Einsatz von Blockchain im Genehmigungswesen

Am Bayerischen Staatsministerium für
Umwelt und Verbraucherschutz

eingereichter

Projektbericht zur durchgeführten Machbarkeitsstudie

Autoren:	Tobias Fertig	tobias.fertig@h-d-gmbh.de
	Andreas Schütz	andreas.schuetz@h-d-gmbh.de
	Peter Niehues	peter.niehues@govdigital.de
	Marc Behrens	marc.behrens@kdo.de
	Michael Schmitt	michael.schmitt@regioit.de

Auftragnehmer: govdigital
Abgabedatum: 21.08.2023

Inhaltsverzeichnis

1 Einführung

1.1 Motivation

Gemäß der zugrundeliegenden Leistungsbeschreibung steht der Freistaat Bayern vor gravierenden Veränderungen. Ob es um ehrgeizige Ziele im Bereich Klimaschutz und nachhaltige Wirtschaft geht oder um den Einfluss des Trends zur Digitalisierung – sämtliche gesellschaftlichen Akteure sehen sich enormen Herausforderungen gegenüber. Diese Herausforderungen können oft bestehende Paradigmen grundlegend in Frage stellen. Die ehrgeizige Umgestaltung der Wirtschaft hin zu einer treibhausgasneutralen und nachhaltigen Zukunft ist dabei keineswegs allein eine technologische Hürde. Vielmehr hängt der Erfolg der Umsetzung maßgeblich von den Rahmenbedingungen ab.

Die Beschleunigung von Genehmigungsprozessen steht dabei speziell im Kontext des Umweltpakets im Fokus des bayerischen Staatsministeriums für Umwelt und Verbraucherschutz. Dabei soll auch die Digitalisierung voran getrieben werden, um speziell das Bundes-Immissionsschutzgesetz (BImSchG) zu unterstützen. Hierbei setzen sich nicht nur Behörden sondern auch Vertreter der bayerischen und deutschen Industrie besonders dafür ein.

1.2 Zielsetzung

Um die Einsatzmöglichkeiten der Blockchain-Technologie im Anwendungsbereich der Genehmigungsprozesse zu untersuchen, wird diese Machbarkeitsstudie durchgeführt. Teil dieser Studie ist die Erstellung eines technischen Konzepts und basierend darauf eines technischen Demonstrators für die Digitalisierung von Genehmigungsverfahren. Dabei sollen insbesondere Genehmigungsverfahren nach dem BImSchG – sowohl Neu- als auch Änderungsgenehmigungen und Anzeigen – untersucht werden. Die Untersuchung soll bei einer repräsentativen Auswahl der insgesamt 96 Kreisverwaltungsbehörden (KVB) stattfinden. Die Machbarkeitsstudie, inklusive Konzept und Demonstrator, wird in Zusammenarbeit mit dem Verband der Chemischen Industrie e.V., Landesverband Bayern (VCI-LV Bayern), bzw. interessierten Mitgliedsunternehmen durchgeführt.

In der Beziehung zwischen Staat und Wirtschaft ist die Bedeutung von Zulassungsprozessen, sei es für Infrastruktur- oder Industrieprojekte, von zentraler Bedeutung für eine schnelle Umsetzung. Denn die Dauer, Effizienz und Rechtsklarheit solcher Genehmigungsverfahren spielen eine immer wichtigere Rolle im internationalen Standortwettbewerb bei Investitionsentscheidungen – sie sind ein entscheidender Standortfaktor. Zudem wird die Anzahl solcher Verfahren in den kommenden Jahren stark zunehmen, da die Wirtschaft unter hohem Transformationsdruck steht und sowohl gesellschaftliche als auch politische Veränderungen am industriellen Anlagenpark und der Infrastruktur erwünscht sind.

Daraus ergeben sich die folgenden strategischen Ziele für diese Machbarkeitsstudie:

- Förderung des Wirtschaftsstandorts Bayern durch Digitalisierung von Genehmigungsprozessen
- Stärkung Bayerns als führendes Land im Bereich der Blockchain-Technologie
- Durchgängige Digitalisierung von Verwaltungsprozessen von Betrieben der Bayerischen Industrie bis zum Verwaltungsvollzug in den KVB mit redundanter Datenhaltung bei allen beteiligten Einrichtungen.

Die folgenden Forschungsfragen in müssen dieser Machbarkeitsstudie beantwortet werden, um diese strategischen Ziele zu erreichen:

F1) Wie kann die Blockchain-Technologie für eine langfristige, rechtsverbindliche und vertrauliche Speicherung des Genehmigungsprozesses einer Industrieanlage genutzt werden?

F2) Wie können Betriebsgeheimnisse trotz der Transparenz der Blockchain-Technologie bei Genehmigungsprozessen geschützt werden?

F3) Welchen Mehrwert bietet die Blockchain-Technologie bei Genehmigungsprozessen gegenüber herkömmlichen Software-Lösungen?

1.3 Struktur des Projektberichts

Dieser Bericht beginnt mit der Vorstellung der Stakeholder im zweiten Kapitel. Hier werden sowohl Auftraggeber als auch -nehmer und betroffene Partner berücksichtigt. Sofern bekannt, werden hier ebenfalls die Gründe aufgezeigt, weshalb der jeweilige Stakeholder beteiligt ist. Anschließend werden die technischen Grundlagen erläutert. Im Rahmen des Projekts erfolgte bereits eine umfassende Einführung zur Blockchain-Technologie in Form eines Fachvortrags. Die Grundlagen stellen daher nur eine Zusammenfassung des Themas dar.

Im vierten Kapitel wird die angewandte Methodik vorgestellt, um transparent zu zeigen, wie das Konzept erstellt wurde. Die Anforderungsanalyse beschäftigt sich zunächst mit der Ermittlung der IST-Zustände und leitet anschließend daraus die Anforderungen ab. Dabei werden sowohl die Anforderungen der Behörden als auch der Industriepartner berücksichtigt. Dieser Bericht konzentriert sich auf die für diesen Anwendungsfall spezifischen Anforderungen und greift keine Anforderungen auf, die übliche Best Practices der Software-Entwicklung abbilden.

Im Anschluss wird das Konzept des Blockchain-basierten Ansatzes vorgestellt. Hier werden zunächst die verschiedenen technischen Aspekte beschrieben. Das Kapitel endet mit einer Übersicht über verschiedene Abläufe und Interaktionen mit Smart Contracts. Für den Vergleich mit dem IST-Zustand und herkömmlichen Software-Systemen wird eine Bewertungsmatrix vor-

gestellt, in der die Kompatibilität der unterschiedlichen Anforderungen mit Punkten bewertet wird. Alle Bepunktungen werden zudem erläutert und begründet.

In der Diskussion werden die definierten Forschungsfragen beantwortet. Abschließend gibt das Konzept Ausblick auf zukünftige Arbeiten.

2 Vorstellung der Stakeholder

Im Projekt sind Stakeholder aus verschiedenen Interessengruppen involviert. Hierbei handelt es sich sowohl um Branchenvertreter, als auch um politische Vertreter. Alle Stakeholder sind an der Arbeitsgruppe Blockchain im Genehmigungswesen und waren an der zugrundeliegenden Leistungsbeschreibung beteiligt.

2.1 Bayerisches Staatsministerium für Digitales (StMD)

Das Bayerisches Staatsministerium für Digitales (StMD) wurde im Jahr 2018 gegründet und ist für digitale Angelegenheiten in Bayern zuständig. Es gehört zu der Landesregierung Bayerns und hat seinen Sitz in München. Hier kümmert sich das Ministerium um Grundsatzangelegenheiten, Strategie und Koordinierung der Digitalisierung im Freistaat Bayern. Das Ministerium besteht aus den vier Abteilungen Zentrale Angelegenheiten und Recht, Digitale Transformation und Audiovisuelle Medien, Digitale Verwaltung und IT-Strategie sowie IT-Recht, Digitale Koordinierung und Ministerrat.

