Perspektivische Einsatzmöglichkeiten einer Blockchain in einer Landkreisverwaltung

B a c h e l o r a r b e i t
an der Hochschule für öffentliche Verwaltung und Rechtspflege (FH),
Fortbildungszentrum des Freistaates Sachsen
zum Erwerb des Hochschulgrades
Bachelor of Laws (LL.B.)

Vorgelegt von
Marc Junker
aus Lengenfeld

Meißen, 23.03.2020

Inhaltsverzeichnis

Abbildungsverzeichnis....3
Abkürzungsverzeichnis....3
1 Einleitung....4
2 Technische Grundlagen....6
2.1 Allgemein....6
2.2 Kryptografische Grundlagen und asymmetrische Verschlüsselung....7
2.3 Hashwert und Hashfunktion....8
2.4 Verwendung der Blockchain in Kryptowährungen....9
2.4.1 Blockerstellung....10
2.4.2 Blockstruktur und Berechnung des Hash-Wertes....10
2.5 Miningprozess....12
2.6 Proof of Work....12
2.7 Proof of Stake....15
2.8 Smart Contracts....15
2.9 Ausprägungen....16
2.9.1 Public/Private....16
2.9.2 Permissioned und Permissionless....17
2.10 Oracle Problem....17
2.11 Zusammenfassung....17
3 Projekte in Deutschland....18
3.1 Strategiepapier Bundesregierung....18
3.2 Koordinierungsprojekt Blockchain des IT-Planungrates....19
3.3 Blockchain Competence Center Mittweida....20
4 Aktueller Einsatz....20
4.1 „Krypto-Valley“ Kanton Zug (Schweiz)....21
4.2 E-residency (Estland)....23
4.3 Blockchain-basiertes Grundbuch in Schweden....23
5 Hyperledger....24
6 Zukünftige Einsatzmöglichkeiten in einer Landkreisverwaltung....25
6.1 Digitale Identitäten und Führerscheine....25
6.2 Grundbücher und Eigentumsverhältnisse....31
6.3 Wahlen....33
6.4 Kontrolle der Kühlkette mittels Blockchain....37
6.4.1 Technische Umsetzung mittels IBM Food Trust....39
6.4.2 Technische Umsetzung mittels Seafood Supply Chain....39
6.4.3 Technische Umsetzung mittels TradeLens....40
6.5 Bezahlung von Verwaltungsdienstleistungen mit Kryptowährungen....41
7 Fazit....43
Kernsätze....47
Literaturverzeichnis....48
Internetquellenverzeichnis....50
Eidesstattliche Versicherung....54

Abbildungsverzeichnis

Abbildung 1: Kollision einer Hashfunktion.....10
Abbildung 2: Hashbaum.....12

Abkürzungsverzeichnis

Abkürzung	Erläuterung
BAMF	Bundesamt für Migration und Flüchtlinge
BCCM	Blockchain Competence Center Mittweida
BMBF	Bundesministerium für Bildung und Forschung
IoT	Internet of Things (dt. Internet der Dinge, steht u. a. für die Vernetzung von Gegenständen)
NFC	Near Field Communication
PBFT	Practical-Byzantine-Fault-Tolerance
RBFT	Redundant-Byzantine-Fault-Tolerance
SSI	Self Sovereign Identity (dt. Selbstsouveräne Identität)
ZFER	Zentrales Fahrerlaubnisregister

1 Einleitung

Die Digitalisierung hält im Jahr 2020 in alle Bereiche des gesellschaftlichen Lebens Einzug. Dabei kommen immer neue Technologien zum Einsatz, deren Verwendung zumeist zu Zeitersparnis und Effizienzsteigerung führen kann, aber auch zu Problemen. Vor allem mangelnder Datenschutz spielt dabei eine erhebliche Rolle. Dabei ist die Nutzung von Daten für personalisierte Werbung bereits in vollem Gange. Zusätzlich geht auch die Angst vor Überwachung durch Staat oder Unternehmen in der Bevölkerung um. Auch die elektronische Abwicklung des Zahlungsverkehrs trägt zu dieser Sorge bei. Als Möglichkeit zur Anonymisierung von Zahlungen werden oftmals Kryptowährungen ins Spiel gebracht. Datenschutz und Anonymität wird bei dieser Art Währung teils fälschlicherweise als gegeben betrachtet, in der allgemeinen Wahrnehmung dienen diese Währungen (allen voran Bitcoin) in erster Linie dazu, Drogen und Waffenhandel über versteckte Online-Marktplätze abzuwickeln. Aber spätestens seit den extremen Kursschwankungen und dem Rekordhoch von Bitcoin Ende 2017 ist die Kryptowährung in aller Munde[1]. Doch was steckt eigentlich hinter den Kryptowährungen, und könnte diese Technologie nicht auch für andere Anwendungen eingesetzt werden?

Die Technologie hinter den Kryptowährungen ist die sog. Blockchain, eine Distributed-Ledger-Technologie (dt. „Verteilte-Datenbanken-Technologie). Erste Grundlagen zu dieser Technologie wurden Ende der 1990er Jahre entwickelt[2]. Der große Durchbruch gelang dieser Technologie aber erst im Jahr 2008, als eine Person unter dem Pseudonym Satoshi Nakamoto via E-Mail verkündete, an einem neuen elektronischen Geldsystem zu arbeiten, welches ohne eine vertrauenswürdige dritte Partei auskomme[3]. Die aktuell wohl bekannteste Kryptowährung Bitcoin war geboren. Es existieren jedoch auch weitere Anwendungsmöglichkeiten dieser Technologie, deren konkrete Funktionalität von Nakamoto für die Währung Bitcoin in einem Whitepaper konkretisiert wurde. Durch eine Reihe von Eigenschaften und Funktionalitäten bietet sich auch eine Verwendung in der öffentlichen Verwaltung an, welche die Bundesregierung in ihrem Strategiepapier zum Thema Blockchain teilweise aufgreift. Demnach sollen u. a. digitalisierte Verwaltungsdienstleistungen bereitgestellt werden, z. B. digitale Identitäten von Personen.

In dieser Arbeit sollen neben den technischen Grundlagen und Funktionsweisen auch Einsatzmöglichkeiten in der Verwaltung allgemein aufgezeigt werden. Um den aktuellen Stand der Entwicklung und Etablierung dieser Technologie in Deutschland sichtbar

[1] Vgl. https://www.faz.net/aktuell/finanzen/digital-bezahlen/kryptowaehrung-bitcoin-kurs-bricht-um-mehr-als-1000-dollar-ein-16402059.html (zuletzt geöffnet am 08.01.2020).
[2] Z. B. die Arbeit zum Thema: „Sichere Log-Dateien auf Grundlage kryptographisch verketteter Einträge“, abrufbar unter http://www.konst.de/stefan/seclog.pdf (zuletzt geöffnet am 03.02.2020).
[3] Vgl. https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html (zuletzt geöffnet am 04.02.2020).

zu machen, wird auch auf Projekte in Deutschland eingegangen, aus denen beispielsweise hervorgeht, dass die Forschung an der Blockchain auch von staatlicher Seite aus eine Rolle spielen soll. Es werden auch Anwendungen aus anderen Ländern aufgeführt, in denen die Digitalisierung der öffentlichen Verwaltung stärker fortgeschritten ist als in Deutschland. Nach Betrachtung dieser soll eine Ableitung zu potenziellen Verwendungen auf Verwaltungsebene der Landkreise erfolgen und auf die mögliche technische Umsetzung eingegangen werden. Dabei wird auch ein Augenmerk darauf gelegt, ob die Blockchain-basierte Lösung gegenüber der bestehenden Lösung Verbesserungspotenzial mit sich bringt, da nur dann der Mehraufwand für Entwicklung und Unterhaltung einer solchen Lösung gerechtfertigt wäre.

2 Technische Grundlagen

Bevor jedoch auf Anwendungsmöglichkeiten sowie -beispiele näher eingegangen wird, werden zunächst die technischen Grundlagen betrachtet.

2.1 Allgemein

In der Informationstechnik gibt es den Byzantinischen Fehler (auch genannt Problem der byzantinischen Generäle). Dieser beschreibt den Umgang mit Falschinformationen durch zuverlässige Computersysteme, ausgedrückt durch die abstrakte Situation der Belagerung einer Stadt durch mehrere Generäle, die sich untereinander nicht vertrauen. Um die Stadt einzunehmen, müssen sich die Generäle auf einen Schlachtplan einigen. Die Kommunikation erfolgt ausschließlich über Boten. Um Manipulationen des Schlachtplans durch einzelne Generäle zu vermeiden, kommen letztendlich nur fälschungssichere schriftliche Boten als Mittel der sicheren Kommunikation in Frage, da bei Verwendung mündlicher Botschaften bereits ein Anteil von einem Drittel verräterischer Generäle ausreicht, um den Schlachtplan zunichte zu machen und alle Generäle zu verwirren. Bei dieser Problemlösung handelt es sich um einen Konsensalgorithmus, wie er bei einer Blockchain zur Anwendung kommt, auch wenn dieser Algorithmus eigentlich für die Netzwerktechnik entwickelt wurde.[4]

Eine Blockchain benutzt demzufolge einen Konsensalgorithmus, um Manipulationssicherheit zu gewährleisten. Die Daten allerdings werden weiterhin in einer Datenbank gespeichert, wenn auch dezentral. Eine Blockchain ist somit eine Kombination aus einer dezentralen Datenbank und einem Konsensalgorithmus[5]. Eine umfassendere Definition gibt Julian Hosp: „Eine Blockchain ist eine digitale Datei, in der dieselbe Information von allen Mitgliedern einer Gesellschaft abgespeichert und Updates in regelmäßigen Zeitblöcken an die bereits bestehende Information gehängt werden, sodass jeder Teilnehmer die gesamte Information besitzt und sich nicht auf andere verlassen muss“[6]. Da die Technologie der Blockchain außerhalb der Kryptowährungen noch am Anfang ihrer Entwicklung steht, hat sich noch keine einheitliche Definition durchgesetzt[7]. Es muss aber zwischen der Blockchain als Datei und zwischen dem zugrunde liegenden System einer Netzwerkstruktur aus mehreren Teilnehmern unterschieden werden[8]. Die Blockchain als Datei an sich wird oft als eine Art Datenbank bezeichnet, in der die einzelnen Datensätze in Blöcke gruppiert werden, die dann mittels kryptogra-

[4]Vgl. Lamport, Shostak, Pease (1982, S. 383 ff.).
[5]Vgl. Meier, Stormer (2018, S. 1141).
[6]Hosp (2018, S. 42).
[7]Vgl. Swan (2015).
[8]Vgl. Schlatt et al. (2016, S.8).

fischer Signatur in bestimmter Reihenfolge miteinander verknüpft werden[9]. Diese Datenbank kann jeder der Teilnehmer in einem Netzwerk einsehen und ergänzen, aber nachträglich nicht mehr abändern. Außerdem wird eine zentrale Autorität im Netzwerk vermieden, alle Teilnehmer sind gleichberechtigt und verifizieren die Ergänzungen der Datenbank[10].

Zusammenfassend lässt sich festhalten: Eine Blockchain ist eine verteilte Datenbank, welche von mehreren Teilnehmern eines Netzwerks identisch gespeichert und regelmäßig aktualisiert wird. Die Einträge in der Datenbank bestehen dabei jeweils aus Blöcken, bei denen der nachfolgende Block den kryptografisch verschlüsselten vorangegangen Block enthält (Verkettung). Ein Ausfall eines Netzwerkteilnehmers behindert nicht die Abläufe im Netzwerk. Der Konsensalgorithmus stellt sicher, dass die Inhalte der Datenbank von allen Teilnehmern verifiziert, also auf Richtigkeit überprüft werden. Nachträgliche Änderungen der Inhalte sind nur mit extrem großen Aufwand möglich, da bei allen Netzwerkteilnehmern die gesamte Datenbank gleichzeitig geändert werden müsste, da durch kryptografische Verkettung jeder Eintrag (Block) auf dem vorhergehenden basiert.

2.2 Kryptografische Grundlagen und asymmetrische Verschlüsselung

Kryptografie bedeutet in etwa die Lehre vom Geheimen Schreiben. Es geht darum, einen Text (Klartext), der vom Sender verfasst wurde, in eine Form zu bringen, die für Dritte nur eine unverständliche Zeichenfolge darstellt (Chiffretext). Nur der Empfänger kann den Chiffretext mittels eines Schlüssels wieder in eine verständliche Form bringen. Die Verschlüsselung von Klartext in Chiffretext nennt man chiffrieren, die Entschlüsselung dechiffrieren. Der Schlüssel ist dabei das Regelwerk bzw. der Informationsträger, welches die Regeln für die Verschlüsselung bestimmt.[11]

Von einer symmetrischen Verschlüsselung spricht man, wenn zum Chiffrieren und zum Dechiffrieren derselbe Schüssel (Key) zum Einsatz kommt oder wenn sich ein Schlüssel leicht aus einem anderen berechnen lässt. Dabei ist die Übertragung des Schlüssels kritisch, diese muss über einen sicheren Weg erfolgen, da ein Abfangen des Schlüssels durch Dritte eine Verschlüsselung obsolet machen würde.[12]

Bei der sog. Public-Key-Verschlüsselung oder auch asymmetrischen Verschlüsselung (1976 von Diffie und Hellman[13] entwickelt) existieren zwei unterschiedliche Schlüssel für jeden Benutzer, ein privater Schlüssel und ein öffentlicher Schlüssel. Der öffentliche

[9]Vgl. Walport (2015, S.17).
[10]Vgl. Glaser, Bezzenberger (2015, S.8 ff.).
[11]Vgl. Wätjen (2018, S. 1 f.).
[12]Vgl. Wätjen (2018, S. 4).
[13]In New Directions in Cryptography. IEEE Trans. on Info. Theory IT-22 (1976), 644–654.

Schlüssel (Public Key) wird aus dem privaten Schlüssel (Private Key) berechnet; eine Umkehrung dieser Rechenoperation ist nicht möglich. Die verschlüsselte Kommunikation beruht auf dem Austausch der Public Keys. Der Sender verschlüsselt den Klartext der Nachricht mithilfe des öffentlichen Schlüssels des Empfängers, somit kann nur dieser die Nachricht mittels seines eigenen Private Key dechiffrieren. Dieser Vorgang ist auch unter umgekehrter Verwendung der Schlüssel möglich, allerdings unter dem Aspekt der Geheimhaltung des Nachrichtentextes sinnlos, da jeder mit Kenntnis des Public Key die Nachricht dechiffrieren könnte. Der Private Key muss sicher und vor Zugriffen Dritter geschützt aufbewahrt werden. Eine sichere Kommunikation zwischen Sender und Empfänger ist gewährleistet. Eine weitere Anwendungsmöglichkeit des Public-Key-Verfahrens sind digitale Signaturen. Diese dienen dem Nachweis der Authentizität einer Nachricht, d.h. der Sender einer Nachricht ist dadurch verifizierbar. Dazu muss der Sender die Nachricht mit seinem Private Key verschlüsseln (ohne das dieser veröffentlicht wird). Wird die Nachricht dann mit dem Public Key des vermeintlichen Versenders entschlüsselt, so muss sich ein sinnvoller Klartext ergeben, ansonsten stammt die Nachricht nicht vom entsprechenden Absender. Die Identität des Versenders kann mit diesem Verfahren bestätigt werden.[14]

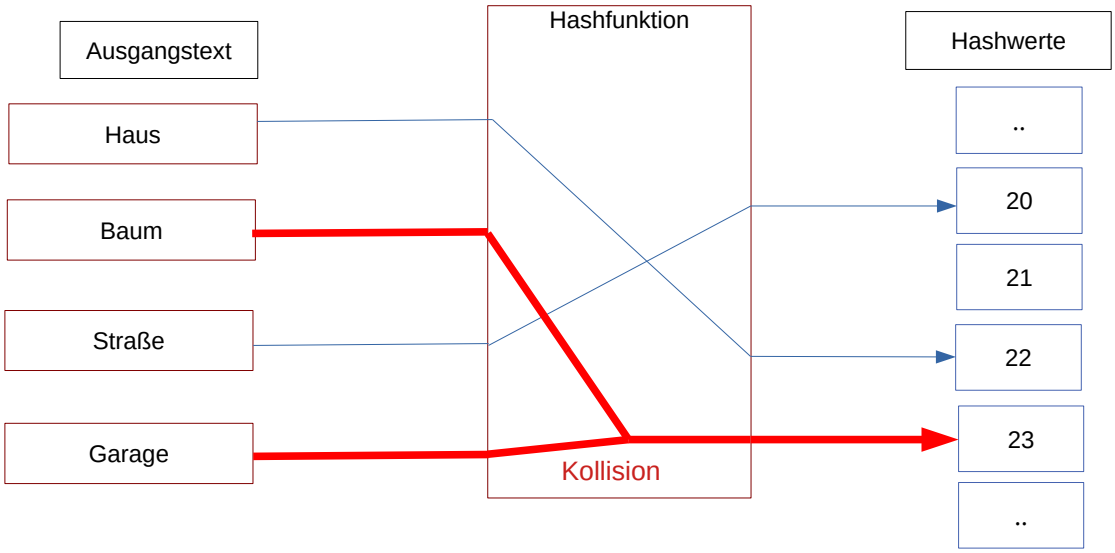
2.3 Hashwert und Hashfunktion

Ebenso von Bedeutung für eine Blockchain sind kryptografische Hashfunktionen. Hashen (engl.) bedeutet dabei in etwa soviel wie „zerhacken“. Dabei sollen Kollisionen (s. Abbildung 1) verhindert werden. Mittels einer Hashfunktion wird eine Prüfsumme bzw. Zusammenfassung von fester Länge (z.B: 256 Bit) für einen Ausgangstext von beliebiger Länge erzeugt. Es ist praktisch unmöglich, aus der Prüfsumme (Hashwert) den Ausgangstext zu berechnen, da dieser Hashwert eine nahezu eindeutige Kennzeichnung des Ausgangstextes darstellen soll. Ebenso soll es unmöglich sein zwei Ausgangstexte zu finden, die den selben Hashwert besitzen sowie aus einem Text samt Hashwert einen zweiten Text zu ermitteln, welcher den selben Hashwert ergibt. Werden diese beiden Bedingungen erfüllt, gilt die Hashfunktion als kollisionsfrei. Bei der Verwendung digitaler Signaturen wird im Regelfall auch nur die Prüfsumme mit dem Private Key des Senders verschlüsselt, da eine Verschlüsselung der gesamten Nachricht sehr zeitintensiv ist. Anschließend wird mittels derselben Hashfunktion ein Hashwert aus der Nachricht gebildet und mit dem zuvor durch den öffentlichen Schlüssel des Senders dechiffrierten Hashwert verglichen Bei Übereinstimmung ist die Authentizität des Absenders gewährleistet[15]. Die Aussagen beziehen sich auf einen klassischen

[14]Vgl. Wätjen (2018, S. 75 ff.).
[15]Vgl. Meier, Stormer (2018, S. 1143).

