Kanton Zürich
Staatskanzlei
Digitale Verwaltung und E-Government

Studie zum Einsatz der Blockchain-Technologie in der kantonalen Verwaltung

Impressum

Die vorliegende Studie wurde im Rahmen des Projekts IP1.5 «Einsatz Blockchain-Technologie» erarbeitet und am 28. August 2020 publiziert. Das Projekt ist Teil des Impulsprogramms der «Strategie Digitale Verwaltung 2018–2023» des Kantons Zürich.

Autoren
- Rauschenbach, Rolf, Dr. rer. publ., Procivis AG
- Stucki, Sven, MSc ETH Elektrotechnik und Informationstechnologie, Procivis AG

Projektauftraggeber
- Giarritta, Peppino, Dr. sc. nat., Leiter Abteilung Digitale Verwaltung und E-Government, Staatskanzlei

Projektleiter
- Lehmann, Benjamin, B.A., Digitale Verwaltung und E-Government, Staatskanzlei

Projekt-Fachgruppe
- Amsler, Andreas, M.A., Leiter OpenZH, Fach- und Koordinationsstelle OGD, Statistisches Amt
- Gnädinger, Beat, Dr. phil., Staatsarchivar
- Hasler-Dierauer, Beatrice, lic. rer. publ., Kommunikation, Digitale Verwaltung und E-Government, Staatskanzlei
- Hefti, Esther, Dr. iur., Rechtsdienst, Koordinationsstelle IDG, Staatskanzlei
- Spada, Paolo, Dipl. Betriebs- und Produktionsingenieur ETHZ, Strassenverkehrsamt
- Stamm, Christa, Dr. iur., Abteilung Recht und Informationssicherheit, Datenschutzbeauftragte des Kantons Zürich
- Waldvogel, Bernhard, MAS Informationssicherheit, Abteilung Recht und Informationssicherheit, Datenschutzbeauftragte des Kantons Zürich
- Weibel, Lukas, Executive MBA HSG Business Engineering, Leiter Business Engineering und Serviceentwicklung, Digitale Verwaltung und E-Government, Staatskanzlei
- Zeugin, Marc, Amt für Informatik

Inhalt

1. Zielsetzung und Vorgehen 5
1.1. Ausgangslage 5
1.2. Ziele und Abgrenzung 5
1.3. Auftrag 5
1.4. Vorgehen 6

2. Einführung 7
2.1. Was ist eine Blockchain? 7
2.2. Welche Arten von Blockchains gibt es? 9
2.3. Welche Konsensregeln gibt es? 10
2.4. Was sind Smart Contracts? 13
2.5. Wie entwickelt sich die Blockchain-Technologie weiter? 14
2.6. Wann machen Blockchains in der öffentlichen Verwaltung grundsätzlich Sinn? 15

3. Konkrete Anwendungsbeispiele aus der öffentlichen Verwaltung 19
3.1. Handelsregisterauszug (Kanton Genf) 21
3.2. Unterschriftsberechtigungen (Kanton Genf) 22
3.3. Betreibungsregisterauszug (Kanton Schaffhausen) 24
3.4. Bezahlung amtlicher Gebühren mit Kryptowährungen (Stadt und Kanton Zug) 26
3.5. Elektronische Identität (Stadt Zug) 27
3.6. Internetbasiertes Abstimmen (Stadt Zug) 29
3.7. Cardossier (Strassenverkehrsamt Aargau und andere) 30
3.8. Reparaturbestätigungsverfahren (Fürstentum Liechtenstein) 32

4. Mögliche Anwendungsbeispiele für den Kanton Zürich 34
4.1. Registrierung von amtlichen Dokumenten auf der Blockchain zur Stärkung der Rechtssicherheit 36
4.2. Personendossier mit Blockchain-basiertem Logbuch zur Erhöhung der Transparenz 40
4.3. Inventarkontrolle auf der Blockchain zur Stärkung der Rechtssicherheit 43
4.4. Öffentliche Ausschreibungen auf der Blockchain 47
4.5. Vergleich der möglichen Anwendungsbeispiele 49

5. Zusammenfassung 51

6. Fazit 53
6.1. Allgemeine Einschätzung 53
6.2. Mehrwerte der Blockchain-Technologie 53
6.3. Handlungsbedarf 54
6.4. Nächste Schritte 55

7. Weiterführende Literatur 56

Abbildungen

Abbildung 1: Schematischer Ablauf der Registrierung von amtlichen Dokumenten 37
Abbildung 2: Schematischer Ablauf des Personendossiers mit Blockchain-basiertem Logbuch 41
Abbildung 3: Schematischer Ablauf der Blockchain-basierten Inventarkontrolle 44

Tabellen

Tabelle 1: Blockchains mit unterschiedlichen Graden der Zugangsrechte 10
Tabelle 2: Konsensregeln für Blockchains 11
Tabelle 3: Vergleich der vier möglichen Anwendungsbeispiele 50

1. Zielsetzung und Vorgehen

1.1. Ausgangslage

Der Regierungsrat hat am 25. April 2018 die Strategie «Digitale Verwaltung 2018–2023» festgesetzt. Sie zeigt auf, wie die kantonale Verwaltung die digitale Entwicklung gestalten und die Chance der Digitalisierung nutzen will. Teil der Strategie ist ein Impulsprogramm mit Digitalisierungsvorhaben, die vorrangig und eng koordiniert angegangen werden. Das Impulsprogramm beinhaltet unter Ziel 1 «Vereinfachung und Ausbau des digitalen Leistungsangebotes» das Projekt IP1.5 «Einsatz der Blockchain-Technologie».

Die Blockchain-Technologie ist in der Verwaltung des Kantons Zürich bisher nicht im Einsatz. Das Interesse an Informationen zu Blockchain ist gross, sowohl betreffend allgemeine Grundlagen als auch konkreten Anwendungsbeispielen. Mit diesem Projekt soll eine Einschätzung des Potentials der Blockchain-Technologie mit Fokus auf Geschäftsfälle der kantonalen Verwaltung vorgenommen werden und eine Informationsgrundlage hinsichtlich fachlicher, technischer, rechtlicher und politischer Aspekte zur Verfügung gestellt werden.

1.2. Ziele und Abgrenzung

Mit diesem Projekt werden die folgenden Ziele verfolgt:

- Einschätzen des Potenzials der Blockchain-Technologie mit Fokus auf Geschäftsfälle der kantonalen Verwaltung
- Prüfen, in welchen Arten von Geschäftsfällen und Transaktionen in der kantonalen Verwaltung der Einsatz der Blockchain-Technologie Mehrwert bieten würde
- Eruieren, welche Anforderungen für einen Einsatz erfüllt werden müssen
- Analysieren und Beurteilen der aktuellen Marktentwicklung und bestehender Anwendungsfälle anderer Kantone und anderer Länder
- Bereitstellung einer allgemeinen Informationsgrundlage zum Thema Blockchain-Technologie in der kantonalen Verwaltung
- Formulierung von Empfehlungen zu den Bereichen Politik, Recht, Fach und Technik, wie der Einsatz der Blockchain-Technologie in der öffentlichen Verwaltung weiter vorbereitet werden kann.

Nicht Bestandteil dieses Projekts sind die Planung und Entwicklung konkreter technischer Lösungen und der Einsatz in konkreten Geschäftsfällen der Verwaltung.

1.3. Auftrag

Mit der Durchführung der Studie wurde die Procivis AG betraut. Das Mandat umfasste insbesondere die Erarbeitung folgender Inhalte:

- Einführung ins Thema Blockchain
- Darstellung nationaler und internationaler Anwendungsbeispiele der Blockchain-Technologie im öffentlichen Sektor
- Beschreibung von möglichen Anwendungsbeispielen für den Kanton Zürich
- Schlussfolgerungen und Handlungsempfehlungen

1.4. Vorgehen

Die Autoren erarbeiteten die vorliegende Studie zwischen Juli 2019 und August 2020. In Arbeitssitzungen mit Vertreterinnen und Vertretern der kantonalen Verwaltung, insbesondere der Abteilung Digitale Verwaltung und E-Government sowie aus den Bereichen Fach, Recht, Datenschutz und Technik wurden die Fragestellungen erarbeitet und verfeinert und die Studieninhalte geprüft. Die Darstellungen der Anwendungsbeispiele anderer Kantone und Städte sind im Austausch mit Vertreterinnen und Vertretern dieser Projekte entstanden.

Die Autoren danken an dieser Stelle dem Projektteam und allen Dritten, die an dieser Studie mitgearbeitet haben, namentlich:

- Candrian, Severin, Head of Product Design, Gasteiger, Daniel, CEO, Graber, Patrick, Chief Commercial Officer, Jakelj, Sven, Business Development, Loetscher, Jonas, Chief Product Officer, alle Procivis AG
- Denzler, Alexander, Professor, Head Blockchain Lab, Hochschule Luzern
- Diemers, Daniel, Dr. oec., Swiss Blockchain Federation
- Fleck, Titus, Abteilungsleiter Application & eGovernment Services, Stv. Geschäftsführer, KSD Schaffhausen
- Frommelt, Otto C., Dr., Amtstellenleitung, Amt für Strassenverkehr, Fürstentum Liechtenstein
- Gerlach, Jan, IT-Systems Engineer, Stadt Zug
- Hess, Andreas, Leiter Handelsregister- und Konkursamt, Kanton Zug
- Killer, Christian, Doktorand, Department of Informatics - Communication Systems Group, Universität Zürich
- Lemaître, Nicolas, Projektleiter Smart City, Stadt Zug
- Luethi, Eva, Manager New Business Development, Digital Business Building, Harms, Holger, Manager Banking Technology, beide Swisscom AG
- Moi, Giancarlo, Affaires numériques, Département de l'Economie, Direction générale du développement économique, de la recherche et de l'innovation (DG DERI), République et Canton de Genève
- Nyffenegger, Florian, Chief Digital Officer, Abraxas Informatik AG
- Schenker, Melanie, Leiterin Einwohnerkontrolle, Stadt Zug
- Sprenger, Martin, Stabsbereichsleiter Fachservices und Personal, Kanton Aargau, Präsident, Verein Cardossier
- Willemin, Philippe, Architecte logiciel, République et Canton du Jura
- Würmli, Martin, Stadtschreiber Zug
- Zavolokina, Liudmila, Dr. sc. UZH in Wirtschaftsinformatik, Consultant, Ergon Informatik AG

2. Einführung

Die erste Blockchain – Bitcoin – wurde lanciert, um ein Währungssystem zu schaffen, das weder auf eine Zentral- noch auf Geschäftsbanken angewiesen war. Dies gelang dank der Verknüpfung von Ansätzen aus der Verschlüsselungs- und Netzwerktechnologie und der Ökonomie. Bitcoin funktioniert bis heute dank konsequenter Transparenz, einem Verfahren, dass Veränderungen der Geschichte praktisch verunmöglicht. Mit dem Bekanntwerden der Blockchain-Technologie kam die Frage auf, in welchen anderen Bereichen dieser Ansatz ebenfalls Nutzen stiften kann, sind doch **Transparenz** und **Unverfälschbarkeit** Anforderungen, die vielerorts relevant sind. Mit der Weiterentwicklung der Blockchain-Technologie wurde auch deutlich, dass diese zur Erhöhung der **Effizienz** eingesetzt werden kann. Mit Fragen der Transparenz und Effizienz sehen sich auch eine kantonale Verwaltung konfrontiert. Inwiefern die Blockchain-Technologie hierauf eine Antwort bedeutet, beleuchtet die vorliegende Studie. Sie ist folgendermassen aufgebaut:

Im Kapitel 2 werden die **Grundlagen** gelegt, die zum Verständnis der Blockchain-Technologie erforderlich sind. Ausgehend davon wird diskutiert, wann die Anwendung der Blockchain-Technologie in der öffentlichen Verwaltung Sinn macht. Im Kapitel 3 werden die **bisherigen Erfahrungen** bei der Anwendung der Blockchain-Technologie in der öffentlichen Verwaltung dargestellt. Dabei wird der Fokus auf die Projekte gelegt, die in der Schweiz und dem Fürstentum Liechtenstein realisiert wurden oder zurzeit laufen. Im Kapitel 4 werden vier konkrete **Anwendungsfelder** aufgezeigt, in denen die Blockchain-Technologie eingesetzt werden könnte. Eine erste Beurteilung dieser Beispiele macht deutlich, dass eine Blockchain-Lösung in unterschiedlichem Masse Nutzen stiften kann. Nach einer **Zusammenfassung** (Kapitel 5) wird die Studie mit einem **Fazit** (Kapitel 6) abgerundet.

2.1. Was ist eine Blockchain?

Eine Blockchain ist die Aneinanderreihung von Datensätzen, Blöcke genannt, die durch kryptographische Verfahren miteinander fest verkettet sind. Die Darstellung von Informationen als Kette («Chain») von Blöcken («Block») ergibt das Kunstwort «Blockchain».

Ein einzelner **Block** beschreibt einen Sachverhalt zu einem bestimmten Zeitpunkt. Dieser Sachverhalt kann zum Beispiel ein Kontostand oder ein Kontoübertrag sein; es ist aber auch möglich, in einem Block eine Vielzahl von Transaktionen darzustellen. Anstelle von monetären Werten können aber auch andere Sachverhalte beschrieben werden: Attribute von Objekten und Personen, computerlesbare Medien, rechtliche Ansprüche im weiteren Sinne und vieles mehr. Aus einem Block wird eine **Blockchain,** indem mehrere Blöcke chronologisch aneinandergereiht werden. Jeder Block beschreibt den Zustand oder die Veränderung des von der Blockchain abgebildeten Sachverhalts zum jeweiligen Zeitpunkt. Anhand der Blockchain kann also die Entwicklung eines Sachverhalts Schritt für Schritt – sprich Block für Block – nachvollzogen werden. Eine Blockchain entspricht damit, vereinfacht formuliert, einer Abfolge von Versionen einer Datenbank.

Die Blöcke einer Blockchain sind durch kryptografische Verfahren so miteinander verknüpft, dass sie untrennbar werden. Denn in jedem Block ist ein Fingerabdruck des vorangehenden Blocks enthalten und somit kann – Block für Block – die Authentizität der Blockchain geprüft werden. Möglich wird dies mittels kryptografischer **Hash-Funktionen.** Eine Hash-Funktion erlaubt es, eine beliebig grosse Eingabemenge – in unserem Fall einen Block – auf eine

kleine Zielmenge, als eindeutigen Fingerabdruck, abzubilden. Die Zielmenge ist immer konstant gross, beispielsweise eine Abfolge von 256 Bit. Während die Berechnung der Zielmenge einfach und schnell erfolgt, ist das Zurückrechnen von der Zielmenge auf die Eingabemenge praktisch unmöglich. Indem jeder Block den Hash des vorangehenden Blocks enthält, wird die Geschichte des beschriebenen Sachverhalts mit geringem Aufwand unumkehrbar tradiert. Zudem ist es praktisch unmöglich einen einzelnen Block unbemerkt zu manipulieren, da der Fingerabdruck im folgenden Block ungültig würde und dies bei Prüfungen auffiele.

Blöcke beziehungsweise eine Blockchain kann zentral auf einem Rechner generiert werden. Es ist aber auch möglich und üblich, eine Blockchain dezentral von einer Vielzahl von unabhängigen Rechnern generieren zu lassen. Damit wird die in der Blockchain enthaltene Information auf unabhängige Systeme verteilt. Da über den abgebildeten Sachverhalt nun verteilt («Distributed») Buch («Ledger») geführt wird, fällt die Blockchain-Technologie in die Kategorie der **Distributed Ledger-Technologien** (DLT). Die Begriffe «DLT» und «Blockchain» werden häufig synonym und austauschbar verwendet. Dies ist nicht ganz richtig, denn es existieren auch DLT, die zwar Informationen verteilen, aber nicht als Blockchain speichern. Durch das Verteilen wird es sowohl bei DLT als auch bei Blockchain praktisch unmöglich, Information zu manipulieren oder gar zu zerstören. Bei den meisten frei zugänglichen Blockchains (siehe dazu den Abschnitt über die Konsensregeln in Kapitel 2.2) wäre es erforderlich, die Kontrolle über die absolute Mehrheit der beteiligten Rechner auszuüben.

Mit dem **Bitcoin** wurde 2009 die erste grosse Blockchain-Anwendung lanciert, wobei Bitcoin sowohl eine spezifische Blockchain als auch ein digitales Zahlungsmittel bezeichnet. Die Bitcoin-Blöcke speichern als Sachverhalt die Transaktionen, die mit dem Bitcoin durchgeführt wurden. Aus der Gesamtheit aller in den Blöcken enthaltener Transaktionen kann der Stand jedes Bitcoin-Kontos errechnet werden. Die Innovation, die mit Bitcoin gelungen ist, liegt darin, dass eine Lösung für das Double-spending-Problem gefunden wurde, die ohne zentrale Autorität auskommt. Das Double-spending-Problem beschreibt die Gefahr, dass jemand versuchen kann, mit dem gleichen Geld unterschiedliche Forderungen zu begleichen. Traditionellerweise verhindern Banken solchen Missbrauch. Die Lösung von Satoshi Nakomoto (2008) liegt in einer Kombination von Kryptografie, Netzwerk- und Spieltheorie. Kryptografische Verfahren kommen insbesondere zum Einsatz bei der Vergabe der Bitcoin-Konten (öffentliche und private Schlüssel), der Erzeugung von Hashes von Blöcken und der Proof-of-Work-Konsensregel (siehe Kapitel 2.3.). Auf netzwerktheoretischen Überlegungen basiert die offene, dezentrale Architektur der Bitcoin-Nodes. Die Anreize, die dafür sorgen, dass Bitcoin seit über zehn Jahren erfolgreich betrieben wird, folgen spieltheoretischen Überlegungen (Narayanan & Clark, 2017).

In der Zwischenzeit sind mehrere Hunderte solcher digitalen Zahlungsmittel lanciert worden. Basiert ein digitales Zahlungsmittel auf einer eigenständigen Blockchain, wird die Währung als **Coins** bezeichnet. Zahlungsmittel, die auf einer gegebenen Blockchain aufbauen – zum Beispiel auf Ethereum – werden als **Tokens** bezeichnet; mit ihnen lassen sich komplexere Anwendungen programmieren. Der Wert von Coins und Tokens muss sich – wie auch bei jeder anderen Währung – täglich neu bestätigen. Da aus technischer Sicht nicht nur Geldwerte auf einer Blockchain abgebildet werden können, sondern jegliche Informationen, sind in der Zwischenzeit alle erdenklichen Anwendungsfälle ins Spiel gebracht worden. Grundsätzlich können auf einer Blockchain unstrukturierte (zum Beispiel ein Dokument mit einem Kontostand) oder strukturierte (zum Beispiel der Kontostand in Verbindung mit einem Datum) Daten dargestellt werden, dies zudem in verschlüsselter oder unverschlüsselter Form. Die jeweilige Wahl ergibt sich aus dem konkreten Anwendungsfall.

2.2. Welche Arten von Blockchains gibt es?

Seit der Lancierung von Bitcoin sind unzählige andere Blockchains entwickelt worden, mit teilweise komplett unterschiedlichen Eigenschaften. Einen vollständigen Überblick zu erlangen ist praktisch unmöglich geworden. Blockchains können nach verschiedenen Kriterien gruppiert werden, wobei in der Regel die Zugangsrechte im Vordergrund stehen; sie werden in diesem Kapitel vorgestellt. Im nächsten Kapitel wird auf die Konsensregeln eingegangen, die ein weiteres wichtiges Unterscheidungsmerkmal von Blockchains sind; sie hängen von der Art der Zugangsrechte ab.

Das **Zugangsrecht** legt fest, ob die Leserechte sowie Schreibrechte auf die Blockchain eingeschränkt sind. Sind die Leserechte nicht eingeschränkt (**public**), kann jede Person mit einem Zugang zur Blockchain diese auch einsehen. Sind die Leserechte auf eine Benutzergruppe eingeschränkt (**private**), können hingegen nur autorisierte Personen die Blockchain einsehen. Analog kann der Schreibzugriff entweder nicht eingeschränkt (**permissionless**) oder auf eine Benutzergruppe beschränkt sein (**permissioned**).

Lese- und Schreibrechten können in allen Kombinationen gewährt werden. Die Wahl des Grads der Zugangsrechte hängt typischerweise davon ab, welche Anwendungen und Funktionen mit der Blockchain abgedeckt werden sollen. Entsprechend erscheint beispielsweise die Eigenschaft Transparenz je nach Kontext als Vorteil (niederschwelliger Zugang zu Informationen, die auf einer [public] Blockchain abgebildet sind) oder als Nachteil (Transparenz verstösst gegen das Datenschutzrecht).