2.2 Bayerisches Staatsministerium für Umwelt und Verbraucherschutz (StMUV)

Das Bayerisches Staatsministerium für Umwelt und Verbraucherschutz (StMUV) gehört zur Landesregierung Bayerns und hat seinen Sitz in München. Das Ministerium hat die Aufgabe, die Umwelt-, Natur- und Klimaschutzpolitik in Bayern zu gestalten und umzusetzen. Es entwickelt Strategien, Konzepte und Maßnahmen zur nachhaltigen Nutzung und Erhaltung der natürlichen Ressourcen in Bayern. Dazu gehören der Schutz der Gewässer, die Förderung erneuerbarer Energien, die Reduzierung von Treibhausgasemissionen und die Erhaltung der biologischen Vielfalt. Im Bereich Verbraucherschutz setzt sich das Ministerium für die Sicherheit von Lebensmitteln und Produkten ein und informiert die Öffentlichkeit über Verbraucherfragen. Eine weitere Aufgabe ist die Zusammenarbeit innerhalb der Europäischen Union und international. Auf Landesebene arbeitet das StMUV eng mit anderen Ministerien und Institutionen zusammen, um eine koordinierte Politik und Maßnahmen zur Förderung einer nachhaltigen Entwicklung und des Verbraucherschutzes zu gewährleisten.

2.3 Bayerisches Landesamt für Umwelt (LfU)

Das Bayerische Landesamt für Umwelt (LfU) ist die zentrale Umweltfachbehörde in Bayern, welche Umweltdaten erfasst und bewertet, um den Zustand der Umwelt in Bayern zu analysieren und diese Informationen Behörden, Kommunen, Politik, Wirtschaft, Wissenschaft und der Öffentlichkeit zur Verfügung zu stellen. Weitere Tätigkeiten des LfUs umfassen die Beratung sowie die Erstellung von Arbeitshilfen und Merkblättern im Rahmen der Fach- und

Vollzugsaufgaben. Zudem organisiert es Fachtagungen und ist in nationalen und internationalen Gremien tätig. Die Aufgabenbereiche des LfUs umfassen Naturschutz und Landschaftspflege, Klimaschutz, Abfallentsorgung, Immissionsschutz, Wasserversorgung, Gewässerschutz und Gewässerkunde, Geologie, Geophysik, Geochemie und Bodenkunde sowie die Energiewende. Das LfU ist eine Behörde im Geschäftsbereich des StMUV und diesem unmittelbar nachgeordnet. Im Bereich Energiewende untersteht es der Fachaufsicht des Bayerischen Staatsministeriums für Wirtschaft, Landesentwicklung und Energie. Am LfU sind rund 1.100 Mitarbeitende an zehn Dienststellen beschäftigt. Der Hauptsitz befindet sich in Augsburg.

2.4 Regierung Oberfranken

Die Regierung von Oberfranken ist eine staatliche Behörde und eine von sieben Regierungsbezirken in Bayern. Sie hat ihren Sitz in Bayreuth und ist für die Verwaltungsaufgaben in der Region Oberfranken zuständig. Die Regierung von Oberfranken nimmt verschiedene Aufgaben wahr, darunter die Umsetzung und Durchsetzung von Gesetzen und Verordnungen auf Landesebene in ihrem Zuständigkeitsbereich. Sie ist eine Mittelbehörde zwischen der bayerischen Landesregierung und den Landkreisen sowie kreisfreien Städten in Oberfranken. Zu den Aufgaben der Regierung von Oberfranken gehört die Gewährleistung einer effizienten Verwaltung in verschiedenen Bereichen, wie beispielsweise im Bauwesen, Umweltschutz, Gesundheitswesen, Landwirtschaft, Bildung und Kultur. Sie überwacht die Einhaltung von Vorschriften und Gesetzen, fördert die regionale Entwicklung und stellt sicher, dass staatliche Leistungen und Dienstleistungen den Bürgerinnen und Bürgern in Oberfranken zugutekommen.

2.5 Verband der chemischen Industrie e.V. (VCI)

Der Verband der chemischen Industrie e.V. (VCI) und seine Fachverbände vertreten die Interessen von rund 1.900 Unternehmen aus der chemisch-pharmazeutischen Industrie und chemienaher Wirtschaftszweige gegenüber der Politik, Behörden, anderen Bereichen der Wirtschaft, der Wissenschaft und den Medien. Der Verband nimmt eine Schlüsselrolle ein, wenn es darum geht, die Belange der Mitgliedsunternehmen zu vertreten, den Dialog zwischen Industrie, Politik und Gesellschaft zu fördern sowie günstige Rahmenbedingungen für die chemische Industrie zu schaffen.

Im Zentrum der Arbeit des VCIs steht die Förderung einer nachhaltigen und wettbewerbsfähigen Entwicklung der Branche. Dazu zählt die Unterstützung von Innovationen, die Stärkung der internationalen Wettbewerbsfähigkeit des deutschen Industriestandorts für Chemieunternehmen sowie – im Rahmen der Initiativen Responsible Care und Chemie3 – die Verankerung von Nachhaltigkeit als Leitbild in der Branche. Der VCI vereint in seinen Reihen sowohl große Chemieunternehmen als auch kleine und mittelständische Firmen. Durch enge Zusammenarbeit u.a. mit anderen Industrieverbänden, Wissenschaftseinrichtungen und Regierungsbehörden setzt sich der Verband für die Interessen der chemischen Industrie ein und gestaltet aktiv die

Rahmenbedingungen der Branche mit. Eine Besonderheit in der Struktur des VCIs ist die Organisation über verschiedene Landesverbände. Der Verband der Chemischen Industrie e.V., Landesverband Bayern (VCI-LV Bayern) bündelt und vertritt dabei die wirtschaftspolitischen Interessen der VCI-Mitgliedsfirmen mit Standorten im Freistaat. Der Wirtschaftsverband der bayerischen chemischen Industrie vertritt ca. 270 Mitgliedsfirmen.

2.6 BASF SE

Die BASF SE gilt als eines der größten Chemieunternehmen der Welt. Es wurde im Jahr 1865 gegründet und hat seinen Hauptsitz in Ludwigshafen, Deutschland. BASF ist in verschiedenen Bereichen tätig, darunter Chemikalien, Kunststoffe, Veredelungsprodukte, Pflanzenschutzmittel, Öl und Gas. Diese Bereiche spiegeln sich ist in den unterschiedlichen Segmenten des Unternehmens wieder: „Chemicals", „Materials", „Industrial Solutions", „Surface Technologies", „Nutrition & Care" und „Agricultural Solutions". BASF produziert eine breite Palette von chemischen Produkten, die in zahlreichen Industriezweigen Anwendung finden, wie zum Beispiel in der Automobilindustrie, im Bauwesen, in der Elektronik, in der Landwirtschaft und in der Verpackungsindustrie. Neben einem starken Fokus auf Forschung und Entwicklung, engagiert sich BASF auch für Nachhaltigkeit und strebt an mit den eigenen Lösungen die Umweltbelastung zu reduzieren und Ressourcen effizienter zu nutzen.

BASF ist international tätig und hat Produktionsstandorte, Forschungseinrichtungen und Vertriebsgesellschaften in vielen Ländern weltweit. Das Unternehmen beschäftigt 2022 111.481 Mitarbeitende und erwirtschaftet einen Umsatz von 87,3 Milliarden Euro.

2.7 Wacker Chemie AG

Die Wacker Chemie AG ist ein deutsches Chemieunternehmen mit Hauptsitz in München. Es wurde im Jahr 1914 gegründet und zählt zu den führenden Herstellern von chemischen Produkten weltweit. Das Unternehmen ist in verschiedenen Geschäftsfeldern aufgeteilt: darunter Silicones, Polymers, Biosolutions und Polysilicon. Im Bereich Silicones werden Produkten auf Basis von Silicium hergestellt. Die Produkte werden dabei in zahlreichen Anwendungen eingesetzt, wie z.B. in der Bauindustrie, der Elektronik, der Automobilbranche und in der Solarindustrie. Darüber hinaus ist Wacker Chemie in der Herstellung von Polymeren auf Basis von Ethylen, insbesondere von Dispersionspulvern und Dispersionen, aktiv. Diese werden in der Bauindustrie, der Farben- und Lackindustrie, der Textilindustrie und vielen anderen Bereichen verwendet. Im Bereich Biosolutions entwickelt Wacker Chemie biotechnologische Lösungen, die in der Pharmazie, der Lebensmittelindustrie und der Landwirtschaft Anwendung finden. Hierzu zählen z.B. zellkulturbasierte Produkte, Cyclodextrine und bioaktive Peptide. Ein weiteres wichtiges Geschäftsfeld von Wacker Chemie ist die Produktion von polykristallinem Silizium, das für die Herstellung von Solarzellen verwendet wird. Das Unternehmen ist einer der weltweit

größten Hersteller von hochreinem polykristiallinen Silizium und bedient damit die Nachfrage der Solarindustrie.

