

Universität Leipzig

Institut für Informatik

Seminar: Gesellschaftliche Strukturen im Digitalen Wandel

Prof. Dr. Hans Gert Gräbe

# Das digitale Rathaus- Smart Contracts in der Verwaltungsinformatik

Thees Burfeind

Digital Humanities

[tb79bedo@studserv.uni-leipzig.de](mailto:tb79bedo@studserv.uni-leipzig.de)

3700947

## Inhaltsverzeichnis

<b>1. EINLEITUNG .....</b>	<b>3</b>
<b>2. BEGRIFFLICHKEITEN .....</b>	<b>4</b>
2.1 BLOCKCHAIN .....	4
2.2 SMART CONTRACT .....	5
2.3 ÖFFENTLICHE VERWALTUNG / VERWALTUNGSHANDELN .....	6
2.4 VERWALTUNGSINFORMATIK .....	6
<b>3. SMART CONTRACTS ZUR UNTERSTÜTZUNG VON VERWALTUNGSVORGÄNGEN.....</b>	<b>6</b>
3.1 ALLGEMEINES .....	6
3.2 DIE ROLLE DER BLOCKCHAIN .....	8
3.3 ZENTRAL VERSUS DEZENTRAL.....	8
3.4 EINE FRAGE DER (TECHNISCHEN) SICHERHEIT.....	9
<b>4. VERANSCHAULICHUNG DES EINSATZES ANHAND PRAKTISCHER BEISPIELE .....</b>	<b>11</b>
4.1 SMART CONTRACTS IM PATENTAMT .....	11
4.2 TRANSAKTIONEN VON IMMOBILIEN MITTELS SMART CONTRACT .....	12
4.3 SMART CONTRACTS IM FINANZAMT.....	15
4.4 SMART CONTRACTS UND DIE WAHLEN VON MORGEN .....	16
<b>5. UMSETZBARKEIT UND RECHTSFRAGEN .....</b>	<b>18</b>
<b>6. FAZIT.....</b>	<b>19</b>
<b>LITERATURVERZEICHNIS .....</b>	<b>20</b>
<b>ONLINEQUELLEN.....</b>	<b>22</b>

## 1. Einleitung

Die deutsche Verwaltungslandschaft befindet sich seit einigen Jahren im Umbruch. Das Thema der Digitalisierung wandelt sich zunehmend von einer theoretischen und vorsatzgeprägten Richtungsangabe zu einem praktischen und umsetzungsorientierten Projekt. Nichtsdestotrotz bietet der derzeitige Stand noch einiges an Aufholbedarf. Sinkende Budgets bei wachsenden Aufgabenfeldern drängen immer mehr auf Antworten aus dem Bereich der Informatik, ebenso die langen Wartezeiten in den Bürgerämtern. Das Internet mit all seinen Möglichkeiten zeigt sich vielversprechend, aber besonders der Sicherheitsaspekt stellt große Hürden auf dem Weg in ein digitales Deutschland.

Auf der anderen Seite: Blockchain, „the next big thing“. Spätestens seit dem explosionshaften Aufstieg von Bitcoin und Co. ist alle Welt daran interessiert, Start-Ups schießen förmlich aus dem Boden, „Hauptsache Blockchain“ ist die Devise. Die Erwartungen in die Technologie sind hoch und entsprechend optimistisch sind viele der Visionen. Während manche in ihr schon die Zukunft einer globalen Gesellschaft sehen, losgelöst von Autoritäten und einzig durch den kollektiven Konsens einer Blockchain bestimmt, gibt es jedoch auch solche, die eine Gefahr für die freiheitliche Gesellschaft sehen, indem Staaten und Institutionen die Blockchain als sichere Bank für Überwachungsdaten und Kontrollmechanismen gegen die Bevölkerung verwenden. Doch das ist wohl vorerst Science-Fiction. Fakt ist, dass blockchaingeschützte Technologien vor allem eines unbedingt garantieren: Integrität und Sicherheit. Ein Grund, weshalb das Thema auch zunehmend in den Fokus der Verwaltungsinformatik rückt. Hier verspricht man sich Lösungen für die Probleme der Digitalisierung, die mit verfügbarer Technologie nicht hinreichend zu beheben sind. Dabei gewinnt auch das Prinzip sogenannter „Smart Contracts“ immer mehr an Beachtung, die als eine Art Schnittstelle für Interaktionen innerhalb eines Blockchain-Systems verstanden werden können. Im Folgenden möchte daher einen Überblick über die kurzfristigen Anwendungsmöglichkeiten von Smart Contracts in der deutschen Verwaltungslandschaft geben.

## 2. Begrifflichkeiten

### 2.1 Blockchain

Der Begriff „Blockchain“ bezeichnet ein Datenbankkonzept, bei dem die enthaltenen Datensätze durch die Anwendung kryptographischer Verfahren miteinander verbunden werden und so eine Kette aus Informationsblöcken bilden. Ein Block besteht dabei aus einer Kopfzeile, die auf den vorhergehenden Block verweist, einer festgelegten Anzahl von Speichereinträgen und einer Prüfsumme, die den Block identifiziert. Wird ein neuer Eintrag gemacht, so wird dieser zunächst mitsamt eines Zeitstempels und – je nach Ausführung der Datenbank – einer Signatur des Einträgers innerhalb des neusten Blocks gespeichert. Hat der Block die maximale Anzahl von Einträgen erreicht, wird aus dem gesamten Inhalt des Blocks mithilfe einer kryptographischen Hashfunktion eine eindeutige, irreversible Prüfsumme definierter Länge gebildet und an das Ende des Blocks gesetzt, wodurch er als abgeschlossen gilt. Diese Prüfsumme wird schließlich in die Kopfzeile des folgenden, anfangenden Blocks gesetzt und bei dessen Abschluss ebenfalls mit in die Prüfsummenbildung einbezogen. Durch diese Einbeziehung erhält die Datenbank ihren kettenartigen Charakter und gestaltet nachträgliche Änderungen am Datensatz beinahe unmöglich, da das Verändern eines beliebigen Eintrags eine Änderung aller nachfolgenden Blöcke nach sich ziehen müsste, andernfalls würde die Kette unterbrochen.

Im Wesentlichen lässt sich zwischen zwei Ausführungsansätzen unterscheiden. Das gemeinhin populärere Blockchainedkonzept mit einer dezentral geführten Datenbank wurde erstmals von Satoshi Nakamoto im Jahr 2008 beschrieben<sup>1</sup> und bildet unter anderem die Grundlage für die ebenfalls von ihm ins Leben gerufene Kryptowährung „Bitcoin“. Hierbei wird die Blockchain an jedem Knotenpunkt eines öffentlich zugänglichen Peer-to-Peer Netzwerks gespeichert und verwaltet. Neue Einträge werden in das Netzwerk gesendet und vor ihrer Eintragung in die Datenbank in einem Zwischenspeicher abgelegt. Computer innerhalb des Netzwerks, die sich ausschließlich mit der Verifikation der Transaktionen befassen (sog. „Miner“), bilden aus diesen Einträgen Blöcke und versuchen schließlich bei einer Art digitalem Puzzle, das gleichzeitig bei allen Minern stattfindet, diesen zur Blockchain

---

<sup>1</sup> <https://www.economist.com/special-report/2015/05/09/the-next-big-thing> [05.10.2018]

hinzuzufügen. Ziel bei diesem ist es, eine zufällige Zahl zu finden, die bei Einbeziehung in die Prüfsummenbildung einen im Vorfeld festgelegten Wert erzeugt. Der Miner, der dieses Ziel zuerst erreicht, erhält eine Prämie und sendet den von ihm generierten Block an das Netzwerk. Dieses „Proof of Work“ genannte Verfahren gewährleistet zum einen die Sicherheit durch die Unabänderlichkeit der Einträge und bildet zum anderen die Grundlage für die Konsensvereinbarung unter den Teilnehmern, bei der immer die Blockchain mit den meisten enthaltenen Blöcken, also die, an der am meisten „gerechnet“ wurde, als die korrekte angesehen wird und über deren Richtigkeit sich mindestens 51% der Knotenpunkte im Netzwerk einig sind.