Computer, die Möglichkeiten eines funktionsfähigen Quantencomputers werden dabei außer Acht gelassen.[16]

Abbildung 1: Kollision einer Hashfunktion[17]



2.4 Verwendung der Blockchain in Kryptowährungen

Um die Funktionsweise einer Blockchain beispielhaft zu erläutern, soll im Folgenden die populärste Kryptowährung Bitcoin herangezogen werden. Mit Bitcoin sollte ein elektronisches Peer-to-peer-Währungssystem geschaffen werden, das Geldtransaktionen ohne eine dritte Partei (z. B. eine Bank) ermöglichet.

Ein Peer-to-peer-System (P2P-System) ist eine dezentrale Netzwerkarchitektur, bei der alle Knoten bzw. Teilnehmer (Peers) am Netzwerk direkt miteinander kommunizieren (ohne Umleitung über einen Server). Die Peers kommunizieren symmetrisch miteinander und können auch gemeinsam Daten nutzen. Diese Daten müssen redundant auf allen Peers im Netzwerk gespeichert werden, um bei Abwesenheit eines Peers weiterhin Vollständigkeit der Daten im Netzwerk zu gewährleisten. Da kein Server im Netzwerk vorhanden ist, müssen die Peers auch Infrastrukturaufgaben (z. B. Adresszuweisung) eigenständig wahrnehmen.[18]

Den Grundstein für die Entwicklung der Kryptowährung legte der Entwickler mit dem Pseudonym Satoshi Nakamoto mit seinem Artikel „Bitcoin: A Peer-to-Peer Electronic Cash System“. Dabei soll das Vertrauen, dass bei Geldtransaktionen in einen Dritten (in diesem Fall die Bank) vorhanden sein muss, durch kryptografische Beweise ersetzt werden. Eine Geldeinheit (sog. Bitcoin, kurz BTC) ist eine Aneinanderreihung von elek-

[16]Vgl. Wätjen (2018, S. 93 ff.).
[17]In Anlehnung an Jorge Stolfi.
[18]Vgl. Dunkel et al. (2008, S. 142 ff.).

tronischen Signaturen. Diese Signaturen stellen die Transaktionen dar, für welche der Bitcoin verwendet wurde. Demzufolge gibt es auch keine Kontostände, es wird lediglich die Summe aus den Transaktionen gebildet, um nachzuweisen, dass eine Ausgabe von vorhandenen Bitcoins möglich ist. Anweisungen von Transaktionen werden mittels den oben genannten Verschlüsselungsprinzipien authentifiziert. Eine Anweisung zu einer Transaktion wird im Netzwerk öffentlich gemacht und mit dem Private Key des Anweisungsgebers signiert. So ist die Authentizität der Anweisung sichergestellt, da niemand, der nicht den privaten Schlüssel des Anweisungsgebers besitzt, die Anweisung signieren kann. Die Herkunft der Anweisung kann mit dem öffentlichen Schlüssel durch jeden Peer überprüft werden. Empfänger und Absender werden nur durch die Hashwerte der jeweiligen öffentlichen Schlüssel identifiziert (im Prinzip Kontonummern bei herkömmlichen Währungssystemen). Will der Empfänger wiederum die erhaltenen Bitcoins weiterverwenden, veröffentlicht er nun ebenfalls eine signierte Anweisung, die zusätzlich noch enthält, dass die Bitcoins vorher erhalten wurden.[19]

2.4.1 Blockerstellung

Diese Transaktionen werden in regelmäßigen Zeitabständen in einem Block zusammengefasst. Dabei enthält jeder neue Block den Hashwert des vorangegangen Blocks. Dadurch kann eine Änderung der Blockinhalte durch Unbefugte im Nachhinein verhindert werden. Um die Funktion des Netzwerks zu gewährleisten, muss die regelmäßige Erstellung neuer Blöcke gewährleistet sein. Deshalb werden Bitcoins an diejenigen Peers ausbezahlt, die Ressourcen für die Erstellung neuer Blöcke bereitstellen. Nur mittels des öffentlichen Schlüssels überprüfte Transaktionen werden in einen Block aufgenommen. Ein Block enthält also den Hashwert des Vorgängerblocks sowie eine bestimmte Anzahl an Transaktionen. Dieser Block wird nun von anderen Peers überprüft und bei Korrektheit in die knoteneigene Kopie der Blockchain aufgenommen. Anschließend werden die neuen folgenden Transaktionen wiederum in einen neuen Block zusammengefasst. Die beschriebenen Vorgänge werden auch als Mining[20] bezeichnet und sichern die Akzeptanz der Blöcke und somit auch der Transaktionen durch das gesamte Netzwerk ab.[21]

2.4.2 Blockstruktur und Berechnung des Hash-Wertes

Ein Block in einer Blockchain besteht aus dem Block-Header und einem Hashbaum. Ein Hashbaum ist ein Baum aus den Hashwerten von Datensätzen einer Datei, dieser wurde von Ralph Merkle entwickelt und trägt deshalb auch den Namen Merkle Tree.

[19]Vgl. Böhme et al. (2015, S. 215 ff.).
[20]Auf den Miningprozess wird in Abschnitt 2.5 noch näher eingegangen.
[21]Vgl. Böhme et al. (2015, S. 215 ff.).

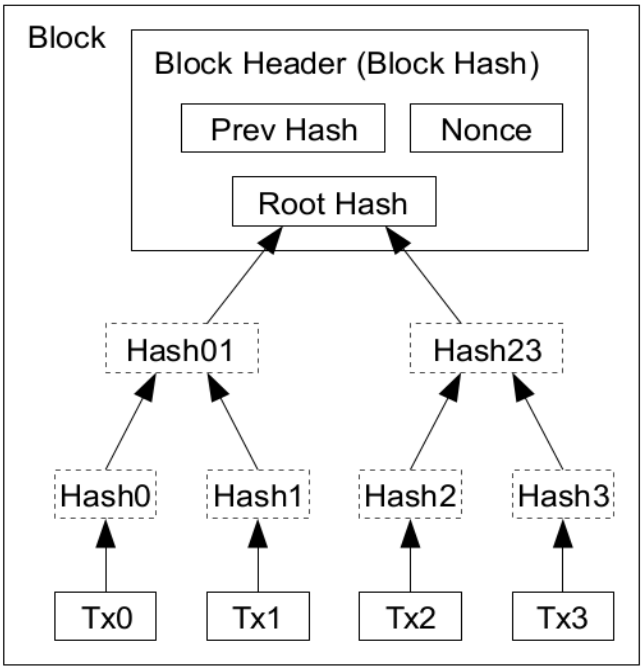
Bei der Bitcoin-Blockchain werden beispielsweise die Transaktionen 0 und 1 gehasht (es wird also die Hashfunktion berechnet), die jeweils Hash 0 und Hash 1 ergeben (siehe Abbildung). Um nun Hash 01 zu erhalten, werden die beiden Hashwerte 0 und 1 zusammen nochmals gehasht. Die Hashfunktion aus Hashwert 01 und Hashwert 23 ergibt den Root-Hash, der Teil des Block-Headers ist. Ebenfalls im Block-Header zu finden ist der Hashwert des Vorgänger-Blocks. Dies stellt sicher, dass Blockinhalte in einem Block nicht mehr geändert werden können, ohne alle vorhergehenden Blöcke zu ändern. Der Zeitstempel ist auch Teil des Block-Headers und gibt den Zeitpunkt der Block-Erstellung an. Im Header wird auch ein Schwierigkeitsgrad aufgeführt, der angibt, wie klein ein gültiger Hashwert sein muss. Dies wird realisiert, in dem die Anzahl Nullen, die am Anfang des Hashwertes stehen muss, festgelegt wird. Des weiteren existiert noch eine Nonce (Number used once). Diese muss per Zufallsverfahren variabel geändert werden, um einen gültigen Hashwert zu finden, der mit der vorgeschriebenen Anzahl an Nullen beginnt. Der Hashwert eines Blockes muss aus allen aufgeführten Inhalten berechnet werden.[22]

Ein Block-Header könnte also folgendermaßen Aussehen:

Hashwert	0000000000000000000a3e370954c035ee4f234fed9fcd34663b2611618c7115
Root-Hash	c7972e-ca48b63083532287a45003f857107e6cd-d42572455c536b6419f8cf101
Hashwert des Vorgänger-Blocks (Prev Hash)	0000000000000000000304ba1531985e9e53c80dc5f1636a3291ce54aedab47a
Zeitstempel	2020-02-12 17:50
Schwierigkeit	Vereinfacht: Die ersten 19 Stellen des Hashwertes müssen 0 sein.
Nonce	314.867.287

[22]Vgl. Meier, Stormer (2018, S. 1144 ff.).

Abbildung 2: Hashbaum[23]



2.5 Miningprozess

Das Erstellen neuer Blöcke ist zwingend notwendig für die Funktion einer Blockchain. Auch ist es durch die verteilte Topologie des Peer-to-Peer-Netzwerkes und der daraus resultierenden Datenübertragungsgeschwindigkeit notwendig, die Erstellung neuer Blöcke soweit zu verzögern, bis die Daten über neue Transaktionen bei allen Peers angekommen sind. Dieses Problem kann durch einen Proof-of-Work (dt. Arbeitsnachweis) gelöst werden.

2.6 Proof of Work

Der Proof-of-Work stellt in der Bitcoin-Blockchain das Finden der Nonce[24] dar, um die vorgeschriebene Größe des Hashwertes (Schwierigkeit) nicht zu überschreiten. Das Problem der Ermittlung einer gültigen Nonce lässt sich nur durch Ausprobieren verschiedener zufälliger Werte für die Nonce und dem anschließenden Berechnen des jeweiligen Hashwertes lösen, bis ein solcher Hashwert die vorgegebene Höchstgröße unterschreitet. Dies erfordert je nach Schwierigkeit einen erheblichen Rechenaufwand, der durch die dafür benötigte Zeit die Übertragung der Daten an alle Peers im Netzwerk sichert und löst somit das Problem der Netzwerkgeschwindigkeit. Durch die steigende Rechenleistung im Bitcoin-Netzwerk wird die Schwierigkeit kontinuierlich erhöht, damit im Schnitt nur alle zehn Minuten ein gültiger Hashwert gefunden wird. Die Berechnungen werden in der Regel von allen Peers im Netzwerk ausgeführt. Um die kon-

[23]Entnommen aus: Nakamoto (2008, S.4).
[24]Siehe Abschnitt 2.4.2

tinuierliche Erstellung neuer Blöcke zu gewährleisten und einen Anreiz zu schaffen, sich als Peer am Netzwerk zu beteiligen, erhält ein Knoten, der als erstes einen gültigen Wert findet, eine Belohnung. Dies geschieht dadurch, dass in einen Block eine Transaktion aufgenommen wird, bei welcher der Knoten selbst neue Bitcoins in vorgegebener Höhe an sich überträgt, diese sozusagen generiert. Ein neuer Block wird anschließend an andere Netzwerkteilnehmer gesendet und von diesen überprüft. Die Überprüfung besteht aus dem Ermitteln des Hashwertes des Blocks unter Verwendung der vom jeweiligen Peer vorgeschlagenen Nonce. Stimmen die Hashwerte überein und überschreitet der Block die Höchstgröße nicht, nimmt jeder Peer den Block in seine eigene Blockchain-Kopie auf und speichert diesen ab.[25]

Zusätzlich zur o. g. Kontrolle der Authentizität des Anweisungsgebers werden durch die Peers weitere Überprüfungen der in einem Block enthaltenen Transaktionen durchgeführt. Unter anderem wird überprüft, ob der Absender bei einer Transaktion die entsprechende Menge Bitcoins vorher erhalten hat, ob die Höhe der Belohnung für das Ermitteln eines korrekten Hashwertes mit den Vorgaben übereinstimmt. Erst wenn der Block durch die Peers vollständig verifiziert ist, wird dieser in die lokale Kopie der Blockchain übernommen.[26]

Ein Problem, welches in einer Blockchain durch den Proof-of-Work-Mechanismus gelöst wird, ist das sog. Double-Spending-Problem. Dieses tritt auf, wenn ein berechtigter Anweisungsgeber zwei Transaktionen zeitgleich bekanntgibt, die sich auf dasselbe Guthaben an Bitcoins bezieht. Angenommen, die Nachrichten über die Transaktionen verbreiten sich so ungünstig im Netzwerk, das ein Knoten die Nachricht über die erste Transaktion erhält, während ein zweiter Knoten die Nachricht über die zweite Transaktion zuerst erhält. Da die Transaktionen vom berechtigten Teilnehmer veröffentlicht wurden, stellen die Knoten bei der Überprüfung der jeweiligen Nachrichten keine Ungültigkeit fest. Jeder dieser Knoten nimmt nun die jeweils erhaltene Transaktionen in seinen Block auf und beginnt mit dem Suchen der Nonce. Wird diese von einem Knoten gefunden, sendet er seinen erstellten Block an alle anderen Teilnehmer im Netzwerk, die diesen nun überprüfen. Da dieser keine Fehler enthält, wird dieser von den Knoten in ihre Blockchain-Kopie aufgenommen, auch von jenem Knoten, der die andere Transaktion erhalten hat und seinen Block (der eben diese zweite Transaktion enthält) verwirft. Wird die zweite Transaktion, die sich (noch) nicht in einem Block befindet, nun von einem Knoten wieder aufgenommen und in einen neuen Block integriert, stellt dieser Knoten fest, dass der Anweisungsgeber nicht mehr über die entsprechenden

[25]Vgl. Berentsen, Schär (2017, S. 54 ff.).
[26]Vgl. ebenda (S. 205).

Bitcoins verfügt und nimmt diese Transaktion nicht in seinen Block auf, da er somit riskiert, dass die anderen Peers seinen Block nicht akzeptieren und er seine Belohnung nicht erhält. Somit ist dieses Problem mittels einer Blockchain gelöst.[27]

Eine weitere Vereinbarung der Knoten untereinander zur Erreichung eines Konsensus ist, dass die Peers nur die längste Blockkette als gültig akzeptieren[28]. Ein Angreifer, der eine Transaktion in einem weiter zurückliegenden Block zu seinen Gunsten ändern möchte, müsste zunächst den Hashwert von diesem Block und allen Folgenden neu berechnen (unter Berücksichtigung der entsprechenden Transaktion). Dabei müsste er die Geschwindigkeit der Erstellung neuer Blöcke, die das gesamte Netzwerk bereit stellt, übertreffen, um im Laufe der Zeit eine längere Kette zu berechnen, die dann von den anderen Knoten akzeptiert wird. Ein Angriff auf die Blockchain wäre also nur möglich, wenn der potenzielle Angreifer mehr als die Hälfte der Rechenleistung aller Peers zur Verfügung hat oder genügend Peers kontrolliert[29]. Dieser Weg eines potenziellen Angriffs wird durch den Arbeitsnachweis, der bei der Erstellung neuer Blocks notwendig ist, erheblich erschwert und ist bei der aktuellen Rechenleistung des Bitcoin-Netwerkes nahezu unmöglich.[30]

Zusammenfassend lässt sich sagen: Eine Blockchain besitzt durch die zugrunde liegende Netzwerkstruktur (Peer-to-Peer) und die Konsensusmechanismen ein hohes Maß an Fälschungssicherheit. Für Konsens sorgen dabei folgende Prinzipien:

Als erstes das Prinzip der Legitimität, welches durch Kontrolle der Transaktionen sowie allen sonstigen Inhalten die Richtigkeit dieser sicherstellt.

Als zweites Prinzip folgt die Verkettung der einzelnen Blöcke mittels Einbeziehung des Vorgänger-Blocks. Dies stellt sicher, dass die Änderung einer einzelnen zurückliegenden Transaktion die Neuberechnung aller folgenden Blöcke erfordert.

Dies steht in Verbindung mit dem dritten Prinzip, dem Arbeitsnachweis. Dieser sorgt dafür, dass die Erstellung neuer Blöcke mit einem Aufwand verbunden ist, sodass die Erstellung von Blöcken eine bestimmte Zeit sowie Rechenleistung erfordert.

Mit dem Proof-of-Work hängt auch die Schwierigkeit zusammen, die bei steigender Rechenleistung die Erstellung neuer Blöcke begrenzt. Um das fortlaufende Erstellen neuer Blöcke zu gewährleisten, wird ein Anreiz durch Entlohnung des erfolgreichen Peers geschaffen.

[27]Vgl. Berentsen, Schär (2017, S.57 ff.).
[28]In der Bitcoin-Blockchain trifft dies nicht zur Gänze zu, dort wird die Kette als legitim akzeptiert, deren Erstellung den höheren Rechenaufwand notwendig machte. Aufgrund der mangelnden Bedeutung für den übrigen Teil der Arbeit wird hier auf weitergehende Ausführung dieses Themas verzichtet.
[29]Vgl. Nakamoto (2008, S.4).
[30]Vgl. Berentsen, Schär (2017, S. 59 ff.)

Abschließend gilt noch das Prinzip der längsten Kette, sodass ein Angriff durch Nachberechnung aller Blöcke erschwert wird. Mittels dieser Algorithmen lässt sich ein Konsens erzeugen, der auch das eingangs erwähnte Problem der byzantinischen Generäle löst.

Neben der Kryptowährung Bitcoin existieren noch weitere solcher Währungen, welche auf den erläuterten Prinzip beruhen, allerdings mit geringen Änderungen. So gibt es z. B. die Kryptowährung Monero, deren Fokus auf Privatsspäre liegt[31], oder Litecoin, bei der die Erstellung neuer Blöcke schneller als im Bitcoin-Netzwerk erfolgt, was zu einer höheren Transaktionsgeschwindigkeit führt[32].

