Marc Lenze / Jonas Müller

/// Der Wert und Nutzen von Daten

Die Blockchain-Technologie in der Verwaltung

Personenbezogene Daten sind seit einiger Zeit fester Bestandteil des gesellschaftlichen Diskurses. Mit der zunehmenden Verlagerung privater wie beruflicher Lebenswelten ins Digitale gewinnen die Daten des Einzelnen immer mehr an Wert und provozieren die Frage nach der Verantwortlichkeit für ihren Schutz.

Einführung

Neue Technologien bieten die Möglichkeit, der steigenden Gefahr digitalen Datenmissbrauchs entgegenzuwirken, und bergen gleichzeitig das Potenzial, komplexe Prozesse für den Bürger einfacher zu gestalten. Die Technologien befähigen den Staat, als schützende Instanz einzuschreiten und eine Umgebung zu erzeugen, die es dem Bürger erlaubt, sich frei von Sorgen im Internet zu bewegen. Das World Wide Web unterzieht sich aktuell dabei einem essenziellen Wandel: vom Speicher reiner Information zum Ort monetärer und materieller Geltung – zum Internet der Werte.

Vom Internet der Informationen hin zum Internet der Werte.

Das Internet der Werte und die damit verbundenen Chancen des sicheren digitalen Austauschs werden durch die Blockchain-Technologie ermöglicht.[1] Ihre Verwendung birgt das Potenzial, jedem Bürger die volle Kontrolle über die Verwendung seiner Daten zu geben, und gewährleistet darüber hinaus die Integrität, Authentizität, Anonymität und Verfügbarkeit der Daten zu jedem Zeitpunkt.

Wie auch das Phänomen der sogenannten Künstlichen Intelligenz und der Robotik, so ist auch die Blockchain-Technologie bisher nur in vereinzelten Pilotprojekten, kleineren Teststrecken oder abgeschlossenen Bereichen realisiert. Auch wenn diese wie die erwähnten technologischen Entwicklungen häufig mit dem Label „disruptiv" bezeichnet werden, so gilt jedoch für die Blockchain-Technologie besonders, dass es sich dabei um einen langsam sich fortentwickelnden, evolutorischen Prozess handelt.

Der vorliegende Beitrag versucht daher die Vorteile, Chancen und Risiken der Blockchain-Technologie anzuführen und den Mehrwert für den Bürger und für die öffentliche Verwaltung in Deutschland herauszuarbeiten.

Die Blockchain-Technologie

Im World Wide Web existiert keine Instanz, die es global kontrollieren kann.

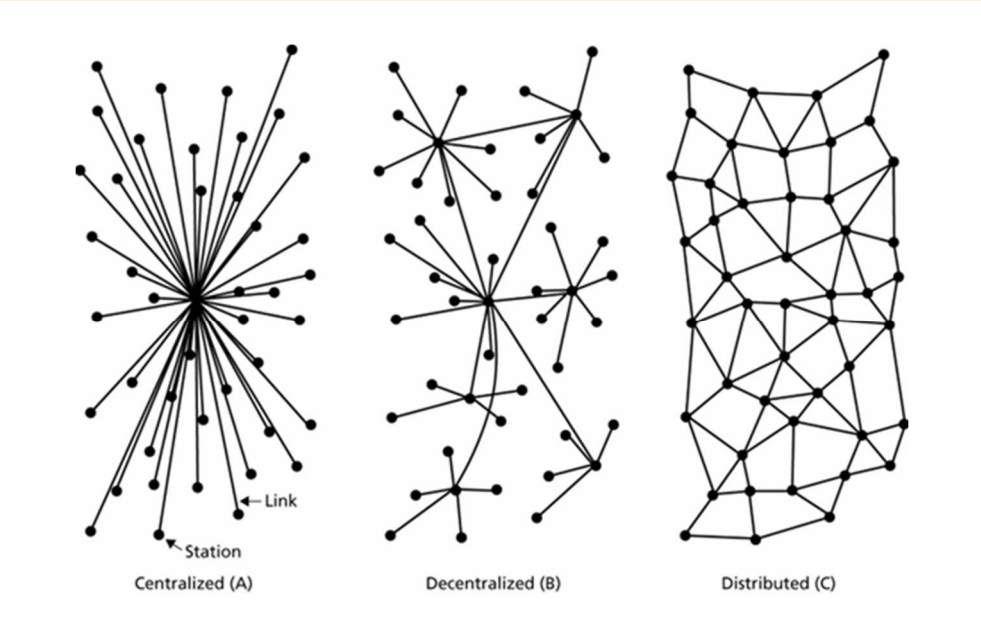
Grundlage des World Wide Web bzw. des Internets ist eine dezentrale Maschentopologie, in der aktive Netzwerkkomponenten das Routing, also den Transport der jeweiligen Datenpakete, übernehmen. Dieses sogenannte Mesh-Net ist in sich selbst dezentral ausgelegt. D. h. beim Ausfall einer Verbindung stehen im Regelfall alternative Routen zur Verfügung, um den Datenverkehr unterbrechungsfrei fortführen zu können. Global betrachtet gibt es keine zentrale Instanz, die das Internet kontrollieren oder es außer Betrieb setzen kann.[2]

