IT-Sicherheit.

1 Relevanz der Blockchain-Technologie

Zum Thema „Relevanz der Blockchain-Technologie“ bat die Bundesregierung um eine generelle Stellungnahme.

Position des FZI:
Mithilfe der Blockchain-Technologie lässt sich ein dezentraler Datenspeicher realisieren, der die Unveränderlichkeit der dort abgelegten Daten garantiert, selbst wenn einem Teil der Nutzer des Systems misstraut wird. Diese Garantien kommen jedoch mit einem Preis, der, je nach System, mit Strom, Rechenzeit oder dem Einsatz von finanziellen Ressourcen erbracht werden muss. Unveränderlichkeit und Korrektheit sind dabei nicht für alle Datenarten gleichermaßen erreichbar: nur für Daten, deren Korrektheit von anderen Nutzern des Systems verifiziert werden können, lassen sich diese Eigenschaften garantieren.

Der digitale Wandel ist für die deutsche Wirtschaft unbestritten ein essentieller Schritt, um in Zukunft wettbewerbsfähig zu bleiben. Ein Vielzahl der dabei auftretenden Herausforderungen lassen sich jedoch nicht durch einen unveränderlichen, dezentralen Datenspeicher lösen. Private Unternehmen und öffentliche Einrichtungen stehen vielmehr häufig vor Herausforderungen, die bereits durch existierende Technologien oder Verfahren, wie verteilte Datenbanken und kryptographische Signaturen, effizient und kostengünstig bewältigt werden können. Das Wissen um den korrekten Einsatz dieser Technologien fehlt jedoch häufig in Unternehmen, deren Kerngeschäft nicht die Entwicklung von Software-Produkten oder IT-Dienstleistungen ist. Zudem ist die Bewertung von blockchain-basierten Lösungen im Vergleich zu ausgereiften Digitalisierungslösungen häufig nur für Experten möglich. In vielen Anwendungsfällen stellen sich, insbesondere an der Schnittstelle zur realen Welt, außerdem weitere nicht-technische Herausforderungen, die mit keiner Digitalisierungsstrategie gelöst werden können. Teilnehmer einer Blockchain müssen in der Lage sein, die dort abgelegten Daten hinsichtlich ihrer Korrektheit zu prüfen. Handelt es sich dabei um Daten mit Bezug zu physischen Objekten kann das unmöglich sein. So lassen sich beispielsweise Informationen aus Lieferketten sicher und unveränderlich in einer Blockchain speichern. Der Nachweis, dass Daten korrekt eingetragen wurden, lässt sich aber nur durch organisatorische Maßnahmen erbringen, da nur anhand der eingetragenen Daten unmöglich zu erkennen ist, welches Produkt tatsächlich verpackt wurde.

Neben der Erforschung der Potentiale der Blockchain-Technologie ist es daher nach unserer Auffassung mindestens gleichermaßen wichtig den Einsatz von modernen Digialisierungslösungen, die ohne Einsatz von Blockchain-Technologie auskommen, zu fördern.

2 Funktionsweise der Blockchain

Zum Thema „Funktionsweise, Anwendungen, Potenziale“ bat die Bundesregierung um Stellungnahme zu ihrer Darstellung der Kernfunktionalitäten der Blockchain.

Position des FZI:
Blockchain-Kerntechnologien und deren Anwendungen weisen eine hohe fachliche Komplexität auf, die selbst von Experten häufig nicht durchschaut werden kann. Daher ist uns sehr daran gelegen, die technologischen Grundlagen präzise darzustellen.

In diesem Abschnitt finden sich einige inhaltliche Ungenauigkeiten und falsche Informationen:

- Viele der Grundideen der Blockchain-Technologie wurden bereits deutlich vor 2008 veröffentlicht (Stuart Haber, W. Scott Stornetta: How to Time-Stamp a Digital Document, Ross J. Anderson: The Eternity Service, Bruce Schneier, John Kelsey: Cryptographic Support for Secure Logs on Untrusted Machines). Die meisten technologischen Grundlagen, wie Hashfunktionen und Signaturen sind sogar noch älter. Der Wesentliche Beitrag von Satoshi Nakamoto ist die Integration der unterschiedlichen Technologien im Rahmen der Anwendung Bitcoin.