2.7 Proof of Stake

Da der Proof-of-Work-Mechanismus sehr energieintensiv für die jeweiligen Peers ist, gibt es eine Alternative namens Proof-of-Stake. Dieser Mechanismus wählt den Miner nach dem Anteil, den der Miner an der Kryptowährung (oder einer anderen Währung in der Blockchain, oftmals als Token bezeichnet[33]) besitzt aus. Dieser darf anschließend den neuen Block erzeugen, der sich einfacher erzeugen lässt als beim Proof-of-Work-Verfahren (geringere Schwierigkeit). Daneben existieren noch weitere Konsensverfahren, z. B. die praktische byzantinische Fehlertoleranz. Jedes dieser Verfahren besitzt entsprechende Vor- und Nachteile, auf nähere Erläuterung der einzelnen Verfahren wird an dieser Stelle verzichtet.[34]

2.8 Smart Contracts

Neben reinen Transaktionsdaten können noch weitere Inhalte in der Blockchain gespeichert und ausgeführt werden. Das Prinzip der Smart Contracts (dt. intelligente Verträge) wurde bereits entwickelt, als sich eine Blockchain noch nicht als Konsensmechanismus etabliert hatte. Sie stammt ursprünglich von Nick Szabo[35] und bezieht sich auf digitale Verträge, die selbstständig durch Eintreten einer Bedingung erfüllt werden. Es existiert eine weitere Kryptowährung mit erweitertem Funktionsumfang im Vergleich zu Bitcoin, die u.a. die Umsetzung von Smart Contracts ermöglicht. Die Währung trägt den Namen Ethereum und wurde von Vitalik Buterin entwickelt. Smart Contracts werden in der Ethereum-Blockchain als „kryptografische Boxen“ hinterlegt, die einen bestimmten Wert enthalten, der sich automatisch an eine vorher festgelegte Adresse aus-

[31]Vgl. https://web.getmonero.org/ (zuletzt geöffnet am 14.02.2020).
[32]Vgl. https://litecoin.org/ (zuletzt geöffnet am 14.02.2020).
[33]z. B. bei der Kryptowährung TRON (https://tron.network/static/doc/white_paper_v_2_0.pdf; zuletzt geöffnet am 14.02.2020).
[34]Vgl. https://medium.com/nakamo-to/what-is-proof-of-stake-pos-479a04581f3a (zuletzt geöffnet am 14.02.2020).
[35]Vgl. http://alamut.com/subj/economics/nick_szabo/smartContracts.html (zuletzt geöffnet am 14.02.2020).

zahlt, wenn eine Bedingung eingetreten ist[36]. Smart Contracts bestehen aus einem Vertrag zwischen zwei Parteien sowie dem in Blockchain hinterlegten Programmcode, dabei wird laufend geprüft, ob eine der Vertragsbedingungen eingetreten ist[37]. Es existierte eine Versicherung gegen Flugausfälle und Verspätungen des AXA-Konzerns, wobei die Zahlung der Entschädigung bei Eintritt des Versicherungsfalles durch einen Smart Contract auf der Ethereum-Blockchain ausgelöst wurde[38].Da Smart Contracts über eine Blockchain abgewickelt werden, ist eine Manipulation der Verträge mit erheblichem Aufwand verbunden. Es entstehen jedoch erhöhte Kosten, da die kontinuierliche Überprüfung der Bedingungen im Zuge der Erstellung neuer Blöcke Rechenleistung benötigt[39]. Problematisch bei Smart Contracts ist es, dass es sich um automatisiert überprüfbare Bedingungen handeln muss, da sonst weiterhin eine unabhängige dritte Instanz zur Überprüfung benötigt wird. Dies ist zum Beispiel notwendig, wenn die Qualität einer Arbeitsleistung oder ähnliches überprüft werden muss[40]. Auch das Oracle-Problem spielt hierbei eine Rolle, dazu aber mehr in Abschnitt 2.10. Aus rechtlicher Sicht stellen Smart Contracts Verträge mit Selbstvollzug dar, die nach Vertragsschluss automatisch die Rechtsfolge eintreten lassen.[41]

2.9 Ausprägungen

Für eine Blockchain existieren verschiedene Ausprägungen, die je nach Anwendungsfall verwendet werden können und jeweils Vorteile sowie Nachteile besitzen.

2.9.1 Public/Private

In der Bitcoin-Blockchain sind alle Anweisungsgeber für bestimmte Transaktionen durch die Hashwerte ihrer öffentlichen Schlüssel bekannt. Durch Nachverfolgung aller Transaktionen lässt sich unter bestimmten Umständen herausfinden, welche natürliche Person sich hinter einer solchen Adresse verbirgt. Die Transparenz einer Blockchain geht also in diesen Falle zu Lasten der Vertraulichkeit sowie des Datenschutzes.

Vertraulichkeit lässt sich aber in bestimmtem Maße wiederherstellen, indem nur ausgewählten Teilnehmern Zugang zu einer Blockchain gewährt wird. Dabei unterscheidet man zwischen Public und Private Blockchains. Während Public Blockchains allen Leserechte sowie jedem, der sich an der Erstellung neuer Blöcke beteiligen möchte, diese Rechte gewähren, sind bei Private Blockchains beide Rechte auf eine Gruppe von

[36]Vgl. https://github.com/ethereum/wiki/wiki/White-Paper (zuletzt geöffnet am 14.02.2020).
[37]Vgl. Tönnissen, Teuteberg (2018, S.1173 ff.)
[38]Vgl. https://fizzy.axa/en-gb/faq (zuletzt geöffnet am 14.02.2020).
[39]In der Ethereum-Blockchain erhalten die Miner bei Überprüfung eines Smart Contracts in einem Block eine gewisse Belohnung (in Kryptowährung), die bei der Erstellung des Contracts festgelegt wurde. Ein Smart Contract ist deshalb mit laufenden Kosten verbunden.
[40]Vgl. Schütz et al. (2018, S. 1164 ff.).
[41]Vgl. Tönnissen, Teuteberg (2018, S.1173 ff.)

Teilnehmern eingeschränkt. Dies führt zur Aufhebung der Transparenz für andere potenzielle Teilnehmer, die weder Blöcke erstellen können noch auf die Blockchain zugreifen können. Durch den eingeschränkten Teilnehmerkreis sind Daten auch nur für privilegierte Teilnehmer sichtbar, eine gewisse Vertraulichkeit ist damit gegeben.[42]

2.9.2 Permissioned/Permissionless

Das Mining (Berechnung eines gültigen Hashwertes) ist vor allem in der Bitcoin-Blockchain sehr energieintensiv[43], aber generell bei allen Blockchains, die das Proof-of-Work-Protokoll verwenden, prinzipbedingt verhältnismäßig hoch. Allerdings kann jeder Peer im Netzwerk sich am Mining beteiligen und neue Blöcke erzeugen, was zu hoher Manipulationssicherheit führt. Eine solche Blockchain nennt man Permissionless Blockchain (Genehmigungsfreie Blockchain). Wird das Recht, neue Blöcke zu erstellen, auf eine Gruppe von Peers beschränkt, spricht man von einer Permissioned Blockchain (Genehmigungspflichtige Blockchain). Diese Gruppe von Teilnehmern muss im Vorfeld anhand von festgelegten Kriterien ausgewählt werden. Die Geschwindigkeit der Erstellung neuer Blöcke kann somit durch eine Vereinfachung des Proof-of-Work gesteigert werden, führt jedoch zu Einbußen bei der Sicherheit der Blockchain, da ein kleinerer Teilnehmerkreis leichter von einem potenziellen Angreifer übernommen werden kann.[44]

2.10 Oracle Problem

Bei Verwendung von Smart Contracts müssen unter Umständen Bedingungen aus der Realität überprüft werden. Dies kann zu Problemen führen, wenn die Schnittstelle, über die die zur Kontrolle der benötigten Daten leicht manipulierbar ist. Verspätungen von Flügen stellen vermutlich höhere Anforderungen an eventuelle Manipulationen als ein einfacher Sensor, der z. B. die Temperatur misst. Die Bedingungen aus der Realität werden als Oracle bezeichnet, deshalb spricht man bei Problemen mit der Korrektheit dieser von einem Oracle-Problem.[45]

2.11 Zusammenfassung

Eine Blockchain ist eine verteilte Datenbank, die auf mehreren Computern in einem Netzwerk ausgeführt wird, welches in einer Peer-to-Peer-Struktur organisiert ist und durch verschiedene Konsensmechanismen Korrektheit, Manipulationssicherheit und Transparenz gewährleistet. Durch den Proof-of-Work, der die Manipulationssicherheit in erster Linie sicherstellt, entsteht allerdings ein nicht unerheblicher Energieaufwand.

[42]Vgl. Drescher (2017, S. 227)
[43]Die Bitcoin-Blockchain benötigt jährlich mehr Strom als das Land Österreich pro Jahr verbraucht. (Siehe https://www.zeit.de/2019/32/bitcoin-kryptowaehrung-energieverbrauch-kilowatt-stimmts [zuletzt geöffnet am 20.03.2020]).
[44]Vgl. Drescher (2017, S. 228).
[45]Vgl. Mahn (2019, S. 76).

Dieser kann durch Verwendung einer anderen Ausprägung der Blockchain minimiert werden, was aber zu Lasten des Schutzes vor Manipulationen geht. Durch die Transparenz einer verteilten Datenbank, die jeder Peer durchsuchen kann, sind Anforderungen an den Datenschutz nicht zu erfüllen. Wird der Zugang zur Blockchain eingeschränkt, kann Vertraulichkeit und Datenschutz besser gewährleistet werden, die Blockchain ist dann aber nur für den ausgewählten Teilnehmerkreis transparent. Es besteht eine Möglichkeit, intelligente Verträge (Smart Contracts) im Programmcode einer Blockchain unterzubringen, die bei Eintritt bestimmter Bedingung automatisch erfüllt werden. Smart Contracts profitieren von Transparenz und Manipulationssicherheit einer Blockchain, sind aber mit Kosten verbunden, die durch ständige Überprüfung der Vertragsbedingungen entstehen. Smart Contracts sind problematisch, wenn die Bedingung sich in der Realität nur eingeschränkt überprüfen und leicht manipulieren lässt.

3 Projekte in Deutschland

Da die Blockchain in der BRD von staatlicher Seite aus bisher nur wenig Beachtung fand, sollen nachfolgend einige Projekte vorgestellt werden, die zeigen, dass das Potenzial der Technologie mittlerweile auch hier erkannt wurde und von staatlicher Seite testweise genutzt wird. Auch auf die potenzielle Verwendung dieser in einer Landkreisverwaltung soll eingegangen werden.

3.1 Strategiepapier Bundesregierung

Die Blockchain-Strategie[46], welche die Bundesregierung am 18.09.2019 verabschiedete, thematisiert neben der Rolle der Blockchain im Finanzsektor und Pilotprojekten in verschiedenen Bereichen auch digitale Verwaltungsdienstleistungen. Unabhängig von diesen Verwaltungsdienstleistungen wird auch auf den Einsatz der Blockchain in Liefer- und Wertschöpfungsketten eingegangen, welche auch für die öffentliche Verwaltung in Bezug auf Lebensmittelüberwachung (z. B. Nachweis der lückenlosen Kühlkette bei Schlachttieren) und Steuererhebung relevant sein könnten.

Explizit erwähnt wird jedoch eine Veränderung des Identifikationsnachweises im Zulassungswesen, die aktuell geprüft wird. Problematisch sieht die Bundesregierung hier das hohe Vertrauensniveau in den Nachweis der Identität und den hiermit verbundenen Sicherheitsanforderungen.

Die Sicherheit einer Blockchain wird ebenfalls thematisiert. Dabei wird unter anderem auf das Dokument „Blockchain sicher gestalten. Konzepte, Anforderungen, Bewertun-

[46]Abrufbar unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=10

gen“[47] des Bundesamtes für Sicherheit in der Informationstechnik verwiesen. Darin wird unter anderem auf die Alternativen zum Proof-of-Work-Mechanismus sowie auf eine fehlende Standards verwiesen, um Kompatibilität verschiedener Systeme zu gewährleisten.

Für eine Landkreisverwaltung könnte auch die im Papier aufgeführte Blockchain-basierte Energieanlagenanbindung interessant sein. Erfolgt der Betrieb von Energieversorgungseinrichtungen durch Landkreise, könnte diese Option bei der Digitalisierung des Energiehandels eine Rolle spielen.

Als digitalisierte Verwaltungsdienstleistungen werden im Strategiepapier explizit nur digitale Identitäten von Personen sowie elektronische Vertrauensdienste erwähnt. Weiterhin wird eine staatliche Blockchain-Infrastruktur genannt, weitergehende Angaben dazu fehlen jedoch. Elektronische Vertrauensdienste sind in der eIDAS-Verordung der Europäischen Union geregelt und stellen bspw. Regelungen zur europaweiten Vereinheitlichung von elektronischen Zertifikaten, Siegeln und Zeitstempeln dar[48].

Weiterhin sieht die Bundesregierung keine Notwendigkeit darin, bereits bestehende Verwaltungsprozesse und Register durch Blockchain-basierte Anwendungen zu ersetzen, vor allem bei Verwendung der hinterlegten Daten durch staatliche Stellen. Möglichkeiten zur Anwendung werden in der Fahrzeughaltung sowie im Nachweis der Echtheit von Dokumenten (z. B. Urkunden) gesehen. Beispielhaft erwähnt werden Leuchtturmprojekte, die öffentlichkeitswirksam gefördert werden sollen, u.a. eine vom BAMF pilotierte Lösung zur Unterstützung der Kommunikation zwischen Behörden im Asylverfahren. Diese Anwendung könnte auch für eine Landkreisverwaltung interessant sein, da diese asyl- und ausländerrechtliche Angelegenheiten von Asylbewerbern und Flüchtlingen sowie Zahlung von Leistungen an diese Personengruppen wahrnimmt.

Zusammenfassend lässt sich sagen, dass die Bundesregierung den Trend zur Blockchain in verschiedenen Anwendungsfeldern erkannt hat. Dazu zählen unter anderem der Energiehandel, eine Plattform zum Identitätsnachweis sowie die Verifikation von Urkunden und anderen Dokumenten. Jedoch sind nur wenige konkrete Maßnahmen im vorliegenden Strategiepapier beschrieben, der größte Teil ist recht allgemein gehalten und die Umsetzung erscheint offen.

[47]Abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=5
[48]Vgl. Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates

3.2 Koordinierungsprojekt Blockchain des IT-Planungrates

Das Koordinierungsprojekt Blockchain[49] wurde vom IT-Planungsrat in einer Sitzung im März 2019 beschlossen. Der IT-Planungsrat ist ein zentrales Gremium für die förderale Zusammenarbeit in der Informationstechnik, geschaffen durch den IT-Staatsvertrag, der auf Grundlage des Art. 91 c Grundgesetz (GG) entwickelt wurde[50]. Projektziele sind unter anderem die Entwicklung einer deutschlandweiten Government-Chain und Nutzung dieser sowie die Verstärkung der Öffentlichkeitsarbeit. [51]

Die Anzahl der Projekte ist allerdings noch überschaubar und beschränkt sich größtenteils auf das Land Nordrhein-Westfahlen[52]. Insgesamt zeigt das Koordinierungsprojekt Blockchain bisher nur wenige Ansatzpunkte zur Entwicklung der Blockchain im öffentlichen Sektor in Deutschland.

3.3 Blockchain Competence Center Mittweida

Das Blockchain Competence Center Mittweida (BCCM) ist ein Institut der Hochschule Mittweida, welches als Ansprech- und Entwicklungspartner für Verwaltung und Privatwirtschaft fungiert. Zusätzlich zu Forschungs- und Entwicklungsprojekten sieht das Institut seine Aufgaben in der Initiierung von Start-ups.[53]

Ein Projekt des BCCM ist die Blockchain-Schaufenster-Region Mittweida, welches vom BMBF gefördert wird und sich bereits in der Umsetzungsphase befindet. Dabei sollen Blockchain-basierte Anwendungen innerhalb von Geschäftsprozessen getestet werden.[54]

Das BCCM sieht unter anderem die Bereitstellung einer Landesblockchain Sachsen als notwendig an. Vorteile werden dabei in der Attraktivität des Freistaates als innovativer Wirtschaftsstandort, in der Verwaltungsautomatisierung sowie in der geografischen Lage der notwendigen Infrastruktur gesehen. So können z. B. sicherheitsrelevante Daten in Deutschland bzw. Sachsen gespeichert werden, eine Nutzung von Rechenkapazitäten in den USA oder anderen Ländern ist dann nicht mehr notwendig. Auch sieht das BCCM weitergehende Anwendungen der Blockchain in der öffentlichen Verwaltung als die Bundesregierung, so z. B. in öffentlichen Registern wie dem Grundbuch.[55]

---

[49]Die Arbeitsergebnisse sollen unter https://dezentraleverwaltung.de abrufbar sein.
[50]Vgl. https://www.it-planungsrat.de/DE/ITPlanungsrat/RechtlicheGrundlagen/rechtliche_grundlagen_node.html (zuletzt geöffnet am 20.02.2020).
[51]Vgl. https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/30_Sitzung/Blockchain_Bericht.pdf?__blob=publicationFile&v=1 (zuletzt geöffnet am 20.02.2020).
[52]Vgl. https://dezentraleverwaltung.de/index.php/blockchain-projekte-in-deutschland/ (zuletzt geöffnet am 20.02.2020).
[53]Vgl. https://blockchain.hs-mittweida.de/ueber-uns/ (zuletzt geöffnet am 19.02.2020).
[54]Vgl. https://blockchain.hs-mittweida.de/bsrm/ (zuletzt geöffnet am 19.02.2020).
[55]Vgl. https://blockchain.hs-mittweida.de/wordpress/wp-content/uploads/2018/04/Landesblockchain_fuer_Sachsen.pdf (zuletzt geöffnet am 20.02.2020).

4 Aktueller Einsatz

Nachfolgend sollen einige Beispiele aus anderen Ländern erläutert werden, die zeigen, wie die Blockchain in der öffentlichen Verwaltung bereits verwendet wird.

4.1 „Krypto-Valley“ Kanton Zug (Schweiz)

Der Kanton Zug liegt zentral in der Schweiz und ist mit 126.837 Einwohnern (Stand 31.12.2018)[56] und 238,73 km² Fläche[57] der kleinste Kanton, hat aber mit ca. 500 EW pro km² eine relativ hohe Bevölkerungsdichte (Vergleich Sachsen: ca. 220 EW pro km²) und gilt als sehr wohlhabend[58].

Neben der Ansiedlung der Ethereum-Stiftung im Kanton Zug[59] existieren dort noch weitere Unternehmen, die sich mit Blockchain-Anwendungen beschäftigen. Einige haben sich in der Crypto Valley Association zusammengeschlossen, einer Vereinigung, welche vom Schweizer Staat unterstützt wird, um Blockchain-basierte Anwendungen zu erforschen und zu entwickeln[60]. Von der Crypto Valley Association wurde der Standort im Kanton Zug gewählt, weil das Kanton nur niedrige Steuern erhebt und ein unternehmensfreundliches Umfeld bietet[61]. Durch diese Standortfaktoren hat auch die lokale Verwaltung begonnen, diese Technologie in Verwaltungsprozesse zu implementieren. So können z. B. seit 2016 Bitcoins als Zahlungsmittel für bestimmte Leistungen der Stadtverwaltung Zug (bis 200 Schweizer Franken) verwendet werden[62]. Die direkte Zahlung erfolgt allerdings an einen Finanzdienstleister, welcher der Stadt den entsprechend Betrag in Schweizer Franken überweist[63].