Bitcoin ist eine jener public Blockchains, die das Prinzip des freien Zugangs radikal umsetzen. Wer eine Internetverbindung hat, kann die Blockchain herunterladen und uneingeschränkt mitlesen (public), wie sich die Bitcoin-Blockchain entwickelt. Gleichfalls ist es möglich, selbst uneingeschränkt Bitcoin-Transaktionen als Blöcke auf die Blockchain zu schreiben (permissionless). Andere Blockchains – wie zum Beispiel Ripple – gewähren zwar allen Einblick (public); das Recht, Transaktionen vorzunehmen und Blocks zu berechnen, ist allerdings einem eingeschränkten Kreis vorbehalten (permissioned).

Private (permissioned) Blockchains finden in geschlossenen Gruppen ihre Anwendung. Zudem kann für private Blockchains unterschieden werden, ob sie von einer einzelnen Organisation (private Blockchain) oder einem Konsortium (Consortium Blockchain) betrieben werden. Konsortien haben den Vorteil der geringeren Zentralisierung und höheren Datenintegrität. Sinnvoll sind private Blockchains für die öffentliche Verwaltung immer dann, wenn die Hoheit über den Zugang und Inhalt von Daten gewahrt werden soll.

Beispielsweise könnten Kantone und der Bund in einem Konsortium übergreifende Informationen wie Betreibungsregister, Strafregister oder Schulabschlüsse auf einer private-permissioned Blockchain hinterlegen und sich einander zugänglich machen. Die Infrastruktur kann dabei von den staatlichen Institutionen als Konsortium betrieben oder als Service bezogen werden. Der Kanton Schaffhausen setzte für den Testbetrieb Betreibungsregister (Kapitel 3.3) beispielsweise die «Consensus-as-a-Service»-Blockchain-Infrastruktur (neu «Swiss Trust Chain») von Die Post und Swisscom ein.

		Schreibrecht, um Transaktionen vorzunehmen und Blöcke zu generieren	
		eingeschränkt (permissioned)	**nicht eingeschränkt (permissionless)**
Leserecht, um Verlauf nachzuvollziehen	**eingeschränkt (private)**	**private-permissioned** Insbesondere geeignet für schützenswerte Daten. In der Regel in Kombination mit der Konsensregel Proof-of-Authority Beispiele • Hyperledger Fabric • Enterprise Ethereum Alliance	**private-permissionless** Bisher als theoretisch erachtete Kombination. Wenn Datenschutz wichtig ist, aber kein Konsortium gebildet werden kann, um diesen mit permissioned zu garantieren, versprechen neue Projekte, dass dies durch eine Kombination von on- und off-chain-Prozessen möglich sei. Beispiele • Holochain • LTO network
	nicht eingeschränkt (public)	**public-permissioned** Insbesondere geeignet für Daten, die als nicht schützenswert gelten. In der Regel in Kombination mit den Konsensregeln Proof-of-Stake oder Proof-of-Authority Beispiele • Sovrin • EOS	**public-permissionless** Insbesondere geeignet für Daten, die als nicht schützenswert gelten. In der Regel in Kombination mit der Konsensregel Proof-of-Work Beispiele • Bitcoin • Ethereum

Tabelle 1: Blockchains mit unterschiedlichen Graden der Zugangsrechte

2.3. Welche Konsensregeln gibt es?

Eine Blockchain bildet jeweils einen Sachverhalt ab, der einen erheblichen materiellen, inhaltlichen oder ideellen Wert haben kann. Wer neue Blöcke berechnen kann, verfügt damit über erhebliche Macht, weil er oder sie bestimmt, was «ist». Insbesondere im Fall von Blockchains mit nicht eingeschränktem Schreibzugriff (permissionless) müssen zusätzliche Vorkehrungen getroffen werden, damit bei der Berechnung neuer Blöcke Missbrauch ausgeschlossen wird. Dies geschieht, indem **Konsensregeln** zur Anwendung gebracht werden. Eine Konsensregel legt fest, nach welchen Prinzipien entschieden wird, wer den neuen Block berechnen darf beziehungsweise wie dieser erzeugt wird. Auch bei den Konsensregeln liegt inzwischen eine Vielzahl von Varianten vor. Die folgende Tabelle listet die wichtigsten auf:

Konsensregel	Beschreibung der Konsensregel	Beispiele
Proof-of-Work	Konsens entsteht durch das Lösen von vorgegebenen komplexen mathematischen Problemen. Die Lösung kann nur durch den Einsatz von viel Rechenleistung gefunden werden; die Überprüfung der Richtigkeit der Lösung ist allerdings einfach. Eine ausführliche Darstellung erfolgt im Anschluss an diese Tabelle. Eine ähnliche Konsensregel ist Proof-of-Capacity. • Insbesondere geeignet für Daten, die als nicht schützenswert gelten. In Kombination mit public-permissionless Blockchains. • Erschwerte Skalierbarkeit	Bitcoin, Ethereum
Proof-of-Stake	Zentraler Aspekt dieser Konsensregel ist, dass jene, die neue Blocks erzeugen wollen, dafür einen Vermögenswert als Garantie hinterlegen müssen. Dieser kann bei Regelverstoss eingezogen werden. Eine ausführliche Darstellung erfolgt im Anschluss an diese Tabelle. Ähnliche Konsensregeln sind Delegated Proof-of-Stake, Leased Proof-of-Stake, Proof-of-Importance, Proof-of-Burn, Proof-of-Weight. • Geeignet für Daten, die als schützenswert oder nicht schützenswert gelten. Insbesondere in Kombination mit public-permissionless Blockchains. • Problemlose Skalierbarkeit	NEO
Practical Byzantine Fault Tolerance	Aufgrund der Annahme, dass einzelne Teilnehmerinnen und Teilnehmer eines Netzwerks fehlerhaft oder missbräuchlich arbeiten, werden bei diesem Verfahren so lange Nachrichten untereinander ausgetauscht, bis mit hoher statistischer Sicherheit gesagt werden kann, dass diese zutreffen. Sobald dieser Zustand erreicht ist, wird per Mehrheitsbeschluss der neue Block berechnet. Ähnliche Konsensregeln sind Simplified Byzantine Fault Tolerance, Delegated Byzantine Fault Tolerance. • Geeignet für Daten, die als schützenswert oder nicht schützenswert gelten. Insbesondere in Kombination mit public-permissionless Blockchains. • Skalierbarkeit teilweise erschwert	Hyperledger Fabric
Proof-of-Authority	Diese Konsensregel wird bei permissioned (public/private) Blockchains angewendet, bei denen der Zugang, insbesondere bezüglich der Berechnung neuer Blocks, limitiert ist. Je nach der Ausgestaltung der Konsensregel besteht eine fixe Abfolge der Berechtigung zur Berechnung der neuen Blocks, oder diese ist gleich verteilt. • Insbesondere geeignet für schützenswerte Daten. In Kombination mit private Blockchains. • Problemlose Skalierbarkeit	Ethereum Rinkeby Testnet

Tabelle 2: Konsensregeln für Blockchains

Im Fall von **Proof-of-Work** ist jener Rechner autorisiert, den nächsten Block zu erzeugen, der das in diesem Zusammenhang formulierte mathematische Problem als Erster gelöst hat. Das mathematische Problem ist so gestaltet, dass es nur durch «Ausprobieren» gelöst werden kann. Dies bedeutet, dass jene, die über mehr Rechenleistung verfügen, im Vorteil sind und statistisch gesehen öfter das Problem lösen können als jene mit weniger Rechenleistung. Die Tätigkeit des «Ausprobierens» wird mit «Mining» (Schürfen) bezeichnet, ein entsprechender Rechner heisst «Mining Node» (Schürfknoten). Der Schwierigkeitsgrad des mathematischen Problems richtet sich üblicherweise dynamisch an der im gesamten Netzwerk verfügbaren Rechenleistung aus.

Mit dem Mining sind erhebliche Kosten verbunden: Es ist dafür spezialisierte Hardware und viel Strom erforderlich. Aus diesem Grund werden die Mining Nodes entlohnt; in der Regel in dem sie gleichzeitig mit der Erzeugung eines neuen Blocks auch neue Coins emittieren können. Über das ganze Netzwerk gesehen, ist der Aufwand zur Berechnung neuer Blocks damit gross, denn nicht nur jener Mining Node, der den neuen Block generieren darf, hat zuvor versucht, das mathematische Problem zu lösen, sondern alle Mining Nodes. Der Vorteil dieses Umstands ist, dass damit eine Manipulation nur mit unverhältnismässigem Aufwand möglich wäre. Der Nachteil ist, dass dabei Ressourcen im grossen Stil und scheinbar sinnlos verbraucht werden. Aus ökologischer Sicht ist diese Kritik nachvollziehbar. Es ist aber just der mit dem Ressourcenverbrauch verbundene Aufwand, der das System so sicher und – aus der subjektiven Sicht der Teilnehmenden – so wertvoll macht.

Die **Proof-of-Stake**-Konsensregel ist ein Versuch, die Probleme von Proof-of-Work zu entschärfen. Neben dem hohen Ressourcenverbrauch fällt bei Proof-of-Work auch ins Gewicht, dass pro Zeiteinheit nur eine begrenzte Anzahl von Transaktionen verarbeitet werden kann (Problem der Skalierung). Die konkrete Ausgestaltung der Proof-of-Stake-Konsensregel kann unterschiedlich ausfallen, Bestandteil ist aber immer das Deponieren von Vermögenswerten auf der Blockchain als Garantieleistung. Aus naheliegenden Gründen handelt es sich bei diesen Vermögenswerten jeweils um Coins der entsprechenden Blockchain; beinhaltet eine Blockchain keine Coins, macht Proof-of-Stake keinen Sinn. Je grösser die Garantieleistung, desto höher die Chance, den nächsten Block «forgen» (schmieden) zu können. Damit nicht nur vermögende «Forging Nodes» zum Zuge kommen, wird die Berechtigung, den nächsten Block erzeugen zu können, durch weitere Faktoren beeinflusst. So spielt oft der Zeitpunkt, wann eine Garantie geleistet worden ist, eine Rolle. Der Aufwand, einen «Forging Node» zu betreiben, ist im Vergleich zu einem «Mining Node» deutlich kleiner; vergütet wird er durch Transaktionsgebühren, die das Netzwerk dem «Forger» gutschreibt. Will ein Forger das Forgen aufgeben, muss er erst eine Reihe von Blocks abwarten, bis sein Einsatz und die verdienten Transaktionsgebühren frei verfügbar gemacht werden. Sollte sich herausstellen, dass er einen Manipulationsversuch unternommen hat, verliert er seinen Einsatz und wird für zukünftiges Forgen gesperrt. Auch im Fall von Proof-of-Stake wäre es mit extremem Aufwand möglich, das Forgen systematisch zu manipulieren. Allerdings würde dies voraussetzen, dass der Forger über mehr als die Hälfte der entsprechenden Coins verfügt. Die Kosten für den Erwerb dieser Coins würden aber in keinem günstigen Verhältnis zu den möglichen Gewinnen stehen.

Die Konsensregeln Proof-of-Work und Proof-of-Stake machen nur bei Blockchains Sinn, die Einsicht und Einträge auf die Blockchain nicht einschränken. Für Blockchains, bei denen die freie Einsicht und insbesondere das freie Eintragen eingeschränkt beziehungsweise nicht möglich sind, bietet sich Proof-of-Authority als Konsensregel an.

2.4. Was sind Smart Contracts?

Jede Blockchain ist ein maschinell lesbarer und bearbeitbarer Datensatz. Die Blockchain kann mit maschinell ausführbaren Anweisungen erweitert werden, die als **Smart Contracts** bezeichnet werden. Smart Contracts erlauben es, gewisse Transaktionen auf der Blockchain zu automatisieren. Vereinfacht gesagt, erlauben sie das Lesen und Schreiben auf die Blockchain ohne manuelles Zutun durchzuführen, falls vorher vereinbarte Bedingungen erfüllt werden. Die maschinell ausführbaren Anweisungen können vertragliche Regelungen (Contracts) abbilden und erhöhen die Transparenz, Geschwindigkeit und Genauigkeit. Ob Smart Contracts im juristischen Sinne verbindlich sind, hängt davon ab, inwieweit ein Smart Contract sämtliche relevanten Rechtsaspekte regelt, wie Rechtsstreitigkeiten entschieden und Gerichtsentscheide durchgesetzt werden können. Je nach Rechtsordnungen werden diese Fragen unterschiedlich gehandhabt.

Insbesondere wenn zwei oder mehr Parteien an der Formulierung eines Smart Contracts beteiligt sind, wird deren Potenzial klar. Dies sei an einem Beispiel erläutert. In die Handänderung einer Immobilie sind traditionellerweise eine Reihe von Personen und Institutionen involviert. Dies, weil Käufer und Verkäufer oft nicht Gewissheit haben, ob die andere Partei vertragsfähig und willig ist, den Vertrag zu erfüllen. Makler, Banken, Grundbuchämter usw. reduzieren oder eliminieren mit ihren Dienstleistungen entsprechende Risiken, haben aber auch ihren Preis. Auf einer Blockchain kann die gleiche Transaktion mithilfe eines Smart Contracts folgendermassen ausgeführt werden: Der Käufer überweist den Kaufpreis in Kryptowährungen auf ein eigens für diese Transaktion eröffnetes Konto (Wallet). Dieses Konto gehorcht einem Smart Contract. Sobald der Smart Contract feststellt, dass die Handänderung der Immobilie in dem auf einer Blockchain geführten Grundbuch vorgenommen worden ist, wird die Überweisung des Kaufpreises an den Verkäufer ausgelöst. Sollte sich diese Bedingung innerhalb der vereinbarten Frist nicht erfüllen, wird der Betrag dem Käufer rückerstattet. Nicht alle Blockchains sind für eine Erweiterung mit Smart Contracts gleichermassen geeignet. Ethereum ist zurzeit jene Blockchain, die für Smart-Contracts-Applikationen am weitesten verbreitet ist.

Smart Contracts auf automatisierte Mechanismen kryptobezogener Bedingungen zu reduzieren, greift zu kurz. Grundsätzlich sind jegliche quantifizierbaren Sachverhalte in Smart Contracts abbildbar. Insofern ist auch der Begriff Smart Contract eher irreführend, da in vielen Fällen kein rechtlicher Vertrag im engeren Sinne zugrunde liegt. Ob Transaktionen, die durch einen Smart Contract ausgelöst werden, in sich smart sind, kann auch hinterfragt werden, sind diese doch immer vorprogrammiert. Sobald die Blockchain die vordefinierten Bedingungen als strukturierte Daten vorfindet und diese eindeutigen personalen oder objektbezogenen Identitäten zugeordnet werden können, wird die Transaktion ungeachtet aller anderen Umstände ausgelöst.

2.5. Wie entwickelt sich die Blockchain-Technologie weiter?

Obwohl Blockchains seit zehn Jahren entwickelt werden, sind deren Innovationspotenziale in der Praxis noch lange nicht ausgeschöpft. Hinzu kommt, dass die Technologie ständig weiterentwickelt wird, zum Beispiel was die Energieeffizienz der Proof-of-Work Konsensregel, generell die Steigerung der Transaktionsvolumina, den Schutz der Privatsphäre, die Interoperabilität zwischen unterschiedlichen Blockchains und die Bedienungsfreundlichkeit anbetrifft. Die Weiterentwicklung erfolgt auf zwei Schienen: Forks und Generationen.

Wenn eine bestehende Blockchain rückwärtskompatibel weiterentwickelt wird, kann von einer **Soft Fork** (weiche Gabelung) gesprochen werden. Deren Bedeutung wird im Vergleich zur Hard Fork deutlich: Bei einer **Hard Fork** (harte Gabelung) wird neben der bestehenden Blockchain eine neue Blockchain lanciert. Das heisst, nach einer Hard Fork existieren zwei Blockchains: die ursprüngliche, die unverändert weiterläuft und die geforkte. Die geforkte Blockchain teilt mit der ursprünglichen Blockchain die Geschichte bis zur Hard Fork (der ursprüngliche Code sowie die Blocks, die bis zur Hard Fork generiert wurden), unterscheidet sich aber danach im Code so stark, dass nach der Hard Fork keine Rückwärtskompatibilität mehr gegeben ist und entsprechend eine neue Blockchain gebildet wird.

Werden mit einer Blockchain gänzlich neue Funktionalitäten eingeführt, spricht man von neuen **Generationen**:

- Blockchains der **ersten** Generation ermöglichen die Herausgabe von Kryptowährungen. Klassisches Beispiel für eine Blockchain erster Generation ist Bitcoin.

- Blockchains **zweiter** Generation ermöglichen neben der Herausgabe von Kryptowährungen weitere Funktionalitäten, insbesondere die Programmierung von Smart Contracts. Klassisches Beispiel für eine Blockchain zweiter Generation ist Ethereum.

- Blockchains **dritter** Generation suchen bessere Antworten auf Probleme, welche die erste und zweite Generation nicht haben vollständig lösen können: Skalierbarkeit, Governance, Einfachheit der Nutzung usw. Dabei kommen teilweise Konzepte zur Anwendung, die nur noch zu einem Bruchteil auf den Ansätzen der ersten und zweiten Generation basieren. Vertreter der dritten Generation sind Cardano, IOTA oder Hashgraph.

2.6. Wann machen Blockchains in der öffentlichen Verwaltung grundsätzlich Sinn?

Die ersten Blockchains wurden entwickelt, um einen **Vertrauensmechanismus** zu etablieren, der nicht von einer zentralen Autorität abhängig ist. Dies ist Blockchains wie Bitcoin oder Ethereum bisher auch teilweise gelungen, zumindest solange das Aushandeln von Ansprüchen im digitalen Raum – idealerweise ausschliesslich auf der jeweiligen Blockchain selbst – vollzogen wird. Sobald Ansprüche in der analogen Welt durchgesetzt werden sollen, sind dazu in letzter Konsequenz physische Mittel erforderlich. Sehen wir von Selbstjustiz ab, müssen dazu staatliche Durchsetzungsmechanismen aktiviert werden.

Staaten beanspruchen innerhalb ihres Territoriums ein **Gewaltmonopol**, mit dem sie im Fall von rechtsstaatlich verfassten politischen Systemen ihre Rechtsordnung durchsetzen, im Fall von Diktaturen die Interessen der illegitim Herrschenden. Gemeinsam ist allen Staaten, dass sie eine Autorität darstellen, die auf ein Zentrum konvergiert; föderale Strukturen schwächen diesen Grundsatz ab, sie setzen ihn aber nicht ausser Kraft. Die zentralistische Grundstruktur von Staaten ist an sich nicht problematisch – im Gegenteil: Sie ist Voraussetzung für die Gleichbehandlung der Rechtssubjekte.

Der **ideale Staat** ist effizient und gerecht. Er verfügt über die erforderlichen Mittel, um seine Rechtsordnung – ob digital oder physisch – durchzusetzen. Dazu sind Blockchains nicht nötig, insbesondere nicht zugangsfreie. Als Inhaber des Gewaltmonopols ist es für den gerechten Staat selbstverständlich, alle Rechtssubjekte gleich zu behandeln. Dies ist in der unstrukturierten, analogen Realität viel herausforderungsreicher als im digitalen, maschinenlesbaren Raum. Daher verfügt der Staat so lange über Legitimität und Vertrauen, als ihm die gerechte Anwendung des Gewaltmonopols auch in den verworrensten Situationen gelingt. In einer säkularisierten Gesellschaft ist dazu keine andere Institution in der Lage. Es ist im Interesse aller Rechtssubjekte, dass es die Instanz Staat gibt, denn ohne ihn sind sie ihrer Rechte nicht mehr gewiss.

Damit Rechtsansprüche durchgesetzt werden können, sind entsprechende Beweismittel erforderlich. Diese können ihre Kraft nur entfalten, wenn die Identität der beteiligten Rechtssubjekte eindeutig feststellbar ist. Der Staat anerkennt Identitäten hoheitlich; für ihn zählt, was in seinen «Büchern» und je länger je mehr auch in seinen digitalen Unterlagen steht. Private Rechtssubjekte sind darauf angewiesen, alle ihre Transaktionen mit ihnen zuordenbaren Beweismitteln zu dokumentieren. Bei digitalen Transaktionen mit dem Staat ist es ausreichend, wenn diese zum Beispiel mit entsprechenden qualifizierten Signaturen versehen sind. Diese mit zusätzlicher kryptografischer und organisatorischer Komplexität zwecks Erhöhung der Rechtssicherheit zu erweitern, wie es Blockchains bieten, macht in einem funktionierenden Staatswesen keinen Sinn, da dadurch kein Zusatznutzen entsteht.

