

Blockchains zwischen Anarchie und Governance: Steuerungsansätze für die öffentliche Verwaltung

Ralf Klischewski¹

¹ German University in Cairo, Egypt
ralf.klischewski@guc.edu.eg

Abstract. Blockchain-Technologie gilt als disruptiv, da sie potenziell völlig neue Abläufe bzw. Organisation von Leistungen ohne bisher etablierte Intermediäre ermöglicht. Dies stellt staatliche oder anderweitig politisch legitimierte Institutionen vor neue, bisher kaum diskutierte Herausforderungen an die Steuerung. Bezugnehmend auf den Stand der Bewertung von Blockchains werden Notwendigkeiten zur Steuerungsfähigkeit identifiziert und in Abhängigkeit zur technisch-organisatorischen Ausprägung der Blockchain-Anwendung und dem rechtlich legitimierten Aktionsradius der Akteure gebracht: Je stärker der Grad der Dezentralisierung von Registeranwendungen, umso mehr müssen föderierte und dezentralisierte Mechanismen der Blockchain-Governance etabliert werden und sich als effektiv erweisen. Abwägung von Vor- und Nachteilen der Technologieanwendung sowie angemessene Formen der netzwerkbasierter Steuerung gilt es zukünftig zu erforschen, im Zusammenhang mit Visionen für die Dezentralisierung der öffentlichen Verwaltung insgesamt.

Keywords: Blockchain, öffentliche Verwaltung, Anarchie, Governance, Steuerung, Dezentralisierung

1 Einleitung

Die Diskussion um Blockchains hat inzwischen auch die öffentliche Verwaltung und die sie begleitende Verwaltungsinformatik erreicht. Anwendungen dieser Technologie stehen dort noch am Anfang, und so versucht die fachspezifische und wissenschaftliche Diskussion vor allem, die Potenziale und Risiken zu analysieren und zu bewerten, um so eine fundierte Handlungsorientierung zu ermöglichen. Analysten sind sich einig, dass die Blockchain-Technologie als disruptiv einzuschätzen ist, da sie völlig neue Abläufe bzw. Organisation von Leistungen ermöglicht – und dies eben auch in der öffentlichen Verwaltung mit womöglich weitreichenden Folgen für Funktion und Selbstverständnis staatlicher Institutionen.

Über wichtige technische und anwendungsspezifische Aspekte hinaus ist die Steuerung („Governance“) der Technologieanwendung von besonderer Bedeutung, denn dies berührt die öffentliche Verwaltung in ihrem Kern: Können bzw. sollten staatliche oder anderweitig politisch legitimierte Institutionen eine Technologie fördern und einsetzen, die den legitimierten Kontrollanspruch dieser Institutionen als Intermediär tendenziell überflüssig macht? Und wenn ja, welche Technologie-

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

varianten und welche Formen der Governance sind geeignet, die öffentliche Verwaltung in der Wahrnehmung ihrer Verantwortung zu unterstützen?

Die Weiterentwicklung der Blockchain-Governance wird eingefordert (u.a. [4, 16, 17]), bisher liegen dazu aber kaum systematisch erarbeitete Ergebnisse vor. Im Folgenden wird daher zunächst der Stand der Bewertung von Blockchains in der öffentlichen Verwaltung anhand von mehreren Dimensionen zusammengefasst. Darauf aufbauend werden dann die verschiedenen Notwendigkeiten zur Steuerungsfähigkeit von Blockchain-Anwendungen identifiziert und in Abhängigkeit von beteiligten Akteuren und Technologievarianten gebracht, um so öffentliche Verwaltungen bei deren Entscheidungen zur Einführung und Anwendung von Blockchain-Technologie zu unterstützen. Der abschließende Ausblick verweist auf zukünftige Forschungsbedarfe.

2 Blockchains in der öffentlichen Verwaltung: Stand der Bewertung

Die Blockchain-Technologie ist weltweit bekannt geworden durch ihre Anwendung bei Management und Validierung von Transaktionen in der Kryptowährung Bitcoin (zu Funktion und beteiligten Akteuren siehe z.B. [2]). Doch der Anwendungsbereich der Technologie geht weit darüber hinaus: „Eine Blockchain ist also ein verteiltes, dezentrales Register, das Transaktionen in chronologischer Reihenfolge unveränderbar und nachvollziehbar speichert und miteinander verkettet. Durch eine Kombination aus kryptografischen Funktionen, verteilten Netzwerken und komplexen technischen Mechanismen erlaubt die Blockchain eine Transaktionsabsicherung, ohne dabei auf eine vertrauenswürdige dritte Instanz zurückgreifen zu müssen.“ ([19], S. 17)

Anwendungen von Blockchains in der öffentlichen Verwaltung sind bisher noch nicht weit verbreitet und eher im Experimentierstadium [12, 17], wobei international erhebliche Unterschiede bestehen. Beispielsweise wurden bei staatlichen Organisationen in Holland im April 2017 bereits 25 abgeschlossene Pilotprojekte gezählt,¹ während in Deutschland bis dato nur Absichtserklärungen kursieren. Mangels belastbarer empirischer Untersuchungen der Anwendungspraxis fokussiert sich die wissenschaftliche und fachspezifische Diskussion in erster Linie auf die Potenzialanalyse und Risikobewertung. Im Zentrum stehen dabei vor allem die Dimensionen Anwendungen in der Verwaltung, technische Infrastruktur, Risiken und Vertrauenswürdigkeit sowie Steuerung (Governance) und Beteiligung.