Dem gegenüber stehen zentral bzw. privat geführte Blockchains, bei denen das zugrunde liegende Peer-to-Peer Netzwerk zugangsbeschränkt und somit nicht-öffentlich ist. Alle Teilnehmer des Netzwerks sind bekannt und es lässt sich zwischen schreibberechtigten und leseberechtigten Knotenpunkten unterscheiden, wodurch der „Proof of Work“ oder vergleichbare Validierungsmechanismen redundant werden<sup>2</sup>.

## 2.2 Smart Contract

Smart Contracts sind Computerprotokolle, die die Umsetzung von Vertragsklauseln übernehmen<sup>3</sup>. Sie sind per se keine Verträge im rechtlichen Sinne, sondern verwalten, überwachen und/oder verhandeln die inhaltlichen Aspekte eines zugrunde liegenden Vertrages völlig autonom. Um die Transparenz und das Vertrauen zwischen den Vertragspartnern zu sichern, werden Smart Contracts auf einer Blockchain gespeichert und dokumentieren auf dieser auch alle durch sie ausgeführten Handlungen.

Die derzeit relevanteste Plattform für Smart Contracts im privaten Sektor ist Ethereum. Dort können Nutzer eigene Protokolle erstellen und sie auf einer dezentral geführten Blockchain abspeichern und ausführen. Die Nutzungsbereiche liegen hauptsächlich innerhalb von Transaktionen und Crowdfundingprojekten und in e-Voting genannten Abstimmungen.

Die Protokolle werden in einer eigenen, zweckgebundenen Programmiersprache geschrieben. Beispiele hierfür sind Solidity, worin Smart Contracts innerhalb Ethereums verfasst werden, Vyper und LLL.

---

<sup>2</sup> Vgl. <https://medium.com/@lkolisko/do-we-need-mining-in-private-and-permissioned-blockchains-1a69b4c2c7a1> [11.10.2018]

<sup>3</sup> Vgl.

<http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> [11.10.2018]

## 2.3 Öffentliche Verwaltung / Verwaltungshandeln

Unter der öffentlichen Verwaltung versteht man jenen Teil der Exekutive, der mit der Erfüllung von öffentlichen Aufgaben betraut ist. Von ihm durchgeführtes Verwaltungshandeln ist definiert als „die nach außen wirkende Tätigkeit der Behörden, die auf die Prüfung der Voraussetzungen, die Vorbereitung und den Erlass eines Verwaltungsaktes oder auf den Abschluss eines öffentlich-rechtlichen Vertrags gerichtet ist; es schließt den Erlass des Verwaltungsaktes oder den Abschluss des öffentlich-rechtlichen Vertrags ein.“<sup>4</sup>

## 2.4 Verwaltungsinformatik

Richard Lackes definiert die Verwaltungsinformatik als die „Wissenschaft der informationstechnikgestützten Gestaltung von Verwaltungshandeln. Die Verwaltungsinformatik befasst sich mit Lösungen zur Verwaltungsautomation. Zur Wahrnehmung ihrer Gestaltungsaufgaben verwendet die Verwaltungsinformatik Informatikkonzepte, Organisationsverfahren sowie Verwaltungsprinzipien und -strukturen.“ Sie ist ein Teilgebiet der Wirtschaftsinformatik und findet in allen Bereichen des öffentlichen Sektors Anwendung.

# 3. Smart Contracts zur Unterstützung von Verwaltungsvorgängen

## 3.1 Allgemeines

Smart Contracts eröffnen in der fortschreitenden Digitalisierung der öffentlichen Verwaltung eine Vielzahl von innovativen Möglichkeiten, um bestehende Verfahrens- und Verwaltungsstrukturen effizienter zu gestalten. Melanie Swan geht noch einen Schritt weiter und beschreibt in ihrem Werk „Blockchain – Blueprint for a New Economy“<sup>5</sup> eine Gesellschaft, in der der Staat nicht mehr in Form des „für alle gleichen, höheren Wohl“-Modells<sup>6</sup> auftritt, sondern auf Grundlage der Blockchaintechnologie personalisierte

---

<sup>4</sup> Vgl. §9 VwVfG

<sup>5</sup> Vgl. Swan, M. (2015): Blockchain – Blueprint for a New Economy, O'Reilly Media S.44 ff.

<sup>6</sup> Vgl. Swan, M. (2015) S.44

Regierungsarbeit leistet, wie beispielsweise die individuelle Wahl von Steuergeldverteilungen oder ähnlichem. In der Blockchain sieht sie dabei gleichsam das „Instrument zum Regieren in der Gegenwart und die Sammlung aller Dokumente, Register und Archive für die Zukunft“<sup>7</sup>.

Doch auch deutlich weniger visionäre Implikationen sind denkbar. Die Einsatzgebiete erstrecken sich dabei von der Registerverwaltung, über Herkunfts- und Identitätsnachweise bis hin zu Zertifikations- und Verifikationsverfahren und darüber hinaus. Durch ihre autonome und transparente Funktionsweise bedarf es innerhalb der von ihnen übernommenen Prozesse weniger bis keiner vertrauenswürdigen Intermediäre mehr, die den entsprechenden Vorgang überwachen und kontrollieren. Das hätte, neben den offensichtlichen Zeit- und Effizienzaspekten, die eine Digitalisierung im Allgemeinen mit sich bringt, zur Folge, dass besonders am Beispiel der deutschen Verwaltung große finanzielle Einsparungen sowohl für den Staat, als auch für seine Bürger erwartet werden könnten.

Vorreiter im Feld der innovativen e-Governance ist derzeit Estland. Dort sind eigenen Angaben zufolge 99% aller öffentlichen Serviceleistungen rund um die Uhr online verfügbar und haben seit ihrer Inbetriebnahme über 800 Jahre an Arbeitszeit eingespart<sup>8</sup>. Auch blockchainbasierte Technologien sind dabei erstmals auf nationaler Ebene im Einsatz. Als Reaktion auf eine groß angelegte Cyberattacke wird die Integrität von medizinischen Akten und Dokumenten seit 2012 mit Hilfe einer der Blockchain sehr ähnlichen Technologie geschützt und seit 2015 bietet das Land einen blockchainbasierten Dienst namens „e-Notary“ an<sup>9</sup>, der Notaren die elektronische Kommunikation mit anderen Notaren und staatlichen Institutionen sowie ihren Registern ermöglicht<sup>10</sup>.