Daneben wurde 2017 eine digitale Identität eingeführt. Sie ermöglicht Einwohnern der Stadt Zug, ihre Identität elektronisch nachzuweisen. Diese digitale Identität basiert auf der Ethereum-Blockchain (siehe oben). Benutzer dieser Identität müssen sich online registrieren und eine App auf ihr Smartphone herunterladen. Die Überprüfung der Identität erfolgt durch die Stadt Zug. In diesem Prozess werden die bei der Online-Registrierung angegebenen Daten überprüft und mit dem physischen Ausweis bzw. Pass verknüpft. Verwendet werden kann die digitale Identität z. B. bei allen elektronischen

[56]Vgl. https://www.bfs.admin.ch/bfs/de/home/statistiken/bevoelkerung/stand-entwicklung.assetdetail.9447644.html (zuletzt geöffnet am 20.02.2020).
[57]Vgl. https://www.zg.ch/portraet/kennzahlen (zuletzt geöffnet am 20.02.2020).
[58]Vgl. https://www.srf.ch/play/tv/reporter/video/die-vertreibung-aus-dem-paradies-wie-zug-den-zugern-allmaehlich-abhanden-kommt?id=c96dcd39-f98a-47aa-a6d9-345e907283bc (zuletzt geöffnet am 20.02.2020).
[59]Vgl. https://docs.ethhub.io/ethereum-basics/ethereum-foundation/ (zuletzt geöffnet am 22.02.2020).
[60]Vgl. https://cryptovalley.swiss/about-the-association/ (zuletzt geöffnet am 22.02.2020).
[61]Vgl. https://cryptovalley.swiss/why-switzerland/ (zuletzt geöffnet am 22.02.2020).
[62]Vgl. https://www.stadtzug.ch/newsarchiv/321666 (zuletzt geöffnet am 22.02.2020).
[63]Vgl. https://www.heise.de/newsticker/meldung/Im-tiefen-Tal-der-Kryptowaehrungen-Ein-Besuch-in-Zug-3760567.html?seite=all (zuletzt geöffnet am 22.02.2020).

Behördendienstleistungen sowie beim Ausleihen von Fahrrädern und beim Ausleihen von Büchern aus der Bibliothek.[64]

Im Jahr 2018 wurde Testlauf für das sog. E-Voting durchgeführt. Dies erfolgte mittels einer Probeabstimmung, welche als Umfrage zum Blockchain-basierten Wahlverfahren gestaltet wurde. Der Wahlprozess gestaltete sich folgendermaßen:

Jeder Wahlberechtigte muss im Besitz einer gültigen digitalen Identität sein. Anschließend erarbeitet die Wahlbehörde die Wahlvorlage als Liste mit Auswahlmöglichkeiten. Die Abstimmungsdauer und der Wählerkreis wird ebenso bestimmt. Der Wähler logt sich in das entsprechende Wahlportal ein und fordert seinen Stimmzettel an. Die Authentifizierung erfolgt mittels dem der digitalen Identität zugeordneten öffentlichen Schlüssel. Der Wähler hat die Möglichkeit, einen eigenen Peer im Blockchain-Netzwerk zu betreiben, über den der Abstimmungsprozess erfolgt, falls er den anderen Peers nicht vertraut. Die Wahlbehörde authentifiziert den Wähler und übermittelt den Stimmzettel. Der ausgefüllte Stimmzettel wird vom Wähler mit seinem privaten Schlüssel signiert. Der Stimmzettel selbst wird mit dem öffentlichen Schlüssel der Wahlbehörde verschlüsselt, sodass nur diese den Inhalt entschlüsseln kann. Die ausgefüllten Stimmzettel werden in der Blockchain dezentral gespeichert. Nach Ende der Abstimmung werden die Stimmzettel von der Wahlbehörde abgerufen und nach Überprüfung der Signaturen ausgewertet. Anhand der Signatur kann die Wahlbehörde die Identität des Wählers überprüfen. Nach Veröffentlichung der Wahlergebnisse können alle Peers die Resultate überprüfen, da die Wahlbehörde diese mittels eines Zero-Knowledge-Protokolls[65] auf der Blockchain veröffentlicht hat. Auch der einzelne Wähler kann prüfen, ob sein Stimmzettel korrekt ausgewertet wurde. Vorteile gegenüber herkömmlichen Wahlverfahren sind in mehreren Faktoren zu finden. So ist z. B. die Veränderung der einmal abgegebenen Daten, welche in der Blockchain gespeichert werden, nachträglich nur sehr schwer möglich. Auch der Identitätsnachweis mittels Blockchain-basierter Identität ist durch die beinahe Unmöglichkeit von Manipulationen schwieriger als bei herkömmlichen E-Voting-Systemen, die Daten nicht auf einer Blockchain speichern. Auch das Vertrauen in das E-Voting-System durch die Wähler kann höher sein, wenn diese die technischen Grundlagen verstehen und bewerten können. Ein weiterer Vorteil ist die Transparenz und die Kontrollmöglichkeit durch die Wähler. Insgesamt bietet das Blockchain-basierte E-Voting-System deutlich mehr Sicherheit und Transparenz als herkömmliche Wahlsysteme, ob elektronisch oder analog.[66]

[64]Vgl. https://www.stadtzug.ch/newsarchiv/431448 (zuletzt geöffnet am 22.02.2020).
[65]Dabei handelt es sich um ein kryptografisches Protokoll, bei dem eine Partei die andere Partei davon überzeugen kann, ein Geheimnis zu kennen, ohne das Geheimnis dabei preiszugeben.
[66]Vgl. https://www.stadtzug.ch/_docn/1939723/eVoting_Stadt_Zug_Abschlussbericht_DE.pdf (zuletzt geöffnet am 22.02.2020).

Die Schweiz bietet mit dem Kanton Zug ein ideales Ökosystem zur Ansiedelung aufstrebender IT-Unternehmen. Dabei spielen die niedrigen Steuern eine Rolle, aber auch mangelnde gesetzliche Regelungen für Kryptowährungen, was den betreffenden Unternehmen große Spielräume lässt[67]. Durch die große Anzahl an Unternehmen vor Ort wurde es auch der lokalen öffentlichen Verwaltung ermöglicht, neue Projekte mit erfahrenen Partnern anzugehen (z. B. die Zahlung von Verwaltungsgebühren in Bitcoins).

4.2 E-residency (Estland)

Estland als flächenmäßig kleinster Staat des Baltikums hat ca. 1,3 Mio Einwohner[68]. Nach dem Zerfall der Sowjetunion wurde Estland wieder selbstständig und entwickelte sich schnell zum Vorreiter in Sachen digitale Verwaltung. Eine weitere Besonderheit an Estland ist der verfassungsmäßig garantierte Internetzugang für jeden Einwohner und viele freie Internetzugänge, die über das ganze Land verteilt sind. Deshalb war es möglich, viele Verwaltungsdienstleistungen online anzubieten. Aber nicht nur Einheimische können von den digitalen Dienstleistungen anbieten. Mit der E-residency, einer Art elektronischer Staatsbürgerschaft, ist es auch für Einwohner anderer Länder möglich, die digitalen Dienstleistungen zu nutzen. Der Interessent erhält gegen Zahlung einer Gebühr eine Smartcard samt zugehörigen Lesegerät, mit welcher er sich online identifizieren kann. Dabei sind besonders die einfachen und wenig zeitaufwändigen Unternehmensgründungen interessant, auch da manche Unternehmensformen nur ein geringes Startkapital erfordern.[69]

Es herrscht allerdings Uneinigkeit darüber, ob die digitale Identität in Estland mittels Blockchain vor Manipulationen geschützt wird, was bei der elektronischen Patientenakte der Fall ist[70]. Während manche Quellen davon ausgehen[71], widerlegen andere diese These[72]. Sicher ist jedoch, das Estland einen der fortschrittlichsten Verwaltungsapparate der ganzen Welt besitzt.

4.3 Blockchain-basiertes Grundbuch in Schweden

In Schweden hat das Lantmäteriet (die schwedische Behörde für Kataster und Grundbuch) mit weiteren Partnern ein Projekt zur Blockchain-basierten Grundbuchführung initiiert. Als Partner fungierte dabei unter anderem die Firma ChromaWay, welche den Prozess des Eigentümerwechsels einer Immobilie in 34 Schritte gliederte. In diesem

[67]Vgl. https://www.heise.de/newsticker/meldung/Im-tiefen-Tal-der-Kryptowaehrungen-Ein-Besuch-in-Zug-3760567.html?seite=all (zuletzt geöffnet am 22.02.2020).
[68]Stand: 31.12.2019.
[69]Vgl. Prause (2018, S.14 ff.).
[70]Vgl. https://www.gg-digital.de/2019/06/ein-kleines-land-schreibt-e-health-gross/index.html (zuletzt geöffnet am 25.02.2020).
[71]Vgl. Jacobovitz (2016, S. 3 f.)
[72]Vgl. https://hackernoon.com/e-estonia-is-not-on-blockchain-22iy2gx6 (zuletzt geöffnet am 25.02.2020).

Prozess sah Chromaway einige Nachteile, z. B. die späte Einbeziehung der Behörde, die Langwierigkeit des Prozesses sowie der Informationsaustausch via Brief und herkömmlicher Email. Durch Digitalisierung des Prozesses kann die Dauer deutlich verkürzt werden und die Sicherheit gesteigert werden, die Grundbucheintragung könnte sogar automatisiert werden.

Beim dem durch ChromaWay angebotenen Verfahren bleibt das Grundbuch (in diesem Fall in der digitalen Form) bestehen und wird mittels den in der Blockchain hinterlegten Änderungen gemäß den gesetzlichen Bestimmungen aktualisiert. Die Software hinter dieser Blockchain ist open-source und wird vom Lantmäteriet und weiteren Peers überprüft und ausgeführt. Jede Änderung des Status einer Immobilie ist für alle Teilnehmer der Blockchain sichtbar, dazu gehören der Makler, der Käufer sowie der Verkäufer und die Behörde (eine Bank kann bei Finanzierung der Immobilie ebenfalls dazugehören). In der Blockchain werden Echtheitsnachweise der Dokumente (z. B. Kaufvertrag) gespeichert. Durch die dezentrale Speicherung der Daten ist Ausfallsicherheit bei gleichzeitiger Transparenz durch Sichtbarkeit der Daten für alle Beteiligten gewährleistet. Das Blockchain-basierte Grundbuch bietet somit mehr Sicherheit und Transparenz bei der Immobilienübertragung.

5 Hyperledger

Hyperledger Fabric (auch kurz Fabric) ist eine modulare Open-Source-Blockchain-Plattform. Dieses wird mittlerweile von der Linux Foundation entwickelt und ist für ein breites Spektrum von Anwendungen einsetzbar[73]. Es handelt sich um eine Permissioned Blockchain, die eigentlich für den Einsatz in Unternehmen entwickelt wurde. Gegenüber anderen Lösungen bietet Hyperledger Fabric einige Vorteile, unter anderem können Smart Contracts (die hier Chaincodes heißen) in gängigen Programmiersprachen wie z. B. Java programmiert werden. Diese enthalten auch den Programmcode zur Ausführung der Blockchain. Es können zudem verschiedene Konsensalgorithmen verwendet werden.[74]

In Hyperledger-Fabric-Netzwerken gibt es zwei Arten von Knoten. Auf der einen Seite den normalen Peer-Knoten, welcher Transaktionen der Teilnehmer aufnimmt und eine Kopie der Blockchain speichert. Daneben gibt es Ordering-Service-Knoten, die für den Konsensalgorithmus zuständig sind und die Kommunikation im Netzwerk steuern.[75]

[73]Vgl. https://wiki.hyperledger.org/display/fabric (zuletzt geöffnet am 27.02.2020).
[74]Vgl. https://hyperledger-fabric.readthedocs.io/en/release-1.4/whatis.html (zuletzt geöffnet am 27.02.2020).
[75]Vgl. https://hyperledger-fabric.readthedocs.io/en/release-1.4/arch-deep-dive.html (zuletzt geöffnet am 28.02.2020).

Teilnehmer einer Blockchain haben bestimmte Identitäten und identifizieren sich mit Zertifikaten. Datenschutz und Vertraulichkeit sind somit hergestellt, da es sich dadurch um eine Permissioned Blockchain handelt. Für die Verwaltung der Teilnehmer und der Zertifikate existiert ein spezielles Modul im Fabric-Baukasten. Die Werte (dies können Gegenstände sein), die auf der Blockchain verwaltet werden sollen, werden als Assets bezeichnet. Die Assets werden als Schlüssel-Werte-Paare gespeichert und können mittels Chaincode verändert werden. Änderungen an Assets werden im Netzwerk öffentlich gemacht und werden bei Akzeptanz durch die anderen Teilnehmer in ihre Kopie der Blockchain übernommen. In einem Netzwerk lassen sich verschiedene Channels erstellen, die Gruppen von Teilnehmern voneinander abgrenzen. Für jeden Channel wird dabei eine eigene Datenstruktur geführt. So ist es möglich, Datenschutz zu gewährleisten, auch wenn die selbe Netzwerkstruktur verwendet wird. Somit eignet sich Fabric eher für eine gegenstandsbezogene Blockchain, bezogen auf die Landkreisverwaltung wären dies z. B. Grundbücher oder Lebensmittel.[76]

Im Hyperledger-Projekt werden noch weitere Lösungen entwickelt, so z. B. Hyperledger Indy. Diese Open-Source-Lösung bietet Werkzeuge, Bibliotheken und weitere Komponenten zur Bereitstellung Blockchain-basierter digitaler Identitäten[77]. Auch die oben erwähnte digitale Identität des Kanton Zug basiert auf dem Hyperledger-Projekt[78].

6 Zukünftige Einsatzmöglichkeiten in einer Landkreisverwaltung

Im folgenden Teil sollen zukünftige Einsatzmöglichkeiten in einer Landkreisverwaltung aufgezeigt werden. Dabei soll bei jeder potenziellen Anwendung auf die bestehenden Probleme der aktuellen Abläufe eingegangen werden und auf die Vorteile, die eine Blockchain-basierte Lösung mit sich bringen würde. In einem abschließenden Vergleich wird die bestehende mit der neuen Lösung verglichen und auf eine wirkliche Verbesserung hin überprüft. Als abschließender Punkt soll eine reale Möglichkeit zur Umsetzung der Blockchain-Lösung aufgezeigt werden.

6.1 Digitale Identitäten und Führerscheine

Wie bereits in 4.1 angeführt, existiert für Einwohner der Stadt Zug eine digitale Identität. In der Bundesrepublik Deutschland liegt diese Aufgabe gemäß dem Gesetz zur Ausführung des Pass- und Personalausweisgesetzes im Freistaat Sachsen bei den Gemeinden. Die Landkreise sind hier in erster Linie nicht zuständig. Der Bürger muss sich jedoch bei fast allen Dienstleistungen, die er von einer Landkreisverwaltung in An-

[76]Vgl. https://www.informatik-aktuell.de/betrieb/virtualisierung/eine-blockchain-anwendung-mit-hyperledger-fabric-und-composer.html (zuletzt geöffnet am 28.02.2020).
[77]Vgl. https://wiki.hyperledger.org/display/indy/Hyperledger+Indy (zuletzt geöffnet am 28.02.2020).
[78]Vgl. https://www.it-markt.ch/news/2018-06-25/zug-steigt-mit-der-blockchain-in-den-e-voting-ring (zuletzt geöffnet am 28.02.2020).

spruch nimmt, mittels geeignetem Dokument identifizieren. Dies ist in erster Linie der Personalausweis, manchmal auch der Reisepass. Auch der Führerschein ist mit der Identität einer Person verbunden, allerdings wird dieser in der Regel nicht zum Identitätsnachweis benutzt, sondern nur zum Nachweis der Berechtigung zum Führen von Kraftfahrzeugen. Der physische Führerschein (meist im Scheckkartenformat) ist nicht gleichzusetzen mit der Fahrerlaubnis. Der Führerschein darf gemäß § 25 Abs. 1 Nr. 3 Fahrerlaubnisverordnung (FeV) nur derjenigen Person ausgestellt werden, die eine gültige Fahrerlaubnis besitzt. Hier besteht Missbrauchspotenzial. Beim Entzug der Fahrerlaubnis muss sichergestellt werden, dass auch der physische Führerschein eingezogen wird. Wenn dieser jedoch von der betroffenen Person nicht freiwillig abgegeben wird und bei einer richterlich angeordneten Hausdurchsuchung nicht aufgefunden wird, besteht das Problem, dass der Führerschein weiterhin im Umlauf ist und missbräuchlich benutzt werden kann. Die Problematik besteht auch, wenn ein Ersatzführerschein ausgestellt wurde, da der oder die Betroffene durch eine Falschaussage den Führerscheinverlust gesetzeswidrig meldete. Auch dann ist ein weiterer Führerschein im Umlauf, obwohl der Betroffene keine Fahrerlaubnis mehr besitzt. Behörden sind hiervon jedoch nicht betroffen, da sie durch das Zentrale Fahrerlaubnisregister (ZFER)[79] Kenntnis über den Besitz einer Fahrerlaubnis erlangen. Problematisch wird dies vor allem bei einer Fahrzeuganmietung für den Vermieter, welcher fälschlicherweise davon ausgeht, das der Mieter im Besitz einer gültigen Fahrerlaubnis ist, wenn er den physischen Führerschein vorlegt. Dieses Problem könnte man mittels eines Blockchain-basierten Führerscheinregisters lösen.

Fraglich ist jedoch, ob es nicht einfacher wäre, dem Fahrzeugvermieter Zugriff auf das ZFER oder eine beschränkte Version dessen zu gewähren. Bei einem reinen Auskunftssystem über eine gültige Fahrerlaubnis wäre der Aufwand für eine Blockchain-Lösung nicht notwendig. Es könnte einfach ein zentrales System geschaffen werden, bei dem der Vermieter Zugriff auf ein Interface erhält, welches das ZFER ausliest und relevante Daten (gültige Fahrerlaubnisklassen) weitergibt. Um Missbrauch zu verhindern, könnte man eine Genehmigung bei der betreffenden Person (Mieter) anfordern (z. B. per Mail oder online), sodass nur dann die Daten weitergegeben werden, wenn der Mieter damit einverstanden ist. Der Aufwand für eine Blockchain-basierte Lösung wäre nur dann sinnvoll, wenn eine Kopplung der Fahrerlaubnis mit der digitalen Identität erfolgt.

Solche digitalen Identitäten können nach dem Konzept einer Self Sovereign Identity (dt. Selbstsouveräne Identität, kurz SSI) verwirklicht werden. Eine SSI wird von ihrem

[79]Vgl. https://www.kba.de/DE/ZentraleRegister/ZFER/zfer_node.htmlgl (zuletzt geöffnet am 03.03.2020).

Besitzer (z. B. dem Bürger) in einem sog. Identity Wallet gepflegt. Dazu gehören Name, Wohnsitz und eben auch der Führerschein. Diese Daten liegen als Kopien mit Echtheitszertifikat vor. Will der Bürger einen Dienst in Anspruch nehmen und sich dabei authentifizieren, kann er dies mit der SSI tun und dabei individuell bestimmen, welche Daten er an den Diensteanbieter weitergibt. Somit kann eine Identität für mehrere Dienste verwendet werden, anders als bei der heute verbreiteten Art und Weise, für jeden Dienst ein separates Benutzerkonto mit oftmals redundanten Daten zu erstellen.[80]

Zur technischen Umsetzung bietet sich das Projekt Hyperledger Indy an. Durch den frei verfügbaren Quellcode kann dieser von technisch versierten Bürgern eigenständig geprüft und bewertet werden. Das leistet einen wichtigen Beitrag zur Akzeptanz einer Blockchain-basierten digitalen Identität in der Bevölkerung. Außerdem entstehen keine zusätzlichen Kosten durch den käuflichen Erwerb einer Software. Lediglich die Implementierung und Anpassung dieser zieht finanzielle Ausgaben nach sich.