Wie in Abbildung 1 zu sehen, sind dezentralisierte Netze allerdings genauso denkbar wie zentralisierte und verteilte Netze. Die Abbildung verdeutlicht, dass dezentralisierte und zentralisierte Systeme eine hohe Abhängigkeit von einem oder mehreren Akteuren beinhalten. Dennoch sind dezentralisierte und zentralisierte Netze aktuell die wichtigsten und verbreitetsten Softwarearchitekturen. Die hohe Abhängigkeit der beiden Systeme birgt jedoch zwei Probleme:

- Die (Haupt-)Akteure tragen enorme Verantwortung und müssen einen hohen Aufwand für die Koordination und die Kommunikation innerhalb des Netzes betreiben.

- Wenn sich eine Gruppe von dezentral verantwortlichen Akteuren entscheidet, nicht mehr im Sinne aller zu handeln, und stattdessen ausschließlich eigene Interessen verfolgt, gibt es so gut wie keine Möglichkeit für die restlichen Akteure, etwas dagegen zu unternehmen. Der Missbrauch von Daten durch unseriöse Akteure kann somit nur bedingt verhindert werden.[3]

Abbildung 1: Zentralisierte, dezentralisierte und verteilte Netze[4]



Im Vergleich dazu hebt sich eine verteilte, dezentrale Softwarearchitektur (engl. distributed ledger) dadurch hervor, dass diese aus einer großen Anzahl unabhängiger Knoten bzw. Akteure besteht, die „miteinander über ein Kommunikationsmedium kooperieren, um ein bestimmtes Ziel zu erreichen, ohne dass dabei ein zentralisiertes Element zur Kontrolle oder zur Koordinierung zum Einsatz kommt“.[5]

Es ist somit im Gegensatz zu dezentralisierten und zentralisierten Netzen nahezu unmöglich, dass in verteilten Softwarearchitekturen die Integrität der Daten(-bank) zerstört wird bzw. verloren geht.

Eine bereits etablierte, verteilte Softwarearchitektur ist aktuell die sogenannte Blockchain-Peer-to-Peer-Technologie. Im Vergleich zu allen bisherigen Softwarearchitekturen hat die Blockchain es geschafft, grundlegende Probleme für den Datenaustausch in einem verteilten Netz ohne zentrale Instanz(en) zu lösen.[6]