Die Wacker Chemie AG ist international tätig und betreibt 27 Produktionsstandorte und 52 Vertriebsbüros weltweit. Das Unternehmen beschäftigt 15.700 Mitarbeitende und erwirtschaftete 2022 einen Jahresumsatz von 8,21 Milliarden Euro.

2.8 Evonik Industries AG

Die Evonik Industries AG ist ein Essener Chemieunternehmen. Das Unternehmen wurde im Jahr 2007 gegründet und entstand aus dem Zusammenschluss des Essener Teils der RAG (Ruhrkohle AG) mit dem Chemiekonzern Degussa. Das Unternehmen ist in verschiedenen Geschäftsbereichen tätig und bietet Spezialchemikalien, Hochleistungsmaterialien und Additiven an. Zu den Hauptgeschäftsfeldern gehören Specialty Additives, Nutrition & Care, Smart Materials, Performance Materials und Services. Die Kunden kommen aus der Automobilindustrie, Bauindustrie, Energiebranche, Kosmetikindustrie, Lebensmittel- und Tierfutterindustrie sowie die Pharmazie. Im Bereich Specialty Additives stellt das Unternehmen Additive und Vernetzer her, die die Widerstandsfähigkeit von Oberflächen erhöhen. Im Bereich Nutrition & Care produziert Evonik Inhaltsstoffe für Lebensmittel, Tiernahrung, pharmazeutische Anwendungen und Körperpflegeprodukte. Das Geschäftsfeld Smart Materials umfasst verschiedene Produkte und Lösungen, wie Wasserstoffperoxid oder Mono-Siliane. Der Bereich Performance Materials stellt Hochleistungskunststoffe, Polymerwerkstoffe und Spezialadditive her, die in verschiedenen Industriebereichen eingesetzt werden. Zusätzlich bietet die Evonik Industries AG auch eine breite Palette an technischen Services an. Hierzu zählen Analytics, Engineering-Dienstleistungen, technische Beratung und Anwendungsentwicklung.

Das weltweit agierende Unternehmen beschäftigte 2021 33.004 Mitarbeitende und erwirtschaftete einen Umsatz von 15 Milliarden Euro.

2.9 Govdigital

Die govdigital eG ist eine Genossenschaft, die im Dezember 2019 gegründet wurde, um innovative IT-Lösungen im öffentlichen Sektor zu integrieren. Ihre Kernkompetenz liegt in der gemeinsamen Entwicklung, Umsetzung und dem partnerschaftlichen Betrieb von IT-Lösungen, insbesondere rechenzentrumsübergreifenden und cloud-basierten Infrastrukturen wie Blockchain. Ihr Ziel ist es, neue Technologien auf Basis digitaler Infrastrukturen in der öffentlichen Hand zu fördern und mit anderen Gebietskörperschaften zu teilen. Die govdigital agiert als Plattform für den Austausch und die Entwicklung von innovativen IT-Technologien im öffentlichen Sektor und ihre Mitglieder bestehen ausschließlich aus Einheiten der öffentlichen Verwaltung und öffentlichen Unternehmen, die Dienstleistungen für den Public Sektor anbieten. Seit dem

zweiten Quartal 2022 betreibt govdigital eine eigene Blockchain-Infrastruktur auf Basis des Open-Source-Projekts Hyperledger.

3 Technische Grundlagen

3.1 Blockchain

Blockchain ist erstmalig 2009 als realisierende Technologie der Kryptowährung Bitcoin in Erscheinung getreten. Durch das Lösen der Zentralisierung-, Vertrauens- und Double-Spending-Problematik des Internets konnte mit ihr zum ersten Mal eine digitale Peer-to-Peer Währung ohne zentrale Kontrollinstanz implementiert werden (Fertig & Schütz, 2019). Je nach Publikation wird die Blockchain als Datenbank, Protokoll, Logfile, Datenstruktur oder Ledger bezeichnet, verbunden mit den Charakteristiken des verteilten oder dezentralen Aufbaus (Schlatt et al., 2016). Es ist jedoch sinnvoll bei der Betrachtung der Blockchain-Technologie zwischen zwei grundlegenden Komponenten zu differenzieren. Diese sind die Datenstruktur Blockchain und das Blockchain-System, über das die Verwaltung der Datenstruktur ermöglicht wird. Ein Blockchain-System besteht aus vielen verteilten Servern (genannt Knoten), die in einem Netzwerk zusammengeschlossen sind. Jeder Knoten des Netzwerks besitzt und verwaltet eine Kopie der Datenstruktur Blockchain. Diese redundante Speicherung ist ein wesentliches Sicherheitsmerkmal der Blockchain-Technologie. So kann trotz eines Ausfalls oder einer Manipulation von einzelnen Knoten die Integrität und Verfügbarkeit der Daten durch das Netzwerk sichergestellt werden. Das Netzwerk sorgt insbesondere dafür, dass die einzelnen Kopien der Datenstrukturen aktuell gehalten werden. Außerdem werden Schreiboperationen von neuen Datensätzen in die Blockchain vom Netzwerk auf ihre Gültigkeit geprüft. Diese Aufgabe wird als Konsensfindung bezeichnet. Schreiboperationen, wie bspw. die Transaktion von Einheiten einer Kryptowährung, dürfen nur von berechtigten Entitäten durchgeführt werden.

Die in der Blockchain gespeicherten Daten (Transaktionen, Datensätze oder Ereignisse) werden in Datenpaketen (Blöcken) bestimmter Größe gespeichert. Ein Block wird von einem Teilnehmer im Netzwerk konstruiert und dann an die anderen Netzwerkteilnehmer propagiert. Diese fügen den Block nach einer Überprüfung ihrer Kopie der Datenstruktur Blockchain zu. Die Blöcke sind miteinander verkettet, woher auch der Name Blockchain rührt. Jeder Block beinhaltet hierfür einen Hashwert des jeweiligen Vorgängerblocks. Dadurch baut ein beliebiger Block auf allen seinen Vorgängerblöcken auf. Nachträgliche Änderungen im einem Block werden bei einer Überprüfung dadurch schnell sichtbar. Netzwerkteilnehmer werden in einem Blockchain-System durch Adressen repräsentiert und authentisieren sich durch asymmetrische Kryptografieverfahren (Private und Public Key). Besonders der Private Key ist eine wichtige Instanz in der Blockchain. Mit dem Private Key können Adressinhaber ihre Schreiboperationen digital signieren. Mit dem Public Key können die anderen Netzwerkteilnehmer die Authentizität dieser Signatur überprüfen.

Die ursprüngliche Bitcoin-Blockchain ist als öffentliche (Public) Blockchain konzipiert. Jede Person mit Zugang zum Internet kann die in der Blockchain gespeicherten Daten einsehen

oder Transaktionen versenden. So kann ermöglicht werden, dass auch jede Person am Netzwerk teilnehmen kann, indem beispielsweise mit dem eigenen Rechner Transaktionen gesendet werden. Dieser Open-Source-Charakter unterstützt die dezentrale Verteilung und damit auch Sicherheit des Blockchain-Systems. Bei einer nicht-öffentlichen (Private) Blockchain können nur festgelegte Personen die Daten der Blockchain lesen und am Netzwerk teilnehmen. Diese Variante hat sich vor allem für Organisationen oder Organisationsverbände durchgesetzt, die verhindern wollen, dass sensible Daten durch Dritte eingesehen werden können oder fremde Menschen Transaktionen senden. Neben den beiden beschriebenen Zugriffskriterien können Blockchain-Systeme auch nach Verwaltungskriterien kategorisiert werden. Sie bestimmen, wer an der Konsensfindung im Netzwerk teilhaben darf. Die Bitcoin-Blockchain ist aufgrund ihrer Charakteristik genehmigungsfrei (permissionless). So kann jeder Teilnehmer im Netzwerk an der Verwaltung teilnehmen. Für Firmen haben sich allerdings genehmigungspflichtige (Permissioned) Varianten etabliert. Eine benannte Gruppe von Teilnehmern (Konsortium) hat bei dieser Variante das Recht die Blockchain zu verwalten.