Hyperledger Indy (kurz: Indy) ist eine Distributed-Ledger-Software[81]. Der Begriff Distributed Ledger (dt. verteiltes Hauptbuch) wird als Oberbegriff für verschiedene Blockchain-ähnliche Techniken gesehen, welche alle ein dezentrales System zur Validierung von Transaktionen darstellen. Unterschiede bestehen im Konsensalgorithmus sowie bei Zugriffs- und Schreibrechten[82].

In Indy laufen die Transaktionen zwischen sog. Nodes (Knoten) ab. Mehrere Nodes bilden einen Pool. Erst wenn sich eine Node mit einem Pool verbunden hat, ist es der Node möglich, Transaktionen zu lesen und zu erstellen. Einige Knoten bekommen die Rolle eines Trust Anchor (dt. Vertrauensanker). Trust Anchor kann nur werden, wer durch einen anderen bereits vorhandenen Trust Anchor zu einem solchen ernannt wird. Als Trust Anchor kann man DIDs (Decentraliced Identifier, eine Art Schlüssel) veröffentlichen. Ein DID ist mit einem Identitätsdatensatz verknüpft, also den Daten, die bei Weitergabe der Identität weitergegeben werden. Ein Identitätsbesitzer (z. B. ein Bürger) kann mehrere DIDs besitzen, um bei bestimmten Verwendungen seiner digitalen Identität anonym zu bleiben. Es gibt auch DIDs, die mit der Rechtspersönlichkeit des Identitätsbesitzers gekoppelt sind, welche von den Entwicklern von Indy Verinyms genannt werden. Diese Daten werden in einem Wallet (dt. Brieftasche) gespeichert. Um eine DID zu erstellen und diese im Netzwerk bekannt zu machen, ist eine Transaktion notwendig. Eine solche Transaktion wird NYM-Transaktion genannt und kann neben der Erstellung von DIDs noch für weitere Aktionen verwendet werden.

[80]Vgl. Next e.V. (2019, S. 5 ff.).
[81]Näheres dazu auch unter 5.
[82]Vgl. Kannengießer et al. (2019, S. 1 ff.).

Als Konsensalgorithmus verwendet Hyperledger Indy weder Proof-of-work noch Proof-of-stake, sondern den Redundant Byzantine Fault Tolerance Algorithmus (dt. Redundanter Byzantinischer-Fehlertoleranz-Algorithmus, kurz RBFT), der im Kernmodul von Indy Anwendung findet[83]. Anders als beim Practical Byzantine Fault Tolerance Algorithmus (dt. Praktischer Byzantinischer-Fehlertoleranz-Algorithmus, kurz PBFT) werden beim RBFT mehrere PBFT-Algorithmen nebeneinander ausgeführt, welche es möglich machen, einen bösartigen Leitknoten zu erkennen[84].

Ein PBFT-Algorithmus funktioniert in einem Netzwerk aus mehreren Knoten, wobei es einen Leitknoten gibt, welcher die Anfragen koordiniert, dabei aber in bestimmten Zeitabständen wechselt. Diese Anfragen kommen von einem Clienten, der zunächst die Anfrage an den Leitknoten stellt. Dieser gibt die Anfrage an alle anderen Knoten weiter. Diese führen die Anfragen aus und geben das Ergebnis der Anfrage an den Clienten zurück. Der Client wartet auf eine gewisse Anzahl Nachrichten von den Knoten, dabei muss er immer eine Nachricht mehr erhalten, als bösartige Knoten existieren. Ein bösartiger Knoten kann nicht mehrere Nachrichten an den Klienten schicken, da Nachrichten mit einer fälschungssicheren Signatur des jeweiligen Knoten versehen sind. Schwächen besitzt dieses System bei der Skalierung, ab einer gewissen Größe ist der Nachrichtenversand recht zeitaufwändig, wenn die Verbindungsgeschwindigkeit nicht angepasst wird. Auch könnte ein Angreifer eine große Anzahl an Knoten generieren und durch zusätzliche Unterbrechung der Verbindung zu anderen Knoten das System manipulieren.[85]

Dieser Algorithmus wird genutzt, um Konsens über die DIDs, die Referenzschemata sowie die Schema-Definitionen zu erhalten. Nebenbei benutzt Hyperledger Indy noch ein Public-Key-System zur Bereitstellung der DIDs. Die DIDs bestehen aus den ersten 16 Bytes des sog. Verkeys, welcher dem Public Key entspricht. Der Private Key, genannt Signkey, wird im Wallet gespeichert und dient der Erstellung von Signaturen.[86]

Von einem Trust Anchor (welcher z. B. ein Bundesministerium sein kann) wird ein Referenzschema festgelegt. In diesem Schema werden die Attribute aufgeführt, die ein bestimmter Nachweis enthalten soll. Im Beispiel der Fahrerlaubnis könnten das folgende Attribute sein: Fahrerlaubnisklasse, erworben am, gültig bis, Auflagen/Beschränkungen. Dazu erstellen die Nutzer dieses Schemas (z. B. die Fahrerlaubnisbehörde des Landkreises) eine eigene Definition dazu, welche öffentlich zugänglich gemacht wird

[83]Vgl. https://github.com/hyperledger/indy-plenum (zuletzt geöffnet am 05.03.2020).
[84]Vgl. Aublin et al. (2013, S. 297).
[85]Vgl. Casro, Liskov (1999, S. 3 ff.).
[86]Vgl. https://github.com/hyperledger/indy-sdk/blob/master/docs/getting-started/indy-walkthrough.md (zuletzt geöffnet am 05.03.2020).

und weitere Daten, die den Herausgeber (den Schema-Nutzer) betreffen. Die Schema Nutzer geben dann die eigentliche Referenz (auch Credential genannt) heraus. Eine Referenz (ähnlich wie ein Ausweis oder Berechtigungsnachweis, in der Dokumentation von Indy „Transkript“ genannt) enthält Informationen über eine Identität, die angeblich wahr sein sollen. Diese Referenz wird von einem Emittenten (oder auch Aussteller) angeboten und im Wallet des Identitätsbesitzers gespeichert. Dabei kann jeder Identitätsinhaber, der dem Netzwerk bekannt ist, eine solche Referenz ausstellen, und zwar über jeden anderen Identitätsinhaber, der ihm bekannt ist. Das erscheint auf den ersten Blick problematisch, stellt aber in der Realität kein Problem dar, da der Aussteller nachweislich und überprüfbar bekannt ist, was durch einen Konsensalgorithmus sichergestellt wird. So kann die Verlässlichkeit einer Referenz geprüft werden. Im obigen Beispiel könnte sich eine Person, welche keine offizielle Fahrerlaubnis besitzt, sich selbst eine Fahrerlaubnis der Klasse B ausstellen. Der Mietwagenbesitzer würde dann dieser Fahrerlaubnis keinen Glauben schenken, da er bemerkt, dass diese von selbiger Person ausgestellt wurde. Es müssen auch nur die Merkmale preisgegeben werden, die für die entsprechende Aktion von Belang wären. Im Beispiel wäre dies eine Information wie „Fahrerlaubnis Klasse B gültig bis Ende des Mietzeitraums ohne sicherheitsrelevante Auflagen“.[87]

Zusammenfassend lässt sich sagen, dass die Nodes, die gleichzeitig Akteure in einem Netzwerk darstellen, gleichberechtigt miteinander kommunizieren (Peer-to-Peer). Eine Referenz stellt die Grundlage einer Authentifizierung dar. Diese Referenz kann von anderen Akteuren überprüft werden. Wenn der Identitätsbesitzer sich identifiziert, nutzt er dazu die in seiner Wallet gespeicherten Referenzen . Diese stellen die Identität sowie bestimmte Merkmale/Eigenschaften dar, die vom Überprüfenden anerkannt werden. Oftmals kann auch nur der Beweis für eine Bedingung verwendet werden. Jeder Akteur erhält mehrere DIDs, die für verschiedene Arten von Authentifizierungen verwendet werden. Dies stellt den Datenschutz sicher und verhindert, dass ein Akteur Daten über einen anderen Akteur sammeln kann.

Als Beispiel wird im folgenden kurz ein Prozess von der Ausstellung einer Fahrerlaubnis bis zum Abschluss eines Mietvertrages über einen Mietwagen erläutert. Dazu müssen das Bundesministerium (für Verkehr und digitale Infrastruktur), das Landratsamt (und die Fahrerlaubnisbehörde) sowie der Mietwagenverleiher die Rolle eines Trust Anchors bekommen. Das Bundesministerium kann dann ein Referenzschema Fahrerlaubnis festlegen. Dies könnte folgende Attribute beinhalten: Name; Vorname; Geburts-

[87]Vgl. https://github.com/hyperledger/indy-sdk/blob/master/docs/getting-started/indy-walkthrough.md (zuletzt geöffnet am 05.03.2020).

datum; Führerschein Klasse AM, erworben am, gültig bis; Führerschein Klasse A1, erworben am, gültig bis (usw.); Auflagen/Beschränkungen; und wird anschließend auf allen Knoten gespeichert. Auf Grundlage dieses Schemas wird von der Fahrerlaubnisbehörde des Landkreises Zwickau eine Schema-Definition erstellt, die neben den Daten des ursprünglichen Schemas noch die Daten zur Fahrerlaubnisbehörde enthält. Diese Definition wird ebenfalls im Netzwerk gespeichert. Der Bürger B hat nach erfolgreicher Absolvierung der Fahrerlaubnisprüfung Anspruch auf Ausstellung einer Fahrerlaubnis und macht diesen geltend. Dazu ruft B die Definition aus dem Netzwerk ab und sendet eine Anfrage an die Fahrerlaubnisbehörde. Diese erstellt nach Prüfung der Voraussetzungen eine Referenz, die alle Werte der Schema-Definition (auch die Daten der im Schema festgelegten Attribute) enthält und sendet diese zurück an B. Dieser speichert die Referenz in seinem Wallet, die dort vor unberechtigten Zugriffen geschützt ist. Für diese Kommunikation werden die DIDs verwendet. Einige Zeit später möchte B einen Mietwagen ausleihen. Dazu wendet er sich an die Firma F. Diese sendet eine Anforderung mit den benötigten Attributen an B. Das sind z. B. Name; Vorname; Alter über 23; Führerschein Klasse B erworben vor mindestens einem Jahr und gültig bis Ende des Mietzeitraums[88]. B kann nach Erhalt der Anforderungen die entsprechenden Daten freigeben und an F senden. F erhält die Informationen und überprüft diese auf Erfüllung der Vertragsbedingungen und ob diese von der Fahrerlaubnisbehörde des Landkratsamtes Zwickau stammen. Wenn alles korrekt ist, akzeptiert F die Daten und dem Vertragsschluss steht nichts mehr im Weg. Auch hier erfolgte die Kommunikation über DIDs, allerdings nicht über die bereits verwendeten. Für jede Verbindung wurde ein anderer Identifier erstellt.

Es gibt bereits einen Pool an Knoten, welcher von der Sovrin Foundation betrieben wird. Die Sovrin Foundation hat ihren Sitz in den USA und einen maßgeblichen Beitrag zur Entwicklung von Hyperledger Indy geleistet[89]. Durch die Foundation erfolgt auch eine Bereitstellung eigener Tools für eine dezentrale elektronische Identität[90].

Für eine Anwendung in einer Landkreisverwaltung müsste ebenfalls ein Pool an Nodes entstehen. Es erscheint sinnvoll, diese Aufgabe an eine unabhängige Stiftung zu übertragen. Diese sollte dann aber mindestens für ein ganzes Bundesland diese Infrastruktur bereitstellen, wenn nicht sogar für Gesamtdeutschland. Eine Erprobungsphase für Einwohner eines bestimmten Gebietes kann aber durchaus sinnvoll sein. Auch private Dritte sollten Knoten betreiben können, um das Vertrauen in die Technologie zu stär-

[88]Das die Fahrerlaubnis der Klasse B normalerweise kein Ablaufdatum besitzt wird hier außer acht gelassen.
[89]Vgl. https://sovrin.org/faqs/ (zuletzt geöffnet am 06.03.2020).
[90]Vgl. https://github.com/hyperledger/indy-node (zuletzt geöffnet am 06.03.2020).

ken. Im Rahmen einer Überprüfung dieser Knoten sollte regelmäßig die darauf ausgeführte Software auf Echtheit getestet werden, um das Risiko von Manipulation zu verringern. So kann ein Pool bzw. Netzwerk an Knoten entstehen, welche von öffentlicher und privater Hand getragen werden und für die digitale Identität genutzt werden können.

Um die Verwendung der Identität zu vereinfachen, sollte die Verwaltung der Wallets mobil und benutzerfreundlich erfolgen. Eine App für Smartphones sowie Softwareprogramme für verschiedene Betriebssysteme würden einen Beitrag dazu leisten. Eine Kopplung der Identität mit dem elektronischen Personalausweis würde das Potenzial von diesem nutzbar machen und bedeutet ein gleichzeitiges Plus an Sicherheit und würde eine Registrierung der Identität für Verwaltungsdienstleistungen (wie in der Stadt Zug) obsolet machen, auch da die eID-Funktion mittlerweile mit fast jedem NFC-fähigen Smartphone nutzbar ist[91].

Schlussendlich kann man sagen: Mittels Hyperledger Indy kann eine Blockchain-basierte digitale Identität geschaffen, die sich durch Dezentralität und ein hohes Maß an Sicherheit auszeichnet. Durch Verwendung von Open-Source-Software kann mit einer verbesserten Akzeptanz in der Bevölkerung gerechnet werden. Kosten entstehen vor allem durch Anpassung der Software und Bereitstellung eines Netzwerks an Nodes. Auch die Verwendung der digitalen Identität für weitere Verwaltungsdienstleistungen wäre denkbar, so z. B. für die Kfz-Anmeldung.

6.2 Grundbücher und Eigentumsverhältnisse

Das Grundbuch ist ein Verzeichnis, das die Eigentumsverhältnisse von Grundstücken und den darauf befindlichen Gebäuden abbildet. Auch Belastungen und Grunddienstbarkeiten werden im Grundbuch aufgeführt[92]. Das deutsche Grundbuchsystem gilt im Vergleich zu anderen Ländern als relativ sicher, Manipulationen kommen zumeist nur bei Angaben über die Beschaffenheit der Grundstücke/Gebäude vor. Anders als z. B. in Italien gilt in Deutschland das sog. Realfoliensystem. Dabei wird für jedes Grundstück ein eigenes Blatt im Grundbuch angelegt[93].

Bei Inaugenscheinnahme dieses Blattes wird der jeweilige aktuelle Eigentümer des Grundstücks sowie die bestehenden Rechte ersichtlich. Dies hat den Vorteil, dass immer die aktuellen Eigentumsverhältnisse klar erkennbar dokumentiert sind. In anderen Ländern, z. B. in Italien, wird das sog. Personalfoliensystem verwendet. Dabei wird

[91]Vgl. https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/So_geht_s/So_geht_s_node.html (zuletzt geöffnet am 06.03.2020).
[92]Vgl. https://amt24.sachsen.de/web/guest/lebenslage/-/lebenslage/Grundbuch-5000850-lebenslage-0 (zuletzt geöffnet am 06.03.2020).
[93]Vgl. § 3 Abs. 1 Grundbuchordnung (GBO)

Personen das Eigentum an Grundstücken zugeordnet. Das Grundbuch stellt sich somit als Auflistung von Rechtsakten dar, die nach den betreffenden Personen sortiert sind. In der Praxis gestaltet es sich deshalb oftmals schwierig, Informationen zu Grundstücken zu erlangen, da nur die Veränderungen aufgeführt sind (ähnlich wie bei Bitcoin, s. Abschnitt 2.4).[94]

Während also bei dem italienischen System durch eine Blockchain eine Verbesserung der Sicherheit und Nachvollziehbarkeit erreicht werden könnte, ist das deutsche System in seiner bestehenden Form recht sicher und gut nachvollziehbar. Auch anders als beim oben erwähnten schwedischen System haben in Deutschland die Makler nicht das Recht, notarielle Aufgaben zu übernehmen. Ein vergleichbares Missbrauchspotenzial liegt an diesem Punkt nicht vor. Es besteht allerdings die Möglichkeit, den Grundstückserwerb mittels Blockchain kostengünstiger abzuwickeln. Dazu soll zunächst der aktuelle Ablauf aufgezeigt werden.

Für einen Kaufvertrag über ein Grundstück gelten besondere Regeln, z. B. bedarf dieser Vertrag der notariellen Beurkundung[95]. Nach den Vertragsverhandlungen zwischen Käufer und Verkäufer und nach Klärung der Finanzierungsmodalitäten muss ein Notar mit der Ausfertigung des eigentlichen Kaufvertrags beauftragt werden. Durch anschließende Auflassung des Grundstücks durch den Verkäufer und Eintragung des Käufers in das Grundbuch erfolgt der Eigentumsübergang. Die beiden Rechtsakte leitet der Notar in die Wege, nach der anschließenden Zahlung der Grunderwerbssteuer hat das Grundstück den Eigentümer gewechselt.

Die notariellen Aufgaben durch eine Blockchain-basierte Anwendung zu ersetzen erscheint aus vielen Gesichtspunkten nicht sinnvoll. Erstens besitzt der Notar die Pflicht zur Neutralität gegenüber den Beteiligten und soll diese auch beraten[96]. Wenn diese Aufgaben nicht mehr wahrgenommen werden, besteht für den Käufer oder den Verkäufer ein größeres Risiko durch unlautere Vertragsmodalitäten. Auch die Überprüfung der Berechtigungen der Beteiligten sowie deren Geschäftsfähigkeit wäre nicht möglich. Angaben zum Grundstück oder Gebäude selbst wären davon nicht betroffen, da diese aktuell auch nicht vom Notar überprüft werden[97]. Verbesserungspotenzial besteht bei Abwicklung der Eintragung ins Grundbuch durch den Notar. Hier könnte ein Blockchain-basiertes System einen zeitlich schnelleren Ablauf ermöglichen, indem der Notar

[94]Vgl. Rupp (2024, S. 571 ff.)
[95]Vgl. § 311b Abs. 1 Bürgerliches Gesetzbuch (BGB)
[96]Vgl. §14 Abs. 1 Bundesnotarordnung (BNotO)
[97]Vgl. https://www.faz.net/aktuell/finanzen/meine-finanzen/mieten-und-wohnen/immobilienkauf-der-notarielle-vertrag-entscheidet-15283721.html (zuletzt geöffnet am 06.03.2020).

die Änderungen digital weitergibt. Ob diese Verbesserung den Aufwand der Entwicklung einer Blockchain-basierten Lösung rechtfertigt, ist fraglich.