Eine besondere Herausforderung hinsichtlich Vertrauens und Transparenz bilden demokratische **Wahl- und Abstimmungsverfahren**, bei denen Bürgerinnen und Bürger ihr Wahlgeheimnis gewahrt wissen, gleichzeitig aber sicher sein wollen, dass ihr politischer Wille korrekt ins Ergebnis fliesst. Auf öffentlichen beziehungsweise public-permissioned Blockchains ist dies möglich; allerdings zum Preis der Unmöglichkeit der späteren Vernichtung der Wahlunterlagen; von weiteren sicherheitstechnischen Fragen vorerst abgesehen. Daher wird für diesen Bereich die Anwendung der Blockchain diskutiert und entsprechend geforscht.

Staaten sind aber nicht ideal, sondern **real**. Sie weichen vom Ideal ab, indem sie mehr oder weniger ineffizient und/oder korruptionsgefährdet sind. In beiden Fällen kann die Blockchain-Technologie Beiträge leisten.

Ineffizienzen entstehen erstens aufgrund von mangelnder **Datenqualität**, die meist von sich widersprechenden oder zumindest nicht miteinander verbundenen Datenbanken herrührt. Daten, die auf einer Blockchain abgelegt sind, sind hingegen unveränderbar. Sie können von allen (berechtigten) Organisationen eingesehen und weiterverarbeitet werden. Aufgrund einer gemeinsamen Datenbasis kann Datenintegrität und -konsistenz gewährleistet und dem **Once-only-Prinzip** nachgelebt werden. Im Kern besagt das Once-only-Prinzip, dass ein spezifischer Datenpunkt nur einmal registriert wird und nicht in parallelen Datenbanken von unterschiedlichen Institutionen. Es ist in der Talinn-Deklaration, die der Bundesrat 2017 mitunterzeichnet hat, verankert.

Ineffizienzen entstehen zweitens durch schwerfällige **Prozesse**. Blockchains entfalten dann ihre volle Wirkung, wenn sie in vollständig digitalisierte, medienbruchfreie Prozesse eingebettet sind. Das Vorhandensein einer Blockchain-Infrastruktur kann die Neugestaltung von digitalen Prozessen insofern befruchten. Hinzu kommt drittens **unbeabsichtigtes menschliches Fehlverhalten**, das oft gar nicht oder erst viel zu spät identifiziert werden kann. Sobald relevante Daten und Prozesse auf einer Blockchain dargestellt sind, ist es möglich, Transaktionen zu vereinfachen oder gar zu automatisieren und zu überwachen. Dadurch können Zeit und Geld eingespart werden.

Blockchains bilden Sachverhalte so ab, wie sie ihnen gefüttert werden. Ob das «Futter» korrekt oder manipuliert ist, kann die Blockchain nicht beurteilen; sie erkennt ausschliesslich Dateninkonsistenzen. Aus diesem Grund wäre es vermessen, zu meinen, dass der Einsatz von Blockchains alle Akteure auf den Pfad der Tugend leitet. Indem jedoch Transaktionen Daten auf einer Blockchain öffentlich einsehbar machen und diese nicht mehr veränderbar sind, vergrössert sich der Druck, sich korrekt zu verhalten. Dass Argument der Prävention von Manipulation oder gar **Korruption** durch die Anwendung der Blockchain-Technologie steht allerdings in der Schweiz nicht im Vordergrund. Zudem besteht dank des Öffentlichkeitsprinzips in der hier geltenden Informations- und Datenschutzgesetzgebung bereits öffentliche Einsichtsrechte; allerdings muss heute der Einzelne meist erst Einsicht in seine Daten einfordern, um sie dann überprüfen zu können. Mit einer sofortigen Publikation von Daten auf einer Blockchain würde Transparenz von Beginn an hergestellt und ein Monitoring könnte automatisiert werden.

Neben den grundsätzlichen Überlegungen zum Einsatz der Blockchain-Technologie in der öffentlichen Verwaltung, sind auch politische und rechtliche Aspekte massgebend. Auf sie wird hier aus genereller Sicht eingegangen; entscheidend ist jeweils die Konstellation im konkreten Einzelfall.

Ohne breit abgestützten **politischen Willen** sind Veränderungsprozesse nicht zu bewältigen. Er ist für die allfällige Schaffung von rechtlichen Grundlagen ebenso erforderlich wie für die motivierende Führung der öffentlichen Verwaltung, welche die Blockchain-Technologie implementieren soll. Nicht zuletzt erschliesst sich aus dem politischen Willen die Akzeptanz in der Bevölkerung und Unternehmerschaft für allfällige Veränderungen. Die Führungsverantwortung gewählter Amtsträgerinnen und Amtsträger ist in diesem Zusammenhang erheblich. Dies gilt umso mehr, als die Herausforderungen in Veränderungsprozessen im Organisatorischen und Kulturellen meist viel grösser sind als in Bezug auf Technik und Recht.

Damit politischer Wille in staatliches Handeln umgesetzt werden kann, muss er verrechtlicht werden. Staatliche Akteure können nur im Rahmen ihrer **gesetzlichen Grundlage** tätig werden. Das gilt auch für den Betrieb einer Blockchain durch den Staat. Die kantonalen Rechtsordnungen kennen den Begriff der Blockchain noch nicht. Auch im Bundesrecht gibt es noch keine verbindlichen Vorgaben für die Blockchain-Technologie, an denen sich die Kantone orientieren könnten.

Im November 2019 hat der Bundesrat die Botschaft zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register veröffentlicht (**DLT-Gesetz**). Der Nationalrat hat im Juni 2020 als Erstrat dem Gesetz nach wenigen Änderungen zugestimmt. Da dieses Bundesgesetz ausschliesslich auf Blockchain-Anwendungen im Finanzbereich zielt, wird es – wenn überhaupt – nur punktuell für die in dieser Studie adressierten Fragen Wirkung entfalten. Interessant ist jedoch die grundsätzliche Vorgehensweise des Gesetzgebers: Entgegen dem Eindruck, den der Titel des Gesetzes wecken kann, handelt es sich nicht um einen eigenständigen neuen Gesetzestext, sondern um Ergänzungen von elf bereits bestehenden Gesetzen. Ein innovativer Aspekt dabei ist, dass vorgeschlagen wird, im Obligationenrecht neu auch von «Wertrechtregistern» zu sprechen. Diese erlauben eine vereinfachte Übertragung von Aktien, ohne die herkömmliche Anforderung der Schriftlichkeit.

Es ist durchaus möglich, dass die gesetzlichen Grundlagen, die für die Anwendung der Blockchain-Technologie in der öffentlichen Verwaltung erforderlich sind, ebenfalls mit Erweiterungen bestehender Erlasse geschaffen werden können. Im Zusammenhang mit der Blockchain-Technologie ist insbesondere das **Datenschutzrecht** von Bedeutung, das stark durch die Dynamik der Europäischen Union beeinflusst wird. Für die Verwaltung des Kantons Zürich ist jedoch in erster Linie das Gesetz über die Information und den Datenschutz (IDG) massgebend. Um für einzelne Anwendungsbereiche verbindliche Aussagen machen zu können, ist jeweils der konkrete Fall zu überprüfen. Folgende Fragen stehen aber in den meisten Fällen im Vordergrund:

- **Art der Daten:** Welche Daten werden auf der Blockchain eingetragen? Handelt es sich um besondere Personendaten? Handelt es sich um Daten betreffend Objekte ohne Rechtspersönlichkeit oder um einen Link auf eine Ressource, die ausserhalb der Blockchain betrieben wird und unabhängig von der Blockchain gelöscht werden kann? Je nach Art der Daten werden die datenschutzrechtlichen Anforderungen unterschiedlich ausfallen.

- **Art der Verschlüsselung der Daten:** Daten werden verschlüsselt, um sie vor unberechtigtem Zugriff zu schützen. Insofern sollten verschlüsselte Daten – insbesondere komplizierte Hashes – unproblematische Einträge auf einer Blockchain darstellen. Trotzdem werden im Datenschutzdiskurs Verschlüsselungen skeptisch diskutiert. Erstens, weil es theoretisch immer möglich ist, eine Verschlüsselung zu durchbrechen. Zweitens, in Anlehnung an den ersten Punkt: Verschlüsselungen, die heute als sicher gelten, können sich in Zukunft dank des technologischen Fortschritts als unsicher herausstellen.

- **Verantwortlichkeit, Klagemöglichkeit:** Staatliches Handeln muss immer einem Akteur zuordenbar sein, um diesen im Schadenfall zur Verantwortung ziehen zu können. Insbesondere im Fall von public-permissionless Blockchains ist die Verantwortlichkeit nicht mehr gegeben. Die an Transaktionen beteiligten Akteure treten mit Pseudonymen in Erscheinung, der Betrieb der Blockchain kann auf eine grosse Zahl von Nodes in allen möglichen Ländern verteilt sein.

- **Möglichkeit der Korrektur:** Da falsche Einträge nie ausgeschlossen werden können, sieht das Datenschutzrecht vor, dass Betroffene ein Recht auf Korrektur haben. Zwar können auch in einer Blockchain Korrekturen vorgenommen werden, allerdings nicht dergestalt, dass alte Einträge geändert werden. Diese bleiben stehen. In einem neuen Block kann zusätzlich der richtige Sachverhalt – einschliesslich eines Hinweises auf den Fehler in der Vergangenheit – festgehalten werden.

- **Recht auf Vergessen:** Das Datenschutzrecht geht noch einen Schritt weiter, indem es dem Einzelnen in gewissen Bereichen ein Recht auf Vergessen einräumt. Solange Daten in zentralen, papierbasierten, nicht redundanten Registern gehalten werden, kann ein Eintrag durch Vernichtung der entsprechenden Registerkarte praktisch zweifelsfrei durchgeführt werden. Bei elektronischen Registern ist das Löschen von Daten bereits eine weniger triviale Angelegenheit. Einträge ganz aus einer Blockchain zu tilgen, ist im Falle von public Blockchains ein Ding der Unmöglichkeit. Im Falle von privaten Blockchains mag das Löschen möglich sein, allerdings wäre es mit erheblichem Aufwand verbunden, insbesondere was die Koordination aller Beteiligten anbetrifft.

- **Pflicht zur Archivierung:** Der Staat hat die Pflicht, seine Tätigkeit zuhanden der Öffentlichkeit zu überliefern, und zwar in Form von Originaldokumenten beziehungsweise authentischen Informationen. Was überliefert wird, um die Tätigkeit des Staats nachvollziehbar zu halten, entscheidet das zuständige Archiv. Diese Überlieferungspflicht steht in Konkurrenz zu individuellen schützenswerten Interessen, solange die entsprechenden Personen noch leben. In diesem Sinne steht die Pflicht zur Archivierung dem Recht auf Vergessen vorübergehend entgegen. Da früher oder später – nach Ablauf mehr oder weniger langer Schutzfristen – alle Daten des Staats öffentlich zugänglich werden, können aber auch Verschlüsselungen die Erfüllung der Archivierungspflicht behindern. Die digitalen Werkzeuge, welche die öffentliche Verwaltung je länger je mehr einsetzt, stellen die Archive also vor neue Herausforderungen. Blockchain-Anwendungen machen hier keine Ausnahme.

3. Konkrete Anwendungsbeispiele aus der öffentlichen Verwaltung

In den Jahren 2016 und 2017, als die Blockchain-Technologie erstmals weltweit für breites Aufsehen sorgte, wurde auch im öffentlichen Sektor eine erhebliche Zahl von Projekten lanciert. Die Illinois Blockchain Initiative listete in einer öffentlichen Datenbank über 200 Blockchain-Projekte der öffentlichen Hand auf; die meisten davon hatten Visions- oder Proof-of-Concept-Charakter. Seit Kurzem ist diese Datenbank nicht mehr online.

Jüngere Publikationen machen deutlich, dass der systematische Einsatz der Blockchain-Technologie in der öffentlichen Verwaltung noch nicht die Regel ist. Dafür mögen Gründe verantwortlich sein, wie sie in Kapitel 2.6 formuliert worden sind. Hinzu kommt, dass die Blockchain-Technologie erst in einem hoch beziehungsweise völlig digitalisierten Kontext ihr volles Potenzial entfalten kann. Davon sind öffentliche Verwaltungen im Allgemeinen noch weit entfernt. Damit verbunden sind auch politische, rechtliche, organisatorische und kulturelle Hürden, die bei der Einführung von Blockchain-Anwendungen überwunden werden müssen. Es wird hier darauf verzichtet, ausländische Anwendungsbeispiele im Detail vorzustellen; vielmehr wird auf einzelne zusammenfassend hingewiesen:

Das OECD-Working Papers 28, das 2018 publiziert wurde, beschreibt acht Projektbeispiele, die sich auf staatliche Aufgaben beziehen oder in denen der Staat involviert ist:

- BenBen, Ghana: Aufbau eines Blockchain-basierten Grundbuchs, das unter anderem auf Satellitenbildern fusst
- Global Blockchain Council, Dubai, Vereinigte Arabische Emirate: Aufbau eines Expertengremiums, als Grundlage für die Einführung der Blockchain-Technologie in der öffentlichen Verwaltung. Die Organisation betreibt Bildungsprogramme und Pilotprojekte.
- Intragovernmental Emerging Citizen Technology Office, USA: Aufbau einer Regierungsorganisation, die Blockchain-Anwendungen in der amerikanischen Verwaltung koordiniert
- Ubin, Singapur: Entwicklung einer Blockchain-basierten Lösung für grenzüberschreitende Banktransaktionen
- Chromaway, Schweden: Aufbau eines Blockchain-basierten Grundbuchs
- Blockchain Trust Accelerator, USA: unabhängiger Think- und Do-Tank, der für öffentliche Verwaltungen weltweit Projekte unterstützt
- Vehicle Wallet, Dänemark: Aufbau eines Blockchain-basierten Dossiers für Fahrzeuge
- Öffentliche Ausschreibungen, Mexico: Abwicklung des öffentlichen Ausschreibungsverfahrens auf einer Blockchain

Eine Studie der Europäischen Kommission, die 2019 publiziert wurde, beschreibt sieben Projekte:

- Exonum, Georgien: Blockchain-basiertes Grundbuch
- Blockcerts, Malta: Blockchain-basierte Verifikation von akademischen Diplomen
- Chromaway, Schweden: siehe oben
- uPort-ID, Zug: Blockchain-basierte elektronische Identität, detaillierte Darstellung siehe Kapitel 3.5
- Infrachain, Luxemburg: Entwicklung einer Governance-Struktur, die für unterschiedliche private Blockchains gleichermassen zur Anwendung kommen soll
- Pension, Niederlande: Vollständige Abwicklung des Pensions-Prozesses auf einer Blockchain
- Stadjerpas smart vouchers, Groningen, Niederlande: Blockchain-basierte Lösung für Vouchers für Einwohnerinnen und Einwohner mit tiefen Einkommen

In der Blockchain-Strategie der Bundesregierung Deutschlands, die ebenfalls 2019 publiziert wurde, werden diverse Bereiche angesprochen, in denen Studien beziehungsweise Versuche durchgeführt werden sollen, um die Eignung der Blockchain-Technologie in der öffentlichen Verwaltung weiter zu prüfen. Neben den Bereichen Energie und Gesundheitswesen stehen folgende Themen im Vordergrund:

- Einsatz von Gültigkeits-Tokens zur Verifikation von Zertifikaten aller Art (Diplome, Geburtsurkunden, Arbeitszeugnisse usw.)
- Blockchain-basierte Identifikationsnachweise und Zulassungswesen von Personen und Geräten
- Vertrauensdienste (vertrauenswürdige elektronische Transaktionen über Ländergrenzen hinweg)
- Aufbau einer staatlichen Blockchain-Infrastruktur, die für die öffentliche Verwaltung und private Akteure zugänglich sein soll
- Blockchain-Lösung, um die behördenübergreifende Kommunikation und Zusammenarbeit im Asylbereich zu unterstützen
- Nachvollzug und Steuerung von Gebermitteln in der Entwicklungszusammenarbeit
- Blockchain-basierte Bestimmung des Zollwertes von grenzüberschreitenden E-Commerce-Transaktionen
- Blockchain-Lösung, die unterschiedliche Daten von Kraftfahrzeugen miteinander verknüpft

Diese Übersicht verdeutlicht, wie breit das Anwendungsspektrum der Blockchain-Technologie in der öffentlichen Verwaltung angedacht wird. Gleichzeitig wird jedoch auch klar, wie anforderungsreich dieses Unterfangen ist, müssen doch für jeden Anwendungsfall ganz spezifische Lösungen gefunden werden. Diese Beobachtung kann auch in der Schweiz gemacht werden. Im Folgenden werden acht Projekte, die im Rahmen der vorliegenden Studie in öffentlichen Verwaltungen der Schweiz und dem Fürstentum Liechtenstein haben identifiziert werden können, im Detail dargestellt. Zusätzlich ist zu erwähnen, dass im Rahmen der Innovationen und E-Partizipationsprojekte 2020 von E-Government Schweiz der Kanton Jura eine «ökologische Blockchain für digitales Vertrauen in der Schweiz» entwickelt. Detaillierte Informationen dazu sind noch nicht verfügbar.

3.1. Handelsregisterauszug (Kanton Genf)

Ausgangslage

- Handelsregisterauszüge standen bis 2018 nur in physischer Form zur Verfügung. Elektronische Dokumente hatten keine Rechtskraft.

Lösung

- Seit Februar 2018 erlaubt die «Verordnung über die Erstellung elektronischer öffentlicher Urkunden und elektronischer Beglaubigungen (EBÖV)» des Bundes (SR 943.03) das elektronische Ausstellen von staatlichen Dokumenten.
- Es wurde ein Proof-of-Concept erarbeitet, der es ermöglicht, Handelsregisterauszügen online zu beziehen. Die Gebühren können mit Kreditkarte bezahlt werden. Der elektronische Handelsregisterauszug wird per E-Mail zugestellt. Dieser ist mit einem Echtheitsbeweis versehen, der von Dritten auf der Ethereum-Blockchain überprüft werden kann.
- Die elektronischen Handelsregisterauszüge werden gleichzeitig mit einem Zeitstempel (OpenTimeStamp) auf Ethereum versehen.
- Ein Internet-basierter Verifikationsdienst erlaubt, die Echtheit von elektronischen Handelsregisterauszügen zu überprüfen. Dazu ist das fragliche Dokument auf eine Internetseite hochzuladen. Im Hintergrund wird überprüft, ob dieses auf der Ethereum-Blockchain registriert ist. Die Verifikationen selbst werden aus datenschutzrechtlichen Gründen nicht protokolliert.

Tatsächliche Nutzung

- Seit der Lancierung im März 2018 wurden bis August 2019 etwa 300 Handelsregisterauszüge elektronisch bezogen. Über die elektronische Überprüfung der Auszüge durch Dritte wird keine Statistik geführt.

Fazit

- Das Projekt war im Sinn eines Proof-of-Concept ein Erfolg und hat zur Entwicklung einer Reihe von Komponenten geführt, die nun für andere behördliche Register eingesetzt werden können. Das Experiment wurde vorerst unterbrochen und soll zu einem späteren Zeitpunkt mit folgenden Funktionen weitergeführt werden: Registerauszüge sollen mit qualifizierten elektronischen Signaturen des Handelsregisteramts und der Bescheinigung des Bundes, der das Handelsregisteramt zur Ausstellung des Auszugs ermächtigt, erweitert werden. Zudem sollen die manuellen Arbeitsschritte der Extraktion aus dem zentralen Register und der Versand per E-Mail automatisiert werden.
- Der Einsatz einer public Blockchain bietet eine fälschungssichere Grundlage, mit der die Echtheit der Registerauszüge im Internet überprüft werden kann, ohne dass vom Handelsregisteramt ein zusätzlicher Aufwand entsteht. Eine zentrale Datenbank kann vom Betreiber unbemerkt manipuliert werden und bietet dem Empfänger somit nicht die gleiche Sicherheit.

Weitere Hinweise

- Genève numérique – Blockchain

3.2. Unterschriftsberechtigungen (Kanton Genf)

Ausgangslage

- Elektronisch unterzeichnete Dokumente sind nur dann gültig, wenn sie mit einer qualifizierten elektronischen Signatur versehen sind (Art. 14 Abs. 2^{bis} OR).
- Eine qualifizierte elektronische Signatur beweist ausschliesslich, dass eine digitale Unterschrift gültig ist. Sie kann jedem beliebigen Dokument hinzugefügt werden. Im Fall von Signaturen von natürlichen Personen ist in der Regel einfach überprüfbar, ob die richtige Person unterzeichnet hat. Für juristische Personen zeichnen berechtigte natürliche Personen. Ob eine natürliche Person berechtigt ist, im Namen einer juristischen Person zu zeichnen, geht auch aus einer qualifizierten elektronischen Unterschrift nicht hervor.
- Für Unternehmen, die Garantien für die Echtheit von Unterschriften und die Legitimität der Unterzeichnenden wünschen, birgt diese Situation Risiken. Dies gilt insbesondere für den Rohstoffhandel, eine sehr wichtige Handelstätigkeit in Genf, wo viele Transaktionen zwischen internationalen Partnern stattfinden. Das gleiche Problem der Zuverlässigkeit stellt sich aber für KMU, die aufgrund mangelnden Vertrauens nur ungern im E-Commerce tätig sind.