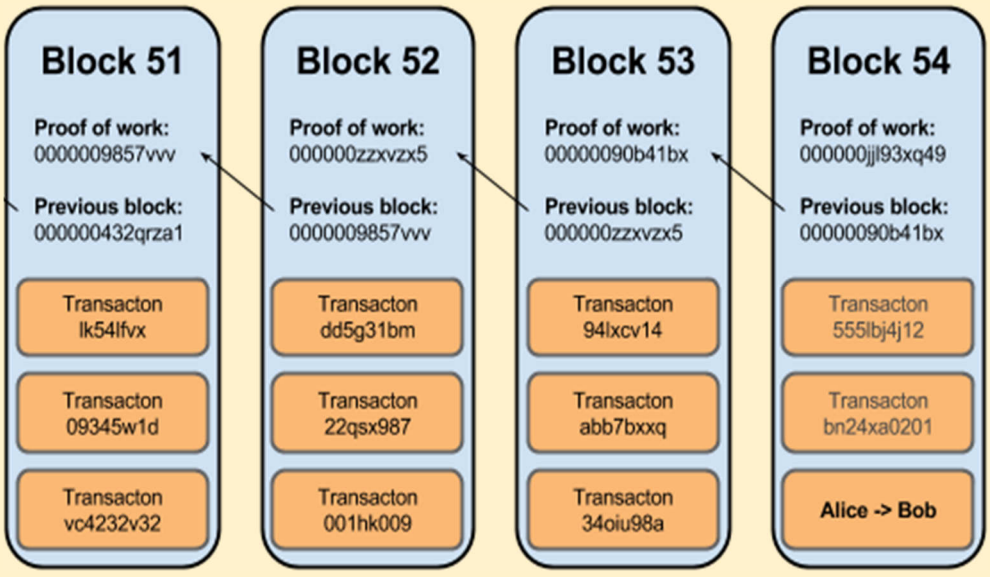
Grundlagen der Blockchain-Technologie

Maximal abstrahiert ist eine Blockchain eine komplexe Verknüpfung von verschiedenen Hash-Werten. Ein Hash-Wert wird häufig auch als „Fingerprint“ bezeichnet, da er eine nahezu eindeutige Kennzeichnung einer Datenmenge darstellen kann. Jeder Hash-Wert repräsentiert entweder einen Block oder eine Transaktion. In jedem Block befindet sich eine gewisse Anzahl an Transaktionen, welche ebenfalls miteinander verhasht worden sind (siehe Abb. 2).

Die Art und Weise, wie besagte Blöcke erzeugt werden, welche Transaktionen für den jeweiligen Block ausgewählt werden und wie festgelegt wird, welcher Block als nächster (valider) Block an die Kette der bereits vorhandenen Blöcke „angeheftet“ wird, ist abhängig von der jeweils vorab definierten Adaption der Blockchain-Technologie und der Wahl des entsprechenden Konsensus-Algorithmus.

Dieser Algorithmus ist das Besondere, das technologisch Revolutionäre, denn dieser verhindert das sog. Double Spending. Es wird somit gewährleistet, dass eine einzigartige Transaktion nicht mehrfach in die einzelnen Blöcke geschrieben werden kann.[7]

Abbildung 2: Illustration der Grundlagen der Blockchain-Technologie[8]



Die Relevanz von Double Spending lässt sich am Beispiel des Bitcoins verdeutlichen. Jeder im System vorhandene Bitcoin ist eindeutig einer (verschlüsselten) digitalen Brieftasche, Wallet genannt, zugeordnet. Wenn beispielsweise eine Transaktion zum Transfer eines Bitcoins von Wallet A zu Wallet B durchgeführt wird, dann muss das System sicherstellen, dass Wallet A den Bitcoin nach der Transaktion nicht mehr besitzt und dieser eindeutig und nur in der digitalen Brieftasche von B liegt. Ließe sich dies nicht verhindern, dann könnte Wallet A mit dem gleichen Bitcoin mehrfache Transaktionen durchführen und den Wert zweimal gegen z. B. Waren tauschen. Allgemein formuliert wäre es dementsprechend möglich, mit dem gleichen Euro zweimal etwas zu kaufen, obwohl man bei dem ersten Kauf den Euro schon gegen die Ware getauscht hat.[9]

Sichergestellt wird die Verhinderung von Double Spending u. a. durch asymmetrische Kryptografie in Form einer speziellen Schlüsselcharakteristik: Das Public-Key-Verschlüsselungsverfahren mit digitaler Signatur macht es unmöglich, zwei Datensätze bzw. Transaktionen zu erzeugen, die die gleiche Signatur (bzw. Hash-Wert-Kombination) enthalten, aber nicht von der gleichen Person (d. h. also nicht mit dem gleichen privaten Schlüssel) erzeugt worden sind. So sichert das System unter anderem Integrität, Authentizität, Anonymität und Verfügbarkeit.[10] Besagte Begriffe werden im Folgenden tiefergehend erläutert.

Nur der Besitzer eines privaten Schlüssels kann den dazu passenden öffentlichen Schlüssel erzeugen.