Eine Umsetzung eines Blockchain-basierten Grundbuchs wäre mittels Hyperledger Fabric möglich. Auf nähere Ausführungen wird hier aufgrund des geringen Verbesserungspotenzials für das deutsche Grundbuchsystem verzichtet.

6.3 Wahlen

In einer Demokratie sind Wahlen ein wichtiges Instrument, damit der Einzelne sich an Entscheidungen der Parlamente, wenn auch nur indirekt, beteiligen kann. Die Anforderungen an eine Wahl in der Bundesrepublik sind in Art. 28 des Grundgesetzes (GG) geregelt. Diese sog. Wahlgrundsätze legen fest, dass neben der Wahl zum deutschen Bundestag auch alle anderen Parlamentswahlen (als auch die Wahl zum Kreistag) allgemein, unmittelbar, frei, gleich und geheim ablaufen müssen. „Allgemein“ bedeutet in diesem Kontext, dass jeder Bürger in Deutschland das Recht hat, wählen zu gehen. „Unmittelbar“ nimmt Bezug auf die direkte Wahl eines Kandidaten (anders als das Wahlmännersystem in den USA) und „Frei“ soll der Bürger im Hinblick auf seine Entscheidung sein. Das Wort „Gleich“ manifestiert die gleiche Wertigkeit aller Stimmen und „Geheim“ die unbeobachtete Stimmabgabe.[98]

Bei der Bundestagswahl im Jahr 2005 ging Deutschland erste Schritte in Richtung E-Voting (dt. Elektronisches Wählen). Der Einsatz der Wahlcomputer der niederländischen Firma Nedap wurde 2009 allerdings vom Bundesverfassungsgericht für verfassungswidrig erklärt. Im Urteil vom 03.03.2009 legten die Richter dar, dass die Verwendung der Wahlcomputer gegen Art. 38 i. V. m. Art. 20 Abs. 1 und 2 GG verstößt. Demnach konnten beim Einsatz dieser Wahlcomputer nicht alle wesentlichen Schritte der Wahlhandlung und Ergebnisermittlung von Bürgern ohne besondere Sachkenntnis überprüft werden[99]. Außerdem wurden vom Chaos-Computer-Club erhebliche Sicherheitsmängel des verwendeten Modells festgestellt[100]. Auch deshalb wurde in Deutschland zunächst Abstand von elektronischen Wahlverfahren genommen. Im etwas veralteten Lexikon des Bundeswahlleiters ist nach wie vor zu lesen, dass Kontrollmechanismen für technisch nicht versierte Bürger für Online-Wahlen nicht in Sicht wären[101]. Hier könnte die Blockchain mit ihren passenden Eigenschaften eingesetzt werden.

[98]Vgl. https://www.bpb.de/nachschlagen/lexika/das-junge-politik-lexikon/161767/wahlgrundsaetze (zuletzt geöffnet am 06.03.2020).
[99]Vgl. BVerfG, Urteil des Zweiten Senats vom 03.03.2009, - 2 BvC 3/07 -.
[100]Vgl. https://www.ccc.de/system/uploads/105/original/nedapReport54.pdf (zuletzt geöffnet am 06.03.2020).
[101]Vgl. https://www.bundeswahlleiter.de/service/glossar/o/online-wahlen.html (zuletzt geöffnet am 06.03.2020) Anmerkung: Webseite ist Stand 2015.

Es stellt sich aber nach wie vor die Frage nach Sinn und Nutzen der Etablierung eines neuen Wahlsystems, auch da die analoge Wahl weiterhin möglich sein müsste, da nach wie vor nur ca. 88 Prozent der deutschen Bevölkerung das Internet nutzen (Stand: 2019)[102]. Es könnten aber Auswirkungen auf die Wahlbeteiligung zu erwarten sein. So stieg in Estland nach Einführung einer Möglichkeit zur Stimmangabe die Wahlbeteiligung leicht an[103]. In Estland existiert allerdings kein Blockchain-basiertes Wahlsystem, die Wähler authentifizieren sich mittels E-ID-Card und geben dann ihre Stimme online ab[104]. Ein Blockchain-basiertes Online-Wahlsystem könnte also zu einer steigende Wahlbeteiligung in Deutschland führen. Auch würde ein solches System Papier- und Druckkosten sparen. Die Einführung würde sich aber erst nach einer längeren Zeit amortisieren, da die Entwicklung einen nicht unbeträchtlichen finanziellen Aufwand verursachen würde. Eine Einführung eines solchen Wahlsystems, welches auf die Wahlen zum Kreistag beschränkt wäre, würde den Aufwand der Entwicklung und Implementierung nicht rechtfertigen. Die Einführung eines solchen Wahlsystems wäre nur sinnvoll, wenn dies für alle Wahlen genutzt werden könnte. Die Landkreisverwaltung könnte dann auch von den Einsparungen profitieren, da diese die Kosten für die Wahl zu tragen hat[105]. Die Verteilungen der Einführungskosten auf die einzelnen Gebietskörperschaften müsste vorher geklärt werden.

Als Softwarelösung zur Umsetzung eines E-Voting-Verfahrens kommen mehrere Möglichkeiten in Betracht. Es existiert z. B. eine Lösung der Luxoft Inc., welche auf Hyperledger Fabric basiert. Diese wurde auch testweise von der Stadt Zug in der Schweiz eingesetzt (siehe 4.1). Die technische Umsetzung ist jedoch nicht klar nachzuvollziehen.[106]

Im Folgenden soll deshalb eine Lösung basierend auf Hyperledger Fabric vorgestellt werden. Eine Verknüpfung der E-Voting-Anwendung mit den digitalen Identitäten in Hyperledger Indy befindet sich in Entwicklung[107].

Im Abschnitt 5 wurden bereits einige Funktionalitäten von Fabric erläutert. Dieses nutzt den unter 6.1 bereits erwähnten PBFT- Algorithmus zur Konsens-Generierung im Netzwerk, der jedoch anwendungsabhängig modifiziert werden kann[108]. Für eine E-Voting-

[102]Vgl. https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/IT-Nutzung/Tabellen/zeitvergleich-computernutzung-ikt.html;jsessionid=81AAE09B9353E1B6F40FF918D46522F3.internet712 (zuletzt geöffnet am 06.03.2020).
[103]Vgl. Goos (2011, S.64).
[104]Vgl. ebenda (S.61).
[105]Vgl. § 55 Sächsisches Kommunalwahlgesetz.
[106]Curran (2018, S.2 f.).
[107]Vgl. https://wiki.hyperledger.org/display/INTERN/Extending+HL+Fabric+for+connecting+with+HL+Indy (zuletzt geöffnet am 10.03.2020).
[108]Vgl. https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html (zuletzt geöffnet am 10.03.2020).

Anwendung sind vor allem die Identitäten in einem Blockchain-Netzwerk von Bedeutung. Die Identitäten in Fabric besitzen Attribute, die Vereinigung von Identität und Attributen wird Principal genannt und erfüllt in etwa die Form einer Benutzernummer. Ähnlich wie bei Hyperledger Indy werden Identitäten in Fabric von einem Membership Service Provider (MSP) authentifiziert, vereinfacht gesagt wird durch einen MSP festgelegt, dass eine Identität akzeptiert wird. Eine digitale Identität entspricht einem digitalen kryptografischen Zertifikat und wird von einer Zertifizierungsstelle (genannt Certificate Authority, kurz CA) ausgestellt. Ein Zertifikat ist ein Dokument, welches Attribute über den Inhaber beinhaltet und von einer Zertifizierungsstelle mit ihrem Private Key verschlüsselt wurde. So wird sichergestellt, dass die Daten nach Verschlüsselung durch die CA nicht mehr verändert werden können. Wenn eine dritte Partei der jeweiligen Certificate Authority vertraut, kann diese Partei sicher sein, dass die Daten über die Identität nicht verändert wurden.[109]

Für ein E-Voting-System sind noch weitere Teilnehmer im Netzwerk notwendig. Als übergeordnetes Element existieren sog. Organisationen. Jeder andere Netzwerkteilnehmer (ob Peer oder Client) ist durch ein Zertifikat einer Organisation zugehörig. Bei dem Clienten handelt es sich um den Endbenutzer des Netzwerks. Ein Client kann in der Blockchain-Datenstruktur lesen und diese mithilfe eines Peer-Knotens verändern. Ein Peer-Knoten speichert eine Kopie der Blockchain ab und stellt Smart Contracts zur Verfügung, die die Art und Weise der Datenänderungen regeln. Ein Ordering-Service-Knoten sammelt alle Transaktionen in Reihenfolge des Eintreffens und sortiert diese in Blöcke. Dieser Knoten führt einen Apache-Kafka-Dienst aus. Dabei handelt es sich um ein Kommunikationssystem, welches mittels eines Publish-Subscribe-Pattern (dt. Herausgeber-Abonnent-Muster) die Datenzugriffe und -verarbeitung organisiert. Bei einem Publish-Subscribe-Pattern handelt es sich um eine Methode, um den Sender vom Empfänger einer Nachricht zu entkoppeln. Dieses bietet unter anderem folgende Vorteile: Der Ausfall eines Empfängers (welcher ein Knoten sein kann) wirkt sich nicht auf den Sender aus, welcher durch eventuell auftretende Fehlermeldungen beeinflusst wird. Der Sender kann sich auch nach Absendung einer Nachricht sofort wieder seiner Hauptaufgabe zuwenden und muss seine Rechenleistung nicht für den Nachrichtenversand an mehrere Empfänger aufwenden[110]. In Apache-Kafka wird die Verteileinrichtung für Nachrichten Kafka-Cluster genannt und besteht aus mehreren Knoten (ge-

[109]Vgl. https://hyperledger-fabric.readthedocs.io/en/release-1.4/identity/identity.html (zuletzt geöffnet am 10.03.2020).
[110]Vgl. https://docs.microsoft.com/en-us/azure/architecture/patterns/publisher-subscriber (zuletzt geöffnet am 13.03.2020).

nannt Broker). Empfänger können Nachrichten zu einem bestimmten Thema abonnieren, die Zustellung erfolgt anschließend über den Cluster.[111]

Smart Contracts werden auf die entsprechenden Peer-Knoten zur Ausführung übertragen. Nachdem der Contract auf den Peers installiert wurde, muss dieser händisch aktiviert werden[112]. Dafür werden die Peers festgelegt, die eine Datenänderung unterstützen müssen, damit diese Teil der Blockchain wird. Wenn ein Client Daten ändern möchte, muss dieser seinen Änderungsvorschlag an alle vorher festgelegten Peers senden. Die Peer-Knoten geben den veränderten Datensatz an den Clienten zurück, dieser sammelt diese Antworten und leitet diese an einen Ordering-Service-Knoten weiter, der die Antworten sortiert und in einen Block schreibt. Der Block wird anschließend an alle zuständigen Peer-Knoten weitergeleitet, es können auch mehrere Transaktionen zur Änderung von Datensätzen aufgenommen werden. Diese überprüfen die Transaktionen im Block auf Richtigkeit (also auf Vorliegen der Bestätigung von allen Peers) und auf Gültigkeit (die bei Änderungen in der Blockchain nach Zeitpunkt des Sendens des veränderten Datensatzes nicht mehr gegeben sein könnte). Nach Prüfung wird der Block mit allen gültigen Transaktionen an die Datenstruktur angehängt.[113]

Bei einem Wahlvorgang erhält der Wähler zunächst ein Zertifikat. Dieses sollte unter Nachweis der physischen Identität ausgestellt werden. Eine Kopplung mit einer digitalen Identität erscheint hier sinnvoll. Das Zertifikat garantiert auch, dass der Wähler seine Stimme nur einmal abgeben kann und es wird für eine anonyme (die für alle Wähler gleich ist) sowie für eine nachverfolgbare Identität ausgestellt. Für jede Identität wird ein Schlüsselpaar erzeugt. Der digitale Stimmzettel wird auf der Blockchain bereitgestellt und der Wähler lädt sich diesen herunter. Er füllt diesen aus und signiert diesen mit seinem privaten Schlüssel, welcher zur nicht anonymen Identität gehört. Anschließend wird von den Peer-Knoten überprüft, ob der Wähler zur Teilnahme an der Wahl berechtigt ist. Nach dem der Wähler seinen Stimmzettel mit seiner anonymen Identität an die Blockchain übergeben hat und die Wahl abgeschlossen ist, werden den berechtigten Institutionen die Schlüssel zur Entschlüsselung der Stimmzettel bereitgestellt. Die Wähler können die Ergebnisse danach auf der Blockchain überprüfen.[114]

Dieses System erfüllt alle Anforderungen an ein Wahlsystem. Wenn die Hyperledger-Umgebung korrekt eingerichtet wurde und alle Verbindungen verschlüsselt ablaufen, ist es für einen Dritten unmöglich, die Wahlentscheidung eines Wählers herauszufinden. Die Anforderung des Wahlgeheimnisses ist erfüllt. Auch die Nachprüfbarkeit der

[111]Vgl. Gajek, Lewandowsky (2019, S. 8 f.).
[112]Die Aktivierung entspricht dem Prozess der Instanziierung der Informatik.
[113]Vgl. Gajek, Lewandowsky (2019, S. 9 f.).
[114]Vgl. Gajek, Lewandowsky (2019, S. 11 ff.).

korrekten Berücksichtigung des eigenen Stimmzettels sowie die Kontrolle der Korrektheit der Auszählung des Wahlergebnisses ist für den Wähler gewährleistet. Dies wird gewährleistet, indem der Wähler Zugang zur Blockchain erhält und dadurch die Ergebnisse prüfen kann.[115]

Problematisch könnte die Kontrolle der Wahlergebnisse für den technisch nicht versierten Laien werden. Die Verwendung von blinden Signaturen[116] sowie weiterer kryptografischer Funktionen ist dem Großteil der Bevölkerung nicht geläufig. Diesem Problem könnte mit der Schaffung von grafischen Interfaces, die den Ablauf des Wahlvorgangs vereinfacht darstellen, entgegengewirkt werden. Die Prozesse, welche die Sicherheit des Systems gewährleisten, laufen dabei aber weiterhin im Hintergrund ab. Eine vollständige Transparenz kann dadurch nicht gewährleistet werden. Deshalb bleibt fraglich, ob das System den Anforderungen in Deutschland genügt, da auch bereits die oben erwähnten Wahlcomputer dem Anspruch nicht gerecht wurden. Eine umfangreiche und verständliche Dokumentation könnte dieses Problem zu einem Teil lösen. Es besteht die Möglichkeit, dass im oben erläuterten System der Wähler selbst Knoten mit der entsprechenden Software betreibt, wenn er den übrigen Institutionen nicht vertraut. Auch existieren zudem noch weitere Möglichkeiten, ein E-Voting-System mittels Hyperledger zu errichten, z. B. mit dem weiteren Projekt Hyperledger Sawtooth[117].

Es lässt sich resümieren, dass ein Blockchain-basiertes E-Voting-System den Anforderungen an ein Wahlsystem in Deutschland durchaus genügt. Die wichtigen Grundpfeiler Anonymität bei der Stimmabgabe und die Nachprüfbarkeit des Wahlergebnisses sind gewährleistet. Die Überprüfung des Systems durch einen technisch nicht versierten Laien ist allerdings nur eingeschränkt möglich. Bei einer grafischen Veranschaulichung der komplexen Hintergrundprozesse bleiben die genauen Abläufe weiterhin verborgen. Durch die Veröffentlichung einer Dokumentation über die Funktionsweisen des Systems könnte die Überprüfung für einen Laien zumindest teilweise vereinfacht werden.

6.4 Kontrolle der Kühlkette mittels Blockchain

Besonders im Sommer verderben Lebensmittel bei unzureichender Kühlung recht schnell. Vor allem Fleisch-, Wurst- und Milchprodukte sind davon betroffen. Der Verzehr von verdorbenen Produkten dieser Gattungen kann z. T. erhebliche Gesundheitsschäden verursachen. Den Verbraucher vor dieser Gefahr zu schützen, ist Aufgabe der

[115]Vgl. ebenda (S. 16 f.).
[116]Dabei handelt es sich um eine Signatur, bei welcher der Signierende den Inhalt der zu signieren Nachricht nicht kennt. Weitere Ausführungen sind durch den limitierten Umfang der Arbeit nicht möglich.
[117]Vgl. https://www.hyperledger.org/blog/2018/09/20/bitagora-a-decentralized-voting-platform-built-on-hyperledger-sawtooth (zuletzt geöffnet am 15.03.2020).

staatlichen Gewalt. § 5 Abs. 1 des Lebensmittel-, Bedarfsgegenstände- und Futtermittelgesetzbuch (LFBG) regelt das Verbot der Inverkehrbringung gesundheitsschädlicher Lebensmittel. Die Zuständigkeit für die Durchsetzung und Überwachung der Lebensmittel wurde in der Landesgesetzgebung verankert. Demnach sind nach § 1 des Gesetzes zur Ausführung des Lebensmittel- und Bedarfsgegenständegesetzes im Freistaat Sachsen (SächsAGLMBG) die Landkreise und kreisfreien Städte die unteren Lebensmittelüberwachungsbehörden, die gemäß § 1 Abs. 1 i. V. m. § 9 SächsAGLMBG für die Durchführung der Überwachungsmaßnahmen zuständig sind. Es handelt sich demnach um eine Aufgabe der Landkreisverwaltungen, die Unversehrtheit von verderblichen Lebensmitteln zu kontrollieren. Dies geschieht aktuell nur durch regelmäßige unangekündigte Kontrollen und verstärkte Kontrollen im Verdachtsfall[118]. Es besteht auch die Pflicht zur Eigenkontrolle durch den Hersteller bzw. Händler, um die Sicherheit der Lebensmittel zu garantieren[119]. Zusätzlich ist es noch Aufgabe der Landkreise und kreisfreien Städte, gesundheitsschädliche Lebensmittel aus dem Verkehr zu ziehen und entsprechende Ordnungsgelder zu verhängen[120].