- Der Abschnitt zu Verschlüsselung ist irreführend und technisch nicht korrekt. Verschlüsselung ist ein fest definierter Begriff, der Verfahren bezeichnet, die zur Herstellung von Vertraulichkeit geeignet sind. Vertraulichkeit ist üblicherweise aber kein Ziel von Blockchains und Verschlüsselung kommt daher in der Regel nicht zum Einsatz. Die Transaktionsdaten in einer Blockchain sind nicht verschlüsselt, da Teilnehmer ihre Korrektheit ansonsten nicht verifizieren können. Die verwendeten kryptographischen Mechanismen sind in der Regel nur dafür gedacht, Transaktionen transparent und nachvollziehbar zu machen, jedoch nicht dafür die Identität der Akteure zu verbergen. Die Verwendung eines öffentlichen Schlüssels ist, genau wie die Verwendung einer Kontonummer, kein geeigneter Mechanismus zum Schutz von Identitäten. Die meisten Blockchains bieten ihren Nutzern daher nur eine pseudonyme Nutzung, die nicht mit einer anonymen Nutzung verwechselt werden darf.

- Bei „Proof-of-Stake“ werden immer Nutzer ausgewählt, die einen Anteil an der zugrunde liegenden Kryptowährung haben. Ein rein zufällige Auswahl unter allein Teilnehmern des Netzwerks würde die Sicherheit der Blockchain gefährden. Richtig wäre daher, dass Teilnehmer auf Basis ihres Anteils und nach einem Zufallsprinzip ausgewählt werden.

3 Anwendungsfeld Finanzsektor

Zum Thema „Finanzsektor“ stellte die Bundesregierung unterschiedliche Fragen im Zusammenhang mit Kryptowährungen, Tokens, Initial Coin Offerings und Kapitalmarktrecht.

Das FZI antwortet auf die Frage „Welche Missbrauchsrisiken bestehen? Welche Risiken bestehen für Kleinanleger?“:
Anleger, die in emittierte Tokens oder Coins von Kryptowährungen investieren, kaufen ein Versprechen darauf in Zukunft eine digitale Dienstleistung in Anspruch zu nehmen, die meist keinen gesicherten physischen Gegenwert hat. Es handelt sich daher um reine Spekulationsobjekte, die, im Gegensatz zu Aktien, nicht an den Erfolg des emittierenden Unternehmens gekoppelt sind. Wie auch bei Gutscheinen ist eine Wertsteigerung rein spekulativ. Zudem ist der Markt für Blockchain-basierte Finanzprodukte nicht reguliert und bietet damit ein großes Risiko für Betrug.

4 Technologische Herausforderungen im Bezug zu IT-Sicherheit

Zum Thema „Technologische Herausforderungen im Bezug zu IT-Sicherheit“ stellte die Bundesregierung unterschiedliche Fragen im Zusammenhang mit dem Betrieb und Einsatz von Blockchains.

Das FZI antwortet auf die Frage „Welche Anforderungen an die IT-Sicherheit eines Blockchain-Systems stellen technologiebedingt eine besondere Herausforderung dar?“:
Der korrekte Einsatz von kryptographischen Mechanismen ist selbst für Experten schwierig. Die Blockchain vereint eine Vielzahl solcher Mechanismen. Bereits kleine Fehler in der Anwendung eines einzelnen Mechanismus können jedoch zu dem vollständigen Verlust der Sicherheit des Gesamtsystems führen. Im Fall der Blockchain ist das besonders kritisch, da jeder Teilnehmer die gleiche Client-Software verwenden muss und die Sicherheit des Netzwerks daher davon abhängt, dass diese keine Fehler enthält. Ähnlich verhält es sich auch mit Smart Contracts, die automatisch bei allen Teilnehmern ausgeführt werden. Hier sind Sicherheitslücken besonders fatal.