Die grundlegenden Vorteile der Blockchain-Technologie

Integrität: Die Integrität der Daten wird durch die Verwendung von Hash-Funktionen gewährleistet, welche kryptografisch einen einmaligen Wert der Datensätze / Transaktionen erzeugen. Bei einer potenziellen Veränderung der Datensätze verändert sich auch automatisch deren Hash-Wert, was eindeutig auf eine Manipulation der Daten hinweist.[11]

Authentizität: Die Basis jeder Blockchain-Transaktion bilden auf Basis von asymmetrischer Kryptografie erzeugte digitale Signaturen. Es ist für jede im Netzwerk befindliche Entität eindeutig, wer welche Transaktion signiert hat, da einzig der Besitzer eines bestimmten privaten Schlüssels einen spezifischen / korrespondierenden öffentlichen Schlüssel erzeugen kann.[12]

Anonymität: Grundsätzlich kann, bei oberflächlicher Betrachtung, die „Basis"-Blockchain-Technologie zunächst als pseudoanonym eingestuft werden, da ein öffentlicher Schlüssel immer Rückschlüsse auf einen privaten Schlüssel enthalten muss und somit theoretische Querverbindungen zu genau einer privaten-Schlüssel-Adresse erstellt werden können.[13]

Verfügbarkeit: Die verteilte Softwarearchitektur sorgt dafür, dass auf jedem Knoten (siehe Abb. 1) des Netzwerks zu jeder Zeit alle Transaktionen der gesamten Blockchain-Historie liegen. Es ist somit bis zu einem hohen Grad an Netzausfällen die Verfügbarkeit der Datensätze gewährleistet. Dies wird unter anderem dadurch sichergestellt, dass alle Knoten zu jeder Zeit im Austausch miteinander stehen und gemeinschaftlich entschieden wird, welche Datensätze / Transaktionen in die Blockchain aufgenommen werden.

Nutzen und Wert der Blockchain-Technologie

Die Frage nach dem Nutzen der Blockchain-Technologie muss für jeden Einzelfall neu bewertet werden.

Der Nutzen sowie der Wert der Technologie liegen im einzelnen Anwendungsfall. Faktoren wie Integrität, Authentizität, Anonymität und Verfügbarkeit können zwar als allgemeine Vorteile betrachtet werden, dies ist aber nur zutreffend, sofern der konkrete Anwendungsfall diese Vorteile auch braucht. Grundsätzlich muss somit die Frage nach dem Wert bzw. dem Nutzen der Blockchain-Technologie immer einzeln pro Szenario, Prozess und Anwendungsfall betrachtet sowie bewertet werden.

Die Blockchain-Technologie im Kontext der DSGVO

Die am 25. Mai 2018 eingeführte europäische Datenschutz-Grundverordnung (DSGVO) basiert auf einer zentralisierten Betrachtung der digitalen Welt. Jegliche dezentrale bzw. verteilte Softwarearchitekturen sind im Kern nicht betrachtet worden und müssen aktuell im Einzelnen bewertet werden.[14]

Die grundsätzlichen Fragen im Kontext der DSGVO sind u. a.:

- Können persönliche Daten auf einer Blockchain überhaupt anonym sein?
- Wer kontrolliert die Daten?
- Wer verarbeitet und validiert die Daten?

Eine grundsätzliche Antwort auf diese Fragen gibt es aktuell für die Blockchain-Technologie nicht. Allerdings existiert innerhalb der einzelnen Paragrafen bewusst ein gewisser Interpretationsspielraum für den jeweiligen Einzelfall. So ist z. B. innerhalb des Paragrafen 17 (Recht auf Vergessen) definiert, dass der Verantwortliche „unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen“[15] treffen muss, um die Daten zu löschen. An dieser Stelle sei darauf hingewiesen, dass die Blockchain häufig als reines Transaktionsmodell verwendet wird, in dem die Originaldokumente gar nicht gespeichert werden, sondern lediglich ihre Hash-Werte.