2.1 Anwendungspotenzial

Der potenzielle Anwendungsbereich von Blockchains in der öffentlichen Verwaltung wird in der Literatur relativ klar umrissen: „Jegliche Formen von Registern, die über eine öffentlich überprüfbare Transaktionshistorie verfügen und manipulationssicher sein müssen, sind grundsätzlich für eine Blockchain-Umsetzung geeignet. Dies können Grundbucheinträge, Personalausweise, Waffen- oder Kfz-Register, Patientenakten, Geburtsurkunden u.v.a.m. sein.“ ([4], S. 5) Etwas allgemeiner formuliert eine

¹ <https://www.blockchainpilots.nl/results> (Zugriff am 23.11.2017)

FOKUS-Studie ([19], S. 18): „Die Blockchain-Technologie setzt da an, wo derzeit zentrale Institutionen die Umsetzung von Regeln sicherstellen“, und verweist auf bereits in der Diskussion befindliche Anwendungsszenarien zu Register und Eigentumsverhältnissen, Verifikation und Bestätigung, Herkunftsnachweisen, Digitale Identitäten, Transparenz und Offenheit sowie Wahlen.

In vergleichbarer Weise wird das Anwendungspotenzial in einer verteilten und transparenten Buchführung gesehen [17], in der Aktenverwaltung generell [8] oder als dezentraler, konsensgesteuerter öffentlicher Verwahrungsort [1]. Der britischen Regierung werden z.B. Anwendungsszenarien empfohlen wie Schutz von kritischer Infrastruktur gegen Cyberattacken, Reduzierung von operationalen Kosten und Prüfung von Sozialhilfeberechtigungen, Transparenz und Nachvollziehbarkeit von öffentlichen Finanzhilfen, Stärkung von KMUs und Vermeidung von Steuerbetrug [17]. Und China hat angekündigt, dass es „die Blockchain-Technologie für die Sozialbesteuerung und für das elektronische Rechnungswesen nutzen wird“.² Auch große IT-Hersteller bauen Blockchain-Kompetenzzentren auf und implementieren Pilotprojekte (IBM z.B. für Handelsregister und Außenhandelsfinanzierung [6]).

Die Bewertung der Potenziale ist vor allem dort kontrovers, wo neue technische Möglichkeiten mit den Kernaufgaben öffentlicher Verwaltung konkurrieren: „Manipulationssichere Registerführung und Beglaubigung stellen gleichermaßen zentrale Aufgaben der Verwaltung sowie das Kernversprechen der Blockchain dar. Sie hat deshalb das Potential, die durch zentrale Organisationsparadigmen geprägte Verwaltung nachhaltig zu verändern.“ ([4], S. 6). Disruptiv ist die Technologie insofern, als sie die Rolle von vertrauensvollen Vermittlern in Frage stellt, insbesondere in Notariaten, Banken und Verwaltungsabteilungen [16, 17]. Teilweise wird dies als Chance bewertet, um Verwaltungsleistungen zukünftig persönlicher, unmittelbarer und (wirtschaftlich) effizienter erbringen zu können [17] oder um den Abbau von Transaktionskosten und die Beschneidung von Zentralstaatlichkeit zu ermöglichen [10]. Letztlich sind immer Vor- und Nachteile abzuwägen, und die Chance geraten vor allem dann in den Blick, wenn zentrale Institutionen als dysfunktional erscheinen (z.B. wg. Korruption) oder in horizontalen Netzwerken schwer zu etablieren sind (z.B. bei Lebensmittellieferketten, offene Registraturen, internationaler Zahlungsverwicklung; vgl. [15]). Von daher bleiben die meisten Analysten angesichts der Risiken (siehe 2.3) eher vorsichtig und fragend, und manche warnen sogar explizit vor dem technisch induzierten Verlust von staatlicher und ggf. auch demokratischer Kontrolle (z.B. [1], siehe 2.4).

2.2 Technisch-organisatorische Infrastruktur

Laut [19] gehören zu den wesentlichen Merkmalen einer Blockchain: verteilte redundante Datenhaltung, Änderungsresistenz (Zensurreistenz), Anreizsystem, pseudonymer Zugang, Kryptografie-basierte Sicherheit, transparente Buchhaltung, sowie ggf. Kryptowährung-basierte Abrechnung. Bei jedem Merkmal existieren mehr oder

² <http://www.z-punkt.de/de/news/item/china-blockchain-zur-steuereintreibung-und-zum-rechnungsversand/558> (Zugriff am 21.9.17)

weniger große Gestaltungsspielräume, etwa beim Grad der Dezentralisierung von verschiedenen Registertechnologien („permissioned“/„permissionless“, geschlossen/öffentlich) oder beim verwendeten Konsensmechanismus (s.u.). Entsprechend werden in der Diskussion durchaus verschiedene Aspekte hervorgehoben und unterschiedlich bewertet. So bleibt eine auf den ersten Blick plausible Beschreibung der Blockchain als „eine Datenbank mit vier besonderen Eigenschaften: ohne zentrale Instanz, öffentlich einsehbar, manipulations- und ausfallsicher“ ([4], S. 1) in keinem dieser Aspekte unhinterfragt:

- Die für das Mining in öffentlichen Blockchains erforderliche enorme Rechenkapazität wird nur in wenigen großen Rechenzentren vorgehalten (v.a. in China [1]), wobei stets das Risiko der Kartellbildung besteht. Eine vergleichbare Zentralisierung gilt für die Entwicklergruppe des Softwarekerns.
- Bei öffentlichen Blockchains ist die technische Einsicht gegeben – aber wie lange? Bisher gibt es keine Bestandsgarantien und keine Verabredungen über Langzeitarchivierung [8], und technische Veränderungen können überdies in Zukunft den Zugang behindern.
- Schutz vor Manipulation besteht nicht an sich, sondern nur durch die sehr hohe Wahrscheinlichkeit, dass Manipulationen sofort aufgedeckt würden („tamper evident“). Zudem werden auch ‚unerwünschte‘ Transaktionen abgewickelt, solange sie formal den zugrundeliegenden Konsensregeln folgen [12].
- Ausfallsicherheit lässt sich in der Praxis nicht garantieren und die Literatur (z.B. [1, 8, 19]) listet eine Reihe von Anfälligkeiten (siehe 2.3).

Doch auch wenn man auf die genannten Vorteile vertraut, immer wieder werden auch eine Reihe von unstrittigen Nachteilen erwähnt, auf deren Vermeidung sich Ansätze zur technologischen Weiterentwicklung konzentrieren: insbesondere die Komplexität der technischen Verfahren, deren Unveränderbarkeit bzw. Inflexibilität, die sich verschlechternde Performance bei zunehmender Länge der Blockchain, der immense Energieverbrauch aufgrund der erforderlichen hohen Rechenleistung (z.B. [4]). Um insbesondere Skalierung und Energieeffizienz zu verbessern, werden alternative Konsensmechanismen zum sehr aufwändigen „Proof-of-Work“ diskutiert und erprobt (z.B. „Proof of Stake“ [9]), „Bitcoin Next Generation“, „Hybrid/Bitcoin“, „Solidus“, „Spectre“ [5]). Weitere Entwicklungen zielen darauf, die Blockchain-Technologie als generelle Plattform und mögliche Serviceinfrastruktur bereitzustellen, z.B. organisiert in aufeinander aufbauenden Schichten (Anwendungen / Bitcoin oder andere Währungen / Konsensregeln, Peer-to-peer, Security / Verteilte Blockchain Datenbank [11]), vergleichbar mit dem Internet-Stack.

2.3 Risiken und Vertrauenswürdigkeit

Die Anwendung der Blockchain-Technologie scheint vielen vertrauenswürdig, gerade weil das Transaktionsprotokoll dezentralisiert und durch algorithmische Berechnung („trust-by-computation“, vgl. [1]) abgesichert wird. Übereinstimmend wird konstatiert, dass die Blockchain durch ihre Transparenz eine hohe Fälschungssicherheit bietet und gerade das Fehlen eines zentralen Betreibers gegen eine Vielzahl

klassischer Angriffsmethoden schützt (z.B. [19]). Jedoch ist auch die Blockchain-Technologie in vielfacher Hinsicht angreifbar, wobei die meisten Risiken steigen, je mehr die Blockchain dezentralisiert, unbeschränkt und öffentlich einsehbar ist:

- **Individuelles Sicherheitsmanagement:** Jeder Nutzer muss seine privaten Schlüssel selbst verwalten und schützen. Angreifer, die in Besitz von privaten Schlüssel gelangen können dann Transaktionen signieren und im Fall einer Kryptowährung auch Geld stehlen [8, 19].
- **Kontrolle der Mining-Rechenleistung:** „In aktuellen Blockchain-Netzwerken geht man von der Annahme aus, dass die Mehrheit der Rechenleistung vertrauenswürdig ist. Schafft es ein Angreifer, mehr als die Hälfte der Rechenleistung unter seine Kontrolle zu bringen, kann er statistisch betrachtet langfristig eigene Transaktionen in der Blockchain bestätigen.“ ([19], S. 26) Angreifer (z.B. Betreiber von Botnetzen) müssen über eine große Rechenleistung verfügen. Und da der Aufwand mit der Größe des Netzwerks steigt, sind vor allem kleinere Blockchain-Netzwerke anfällig für diese Angriffe.
- **Sicherheitslücken im Code:** Ein Beispiel hierfür ist der 2016 erfolgte Angriff auf eine Ethereum-Blockchain, der in Ausnutzung eines Bugs der Blockchain-Software 3,6 Millionen Einheiten der Kryptowährung Ethereum aus dem Crowdfunding-Projekt DAO abzweigte.³
- **Sybil-Attacken:** Wenn es einem Angreifer gelingt, genügend Knoten in einem Blockchain-Netzwerk zu kontrollieren, kann er die Weitergabe von Blöcken und Transaktionen verweigern, den Eintrag von Registrierung vom Netzwerk abtrennen und ggf. eigen Blöcke einfügen. Die Wahrscheinlichkeit dieser Art von Angriff nimmt mit wachsender Konzentration von Minern zu [8].
- **Zeitstempelfehler:** die Funktion und Verlässlichkeit der Blockchain hängt wesentlich von der exakten Zeiterfassung ab. Ein Angreifer könnte die Zeitschalter einzelner Knoten manipulieren oder die Aufzeichnung der Transaktionsreihenfolge durch falsche Zeitangaben mittels selbst kontrollierter Knoten stören [8].
- **Denial-of-Service-Attacken:** Angreifer können das Blockchain-Netzwerk mit massenhaften Kleinsttransaktionen oder Synchronisierungsanfragen überfluteten, so dass es für andere Teilnehmer bzw. für legitime Transaktionen nicht mehr nutzbar ist [8, 19].
- **Unzuverlässigkeit:** Registereinträge werden nur formal geprüft, aber nicht sachlich, d.h. aus Verwaltungssicht gibt es erstmal keinen Schutz vor fehlerhaften und unautorisierten Einträgen. Werden Einträge von sogenannten vertrauensvollen Vermittlern vorgenommen, stellt sich auch dort die Frage nach deren Zuverlässigkeit [8].
- **Inflexibilität:** Die Dezentralisierung erhöht die Resilienz des Informationssystems insgesamt, allerdings um den Preis, dass die einmal unter verbindlichen Regeln gestarteten Prozesse im weiteren Verlauf nicht oder nur mit unverhältnismäßig hohem Aufwand geändert werden können [1]. Damit werden das Schließen von Sicher-

