2. Vertrauenswürdige Blockchains

Zusammenfassung

Eine Blockchain ist eine dezentral organisierte Datenbank, die es ermöglicht, Transaktionen zwischen Akteuren – Privatpersonen, Unternehmen und öffentliche Einrichtungen – dezentral zu dokumentieren, digital abzubilden und zu authentifizieren. Die Technologie gewährleistet, dass die Interaktionen genauso wie dokumentiert stattgefunden haben und stellt sicher, dass die Dokumentation nicht verändert werden kann. Neben den bekanntesten Anwendungen, den Kryptowährungen wie Bitcoin, werden Blockchains (auch: distributed ledger technology) zurzeit für weitere Anwendungen in Wirtschaft und Staat entwickelt: Für Eigentumsurkunden, Verträge, Versicherungen, Lizenzen etc. Blockchains haben das Potential, monopolistische Geschäftsmodelle wie Airbnb, ebay und Uber zu überwinden und AnbieterInnen und KundInnen direkt zu verbinden. Allerdings: Wenn Blockchain als Technologie allgegenwärtig werden würde, so würde damit der Lebensalltag aller BürgerInnen umfassend abgebildet und für andere im Zeitverlauf eindeutig nachvollziehbar sein. Eine personen-basierte Blockchain würde bedeuten, dass alle Handlungen im biographischen Verlauf gespeichert werden. Das Missbrauch-Potential ist damit enorm, aber bisher nicht thematisiert.

Überblick zum Thema

Die bekannteste Anwendung eines Blockchain-Algorithmus ist die Kryptowährung Bitcoin im Finanzbereich. Eine Blockchain ist eine kryptografisch verbundene Kette von Blöcken. Diese Blöcke werden in einem bestimmten Zeitintervall erstellt, enthalten Transaktionen, die die TeilnehmerInnen des Systems als ausgeführt akzeptieren, sodass z.B. ein Block bei Erhalt als akzeptiert gilt und damit die zugrundliegende Transaktion zu einem Bestandteil des Systems wird. Da alle TeilnehmerInnen eine Kopie davon besitzen, und die vorangegangenen Datensätze mit den nachfolgenden gekoppelt und gespeichert sind, gelten die Abfolge und die einzelnen Transaktionen als gesichert gegen nachträgliche Manipulation. Das Versprechen lautet, dass die Technik Vertrauen automatisieren kann und damit Instanzen überflüssig macht, die Vertrauen schaffen und dadurch Kosten verursachen. Das Disruptionspotenzial der Blockchain ergibt sich aus dem Charakter einer Peer-to-Peer-Infrastruktur, die Transaktionen ohne Intermediäre ermöglicht. Da Intermediäre im Finanzbereich eine größere Rolle als in anderen Wirtschaftsbereichen spielen, wird die Technologie in diesem Bereich am stärksten diskutiert.

Smart Contracts

Die Funktionalität von Blockchains lässt sich erweitern. Eine der vielversprechendsten Erweiterungen sind *Smart Contracts*. Diese intelligenten Verträge sind kleine Programme, die beim Zusammentreffen von bestimmten Bedingungen automatisch ausgeführt werden. Da diese Smart Contracts beliebig kompliziert sein können, die Komplexität von etablierten Verträgen damit abbilden können, gelten sie als Mittel, klassische Verträge zu ersetzen. Der Ersatz besteht in der Plattform und der Automatisierung, da die Verträge eine neue Form (digital) und einen neue Funkti-