Die Erweiterung um eine Nutzerschnittstelle für Bürger würde in einem solchen Digitalisierungsprozess den nächsten Schritt darstellen. Während Einsichtnahmen, Änderungsanträge, etc. an staatlichen Registern aktuell meist über zentrale Behörden und eingeschaltete Intermediäre wie Anwälte stattfinden, ließe sich durch den Einsatz von entsprechend gestalteten Smart Contracts ein direkter, unmittelbarer Zugang zu den gewünschten Aktionen herstellen. Sie wären nicht vom Nutzer selbst programmierbar, sondern vielmehr aus einer Palette von zulässigen, von der entsprechenden Behörde vordefinierten Bausteinen – auch Templates genannt - generierbar, ähnlich dem Ausfüllen eines Onlineformulars. Die darunter operierende Blockchain gewährleistet dabei die Sicherheit der behandelten Daten, indem sie sämtliche Zu- und Eingriffe inklusive der von

---

<sup>7</sup> Vgl. Swan, M. (2015) S44.

<sup>8</sup> Vgl. <https://e-estonia.com/solutions/e-governance/> [11.10.2018]

<sup>9</sup> Schütte, J./Fridgen, G./Prinz, W. (2017) BLOCKCHAIN UND SMART CONTRACTS München: Frauenhofer-Gesellschaft S.30

<sup>10</sup> Vgl. <http://www.rik.ee/en/other-services/e-notary> [11.10.2018]

Smart Contracts ausgelösten Aktionen dokumentiert und in diesem Zuge auch eine Rückverfolgbarkeit garantiert.

Die Kombination aus diesen beiden Elementen bildet den großen Vorteil gegenüber einer Umsetzung auf konventionellem Wege, bei dem ein direkter Zugang zu den betreffenden Datensätzen immer auch ein Sicherheitsrisiko birgt.

### 3.2 Die Rolle der Blockchain

Eine Blockchain eignet sich aufgrund ihrer Beschaffenheit nicht zur Speicherung beliebiger Informationen. Da sie einzig das Hinzufügen neuer Daten, nicht aber die Editierung bereits vorhandener Einträge unterstützt, ist sie nicht in jedem Bereich der staatlichen Registerführung als Datenbankmodell einsatztauglich. Sie kann jedoch als Sicherheitsinstanz auf einer herkömmlichen Datenbank operieren, indem sie beispielsweise die Metadaten (und ggf. auch die Inhalte) von Editierungen erfasst und so eine Art verbindlicher Referenzdatenbank darstellt. Die in Estland eingesetzte KSI-Blockchain, die unter anderem auch im militärischen Bereich von der NATO und dem US-Verteidigungsministerium genutzt wird<sup>11</sup>, sichert so erfolgreich die Integrität der im Rahmen des e-Estonia Programms online gestellten Datenbanken und regelt gleichzeitig die Zugriffs- und Leserechte für seiner Nutzer. Smart Contracts ließen sich somit auch in Register implementieren, die nicht durch eine Blockchain dargestellt werden könnten, indem sie auf einer Sicherungsblockchain gespeichert und ausgeführt würden.

### 3.3 Zentral versus dezentral

Das Konzept der Blockchain wurde durch das Paradigma der Dezentralität populär und hat nicht zuletzt auch aufgrund der gesellschaftlichen Konsequenzen eines solchen Systems weit über die Grenzen der IT-Welt hinaus für Aufsehen gesorgt.

Gemeinhin versprechen dezentral geführte Blockchains vor allem eine Unabhängigkeit von Intermediären, denen die betroffenen Nutzer des jeweiligen Systems vertrauen müssen. Auf staatliche Stellen übersetzt würde das bedeuten, dass Bürger nicht mehr auf die Integrität und Gewissenhaftigkeit des Staates angewiesen wären, sondern stattdessen eine stetige Gewissheit

---

<sup>11</sup> Vgl. <https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf> [11.10.2018]



über die Korrektheit ihrer Dokumente und Daten aus der unmöglich zu manipulierenden Blockchain, auf der diese gespeichert sind, schöpfen könnten. Besonders in Ländern mit Korruptionsproblemen könnte das eine Möglichkeit des Schutzes darstellen.

In Deutschland herrscht jedoch gemeinhin sehr wenig Misstrauen gegenüber den Behörden und Ämtern, weshalb eine ganz andere Frage hier im Vordergrund stehen muss: Öffentlich oder nicht öffentlich? „Dezentral“ bedeutet zwangsläufig auch immer, dass sämtliche Einträge der Blockchain öffentlich eingesehen werden können. Folglich ist eine so geführte Blockchain gänzlich untauglich für die Aufbewahrung sensibler beziehungsweise vertraulicher Daten.

Weiterhin unterliegen dezentral geführte Blockchains dem Problem der Skalierbarkeit. Der „Proof of Work“-Mechanismus funktioniert einzig auf der Basis von Rechenleistung und beansprucht somit große Energieressourcen. Außerdem setzt er eine möglichst umfangreiche Zahl von Minern voraus, die wiederum für ihre Ressourcenaufbringung entschädigt und entlohnt werden müssen, was einen gewissen Kostenpunkt darstellt. Weiterhin müssen sämtliche Teilnehmer des Netzwerks, also auch solche, die einen Smart Contract erzeugen möchten, eine Kopie der Blockchain auf ihrem Endgerät abspeichern. In Anbetracht der Datenmengen, die bereits jetzt in staatlichen Registern gespeichert sind und der längerfristigen Auslegung von Digitalisierungsprojekten, erfordert dies schnell horrende Mengen an Speicherplatz für jeden, der das System nutzen möchte und kann unter Umständen auch zum Ausschluss einzelner führen, die diesen Speicherplatz nicht aufbringen können.

Wenngleich dieses Problem Gegenstand aktueller Forschung ist, so gibt es bis dato noch keinen zufriedenstellenden Lösungsvorschlag. Allein schon deshalb dürften sich praktische Umsetzungen dezentraler Blockchains für die meisten Bereiche des deutschen Verwaltungsapparats kurzfristig als sehr schwierig erweisen.

### 3.4 Eine Frage der (technischen) Sicherheit

Die obersten Paradigmen für die Digitalisierung staatlicher Dienste sind Datenschutz, IT-Sicherheit und die Widerstandsfähigkeit der Infrastruktur<sup>12</sup>. Dezentral geführte Blockchains gewährleisten Letzteres schon aufgrund ihrer mittelpunktlosen Beschaffenheit. Bei zentral geführten Blockchains müssten die netzwerkexternen Zugriffspunkte entsprechend gesichert werden, das soll jedoch mit einem Verweis auf bestehende Lösungen und Mechanismen nicht

---

<sup>12</sup> Vgl. <https://www.bmwi.de/Redaktion/DE/Meldung/2015/20150316-aufholen-im-digitalen-wettlauf-arbeitskreis-smart-service-welt-uebergibt-bericht-an-sigmar-gabriel.html> [11.10.18 14:56]

Gegenstand dieser Arbeit sein. Weiterhin zeigt die estländische Implementierung, dass besonders der für sensible Daten unabdingbare Sicherheitsaspekt mithilfe einer Blockchain gewährleistet werden kann. Da sich somit für eine Umsetzung innerhalb der deutschen Verwaltung auf bereits existierende und Lösungen zurückgreifen ließe, soll an dieser Stelle nur die Sicherheit der Smart Contracts im Vordergrund stehen.