3.2 Smart Contracts

Bei Smart Contracts handelt es sich um digitale Verträge, die in der Form von Computerprotokollen abgebildet werden (Fertig & Schütz, 2019). Die Verträge können von mehreren Parteien über das Internet geschlossen werden und ersetzen so das schriftliche Ausformulieren der Vertragsbedingungen. Die Einhaltung der definierten Bedingungen zur Vertragserfüllung wird automatisiert überprüft, und vereinbarte Leistungen werden automatisiert erfüllt. Dies spart Zeit und Kosten und ermöglicht Maschinen oder Programmen, untereinander Verträge zu schließen, die an verschiedene Bedingungen gekoppelt sind. Seit der Vorstellung der Blockchain haben Smart Contracts auch in diesen verteilten Systemen immer mehr an Bedeutung gewonnen. Die Besonderheiten von Blockchain-Netzwerken sorgen dafür, dass die in Smart Contracts vereinbarten Bedingungen garantiert ausgeführt werden. Voraussetzung ist die Möglichkeit zur transparenten Überprüfung der Bedingungen und eine digitale Leistungserbringung, wie bspw. die Freischaltung digitaler Assets.

Für die Implementierung von Smart Contracts haben sich verschiedene Prinzipien etabliert, die vor allem durch die Vorarbeiten von Szabo (1996) und Grigg (2004) beeinflusst sind. Szabo (1996) beschrieb die fünf Prinzipien Beobachtbarkeit, Überprüfbarkeit, Privity (Mitwirkungswissen) und Durchsetzbarkeit. Das Prinzip der Beobachtbarkeit besagt, dass die beteiligten Parteien die Erfüllung des Vertrags beobachten können müssen. Falls dies nicht möglich ist, sollte zumindest nachweisbar sein, dass bestimmte Handlungen stattgefunden haben. Das Prinzip der Überprüfbarkeit fordert, dass die Bedingungen eines Vertrags überprüfbar sein müssen, um festzustellen, ob sie erfüllt wurden oder nicht. Privity beschreibt, dass Wissen und Kontrolle über die Vertragsinhalte und die Ausführung des Vertrags nur so weit wie notwendig auf die beteiligten Parteien verteilt werden sollten. Beim Prinzip der Durchsetzbarkeit soll die Beteili-

gung der Vertragsparteien an der eigentlichen Durchsetzung des Vertrags möglichst minimiert werden. Stattdessen soll der Vertrag sich weitgehend selbst durchsetzen können. Grigg (2004) beschrieb mit dem Ricardischen Vertrag wie ein Smart Contract in Systeme eingebettet werden könnte. Dabei identifizierten sie folgende Merkmale. Ein Smart Contract erfordert einen Herausgeber, der den Vertrag potenziellen Vertragspartnern zur Verfügung stellt. Der Inhalt des Vertrags sollte ein Recht von bestimmtem Wert sein, das vom Herausgeber des Vertrags verwaltet und an die Vertragspartner weitergegeben wird. Außerdem solle ein Smart Contract für Menschen so einfach lesbar sein, wie ein auf Papier geschriebener Vertrag, jedoch auch von Maschinen gelesen und interpretiert werden können. Es sei ebenfalls wichtig, dass ein Smart Contract digital signiert wird, einen Schlüssel und Serverinformationen enthält und über einen eindeutigen und sicheren Identifier zweifelsfrei identifizierbar ist.

Moderne Smart Contracts zeichnen sich durch ihre dezentrale Verteilung auf zahlreichen Knoten im Blockchain-Netzwerk aus. Sie werden in spezifischen Programmiersprachen implementiert, wobei Smart Contracts auf der Ethereum Blockchain vor allem Solidity verwenden. Jeder Smart Contract definiert präzise Input-Parameter und Ausführungsschritte. Im Wesentlichen stellen dezentrale Smart Contracts eine Art „Wenn-dann"-Beziehung dar oder kombinieren mehrere solcher Beziehungen miteinander.

Die Verwendung von Smart Contracts im Kontext der Blockchain bringt jedoch auch einige Herausforderungen mit sich. Zum einen sind die Implementierungen aktueller Smart Contracts ohne fundierte Vorkenntnisse nicht leicht lesbar. Ein weiteres Problem besteht in der Schnittstelle zur realen Welt, da der Zugriff auf Off-Chain-Ressourcen schwierig ist. Es besteht das Risiko, dass zentrale Schnittstellen für die Übergabe falscher Informationen genutzt werden.

Ein weiteres Hindernis ist die mangelnde Flexibilität. Es gestaltet sich generell schwierig, einen einmal geschlossenen Smart Contract an neue Umstände anzupassen oder aufzulösen. Diese Aspekte müssen bereits während der Entwicklung sorgfältig bedacht werden. Zu den weiteren Herausforderungen gehören die Gefahr von Bugs oder Hacks, die es bei herkömmlichen Verträgen nicht gibt. Die dezentrale Verteilung von Smart Contracts führt auch zu gänzlich neuen Anforderungen hinsichtlich der Anwendbarkeit von Recht und der Bestimmung des Gerichtsstands.

3.3 Solidity und Standards

Solidity[1] gilt derzeit als die führende und am weitesten fortgeschrittene Programmiersprache für Smart Contracts auf der Ethereum-Plattform. Diese objektorientierte Hochsprache wurde speziell für die Entwicklung von Smart Contracts entwickelt. Allerdings hat sich im Englischen zunehmend der Begriff „Contract-oriented Programming Language" etabliert, um ihre Hauptfunktion als Programmiersprache für Smart Contracts zu betonen. Während der Entwicklung

[1] https://soliditylang.org/

von Solidity wurden die Programmiersprachen C++, Python und JavaScript als Vorbilder herangezogen. Besonders die Syntax weist eine starke Ähnlichkeit mit der von JavaScript auf, was es Entwicklern, die bereits Erfahrung mit JavaScript haben, erleichtert, sich schnell mit Solidity vertraut zu machen. Es ist wichtig zu beachten, dass Solidity speziell für die Blockchain- und Smart-Contract-Entwicklung entwickelt wurde und daher bestimmte Eigenschaften und Sicherheitsaspekte aufweist, die es von herkömmlichen Programmiersprachen unterscheiden. Daher sollten Entwickler vor der Programmierung von Smart Contracts mit den spezifischen Merkmalen und Best Practices von Solidity vertraut sein, um potenzielle Sicherheitsrisiken zu minimieren. Solidity befindet sich aktuell in der Version 0.8.21.

Im Laufe der Zeit haben sich einige bedeutende Standards zur Realisierung von Smart Contracts auf der Ethereum-Blockchain mit Solidity entwickelt. Diese Standards werden als Ethereum Request for Comments (ERC)-Standards bezeichnet. Die wichtigsten Standards werden an dieser Stelle vorgestellt.

3.3.1 ERC-20 Token Standard

Der ERC-20 war einer der frühen Standards für Ethereum und soll die Entwicklung von Smart Contracts zur Erschaffung und Verwaltung von Token vereinfachen (Vogelsteller & Buterin, 2015). Der Fokus liegt hierbei auf Token, die sich an den grundlegenden Funktionalitäten von Kryptowährungen orientieren. Diese Tokens werden Fungible Tokens (FTs) genannt, weil sie untereinander gleichwertig und somit austauschbar sind. Der Standard wurde häufig in Initial Coin Offerings (ICOs) verwendet, um den Investoren eine bestimmte Anzahl der Token zur Verfügung zu stellen. Die Tokens fungierten hierbei als Kryptowährung und Anteilsschein zugleich. Der ERC-20 Standard bietet die Möglichkeit für die Tokens die Attribute Name, Kürzel und auch die Anzahl der möglichen Dezimalstehlen zu definieren. Außerdem bietet ein Smart Contract nach ERC-20 die Möglichkeit Tokens an andere Adressen zu transferieren. Die einzelnen Transaktionen werden über den Smart Contract genehmigt. Der Standard beinhaltet in diesem Zusammenhang die Möglichkeit zur Einrichtung einer Erteilung von Vollmachten. Diese Vollmachten werden als Allowances bezeichnet. Mit einer Allowances kann eine Adresse eine bestimmte Anzahl von Tokens im Namen einer anderen Adresse verschicken. Die Anzahl wird mit der Funktion `approve()` definiert.