Lösung

- Unternehmen können zur Unterschrift berechtigte Personen auf dem E-Government-Portal des Kantons Genf registrieren. Bezüglich des Standortes der Firma bestehen keine Einschränkungen, dieser kann auch im Ausland liegen. Entscheidend ist, dass zumindest eine Vertragspartei Sitz in Genf hat und der Gerichtsstand Genf ist.
- Das Onboarding von Personen, Unternehmen oder anderen (internationalen) Organisationen ist an Genfer Notariate delegiert. Die Kammer der Genfer Notare (Chambre des Notaires de Genève) begleitet das Projekt.
- Der Signierungsprozess von Verträgen kann via API durch die firmeninterne Applikation ausgelöst werden.
- Signiert wird mit einer App, die vom Kanton Genf zur Verfügung gestellt wird.
- Sobald jemand mit dieser App signiert, wird überprüft, ob diese Person über die erforderliche Berechtigung verfügt und ob die elektronische Signatur gültig ist.
- Sind diese Bedingungen erfüllt, wird die Signatur auf einer Blockchain registriert; ausschliesslich der Kanton Genf hat die Berechtigung, diese Registrierung in einem Smart Contract vorzunehmen.
- Anschliessend können Dritte via Blockchain überprüfen, ob ein Vertag durch berechtigte Personen und mit gültigen Signaturen unterzeichnet worden ist.
- Die Lösung entspricht geltendem Recht (öffentliche Urkunden, ZertES).
- Der Proof-of-Concept wurde auf Etherum entwickelt und basiert auf dem elektronischen Signaturservice mobileID von Swisscom.
- Der Proof-of-Concept wurde von E-Government Schweiz mitfinanziert.

Tatsächliche Nutzung

- Der Proof-of-Concept wurde im August 2019 initiiert. Es waren Firmen aus den Bereichen Rohstoffhandel und -finanzierung, Logistik und Registrierung von geistigem Eigentum beteiligt.
- Die Testphase wurde im ersten Halbjahr 2020 erfolgreich abgeschlossen.

Fazit

- Ohne dass dem Staat zusätzliche Kostenentstehen, kann bei digitalen Transaktionen überprüft werden, ob alle beteiligten Personen auch tatsächlich dazu berechtigt sind. Durch die Verwendung einer public Blockchain kann der Verifikationsprozess unveränderbar dokumentiert werden.
- Mit dieser Dienstleistung will der Kanton Genf seine Standortattraktivität erhöhen, insbesondere im Bereich des Rohstoffhandels. Sie unterstütz den Aufbau eines digitalen Ökosystems (mehr dazu siehe Trust Valley).
- Gleichzeitig kann damit die Rechtssicherheit der Beteiligten im Vergleich zu herkömmlichen Signaturverfahren verbessert werden, wodurch Rechtsstreitigkeiten verhindert und die Gerichte entlastet werden.
- Der Kanton Genf ist zurzeit daran, den Proof-of-Concept in eine skalierbare Lösung weiterzuentwickeln. Sie soll 2021 produktiv zur Verfügung stehen.

3.3. Betreibungsregisterauszug (Kanton Schaffhausen)

Ausgangslage

- Antragsteller eines Betreibungsregisterauszugs müssen sich normalerweise zwei bis drei Tage gedulden, bis ihnen dieser per Post zugestellt wird.
- Nach Erhalt des Auszugs wird dieser vom Empfänger meist eingescannt und der Drittpartei, die den Auszug verlangt, als PDF zustellt.
- Es ist nicht ausgeschlossen, dass ein eingescannter Auszug mit Bildbearbeitungssoftware manipuliert wird.
- Es gibt bereits unabhängige Anbieter, die den Bestellprozess für Kundinnen und Kunden abwickeln und der anfordernden Partei Zugriff auf die digitale Kopie geben. Der unabhängige Anbieter garantiert für die Authentizität des elektronischen Dokuments. Dieser Prozess ist jedoch für den Kunden mit Zusatzkosten verbunden. Rechtskraft weist ein solches elektronische Dokument nicht auf.
- Grundsätzlich ist es möglich, amtliche Dokumente mit einer elektronischen Signatur zu versehen: entweder mit einem geregelten Zertifikat, auch Organisationszertifikat genannt (Art. 7 ZertES) oder mit einer qualifizierten elektronischen Signatur (Art. 8 ZertES). Allerdings weisen diese Varianten folgende Nachteile auf:
    - Fehlende Flexibilität: Diese Art der Signatur kann nur auf PDF-Dokumenten angebracht werden. Andere Formate, beispielsweise für Bild, Ton oder für strukturierte Daten werden nicht unterstützt.
    - Anbieter von Zertifizierungsdiensten nach ZertEs müssen von der Akkreditierungsstelle als solche anerkannt werden. Das Anerkennungsverfahren ist mit erheblichen Kosten verbunden, die sich in den Preisen für die Signaturen niederschlagen. Aus dem gleichen Grund ist die Zahl der Anbieter für Zertifizierungsdienste verhältnismässig klein.
    - Keine Möglichkeit, Zero-Knowledge-Proof-Funktionen zu etablieren: Zero-Knowledge-Funktionen erlauben es, die Kenntnis eines Geheimnisses zu beweisen, ohne dass das Geheimnis preisgegeben werden muss. Im vorliegenden Fall würde eine Zero-Knowledge-Funktion zum Beispiel beinhalten, dass es möglich ist, die Gültigkeit der Signaturen zu überprüfen, ohne das signierte Dokument öffnen und damit auch dessen Inhalt lesen zu können.

Lösung

- Erweiterung der bestehenden eID+, sodass Betreibungsregisterauszüge direkt über diese App bezogen werden können.
- Die eID+ ist eine App-basierte elektronische Identität, die vom Kanton Schaffhausen betrieben wird. Die App kann in den regulären App-Stores heruntergeladen werden und die Nutzerinnen und Nutzer können ihr Profil eigenständig anlegen. Zur Verifizierung ihrer Attribute müssen sie bei der Einwohnerkontrolle oder auf der Gemeindeverwaltung vorsprechen. Bei korrekten Angaben signiert die Amtsstelle die Attribute, womit sich die Person mit hoheitlich zertifizierten Attributen im digitalen Raum ausweisen kann. Die gesicherte Identifizierung erfolgt durch die Überprüfung einer Reihe von kryptografischen Zertifikaten zwischen den eID-Nutzenden, dem Kanton Schaffhausen (Identity-Provider) und der Drittpartei, die sich von der Identität der eID-nutzenden Person überzeugen lassen will (Relying Party).
- Mit der eID+ kann ein Betreibungsregisterauszug mit wenigen Klicks angefordert werden (document request).

- Das Betreibungsamt generiert den entsprechenden Registerauszug und sendet das PDF auf die eID+ (document push).
- Gleichzeitig wird das PDF gehasht und mit einem Zeitstempel auf einer Blockchain registriert (Hyperledger Fabric, Consensus-as-a-Service von Swisscom und Die Post).
- Anschliessend ist es für Drittparteien möglich, mittels eines Signatur-Verifikators die Authentizität eines PDFs zu überprüfen (Vergleich der Hash-Werte).
- Sowohl die eID+ als auch die Infrastruktur für den digitalen Betreibungsregisterauszug wird von Procivis AG entwickelt.

Tatsächliche Nutzung

- Der Testbetrieb wurde im September und Oktober 2019 erfolgreich durchgeführt.

Fazit

- Eine Rechtsgrundlage, die Blockchain-Signaturen anerkennt und reguliert, fehlt gegenwärtig noch. Bestehende Gesetze wie ZertES müssten so angepasst werden, dass alle Dateiformate signiert werden können und Zero-Knowledge-Funktionen ermöglicht werden.
- Der Einsatz einer public Blockchain bietet eine fälschungssichere Grundlage, auf der die Echtheit der bezogenen Registerauszüge via Internet überprüft werden kann, ohne dass dem Betreibungsamt ein zusätzlicher Aufwand entsteht.
- Eine zentrale Datenbank müsste für diesen Zweck eigens aufgebaut werden, wobei zentrale Datenbanken traditionellerweise nicht dafür geeignet sind, eine fälschungssichere Historie abzubilden.

3.4. Bezahlung amtlicher Gebühren mit Kryptowährungen (Stadt und Kanton Zug)

Ausgangslage

- Bisher können an den Schaltern der Verwaltung nur gegen Bezahlung in Schweizer Franken Dienstleistungen bezogen werden.
- Die Verwaltung verfügt kaum über eigene Erfahrung mit Blockchain-Lösungen.

Lösung

- Gebühren bis zu Fr. 200 können mit Bitcoin oder Ether bezahlt werden.
- Für jede Transaktion wird ein Wallet generiert.
- Die Kunden oder der Kunde scannt den QR-Code mit der Adresse des Wallets und überweist anschliessend den Betrag in Bitcoin oder Ether.
- Die Krypto-Coins werden sofort in Schweizer Franken gewechselt, womit das Währungsrisiko für die öffentliche Verwaltung eliminiert ist.
- Das Einwohneramt setzt eine technische Lösung ein, die von Bitcoin Suisse AG entwickelt wurde; die gleiche Firma erbringt auch die Krypto- und Finanzdienstleistungen. Die technische Lösung des Handelsregisteramts stammt von der inacta AG.

Tatsächliche Nutzung

- Im Rahmen des Pilotprojekts, das vom Einwohneramt zwischen 1. Juli und 31. Dezember 2016 durchgeführt worden ist, wurden rund 15 Transaktionen mit einem durchschnittlichen Wert von Fr. 15 durchgeführt; das ergibt insgesamt einen Umsatz von rund Fr. 225.
- Diese Möglichkeit besteht seither weiter. Im Durchschnitt wünschen die Kundinnen und Kunden des Einwohneramts alle zwei Monate, eine Gebühr mit Bitcoin oder Ether zu bezahlen; der Betrag einer durchschnittlichen Transaktion entspricht jener der Pilotphase.
- Seit November 2017 ist es auch beim Handelsregisteramt des Kantons Zug möglich, Dienstleistungen mit Bitcoin und Ether zu bezahlen. Seither wurden rund 40 Transaktionen mit einem Durchschnittswert von rund Fr. 460 in Kryptowährungen bezahlt.

Fazit

- Der Anteil der Gebühren, der mit Bitcoin und Ether bezahlt wird, ist marginal. Das Einwohneramt der Stadt Zug hat seit der Einführung in rund 30 Transaktionen Bitcoins und Ether im Wert von rund Fr. 500 entgegengenommen. Das Handelsregisteramt des Kantons Zug hat zwar in absoluten Werten deutlich mehr Umsatz in Kryptowährungen generiert (knapp Fr. 20 000); bezogen auf den Gesamtumsatz ist jedoch auch dieser Betrag gering. Allerdings bestand nie die Erwartung, einen erheblichen Anteil zu erzielen – ein anderes Ziel stand im Vordergrund.
- Mit der Zulassung von Bitcoin und Ether als Zahlungsmittel wurde innerhalb der Stadtverwaltung ein Zeichen gesetzt und ein Kulturwandel hin zu einer Offenheit gegenüber digitalen Technologien in Gang gesetzt. Mitarbeiterinnen und Mitarbeiter hatten konkreten Anlass, sich mit dem Thema Blockchain auseinanderzusetzen und erste Kenntnisse und Erfahrungen zu sammeln. Der technische Aufwand der Einführung war überschaubar.
- Zudem erlaubte diese Massnahme, Standortmarketing zu betreiben. Das Einwohneramt der Stadt Zug war die erste staatliche Institution, die Bitcoin und Ether als Zahlungsmittel anerkannte. Dies löste weltweit grosses Medienecho aus und hat den Ruf von Zug als Crypto-Valley klar gestärkt.

3.5. Elektronische Identität (Stadt Zug)

Ausgangslage

- Im Gegensatz zu physischen Identitätsdokumenten (Identitätskarte, Pass) stehen noch keine staatlich anerkannten, elektronischen Identitäten zur Verfügung.
- Dieser Mangel wurde vom Bundesgesetzgeber erkannt, er hat im September 2019 ein entsprechendes Gesetz verabschiedet (Bundesgesetz über elektronische Identifizierungsdienste, BGEID). Gegen dieses wurde das Referendum ergriffen. Die Gegner stossen sich insbesondere am Umstand, dass die Herausgabe der elektronischen Identitäten vornehmlich durch private Anbieter erfolgen soll. Der Staat tritt als Regulator in Erscheinung, zudem autorisiert er die Herausgabe der einzelnen elektronischen Identitäten mittels eines Abgleichs mit dem Personenregister des Bundesamts für Polizei fedpol. Zum Zeitpunkt der Publikation dieser Studie herrscht noch keine Klarheit, wie die Herausgabe von hoheitlichen, elektronischen Identitäten auf Bundesebene erfolgen soll.

Lösung

- Die Einwohnerin oder der Einwohner der Stadt Zug lädt die uPort-App auf sein Smartphone und registriert sich. Dabei wird eine uPort-ID generiert (ein öffentlicher Schlüssel eines Smart Contracts auf Ethereum).
- Der Einwohner registriert seine uPort-ID über das Webportal der Stadt Zug, indem er seine uPort-ID-Nummer mit seinem Geburtstagsdatum verbindet. Dadurch wird eine Verknüpfung mit dem Einwohnerregister möglich. Am Ende dieser Etappe signiert der Einwohner seinen Antrag mit der uPort-ID.
- Anschliessend muss sich der Einwohner durch persönliches Erscheinen und Vorlage von Pass oder Identitätskarte bei der Einwohnerkontrolle identifizieren lassen. Können die Angaben bestätigt werden, werden sie mit dem Schlüssel der Stadt Zug signiert und als Zertifikat in der uPort-App abgelegt.
- Die uPort-ID wird auf einem Ethereum-Testnet betrieben. Die Lösung wurde von der ti&m AG erarbeitet.

Tatsächliche Nutzung

- Start: 15. November 2017
- Anzahl ausgestellter eIDs: rund 250
- Die uPort-ID ermöglicht die Teilnahme an einer Konsultativabstimmung (siehe Kapitel 3.6) sowie die Ausleihe von öffentlichen Velos.

Fazit

- Die Lancierung der uPort-ID der Stadt Zug kann im Sinne eines Proof-of-Concept als Erfolg gewertet werden. Wie mit der Ermöglichung der Bezahlung von Gebühren war auch hier die Stadt Zug die erste Behörde, die eine Blockchain-basierte Identität eingeführt hat.
- Wie beim Proof-of-Concept zu erwarten, hält sich die quantitative Verbreitung der uPort-ID in Grenzen. Der provisorische Charakter der Lösung wird auch deutlich durch den Umstand, dass die uPort-ID auf einem Testnet lief. Es liegen noch keine Erkenntnisse hinsichtlich der Skalierung vor. Ebenfalls ist unklar, welche Kosten anfallen würden, falls die uPort-ID auf dem Ethereum Mainnet betrieben würde. Und schliesslich ist die Frage ungeklärt, wie aus datenschutzrechtlicher Perspektive eine Identitätslösung auf einer öffentlichen Blockchain zu bewerten ist.

- Aufgrund des Proof-of-Concept-Charakters ist der Gewinn, den dieses Projekt den Nutzenden gestiftet hat, begrenzt. Hingegen konnte die Zuger Stadtverwaltung erheblich profitieren, indem sie politische, organisatorische und technische Erfahrungen zum Thema elektronische Identitäten hat sammeln können.
- Die Blockchain-Technologie bietet erhebliche Vorteile bei einer Identitätslösung. Insbesondere wenn eine public Blockchain verwendet wird, dient diese als Anlaufstelle zur Überprüfung von Identitäten und man ist nicht auf einen einzelnen zentralen Anbieter angewiesen. Die Vorteile kommen in erster Linie bei vielen Teilnehmenden (Ökosystem) und mehreren Ausstellenden von Identitäten zum Tragen. Wenn die alleinige Kontrolle über die kryptografischen Schlüssel bei den Benutzenden liegt – wie bei Blockchain-Lösungen üblich – gibt es allerdings diverse Herausforderungen bezüglich Benutzerfreundlichkeit und dementsprechend einen hohen Aufklärungsbedarf.
- Im Rahmen des Aufbaus der Smart-City-Infrastruktur hat die Stadt Zug entschieden, den Testbetrieb der uPort-ID einzustellen und im Herbst 2020 mit eZug eine elektronische Identität und Smart-City-App ohne Blockchain zu lancieren. Die Wahl der neuen Lösung war kein Entscheid gegen Blockchain, sondern ergab sich aufgrund des Anforderungskatalogs, der neben der Funktion der elektronischen Identität auch Smart-City-Anwendungen umfasste.

3.6. Internetbasiertes Abstimmen (Stadt Zug)

Ausgangslage

- Bisher kann in der Stadt Zug nur an der Urne oder brieflich abgestimmt werden.

Lösung

- Ermöglichung des internetbasierten Abstimmens
- Die E-Voting-Plattform basiert auf Hyperledger Fabric und verwendet homomorphe Verschlüsselungsverfahren. Daten, die homomorph verschlüsselt worden sind, können in verschlüsselter Form weiterverarbeitet werden. So können homomorph verschlüsselte Stimmen gezählt werden, ohne dass sie entschlüsselt werden müssen. Die E-Voting-Plattform wurde von der Hochschule Luzern (HSLU) und Luxoft entwickelt und lief auf drei Nodes.
- Der Code der E-Voting-Plattform wurde bisher nicht publiziert.

Tatsächliche Nutzung

- Es wurde zwischen dem 24. Juni und dem 2. Juli 2018 eine Konsultativabstimmung durchgeführt. Dabei wurden Fragen zum Zuger Seefest, zum Abstimmungsprozess und zur Anwendung der uPort-ID gestellt (Kapitel 3.5).
- Um an der Konsultativabstimmung teilnehmen zu können, war eine uPort-ID erforderlich; 72 Personen haben sich an der Abstimmung beteiligt.

Fazit

- Der Proof-of-Concept kann aus technischer Sicht als Erfolg gewertet werden. Gleichzeitig macht er klar, dass die Lösung weder in Bezug auf Funktionalität noch Skalierbarkeit und Sicherheit für offizielle politische Abstimmungen geeignet ist.
- Die tiefe Wahlbeteiligung (bezogen auf die Gesamtbevölkerung der Stadt Zug) kann durch die ebenfalls geringe Verbreitung der uPort-ID und den konsultativen Charakter der Abstimmung erklärt werden.
- Wie in Kapitel 2.6 erwähnt, macht es konzeptionell Sinn, Wahlen und Abstimmungen auf öffentlichen Blockchains durchzuführen. Sicherheitstechnische Fragen, insbesondere bezüglich der Übermittlung der Stimmen, müssen gesondert diskutiert werden; sie stellen sich unabhängig vom Einsatz einer Blockchain. Die in Zug verwendete Blockchain war nicht öffentlich, auch wurde der Source Code zu keinem Zeitpunkt publiziert. Eine Weiterentwicklung von E-Voting-Plattformen müsste unbedingt im Open-Source-Modus erfolgen.
- Ergänzend ist zu bemerken, dass die Diskussion von E-Voting in der Schweiz kontrovers verläuft. Die von der Bundeskanzlei geplante Überführung vom Testbetrieb zum ordentlichen Betrieb wurde nicht vollzogen. Die bisherigen Systemanbieter haben sich aus finanziellen (Kanton Genf) und sicherheitstechnischen Gründen (Die Post) aus dem Markt zurückgezogen, wobei Letztere noch 2020 eine neue Lösung lancieren will. Bis am 12. September 2020 werden Unterschriften für eine Volksinitiative gesammelt, die ein E-Voting-Moratorium fordert. Vor diesem Hintergrund hat der Bundesrat der Bundeskanzlei den Auftrag erteilt, bis Ende 2020 mit den Kantonen eine Neuausrichtung des Versuchsbetriebs zu konzipieren.