Bei ihrer Entwicklung muss vor allem ein Punkt sichergestellt werden: dass die erzeugten Smart Contracts aufgrund von unsachgemäßen Eingaben oder semantischen Fehlern innerhalb der Programmierung keine rechtswidrigen Handlungen vornehmen beziehungsweise in einem rechtlichen Schwebezustand münden. Darunter zählt auch der Aspekt, dass ein Smart Contract immer nur Zugriff auf diejenigen Daten erhält, die seinem Ersteller eindeutig zuzuordnen sind. Ist ein Smart Contract einmal auf der Blockchain abgelegt, kann er aus dieser nicht mehr entfernt werden und sollte besonders aufgrund seiner Vertrauenswürdigkeit keine nachträglichen Veränderungen am Code zulassen. Auch die Implementierung einer Art Notabschaltvorrichtung ist dahingehend problematisch, dass auch eine solche zu Missbrauchszwecken genutzt werden kann. Es bestünde zwar die Möglichkeit, ihre Aktivierung an eine Zustimmung aller in den Smart Contract involvierten Parteien zu knüpfen, was ihre Funktion als Sicherungsmechanismus jedoch dahingehend hemmt, dass ein fehlerhaftes Protokoll in der verstreichenden Zeit bis zur Kenntnisnahme und der Bestätigung durch die Eingebundenen bereits fatale Schäden angerichtet haben könnte, oder aber, dass sie im Falle einer vorsätzlich herbeigeführten Fehlfunktion gar nicht erst zum Einsatz kommt – schließlich würde der Verursacher einer Abschaltung vermutlich nicht zustimmen.

Es muss also bereits bei der Entwicklung 100-prozentig sichergestellt werden, dass die Protokolle völlig zuverlässig und regelkonform operieren. Dazu bedarf es vor allem einer Programmiersprache deren Eigenschaften das ermöglichen.

Aktuell ist Solidity die populärste Lösung, wenn es um das Verfassen von Smart Contracts geht, nicht zuletzt aufgrund ihrer Rolle als Hausprogrammiersprache für Ethereum. Allerdings weist sie eine Vielzahl von Schwachstellen und Sicherheitsrisiken auf. So bietet Solidity weder einen User-Support, eine umfangreiche Dokumentation, noch eine Möglichkeit zur Verifikation, dass das Programm bei allen möglichen Eingaben korrekt operiert. Darüber hinaus sind in Solidity verfasste Protokolle anfällig für sogenannte „reentrancy attacks“, bei denen der betroffene Smart Contract in eine Wiederholungsschleife gerät und gewisse Zeilen im Code immer und immer wieder ausführt. Auf diese Weise gelang es Angreifern 2016 im

Zuge des sogenannten „DAO-Angriffs“ Ether (die Kryptowährung von Ethereum) im Wert von über 60 Millionen US-Dollar zu stehlen<sup>13</sup>.

Zwar wird an Solidity weiterhin gearbeitet, eine sichere Grundlage für Smart Contracts in staatlichen Stellen wird sie aus den genannten Gründen heraus jedoch vorerst nicht sein können. Viele der anderen, zumeist noch in der Entwicklung steckenden Sprachen wie Vyper und LLL zielen ebenfalls auf den Einsatz innerhalb Ethers ab und sind auf diesen optimiert. Es wäre darum vermutlich die beste Lösung eine neue Sprache zu entwickeln, die exakt auf die Anforderungen einer Anwendung innerhalb der öffentlichen Verwaltung zugeschnitten ist.

## 4. Veranschaulichung des Einsatzes anhand praktischer Beispiele

### 4.1 Smart Contracts im Patentamt

Ein erstes Beispiel für die praktische Einsetzbarkeit von Smart Contracts liefert Thomas Heinz Meitinger<sup>14</sup>. Es beschäftigt sich mit dem Erwerb und Erhalt von Patenten. Diese unterliegen dem deutschen Patentgesetz und werden vom Patentamt in einem öffentlichen Register geführt. Bei einer Anmeldung wird das Patent zunächst vom Patentamt auf Neuheit und erfinderische Tätigkeit und auf die Einhaltung aller Formalien durch den Anmelder geprüft. Wenn beides konform ist, wird das Schutzrecht erteilt und das Patent wird in das Patentregister aufgenommen. Der Anmelder muss dann innerhalb bestimmter Fristen pünktlich Beträge in korrekten Höhen zahlen um sein Schutzrecht zu erhalten, andernfalls droht ein Entfall. Das erfordert ein präzises Fristenüberwachungssystem und wird daher häufig von den Anmeldern an spezialisierte Anwaltskanzleien für Patentrecht abgegeben. Diese unterstützen den Antragsteller bei der Anmeldung und kümmern sich anschließend um die fristgerechten Zahlungen der entsprechenden Gebühren. Ein solches Verfahren kostet im Schnitt ungefähr 10000€ bei der Anmeldung und dann über die Laufzeit des Patents von 20 Jahren weitere 500€-2000€ pro Jahr mit einem sehr großen, vom Patent abhängigem Spielraum<sup>15</sup>. Das hat zur Folge, dass besonders Erfinder mit einem geringen Budget keine Möglichkeit besitzen, ein Patent auf ökonomische Weise zu halten.

---

<sup>13</sup> Vgl. [https://medium.com/@John\\_Potter\\_XBY/the-problem-with-solidity-be7e6c277a58](https://medium.com/@John_Potter_XBY/the-problem-with-solidity-be7e6c277a58) [07.10.2018]

<sup>14</sup> Vgl. Meitinger, T. (2017): Smart Contracts, Informatik Spektrum Ausgabe 4/2017 S.373

<sup>15</sup> <http://www.patentanwalt.cc/2014/11/was-kostet-ein-patent.html> [21.08.19]

Allerdings ließe sich dieser Vorgang auch mit Hilfe eines Smart Contracts lösen. In diesen würden zunächst die gesetzlichen Vorschriften in Form von „if-then“-Beziehungen implementiert werden. Das Protokoll wäre daraufhin im Stande, die formalen Anforderungen einer Patentanmeldung eigenständig zu überprüfen und Korrekturvorschläge zu machen beziehungsweise auf Mängel hinzuweisen. Es könnte außerdem die Zahlungen überwachen und im Falle eines Nichtigkeitsverfahrens oder Ähnlichem Zahlungen automatisch einstellen. Das vom Patentamt geführte, online verfügbare Register, in dem zu jedem Patent auch die zugehörigen Transaktionen gelistet sind, würde in Form einer öffentlich einsehbaren Blockchain innerhalb des Smart Contracts gespeichert werden. Neue Anmeldungen würden über eine Website des Patentamts getätigt werden, wo Nutzer die Möglichkeit hätten, einen vorschriftskonformen Smart Contract zu erzeugen.

Da der Smart Contract autonom operiert und in jedem Fall gesetzeskonforme Ausführungen tätigt, bedürfte es keinerlei Kontrollinstanzen innerhalb des Patentamts mehr. Folglich ließen sich zwei der drei Hauptaufgabenfelder vollständig an das Protokoll übergeben, einzig die Überprüfung auf erfinderische Tätigkeit würde weiterhin von Mitarbeitern des Amtes getätigt werden.