3.3.2 ERC-721 Non-Fungible Token Standard (NFT)

Der ERC-721 ist ein Standard für Smart Contracts, der die Erstellung und Verwaltung von Assets zu ermöglicht (Entriken et al., 2018). Im Gegensatz zu den meisten Kryptowährungen, die untereinander gleichwertig sind (fungible), repräsentiert jedes ERC-721 Token ein einzigartiges digitales Objekt oder einen digitalen Besitz, beispielsweise digitale Kunstwerke, Sammlerstücke, virtuelle Grundstücke in virtuellen Welten, In-Game-Gegenstände und vieles mehr. Das Ziel ist, die einzigartigen Tokens innerhalb von Smart Contracts verfolgen und transferieren zu können.

Ein Asset soll dabei sowohl digitale als auch physische Werte repräsentieren können. Dadurch, dass kein Asset einem anderen gleicht, muss der Besitzer jedes Assets separat verwaltet werden. Als Synonym für die Assets hat sich der Begriff Non-fungible Token (NFT) etabliert. Der Funktionsumfang des Standards ähnelt dem ERC-20-Standard. Zusätzlich gibt es aber die Möglichkeit eines sicheren Transfers, der die Übertragung an Smart Contracts verhindern soll, die die Assets u. U. nicht verarbeiten können. In diesem Fall findet eine Rücküberweisung statt. Um die Kompatibilität mit dem ERC-20 zu wahren, wird die alte Transferfunktion aber ebenfalls verfügbar gemacht. Die Funktion zur Einrichtung von Vollmachten ist hier ebenfalls verfügbar. Zusätzlich können bei ERC-721 Metadaten, wie etwa Links zu einer Bilddatei, hinterlegt werden.

3.3.3 ERC-1155 Multi Token Standard

Der ERC-1155-Standard ermöglicht die Erstellung und Verwaltung von Multi-Token-Verträgen (Radomski et al., 2018). Smart Contracts werden nach diesem Standard entwickelt, falls der Anwendungsfall die flexible Verwendung verschiedener Arten von Token erfordert. Im Gegensatz zum ERC-721-Standard, der einzelne eindeutige NFTs darstellt, erlaubt der ERC-1155-Standard die Erstellung von mehreren FTs und NFTs innerhalb eines einzigen Smart Contracts. Der ERC-1155 Standard kombiniert die Funktionen der ERC-20 und ERC-721 Standards.

3.4 Wichtige Funktionen in Smart Contracts

3.4.1 Die Mint-Funktion

Die Funktion `mint()` beschreibt eine Methode oder Funktion, die die Erstellung oder Generierung neuer Token in einem Smart Contract ermöglicht. Sie wird in den oben beschriebenen Standards ERC-20, ERC-721 und ERC-1155 verwendet. Das Minten (auf deutsch Prägen) wird verwendet, um die Token-Versorgung zu erhöhen, indem neue Token erstellt und an bestimmte Adressen ausgegeben werden. Diese Funktion wird normalerweise von einem Smart Contract-Betreiber oder einem anderen autorisierten Akteur aufgerufen. Die Funktion ist mit bestimmten Bedingungen und Berechtigungen versehen, um eine unkontrollierte Erzeugung neuer Token zu verhindern. Gemeinsam mit Funktionen wie `burn()` (Verbrennen) oder `transfer()` (Übertragung) ermöglicht sie eine umfassende Verwaltung von Token.

3.4.2 Die Burn-Funktion

Die Funktion `burn()` in Smart Contracts beschreibt auf eine Methode oder Funktion, die dazu dient, bestimmte Token oder eine bestimmte Summe einer Kryptowährung dauerhaft aus dem Umlauf zu entfernen, indem sie zerstört (übersetzt „verbrannt") werden. Das „Burning" von Token ist eine irreversible Aktion. Die betroffenen Tokens können danach nicht mehr verwendet oder transferiert werden. Das Burning ist eine Grundfunktionalität in den bereits beschriebenen

Token-Standards wie ERC-20, ERC-721 oder ERC-1155. Es gibt verschiedene Gründe die Burn-Funktion zu verwenden. Ist an ein Token eine bestimmte Leistung gekoppelt, kann der Abruf der Leistung u. U. an die Zerstörung des Tokens gekoppelt sein. Dies kommt der Funktionalität eines Gutscheins gleich, der eingelöst wird. Weiterhin wird die Zerstörung von Token auch genutzt, um den Wert von Token durch die gestiegene Limitierung zu erhöhen.

3.5 Kryptographie

3.5.1 Asymmetrische Verschlüsselungsverfahren

Asymmetrische Verschlüsselungsverfahren gehören zu den Standards in modernen IT-Landschaften und sind auch ein wichtiger Grundpfeiler der Blockchain-Technologie. Bei asymmetrischen Verschlüsselungsverfahren werden zwei Schlüssel verwendet: ein öffentlicher Schlüssel (Public Key) zum Entschlüsseln einer Nachricht und ein geheimer Schlüssel (Private Key) zum Verschlüsseln der Nachricht. Daher werden asymmetrische Verfahren auch als Public-Key-Verfahren bezeichnet.

Möchte ein Nutzer A über einen sicheren Kanal kommunizieren, muss er sich einen Private Key generieren aus dem wiederum der Public Key abgeleitet wird. Bei dieser Ableitung handelt es sich um eine Einwegfunktion, d.h. mit dem Private Key kann immer der Public Key berechnet werden, aber aus dem Public Key nie der Private Key. Daher darf der Private Key nur dem Eigentümer bekannt sein. Der Public Key wird für alle Kommunikationspartner veröffentlicht. Möchte Kommunikationspartner B nun an Nutzer A eine Nachricht schicken, verwendet er den Public Key von A um die Nachricht vor dem Versenden zu verschlüsseln. Die Nachricht kann anschließend nur mit dem dazugehörigen Private Key von A entschlüsselt werden.

Eine weitere Funktionalität der Verfahren sind digitale Signaturen. Möchte Nutzer A eine Nachricht an Kommunikationspartner B schicken, kann diese wie oben beschrieben wiederum mit dem Public Key von B verschlüsselt werden. Nutzer A kann aber seinen eigenen Private Key nutzen, um die Nachricht zu signieren, um zweifelsfrei die Authentizität des Absenders nachzuweisen. Die Signatur kann von B wiederum mit dem Public Key von A überprüft werden.

Das bekannteste asymmetrisch Verschlüsselungsverfahren ist das RSA-Verfahren (Moriarty et al., 2016). Das Verfahren funktioniert auf Basis der folgenden Tatsache: Zwei Primzahlen können einfach multipliziert werden. Allerdings gibt es keinen effizienten Algorithmus, das Ergebnis wieder in seine ursprünglichen Primfaktoren zu zerlegen. Je größer die Zahl, umso länger benötigt ein Computer, eine solche Zerlegung zu berechnen, obwohl der Multiplikationsaufwand kaum ansteigt.

3.5.2 Kryptografische Hashfunktionen

Mit kryptografischen Hashfunktionen ist es möglich unkompliziert die Integrität von Daten zu überprüfen. Dabei wird der Funktion eine willkürliche Menge an Daten als Eingabeparame-

ter übergeben. Die Funktion transformiert diese Daten in eine Zeichenkette fester Größe, die als Hash bezeichnet wird. Die Größe des Hashes hängt von der jeweiligen Hashfunktion ab. Hashfunktionen sind deterministisch und liefern für gleiche Eingabewerte auch immer den gleichen Hash als Ausgabe. Außerdem sind Hashfunktionen Einwegfunktionen (vgl. asymmetrische Verschlüsselungsverfahren). Eine Besonderheit von kryptografischen Hashfunktionen gegenüber regulären Hashfunktionen ist, dass diese kollisionsresistent sind. Dies bedeutet, dass mit unterschiedlichen Eingabewerten kein gleicher Hashwert als Ausgabe herauskommen soll. Bekannte Beispiele für Hashfunktionen sind der Message-Digest Algorithm 5 (MD5) (Rivest, 1992) oder der Secure Hash Algorithm (SHA) (Hansen & Eastlake 3rd, 2011).