³ <https://www.heise.de/newsticker/meldung/Nach-dem-DAO-Hack-Verbliebenes-Kryptogeld-mit-freundlichem-Hack-gesichert-3246539.html>

heitslücken und auch die Anpassung von verwaltungstechnischen Abläufen erheblich erschwert.

- **Fragliche Dauerhaftigkeit:** Bislang gibt es keine verbindlichen Standards, wie lange Blockchains und die von Nutzern vorgenommenen Einträge vorzuhalten bzw. zu archivieren sind [8]. Wird die Anwendung von Blockchain-Technologie mittels Plattformen im Rahmen einer mehrschichtigen Infrastruktur vorgenommen [11], steigen auch die Risiken der technischen Diskontinuität.
- **Systemische „Selbsterstörung“:** das technisch-organisatorische System kann schnell an seine immanenten Grenzen stoßen, wenn die Profitabilität der Miner erodiert, die enormen Investitionen in die Hashing-Infrastruktur sich nicht mehr lohnen, die Netzwerkneutralität nicht mehr (hinreichend) gegeben ist, ein Mangel an Controlling-Daten besteht und (dadurch ggf. irrationale) Erwartungen der Investoren nicht befriedigt werden [1].

In diesem Abschnitt wurde vornehmlich auf technische und systemische Aspekte der Blockchain-Anwendung eingegangen. Für eine umfassende Risikobewertung greift dies jedoch zu kurz, denn die Verwaltung hat „in zentralen Vorgängen die Rolle des vertrauenswürdigen, neutralen Intermediärs inne“, der bei der Abwicklung komplexer Vorgänge auf ein gewachsenes Arsenal an Instrumenten wie Urkunden, Siegel, notariell beglaubigte Abschriften, Zeugnisse, Zertifikate, Durchschläge usw. zurückgreifen kann ([4], S. 6) Auf weitere Aspekte bezüglich staatlicher Verantwortung, Recht, Verfahrenssicherheit, Personal, Staat-Bürger-Verhältnis kann an dieser Stelle nicht näher eingegangen werden (siehe dazu Abschnitt 4.).

2.4 Governance und Beteiligung

Die Literatur zur Steuerungsfähigkeit von IT-Anwendungen ist vor allem englischsprachig geprägt, weshalb im Folgenden der Begriff Governance verwendet wird. Im Kern geht es dabei um folgende Fragen: Welche Entscheidungen sind zu treffen? Wer sollte diese Entscheidungen treffen? Wie sind diese Entscheidungen zu erreichen? Mit welchem Ablauf werden die Ergebnisse überprüft? Dies gilt auch für den IT-Bereich: “IT governance is specifying the decisions, rights, and accountability framework to encourage desirable behavior in the use of IT.” ([18], siehe auch [13], S. 5)

Die öffentliche Hand hat stets versucht, bei der IT-Governance mit neuen Technologien und Anwendungen Schritt zu halten. Die technische und organisatorische Dezentralisierung der Blockchain-Anwendung bringt jedoch in mehrfacher Hinsicht neue Herausforderungen mit sich:

- **Kontrolle von Blockchains:** „Klassische Regulierungsmechanismen stoßen an ihre Grenzen, wenn Ansprechpartner und Verantwortlichkeiten fehlen. In der Diskussion um die Blockchain wird daher oft von Regulierungsresistenz gesprochen.“ ([4], S. 24) Doch auch in Blockchain-Netzwerken gibt es Schlüsselrollen wie Miner, Händler und Softwareentwickler. Jedoch agieren diese i.d.R. global, was eine nationalstaatliche Regulierung erheblich erschwert [1].
- **Rechtsvorschriften versus Rechenvorschriften:** Rechtsvorschriften sind ‘extrinsisch’, d.h. die Regeln können gebrochen werden, aber die daraus folgenden