Auf Seiten des Anmelders könnte der Smart Contract die Zahlungen der Jahresgebühren überwachen und diese im Falle einer erreichten Frist auf Nachfrage automatisch vornehmen. Somit bräuchte er im Zuge des Gesamtprozesses keine dritte Instanz in Form einer Anwaltskanzlei mehr in den Erwerb und Erhalt seines Patents einzubeziehen und könnte seine Kosten so erheblich senken. Das Patentamt wiederum könnte eine Vielzahl an Arbeitsstunden für die Prüfung der Formalien sparen und so die Personalkosten reduzieren, was sich im Optimalfall in einer Gebührensenkung ebenfalls für den Anmelder bemerkbar machen würden. Die Kosten für die Führung und Verwaltung des Registers ließen sich in die Kosten für die Pflege der Blockchain übersetzen und könnten gegebenenfalls sogar zu weiteren Einsparungen führen.

#### 4.2 Transaktionen von Immobilien mittels Smart Contract

Ein weiteres Beispiel soll der Einsatz von Smart Contracts in der Führung und Verwaltung des Grundbuchs darstellen. In einigen Ländern, darunter Honduras und Griechenland<sup>16</sup>, wird bereits an der praktischen Umsetzbarkeit eines blockchainbasierten Grundbuchs geforscht und

---

<sup>16</sup> Vgl. Meitinger, T. (2017)

in Schweden ist 2017 ein erster Testlauf erfolgreich abgeschlossen worden<sup>17</sup>. Um ein solches System anhand der deutschen Grundbuchführung zu illustrieren, möchte ich zunächst kurz den allgemeinen Vorgang eines Grundstückerwerbs beziehungsweise -verkaufs erklären.

Nachdem sich Käufer und Verkäufer über die Einzelheiten einer Grundstücksübergabe besprochen und geeinigt haben, wird ein Termin bei einem Notar vereinbart um alle Einzelheiten der Übergabe in einem Kaufvertragsentwurf festzuhalten. Meist lassen beide Parteien diesen Entwurf anschließend von ihren eingeschalteten Anwälten prüfen und nehmen gegebenenfalls bei weiteren Treffen mit dem Notar Änderungen vor. Ist ein Entwurf beidseitig akzeptiert, setzt der Notar den endgültigen Kaufvertrag auf, der von beiden Parteien in dessen Gegenwart unterschrieben wird (alternativ sind auch bevollmächtigte Dritte stellvertretend berechtigt die Unterschrift vorzunehmen, ein persönliches Erscheinen der beiden Vertragspartner ist nicht zwingend notwendig). Der Notar veranlasst daraufhin eine Auflassungsvormerkung für die entsprechende Immobilie beim Grundbuchamt, wodurch das Grundstück vom Verkäufer nicht mehr anderweitig verkauft werden kann. Außerdem erfolgt im Falle einer Fremdfinanzierung eine Grundschuldeintragung im Grundbuch durch den Notar, die dem Darlehensgeber über die Laufzeit der Finanzierung ein Sicherungsrecht für den Fall eines Zahlungsausfalls einräumt. Im letzten Schritt schickt der Notar eine Zahlungsaufforderung über den vereinbarten Preis an den Käufer und veranlasst nach dessen Zahlung die Eintragung des neuen Eigentümers der entsprechenden Immobilie im Grundbuch. Hatte das Grundstück zum Zeitpunkt der Übernahme noch Grundschuldeinträge oder Hypotheken eines Vorbesitzers, werden diese entweder nach einer Tilgung gelöscht oder an den Käufer weitergegeben. Die Rolle des Notars ist bei diesem Prozess im § 311b Abs. 1 BGB durch den Wortlaut „Ein Vertrag, durch den sich der eine Teil verpflichtet, das Eigentum an einem Grundstück zu übertragen oder zu erwerben, bedarf der notariellen Beurkundung. [...]“ gesetzlich verankert<sup>18</sup>.

Ein adäquat umgesetzter Smart Contract wäre im Stande, viele der oben genannten Schritte eigenständig durchzuführen. Käufer und Verkäufer würden sich daher zunächst mittels e-Identifikation ihrer Personalausweise in einem zu diesem Zweck eingerichteten Onlineportal des Grundbuchamts authentifizieren und dort einen gemeinsamen, allen immobilienrechtlichen Bestimmungen entsprechenden Smart Contract auf Grundlage eines Kaufvertrags erzeugen. Darin wird das betreffende Grundstück, die Personalien beider

---

<sup>17</sup> <https://www.btc-echo.de/schweden-nutzt-jetzt-offiziell-die-blockchain-fuer-grundbucheintragungen/> [24.08.2019]

<sup>18</sup> Vgl. § 311b Abs. 1 BGB

Parteien und der Kaufpreis festgehalten. Sind Dritte, wie beispielsweise Banken, in die Finanzierung eingebunden, werden auch diese ihrer Rolle entsprechend mit in den Smart Contract eingebunden. Der Smart Contract prüft daraufhin die Korrektheit aller Eingaben und untersucht eigenständig die Verkaufsgrundlagen im entsprechenden Eintrag des Grundbuchs. Liegt beispielsweise bereits eine Auflassungsvormerkung vor, weist der Smart Contract alle Parteien darauf hin und pausiert beziehungsweise beendet die Transaktion. Im Falle einer vorliegenden Hypothek, Grundschuldbelastung oder ähnlichem überprüft der Smart Contract mittels Nachfrage, ob der Käufer darüber in Kenntnis gesetzt ist und leitet gegebenenfalls eine Beendigung oder Korrektur des Vertrags ein. Anschließend wird die Auflassungsvormerkung und ggf. eine Grundschuld durch den Smart Contract in das Grundbuch eingetragen und die Zahlung des Kaufpreises wird initiiert. Aufgrund der zumeist sehr hohen Beträge, die bei einem Immobilienhandel gezahlt werden müssen, bliebe zu entscheiden, ob der Smart Contract diese eigenständig übernimmt oder lediglich überwacht.

Nach erfolgreicher Transaktion überschreibt der Smart Contract das Grundstück im Grundbuch dem neuen Besitzer und veranlasst nach „Rücksprache“ mit den Gläubigern des Vorbesitzers, je nach vertraglicher festgelegter Vorgehensweise, eine Löschung oder Übernahme alter Grundschuldeinträge. Da die Einträge des Grundbuchs variabel bleiben müssen, eignet sich eine Blockchain per se nicht zur Speicherung eines solchen<sup>19</sup>. Allerdings kann eine Blockchain den Verlauf aller Editierungen dokumentieren und diese so validieren. Der beschriebene Smart Contract würde seine Aktionen somit auf die Blockchain schreiben und damit einen weiteren Befehl auslösen, der diese dann ins Grundbuch übernimmt, wodurch nicht autorisierte Änderungen an der Datenbank des Grundbuchs aufgrund ihrer fehlenden Referenz innerhalb der Blockchain sofort auffielen. Die Blockchain selbst würde, wie auch im schwedischen Projekt, zentral und nicht-öffentlich gespeichert werden.