Eine besondere Anwendung von Hashfunktionen sind Checksummen (BSI, 2023). Eine Checksumme (auch als Prüfsumme bezeichnet) ist eine numerische Wertdarstellung, die aus den Daten eines bestimmten Datensatzes oder einer Datei berechnet wird, um deren Integrität und Richtigkeit zu überprüfen. Die Checksumme wird häufig verwendet, um Datenfehler oder Übertragungsfehler zu erkennen, die während der Speicherung oder Übertragung von Daten auftreten können. Die Berechnung der Checksumme erfolgt im Normalfall durch die Anwendung von Hashfunktionen. Die Checksumme bezeichnet den Ergebniswert der Funktion und wird oft als Hexadezimalzahl oder als Reihe von Zahlen und Buchstaben dargestellt. Beim Empfangen oder Zugreifen auf die Daten kann die Checksumme erneut berechnet werden und mit der ursprünglichen Checksumme verglichen werden. Wenn die beiden Checksummen übereinstimmen, deutet dies darauf hin, dass die Daten intakt und unverändert sind. Wenn die Checksummen nicht übereinstimmen, bedeutet dies, dass die Daten beschädigt wurden oder Fehler aufgetreten sind.

4 Angewandte Methodik

Zu Beginn des Projekts fand ein Kickoff-Termin mit allen Stakeholdern statt. Hier wurden die Rahmenbedingungen und Ziele definiert und geklärt. Im Rahmen des Kickoffs wurde beschlossen, dass Stakeholder-Gespräche durchgeführt und eine Blockchain Einführung gegeben werden soll. Die Blockchain Einführung wurde während der Projektlaufzeit durchgeführt und bezweckte allen Stakeholdern ein Grundverständnis für die Technologie mitzugeben. Außerdem waren zusätzlich externe Interessenten eingeladen.

Generell wurde ein agiles Vorgehen für das gesamte Projekt definiert (Cockburn, 2006). Hierbei erfolgen regelmäßige Abstimmungstermine, in denen Zwischenergebnisse präsentiert werden. Das gesammelte Feedback wird danach aufgegriffen und eingearbeitet. Da es schwer ist, regelmäßige Termine mit allen Stakeholdern zu vereinbaren, wurden bilaterale Gespräche geführt. Lediglich die Zwischenpräsentation des Gesamtkonzepts erfolgte in der großen Runde.

Die durchgeführten Stakeholder-Gespräche erfolgten in Form von Experten-Interviews.(Bogner et al., 2009). Die Methodik von Bogner et al. (2009) wurde verkürzt, da die Forschungsfragen und die Interviewpartner bereits definiert sind. Bei der Erstellung des semi-strukturierten Fragebogens wurden sowohl fachliche als auch technische Aspekte berücksichtigt. Die Fragen werden offen formuliert und erlauben spontane Folgefragen, je nach Verlauf des Gesprächs. Alle Gespräche wurden mit Microsoft Teams aufgezeichnet und für die Dauer der Transkription und Analyse gespeichert.

Microsoft Teams besitzt eine integrierte Funktion für die Transkription von Videoaufzeichnungen, welche verwendet wurde, um eine thematische Analyse nach Braun und Clarke (2021) durchzuführen. Diese strukturierte Vorgehensweise erlaubte es Muster und wiederkehrende Themen in einer Vielzahl von Daten zu identifizieren. In dieser Machbarkeitsstudie wird dieses Vorgehen genutzt, um relevante Projekt-spezifische Anforderungen herzuleiten und zu definieren. Da das Ergebnis der Analyse in diesem Bericht dargestellt wird, wird kein eigener Report nach Braun und Clarke (2021) erstellt.

Basierend auf den abgeleiteten Anforderungen wird ein Blockchain-basiertes Konzept erstellt, um die Forschungsfragen dieser Machbarkeitsstudie beantworten zu können. Das Konzept basiert auf etablierten Standards und Best Practices im Rahmen der Smart Contract Entwicklung. Hier gilt es zu bedenken, dass die Standards und Best Practices verglichen mit herkömmlicher Software-Entwicklung noch sehr jung sind und sich deshalb noch ändern können. Das Konzept muss also eine Mechanik zur Aktualisierung der zugrundeliegenden Logik in den Smart Contracts berücksichtigen.

Das entwickelte Konzept wird bei Annahme durch die Stakeholder verwendet, um einen vertikalen Prototypen als Demonstrator zu entwickeln. Der Demonstrator soll zeigen, dass Smart Contracts und Blockchain eingesetzt werden können, um die Anforderungen der Stakeholder

umzusetzen. Ob der gesamte Genehmigungsprozess dann in einem Folgeprojekt digitalisiert wird, lässt sich dann mithilfe dieses Konzepts und des Demonstrators entscheiden.

5 Anforderungsanalyse

In diesem Kapitel wird der IST-Zustand vorgestellt. Dafür wurden die verschiedenen Sichtweisen der Stakeholder mittels semi-strukturierten Interviews erhoben. Anhand der Interviews wurde dann der IST-Zustand analysiert und aufbereitet. Nach der Vorstellung der einzelnen Sichtweisen erfolgt eine Zusammenfassung aller Anforderungen in Tabelle 1. Im Konzept wird dann immer wieder Bezug zu den Anforderungen genommen.

5.1 Beschreibung der IST-Zustände

5.1.1 IST-Zustand aus Sicht der Regierung Oberfranken

Generell erfolgt zunächst ein Vorgespräch zwischen dem Unternehmen, welches plant eine Anlage zu errichten oder abzuändern und der Regierung. In diesem Vorgespräch wird bereits grob geprüft, welche Gutachten und Informationen für den Antrag benötigt werden. Danach kann das Unternehmen den Antrag vorbereiten und die Gutachten organisieren. Sobald die Unterlagen bei der Regierung eingegangen sind und Vollständigkeit festgestellt wurde, beginnen die Fristen. Im Falle einer Änderungsanzeige gilt eine Frist von einem Monat. Wurde bis dahin nicht auf die Anzeige reagiert, gilt diese als angenommen.

Laut der Regierung Oberfranken erfolgt die Antragsstellung größtenteils auf analogem Wege über Papier. In einzelnen Fällen gibt es individuelle Absprachen mit Unternehmen, bei denen eine elektronische Übermittlung der Anträge im PDF-Format erfolgt. Während des Genehmigungsprozesses kann die Regierung weitere Gutachten anfordern und weitere Behörden und Ämter einbinden, je nachdem welche Bereiche die Anlage tangiert. Hier werden die Unterlagen dann entweder elektronisch oder analog verteilt. Ist der Antrag bereits elektronisch eingegangen, können die Dokumente direkt elektronisch weitergegeben werden. Andernfalls muss zuvor ein Scan stattfinden.

Der Genehmigungsbescheid wird in allen Fällen auf Papier gedruckt und gestempelt und unterschrieben. Zusätzlich werden spätestens dann die restlichen Dokumente gedruckt und gestempelt. Ein Exemplar wird dann an den Betreiber der Anlage gesendet und ein Exemplar wird archiviert. Der Betreiber muss dann jederzeit den Genehmigungsbescheid vorweisen können.

5.1.2 IST-Zustand aus Sicht des LfU bezüglich ISA-B

Das LfU betreibt ISA-B als zentrale, behördeninterne Fachanwendung zur Erfassung, Verwaltung und Auswertung von Daten zu immissionsschutzrechtlich relevanten Anlagen in Bayern. Neben der Erfassung der Daten zu Betreibern, Standorten, Anlagen und Anlagenteilen einschließlich deren umweltrechtlicher Einstufung sowie weiterer zugehöriger Fach- und Berichtsdaten können in ISA-B über eine Upload-Funktion zusätzlich anlagenspezifisch auch Genehmigungsdokumente im PDF-Format hinterlegt werden. Dies ist optional und wird bisher eher bei

großen Industrieanlagen genutzt. Zusätzlich werden die Verantwortlichkeiten und Kontaktdaten der Unternehmen hinterlegt.