Das ist insbesondere vor dem Hintergrund, dass die Blockchain noch in ihren Kinderschuhen steckt und dementsprechend hochvolatil ist, besorgniserregend. Sicherheitskritische Kernkomponenten erfahren regelmäßig tiefgreifende Änderungen und besitzen nicht den gleichen Reifegrad im Hinblick auf Code-Qualität und durchgeführter Security-Audits, wie sicherheitsrelevante Komponenten anderer Technologien (wie beispielsweise OpenSSL), die flächendeckend im Einsatz sind. Zur Sicherheit eines Produktes gehören weiterhin auch immer operative Aspekte, wie strukturierte Entwicklungs- und Review-Prozesse, Produktpflege, sowie ein definierter Prozess zum Umgang mit Sicherheitslücken. Die meist jungen

Unternehmen, die im Kontext von Blockchain-Technologie tätig sind, besitzen keine gleichermaßen ausgereifte Prozesse des IT-Sicherheitsmanagements, wie auf dem Markt etablierte Unternehmen. Diese und weitere IT-Sicherheitsaspekte der Blockchain-Technologie sind aktuell Gegenstand einer von uns im Auftrag des BSI durchgeführten Studie.

Eine besondere Herausforderung stellt sich außerdem hinsichtlich des Sicherheitsziels der Unveränderlichkeit. Unveränderlichkeit ist nur erreichbar, wenn eine kritische Menge ehrlicher Teilnehmer des Netzwerks aktiv Transaktionen verifizieren. Populäre Anwendungen, wie beispielsweise Ethereum, erreichen diese kritische Menge zur Zeit, jedoch ist es nicht vorherzusagen, ob das in Zukunft auch weiterhin der Fall sein wird. Beispielsweise liegt die Hoheit der Rechenkapazität von Bitcoin bereits jetzt schon zu einem großen Teil in China. Daten, die heute in einem blockchain-basierten, unveränderlicher Datenspeicher abgelegt werden, können daher in Zukunft möglicherweise doch verändert werden. Diese Herausforderungen muss beim Einsatz dieser Technologie stets berücksichtigt werden.

Das FZI antwortet auf die Frage „Sollte es eine Sicherheitszertifizierung für Blockchain-Produkte geben?“:
Unserer Auffassung nach sind Sicherheitszertifizierungen grundsätzlich positiv zu bewerten. Für eine Vielzahl von Technologien, die jetzt schon flächendeckend im Einsatz sind, ist keine Sicherheitszertifizierung vorhanden.

5 Rechtliche Fragestellungen zum Datenschutz

Zum Thema „Rechtliche Fragestellungen zum Datenschutz (insbesondere Anforderungen nach der DSGVO)“ stellte die Bundesregierung mehrere Fragen. Der Einleitungstext befasste sich mit den Datenschutzproblemen beim Einsatz von öffentlichen oder privaten Blockchains.

Position des FZI:
Zwei der wesentlichen Entwurfsziele der Blockchain-Technologie sind Transparenz und Unveränderlichkeit. Transparenz ermöglicht es den Teilnehmern, innerhalb bestimmter Grenzen, zu Überprüfen, ob die eingetragenen Daten korrekt sind. Unveränderlichkeit unterscheidet die Blockchain von einer konventionellen verteilten Datenbank. Diese beiden Entwurfsziele sind unvereinbar mit wesentlichen Zielen des Datenschutzrechts. Die Datenschutzgrundverordnung definiert weitreichende Löschrechte und -pflichten, die in einem unveränderlichen Datenspeicher nicht erfüllt werden können. Die Speicherung von sensiblen Daten “off-chain” kann geeignet sein das Problem zu umgehen, jedoch ist das nur unter substantieller Einschränkung der Transparenz möglich. Daten, die “off-chain” gespeichert werden, können nicht in die Prüfung der Korrektheit im Rahmen des Konsenzverfahrens einbezogen werden. Die Vorteile der Blockchain gegenüber dem Einsatz von konventionellen verteilten Datenbanken ist dann nicht mehr offensichtlich zu erkennen.