Die schwedische Regierung erhofft sich durch eine solche Umsetzung Einsparungen in Höhe von rund 100 Millionen Euro, die bisher für Verwaltungs- und Betrugsverfahren aufgewendet wurden<sup>20</sup>. Für das deutsche System gäbe es jedoch noch einen weiteren, nicht zu verachtenden Faktor: die Zeit. Grundstücksverkäufe nehmen eine nicht zu unterschätzende Zeitspanne in Anspruch, nicht zuletzt wegen Terminknappheit der Notare, Versandzeit und Austausch von Dokumenten und Nachweisen und natürlich Bearbeitungszeiten innerhalb des Grundbuchamts. All diese Faktoren ließen sich mithilfe eines Smart Contracts, in den alle Beteiligten einbezogen werden, verringern oder gar eliminieren.

---

<sup>19</sup>Vgl. <https://www.ito.de/recht/hintergruende/h/blockchain-grundstuecksrecht-immobilien-verkauf-notare-grundbuch-transaktionen-sicherheit/> [24.10.2018]

<sup>20</sup> <https://www.btc-echo.de/schweden-nutzt-jetzt-offiziell-die-blockchain-fuer-grundbucheintragen/>

Die Aufgabe des Notars würde zumindest in seiner Funktion als beglaubigende Instanz obsolet. Die einzige Möglichkeit, unzulässige Transaktionen in einem korrekt und sicherheitsadäquat umgesetzten System dieser Art einzuleiten, ist der Diebstahl eines Personalausweises und seiner dazugehörigen Online-Zugangsdaten. Das Bundesministerium des Innern, für Bau und Heimat listet aktuell vier unabhängige Sicherheitsmechanismen, die den gleichzeitigen Verlust beider vorbeugen sollen<sup>21</sup>.

Nach aktueller Rechtsauffassung ist dies jedoch nicht der einzige Aspekt für ein gesetzliches Vorschreiben einer notariellen Beurkundung in diesem Prozess. So schreibt Richard Kanzleiter in den Münchner Kommentaren, dass die Beteiligten dadurch außerdem vor Übereilung geschützt werden sollen und die besondere Bedeutung eines solchen Geschäfts deutlich wird. Weiterhin sollen eine sachliche Beratung und die Aufklärung über die Konsequenzen der Transaktion durch den Notar gewährleistet sein<sup>22</sup>. Da der Erwerb von Grundbesitz nicht selten eine Aufwendung großer Vermögensteile durch den Käufer notwendig macht, sieht der Gesetzgeber an dieser Stelle ein besonders schützenswertes Rechtsgeschäft und möchte darum insgesamt „den Verkäufer in erster Linie vor der unüberlegten Veräußerung selbst, in zweiter Linie vor der Veräußerung zu unüberlegten Bedingungen, den Erwerber aber nur in zweiter Linie vor dem unüberlegten Erwerb selbst, in erster Linie vor dem Erwerb zu unüberlegten und damit möglicherweise unangemessenen Bedingungen“<sup>23</sup> schützen. Aus diesem Grund bleibt der Notar wohl weiterhin ein fester Bestandteil von Immobiliengeschäften und kann somit nicht als Intermediär von einem Smart Contract ersetzt werden. Nichtsdestotrotz ließe sich ein wie oben beschriebenes Protokoll, mit leichten Veränderungen auf der Initiierungsebene, in das bestehende Prozedere eingliedern und könnte so ebenfalls einen Großteil der erhofften Verbesserungen erzielen.

#### 4.3 Smart Contracts im Finanzamt

Bereits 2015 griff Mark Walport im Rahmen einer Zusammenfassung der Einsatzmöglichkeiten von blockchainbasierten Technologien für die britische Regierungen eine, wie er einschätzt, technisch umsetzbare Lösung für den Steuersektor auf<sup>24</sup>. Barański (2017) beleuchtet einen

---

<sup>21</sup> [https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Sicherheit/sicherheit\\_node.html](https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Sicherheit/sicherheit_node.html) [24.10.2018]

<sup>22</sup> Vgl. Kanzleiter, Richard in Münchener Kommentar zum BGB, § 311b, Rn. 2. S.1654 ff

<sup>23</sup> Vgl. Kanzleiter, Richard S.1655

<sup>24</sup> Vgl. Walport, M. (2015): Distributed Ledger Technology: beyond block chain

solchen Einsatz näher und illustriert in seiner Arbeit auch den Nutzen von Smart Contracts innerhalb eines blockchaingestützten Steuersystems<sup>25</sup>.

Für das deutsche Modell sind, seinem Umfang entsprechend, eine Vielzahl verschiedener Applikationen denkbar, die sich in bestehende Strukturen und Fachbereiche eingliedern ließen. So sind Einsätze im Bereich der KfZ-Steuer, der privaten Steuererklärung, der Mehrwertsteuer aber auch im Bereich der gewerblichen Versteuerung durchaus vorstellbar, erfordern aber einer genaueren, am jeweiligen Beispiel durchgeführten, rechtssicheren Evaluation. Da das Steuerrecht sehr umfangreich und für Laien nur schwer zugänglich ist, macht sich hier also ein erster, kompetenzübergreifender Zugang für das deutsche System notwendig.

Im Rahmen einer Umfrage vom World Economics Forum aus dem Jahr 2015 gaben 73% der befragten IT-Experten an, dass sie einen erstmaligen Steuereinzug per Blockchain-System durch eine Regierung in den kommenden 10 Jahren erwarten<sup>26</sup>. Auch aus den Bestrebungen diverser Regierungen, wie beispielsweise der britischen Administration, lässt sich interpretieren, dass besonders in diesem Bereich innerhalb der kommenden Jahre Fortschritte erzielt werden, die sich gegebenenfalls auch für das deutsche Steuerwesen adaptieren ließen. Dieser Abschnitt versteht sich somit eher als Verweis auf einen Einsatzbereich, an dem bereits praktisch gearbeitet wird und gibt anstelle beispielhafter Darlegungen einen Ausblick auf bestehende und kommende Ausarbeitungen.

#### 4.4 Smart Contracts und die Wahlen von morgen

Die Idee, Regierungswahlen mithilfe des Internets abzuhalten ist nicht neu. Allerdings sind die bisherigen Bemühungen eine gesetzeskonforme Umsetzung für das deutsche Wahlverfahren zu entwickeln immer an einer Vielzahl technisch bedingter Schwierigkeiten gescheitert.

Für Wahlen gelten die fünf Wahlrechtsgrundsätze: allgemein, frei, unmittelbar, gleich und geheim<sup>27</sup>. Diese müssen bei einer Übersetzung ins Digitale zwingend gewährleistet sein und dürfen unter keinen Umständen verletzt werden. Weiterhin kommen bei einer solchen zwei weitere Aspekte hinzu, die es zu beachten gilt: Manipulationssicherheit und eine

---

<sup>25</sup> Vgl. Barański, P. (2017): Blockchaintechnology and its potential in taxes, Deloitte

<sup>26</sup> Vgl. Schlatt, V./Schweitzer, A./Urbach, N./Fridgen, G. (2016): Blockchain: Grundlagen, Anwendungen und Potenziale, Projektgruppe Wirtschaftsinformatik des Fraunhofer- Instituts für Angewandte Informationstechnik (FIT)

<sup>27</sup> Vgl. Art. 38 GG Abs.1



Nachvollziehbarkeit über das Auszählungsverfahren für die Wähler<sup>28</sup>. Der Bundeswahlleiter sieht vor allem die Grundsätze der allgemeinen, freien und geheimen Wahl bei Online-Wahlen als nicht hinreichend gewährleistet, selbiges gilt für die Transparenz des Auszählungsverfahrens<sup>29</sup>.