Sobald eine neue Anlage genehmigt wurde, werden die zugehörigen Informationen in ISA-B eingetragen, was im Normalfall durch die Genehmigungsbehörde geschieht. In den anderen Bundesländern gibt es ähnliche Anlageninformationssysteme, ISA-B wird deshalb ausschließlich in Bayern genutzt. ISA-B wurde auf Basis der LfU-eigenen ADAMAS-Plattform als standardisierte Entwicklungsumgebung umgesetzt und umfasst kein Workflow-Management-System. Das Portal selbst basiert auf Java und AngularJS. Die REST API könnte zusätzliche Schnittstellen zur Verfügung stellen.

5.1.3 IST-Zustand aus Sicht des VCI Verbands

Laut VCI findet aktuell die Antragsstellung und -genehmigung vorwiegend auf Papier statt. Je nach Anlagengröße und Anzahl Ausfertigungen können hier ganze LKW-Ladungen an Papier verschickt werden. Ganze Kopierräume würden bei der Anfertigung der Unterlagen verschlissen.

Der Versand der Papiere nimmt viel Zeit in Anspruch, was durch elektronische oder digitale Lösungen beschleunigt werden könnte. Für kleine und mittlere Unternehmen (KMU) könnten die Kosten über elektronische oder digitale Wege ebenfalls reduziert werden. Das Einlagern vieler Papier-Dokumente benötigt ebenfalls je nach Anlagenmenge größere Räumlichkeiten.

VCI erwähnte vor allem Sicherheitsbedenken bei Verfahren mit Öffentlichkeitsbeteiligung. Bisher wurden die Papier-Anträge ausgelegt und wer diese Einsehen wollte, musste vor Ort vorbei kommen. Würde hier eine digitale Auslage erfolgen, muss sichergestellt werden, dass Betriebsgeheimnisse nicht gefährdet werden.

5.1.4 IST-Zustand aus Sicht der Evonik Industries AG

Evonik bestätigte den Ablauf, den auch die Regierung Oberfranken beschrieben hat. Kopierräume wurden verschlissen, um die Papier-Anträge zu drucken. Anschließend werden die Dokumente von Mitarbeiterenden persönlich zum zuständigen Landratsamt gefahren. Dies liegt an den sensiblen Daten und der erhöhten Sicherheit.

Sobald die gedruckten Unterlagen abgegeben wurden, werden diese ebenfalls auf Vollständigkeit geprüft und danach beginnt die Frist zu laufen. Werden weitere Dokumente oder Gutachten benötigt, können diese angefordert oder nachgereicht werden. Am Ende wird der Genehmigungsbescheid ebenfalls auf Papier gestempelt zugestellt.

Auf Seiten Evonik erfolgt dann eine Digitalisierung: Der Genehmigungsbescheid wird eingescannt und die verordneten Nebenbestimmungen werden in einem eigenen System eingepflegt und verwaltet. Hierfür hat Evonik mehrere Anwälte, die dann regelmäßig prüfen, ob sich Gesetze ändern und Auswirkungen auf die Nebenbestimmungen haben.

5.1.5 IST-Zustand aus Sicht der Wacker Chemie AG

Bei Wacker wird bereits teils eine elektronische Lösung genutzt. Wacker betreibt selbst Datenräume, welche bilateral verwendet werden können. Somit werden immer die benötigten Dokumente in einen bilateralen Datenraum geladen. Zu Beginn eines Antrags ist dies dann der Datenraum zwischen Wacker und dem Landratsamt. Werden zusätzliche Gutachten benötigt, so werden ausschließlich die für das Gutachten relevanten Dokumente in einen neuen bilateralen Datenraum kopiert. Sobald das Gutachten erstellt wurde und ein Zugriff seitens der Gutachter nicht länger relevant ist, wird die Berechtigung wieder entfernt.

Die Behörden können sich die Dokumente herunterladen und bei sich intern ablegen. Wird die Genehmigung erteilt, so wird der Genehmigungsbescheid elektronisch im Datenraum zur Verfügung gestellt. Wacker kann nun bereits mit der Änderung oder dem Bau beginnen. Eine Papier-Ausfertigung wird trotzdem noch postalisch versandt. Laut Aussage von Wacker können jedoch seit der Umstellung auf die elektronische Übermittlung mindestens drei Werktage eingespart werden.

5.1.6 IST-Zustand aus Sicht der BASF SE

BASF hat ebenfalls seit 2019 einen elektronischen Ansatz. Hier wird eine NextCloud auf Seiten des Landratsamts betrieben. BASF kann alle Unterlagen in die Cloud hochladen und sobald dann wieder die Vollständigkeit festgestellt wurde, laufen die Fristen los.

Die PDF Dokumente werden vor dem Ablauf von BASF elektronisch signiert. Dies geschieht mit Hilfe von Adobe Sign. Bei Adobe Sign entsteht während der elektronischen Signatur eine Transaktions-ID - eine Abfolge von Buchstaben und Ziffern. Anhand dieser ID können Dokumente einer Anlage eindeutig zugeordnet werden. Im Genehmigungsbescheid werden dann nicht alle Unterlagen auf Papier gedruckt, sondern lediglich die Transaktions-IDs aufgelistet, auf welche sich der Bescheid bezieht.

Seit 2023 wird der Genehmigungsbescheid ebenfalls rein elektronisch als signiertes PDF versendet. Hier kann also seit diesem Jahr auf Papier komplett verzichtet werden. Der sonst übliche Stempel wird durch die elektronische Signatur abgelöst.

5.2 Herleitung der Anforderungen

In den Gesprächen haben sich unterschiedliche Anforderungen ergeben, die von einem digitalen System berücksichtigt werden sollten. Diese werden hier im Folgenden erklärt und anschließend zusammengefasst.

5.2.1 Anforderungen der Behörden

Die wichtigste Anforderung aus Sicht der Behörden betrifft die Manipulationssicherheit der Dokumente. Deshalb ist hier bisher die Papier-Lösung auch sehr beliebt, da das gestempelte

Papier in zweifacher Ausfertigung als sehr manipulationssicher eingestuft wird. Sollte das Papier auf Seiten der Betreiber manipuliert werden, so ist das Original im Archiv immer noch korrekt. Deshalb bevorzugen die Behörden auch eine Speicherung der Dokumente im Verantwortungsbereich der Behörden. Der Übergang der Dokumente in den Verantwortungsbereich der Behörde muss im elektronischen oder digitalen ähnlich zum Briefkasten-Schlitz funktionieren. Andernfalls könnten elektronische Dokumente nachträglich noch geändert werden.

Da alle Antragsunterlagen sensible Betriebsgeheimnisse beinhalten, ist der Datenschutz ebenfalls von großer Bedeutung für die Behörden. Eine Digitalisierung muss sicherstellen, dass Daten nicht ungewollt abfließen oder von Angreifern extrahiert werden können. Deshalb ist eine strenge Regelung der Zugriffsrechte zu realisieren.

Im Sinne der Dokumentationspflicht sollten alle Inhaltsänderungen, deren Zeitpunkte sowie Zugriffe lückenlos dokumentiert werden. Eine Übersicht über laufende und verstrichene Fristen sollte ebenfalls möglich sein, wenn die Zeitpunkte dokumentiert wurden. Hierbei genügt im Rahmen der Manipulationssicherheit zu wissen, welche Institution welche Änderungen durchgeführt hat. Eine Dokumentation der exakten personenbezogenen Daten muss nicht innerhalb der Blockchain erfolgen, da hier das informationelle Selbstbestimmungsrecht verletzt werden würde.

Ein Zugriff auf die Dokumente muss jederzeit möglich sein. Für die Verfügbarkeit gelten also hohe Anforderungen. Laut Aussage der Behörden darf es nicht so sein, dass erst auf andere Parteien gewartet werden muss, wenn eine Einsicht in Dokumente benötigt wird. Deshalb müssen diese jederzeit im Verantwortungsbereich der Behörden verfügbar und einsehbar sein.