3.7. Cardossier (Strassenverkehrsamt Aargau und andere)

Ausgangslage

- Teilweise inkonsistente Fahrzeugstammdaten und unzuverlässige Informationen zum Zustand von Fahrzeugen in unterschiedlichen lokalen Datenbanken (Strassenverkehrsämter, Versicherungen, Autohändler, Garagen usw.). Unternehmensübergreifende Prozessautomatisierungsbemühungen werden dadurch erschwert beziehungsweise verunmöglicht.
- Umständliche und entsprechend teure Prozesse bei Unternehmen und staatlichen Institutionen was das Verwalten von Fahrzeugdaten anbetrifft. So sind zum Beispiel Neuzulassungen an Papierdokumente gebunden (Formular 1320A), oder elektronische Versicherungsnachweise zeigen in rund zehn Prozent der Fälle Inkonsistenzen auf. Dies führt zu aufwendigen Nachforschungs- und Korrekturarbeiten.
- Fehlende Transparenz und entsprechend geringes Vertrauen im Bereich des Wiederverkaufs von Fahrzeugen. Studien belegen, dass der Occasionsmarkt von Fahrzeugen als einer der am wenigsten vertrauensvollen gilt.

Lösung

- Eine gemeinsame, für alle Beteiligten zugängliche, in sich konsistente Datengrundlage. Diese Infrastruktur bietet bereits für sich einen Mehrwert, da Dateninkonsistenzen ausgeräumt sind. Zudem können darauf aufbauend weitere Funktionalitäten angeboten werden.
- Datengrundlage basiert auf einer Blockchain. In der Anfangsphase werden für alle rund 11 Mio. Fahrzeuge der Schweiz 19 Datenpunkte angeboten (Basic Record). Dabei handelt es sich um bereits heute öffentlich zugängliche Daten:
    1. Stammnummer
       (von der Zollverwaltung vergeben, identifiziert jedes Fahrzeug eindeutig)
    2. Typenscheinnummer
    3. Typenscheingenehmigungsnummer
    4. Fahrzeugart
    5. Marke
    6. Modell
    7. Markencode
    8. Treibstoffcode
    9. Hubraum
    10. Anzahl Zylinder
    11. Getriebeart
    12. Anzahl Gänge
    13. Antriebsart
    14. Anzahl Sitzplätze
    15. Anzahl Türen
    16. Karosserieform
    17. Motorenleistung (KW)
    18. Leergewicht
    19. Gesamtgewicht
- Auf der Blockchain werden diese Daten nicht registriert, sondern sie werden weiterhin in den dezentralen Fachapplikationen und Datenbanken der Beteiligten gehalten. Über die Blockchain wird einzig der Zugriff auf diese Daten gewährt.

- Die Blockchain basiert auf Corda. Es handelt sich um eine private-permissioned Blockchain, das heisst, einzig dazu Berechtigte können direkt auf der Blockchain Einsicht nehmen und auf ihr Einträge vornehmen.
- Verantwortlich für das Projekt zeichnet der gemeinnützige Verein cardossier.ch. Mitglieder der öffentlichen Hand sind: Strassenverkehrsamt Kanton Aargau, Amt für Strassenverkehr Fürstentum Liechtenstein, Bundesamt für Strassen (ASTRA), Vereinigung der Strassenverkehrsämter (asa); weitere Kantone erwägen eine Mitgliedschaft. Zusätzlich sind Mitglied: Auto Gewerbe Verband Schweiz (AGVS-UPSA), AdNovum Informatik AG, AMAG Import AG, AMAG Leasing AG, Audatex Schweiz GmbH, Auto Schweiz, auto-i-dat AG, AutoScout24, AXA, Emil Frey AG, Hochschule Luzern – Informatik, die Mobiliar, Mobility Genossenschaft, MultiLease AG, PostFinance AG, Schweizerischer Leasingverband, Touring Club Schweiz, Universität Zürich.
- Die Mitglieder tragen die Kosten des Vereins, gleichzeitig erhalten sie Zugang zur gemeinsamen Datengrundlage. Eine Datenschutzkommission überwacht Konzept und Betrieb; sie verfügt über Weisungs- und Sanktionsrechte gegenüber dem Vereinsvorstand.
- Zusätzliche Mittel hat zum Beispiel Innosuisse zur Verfügung gestellt.
- Nodes werden von Vereinsmitgliedern betrieben. Vereinsmitglieder mit begrenzten Ressourcen können sich für das Mining zusammenschliessen und gemeinsam einen Multi-user-Node betreiben.
- Technische Entwicklung durch AdNovum AG

Tatsächliche Nutzung

- Entwicklung des Minimum Viable Product (MVP), einschliesslich erster Tests (Oktober 2017 bis Juli 2019). Das MVP wurde erfolgreich abgeschlossen und von Innosuisse abgenommen.
- Seit April 2020 steht der Basic Record allen Vereinsmitgliedern zur Verfügung. Damit erhalten alle Fahrzeuge eine elektronische De-facto-Identität.
- Eine erhebliche Anzahl an weiteren möglichen Partnern ist mit dem Verein Cardossier im Gespräch.

Fazit

- Ein Fazit ist noch nicht möglich.
- Als strategische Stossrichtung soll unter Führung des Bundesamts für Strassen der Basic Record um 110 Attribute erweitert werden, die das Certificate of Conformity (CoC) der Europäischen Union vorgibt. Damit kann CH-Formular 1320A abgelöst werden. Auf dieser Grundlage wird es anschliessend möglich sein, den Prozess der Immatrikulation von neuen Fahrzeugen vollständig digital darzustellen. Neben technischen Fragen werden in diesem Zusammenhang vor allem auch datenschutzrechtliche Probleme zu lösen sein.

Weitere Informationen

- cardossier.ch

3.8. Reparaturbestätigungsverfahren (Fürstentum Liechtenstein)

Ausgangslage

- Genügen Motorfahrzeuge und Anhänger nicht den technischen Anforderungen des Amts für Strassenverkehr des Fürstentums Liechtenstein oder des Strassenverkehrsamts des Kantons Aargau, kann die Fahrzeughalterin oder der Fahrzeughalter in einer dazu berechtigten Werkstätte eine Reparatur durchführen lassen.
- Dieser Prozess wird bis heute mit einem papierbasierten Reparaturbestätigungsverfahren (RBV) abgewickelt. Die Mängel werden auf einem physischen Formular festgehalten, auf dem die Werkstätte mit physischer Unterschrift bestätigt, dass die Mängel behoben worden sind. Anschliessend stellt die Fahrzeughalterin oder der Fahrzeughalter dieses Dokument dem Amt für Strassenverkehr zu oder bringt das Formular beim Amt vorbei, damit nach der Reparatur ein neuer Fahrzeugausweis ausstellt wird.
- Dieser mit Medienbrüchen behaftete Prozess ist zeit- und kostenintensiv und weist wenig Kundenfreundlichkeit auf.

Lösung

- Das Fürstentum Liechtenstein hat seit 1. Januar 2020 ein Blockchain-Gesetz, das Rechtssicherheit und Vertrauen in die Token-Ökonomie schafft. Das Amt für Strassenverkehr (ASV) will daher als erstes konkretes Projekt den RBV-Prozess digitalisieren und über eine Blockchain abwickeln, und zwar unter Verwendung der Token- und Smart-Contract-Technologie.
- Ist eine Reparatur erforderlich, generiert das ASV im neu vorgesehenen Prozess automatisch einen QR-Code und händigt diesen auf Papier dem Fahrzeughalter aus. Bei diesem QR-Code handelt es sich um einen Identifikator. Im Hintergrund werden die entsprechenden Angaben registriert.
- Mit dem Fahrzeug wird auch der QR-Code an die berechtigte Werkstatt übergeben. Diese ruft via den Identifikator die spezifische Mängelliste aus dem IT-System ab. Hierbei kann es sich zum Beispiel um Cari handeln, einer Fachapplikation, die sämtliche Geschäftsprozesse von Strassenverkehrsämtern in der Schweiz und dem Fürstentum Liechtenstein abdeckt.
- Nachdem die Mängelliste von der Werkstatt abgearbeitet wurde, markiert die Werkstatt das Fahrzeug in der Blockchain als repariert.
- Zusätzlich zieht die Werkstatt im Namen des ASV den aktuellen Fahrzeugausweis ein. Damit ist das RBV-Verfahren digital und rechtsverbindlich auf der Blockchain abgeschlossen.
- Zeitgleich wird auf der Grundlage eines Smart Contracts der neue Fahrzeugausweis automatisch beim ASV ausgedruckt und der Kundin oder dem Kunden per Post zugestellt.
- Die Kosten dieser Lösung werden vom ASV getragen; die Strassenverkehrsämter Aargau und Thurgau beteiligen sich ebenfalls an diesem Projekt.
- Auf welcher Blockchain das Reparaturbestätigungsverfahren dargestellt wird, ist noch nicht definitiv entschieden; unterschiedliche Konzepte stehen zur Diskussion. Ziel ist es, eine offene Technologielösung zu entwickeln, an der sich möglichst viele Akteure beteiligen können (Multi-Plattform-Architektur).
- Ebenfalls ist eine Integration der RBV-Lösung mit dem Cardossier (Kapitel 3.7) Gegenstand von aktuellen Überlegungen. Das Amt für Strassenverkehr ist aktives Mitglied des Vereins cardossier.ch

Tatsächliche Nutzung

- Aufgrund von Corona hat sich die Umsetzung des RBV-Projekts verzögert. Der neue Zeitplan ist noch nicht endgültig definiert. Geplant ist, mit einer Pilot- und Testphase zu starten. Diese wird gefolgt von der Produktivphase, in der die neue Technologie und deren rechtsverbindliche Anwendbarkeit im Rahmen von Behördengeschäften aufgezeigt werden soll. Zu diesem Zeitpunkt wird auch die Möglichkeit der Vernetzung mit anderen Prozessen und Partnern im Ökosystem gegeben sein.

Fazit

- Ein Fazit ist noch nicht möglich.
- Im Fürstentum Liechtenstein gilt dieses Projekt als erster Praxistest für das kürzlich erlassene Token- und VT-Dienstleister-Gesetz.
- Die RBV-Blockchain-Lösung zeigt die Möglichkeiten des Einsatzes der Technologie in der öffentlichen Verwaltung auf. Prozessoptimierung und -minimierung stehen im Vordergrund. Das Resultat ist eine Verbesserung der Abwicklung der Geschäftsfälle und eine Erleichterung für Kundinnen und Kunden und andere am Prozess beteiligte Organisationen.

Weitere Informationen

- 360º Vehicle Life Cycle Management

4. Mögliche Anwendungsbeispiele für den Kanton Zürich

Anhand einiger Anwendungsbeispiele lässt sich zeigen, welches Potenzial in der Blockchain-Technologie liegt, aber auch, welche technischen, organisatorischen und rechtlichen Herausforderungen damit verbunden sind. Allen Anwendungsbeispielen ist gemeinsam, dass sie aus Blockchain-Sicht weitgehend im luftleeren Raum gedacht werden müssen.

Erstens liegt im Kanton Zürich zurzeit keine staatlich anerkannte **elektronische Identität** vor, die allgemein verbreitet ist und die eine einfache und sichere Zugangsberechtigung zu einzelnen Blockchain-Applikationen gewähren würde. Die Relevanz elektronischer Identitäten – gerade für die Interaktion zwischen Staat und Bevölkerung – kann nicht überschätzt werden. Viele Geschäftsprozesse können erst dann vollständig digitalisiert werden, wenn sich Einwohnerinnen und Einwohner einfach und rechtsverbindlich digital identifizieren können. Nationalrat und Ständerat haben im November 2019 das Bundesgesetz über elektronische Identifizierungsdienste (BGEID) verabschiedet, das staatlich anerkannte Identitäten ermöglichen soll. Dagegen ist das Referendum ergriffen worden; Aufgrund der COVID-19-Pandemie wird die Volksabstimmung wohl erst im März 2021 durchgeführt. Im Rahmen der Einführung des elektronischen Patientendossiers (EPD) würden bereits elektronische Identitäten zertifiziert zur Verfügung stehen, die dem Anforderungsprofil nach BGEID weitgehend entsprechen beziehungsweise in gewissen Bereichen gar strenger sind. Die Einführung des EPD war ursprünglich für den 15. April 2020 geplant. Beruhend auf den heutigen Plänen der Stammgemeinschaften zeichnet sich ab, dass die Zertifizierungsverfahren zwischen Herbst 2020 und Frühling 2021 abgeschlossen werden können. Zudem ist in diesem Zusammenhang zu erwähnen, dass der Kanton Schaffhausen bereits kantonal anerkannte elektronische Identitäten ausstellt; die Stadt Zug plant, im Herbst 2020 die Blockchain-basierte elektronische Identität durch eine andere elektronische Identität zu ersetzen (siehe Kapitel 3.5).

Zweitens liegt keine kantonale **Blockchain-Infrastruktur** vor (Software und Nodes), auf der diese Anwendungsbeispiele integriert werden können. Auf nationaler Ebene ist diesbezüglich etwas Bewegung: Im Dezember 2018 haben die Schweizerische Post und die Swisscom eine rein schweizerische Infrastruktur für Blockchain-Anwendungen mit dem Namen «Consensus-as-a-Service (Caas)» angekündigt; inzwischen heisst diese Infrastruktur «Swiss Trust Chain». Das Ziel dieser Infrastruktur ist es, eine «private Blockchain» für die Schweiz zu bauen, die höchsten Sicherheitsanforderungen (Banking Grade) erfüllt. Das heisst, die Daten bleiben vollständig in der Schweiz in den Rechenzentren der beiden Betreiberfirmen. Die entsprechende Blockchain beruht auf Hyperledger Fabric und läuft mit einer Proof-of-Authority-Konsensregel. Ziel ist es, dass sich weitere vertrauenswürdige Firmen mit Sitz in der Schweiz an diesem Konsortium beteiligen. Neben privaten Unternehmen könnten auch staatliche Instanzen – insbesondere Bund und Kantone – Teil dieses Konsortiums werden und entsprechende Nodes betreiben. Damit wäre auch die technische Grundlage für Anwendungsfälle gelegt, wie sie im Folgenden beschrieben werden. Tests mit elektronischen Betreibungsregisterauszügen im Kanton Schaffhausen sind auf dieser Infrastruktur bereits erfolgreich durchgeführt worden (siehe Kapitel 3.3).

Sämtliche möglichen Anwendungsbeispiele werden folgendermassen dargestellt: In der **Ausgangslage** wird der Kontext, der für das Anwendungsbeispiel relevant ist, zusammengefasst

und das Problem aufgezeigt, das gelöst werden soll. Die **Idee** beschreibt die mögliche Lösung, wobei es hier vor allem darum geht, den Nutzen aus Anwendersicht in den Vordergrund zu stellen. In den Abschnitten **Infrastruktur** und **Prozess** wird in groben Zügen dargestellt, welche organisatorischen und technischen Vorkehrungen erforderlich sind, um die Idee zu realisieren. Insbesondere geht es um die Frage, welche Infrastruktur erforderlich ist und wie die zentralen Prozesse ausgestaltet werden können. Im Abschnitt **Datenschutz und andere rechtliche Überlegungen** werden erste Hypothesen formuliert. Anschliessend wird eine **Beurteilung** vorgenommen. Neben der Frage, warum eine Blockchain angewendet wird, sind folgende Kriterien relevant:

- **Warum auf einer Blockchain:** Unabhängig von den anderen Kriterien ist zu fragen, ob eine Blockchain tatsächlich erforderlich ist oder ob eine zentrale Datenbank oder eine andere Lösung zur Erfüllung der Aufgabe ausreicht.

- **Transaktionsvolumen:** Anzahl der erwarteten Transaktionen. Je tiefer das Volumen, desto höher muss der Wert jeder Transaktion ausfallen, um den zusätzlichen Aufwand, den eine Blockchain-Lösung mit sich bringt, zu rechtfertigen.

- **Transparenzbedarf:** Je geringer die aktuelle Transparenz heute ist, desto höher der Nachholbedarf. Wenn die meisten Informationen schon jetzt einfach einsehbar sind, ist der Transparenzbedarf tief.

- **Digitalisierungsgrad:** Hier geht es um die Frage, wie weit die Prozesse, die auf der Blockchain protokolliert werden sollen, bereits digitalisiert sind.

- **Rechtliche Hürden, insbesondere bezüglich des Datenschutzes:** Kurze Einschätzung, ob bereits eine ausreichende rechtliche Grundlage vorliegt und ob das Vorhaben mit den Grundsätzen des Datenschutzes im Einklang steht.

- **Schwierigkeit der Umsetzung:** Neben technischen und juristischen spielen oft auch organisatorische, kulturelle und politische Fragen eine Rolle dabei, wie leicht ein Vorhaben tatsächlich umgesetzt werden kann.

Ein kurzes **Fazit** rundet die Darstellung jeweils ab. Es ist wichtig festzuhalten, dass die hier präsentierten möglichen Anwendungsbeispiele nicht auf einer abschliessenden Bedürfnisabklärung beruhen. Auch die Machbarkeit wurde nicht endgültig überprüft.

Am Schluss werden die vier Anwendungsmöglichkeiten aufgrund ihrer Beurteilungen miteinander einem **Vergleich** unterzogen.

4.1. Registrierung von amtlichen Dokumenten auf der Blockchain zur Stärkung der Rechtssicherheit

Ausgangslage

- Die öffentlichen Verwaltungen erstellen eine Vielzahl von Registerauszügen, Beglaubigungen und Bewilligungen.
- Rechtsgültigkeit weisen in der Regel nur Dokumente in Papierform auf.
- Abgesehen von der Überprüfung der Echtheit der physischen Dokumente sind weitere Abklärungen für Dritte mit Aufwand und Kosten verbunden.

Idee

- Um Dritten die Überprüfung der Echtheit zu ermöglichen, werden relevante amtliche Dokumente bei der Ausgabe zusätzlich auf einer Blockchain verankert. Hierzu wird der Hash des Dokuments von der Ausgabestelle auf der Blockchain veröffentlicht, und es wird ein Zeitstempel erstellt.
- Da ein Zeitstempel nur für elektronische Dokumente überprüft werden kann, muss das Dokument auch digital verfügbar sein. Es wird der oder dem Antragstellenden elektronisch zugestellt.
- Zusätzlich sind weitere Methoden denkbar, über welche Dritte das Dokument ebenfalls digital beziehen können. Optional kann dem Dokument ein individueller QR-Code hinzugefügt werden, der ein Passwort und einen Downloadlink zum digitalen Dokument enthält.
- Dritten wird eine Validierungs-Applikation zur Überprüfung des Zeitstempels von Dokumenten auf der Blockchain zur Verfügung gestellt. Dies könnte beispielsweise ein Web-basiertes Interface analog dem Validator für digitale Signaturen der Bundesverwaltung (Link) sein.

Infrastruktur

- **Blockchain:** Als Blockchain kommen primär public-permissioned Blockchains infrage. Die Wahl hängt von der Verfügbarkeit der Lösungen (siehe dazu Kapitel 3) sowie von Kosten, Sicherheit und Vertrauen in die anbietenden Institutionen ab. Die hauptsächlichen Teilnehmenden am System sind Verwaltungseinheiten als Herausgeber von Dokumenten und Personen, welche die Echtheit von Dokumenten überprüfen wollen.
- **Fachapplikation:** Die Applikation, mit der Verwaltungsmitarbeitende digitale Auszüge im PDF-Format erstellen können.
- **Blockchain-Service:** Applikation für Verwaltungsmitarbeitende, die den Zeitstempel von Dokumenten erstellt und mit der Blockchain interagiert.
- **Validator-Service:** Öffentliche Applikation, die es erlaubt, die Blockchain nach Zeitstempeln von Dokumenten zu durchsuchen.

Prozess: Auszug erstellen und auf der Blockchain registrieren

1.1. Die oder der Verwaltungsmitarbeitende erstellt einen digitalen Auszug in der Fachapplikation im PDF-Format. Soll auch die papierbasierte Version des Auszugs elektronisch überprüfbar sein, fügt die Fachapplikation dem PDF einen QR-Code bei, der ein Passwort und einen Downloadlink zum digitalen Dokument enthält. Dieses PDF-Dokument wird anschliessend gedruckt und ausgehändigt.

1.2. Der Blockchain-Service der Verwaltungseinheit berechnet den Hash des Auszugs.

1.3. Der Hash wird in einer Transaktion vom Blockchain-Service an die Blockchain gesendet.
1.4. Sobald die Transaktion in einen Block aufgenommen wurde, ist der Hash unveränderbar in der Blockchain gespeichert. Aus der Erstellungszeit des Blocks ergibt sich der Zeitstempel.
1.5. Der Auszug wird der oder dem Antragstellenden digital zugestellt.