Gerade bei dem mit der Verwendung der Blockchain-Technologie verbundenen hohen Aufwand, um (zumindest theoretisch) ältere, mit persönlichen Daten in Verbindung zu bringende Transaktionen zu löschen, könnte im Einzelfall von dem Recht auf Löschung abgerückt werden, da der Aufwand bzw. die Kosten nicht in Relation zum Recht auf Löschung stehen. Der Punkt der Datenlöschung im Paragrafen 17 ist demnach nicht als ein absolutes Recht zu definieren und obliegt einer Einzelfallbetrachtung.[16]

Vergleichbare Argumente lassen sich auch für die anderen DSGVO-Paragrafen anführen. Demnach lässt sich durchaus eine Kompatibilität der Blockchain-Technologie mit der DSGVO annehmen.[17]

Dies wird zusätzlich durch die Tatsache unterstützt, dass es derzeit viele technologische Entwicklungen im Bereich Blockchain gibt, um der DSGVO, gerade im Hinblick auf die Verwendung von persönlichen Daten (anonym versus pseudoanonym), gerecht zu werden.[18] Kern dieser Lösungsansätze ist u. a. die kryptografische Zero-Knowledge-Proof-Methode, welche es mathematisch ermöglicht, dass der Einzelne sich im Netz authentifiziert, ohne persönliche Daten freigeben zu müssen.[19]

Bei der Zero-Knowledge-Proof-Methode kann man sich authentifizieren, ohne persönliche Daten freizugeben.

Vorteile, die sich aus diesen Methoden ergeben, sind letztendlich der Schutz von sensitiven personenbezogenen Daten – vor allem unter der Betrachtung aus IT-Sicherheitsperspektive –, denn staatliche Einrichtungen, Behörden und Verwaltungen sind stets interessante Ziele für Hackerangriffe.[20]

Hierzu gibt es bereits mehrere technologisch fortgeschrittene Projekte, welche die Blockchain-Technologie mit den Regularien der DSGVO verbinden. Dies gilt sowohl für den Bereich der Transaktionsübermittelung[21] als auch für den Bereich Computation (Datenverarbeitung).[22]

Blockchain in der öffentlichen Verwaltung

Der Alltag der Bürger in der öffentlichen Verwaltung ist zusehends geprägt von immer komplexer werdenden und vielschichtigen Prozessen.

Die Vorteile dieser Prozesse sind für beide Seiten meist schwer zu erkennen und die folgerichtige Frustration führt zu Bestrebungen, einen Großteil der Prozesse zu digitalisieren und zu automatisieren, um so z. B. dem Bürger die Möglichkeit zu geben, viele Vorgänge künftig online erledigen zu können. Die Kehrseite der Digitalisierung: der gefühlte Verlust der Hoheit über die eigenen Daten. Kein Bürger kann sicherstellen, was mit seinen personenbezogenen Daten online geschieht und wofür diese letztendlich verwendet werden.[23]

Lösungsansatz Blockchain

Die Blockchain-Technologie bietet dem Bürger eine bessere Steuerung seiner personenbezogenen Daten.

Aufbauend auf der bereits vorhandenen dezentralen Struktur des Internets bietet die Blockchain-Technologie die Möglichkeit sicherzustellen, was mit den Daten des einzelnen Bürgers zu welcher Zeit geschieht. Der Bürger kann selbst entscheiden, welcher Instanz (oder Person) er für welchen Zweck bzw. Zeitraum persönliche Informationen zur Verfügung stellt. Dies betrifft sowohl den Bereich der reinen Informations- / Transaktionsübermittelung (z. B. Identifikation zum Zugriff auf eine Bürgerplattform der Kommune) als auch die Verarbeitung der persönlichen Daten wie Steuer- oder Rentendaten. Als erfolgreiches Beispiel für die gerade geschilderten Punkte lässt sich die Digitalisierung Estlands anführen.[24]

Blockchain-Technologien haben in den vergangenen Jahren, in der Phase ihres technologischen Reifeprozesses, gezeigt, dass unterschiedlich sinnvolle Anwendungsfälle zur Verbesserung verschiedener Prozessstrukturen identifiziert werden können. Die bekanntesten Beispiele dabei kommen aus der Finanzbranche, Supply Chain Management, Health Care etc.[25]