Bei diesen Aufgaben könnte ein Blockchain-basierte Lösung dazu eingesetzt werden, um eine durchgängige Kontrolle der Kühlkette während der gesamten Dauer zu gewährleisten, in der das Lebensmittel im Umlauf ist. So könnte über entsprechende Sensoren eine dauerhafte und lückenlose Temperaturüberwachung erfolgen. Die Daten des Sensors könnten anschließend in einer permissioned Blockchain gespeichert werden, zu der alle beteiligten Akteure Zugang erhalten. Ein Fleischerzeugnis bekommt z. B. sofort nach der Schlachtung einen Temperatursensor aufgeklebt. Dieser dokumentiert minütlich die Temperatur. Beim Transport, welcher meist noch über Zwischenhändler/Großhändler erfolgt, bevor das Produkt beim Kunden ankommt, kann gewährleistet werden, dass das Produkt eine gewisse Temperatur nicht überschreitet. Sollte die Temperatur dennoch durch unzureichende Kühlung überschritten werden, kann per Smart Contract automatisiert eine Aktion (z. B. Strafe, besondere Kennzeichnung des Produkts) ausgeführt werden. Auch eine Kühlbox mit entsprechenden Sensoren wäre denkbar. Bei solch einer Anwendung könnte das Oracle Problem eine Rolle spielen. Es wäre für einen der Beteiligten verhältnismäßig leicht möglich, den Temperatursensor während des Transportes in einer entsprechend kühlen Umgebung zu deponieren und die Energie für die Kühlung dadurch einzusparen. Diese Vorgehensweise könnte durch entsprechende technische Maßnahmen erschwert werden (z. B. verstecktes Anbringen

[118]Vgl. § 9 Abs. 1 SächsAGLMBG.
[119]Vgl. § 8 SächsAGLMBG.
[120]Vgl. § 10 und § 14 SächsAGLMBG.

des Sensors), aber nicht unmöglich gemacht werden. Eine solche Lösung ist demnach nur so sicher wie die einfachste Möglichkeit zur Manipulation.[121]

Aber selbst mit den erwähnten Problemen/Einschränkungen kann eine Blockchain-basierte Lösung eine Überwachung der Kühlkette besser gewährleisten als die bisherige Lösung durch manuelle Kontrollen. Eine sofortige flächendeckende Implementierung einer solchen Lösung wäre allerdings sehr aufwendig und sollte Schritt für Schritt erfolgen, zunächst auf freiwilliger Basis. So kann gewährleistet werden, dass auch kleinere Unternehmen sich auf die dann notwendigen zusätzlichen Arbeitsschritte einstellen können (z. B. Anbringung Temperatursensoren).

6.4.1 Technische Umsetzung mittels IBM Food Trust

Zur Umsetzung einer Blockchain-basierten Kühlkettenüberwachung bieten sich mehrere Möglichkeiten an, die größtenteils auf den verschiedenen Hyperledger-Projekten basieren. So existiert z. B. eine Anwendung namens IBM Food Trust. Der Blockchain-Teil dieser Anwendung basiert auf Hyperledger Fabric[122]. Dabei haben Teilnehmer des Netzwerks wie Lieferanten und Einzelhändler die Rolle eines Trust Anchors[123]. Diese sind verantwortlich für den Betrieb des Netzwerkes. Dabei kann aber jeder Teilnehmer einen eigenen Peer-Knoten betreiben und Smart Contracts installieren und aktivieren. In den Smart Contracts können entsprechende Geschäftsregelungen abgelegt werden (z. B. Strafe bei Kühlkettenunterbrechung). Datenschutz kann durch die Schaffung verschiedener Kanäle gewährleistet werden, sodass nur diejenigen Akteure Zugriff auf entsprechende Daten erhalten, die sie zwingend benötigen. Neben der Überwachung der Temperatur unterstützt IBM Food Trust auch noch weitere Daten, wie z. B. die aktuelle Position des Lebensmittels. Spezielle technische Ressourcen werden nicht benötigt, der Zugriff erfolgt über einen Internet-Browser, da die Infrastruktur von IBM gehostet werden kann. Auch die Installation eines Peer-Knotens in einer lokalen Umgebung ist möglich, die Administration erfolgt dann über einen Fern-Zugriff.[124]

6.4.2 Technische Umsetzung mittels Seafood Supply Chain

Eine weitere Möglichkeit zur Umsetzung einer automatisierten Kontrolle der Kühlkette bietet die Seafood Supply Chain (dt. Lieferkette von Fisch und Meeresfrüchten). Dieses Projekt basiert auf Hyperledger Sawtooth. Dieses Projekt der Linux Foundation hebt sich besonders durch die Integration von IoT-Sensortechnik hervor[125]. Auch wurde bei diesem Projekt das Kernsystem von der Anwendungsebene getrennt, sodass es mög-

[121]Vgl. Mahn (2019, S. 76).
[122]Vgl. https://www.ibm.com/de-de/blockchain/solutions/food-trust (zuletzt geöffnet am 18.03.2020).
[123]Ähnlich wie bei Hyperledger Indy, s. a. Abschnitt 6.1.
[124]Vgl. IBM (2019, S. 11).
[125]Vgl. https://sawtooth.hyperledger.org/examples/ (zuletzt geöffnet am 18.03.2020).

lich ist, Smart Contracts in vielen Programmiersprachen zu schreiben (z. B. Python und Javascript). Für Hyperledger Sawtooth wurde ein eigener Konsensalgorithmus namens Proof of Elapsed Time entwickelt, welches es ermöglicht, große Teilnehmerzahlen an der Konsensfindung zu beteiligen. Auch andere Konsensalgorithmen sind möglich, z. B. der noch in Entwicklung befindliche RAFT-Algorithmus. Ein weiteres besonderes Merkmal von Sawtooth ist der On-Chain-Governance-Mechanismus, mit dem durch eine spezielle Form von Smart Contracts die Blockchain administriert werden kann. So kann festgelegt werden, dass z. B. die Änderung des Konsensalgorithmus mittels Smart Contract durch einen einzelnen Teilnehmer erfolgen kann oder die Zustimmung mehrerer Teilnehmer notwendig ist.[126]

Im Projekt Seafood Supply Chain werden IoT-Sensoren genutzt, die an dem jeweiligen Objekt oder Lebensmittel angebracht werden. Während des Transports senden diese Sensoren neben Daten über die Temperatur auch andere Daten wie Erschütterungen oder Positionsdaten. Diese Daten können in der Blockchain gespeichert werden und geben dem Endkunde Aufschluss über den Weg des Produkts. Auch die Weitergabe durch eventuelle Zwischenhändler kann vom Kunden überwacht werden. Die Anwendung ist aktuell noch auf Meeresfrüchte und Fisch spezialisiert, eine Ausweitung auf andere Lebensmittel oder sonstige verderbliche Produkte wäre aber ohne weiteres denkbar.[127]

6.4.3 Technische Umsetzung mittels TradeLens

Ein weiteres Projekt von IBM, diesmal in Kooperation mit Maersk, ist TradeLens. Dabei handelt es sich um Blockchain-basierte Plattform zur Nachverfolgung von Lieferketten, vorwiegend von Containern über den Seeweg. Auch hier ist die Auswertung von Sensordaten möglich. Auch diese Anwendung basiert auf Hyperledger Fabric. Da in Sachsen die Versendung von verderblichen Waren in Seecontainern im Transportgewerbe eine eher untergeordnete Rolle spielt, wird auf diese Anwendung nicht weiter eingegangen. Sie könnte aber z. B. für Zollbehörden interessant sein.[128]

Auch die Entwicklung eines eigenen Systems zur Kühlkettenüberwachung auf Basis eines Hyperledger-Projektes wäre möglich. Dabei würde für die entsprechende Behörde aber ein nicht unerheblicher Entwicklungsaufwand entstehen, sodass eine landesweite Kooperation sinnvoll wäre. Bei den oben vorgestellten Lösungen wird die Infrastruktur vom Anbieter bereitgestellt (IBM) oder muss durch den Betreiber selbst unterhalten werden (Seafood). Dies müsste bei einer Eigenentwicklung auch berücksichtigt wer-

[126]Vgl. Olson et al (2018, S. 4 ff.).
[127]Vgl. https://sawtooth.hyperledger.org/examples/seafood.html (zuletzt geöffnet am 18.03.2020).
[128]Vgl. https://www.tradelens.com/ecosystem (zuletzt geöffnet am 19.03.2020).

den. Dabei fällt vor allem die Serverinfrastruktur und die Beschaffung der Sensoren von den Kosten her ins Gewicht. Nach der Anfangsinvestition amortisieren sich die Kosten durch den Wegfall der stichprobenartigen Kontrollen.

Abschließend lässt sich sagen, dass durch ein Blockchain-basiertes System zur Kontrolle der Kühlkette die Sicherheit von Lebensmitteln verbessert werden kann. Auch manuelle Kontrollen könnten wegfallen. Neben den Behörden würden auch die anderen am gesamten Verkaufsprozess Beteiligten profitieren, da eine Verbesserung der Produktqualität erreicht werden kann. So könnte auch ein Anreiz entstehen, sich an der Entwicklung eines solchen Systems zu beteiligen. Die Schwachstelle einer solchen Anwendung ist die Datengewinnung durch Sensoren, die leicht manipuliert werden kann. Diese muss möglichst sicher erfolgen, wobei man eine Manipulation nicht mit Sicherheit verhindern kann.

6.5 Bezahlung von Verwaltungsdienstleistungen mit Kryptowährungen

Die wohl einfachste Anwendung einer Blockchaintechnologie ist die Akzeptanz von Kryptowährungen bei Bezahlung von Verwaltungsdienstleistungen. Die Umsetzung dieser ist ohne weiteres möglich, wenn sich ein Finanzdienstleister findet, der die Zahlungen abwickelt und den entsprechenden Betrag in der Landeswährung an die Behörde überweist.

Dies ist wie im Abschnitt 4.1 bereits erwähnt in der Schweiz bereits möglich. Dort können Verwaltungsdienstleistungen bis zu einer Höhe von 200 Franken[129] bereits in Bitcoin bezahlt werden. Die Zahlung erfolgt aber nicht direkt an die Stadtverwaltung, sondern an die Bitcoin Suisse AG, einen schweizerischen Finanzdienstleister[130], der die Beträge für einen bestimmten Zeitraum abrechnet und in Schweizer Franken an die Stadt Zug überweist. Dadurch besteht auch keine Gefahr, dass durch Kursschwankungen der Wert der erhaltenen Bitcoin, die die Stadt in Ihrem Wallet aufbewahrt, verfällt. Auch wäre eine weitere Verwendung der Bitcoins für die Kommune schwierig, da kaum Möglichkeiten zur Ausgabe existieren. Bei der Entscheidung der Stadtverwaltung, in Zukunft Bitcoins als Zahlungsmittel zu akzeptieren, handelt es sich aber eher um eine Maßnahme des medienwirksamen Standortmarketings, um Offenheit gegenüber neuen Technologien zu signalisieren, als um eine wirkliche Vereinfachung des Zahlungsverkehrs. Dies zeigt auch die geringe Zahl an Transaktionen, die bisher durchgeführt wurden.[131]

[129] Entspricht ca. 180 EUR.
[130] Vgl. https://www.bitcoinsuisse.com/about-us/ (zuletzt geöffnet am 19.03.2020).
[131] Vgl. https://www.heise.de/newsticker/meldung/Im-tiefen-Tal-der-Kryptowaehrungen-Ein-Besuch-in-Zug-3760567.html (zuletzt geöffnet am 19.03.2020).

Für eine Landkreisverwaltung wäre auch denkbar, Bitcoins oder andere Kryptowährungen als Zahlungsmittel zu akzeptieren. Andere Kryptowährungen sollten nach der Höhe ihrer Marktkapitalisierung ausgewählt werden[132]. Auch hier müsste die Abwicklung über einen externen Finanzdienstleister erfolgen, da sich die Kursschwankungen sonst negativ auf das Landkreisvermögen auswirken würde. Dies würde auch dem Grundsatz der Sparsamkeit und Wirtschaftlichkeit verletzen, der in der Landkreisverwaltung verankert ist. Der Einsatz dieser neuen Technologie kann in Verwaltungen und wechselseitig dazu in der freien Wirtschaft ein gewisses Innovationspotential freisetzen. Dies könnte sich positiv auf die Attraktivität eines Landkreises als Wirtschaftsstandort für Unternehmen auswirken.

[132]Eine Übersicht zur Marktkapitalisierung von Kryptowährungen findet sich unter https://coinmarketcap.com/.

7 Fazit

Die Blockchain-Technologie besitzt das Potenzial, einige in der Gesellschaft etablierte Abläufe und Vorgehensweisen nachhaltig zu verändern. Bevor jedoch größere Umstellungen erfolgen, muss genau überprüft werden, ob eine Blockchain-basierte Lösung auch eine Verbesserung mit sich bringt, denn auch diese Technologie hat ihre Nachteile. Überall dort, wo das Vertrauen zwischen mehreren Parteien zur Abwicklung eines Prozesses notwendig ist, könnte der Einsatz einer solchen neuen Lösung geprüft werden. Dabei ist darauf zu achten, ob tatsächlich eine Verbesserung im Vergleich zur bestehenden Lösung erreicht wird. Dies gilt für die öffentliche Verwaltung und hier speziell die Landkreisverwaltungen ebenso wie für alle anderen Bereiche. Der Einsatz dieser neuen Technologie kann ein gewisses Innovationspotential freisetzen und die Attraktivität als Wirtschaftsstandort eines Landkreises erhöhen.

Zusammengefasst kann man sagen, dass es sich bei einer Blockchain um eine bestimmte Art einer Datenstruktur handelt, die von mehreren Teilnehmern im Netzwerk parallel gehalten wird. Um identische Kopien zu halten, einigen sich die Mitglieder des Netzwerks mittels eines Konsensmechanismus auf einen einheitlichen Zustand. Dieser kann unterschiedlich geartet sein. Es gibt z. B. den bei Kryptowährungen verwendeten Proof-of-Work-Algorithmus, bei welchem eine rechenintensive Aufgabe zur Konsens-Generierung gelöst werden muss. Da die Berechnung einen erheblichen Energieaufwand bedeutet, eignet sich dieser Mechanismus kaum zum Einsatz im öffentlichen Sektor. Hier kommen eher andere Algorithmen in Frage, z. B. Proof-of-Stake oder PBFT. Ein Vorteil der Blockchain ist, dass zur Einigung mehrerer Parteien kein vertrauenswürdiger Dritter benötigt wird, da alle Teilnehmer die Vorgänge im System überwachen. Auch der Ausfall einiger Netzwerkteilnehmer ist unproblematisch, da jeder Teilnehmer die gesamte Datenstruktur speichert. Diese Datenstruktur besteht aus Blöcken, bei denen jeder Block auf den Vorgänger-Block verweist. So ist es kaum möglich, in einem Block gespeicherte Daten zu ändern, da sonst alle nachfolgenden Blöcke ebenfalls geändert werden müssten. Das stellt einen großen Sicherheitsvorteil dar.

Durch die verteilte Speicherung der Daten durch jeden Netzwerkteilnehmer kann es zu Datenschutzproblemen kommen. Dieses kann dadurch gelöst werden, dass nur bestimmte Teilnehmer die Datenstruktur einer Blockchain lesen können. Diese muss dann aber mit herkömmlichen Mitteln vor unberechtigten Zugriffen geschützt werden.

Mittels Smart Contracts können automatisiert Vertragsbedingungen auf der Blockchain überprüft werden. Diese werden in Programmcode formuliert und an die Netzwerkteilnehmer übergeben, welche die Erfüllung dieser Bedingungen regelmäßig kontrollieren.

Wenn es sich dabei um Bedingungen aus der Realität handelt, ist es mitunter schwierig, diese manipulationssicher zu gewinnen (möglich ist z. B. die Fälschung von Sensordaten). Dies wird Oracle-Problem genannt.

In Deutschland wurde das Potenzial der Technologie auch von der Bundesregierung erkannt, die deshalb eine Strategiepapier zur Blockchain veröffentlichte. Es fehlen allerdings noch konkrete Maßnahmen zur Anwendung der Technologie. Auch das Koordinierungsprojekt Blockchain bietet bisher nur Ansätze. Konkretere Vorschläge wurden vom Blockchain Competence Center Mittweida gemacht, welches auch als Entwicklungspartner für Unternehmen und Verwaltung fungieren könnte.

In anderen Ländern werden Blockchain-basierte Technologien im öffentlichen Sektor bereits genutzt, wenn auch nur testweise. In Zug in der Schweiz können Verwaltungsdienstleistungen in Bitcoin bezahlt werden und Bürger können eine elektronische Identität beantragen. Unter Verwendung dieser Identität wurde bereits ein Testdurchlauf einer elektronischen Wahl durchgeführt. Estland gilt als Vorreiter in Sachen digitale Verwaltung. Eine Blockchain basierte Lösung wird hier allerdings nur für die elektronische Patientenakte eingesetzt. In Schweden wurde für Immobilien- und Grundstücksverkäufe eine Blockchain-basierte Lösung eingeführt, ähnlich wie in Deutschland das Grundbuch. Das System des Grundbuchs in Schweden unterscheidet sich jedoch nicht unerheblich von dem System in Deutschland, sodass eine Übertragung nicht ohne weiteres möglich ist.

Möglichkeiten zur Umsetzung einer Blockchain-basierten Lösung bietet das Open-Source-Projekt Hyperledger, das unter dem Dach der Linux Foundation entwickelt wird. Es werden mehrere Lösungen für verschiedene Anwendungsfälle entwickelt, die größtenteils modular aufgebaut sind und bereits für Anwendungen verwendet wurden.

In Deutschland sind die Landkreise und kreisfreien Städte für das Führerscheinwesen zuständig. Der physische Führerschein im Scheckkartenformat bietet Missbrauchspotenzial, unter anderem bei der Anmietung von Kraftfahrzeugen. Hier könnte eine Blockchain-basierte Technologie Missbräuche verhindern. Wenn diese allein für Führerscheine genutzt werden würde, wäre der Aufwand zur Entwicklung einer solchen Lösung recht groß und die Umsetzung durch eine herkömmliche zentralisierte Lösung kostengünstiger zu realisieren. Eine Blockchain-basierte Lösung würde sich anbieten, wenn der Führerschein mit einer digitalen Identität gekoppelt würde, die dann auch für andere Anwendungen eingesetzt werden könnte. Die Umsetzung könnte mittels Hyperledger Indy erfolgen.

Um das in Deutschland verwendete Grundbuchsystem zu ersetzen, eignet sich eine digitale Blockchain-basierte Lösung weniger. Vor allem die Aufgaben des Notars könnten nicht adäquat ersetzt werden.

Ein System für das Blockchain-basierte E-Voting könnte die Sicherheitsbedenken, die bisher gegen elektronische Wahlverfahren bestanden, ausräumen. Dabei sollte allerdings bedacht werden, dass der Ablauf einer Wahl, die mittels Blockchain durchgeführt wird, recht komplex ist und nur schwer von einem technisch nicht versierten Laien überprüft werden kann. Dem muss mittels geeigneten Maßnahmen entgegengewirkt werden. Auch wäre die Entwicklung eines solchen Systems durch eine einzelne Landkreisverwaltung nicht sinnvoll, eine landesweite oder bundesweite Kooperation würde für eine effizientere Entwicklung sorgen. Für die Umsetzung würde sich Hyperledger Fabric anbieten.

Die Überwachung der Kühlkette zählt ebenfalls zu den Aufgaben einer Landkreisverwaltung. Durch unzureichende Kühlung verdorbene Lebensmittel gefährden die Gesundheit und müssen aus dem Verkehr gezogen werden. Für die Überwachung der Kühlkette bietet sich eine Blockchain basierte Lösung an, die Sensordaten fälschungssicher und für alle Akteure sichtbar aufzeichnet. Dafür existieren bereits fertige Lösungen, z. B. von IBM. Diese basiert auf Hyperledger Fabric, womit auch eine Eigenentwicklung denkbar wäre. Berücksichtigt werden sollte auch der Aufwand, der durch Anschaffung und Verwendung geeigneter Temperatursensoren entstehen würde sowie die mögliche Manipulation dieser Sensordaten durch konstruktionsbedingte bzw. technische Schwachstellen.