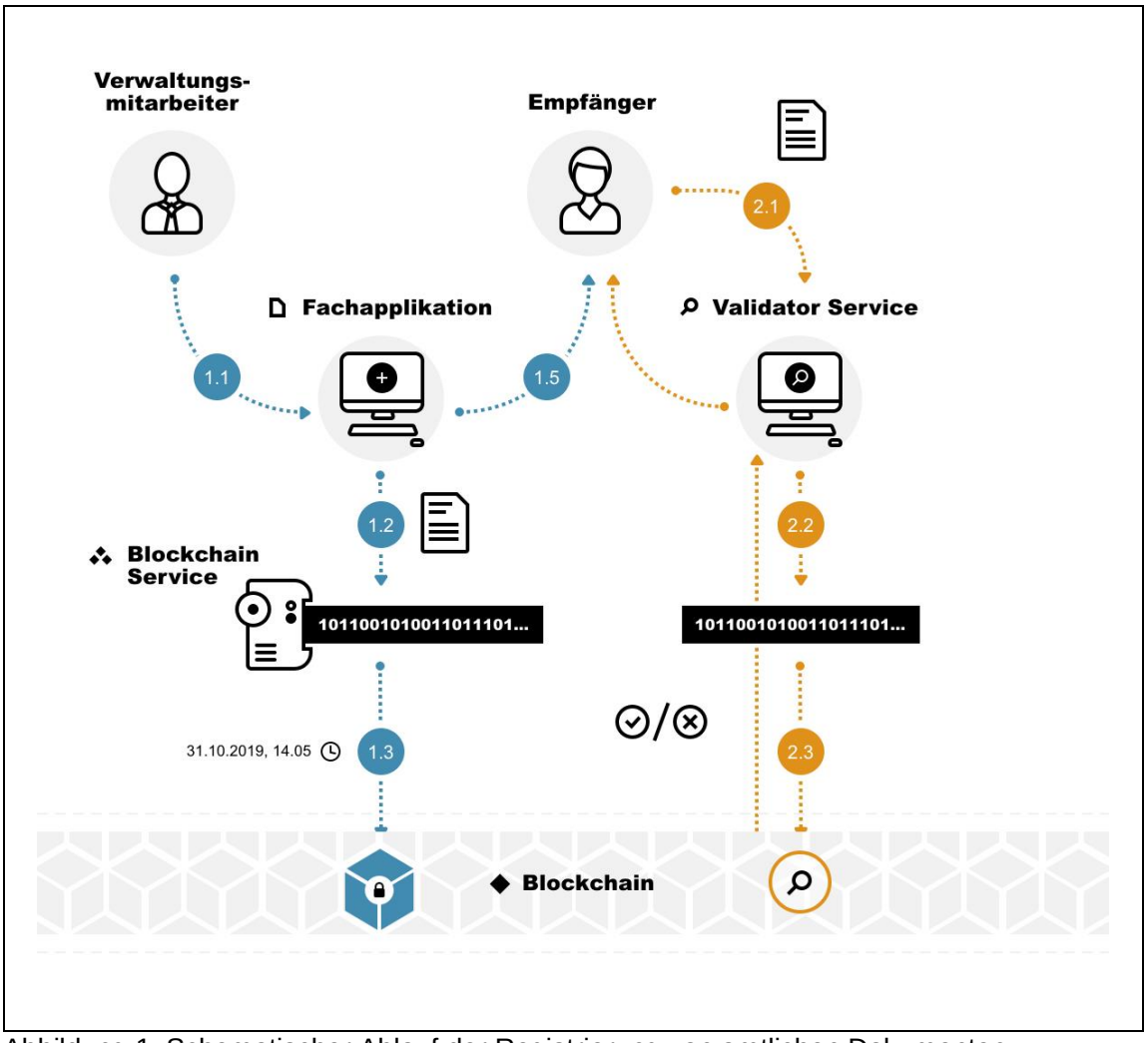

Abbildung 1: Schematischer Ablauf der Registrierung von amtlichen Dokumenten

Prozess: Validität eines Auszugs mithilfe der Blockchain überprüfen

2.1. Die den Auszug empfangende Person lädt diesen in den Validator-Service hoch. Falls sie eine papierbasierte Version überprüfen will, scannt sie den QR-Code, worauf eine digitale Version vom Auszug heruntergeladen wird. Diese vergleicht sie mit der Papiervariante und lädt diese darauf ebenfalls in den Validator-Service hoch.
2.2. Der Validator-Service berechnet den Hash des Auszugs.
2.3. Der Validator-Service durchsucht die Blockchain nach dem Hash und zeigt das Resultat der Empfängerin oder dem Empfänger an. Kann der Hash gefunden werden, handelt es sich um einen unverfälschten Auszug.

Datenschutz und andere rechtliche Überlegungen

- Auf der Blockchain werden ausschliesslich Zeitstempel beziehungsweise Hashes von Dokumenten abgelegt. In den Metadaten sind zusätzlich Herausgeber (Verwaltungseinheit) und Erstellungszeitpunkt des Dokuments ersichtlich. Die Zulässigkeit solcher Einträge muss näher analysiert werden, insbesondere auch mit Rücksicht auf den spezifischen Inhalt der Register.
- Durch die Zeitstempelung der Registerauszüge auf einer Blockchain erlangen diese noch keine rechtliche Wirkung im Sinne einer qualifizierten elektronischen Signatur. Es wird sich zeigen müssen, wie viel Vertrauen der Markt und die Rechtsprechung dieser Lösung entgegenbringen werden.
- Alternativ könnten die amtlichen Dokumente während der Erstellung mit einer qualifizierten elektronischen Signatur oder einer Organisationssignatur versehen werden, um die Rechtskraft zu garantieren. In diesem Fall hätte die Blockchain nur die Rolle eines unabhängigen Transaktions-Logs.
- Verschiedene Fragen zur Archivierungsfähigkeit müssen noch geklärt werden, wie etwa, wann die digitalen Informationen zu einem Geschäft vollständig und authentisch und in welcher Form sie als Paket barrierefrei zugänglich gemacht werden können.

Beurteilung

- Warum auf einer Blockchain: Mit der Zeitstempelung der amtlichen Dokumente wird unmittelbar ein nicht mehr verfälschbarer Audit-Trail angelegt. Dieser erhöht die Transparenz und Rechtssicherheit und kann das Vertrauen in die Behörden weiter stärken. Mit einer Blockchain kann die dezentrale Struktur der Ausgabe von Registerauszügen, Bewilligungen usw. direkt abgebildet werden. Das Konzept kann mit minimalem Aufwand erweitert werden, sowohl für weitere Register als auch weitere Aussteller. So wäre auch eine landesweite oder gar internationale Erweiterung technisch umsetzbar.
- Transaktionsvolumen: hoch, sofern diese Infrastruktur von allen beteiligten Ämtern genutzt wird.
- Transparenzbedarf: hoch.
- Digitalisierungsgrad: mittel, da diese Dokumente ja meist digital erstellt werden und anschliessend gedruckt, mit Stempel, Unterschrift und in gewissen Fällen mit Siegeln, Marken usw. versehen werden. Der Reifegrad der vor- und nachgelagerten Prozesse ist von Fall zu Fall zu analysieren.
- Rechtliche Hürden, insbesondere bezüglich des Datenschutzes: mittel, insbesondere in Abhängigkeit vom Inhalt des jeweiligen Registers.
- Schwierigkeit der Umsetzung: mittel, abhängig davon, ob die vor- und nachgelagerten Prozesse bereits digitalisiert sind. Die Beispiele aus den Kantonen Genf und Schaffhausen zeigen, dass Lösungen möglich sind.

Fazit

- Papierbasierte und elektronische Auszüge, Beglaubigungen usw. könnten mit wenig Aufwand und ohne Risiken öffentlich überprüfbar gemacht werden. Das Verfahren ist einfach auf weitere Stellen ausweitbar und universal anwendbar. Es kann davon ausgegangen werden, dass diese Art von Lösung in Kürze zur staatlichen Grundinfrastruktur werden wird, siehe Beispiele aus Genf und dem Ausland (Malta, Deutschland usw.). Der allgemeine Beitrag zur Digitalisierung einer Gesellschaft, den eine solche Lösung leisten würde, ist als sehr hoch einzuschätzen.
- Als nächster Schritt bietet sich ein Proof-of-Concept für ausgewählte Schriften an, unter Umständen in Zusammenarbeit mit anderen Kantonen, um einer schweizweiten Lösung von Beginn an Vorschub zu leisten.

4.2. Personendossier mit Blockchain-basiertem Logbuch zur Erhöhung der Transparenz

Ausgangslage

- Zahlreiche kantonale und kommunale Behörden führen in den verschiedensten staatlichen Tätigkeitsbereichen Personendossiers, in gewissen Fällen für die ganze Bevölkerung, in anderen Fällen nach Bedarf.
- Die Dossiers enthalten oft Informationen und Dokumente, die von anderen Behörden erstellt wurden oder auch für andere Behörden relevant sind. Beim Austausch zwischen Behörden werden diese Daten oft kopiert und nicht verknüpft.
- Zurzeit haben die betroffenen Personen keine direkte Einsicht in ihr Dossier. Es besteht zwar gemäss IDG das Recht auf Einsicht, aber das damit verbundene Verfahren ist umständlich und zeitintensiv – sowohl für die betroffenen Personen als auch die Behörden. Zudem kann anhand des traditionellen Zugangs nur teilweise nachvollzogen werden, wer wann welche Einträge in einem Dossier vorgenommen hat. Wer wann Einsicht genommen hat, kann kaum je nachvollzogen werden.

Idee

- Die betroffenen Personen bekommen Einsicht in ihr (vollständig digitalisiertes) Dossier.
- Jede Bearbeitung des Dossiers beziehungsweise der darin enthaltenen Dokumente werden auf einer Blockchain protokolliert.
- Die Zugriffsrechte auf das Dossier werden ebenfalls in der Blockchain verwaltet, sodass jede Änderung protokolliert wird.

Infrastruktur

- **Datenspeicher:** Zentraler Dokumentenspeicher, in dem die Dossier Inhalte abgelegt sind. Dieser muss sicherstellen, dass nur Berechtigte auf die jeweiligen Dossiers zugreifen. Prinzipiell kann es auch mehrere unabhängige Datenspeicher geben.
- **Fachapplikation Verwaltung:** Applikation, mit der Verwaltungsmitarbeitende auf die Dossiers zugreifen und Änderungen vornehmen.
- **Personen-Interface:** Öffentliche Applikation, mit der Personen auf ihre Dossiers zugreifen können.
- **Blockchain:** Zur Sicherstellung von Transparenz und Verfügbarkeit empfiehlt sich auch hier eine public permissioned Blockchain.
- **Starke elektronische Identität:** Aus Datenschutzgründen ist eine starke elektronische Identität erforderlich. Diese erlaubt es, für jede Transaktion einen anderen Identifier zu verwenden. Damit wird die generelle Zuordnung der Transaktionen für Aussenstehende verunmöglicht.

Prozess: Dossier bearbeiten

1.1. Die oder der Verwaltungsmitarbeitende führt in der Fachapplikation eine Aktion in einem Dossier aus. Dies kann ein Lese- oder Schreibvorgang sein oder eine Anpassung der Rechte (zum Beispiel Freigabe für eine andere Behörde).
1.2. Die Änderung wird an den Datenspeicher übertragen.
1.3. Die Änderung wird in der Blockchain protokolliert. Der Protokolleintrag umfasst die Identität der oder des Verwaltungsmitarbeitenden, ein eindeutiges Aktenzeichen von Dossier und betreffendem Dokument, die Art der Änderung und eventuell Zusatzin-

formationen zur Änderung. Bei einem Schreibvorgang wird der neue Hash des Dokuments zusätzlich gespeichert, beim Erteilen oder Entzug einer Berechtigung die betreffende Drittpartei.

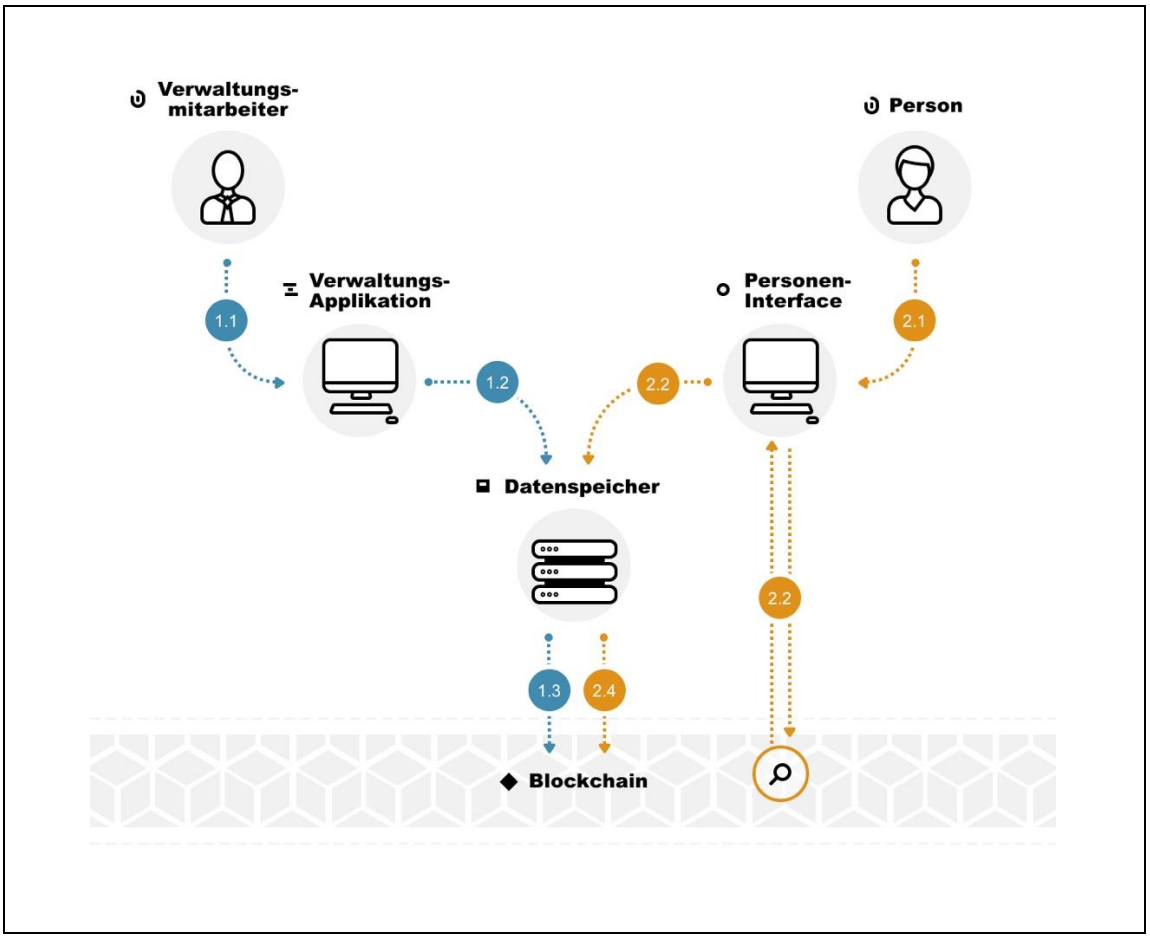

Abbildung 2: Schematischer Ablauf des Personendossiers mit Blockchain-basiertem Logbuch

Prozess: Einsicht in das Dossier durch betroffene Personen

2.1. Die betroffene Person identifiziert sich mit ihrer eID im Personen-Interface.
2.2. Das Personen-Interface durchsucht die Blockchain und zeigt den Inhalt des Dossiers, sowie die Bearbeitungshistorie an.
2.3. Wenn die betroffene Person ein Dokument einsehen will, wird es vom Datenspeicher geladen und angezeigt.
2.4. Die Einsichtnahme der betroffenen Person wird auf der Blockchain protokolliert.

Datenschutz und andere rechtliche Überlegungen

- Die Inhalte der Dossiers werden nur als Hash auf der Blockchain abgelegt.
- Die Zuordnung von einzelnen (verschlüsselten) Dossiers sowie Protokolleinträgen zu konkreten Identitäten muss durch kryptografische Verfahren verhindert werden. Dies erfordert eine starke elektronische Identität.
- Archivierungsfähigkeit und Authentizität: vergleiche Kapitel 4.1

Beurteilung

- Warum auf einer Blockchain: Wichtige Eigenschaften dieses Prozesses können direkt auf einer Blockchain abgebildet werden. Im Vergleich zu herkömmlichen Datenbanken schafft eine Blockchain automatisch Transparenz hinsichtlich der Bearbeitung der Dossiers und hinterlässt einen nicht veränderbaren Audit-Trail. Die Datenhaltung und der Betrieb der Blockchain kann zudem einfacher dezentralisiert und so zum Beispiel auf verschiedene Behörden aufgeteilt werden.
- Transaktionsvolumen: Abhängig von den digital verfügbaren Dossiers; tendenziell hoch.
- Transparenzbedarf: hoch. Wenn Daten zwischen Behörden geteilt werden, sollte die betroffene Person darüber informiert sein, um die Vorgänge überprüfen zu können. Allerdings gibt es wichtige Ausnahmen: Die betroffene Person soll zum Beispiel nicht merken, dass sie in den Fokus einer Strafuntersuchung geraten ist und daher über sie ermittelt wird.
- Digitalisierungsgrad: abhängig von der Art der Dossiers; tendenziell tief. Der häufigste Fall ist noch immer, dass in den öffentlichen Verwaltungen – insbesondere bei ämterübergreifenden Themen – die unterschiedlichen Applikationen nur zu einem geringen Masse integriert sind und entsprechende Datenstandards fehlen. Dies ist teilweise auch dem Datenschutzrecht geschuldet, das mit dem Zweckbindungsgebot Datensilos verlangt oder diese zumindest begünstigt. Wie dieses Gebot in Zukunft mit dem Once-only-Prinzip in Einklang gebracht wird, ist eine politische Frage.
- Rechtliche Hürden, insbesondere bezüglich des Datenschutzes: Wenn ganze Dossiers entsprechend berechtigten Personen verfügbar gemacht werden, sind die Anforderungen an den Datenschutz hoch. Dies namentlich, wenn es sich in einzelnen Fällen um besondere Personendaten gemäss § 3 Abs. 4 IDG handelt. Zudem ist zu beachten, dass gemäss § 3 Abs. 5 IDG auch Zugriffe unter die Datenbearbeitung fallen.
- Schwierigkeit der Umsetzung: hoch, da die vorgelagerten Prozesse erst digitalisiert werden müssen. Dazu sind in gewissen Fällen auch Applikationen zu integrieren und organisatorische Vorkehrungen zu treffen.

Fazit

- Der Nutzen dieser Lösung wäre aus Sicht der Bevölkerung beträchtlich, hätte diese doch erstmals auf digitalem Weg Einsicht in ihre Dossiers und könnte Veränderungen daran jederzeit nachvollziehen. Auch für die Verwaltung wären die Vorteile erheblich, würde doch eine solche Lösung zu bedeutenden Effizienzsteigerung führen.
- Eine Weiterführung dieser Idee macht jedoch erst Sinn, wenn alle relevanten Unterlagen und Prozesse digitalisiert und die jetzt im Einsatz stehenden Applikationen soweit integriert sind, dass ein umfassendes Dossier erzeugt werden kann. Zudem setzt diese Anwendung die Verfügbarkeit von starken elektronischen Identitäten voraus.

4.3. Inventarkontrolle auf der Blockchain zur Stärkung der Rechtssicherheit

Ausgangslage

- Die öffentliche Hand verfügt über grosse Bestände an physischen Gegenständen: Gebrauchsgegenstände, Werkzeuge, Mobilien, Fahrzeuge, Kunstgegenstände usw.
- Die Inventarkontrollen basieren auf unterschiedlichen Prozessen und Technologien. In gewissen Fällen sind diese bereits digitalisiert, in anderen wird weiterhin physisch Buch geführt. Dadurch sind die Inventarkontrollen aufwendig und tendenziell mangelhaft.

Idee

- Alle Gegenstände, die einen gewissen Wert überschreiten, werden mit einem QR-Code oder einem Badge versehen und parallel auf einer Blockchain registriert. Auf der Blockchain werden die Gegenstände durch Tokens repräsentiert. Dadurch wird es möglich, Inventarveränderungen dezentral zu erfassen; Blockchain-basierte Inventarkontrollen sollten damit der Realität näherkommen als herkömmliche Systeme.