Darüber hinaus, wirft die dezentrale Organisation öffentlicher Blockchains im internationalen Kontext die weitreichende Fragestellung auf, wer datenschutzrechtlich als Verantwortlicher i.S.d. Art. 4 Nr. 7 DS-GVO zu qualifizieren ist. Danach bemisst sich auch der räumliche Anwendungsbereich der DS-GVO. Art. 26 DS-GVO ermöglicht die gemeinsame Verantwortlichkeit derjenigen, die über Zwecke und Mittel der Verarbeitung entscheiden. Sofern dies für alle am Netzwerk Teilnehmenden gilt, wären folglich alle Verantwortliche. Gleichzeitig erschwert die pseudonyme Teilnahme die zweifelsfreie Identifikation ohne i.d.R. die Schwelle datenschutzrechtlicher Anonymisierung zu erreichen, welche zur Nichtanwendbarkeit des Datenschutzrechts führen würde. Die DS-GVO ist folglich auf öffentliche Blockchains wie Bitcoin, Ethereum usw. anwendbar. Obgleich eines der wesentlichen Entwurfsziele der Blockchain-Technologie in der Transparenz liegt, werden die Transparenzanforderungen der DS-GVO verletzt, wenn die Informationspflichten nicht erfüllt werden. Auskunfts- und Berichtigungsansprüche sind in Art. 8 Abs. 2 EU-Grundrechtecharta bereits auf grundrechtlicher Ebene verbürgt. Auch hierfür bedürfte es eines Ansprechpartners für betroffene Personen. Eine Reduktion der Verpflichtungen sieht Art. 11 Abs. 2 DS-GVO lediglich dann vor, wenn der Verantwortliche nachweisen kann, dass er/sie nicht in der Lage ist die betroffene Person zu identifizieren. Ob eine hinreichende Anonymisierung identifizierender Daten in einer Blockchain durchgängig möglich ist, erscheint aufgrund der Transparenz und Unveränderlichkeit zweifelhaft. Ob eine Identifizierbarkeit gegeben ist, bemisst sich nach objektiven Faktoren wie den Kosten und dem erforderlichen Zeitaufwand unter Berücksichtigung der verfügbaren Technologie und technologischen Entwicklung und erfordert somit eine regelmäßige Risikobewertung. Durch die Verkettung von Daten steigt grundsätzlich auch die Wahrscheinlichkeit einer Identifizierbarkeit. Sofern die Zuordnung einer natürlichen Person zu einem Datensatz in der Blockchain persistiert wird, kann die Speicherung weiterer (ggf. sensibler) personenbezogener Daten „off-chain“ das Risiko für die Grundrechte und Grundfreiheiten der betroffenen Personen senken, jedoch nicht zur Unanwendbarkeit der DS-GVO führen.

Fußnote

[1] https://www.blockchain-strategie.de/BC/Navigation/DE/Home/home.html (zuletzt aufgerufen: 20.05.2019)

IMPRESSUM

FZI Forschungszentrum Informatik

Haid-und-Neu-Str. 10–14
76131 Karlsruhe
www.fzi.de

Vorstand

Prof. Dr. Andreas Oberweis
Jan Wiesenberger
Prof. Dr.-Ing. J. Marius Zöllner

Vorsitzender des Kuratoriums:
Ministerialdirigent Günther Leßnerkraus

Gestaltung, Layout und Satz

Communications (COM), FZI

Druck

Erscheinungsdatum 31.05.2019

Hinweis: Aus Gründen der einfacheren Lesbarkeit wird in dieser Publikation nur die männliche Form verwendet. Es sind jedoch stets Personen männlichen und weiblichen Geschlechts gleichermaßen gemeint.

Kompetenzzentrum
IT-Sicherheit