Eine Lösung per Smart Contract könnte hier zumindest in einigen Problempunkten Abhilfe verschaffen. Dafür würde zunächst im Zuge der Wahlbenachrichtigung ein Registrierungsverfahren für die Online-Abstimmung eingeleitet werden. Dieses ließe sich auch über einer Website realisieren, auf der sich Interessenten mittels ihres Online-Personalausweises identifizieren und müsste nicht zwingend wie bisher einzig auf postalischem Weg erfolgen. Anschließend wird eine den Registrierungen entsprechende Anzahl digitaler Wallets erstellt, die die abgebbaren Stimmen in Form von Tokens enthalten. Dies ist notwendig, da derzeit nicht davon ausgegangen werden kann, dass jeder Wahlberechtigte die technischen Mittel besitzt oder zu bedienen weiß, um an einer Online-Wahl teilzunehmen, weshalb eine Wahl im Wahllokal weiterhin möglich sein muss. Um aber eine Doppelwahl zu verhindern, bindet die Entscheidung zur Online-Wahl im selben Prinzip wie die Entscheidung zur Briefwahl.

Nach Erstellung der Wallets, die nur mit einer eindeutigen Identifikationsnummer versehen sind, erhalten alle Registrierten einen zufällig ausgewählten, nicht auf den Einzelnen zurückverfolgbaren Zugangscod zu einem dieser Wallets. Am Tag der Wahl können sich die Wähler dann in dieses einloggen und ihre Stimmen abgeben. Ein Smart Contract regelt dabei die korrekte Überschreibung der Tokens auf die zur Wahl eingerichtete Blockchain, entfernt diese anschließend aus dem Wallet und schließt es nach Abgabe aller Stimmen. Er fungiert somit quasi als digitaler Stimmzettel.

Die eingesetzte Blockchain ist dezentral strukturiert und kann von jedem Interessierten eingesehen und gehostet, nicht aber beschrieben werden. Somit ist, zumindest theoretisch, jeder in der Lage, die Wahl eigenständig nachzuvollziehen und zu überwachen. Zusätzlich wäre es möglich, ein Programm zur einfacheren Interpretierung der Blockchain zur Verfügung zu stellen. Ob das den Anforderungen des Bundesverfassungsgerichts entspricht, bliebe jedoch abzuwarten.

Die Vorteile einer digitalen Wahl liegen vor allem in einer leichteren Zugänglichkeit, von der man sich eine höhere Wahlbeteiligung erhofft. Wähler könnten ihre Stimme so von überall aus jederzeit abgeben und müssten dazu nicht einmal das Haus verlassen. Weiterhin

---

<sup>28</sup> Vgl. Urteil Bundesverfassungsgericht vom 3.3.2009 (Az.: 2 BvC 3/07 und 2 BvC 4/07)

<sup>29</sup> <https://www.bundeswahlleiter.de/service/glossar/o/online-wahlen.html> [30.10.2018]

verringern blockchainbasierte Wahlen die Möglichkeiten der Ergebnisverfälschung, indem sie das „einschuggeln“ oder „verlorengehen“ von Stimmzetteln unmöglich machen und Fehler bei der Auszählung verhindern. Was die Sicherheit vor Wahlbetrug angeht, so ist ein wie oben beschriebenes Verfahren mindestens genauso praktikabel wie eine Briefwahl. In beiden Verfahren lässt sich sicherstellen, dass die Zahl der abgegebenen Stimmen korrekt ist, nicht aber, wer die Stimme abgegeben hat und ob die Wahl ohne die direkte Einflussnahme eines dritten stattgefunden hat. Nach Einschätzung von Christoph Schöneberg gefährdet somit also auch die Briefwahl die Grundsätze einer allgemeinen und freien Wahl<sup>30</sup>. Die Diskussion, ob das als Befürwortungskriterium genügt, müsste in gesetzgebender Instanz geführt werden. Damit verbleibt der Aspekt der geheimen Wahl. Hier ließen sich vermutlich technische Lösungen finden, die den Verteilvorgang der Wallets kryptographisch so weit verschlüsseln, dass sie mit aktuellen Möglichkeiten nicht rekonstruierbar wären. Das schließt jedoch einerseits nicht aus, dass diese Möglichkeiten irgendwann zur Verfügung stehen und dann auf vergangene Wahlverfahren angewendet werden und kann andererseits keine Antworten darauf geben, dass Handlungen im Internet immer irgendwo Spuren hinterlassen und einer Datenspionage niemals gänzlich vorgebeugt werden kann. Es herrscht also an dieser Stelle noch ein tiefgreifender Forschungs- und Entwicklungsbedarf um eine geheime Wahl ausnahmslos und unbedingt zu gewährleisten.

## 5. Umsetzbarkeit und Rechtsfragen

Drei der vier genannten Beispiele wären, zumindest vom technischen Standpunkt aus gesehen, umsetzbar oder bedürfen eines zumutbaren Entwicklungsaufwands. Allerdings unterliegt die Verwaltungsstruktur in Deutschland einer klaren Gesetzgebung und ist somit politischen Entscheidungen unterworfen. Da das Thema „Smart Contracts“ erst seit kurzem an Beachtung gewinnt und innerhalb der deutschen Verwaltung höchstens in Fachkreisen bekannt ist<sup>31</sup> bleibt also abzuwarten, wann und in welchem Maße eine Diskussion über den Einsatz dieser Technologie auf politischer Ebene stattfinden wird. In großen Teilen der möglichen Einsatzgebiete wären Gesetzes- und Verfahrensänderungen notwendig, um eine Implementierung möglich zu machen. Dabei dürfte, neben den zum Thema Digitalisierung

---

<sup>30</sup> <https://www.handelsblatt.com/politik/deutschland/bundestagswahl/alle-schlagzeilen/blockchain-wo-man-die-blockchain-schon-zum-abstimmen-einsetzen-kann/20366520-2.html?ticket=ST-2471207-9dpNEHEWpCMraD9eBcCg-ap6> [30.10.2018]

<sup>31</sup> Vgl. Schütte, J./Fridgen, G./Prinz, W. (2017) S.32

immer angebrachten Punkten der Sicherheitsbedenken, vor allem die Frage im Vordergrund stehen, ob eine Verlagerung der glaubwürdigkeits- und vertrauensstiftenden Mechanismen aus der menschlichen Obhut in die Arme einer Technologie<sup>32</sup> vertretbar und angemessen ist. Die Ergebnisse dieser Debatten werden maßgeblich über die Zukunft von Smart Contracts im staatlichen Einsatz entscheiden und eine Art Weichenpunkt für weitere Forschungen auf dem Gebiet des blockchaingestützten e-Governments darstellen.