Konsequenzen gewährleisten wiederum die Einhaltung der Regeln. Technische Rechenvorschriften dagegen sind ‘intrinsisch’, d.h. bei Verletzung der Regeln erfolgt eine Fehlermeldung und keine weitere Aktion wird ausgeführt. Die Ordnungsmäßigkeit wird also nur durch die Ausführung der Rechenvorschriften selbst gewährleistet [17]. Die Implementierung geht davon aus, dass die Ausführung der Rechenvorschriften stets aktiv ist und alle Regelungsbedarfe abdeckt – aber sobald dies mal nicht der Fall ist, fehlen oft etablierte bzw. akzeptierte Mechanismen zur Ausnahmebehandlung.⁴

- **Kodierung der Blockchain-Regeln:** Bei IT-Anwendungen übernimmt der Gesetzgeber i.d.R. die Regulierung und überlässt deren Einhaltung der privatwirtschaftlichen Governance. Genauso wie Rechtsvorschriften müssen auch Rechenvorschriften geschaffen, implementiert und weiterentwickelt werden – von Menschen, die letztlich die von Rechenvorschriften verkörperten Regeln definieren [17]. Bislang liegt die Governance der Code-Entwicklung ad hoc in den Händen weniger Kernentwickler, und belastbare Mechanismen zur kollektiven Entscheidungsfindung und zur Handhabung von Konflikten sind nicht in Sicht.

Dezentralisierung bedeutet aber nicht Demokratisierung im Sinne von Beteiligung. Aus den Händen von vertrauensvollen Vermittlern werden Verwaltungsvorgänge im Rahmen der Blockchain-Anwendung an die verteilte „Vertrauensmaschine“⁵ übertragen. Manche (z.B. [10]) sehen darin die Chance, das Konzept der Zentralstaatlichkeit zu überdenken und den Leviathan zu dezentralisieren. Doch das revolutionäre Potenzial der Netzwerk-Governance kann dabei nicht ausgeschöpft werden, und z.B. Atzori [1] argumentiert, dass die egalitäre Blockchain-basierte Gesellschaft ein Mythos ist, insbesondere bei Anwendung von offenen und nicht zulassungsbeschränkten („unpermissioned“) Blockchains:

- die beteiligten Individuen agieren als Nutzer, aber nicht als Bürger auf der Grundlage eines Gesellschaftsvertrages,
- ein technisch vermittelter Konsens löst keine Konflikte (z.B. Interessenkonflikte, Übertretung von Normen, unethisches Verhalten),
- der Ersatz von Rechts- durch Rechenvorschriften droht so die notwendige Gewaltenteilung und die Balance von Bürgerrechten und Staatsmacht zu verschleiern,
- letztlich dominiert die Marktlogik über grundlegende öffentlichen Leistungen und Bürgerrechte, die eigentlich vor jeder Art Spekulation geschützt sein sollten,
- die Abhängigkeit von Netzwerken privater Oligarchien (z.B. Miner-Kartellen) ist wahrscheinlich und in Ansätzen bereits erkennbar,
- eine dominante Technoelite entsteht, mit wachsenden Überwachungsvollmachten über strategische Leistungen auf globaler Ebene, ohne formale Legitimation.

Wie andere neue Technologien vorher birgt die Blockchain ein großes Potenzial zur Disintermediation. Allerdings, die erforderliche technisch-organisatorische Umge-

⁴ Siehe z.B. <https://blockchainhub.net/blockchain-governance/>

⁵ <https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>

bung („ecosystem“) ist charakterisiert durch eine Vielzahl von Akteuren und gewinnorientierten Unternehmen mit großen Asymmetrien zwischen Entwicklern und Nutzern hinsichtlich Information und Einfluss. Unter diesen Randbedingungen wird sich mitnichten Anarchie einstellen, und die egalitären Hoffnungen einiger Blockchain-Befürworter erscheinen vor diesem Hintergrund unrealistisch (vgl. [1, 16]). Wird nicht weiter eingegriffen, erscheint am Horizont vielmehr die Dystopie der Entmachtung des Bürgers in einer unpolitischen staatenlosen Globalgesellschaft, beherrscht von Technokratie und im Hintergrund agierenden Blockchain-Governance-Oligarchien.

3 Entwicklung der Steuerungsfähigkeit

Die Fähigkeit oder das Vermögen („capability“) zur Governance einer neuen Technologieanwendung kann nicht einfach voraus gesetzt werden, sondern bedarf insbesondere dann der gezielten Entwicklung, wenn Technologie als disruptiv eingeschätzt wird und somit grundsätzlichen neuen Herausforderungen in der Anwendung zu begegnen ist. Seit einer Reihe von Jahren werden auch in der Verwaltungsinformatik die Potenziale der dezentralisierten Leistungserbringung diskutiert sowie die notwendigen Fähigkeiten zu Orchestrierung und Netzwerkmanagement, um alle Beteiligten zusammenzubringen und gemeinsam Probleme zu lösen (z.B. [7, 13]).