Komplexe Prozesse werden sich auch in Zukunft grundsätzlich nicht immer vermeiden lassen. Betrachtet man allerdings die Anwendung von Blockchain-Technologien innerhalb der im Abschnitt zuvor genannten Bereiche und in bereits laufenden Pilotprojekten (z. B. das Projekt des Bundesamt für Migration und Flüchtlinge zur Unterstützung der Zusammenarbeit im Asylprozess[26]), ist schnell erkennbar, dass vorhandene Prozesse teilweise auf ein Minimum reduziert werden können.[27]

Um die Herausforderungen vorhandener Prozessstrukturen innerhalb von Bürgerprozessen mittels Blockchain-Technologie zu minimieren, ist es zunächst notwendig, die Eigenschaften der spezifischen Prozessausprägungen zu betrachten. Dabei spielt vor allem die Thematik der Identität und das generelle Identitätsmanagement eine essenzielle Rolle, besonders auch im Kontext der DSGVO. In Verwaltungsprozessen dienen Identitäten als Grundlage für jegliche Registrations- und Anmeldeprozesse (z. B. Gewerbeanmeldung, Kfz-Anmeldung etc.). Bürgerbezogene Prozesse basieren somit auf individuellen Personendaten und müssen mit den Regularien der DSGVO stets vereinbar gestaltet werden. Betrachtet man die Geschichte und die Ziele der Blockchain[28] sowie die Ziele der Datenschutzgrundverordnung[29], lässt sich erkennen, dass beide Instanzen im Kern das gleiche Ziel verfolgen (nämlich die Rechte von Personen zu schützen), sich jedoch oberflächlich betrachtet zunächst widersprechen.

Vorteile Blockchain-basierter Kommunikation

Grundsätzlich lässt sich sagen, dass Blockchain-basierte Verwaltungsprozesse / -applikationen die Authentifizierung von Identitäten sowie Identitätsdokumenten transparent, sicher und effektiver als traditionelle Prozesse gestalten können. Dabei ist die Möglichkeit der Veränderung vor allem von der Unterstützung und der treibendenden Kraft der entsprechenden staatlichen Behörden abhängig.[30] Der Fokus liegt dabei nicht nur auf dem Sicherstellen von Vertrauen zwischen den einzelnen Behörden, sondern auch auf dem Etablieren einer Vertrauensbasis zwischen Behörde und Bürger. Die Behörde muss dem Bürger das Vertrauen in den Mehrwert der Blockchain-basierten Lösung und die damit einhergehende Steigerung des Schutzes der persönlichen Daten des Einzelnen vermitteln.

Der Kernnutzen muss in der Verschlankung der Prozesse und in der Minimierung des Aufwands liegen.

Neben dem essenziellen Faktor des Vertrauens des Bürgers (und der öffentlichen Verwaltung) in die Technologie muss der Kernnutzen einer solchen Blockchain-Applikation in der Verschlankung bisheriger Prozesse und dem Minimieren des Aufwands liegen (Prozessvereinfachung und Prozessbeschleunigung). Dies gilt sowohl auf Bürger- als auch auf Behördenseite.

Anwendungsfälle in der öffentlichen Verwaltung

Allgemein mögliche Anwendungsmöglichkeiten in der öffentlichen Verwaltung könnten z. B. der Einsatz in Bezug auf Grundbücher oder Patente, der Austausch von Dokumenten, Rechnungen oder die Identitätsprüfung bis hin zur Prüfung von Bürgerkonten sein.

Darüber hinaus wäre auch eine auf Blockchain basierende „Vernetzung“ staatlicher (Kommunen, Land, Bund, EU, Justiz, Polizei), nicht-staatlicher Einrichtungen (Parteien, Presse, NGOs) und Bürgern möglich. Dies würde für alle Beteiligten größtmögliche Transparenz über den Ursprung und die Nutzung von Daten bedeuten. Jegliche Zugriffe und ggf. durchgeführte Änderungen wären für jeden Berechtigten nachvollziehbar und bedürfen der Zustimmung der jeweils berechtigten Parteien. Die Originaldokumente müssten ihre heutige Umgebung nicht verlassen, wenn zwischen den einzelnen Parteien vorab die Authentizität bestätigt worden ist. Die Unabhängigkeit der einzelnen staatlichen Instanzen bliebe somit gewahrt.

Ausblick

Die Technologie soll dem Bürger Sicherheit über seine Daten und Transparenz über deren Verwendung geben.