Infrastruktur

- **Markierungen:** QR-Code oder NFC-/RFID-Badge mit einer eindeutigen Identifikationsnummer für jeden Gegenstand.
- **Eigentümer-Applikation:** Sie dient der erstmaligen Registrierung der Gegenstände; diese kann mit dem Scanner oder im Fall von grossen Volumina über einen Datenimport erfolgen. Mit dieser Applikation kann der Eigentümer auch jederzeit Inventarkontrollen via Blockchain durchführen. Die Eigentümer-Applikation bietet entsprechende Such- und Filterfunktionen. Sie kann Desktop- oder Smartphone-basiert sein.
- **Besitzer-Applikation:** Sie erlaubt es Besitzern, Gegenstände mit einer Scanner-Funktion zu registrieren und Zustandsmeldungen zu machen. Alle von diesem Besitzer registrierten Gegenstände werden in einem oder mehreren Wallets vermerkt.
- **Blockchain:** Public- oder private-permissioned Blockchain.

Prozess: Eigentümer registriert ein neuer Gegenstand

1.1 Markierung des Gegenstands mit einer Identifikationsnummer: Die Behörde, die über die Eigentumsrechte verfügt, versieht alle Objekte mit einer eindeutigen Identifikationsnummer. Je nach Wert oder Risikoprofil kann dafür ein QR-Code oder ein NFC-/RFID-Badge eingesetzt werden.

1.2 Registrieren: Die Behörde registriert das Objekt mit mindestens folgenden Angaben auf der Blockchain:

i. Datum der Registrierung
ii. Objekt-Identifikationsnummer
iii. Beschreibung des Objekts
iv. Beschreibung des Zustands des Objekts
v. Geografischer Standort
vi. Identität des Besitzers/Wallet

1.3 Definitive Aufnahme in die Blockchain: Bei der nächsten Blockgenerierung wird die Registrierung definitiv in die Blockchain aufgenommen.

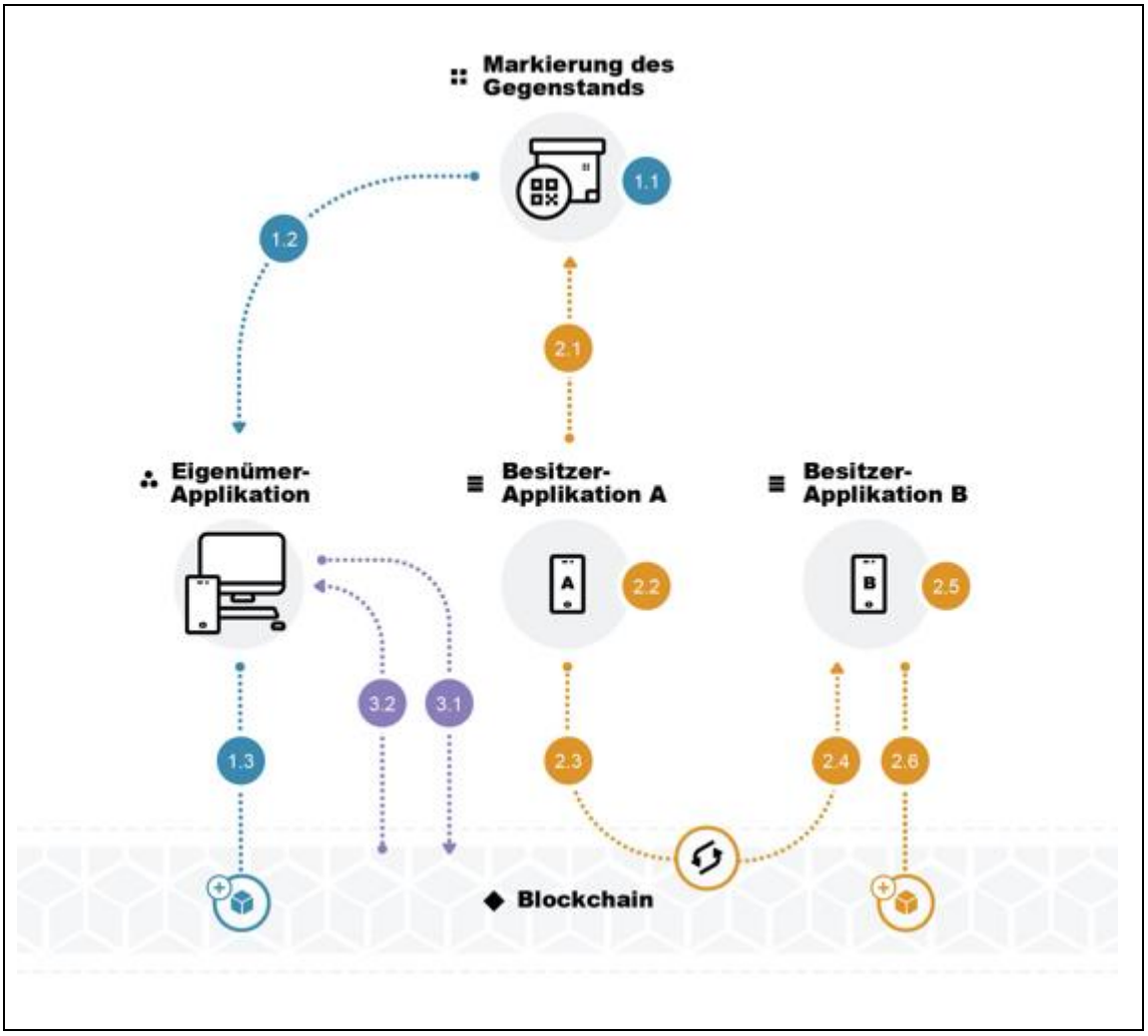

Abbildung 3: Schematischer Ablauf der Blockchain-basierten Inventarkontrolle

Prozess: Besitzerwechsel beziehungsweise Zustands- oder Ortswechsel

2.1 Scannen des Gegenstands: Sobald ein Besitzerwechsel oder eine Aktualisierung des Zustands (Beschreibung des Zustands, geografischer Standort) vollzogen werden soll, scannt der zukünftige Besitzer den QR-Code oder Badge des betreffenden Gegenstands. Dem (zukünftigen) Besitzer werden die Informationen angezeigt, die sich auf der Blockchain befinden:

i. Datum der (letzten) Registrierung
ii. Objekt-Identifikationsnummer
iii. Beschreibung des Objekts
iv. Beschreibung des Zustands des Objekts
v. Geografischer Standort
vi. Identität des aktuellen Besitzers/Wallet

2.2 Erfassen des aktuellen Zustands: Sollte sich der Zustand des Objekts seit der letzten Registrierung verändert haben oder wird der Gegenstand an einen neuen Standort bewegt, kann der zukünftige Besitzer entsprechende Anmerkungen anbringen.

2.3 Übermittlung der Informationen an die Blockchain: Anschliessend bestätigt die erfassende Person sämtliche Einträge und übermittelt diese an die Blockchain. Diese finden dort noch nicht Eingang in einen neuen Block.
2.4 Anfrage an den aktuellen Besitzer: Der aktuelle Besitzer erhält für den gewünschten Besitzerwechsel oder Zustandsänderung eine Anfrage mit folgenden Angaben:
    i. Datum der neuen Registrierung
    ii. Objekt-Identifikationsnummer
    iii. Beschreibung des Objekts
    iv. Beschreibung des aktuellen Zustands des Objekts
    v. Geografischer Standort
    vi. Identität des zukünftigen Besitzers/Wallet
2.5 Zustimmung des aktuellen Besitzers: Sofern der aktuelle Besitzer mit den Änderungen einverstanden ist, stimmt er ihnen zu.
2.6 Definitive Aufnahme in die Blockchain: Bei der nächsten Blockgenerierung werden die Änderungen definitiv mit folgenden Informationen in die Blockchain aufgenommen:
    i. Datum der neuen Registrierung (zur Handänderung)
    ii. Objekt-Identifikationsnummer
    iii. Beschreibung des Objekts
    iv. Beschreibung des aktuellen Zustands des Objekts
    v. Geografischer Standort
    vi. Identität des neuen Besitzers/Wallet

Prozess: Inventur durchführen

3.1 Bestellung einer Inventur: Jederzeit kann der Eigentümer eine Inventur bestellen. Dies geschieht via Eigentümer-Applikation, die entsprechende Such- und Filterfunktionen bietet. Sobald der Umfang einer Inventur definiert ist, wird die Bestellung an die Blockchain übermittelt.
3.2 Durchführung der Inventur: Die Blockchain wird entsprechend den definierten Kriterien durchsucht, und es wird ein Inventar erstellt.

Datenschutz und andere rechtliche Überlegungen

- Die objektbezogenen Informationen, die auf der Blockchain registriert werden, sind bezüglich des Datenschutzes unproblematisch.
- Die personenbezogenen Daten (Identität des Besitzers) können entweder mit dem Einsatz von unterschiedlichen Wallets oder mit starken elektronischen Identitäten geschützt werden – dies, sofern datenschutzrechtlich ein Schutz erforderlich beziehungsweise gegeben ist. Beispielsweise ist es kein datenschutzrechtlich geschützter Umstand, dass das Kunstwerk X im Büro der Amtsperson Y hängt; allenfalls sind zusätzlich polizeilichen Aspekten Beachtung zu schenken.

Beurteilung

- Warum auf einer Blockchain: Mit der Inventarisierung von Gegenständen auf der Blockchain wird unmittelbar ein nicht mehr verfälschbarer Audit-Trail angelegt. Dieser erhöht die Transparenz und Rechtssicherheit, insbesondere zwischen Parteien, die sich nicht uneingeschränkt vertrauen. Mit einer Blockchain kann die dezentrale Struktur der Ausgabe von Gegenständen direkt abgebildet werden. Es ist transparent einsehbar, welche Gegenstände sich in wessen Besitz befinden.
- Transaktionsvolumen: hoch, sofern die Lösung grossflächig zum Einsatz kommt.

- Transparenzbedarf: mittel, je nach Art der Gegenstände, die mit dieser Lösung inventarisiert werden
- Digitalisierungsgrad: mittel
- Rechtliche Hürden, insbesondere bezüglich des Datenschutzes: tief. Die Registrierung von Informationen, die Gegenstände betreffen, sollte unproblematisch sein. Hinsichtlich der personenbezogenen Daten müssen Vorkehrungen getroffen werden, damit diese datenschutzgerecht eingesetzt werden können.
- Schwierigkeit der Umsetzung: technisch: mittel. Vorarbeiten im Bereich SAP sind zu berücksichtigen. Organisatorisch: hoch. Es müssten alle Gegenstände mit einem QR-Code oder Badge versehen werden.

Fazit

- Mit dieser Lösung könnten Transparenz und Qualität von Inventaren erheblich gesteigert werden. Durch die Registrierung des Besitzers wird das Verantwortungsgefühl gesteigert, und mit einer Smartphone-basierten Lösung würde die Abwicklung für alle vereinfacht.
- Inventuren könnten jederzeit durchgeführt werden, und es läge ein unveränderbarer Audit-Trail vor.

4.4. Öffentliche Ausschreibungen auf der Blockchain

Ausgangslage

- Öffentliche Ausschreibungen unterliegen strengen Regeln hinsichtlich der Vergabe. Nichtsdestotrotz kommt es zu Verstössen und Unstimmigkeiten in den Ausschreibungsverfahren. Die Bearbeitung ist zudem aufwendig und der Automatisierungsgrad gering.
- Die Gesamtsumme von Zahlungen im Zusammenhang mit öffentlichen Ausschreibungen in der Schweiz beträgt derzeit rund 41 Mrd. Franken im Jahr.

Idee

- Der ganze Ausschreibungsprozess wird digitalisiert, einschliesslich der Angebotsabgabe in Form von strukturierten Daten und mithilfe von geprüften elektronischen Identitäten der teilnehmenden Parteien. Die Auswertung der Angebote wird so weit wie möglich mithilfe von Smart Contracts automatisiert. Mittels Blockchain-Zeitstempeln wird der gesamte Prozess transparent und fälschungssicher dargestellt.
- Die einzelnen Schritte einer Offerte, namentlich auch das Bieterverfahren, werden mithilfe von Smart Contracts programmiert, und gewisse Überprüfungen wie die des Eintrags im Handelsregister oder der Erfüllung der sozialrechtlichen Verpflichtungen werden so weit wie möglich durch Smart Contracts automatisiert.
- Die Offerten (Teilnehmende und Gebote) werden erst nach Ablauf der entsprechenden Fristen entschlüsselt und öffentlich zugänglich gemacht.

Infrastruktur und Prozesse

- Die eingesetzte Blockchain sollte von der öffentlichen Hand betrieben werden und für unbeteiligte Parteien nicht einsehbar sein (private-permissioned Blockchain).
- Eine Grundlage der Architektur sind geprüfte elektronische Identitäten der teilnahmeberechtigten Parteien. Diese eIDs identifizieren die Teilnehmenden eindeutig, und die Teilnahmeberechtigung am Bieteprozess kann automatisch nachvollzogen werden. Das Erfordernis einer eID muss so ausgestaltet werden, dass dadurch keine grundsätzlich berechtigten Personen vom Ausschreibungsprozess ausgeschlossen werden.
- Die automatisierten Prozessabläufe werden mittels Smart Contracts dargestellt. Folgende Schritte sollten programmiert werden: Registrierung einer neuen Ausschreibung einschliesslich aller nötigen Informationen, Einschreibung und Prüfung der Teilnehmenden (mittels eID), Zeitplan des Ausschreibungsprozesses und automatisierte Evaluation der Eingaben am Ende des Bieteprozess einschliesslich der Offenlegung sämtlicher Prozessschritte (Audit-Trail) und Teilnehmenden.
- Die einzelnen Schritte der Eingaben werden mittels Zeitstempel auf der Blockchain festgehalten.
- Mittelfristig können auch nachgelagerte Prozessteile (zum Beispiel Ausführung und Umsetzung der Ausschreibung) auf der Grundlage der in der Ausschreibung genannten Kriterien (Milestones, Teilzahlungen) automatisiert und fälschungssicher gemacht werden.

Datenschutz und andere rechtliche Überlegungen

- Damit das volle Potenzial einer Blockchain-Lösung ausgeschöpft werden kann, sind erhebliche Anpassungen im Submissionsrecht erforderlich. Dabei ist zu beachten, dass in diesem Bereich hauptsächlich Bundesrecht, im Einklang mit supranationalem Recht, zur Anwendung kommt.

Beurteilung

- Warum auf einer Blockchain: Der ganze Ausschreibungsprozess kann auf einer Blockchain transparent und fälschungssicher dargestellt werden. Damit kann das Vertrauen in diesen Prozess gesteigert werden.
- Transaktionsvolumen: mittel
- Transparenzbedarf: hoch, da Transparenz bei Vergabe von öffentlichen Aufträgen wichtig ist und so Missbrauch eher verhindert werden kann. Heute hat das Submissionsverfahren für Aussenstehende teilweise die Eigenschaft einer Blackbox.
- Digitalisierungsgrad: mittel, die Ausschreibungen selbst werden heute über elektronische Plattformen publiziert. Die Auswertungsprozesse umfassen dagegen in erheblichem Masse manuelle Tätigkeiten.
- Recht und insbesondere Datenschutz: hoher Anpassungsbedarf im Zusammenhang mit der Veröffentlichung der Entscheidungsgrundlagen und der Identität der Bieter. Nach geltendem Recht beschränkt sich die Publikation von Informationen zu einzelnen Ausschreibungsverfahren auf das Einladungsdokument und den Zuschlag. Wer die anderen Anbieter sind, kann in der Regel erst in einem Gerichtsverfahren in Erfahrung gebracht werden. Eine radikale Umsetzung würde daher einen hohen Anpassungsbedarf bedeuten; zu prüfen wäre ausserdem, inwiefern supranationales Recht (EU, GATT/WTO) den Spielraum einschränkt.
- Schwierigkeit der Umsetzung: hoch.

Fazit

- Der Nutzen der Blockchain-Technologie im Zusammenhang mit öffentlichen Ausschreibungen ist gegeben. Die Möglichkeit, die Ausschreibungen und die damit verbundenen Prozessschritte zu automatisieren und fälschungssicher zu machen, gehen auf die Kernfunktionen von Blockchains zurück: Transparenz, Nachvollziehbarkeit und Automatisierung von Entscheidungsprozessen. Die Herausforderungen im Bereich Datenschutz und Prozessautomatisierung sind erheblich und die Umsetzung zurzeit schwierig, allenfalls in Teilbereichen denkbar.

4.5. Vergleich der möglichen Anwendungsbeispiele

Mit der Beurteilung der möglichen Anwendungsbeispiele werden deren Nutzen geschätzt und mögliche Hindernisse identifiziert. So ergeben sich Anhaltspunkte, in welchen Fällen es sich lohnt, weitere Abklärungen vorzunehmen und/oder sie zu realisieren. Die einzelnen Beurteilungskriterien sind wie folgt zu interpretieren:

- **Transaktionsvolumen:** Ein hohes Transaktionsvolumen bedeutet, dass die Anwendung rege genutzt wird. Mit anderen Worten, es ist ein grosser Nutzen zu erwarten. Anwendungsbeispiele, bei denen ein hohes Transaktionsvolumen erwartet wird, empfehlen sich daher für eine weitere Prüfung und oder Realisierung, in der folgenden Tabelle sind sie mit einer grünen Ampel gekennzeichnet. Anwendungsbeispiele, die ein geringes Transaktionsvolumen aufweisen, sind mit einer roten Ampel gekennzeichnet.

- **Transparenzbedarf:** Wenn ein hoher Transparenzbedarf vorliegt, wird davon ausgegangen, dass die Blockchain-Lösung in erheblichem Masse zur Herstellung von Transparenz beiträgt. Daher werden Anwendungsbeispiele mit hohem Transparenzbedarf mit einer grünen Ampel dargestellt. Anwendungsbeispiele, die einen geringen Transparenzbedarf aufweisen, werden mit einer roten Ampel gekennzeichnet.

- **Digitalisierungsgrad:** Anhand des Digitalisierungsgrads kann abgeschätzt werden, welche Hürden mit Blick auf Prozesse und Organisation vorliegen, um eine Blockchain-Lösung implementieren zu können. Bei einem hohen Digitalisierungsgrad fallen diese Hürden weniger ins Gewicht; daher werden entsprechende Anwendungsbeispiele mit einer grünen Ampel dargestellt. Soll eine Blockchain-Lösung in einem Umfeld mit tiefem Digitalisierungsgrad implementiert werden, wird dies mit einer roten Ampel signalisiert.

- **Rechtliche Hürden, insbesondere bezüglich des Datenschutzes:** Anwendungsbeispiele, bei denen davon auszugehen ist, dass hohe rechtliche Hürden vorliegen, werden mit einer roten Ampel gekennzeichnet. Umgekehrt werden Anwendungsbeispiele, bei denen nur tiefe rechtliche Hürden zu veranschlagen sind, mit einer grünen Ampel dargestellt.

- **Schwierigkeit der Umsetzung:** Analog zu den rechtlichen Hürden werden Anwendungsbeispiele, die eine hohe Schwierigkeit der Umsetzung aufweisen, mit einer roten Ampel signalisiert. Anwendungsbeispiele, die einfach umsetzbar sind, werden mit einer grünen Ampel gekennzeichnet.

In der folgenden Tabelle werden die vier möglichen Anwendungsbeispiele anhand der Beurteilungskriterien miteinander verglichen. Die Bedeutung der grünen und roten Ampeln ist oben dargelegt; Orange weist auf eine mittlere Ausprägung hin.

	Registrierung amtlicher Dokumente	Personendossier mit Logbuch	Inventarkontrolle	Ausschreibungen
Transaktionsvolumen				
Transparenzbedarf				
Digitalisierungsgrad				
Recht, insbesondere Datenschutz				
Schwierigkeit der Umsetzung				

Tabelle 3: Vergleich der vier möglichen Anwendungsbeispiele

In Ergänzung zu den Fazits, die in den Kapiteln zu den einzelnen Anwendungsbeispielen formuliert worden sind, lässt sich folgern:

- **Registrierung amtlicher Dokumente:** Der Nutzen scheint sowohl bezüglich des Transaktionsvolumens als auch des Transparenzbedarfs gegeben zu sein. Im Falle einer Realisierung ist mit Hindernissen zu rechnen, diese sollten aber überwindbar sein.

- **Personendossier mit Logbuch:** Auch hier scheint der Nutzen gross zu sein. Diesen Nutzen zu realisieren dürfte allerdings schwierig sein: In allen Hinderniskategorien ist mit erheblichen Schwierigkeiten zu rechnen.

- **Inventarkontrolle:** Der Nutzen einer Blockchain-basierten Inventarkontrolle würde nicht so gross ausfallen wie bei den ersten beiden Anwendungsbeispielen. Aufgewogen wird dieser Nachteil durch geringere Hindernisse.

- **Ausschreibungen:** Auch hier ist kein grosser Nutzen zu erwarten. Gleichzeitig würde eine Umsetzung mit erheblichen Hindernissen konfrontiert, die einen Erfolg kaum zulassen würden.