onsweise erhalten. Doch die Sicherheit des Systems steht zur Diskussion: Der Slogan der Entwicklercommunity von Blockchains heißt: *Code is Law* und genau diese Absolutheit, dass Smart Contracts immer exakt so ausgeführt werden, wie sie geschrieben sind, hat auch bereits zu ersten Sicherheitsbedenken geführt. Denn wenn HackerInnen sich einen „Fehler" im Smart Contract zunutze machen, könnten sie das System knacken – wobei die Rechtslage komplex ist, da das nicht-intendierte Handeln der HackerInnen gerade Teil des Codes ist, dem alle NutzerInnen zugestimmt haben. In der Startup-Szene, in der viele Blockchain-Anwendungen entwickelt werden, wird das Scheitern nicht als Problem gesehen, vielmehr ist das „fail fast" ein integraler Bestandteil der Innovationskultur.[1] Für Anwendungen im öffentlichen Bereich ist dagegen eine Blockchain-Innovationsdynamik notwendig, die die möglichen Folgen umfassend antizipiert, um gerade vertrauenswürdige Anwendungen zu generieren.

Anwendungen, die in Europa thematisiert werden

Auf europäischer Ebene werden vielfältige Blockchain-Anwendungen thematisiert (vgl.Boucher et al. 2017): Neben Währungen ist die Technologie interessant für die Verwaltung von digitalen Inhalten, da sich ein entsprechendes Rechte-Management in Blockchain integrieren ließe. Im Bereich von Patenten könnte es möglich werden, über Blockchain Rechte zu verwalten. Im E-Voting sind Blockchain-unterstützte Systeme mit der Erwartung verknüpft, Mechanismen der direkten Demokratie zu vereinfachen. Blockchain-basierte Dienstleistungen im E-Government und bei der elektronischen Stimmabgabe sollen zu einer transparenteren, dezentralisierten Demokratie beitragen können.[2] Auch die britische Regierung interessiert sich für die Blockchain-Technologie in umfassendem Maße und sieht über Grundbücher hinaus Anwendung im Bereich Steuererhebung, Auszahlung von Leistungen oder auch die Sicherheit von Infrastrukturen wie Straßen und Brücken, wenn diese von Sensoren überwacht werden (Walport/Government Office for Science 2016).

Den vielfältigen Bottom-up-Prozessen der Entwicklung und Erprobung von Blockchains steht noch kein Rahmen gegenüber, der aus einer längerfristigen Zukunftsperspektive heraus und über die verschiedenen Anwendungen hinaus Design-Prinzipien zur Verfügung stellt, die es den unterschiedlichen Akteuren ermöglichen würden, den verschiedenen Anforderungen über die eigene Anwendung hinaus gerecht zu werden[3]. Dies ist jedoch essentiell, um das Potenzial der Blockchain, institutionelles Vertrauen aufzubauen, auszuschöpfen.

Relevanz des Themas für das Parlament und für Österreich

Wirtschaft

In ökonomischer Hinsicht ist die zukünftige wirtschaftliche Bedeutung des Blockchain-Sektors unklar, aber auch mögliche Nutzungsbedingungen

[1] http://www.deutschlandfunk.de/die-welt-veraendern-visionen-und-wahrheiten-aus-der.740.de.html?dram:article_id=378079.

[2] https://aeon.co/essays/how-blockchain-will-revolutionise-far-more-than-money.

[3] Wie z.B. den Schutz persönlicher Daten, vgl. Zyskind, et al. (2015).

(Nutzung der Währungen, Akzeptanz und rechtlicher Rahmen; Privatsphäre).

Währungen

Blockchain-Währungen: Es besteht hohe Unsicherheit im Hinblick auf die Zukunft des Bankensektors, international und in Österreich und im Hinblick auf den KonsumentInnen-Schutz im internationalen Feld.

Nutzen

Nutzen: Es gibt offene Fragen, wer zukünftig unter welchen Bedingungen von dieser Technologie profitieren kann und wie sie die Gesellschaft verändern kann.

Sicherheit

Sicherheit von Blockchain-Anwendungen: Wie unangreifbar sind Blockchains, welche Hacking-Risiken sind abzusehen und wie kann mit ihnen umgegangen werden kann?