Die Akzeptanz von Kryptowährungen als Zahlungsmittel für Verwaltungsdienstleistungen wäre mit geringem Aufwand umsetzbar. Die Abwicklung müsste über einen geeigneten Finanzdienstleister erfolgen, um die Landratsämter nicht mit den Kursschwankungen der Kryptowährungen zu belasten. Dies würde dem Grundsatz der Wirtschaftlichkeit und Sparsamkeit zuwider laufen. Es handelt sich hierbei auch eher um eine Maßnahme, die mehr dem Standortmarketing dient als der Vereinfachung bzw. Optimierung eines Prozesses.

Abschließend lässt sich sagen, dass vor Einführung einer Blockchain-basierten Lösung für einen Verwaltungsprozess genau geprüft werden muss, ob diese das Problem besser oder wirtschaftlicher bewältigen kann als die bestehende Lösung, da der Aufwand zur Schaffung einer Blockchain nicht zu vernachlässigen ist. Auch die Kosten zur Unterhaltung eines solchen Systems sind oftmals höher als die einer zentralisierten Alter-

native. Wenn diese Voraussetzungen jedoch gegeben sind, kann die Blockchain als sinnvolle und zukunftsorientierte Technologie eingesetzt werden.

Kernsätze

1. Eine Blockchain ist eine verteilte Datenbank, von der alle Teilnehmer in einem Netzwerk eine Kopie besitzen.
2. Durch entsprechende Algorithmen wird Konsens über den Inhalt der Datenbank und Fälschungssicherheit erreicht.
3. In Deutschland wurde das Potenzial der Blockchain auch für den öffentlichen Sektor erkannt, konkrete Maßnahmen fehlen im Gegensatz zu anderen Ländern jedoch noch.
4. Für die Umsetzung bietet sich die Open-Source-Lösung Hyperledger an.
5. Blockchain-basierte digitale Identitäten können mit Führerscheindaten verknüpft werden.
6. Die Ersetzung des deutschen Grundbuch-Systems durch eine vollständig digitale Lösung ist nicht zielführend.
7. E-Voting mittels Blockchain erfüllt alle Anforderungen an ein elektronisches Wahlsystem, nur die Überprüfbarkeit durch einen technisch nicht versierten Laien müsste vereinfacht werden.
8. Die Einhaltung der Kühlkette könnte durch eine Blockchain-basierte Lösung erfolgen, wäre aber mit einem erheblichen Anfangsaufwand verbunden.
9. Der Einsatz einer Blockchain-basierten Lösung sollte nur erfolgen, wenn eine Verbesserung zur bestehenden Lösung erreicht wird.
10. Der Einsatz dieser neuen Technologie kann in Verwaltungen und wechselseitig dazu in der freien Wirtschaft ein gewisses Innovationspotential freisetzen.

Literaturverzeichnis

Aublin, Pierre-Louis; **Mokhtar**, Sonia Ben; **Quéma**, Vivien: RBFT: Redundant Byzantine Fault Tolerance, 2013. Abgerufen am 06.03.2020, von https://pakupaku.me/plaublin/rbft/5000a297.pdf.

Berentsen, Alexander; **Schär**, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt, Books on Demand, 2017.

Böhme, Rainer; **Christin**, Nicolas; **Edelman**, Benjamin; **Moore**, Tyler: Bitcoin: Economics, Technology, and Governance. In: Journal of Economic Perspectives. Volume 29, Number 2, 2015, S. 213 – 238.

Castro, Miguel; **Liskov**, Barbara: Practical Byzantine Fault Tolerance, Cambridge, 1999. Abgerufen am 06.03.2020, von http://pmg.csail.mit.edu/papers/osdi99.pdf.

Curran, Kevin: E-Voting on the Blockchain, University of Ulster, 2018. Abgerufen am 13.03.2020, von https://doi.org/10.31585/jbba-1-2-(3)2018.

Drescher, Daniel: Blockchain Grundlagen, mitp Verlags GmbH & Co. KG, Frechen, 2017.

Dunkel, Jürgen; **Eberhart**, Andreas; **Fischer**, Stefan; **Kleiner**, Carsten; **Koschel**, Arne: Systemarchitekturen für verteilte Anwendungen,München, Carl Hanser Verlag, 2008.

Gajek, Sebastian; **Lewandowski**, Marco: Trustless, Censorship-Resilient and Scalable Votings in the Permission-based Blockchain Model, Flensburg, 2019. Abgerufen am 13.03.2020, von https://eprint.iacr.org/2019/617.pdf.

Glaser, Florian; **Bezzenberger**, Luis: Beyond Cryptocurrencies - A Taxonomy Of Decentralized Consensus, Proceedings of the 23rd European Conference on Information Systems, Münster, 2015.

Goos, Kerstin: Wahlen im Internet. Eine Analyse ihrer Bedeutung für die Wahlbeteiligung. Fraunhofer Verlag, Stuttgart, 2011.

Hosp, Julien: Blockchain 2.0: einfach erklärt – weit mehr als nur Bitcion. 3. Auflage, München, 2019.

IBM Corperation: About IBM Food Trust, 2019. Abgerufen am 19.03.2020, von https://www.ibm.com/downloads/cas/8QABQBDR.

Jacobovitz, Ori: Blockchain for Identity Management, 2016. Abgerufen am 25.02.2020, von https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf.

Kairos Future: The Land Registry in the blockchain – testbed, 2017. Abgerufen am 26.02.2020, von https://static1.squarespace.com/static/5e26f18cd5824c7138a9118b/t/5e3c35451c2cbb6170caa19e/1581004119677/Blockchain_Landregistry_Report_2017.pdf.

Kannengießer, Niclas; **Lins**, Sebastian; **Dehling**, Tobias; **Sunyaev**, Ali: What Does Not Fit Can be Made to Fit! - Trade-Offs in Distibuted Ledger Technology Designs, Karlsruhe, 2019.

Lamport, Leslie; **Shostak**, Robert; **Pease**, Marshall: The Byzantine Generals Problem, 1982. Abgerufen am 05.02.2020, von: https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf.

Mahn, Jan: Reine Vertrauensfrage – Blockchain-Technik jenseits von Kryptogeld. In: c‘t 23/2019, S.74 – 76.

Meier, Andreas; **Stormer**, Henrik: Blockchain = Distributed Ledger + Consensus. In: Kaufmann, Michael; Meier, Andreas: Blockchain. Springer Vieweg, Wiesbaden, 2018, S. 1139 – 1154.

Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008

NexT e.V. in Zusammenarbeit mit der Initiative "Blockchain in der Verwaltung Deutschland" (BiVD) und derCommunity of Practice Blockchain des NexT-Expertennetzwerks: Blockchain in der Verwaltung – Anwendungsbereiche und Herausforderungen, 2019. Abgerufen am 03.03.2020, von http://bivd-initiative.de/wp-content/uploads/2019/09/ Blockchain_in_der_Verwaltung_Teil_1_2019-09-06.pdf.

Olson, Kelly; **Bowman**, Mic; **Mitchell**, James; **Amundson**, Shawn; **Middelton**, Dan; **Montgomery**, Cian: Sawtooth: An Introduction, 2018. Abgerufen am 20.03.2020, von https://www.hyperledger.org/wp-content/uploads/2018/01/ Hyperledger_Sawtooth_WhitePaper.pdf.

Prause, Gunnar: e-Government als Standortfaktor, Hochschule Wismar, 2018. Abgerufen am 25.02.2020, von https://www.researchgate.net/profile/Gunnar_Prause/publication/326113548_e-Government_als_Standortfaktor/links/ 5b3a0c1da6fdcc8506e79ecf/e-Government-als-Standortfaktor.pdf.

Rupp, Carolin: Germanisches Grundbuch und romanisches Register, Hamburg, 2014.

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

Schütz, Andreas; **Fertig**, Tobias; **Weber**, Kristin; **Vu**, Henry; **Hirth**, Matthias; **Tran-Gia**, Thomas: Vertrauen ist gut, Blockchain ist besser – Einsatzmöglichkeiten von Blockchain für Vertrauensprobleme im Crowdsourcing. In: Kaufmann, Michael; Meier, Andreas: Blockchain. Springer Vieweg, Wiesbaden, 2018, S. 1155 – 1166.

Swan, Melanie: Blockchain. Blueprint for a New Economy, O´Reilly Media, Sebastopol, CA. 2015.

Tönnissen, Stefan; **Teuteberg**, Frank: Abbildung von Intercompany-Verträgen auf der Blockchain durch Smart Contracts – eine Fallstudie am Beispiel von IT-Services. In: Kaufmann, Michael; Meier, Andreas: Blockchain. Springer Vieweg, Wiesbaden, 2018, S. 1168 – 1184.

Walport, Mark: Distributed Ledger Technology: beyond block chain, 2015 Abgerufen am 06.02.2020, von https://www.gov.uk/government/uploads/system/uploads/ attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

Wätjen, Dietmar: Kryptographie, Grundlagen, Algorithmen, Protokolle, 3. Auflage, Wiesbaden, 2018.

Internetquellenverzeichnis

Axa S.A.	https://fizzy.axa/en-gb/faq (zuletzt geöffnet am 14.02.2020).
Bitcoin Suisse AG	https://www.bitcoinsuisse.com/about-us/ (zuletzt geöffnet am 19.03.2020).
Bundesamt für Sicherheit in der Informationstechnik	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=5 (zuletzt geöffnet am 20.03.2020).
Bundesamt für Statistik (Schweiz)	https://www.bfs.admin.ch/bfs/de/home/statistiken/bevoelkerung/stand-entwicklung.assetdetail.9447644.html (zuletzt geöffnet am 20.02.2020).
Bundesministerium des Innern, für Bau und Heimat	https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/So_geht_s/So_geht_s_node.html (zuletzt geöffnet am 06.03.2020).
Bundesministerium für Wirtschaft und Energie	https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=10 (zuletzt geöffnet am 20.03.2020).
Bundeszentrale für politische Bildung	https://www.bpb.de/nachschlagen/lexika/das-junge-politik-lexikon/161767/wahlgrundsaetze (zuletzt geöffnet am 06.03.2020).
Chaos Computer Club	https://www.ccc.de/system/uploads/105/original/nedapReport54.pdf (zuletzt geöffnet am 06.03.2020).
Crypto Valley Association	https://cryptovalley.swiss/about-the-association/ (zuletzt geöffnet am 22.02.2020).
Crypto Valley Association	https://cryptovalley.swiss/why-switzerland/ (zuletzt geöffnet am 22.02.2020).
Der Bundeswahlleiter (Statistisches Bundesamt)	https://www.bundeswahlleiter.de/service/glossar/o/online-wahlen.html (zuletzt geöffnet am 06.03.2020) Anmerkung: Webseite ist Stand 2015.
Ethereum Foundation	https://docs.ethhub.io/ethereum-basics/ethereum-foundation/ (zuletzt geöffnet am 22.02.2020).
Frankfurter Allgemeine Zeitung	https://www.faz.net/aktuell/finanzen/digital-bezahlen/kryptowaehrung-bitcoin-kurs-bricht-um-mehr-als-1000-dollar-ein-16402059.html (zuletzt geöffnet am 08.01.2020).
Frankfurter Allgemeine Zeitung	https://www.faz.net/aktuell/finanzen/meine-finanzen/mieten-und-wohnen/immobilienkauf-der-notarielle-vertrag-entscheidet-15283721.html (zuletzt geöffnet am 06.03.2020).
GitHub	https://github.com/ethereum/wiki/wiki/White-Paper (zuletzt geöffnet am 14.02.2020).
GitHub	https://github.com/hyperledger/indy-sdk/blob/master/docs/getting-started/indy-walkthrough.md (zuletzt geöffnet am 05.03.2020).

GitHub https://github.com/hyperledger/indy-plenum (zuletzt geöffnet am 05.03.2020).

GitHub https://github.com/hyperledger/indy-sdk/blob/master/docs/getting-started/indy-walkthrough.md (zuletzt geöffnet am 05.03.2020).

GitHub https://github.com/hyperledger/indy-node (zuletzt geöffnet am 06.03.2020).

Heise Medien https://www.heise.de/newsticker/meldung/Im-tiefen-Tal-der-Kryptowaehrungen-Ein-Besuch-in-Zug-3760567.html?seite=all (zuletzt geöffnet am 22.02.2020).

Heise Medien https://www.heise.de/newsticker/meldung/Im-tiefen-Tal-der-Kryptowaehrungen-Ein-Besuch-in-Zug-3760567.html?seite=all (zuletzt geöffnet am 22.02.2020).

HS Mittweida https://blockchain.hs-mittweida.de/ueber-uns/ (zuletzt geöffnet am 19.02.2020).

HS Mittweida https://blockchain.hs-mittweida.de/bsrm/ (zuletzt geöffnet am 19.02.2020).

HS Mittweida https://blockchain.hs-mittweida.de/wordpress/wp-content/uploads/2018/04/Landesblockchain_fuer_Sachsen.pdf (zuletzt geöffnet am 20.02.2020).

IBM Corporation https://www.ibm.com/de-de/blockchain/solutions/food-trust (zuletzt geöffnet am 18.03.2020).

IBM Corporation, Maersk A/S https://www.tradelens.com/ecosystem (zuletzt geöffnet am 19.03.2020).

IT-Planungsrat https://www.it-planungsrat.de/DE/ITPlanungsrat/RechtlicheGrundlagen/rechtliche_grundlagen_node.html (zuletzt geöffnet am 20.02.2020).

IT-Planungsrat https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/30_Sitzung/Blockchain_Bericht.pdf?__blob=publicationFile&v=1 (zuletzt geöffnet am 20.02.2020).

IT-Planungsrat https://dezentraleverwaltung.de/index.php/blockchain-projekte-in-deutschland/ (zuletzt geöffnet am 20.02.2020).

Jonas Verhoelen https://www.informatik-aktuell.de/betrieb/virtualisierung/eine-blockchain-anwendung-mit-hyperledger-fabric-und-composer.html (zuletzt geöffnet am 28.02.2020).

Jorge Stolfi https://de.wikipedia.org/wiki/Hashfunktion#/media/Datei:Hash_table_4_1_1_0_0_1_0_LL.svg (zuletzt geöffnet am 25.03.2020).

Kanton Zug https://www.zg.ch/portraet/kennzahlen (zuletzt geöffnet am 20.02.2020).

Karin Dobberschütz https://www.gg-digital.de/2019/06/ein-kleines-land-schreibt-e-health-gross/index.html (zuletzt geöffnet am 25.02.2020).

Kraftfahrt-Bundesamt https://www.kba.de/DE/ZentraleRegister/

ZFER/zfer_node.htmlgl (zuletzt geöffnet am 03.03.2020).

Laura Marissa Cullell https://hackernoon.com/e-estonia-is-not-on-blockchain-22iy2gx6 (zuletzt geöffnet am 25.02.2020).

Linux Foundation https://wiki.hyperledger.org/display/fabric (zuletzt geöffnet am 27.02.2020).

Linux Foundation https://hyperledger-fabric.readthedocs.io/en/release-1.4/whatis.html (zuletzt geöffnet am 27.02.2020).

Linux Foundation https://hyperledger-fabric.readthedocs.io/en/release-1.4/arch-deep-dive.html (zuletzt geöffnet am 28.02.2020).

Linux Foundation https://wiki.hyperledger.org/display/indy/Hyperledger+Indy (zuletzt geöffnet am 28.02.2020).

Linux Foundation https://wiki.hyperledger.org/display/INTERN/Extending+HL+Fabric+for+connecting+with+HL+Indy (zuletzt geöffnet am 10.03.2020).

Linux Foundation https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html (zuletzt geöffnet am 10.03.2020).

Linux Foundation https://hyperledger-fabric.readthedocs.io/en/release-1.4/identity/identity.html (zuletzt geöffnet am 10.03.2020).

Linux Foundation https://www.hyperledger.org/blog/2018/09/20/bitagora-a-decentralized-voting-platform-built-on-hyperledger-sawtooth (zuletzt geöffnet am 15.03.2020).

Linux Foundation https://sawtooth.hyperledger.org/examples/ (zuletzt geöffnet am 18.03.2020).

Linux Foundation https://sawtooth.hyperledger.org/examples/seafood.html (zuletzt geöffnet am 18.03.2020).

Litecoin Project https://litecoin.org/ (zuletzt geöffnet am 14.02.2020).

Max Thake https://medium.com/nakamo-to/what-is-proof-of-stake-pos-479a04581f3a (zuletzt geöffnet am 14.02.2020).

Microsoft Corporation https://docs.microsoft.com/en-us/azure/architecture/patterns/publisher-subscriber (zuletzt geöffnet am 13.03.2020).

Monero Project https://web.getmonero.org/ (zuletzt geöffnet am 14.02.2020).

Nick Szabo http://alamut.com/subj/economics/nick_szabo/smartContracts.html (zuletzt geöffnet am 14.02.2020).

Oliver Schneider https://www.it-markt.ch/news/2018-06-25/zug-steigt-mit-der-blockchain-in-den-e-voting-ring (zuletzt geöffnet am 28.02.2020).

Sächsische Staatskanzlei https://amt24.sachsen.de/web/guest/lebenslage/-/lebenslage/Grundbuch-5000850-lebenslage-0 (zuletzt geöffnet am 06.03.2020).

Satoshi Nakamoto https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html (zuletzt geöffnet am 04.02.2020).

Schweizer Radio und Fernsehen https://www.srf.ch/play/tv/reporter/video/die-vertreibung-aus-dem-paradies-wie-zug-den-zugern-allmaehlich-abhanden-kommt?id=c96dcd39-f98a-47aa-a6d9-345e907283bc (zuletzt geöffnet am 20.02.2020).

Sovrin Foundation https://sovrin.org/faqs/ (zuletzt geöffnet am 06.03.2020)

Stadt Zug https://www.stadtzug.ch/newsarchiv/431448 (zuletzt geöffnet am 22.02.2020).

Stadt Zug https://www.stadtzug.ch/_docn/1939723/eVoting_Stadt_Zug_Abschlussbericht_DE.pdf (zuletzt geöffnet am 22.02.2020).

Statistisches Bundesamt https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/IT-Nutzung/Tabellen/zeitvergleich-computernutzung-ikt.html;jsessionid=81AAE09B9353E1B6F40FF918D46522F3.internet712 (zuletzt geöffnet am 06.03.2020).

Eidesstattliche Versicherung

Eidesstattliche Versicherung

Ich versichere hiermit an Eides Statt, dass ich die vorgelegte Bachelorarbeit selbstständig verfasst, nur die angegebenen Quellen und Hilfsmittel benutzt sowie alle Stellen der Arbeit, die wörtlich oder sinngemäß aus anderen Quellen übernommen wurden, als solche kenntlich gemacht habe und die Bachelorarbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegt worden ist.

Die gedruckte und digitalisierte Version der Bachelorarbeit sind identisch.

Meißen, 30.03.2020 *Unterschrift*