In [14] werden die Fähigkeiten zur IT-Governance definiert als Verbindung von Qualifikationen und den notwendigen Kapazitäten einer Organisation, um so den maximalen Nutzen ihrer IT im gegebenen Kontext zu erreichen. Die oftmals propagierten strukturellen, prozeduralen, und relationalen Mechanismen [18, 20] werden in [14] jeweils kombiniert zu sog. Patterns zusammengefasst und im Hinblick auf die öffentliche Verwaltung als mögliche zentralisierte, föderierte und dezentralisierte Strukturen unterschieden. Ausgehend von einer Vision des öffentlichen Nutzens, den Quellen der Legitimität und Unterstützung sowie dem erforderlichen Leistungsvermögen (intern oder in Koproduktion) kann eine öffentliche Organisation dann jeweils Kontext, Ziele, Akteure, Prozesse und erforderliche Ressourcen spezifizieren.

Um den o.g. Herausforderungen (2.4) angemessen zu begegnen, können hier nur erste Ansätze der Entwicklung von Fähigkeiten zur Blockchain-Governance durch die öffentliche Verwaltung skizziert werden. Dafür werden die jeweiligen Herausforderungen zunächst kontrastiert mit bisher erkennbaren möglichen Zielen bzw. angestrebten öffentlichen Nutzen sowie beispielhaft dafür geeigneten Prozessen (siehe Tabelle 1). Ohne Anspruch auf Vollständigkeit und Validierung soll hier vor allem verdeutlicht werden, wie notwendig die genaue Analyse der Herausforderungen ist und wie unterschiedlich dann die Steuerungsbedarfe und -prozesse sind bzw. sein müssen, um sich jeweils angemessen auf die neuen Entwicklungen einzustellen.

Dabei sind jeweils alle Akteure zu beteiligen, die bei der Blockchain-Anwendung eine wichtige Rolle spielen bzw. diese schon im Vorfeld beeinflussen: Regulierungsbehörden, Fachbehörden, Nutzer (bzw. deren Vertreter), Blockchain-Initiatoren bzw. Projektmanager, Miner, Softwareentwickler, ggf. Händler oder andere Vermittler bei der Front/End-Nutzung der Blockchain. Die Governance-Strukturen und dazugehörigen

Tabelle 1. Ansätze zur Blockchain-Governance

Herausforderung	Ziele der öffentlichen Hand	Governance-Prozesse
<i>Kontrolle von Blockchains</i>	Etablierung von Regulierungsmechanismen, die die Umsetzung von vereinbarten Rechtsvorschriften im jeweiligen Anwendungsbereich gewährleisten	KPI-basierte Messung von Blockchain-Verlauf und -leistung, Servicelevel-Vereinbarungen, Schiedsgerichtsbarkeit
<i>Rechtsvorschriften versus Rechenvorschriften</i>	Absicherung der Blockchain-Anwendungen jenseits der Rechenvorschriften im Hinblick auf Ausnahmebehandlung, Ausfallsicherheit, Managementversagen, Nachhaltigkeit u.a.	Periodische Risikoanalysen, Vereinbarungen zur Schadensabwendung und -minderung, Mediation
<i>Kodierung der Blockchain-Regeln</i>	Etablierung von kollektiven und legitimierten Mechanismen zur fortlaufenden Qualitätssicherung von beim Blockchain-Betrieb eingesetzter Software	Standardisierung von Requirements und Infrastrukturkomponenten, Zulassung bzw. Zertifizierung, Code-Inspektion

Kommunikationsprozesse können bzw. müssen dabei jeweils verschiedenen Typen (gemäß [14]) folgen, abhängig von der technisch-organisatorischen Ausprägung der Blockchain-Anwendung und dem rechtlich legitimierten Aktionsradius der Akteure:

- *Zentralisiert*: Blockchain ist geschlossen und zulassungsbeschränkt, alle Akteure sind Teil der öffentlichen Verwaltung → formale Prozesse für Kommunikation und Koordination basieren auf existierenden Organisationshierarchien und ggf. neu zu schaffenden Gremien (Lenkungsausschuss, Verwaltungseinheit)
- *Föderiert*: Blockchain ist offen einsehbar, aber zulassungsbeschränkt, alle Akteure sind Teil derselben Rechtseinheit (z.B. Nationalstaat, EU) → erforderlich sind zusätzlich Prozesse für Konfliktmanagement zwischen allen Beteiligten sowie semi-formale Prozesse für horizontale Kommunikation und Koordination
- *Dezentralisiert*: Blockchain ist offen und nicht zulassungsbeschränkt, Akteure agieren global → erforderlich sind zusätzlich Prozesse für Peer-Voting, wechselseitiges Vertrauensmanagement, und Peer-Review

Die Identifikation von Governance-Strukturen und -Prozessen in Abhängigkeit von Technologievarianten und dem rechtlich legitimierten Aktionsradius der Akteure lässt sich auch umkehren, um daraus Handlungsanweisungen für die öffentliche Verwaltung zu generieren:

- In Anlehnung an existierende Rahmenwerke (z.B. [13]) ließe sich z.B. ein „Blockchain Governance Improvement Framework“ erstellen, das die Ausweitung der notwendigen Governance-Fähigkeiten in mehreren Stufen von (meist schon

vorhandenen) zentralisierten Praktiken über föderale bis hin zu dezentralisierten Praktiken organisiert und somit den beteiligten Organisationen sowohl eine Selbsteinschätzung als auch einen Ausblick auf Best Practice ermöglicht.