Umweltpolitik

Ökologie & Energie: Auf umweltpolitischer Ebene stellt sich die Frage des Energieverbrauchs beim Mining und welche Lösungsansätze hinsichtlich Energiefragen zu verzeichnen sind

Die Blockchain-Technologie bietet umfassende Anwendungsmöglichkeiten in Wirtschaft und öffentlicher Verwaltung und hat damit eine politikfeldübergreifende Relevanz.

rechtliche Fragen

Blockchains können *disruptive Auswirkungen auf das Rechtssystem* haben und bedürfen daher einer antizipierenden Politik. Aktuelles Beispiel sind Smart Contracts: Wenn durch ProgrammiererInnen Vereinbarungen in ausführbaren Code übersetzt werden, treffen diese Entscheidungen darüber, wie diese Verträge in der Praxis umgesetzt werden, hätten eine höhere rechtliche Verantwortlichkeit und sind zugleich nicht entsprechend ausgebildet. Die Beurteilung von Vertragsstreitigkeiten und die Durchsetzung von Vertragsklauseln werden Herausforderungen darstellen, wenn sich Blockchains wie erwartet entwickeln.

Die Kompatibilität der Blockchain-Technologie zum politischen Modell Österreichs und die Frage, welche Dienstleistungen der öffentlichen Verwaltung mit der Technologie entwickelt werden könnten, ist eine politikfeldübergreifende Frage.

optimales Zeitfenster

Um einen zukunftsorientierten Rahmen für Blockchain-Technologie zu entwickeln ist zurzeit ein optimales Zeitfenster in Österreich vorhanden. Es gibt bereits eine Blockchain-Strategie[4] und ein Blockchain-Förderprogramm[5] und somit die kritische Masse an Kompetenz und Bottom-up-Entwicklungen, die für die Entwicklung eines innovations- und zukunftsorientieren Rahmens notwendig sind. Daraus ergäbe sich eine hohe Wirksamkeit von übergreifenden Maßnahmen.

Vorschlag weiteres Vorgehen

Im Rahmen einer Langstudie würde zunächst ein systematischer Überblick zu den aktuellen Anwendungsgebieten und technologischen Herausforderungen der Blockchain-Technologie erstellt werden. Dabei würden neben technischen Entwicklungen auch die bereits wissenschaftlich aus-

[4] https://www.blockchain-austria.gv.at/unser-9-punkte-plan/#c2.

[5] https://www.ffg.at/programme/smart-and-digital-services.

gewerteten Erfahrungen von Anwendungen in verschiedenen Ländern und in unterschiedlichen Branchen auf die Situation in Österreich bezogen werden. In einem weiteren Schritt würden österreichische Stakeholder aus verschiedenen Branchen, aus Verwaltung, Blockchain-AnwenderInnen und -EntwicklerInnen etc. identifiziert werden. Ziel wäre es, einen Rahmen zu entwickeln, der das in Österreich bestehende Innovationspotential umfassend und zukunftsorientiert nutzbar macht. Die aktuelle Situation verweist auf ein bereits bestehendes Know-How unterschiedlicher Akteure und bietet noch einen hohen Gestaltungsspielraum hinsichtlich der Innovationspfade von zukünftigen Blockchain-Anwendungen. Die Studie würde den möglichen Handlungsbedarf identifizieren und die Anforderungen definieren, die für die langfristige Nutzung der Blockchain-Technologie in der österreichischen Wirtschaft und Verwaltung zentral sind.

Zitierte Literatur

Boucher, P., Nascimento, S. und Kritikos, M., 2017, *How blockchain technology could change our lives*, im Auftrag von: Scientific Foresight Unit (STOA) – European Parliament.

Walport, M. und Government Office for Science, U., 2016, *Distributed ledger technology: beyond block chain*.

Zyskind, G., Nathan, O., Pentland, A. und Ieee, 2015, Decentralizing Privacy: Using Blockchain to Protect Personal Data, *2015 Ieee Security and Privacy Workshops (Spw)*, 180-184.