Sollte es zu einer positiven Entscheidung kommen so ist zu beachten, dass damit ein internationales Pilotprojekt in Gang gebracht wird. Es gibt bisher, zumindest zu den Smart Contracts, kaum Referenzdaten aus vergleichbaren Bemühungen anderer Länder. Es könnte also nicht einfach auf eine bestehende Softwarelösung zurückgegriffen werden, sondern bedürfe einer Neuentwicklung anhand des vorliegenden Einzelfalls. Das verlangt neben einem Entwicklungsbudget für die technischen Komponenten auch einer genaueren Untersuchung der betroffenen Verwaltungsprozesse und einer darauf abgestimmten Planung durch Fachleute, mit Kenntnissen über das Verwaltungswesen und die technischen Hintergründe, was einen weiteren nicht zu vernachlässigenden Kostenpunkt darstellt. Wenngleich große Einsparungen nach einer Inbetriebnahme zu erwarten sind, wird dieser finanzielle Aspekt, besonders unter dem Gesichtspunkt des schwindenden Budgets für die Erfüllung öffentlicher Aufgaben<sup>33</sup>, einen weiteren Faktor in der Evaluation der Sinnhaftigkeit und Realisierbarkeit durch politische Diskurse darstellen.

Darüber hinaus ist die Führung und Verwaltung einer Blockchain nicht trivial und erfordert Fachpersonal mit speziellen Kenntnissen im Bereich der Informatik. Um umfangreiche Schulungen beziehungsweise Neueinstellungen käme man folglich nicht umher.

## 6. Fazit

Die Zahl der Einsatzmöglichkeiten von Smart Contracts auf staatlicher Ebene scheint beinahe endlos. Wenngleich die technischen Bedingungen noch nicht vollständig gegeben sind, eilt ihnen bisher ein großer Optimismus voraus. Ob dieser Berechtigt ist und welche Probleme bei einer Implementierung aufkommen, wird sich im Zuge einer umsetzungsorientierten Prüfung an den Einzelfällen zeigen. Dort wird auch geklärt werden, ob eine sichere und funktionierende Umgebungsarchitektur für Blockchainsysteme geschaffen werden kann, was

---

<sup>32</sup> Vgl. Schütte, J./Fridgen, G./Prinz, W. (2017) S.32

<sup>33</sup> Ebd.

wiederum nicht Gegenstand dieser Arbeit ist. An dieser Stelle herrscht also Forschungsbedarf, der aber vermutlich in näherer Zukunft durch Gutachter und Wissenschaftler gestillt werden wird. Spätestens dann wird sich zeigen, ob blockchaingestützte Smart Contracts halten können, was sie versprechen. Diese Arbeit soll einen ersten Zugang zur Materie liefern und einen Ausblick auf die Möglichkeiten und Fragen geben, die sich vom derzeitigen Forschungsstand her absehen lassen.

Barański, P. (2017): Blockchaintechnology and its potential in taxes, Deloitte

Meitinger, T. (2017): Smart Contracts, Informatik Spektrum Ausgabe 4/2017 S.373

Maurer, H.(2007): Allgemeines Verwaltungsrecht München: Verlag C.H.Beck

Säcker, F.(2015): Münchner Kommentar zum Bürgerlichen Gesetzbuch, Auflage 7. München: C.H.Beck

Ølnes, S.(2015): Beyond Bitcoin – Public Sector Innovation Using the Bitcoin Blockchain Technology

Swan, M. (2015): Blockchain – Blueprint for a New Economy, O'Reilly Media

Schütte, J./Fridgen, G./Prinz, W. (2017) BLOCKCHAIN UND SMART CONTRACTS München: Fraunhofer-Gesellschaft

Schlatt, V./Schweitzer, A./Urbach, N./Fridgen, G. (2016): Blockchain: Grundlagen, Anwendungen und Potenziale, Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik (FIT)

Walport, M. (2015): Distributed Ledger Technology: beyond block chain

## Onlinequellen

<http://www.patentanwalt.cc/2014/11/was-kostet-ein-patent.html> [21.08.19]

<https://www.recordskeeper.co/blog/centralized-vs-decentralized-blockchain/> [05.10.2018]

<https://www.economist.com/special-report/2015/05/09/the-next-big-thing> [05.10.2018]

<https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things> [05.10.2018]

<https://blockgeeks.com/guides/understanding-vyper/> [07.10.2018]

[https://medium.com/@John\\_Potter\\_XBY/the-problem-with-solidity-be7e6c277a58](https://medium.com/@John_Potter_XBY/the-problem-with-solidity-be7e6c277a58) [07.10.2018]

<https://vyper.readthedocs.io/en/latest/> [07.10.2018]

<https://berlinvalley.com/estland/> [11.10.2018]

<https://www.investinblockchain.com/estonia-blockchain-model/> [11.10.2018]

<https://medium.com/@lkolisko/do-we-need-mining-in-private-and-permissioned-blockchains-1a69b4c2c7a1> [11.10.2018]

<http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> [11.10.2018]

<https://e-estonia.com/solutions/e-governance/> [11.10.2018]

<http://www.rik.ee/en/other-services/e-notary> [11.10.2018]

<https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf> [11.10.2018]

[https://www.digitales.oesterreich.gv.at/documents/22124/403400/20170622-Blockchain-Village\\_BKA-Praesentation.pdf/6087cc17-4461-4b1b-a527-5bfd53703888](https://www.digitales.oesterreich.gv.at/documents/22124/403400/20170622-Blockchain-Village_BKA-Praesentation.pdf/6087cc17-4461-4b1b-a527-5bfd53703888) [23.10.2018]

<https://www.anlegen-in-immobilien.de/digitalisierung-in-der-immobilienbranche-taugt-die-blockchain-als-grundbuch-ersatz/> [24.10.2018]

<https://deutsche-wirtschafts-nachrichten.de/2018/06/17/schweden-will-verkauf-von-grundstuecken-mit-blockchain/> [24.10.2018]

<https://www.btc-echo.de/schweden-nutzt-jetzt-offiziell-die-blockchain-fuer-grundbucheintragungen/> [24.10.2019]

<https://www.lto.de/recht/hintergruende/h/blockchain-grundstuecksrecht-immobilien-verkauf-notare-grundbuch-transaktionen-sicherheit/> [24.10.2018]

<https://www.bitcoinblase.at/blockchain-grundbuch-georgien-und-schweden-vorn/>  
[24.10.2018]

[https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Sicherheit/sicherheit\\_node.html](https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Sicherheit/sicherheit_node.html) [24.10.2018]

<https://medium.com/@spireProtocol/blockchain-smart-contracts-will-revolutionize-voting-in-elections-acb5abc7beb6> [29.10.2018]

<https://www.bundeswahlleiter.de/service/glossar/o/online-wahlen.html> [30.10.2018]

<https://www.handelsblatt.com/politik/deutschland/bundestagswahl/alle-schlagzeilen/blockchain-wo-man-die-blockchain-schon-zum-abstimmen-einsetzen-kann/20366520-2.html?ticket=ST-2471207-9dpNEHEWpCMraD9eBcCg-ap6> [30.10.2018]

<https://www.btc-echo.de/blockchains-die-perfekte-teilloesung-fuer-wahlen/> [30.10.2018]

<https://www.capgemini.com/de-de/2017/03/blockchain-die-wundertechnologie-fuer-wahlen/> [30.10.2018]

## Selbständigkeitserklärung

Hiermit bestätige ich, Thees burfeind, diese Arbeit selbstständig und ohne fremde Hilfe verfasst zu haben. Insbesondere versichere ich, alle wörtlichen und sinngemäßen Übernahmen aus anderen Werken als solche kenntlich gemacht zu haben.

A handwritten signature in black ink, appearing to read 'T. Burfeind'. The signature is stylized and cursive.

Thees Burfeind

Leipzig, den 04.11.2018