- Die Selbsteinschätzung der eigenen Governance-Fähigkeiten erlaubt den in der Verantwortung stehenden Institutionen, jeweils über das für sie vertretbare zulässige Ausmaß der Dezentralisierung (Offenheit, Unbeschränktheit) von Blockchain-Anwendungen zu entscheiden – gemäß der Maxime: was nicht steuerbar ist, darf auch nicht für Erbringung öffentlicher bzw. rechtlich verbindlicher Leistungen eingesetzt werden.

Dies sind nur erste Ansätze, wie die öffentliche Verwaltung Fähigkeiten zur Blockchain-Governance herausbilden und auf der Basis der Selbsteinschätzung dieser Entwicklung entsprechend über Einsatz und Förderung der Technologieanwendung entscheiden kann. Der Handlungsbedarf zum Thema Blockchain-Governance ist von allen Akteuren unbestritten, und die bis dato noch geringe Zahl wissenschaftlicher Veröffentlichungen zeigt, dass auch der Forschungsbedarf noch groß ist.

4 Ausblick und Forschungsbedarf

Um zu gewährleisten, dass die Blockchain-Technologie im Einsatz robust und skalierbar ist, müssen wir die ethischen und sozialen Auswirkungen und die (finanziellen) Kosten und Nutzen verstehen (vgl. [17]). Notwendig ist aus Sicht der öffentlichen Verwaltung zu klären, wie der auf Disintermediation abzielende Einsatz in seinen Vor- und Nachteilen abgewogen und wie er gesteuert werden kann und sollte. Daher wurde eingangs gefragt: Können bzw. sollten staatliche oder anderweitig politisch legitimierte Institutionen eine Technologie fördern und einsetzen, die den legitimierten Kontrollanspruch dieser Institutionen als Intermediär tendenziell überflüssig macht? Und wenn ja, welche Technologievarianten und welche Formen der Governance sind geeignet, die öffentliche Verwaltung in der Wahrnehmung ihrer Verantwortung zu unterstützen?

Nachdem der Stand der Bewertung analysiert und Entwicklung der Steuerungsfähigkeit im Ansatz ausgelotet wurde, lassen sich erste Antworten darauf wie folgt zusammenfassen: Im Sinne der Dezentralisierung von Leistungen der öffentlichen Hand kann der Einsatz von Blockchains sich in ausgewählten Bereichen durchaus als sinnvoll erweisen, sofern angemessene Governance-Mechanismen Prozesse und Ergebnisse der Leistungserbringung nachhaltig absichern und die Verantwortung des Staates und Beteiligung seiner Bürger weiterhin ausgeübt werden können. Welche Technologievarianten und welche Formen der Governance dabei tatsächlich zum Einsatz kommen, sollte abhängig von den Governance-Fähigkeiten der legitimierten Kontrollinstitutionen entschieden werden: je stärker Grad der Dezentralisierung der verschiedenen Registeranwendungen, umso mehr müssen föderierte und dezentralisierte Mechanismen der Blockchain-Governance etabliert werden und sich als effektiv erweisen.

Dass mit der Dezentralisierung der Technologie auch die Dezentralisierung der IT-Governance einhergeht, dem muss auch die öffentliche Verwaltung ins Auge sehen

und sich entsprechend darauf vorbereiten. Ein vom World Economic Forum veröffentlichter Report [16] zur Verwaltung von Blockchains und Kryptowährungen erteilt den Bemühungen um (einzel-)staatliche Regulierung eine klare Absage und propagiert stattdessen ausschließlich dezentrale und netzwerkbasierte Herangehensweisen („stewardship“). Zu diesem Zweck werden zusätzlich zu den oben genannten auch noch weitere Akteure identifiziert (Innovatoren, Risikoanleger, Banken und Finanzdienstleister, Akademiker, Nichtregierungsorganisationen), die sich in insgesamt acht verschiedenen Netzwerken engagieren sollen, um aus verschiedenen Perspektiven und Interessen heraus das technisch-organisatorische Umfeld auszugestalten (u.a. Vereinbarung von Steuerungsmechanismen, Standardisierung, Anwaltschaft, Strategie und Monitoring, Gewährleistung, Wissensmanagement). Welche Akteure sich dazu in welchen Netzwerken mit welchen Zielen engagieren sollten und wie die Umsetzung der Ziele erreicht werden kann, ist eine der wesentlichen Fragen für Praxis und Forschung. Zu empfehlen ist, dass sich dabei internationale Fachorganisationen gerade im Bereich Rechnungswesen (z.B. CIPFA, IFAC) um die Weiterentwicklung ihrer Governance-Empfehlungen für die öffentliche Hand [3] bemühen.

Zu erwarten ist auch eine Ausdifferenzierung der Technologie in Richtung Plattform- und Service-Infrastruktur [11] mit jeweils wählbaren Technologievarianten. Damit einhergehen muss dann auch die Differenzierung der Governance-Mechanismen, und so werden in [16] z.B. drei Ebenen der Blockchain-Governance unterschieden: Plattform (insbes. Blockchain-Protokolle), Anwendung (z.B. Smart Contracts), technisch-organisatorisches Umfeld insgesamt („ecosystem“). Welche Formen der Governance (oder „Patterns“ [14], s.o.) für welche Ebene angemessen sind und sich als effektiv erweisen, ist ein weiteres Thema für die zukünftige Forschung.