Die Verwendung der Blockchain-Technologie kann das Vertrauen in Staat und Politik des einzelnen Bürgers festigen. Vertrauen ist ein entscheidender Faktor der allgemeinen Bürgerzufriedenheit, welche die Basis für ein friedliches gesellschaftliches Miteinander ist. Eine Technologie, welche dem Bürger und dem Staat die Sicherheit über ihre Daten und zugleich Transparenz über deren Verwendung gibt, schafft notwendiges Vertrauen auf beiden Seiten. Dies ist die Basis für die Optimierung bestehender Prozesse, offener Kommunikation und Voraussetzung für die Entwicklung und Akzeptanz neuer Anwendungen, z. B. im Kontext von Smart City bzw. Smart Country-Projekten.

MARC LENZE
Business Development
und Key-Account-Management,
Fujitsu, Düsseldorf

JONAS MÜLLER
IT-Architekt für Distributed
Ledger Technology und Blockchain,
Fujitsu, München

Anmerkungen

1 Vgl. Twesige, Richard: Bitcoin – A simple explanation of Bitcoin and Block Chain technology, o .O. 2015, S. 4.

2 Vgl. Olbrich, Alfred: Netze – Protokolle – Spezifikationen. Die Grundlagen für die erfolgreiche Praxis, Wiesbaden 2003, S. 23 ff.

3 Vgl. Drescher, Daniel: Blockchain Grundlagen. Eine Einführung in die elementaren Konzepte in 25 Schritten, Frechen 2017, S. 32 ff.

4 Baran, Paul: On distributed Communications Networks, Santa Monica 1962, S. 2.

5 Vgl. ebd., S. 37 ff.

6 Vgl. Roßbach, Peter: Blockchain-Technologien und ihre Implikationen, Frankfurt 2016, S. 4 ff.

7 Vgl. Antonopoulos, Anton M.: Bitcoin & Blockchain. Grundlagen und Programmierung, Sebastopol, 2. Aufl., 2018, S. 197 ff.

8 Vgl. https://bitcoinist.com/thoughts-bitcoin-block-size-economics/

9 Vgl. Roßbach: Blockchain-Technologien und ihre Implikationen, S. 4 ff.

10 Vgl. Antonopoulos: Bitcoin und Blockchain, S. 197 ff.

11 Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI): Blockchain sicher gestalten. Konzepte, Anforderungen, Bewertungen, Bonn 2019, S. 15 ff.

12 Vgl. ebd.

13 Vgl. Fink, Michele: Blockchain Regulation and Governance in Europe, Cambridge 2019, S. 88 ff.

14 Vgl. ebd.

15 Vgl. https://dsgvo-gesetz.de/art-17-dsgvo/

16 Vgl. Fink: Blockchain Regulation and Governance in Europe, S. 88 ff.

17 Vgl. ebd.

18 Vgl. https://www.fujitsu.com/global/about/resources/news/press-releases/2018/0514-02.html

19 Vgl. https://www.binance.vision/glossary/zero-knowledge-proofs

20 Vgl. https://www.zdnet.com/article/can-blockchain-help-fix-government-bureaucracy/

21 Vgl. https://z.cash/blog/zcash-shielded-addresses-are-gdpr-compliant-by-default/

22 Vgl. https://blog.enigma.co/

23 Vgl. https://netzpolitik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen/

24 Vgl. Sullivan, Clare / Burger, Eric: E-residency and blockchain, in: Computer Law & Security Report 4/2017, S. 470-481.

25 Vgl. https://openledger.info/insights/hyperledger-enterprise-solutions-top-5-real-use-cases/

26 Vgl. Guggenmos, Florian / Lockl, Jannik / Rieger, Alexander / Fridgen, Gilbert: Blockchain in der öffentlichen Verwaltung – Unterstützung der Zusammenarbeit im Asylprozess, in: Informatik Spektrum 3/2019, S. 174-181.

27 Vgl. ebd.

28 Vgl. Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, S. 1 ff., https://bitcoin.org/bitcoin.pdf

29 Vgl. https://dsgvo-gesetz.de/art-1-dsgvo/

30 Vgl. Sullivan / Burger: E-residency and blockchain, S. 470 ff.