5. Zusammenfassung

Eine Blockchain ist die Aneinanderreihung von Datensätzen, Blöcke genannt, die durch kryptografische Verfahren («Hashes») miteinander fest verkettet sind. Die Darstellung von Informationen als Kette («**Chain»**) von Blöcken («**Block**») ergibt das Kunstwort «Blockchain». Die Verkettung der Blöcke mittels Hashes erlaubt es, die gesamte Vorgeschichte einer Blockchain jeweils in den neuesten Block zu kondensieren. Damit entsteht ein unverfälschbarer Audit-Trail.

Blockchains können unterschiedlich konzipiert werden. Erstens wird differenziert bezüglich des Grads der **Zugangsrechte** (Unterscheidung nach Lese- und Schreibrechten). Zweitens wird unterschieden nach **Konsensregeln**, die festlegen, wer den nächsten Block berechnen und publizieren darf. Es besteht eine logische Abhängigkeit zwischen Zugangsrechten und Konsensregeln. Blockchains, die Lese- und Schreibrechte uneingeschränkt gewähren, wenden normalerweise die Konsensregel Proof-of-Work an. Bei dieser Konsensregel ist die Rechenleistung der einzelnen Teilnehmenden der entscheidende Faktor. Bekannteste Beispiele dieser Art von Blockchain sind Bitcoin und Ethereum. Diese Art von Blockchains hat sich bezüglich der Sicherheit als robust erwiesen; ihr grösster Nachteil ist, dass der Skalierung – also der Fähigkeit, grosse Mengen von Transaktionen durchzuführen – Grenzen gesetzt sind. Zudem brauchen sie grosse Mengen Energie. Am anderen Ende des Blockchain-Spektrums bewegen sich private Blockchains, wo sowohl Lese- als auch Schreibrechte auf einen ausgewählten Kreis beschränkt sind. Hier stellt die Skalierung kein sonderliches Problem dar; auch der Energieverbrauch ist bei solchen Blockchains vernachlässigbar. Allerdings bieten solche Blockchains aufgrund der fehlenden Transparenz und Dezentralisierung nicht die gleichen Vorteile wie öffentliche Blockchains.

Aufgrund der Tatsache, dass Blockchains dynamischen Charakter haben, also die Entwicklung von einzelnen Datenpunkten über die Zeit darstellen, ist es möglich, auf der Blockchain Transaktionen in Abhängigkeit von Bedingungen zu programmieren. Dies geschieht mittels **Smart Contracts**. Diese sorgen dafür, dass Transaktionen ausgeführt werden, sobald gewisse Bedingungen erfüllt sind. Dies erlaubt es, auch komplexe Transaktionen zu automatisieren.

Die Blockchain-Technologie wurde ursprünglich entwickelt, um über eine Infrastruktur zu verfügen, die ohne eine zentrale Autorität auskommt. Deshalb stellt sich die Frage, inwiefern es für den Staat hilfreich/nützlich ist, diese Technologie einzusetzen, ist er als Inhaber des physischen Gewaltmonopols doch das Sinnbild einer zentralen Autorität. Im Falle eines **idealen Staats**, der effizient und rechtmässig arbeitet, bedeutet die Anwendung der Blockchain-Technologie eine Verkomplizierung; zentrale Datenbanken genügen. Ein besonderer Anwendungsbereich bilden demokratische Wahl- und Abstimmungsverfahren, bei denen Bürgerinnen und Bürger ihr Wahlgeheimnis gewahrt wissen, gleichzeitig aber auch sicher sein wollen, dass ihr politischer Wille korrekt ins Ergebnis einfliesst. Auf öffentlichen Blockchains wäre dies möglich; allerdings zum Preis der Unmöglichkeit der späteren Vernichtung der Wahlunterlagen.

Staaten weichen vom Ideal ab, indem sie Strukturen und Prozesse aufweisen, die einen mehr oder weniger effizienten Mitteleinsatz zur Folge haben. Zudem können sich Amtsträgerinnen und Amtsträger und Staatsangestellte mehr oder weniger gesetzeskonform verhalten beziehungsweise Fehler verursachen. Blockchains können die damit verbundenen **Ineffizienzen**

mildern, indem sie die Grundlage für Datenkonsistenz bieten. Darauf aufbauend können Prozesse weiter digitalisiert und automatisiert werden, und (unbeabsichtigtes) menschliches Fehlverhalten kann besser nachvollzogen werden. Blockchains verhindern gesetzeswidriges Verhalten nicht per se, aber ein jederzeit einsehbarer und unverfälschbarer Audit-Trail erhöht den Druck, sich korrekt zu verhalten.

Der Nutzen einer Blockchain-Lösung kann sich nur entfalten, wenn die entsprechenden Rahmenbedingungen gegeben sind. Jeder Veränderungsprozess setzt **politischen Willen** und Führungsverantwortung voraus. Dies ist bei allfälligen Blockchain-Anwendungen umso mehr der Fall, weil deren Implementation Konsequenzen haben, die über technische Aspekte weit hinausgehen. Neben organisatorischen und kulturellen Fragen sind insbesondere auch rechtliche Fragen zu beachten: Erstens ist jeweils zu prüfen, ob für eine Blockchain-Anwendung die erforderliche **rechtliche Grundlage** vorhanden ist, und zweitens, ob diese mit dem **Datenschutzrecht** in Einklang steht, und drittens, ob eine rechtskonforme Archivierung möglich ist. Den verfassungsmässig garantierten Rechten – Schutz von Personendaten, Recht auf Korrektur und Löschung, Recht auf Erinnerung (die zueinander in Konkurrenz stehen können) – ist Rechnung zu tragen.

Im Zuge der allgemeinen Begeisterung über die Blockchain-Technologie im Allgemeinen und Kryptowährungen im Besonderen sind weltweit Hunderte Konzepte formuliert und Pilotprojekte für **Blockchain-Anwendungen in öffentlichen Verwaltungen** durchgeführt worden. Produktive Anwendungen mit namhaften Transaktionsvolumina sind aber noch keine bekannt. Dieser Befund trifft auch auf die Schweiz zu: Im Rahmen dieser Studie konnten acht Blockchain-Projekte identifiziert werden, in denen kantonale Verwaltungen und das Fürstentum Liechtenstein in den Bereichen Register, elektronische Identitäten, E-Voting und Bezahlung von Gebühren erste Erfahrungen gesammelt haben oder sammeln. Diese Projekte sind abgeschlossen worden, teilweise noch im Gang oder in Vorbereitung.

Der Reifegrad der Darstellung der vier Anwendungsbeispiele für den Kanton Zürich ist unterschiedlich, ebenso wie die Schwierigkeiten bei einer allfälligen Umsetzung. Allen ist jedoch gemeinsam, dass sie sich die unmittelbare und nicht mehr verfälschbare **Transparenz** von Blockchains zunutze machen. Zentrale Datenbanken sind nicht dafür ausgelegt, einem grossen Kreis in dynamischer Weise Transparenz zu bieten. Eine solche Funktion kann zwar auch in zentralen Architekturen nachgebaut werden, Blockchains lösen das Problem jedoch eleganter. Hinzu kommt, dass **dezentrale Architekturen,** wie sie Blockchains aufweisen, tendenziell einen **Vertrauensvorsprung** bieten, der von zentral konzipierten Lösungen nicht eingeholt werden kann.

6. Fazit

6.1. Allgemeine Einschätzung

Im Rahmen dieser Studie konnten noch keine Blockchain-Anwendungen in der öffentlichen Verwaltung ausgemacht werden, die Geschäftsprozesse grundlegend verändern und auch skalieren. Dass sich die ursprünglich hohen Erwartungen (noch) nicht erfüllt haben, hat verschiedene Gründe, insbesondere:

- **Technologie**, die sich **noch in Entwicklung** befindet und deren Infrastruktur noch im Aufbau ist;
- die **unvollständige Digitalisierung** von Geschäftsprozessen der öffentlichen Organe, die künftig mit Blockchain-Lösungen abgewickelt werden können;
- fehlende **gesetzliche Grundlagen,** einschliesslich Interoperabilitäts- und Standardisierungsnormen;
- fehlendes **Wissen** und Verständnis der Anwendungsmöglichkeiten;
- fehlende **Infrastruktur.**

6.2. Mehrwerte der Blockchain-Technologie

Grundsätzlich können Blockchain-Lösungen Mehrwert bieten. Erstens, indem sie einen **effizienteren Mitteleinsatz** erlauben:

- Daten auf einer Blockchain sind für alle (Berechtigten) gleichermassen verfügbar. Die Kosten des Zugangs können reduziert und die Datenkonsistenz kann erhöht werden. Damit ist ein Element zur Umsetzung des **Once-only-**Prinzips gegeben.
- Dank allgemein verfügbaren und konsistenten Daten ist es möglich, Geschäftsprozesse zu **vereinfachen;**
- Im Idealfall können Geschäftsprozesse nicht nur vereinfacht, sondern auch neu gedacht und teils **automatisiert** werden. Smart Contracts und andere Blockchain-basierte Mechanismen erlauben es, teure Handarbeit zu vermeiden. So kann sowohl willentliches als auch unbeabsichtigtes menschliches Fehlverhalten ausgeschlossen werden.

Zweitens schaffen Blockchain-Lösungen **Transparenz;** in welchem Grad hängt von der Art der jeweiligen Blockchain ab. Die Transparenz bietet folgende Vorteile:

- Transaktionen, die auf einer Blockchain registriert werden, sind **unmittelbar und automatisch einsehbar.** Dem Blackbox-Charakter, den die Verwaltung für Aussenstehende teilweise aufweist, kann so entgegengewirkt werden.
- Da Einträge auf einer Blockchain unveränderbar sind, wird jeweils ein zuverlässiger **Audit-Trail** generiert. Damit können Geschäftsprozesse auch im Nachhinein detailliert und verlässlich nachvollzogen werden.

Aus der Sicht von **Bevölkerung** und **Wirtschaft** kann der Einsatz der Blockchain-Technologie das **Vertrauen** in die öffentliche Verwaltung stärken. Gerade jenen Personen, die der

Digitalisierung kritisch gegenüberstehen, kann die Verwaltung mit der ausgebauten Transparenz etwas anbieten, was unter analogen Bedingungen unmöglich oder sehr kostspielig ist. Der effizienteren Mitteleinsatz wirkt sich langfristig positiv auf den Staatshaushalt und die **Steuerbelastung** aus.

Für **Politik** und **Verwaltung** kann das Vertrauen in die öffentliche Verwaltung auf eine andere Grundlage gestellt werden. Damit kann das Verhältnis zwischen Amtsträgerinnen und Amtsträgern, Staatsangestellten, Bevölkerung und Wirtschaft offener und partnerschaftlicher gestaltet werden. Mit der Automatisierung von Prozessen werden **Kapazitäten frei** für andere Aufgaben.

6.3. Handlungsbedarf

Ungeachtet von diesen Vorteilen ist immer zu bedenken, dass die Blockchain-Technologie auch **nur eine Technologie** ist. Sie weist kein inhärentes Sinnangebot auf. Ihr Nutzen ergibt sich, wie im Falle von anderen Technologien auch, immer aus ihrem sozialen Kontext. In diesem Sinne sind insbesondere Politik, Recht und Fachbereiche gefordert:

- **Politik:** Der fortgeschrittene Digitalisierungsgrad ist eine wichtige Voraussetzung für den Blockchain Einsatz. Unabhängig von der Wahl der technischen Mittel ist daher die Digitalisierung in der öffentlichen Verwaltung mit Hochdruck voranzutreiben. Zudem sind Pilotprojekte sowie der Aufbau von Basisinfrastrukturen, etwa für elektronische Identitäten, zu priorisieren.

- **Recht:** Angesichts der Tatsache, dass andere Kantone bereits erste Erfahrungen mit Blockchain-Anwendungen gesammelt haben, bietet es sich an, mit diesen in Kontakt und in einen systematischen Erfahrungsaustausch zu treten. Bei diesem Dialog sollte die Frage im Vordergrund stehen, worin der eigene spezifische Rechtsetzungsbedarf besteht und wie er am besten gedeckt werden kann.

- **Fachbereiche:** Auch hier ist unabhängig von der Wahl der technischen Mittel die Digitalisierung der öffentlichen Verwaltung mit Hochdruck voranzutreiben. Insbesondere sind Ideen zu entwickeln, wie Prozesse noch stärker auf die heutigen und künftigen Kundenbedürfnisse ausgerichtet werden können, jenseits der bisherigen departementalen und föderalen Strukturen. Ob Blockchain Teil einer Lösung ist oder nicht, muss im Einzelfall entschieden werden. Die Auseinandersetzung mit der Blockchain-Technologie kann als Inspirationsquelle für die Neugestaltung von Verwaltungsprozessen dienen.

6.4. Nächste Schritte

Zur Realisierung der Mehrwerte, welche die Blockchain-Technologie bietet, kann die Verwaltung erstens Aktivitäten fördern, welche die Grundlagen und Regulierung von Blockchains betreffen:

- Im Rahmen der Erarbeitung der vorliegenden Studie wurde deutlich, dass das in der kantonalen Verwaltung vorhandene Wissen und Erfahrung zur Nutzung der Blockchain noch beschränkt ist und weitgehend privater Initiative zu verdanken ist. Entsprechend soll dieses **Wissen in der Verwaltung gefördert** und mit Hilfsmitteln (wie Leitfäden, Frameworks und Tools) unterstützt werden.

- Es bietet sich auch an, die **Zusammenarbeit** mit Wissenschaft und Privatwirtschaft zu intensivieren, beispielsweise mit dem Blockchain-Zentrum der Universität Zürich. Dabei ist Ansätzen den Vorzug zu schenken, die unterschiedlichen Disziplinen – Natur- und Sozialwissenschaften – und unterschiedliche Technologien – Blockchain, mit künstlicher Intelligenz, Internet of Things usw. – kombinieren.

- Die weitere Steigerung des Reifegrads der Digitalisierung ist aktiv zu verfolgen, da vollständig digitalisierte Prozesse sich am besten für einen Blockchain-Einsatz eignen und weitere Vorteile und neue Möglichkeiten bieten. Es bietet sich an, bei der **Geschäftsprozessanalyse** systematisch die Möglichkeiten der Blockchain-Technologie zu prüfen.

- Es sind rechtliche Grundlagen zu schaffen, die den Einsatz der Technologie möglich machen. Im Rahmen von **Pilotprojekten,** in denen spezifische Aspekte der Umsetzung beschrieben werden, können die Datenschutzbeauftragte und das Staatsarchiv prüfen, inwieweit die von ihnen verantworteten Belange erfüllt werden.

- Darüber hinaus ist eine Beteiligung an der Erarbeitung von **Standards** für Blockchain-Infrastrukturen und Smart Contracts ins Auge zu fassen.

Zweitens kann die Verwaltung mit der zielgerichteten Anwendung der Blockchain-Technologie deren Weiterentwicklung fördern. Hierzu ist zu prüfen, ob:

- Im Sinne von baldigem Gewinn an Erfahrung die Beteiligung an bestehenden Piloten und Prototypen hilfreich/nützlich ist, beispielsweise dem **Cardossier.**

- Für einen eigenen Anwendungsfall und im Sinne von zeitnahem Lernen anhand konkreter Anwendung könnte ein Pilotprojekt, wie die **Registrierung von amtlichen Dokumenten auf einer Blockchain**, ins Auge gefasst werden (siehe dazu Kapitel 4.1). Der Vorteil dieses Anwendungsbereichs ist, dass hier auf die Erfahrungen, die dazu in den Kantonen Genf (Kapitel 3.1) und Schaffhausen (Kapitel 3.3) gemacht wurden, zurückgegriffen werden kann. Eine Zusammenarbeit mit anderen Kantonen ist zu prüfen, auch, um idealerweise eine Lösung zu entwickeln, die schweizweit eingesetzt werden kann. Als Zürcher Innovation bietet sich an, die Überprüfbarkeit der amtlichen Dokumente nicht auf die digitale Version zu beschränken, sondern Papierdokumente mit einem QR-Code zu versehen, der mit dem Smartphone gescannt werden kann, wodurch die Echtheit des **Papierdokuments** überprüfbar wird.

7. Weiterführende Literatur

- Allessie, David & Sobolewski, Maciej & Vaccari, Lorenzino & Pignatelli, Francesco (2019), Blockchain for digital government. An assessment of pioneering implementations in public services, Luxembourg, Publications Office of the European Union, Link.
  Aktuelle, ausgewogene Studie zu Blockchain-Anwendungen im öffentlichen Sektor. Hervorzuheben sind die systematischen, ausführlichen Beschreibungen von konkreten Beispielen.

- Anthamatten, Jennifer & Lago, Pascal (2019), Blockchain nach dem Hype, Avenir Suisse, Link.
  Guter Überblick zur Blockchain-Landschaft der Schweiz, einschliesslich einiger Handlungsempfehlungen. Anwendungen im Bereich der öffentlichen Verwaltung stehen nicht im Vordergrund.

- Antonopoulus, Andreas M. (2017), Mastering Bitcoin. Programming the open blockchain. O'Reilly.
  Standardwerk über Bitcoin; Programmierkenntnisse vorausgesetzt.

- Berryhill, Jamie & Bourgery, Théo & Hanson, Angela (2018), Blockchains unchained: Blockchain technology and its use in the public sector, OECD Working Papers on Public Governance No. 28, Link.
  Prägnante Einführung in die Blockchain-Technologie und deren grundsätzliche Bedeutung für die öffentliche Verwaltung. Hervorzuheben sind die acht Anwendungsbeispiele.

- Casey, Michael & Vigna, Paul (2015), Cryptocurrency. Wie digitales Geld unser Finanzsystem ins Wanken bringt, Econ.
  Umfassende Einführung zu Blockchain und Geldtheorien; besonders lesenswert die Beschreibung der Umstände, die zur Erfindung von Bitcoin geführt haben.

- [Deutsches] Bundesministerium für Wirtschaft und Energie, Bundesministerium der Finanzen (2019), Blockchain-Strategie der Bundesregierung: Wir stellen die Weichen für die Token-Ökonomie, Link.
  Einführung in die Blockchain-Technologie und Token-Ökonomie, Darstellung der Prinzipien, die der Strategie zugrunde liegen, sowie Formulierung der Strategie, einschliesslich konkreter Massnahmen und Verantwortlichkeiten.

- Nakamoto, Satoshi (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, Link.
  Das White-Paper, das Bitcoin ankündet. Bis heute ist die Autorenschaft ungeklärt.

- Narayanan, Arvind & Clark, Jeremy (2017), Bitcoin's Academic Pedigree, acmqueue, Volume 15, Issue 4, Link.
  Überblick über die (akademischen) Vorarbeiten, auf denen Bitcoin basiert. Erlaubt, die damit verbundenen Innovationen in einem breiteren Kontext zu sehen.

- Schwabe, Gerhard (2019), The role of public agencies in blockchain consortia: Learning from the Cardossier, Information Polity, 24(4), p. 437–451, Link.
  Anhand des Projekts Cardossier diskutiert der Artikel die Rolle, die staatliche Organisationen bei Blockchain-Konsortien spielen kann und soll.

- Talinn-Deklaration on eGovernment (2017), Ministerial Meeting during Estonian Presidency of the Council of the European Union, Link.
  Dokument, das die für die EU relevanten Prinzipien im Bereich E-Government festlegt. Die Schweiz ist ebenfalls Signatarstaat.

- Walport, Mark (2016), Distributed Ledger Technology: Beyond block chain, UK Government Office for Science, Link.
  Eine der ersten ausführlichen Studien zum Thema Blockchain, insbesondere mit Blick auf den öffentlichen Sektor.

- Welzel, Christian & Eckert, Klaus-Peter & Kirstein, Fabian & Jacumeit, Voker (2017), Mythos Blockchain: Herausforderungen für den öffentlichen Sektor, Kompetenzzentrum Öffentliche IT, Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS, Link.
  Allgemeine Einführung in das Thema Blockchain, mit besonderem Schwerpunkt auf der öffentlichen Verwaltung.

- World Economic Forum (2020), Inclusive Deployment of Blockchain: Case Studies and Learnings from the United Arab Emirates, Link.
  Darstellung des Blockchain-Ökosystems der Vereinigten Arabischen Emirate, einschliesslich Anwendungsbeispielen aus dem privaten und öffentlichen Sektor.

- Wüst, Karl & Gervais, Arthur (2018), Do you need a Blockchain? Crypto Valley Conference on Blockchain Technology, Link.
  Systematische Argumentation, in welchen Fällen die Anwendung von Blockchains Sinn macht.

(Zum Zeitpunkt der Publikation dieser Studie wurden alle Links erfolgreich überprüft.)