Diverse Aspekte der Zentralstaatlichkeit werden schon länger durch technische Vernetzung und damit einhergehende horizontale Organisations- und Kommunikationsformen in Frage gestellt (z.B. öffentlich-private Partnerschaften, Verwaltungsportale, Interoperabilität, kooperative Leistungserstellung, E-Partizipation). Eine Forschungsagenda zur Blockchain-Technologie im Rahmen von Verwaltungswissenschaft und Verwaltungsinformatik sollte deshalb das der Technologie innewohnende Potenzial zur Disintermediation in den Kontext bereits erfolgter Disruptionen stellen: Das Internet hat radikal neue Möglichkeiten der Bürgerinformation geschaffen, Mobiltechnologie und Sozialen Medien ermöglichen völlig neue Formen der Bürgerkommunikation, und die Blockchain-Technologie öffnet nun ganz neue Formen der Transaktion. In diesem Spannungsfeld von (befürchteter?) Anarchie und (traditioneller) Steuerung muss die öffentliche Verwaltung zunächst ihre eigenen Visionen für die Dezentralisierung entwickeln – in einem Diskurs, der möglichst viele Akteure einbezieht und den die Verwaltungsinformatik befördern sollte.

Literatur

1. Atzori, M.: Blockchain Technology and Decentralized Governance: Is the State Still Necessary? (Last revised: June 13, 2016), <http://dx.doi.org/10.2139/ssrn.2709713>
2. Böhme, R., Christin, N., Edelman, B., Moore, T.: Bitcoin: economics, technology, and governance. *J. Econ. Perspect.* 29(2), 213–238 (2015)

3. CIPFA and IFAC: International Framework: Good Governance in the public sector. International Federation of Accountants and The Chartered Institute of Public Finance & Accountancy (2014); <http://www.cipfa.org/policy-and-guidance/standards/international-framework-good-governance-in-the-public-sector>
4. Dapp, M., Balta, D., Krcmar, H.: Blockchain – Disruption der öffentlichen Verwaltung? Eine Technologie zur Neugestaltung der Verwaltungsprozesse. Analysen & Argumente, Ausgabe 258, Konrad-Adenauer-Stiftung, Berlin (2017)
5. Eyal, I.: Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities. *Computer* 50(9), 38–49 (2017)
6. IBM Point of View: Implementierung elektronischer Handelsregister auf Basis Blockchain Technologie. IBM Corporation (2016)
7. Janssen, M., Estevez, E.: Lean government and platform-based governance—Doing more with less. *Government Information Quarterly* 30, S1–S8 (2013)
8. Lemieux, V.L.: Trusting records: is Blockchain technology the answer? *Records Management Journal* 26(2), 110–139 (2016)
9. Li, W., Andreina, S., Bohli, J.-M., Karame, G.: Securing proof-of-stake blockchain protocols. In: J. Garcia-Alfaro et al. (Eds.): DPM/CBT 2017, Springer LNCS 10436, pp. 297–315 (2017)
10. Müller, P., Proske, N.: Thomas Hobbes und die Blockchain. In: *eGovernment Computing*, 29.06.16, www.egovernment-computing.de/thomas-hobbes-und-die-blockchain-a-540331/ (Zugriff am 18.09.2017)
11. Ølnes, S., Jansen, A.: Blockchain Technology as a Support Infrastructure in e-Government. In M. Janssen et al. (Eds.): EGOV 2017, LNCS 10428, pp. 215–227 (2017)
12. Ølnes, S., Ubacht, J., Janssen, M.: Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly* 34 (3), 355-364 (2017)
13. Pardo, T.A., Burke, G.B.: IT Governance Capability: Laying the foundation for government interoperability. Center for Technology in Government, University at Albany (2009)
14. Rychkova, I., Zdravkovic, J.: Towards Decentralized IT Governance in the Public Sector: A Capability-oriented Approach. In: Rusu, L., Viscusi, G. (eds.): *Information Technology Governance in Public Organizations – Theory and Practice*, Springer, pp. 107–132 (2017)
15. Staples, M., Chen, S., Falamaki, S., Ponomarev, A., Rimba, P., Tran, A. B., Weber, I., Xu, X., Zhu, J.: Risks and opportunities for systems using blockchain and smart contracts. *Data61 (CSIRO)*, Sydney (2017)
16. Tapscott, D., Tapscott, A.: Realizing the Potential of Blockchain. A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies. World Economic Forum, 2017, http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf (Zugriff am 26.09.2017)
17. Walport, M.: Distributed Ledger Technology – beyond block chain. UK Government Office for Science, London, http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (Zugriff am 18.09.2017)
18. Weill, P., Ross, J.W.: *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business School Press. Boston (2004)
19. Welzel, C., Eckert, K.-P., Kirstein, F., Jacumeit, V.: *Mythos Blockchain: Herausforderung für den öffentlichen Sektor*. Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS, Berlin (2017)
20. Winkler, T.: IT Governance Mechanisms and Administration/IT Alignment in the Public Sector: A Conceptual Model and Case Validation. *Proc. Wirtschaftsinformatik*, 53 (2013)