Bezüglich der Prozessoptimierung wäre eine Schnittstelle zu den existierenden Registern, wie bspw. ISA-B wünschenswert. Hier müssen aktuell die Genehmiger manuell alle relevanten Daten eintragen. Ein Datenexport würde hier Zeit und Fehler sparen. Zudem müssten die Daten dann nur noch an einer Stelle gepflegt werden. Viel mehr Spielraum ist laut Behörden nicht am generellen Prozess, da dieser durch das BImSchG vorgegeben wird.

Ein PDF Export der Daten sollte ebenfalls möglich sein, um bei Bedarf den Genehmigungsbescheid auch als Dokument exportieren zu können. Innerhalb des Systems sollten die Daten allerdings strukturiert vorliegen, damit diese automatisiert verarbeitet werden können und auch von anderen Systeme und Schnittstellen verwendet werden können. Trotz aller Anforderungen und Sicherheitsbestimmungen müssen alle Maßnahmen aber zwingend für KMU umsetzbar bleiben. Sollten die Anforderungen zu komplex werden, müssten im Zweifelsfall geeignete Dienstleister eingerichtet werden, welche die nötige Unterstützung für KMU ermöglichen.

5.2.2 Anforderung der Industrie

Die größte Sorge der Industrie-Stakeholder ist die Wahrung der Betriebsgeheimnisse. Gemäß Interviews könnten einfach Diagramme über die Chemikalienflüsse schon ausreichen, um Anlagen zu kopieren. Dies liegt daran, dass die chemischen Prozesse keine neue Wissenschaft sind. Andere Chemiker, die sich mit dem Anlagenbau auskennen, können also einfach über solche Diagramme Anlagen kopieren. Deshalb muss der Schutz der Betriebsgeheimnisse die höchste Priorität darstellen.

Die Industrie weiß, dass Manipulationssicherheit für die Behörden eine große Rolle spielt, würden aber bevorzugen, wenn die Daten und Dokumente in der Verantwortlichkeit der Betreiber bleiben. Die Bedenken, dass Dokumente nicht verfügbar sein könnten, wenn diese im Verantwortungsbereich der Betreiber liegen, wird nicht geteilt. Laut Aussage in den Interviews muss die Verfügbarkeit gewährleistet werden, wenn das Gesetz dies so vorschreibt.

Die Informationssicherheit ist ebenfalls eine der wichtigsten Anforderungen. Von Seiten der Industriepartner gibt es auch Bedenken, dass die eigenen Dokumente ebenfalls abfließen, wenn ein anderer Betreiber Lücken im System hat. Hier wurde eher die Meinung geteilt, dass es besser wäre, jeder Betreiber wäre selbst für die Bereitstellung des Systems und der Dokumente zuständig, so dass im Zweifelsfall nur von einem Betreiber die Daten abfließen. So wäre jeder Betreiber nur von seiner eigenen mangelnden Sorgfalt betroffen. BASF gab allerdings zu bedenken, dass die Dokumente und Daten so oder so bei den Behörden in den Systemen vorliegen werden, da der Dokumentenübergang in deren Verantwortungsbereich sichergestellt werden muss. Somit würden also mehrere Angriffsvektoren entstehen, wenn sowohl Behörden als auch Anlagen-Betreiber eigene Systeme betreiben müssten.

Da die Betriebsgeheimnisse geschützt werden müssen, sind Zugriffberechtigungen auch von sehr großer Bedeutung. Informationen sollten im Idealfall nur für die benötigte Zeit zugänglich sein, so dass ein Gutachter beispielsweise nach Abgabe des Gutachtens keinen weiteren Zugriff mehr erhält. Zudem sollten Daten nur an dem Ort verfügbar sein an dem sie benötigt werden und nicht überall ähnlich dem Lokalitätsprinzip. Da die Betreuung der Zugriffsberechtigungen ebenfalls viel Zeit beansprucht, wäre eine Teilautomatisierung von Vorteil. Sobald bspw. die benötigten Gutachten hochgeladen wurden, können die Zugriffsberechtigungen automatisiert angepasst werden.

Die Dokumentation der Inhaltsänderungen, Zeitpunkte sowie Fristen wäre auch für die Industriepartner von Interesse. So könnte immer nachvollzogen werden, wie es zu den jeweiligen Änderungen kam und wie lange die Fristen aktuell noch laufen. Laut den Industriepartnern müssen personenbezogene Daten allerdings nicht manipulationssicher auf einer Blockchain abgelegt werden. Hier genügen ebenfalls die Informationen über die jeweilige Institution.

Im Sinne der Prozessoptimierung gibt es wenig Spielraum, da der Prozess durch das BImSchG vorgegeben wird. Allerdings wäre eine vollkommen elektronische – und später digitale – Lösung hilfreich, um Arbeitsaufwände und Kosten zu reduzieren und Zeit einzusparen. So wäre ein Management von Nebenbestimmungen wünschenswert, da hier aktuell großer manueller Aufwand ansteht. Die Industriepartner wünschen sich ein System, welches Gesetzesänderungen bis runter auf die Nebenbestimmungen durchreicht. Hier sollten die Betreiber automatisch informiert werden, wenn ein Gesetz bspw. die Grenzwerte einer Anlage betrifft.

Alle Industriepartner haben immer betont wie wichtig die Berücksichtigung von KMU ist. Die großen Konzerne können ohne die Zulieferung durch KMU nicht existieren, weshalb hier besonders auf deren Integration geachtet wird. Deshalb müssen alle Anforderungen und technischen Lösungen immer auch für KMU zugänglich und realisierbar bleiben.

Da nach der Erteilung der Genehmigung auch Bezahlungen fließen, wurde der Vorteil einer automatisierten Zahlung betont. Sollte das System irgendwie an die Buchhaltung gekoppelt werden können, wäre dies wünschenswert. Es bleibt allerdings eine optionale Anforderung.

5.2.3 Zusammenfassung aller Anforderungen

Die zuvor beschriebenen Anforderungen wurden in Tabelle 1 zusammengefasst. Dabei wurden die Pflicht-Anforderungen markiert. Über die ID können die Anforderungen in diesem Dokument verknüpft werden, um genauer darzustellen, an welcher Stelle im Konzept diese berücksichtigt wurden.

Zusammenfasssend lässt sich die Vision der Behörden und Industriepartner als ein vollkommen digitales System, welches den Genehmigungsprozess für Industrieanlagen unterstützt, beschreiben. Hierbei sollen vor allem wiederkehrende Arbeitsschritte und Aufwände reduziert werden. Wichtig war den Industriepartnern vor allem, dass das Endsystem nicht nur ein Datenspeicher für PDFs darstellt, sondern auf strukturierten Daten gearbeitet werden kann. Dies soll langfristig vor allem Schnittstellen ermöglichen und so Aufwände bei der Pflege von Duplikaten in unterschiedlichen Systemen eliminieren. Die Behörden wünschen sich Transparenz im Genehmigungsprozess und eine langfristige, rechtsverbindliche Speicherung aller relevanten Informationen einer Anlage.

Zu den hier abgeleiteten Anforderungen gelten die üblichen Anforderungen an ein Software-Entwicklungsprojekt wie bspw. für die Bereiche Qualitätssicherung und Dokumentation. Zu Gunsten der Klarheit wird in diesem Konzept auf die Wiederholung und Erläuterung von Best-Practices im Rahmen eines Software-Entwicklungsprojekts verzichtet. Sollte dieses Konzept entwickelt werden, werden die zusätzlichen technischen Anforderungen separat ermittelt und berücksichtigt.

Tabelle 1: Übersicht über die gesammelten Anforderungen

ID	Muss	Kurzform	Beschreibung
A1	x	Manipulationssicherheit	Langfristige, rechtsverbindliche, vertrauliche Speicherung des Prozesses einer Anlage
A2	x	Datenschutz	Personenbezogene Daten müssen geschützt werden
A3	x	Reduzierung Verwaltungsaufwand	Papier verursacht viel Logistik und bietet wenig Schnittstellen
A4	x	Nachhaltigkeit	Zur Nachhaltigkeit zählen Dinge wie Stromverbrauch, laufende Kosten etc.
A5	x	Rechtliche Dokumentation	Inhalte, Fristen und Zeitpunkte müssen dokumentiert werden
A6	x	Verfügbarkeit	Der Zugriff auf die Daten und Dokumente muss jederzeit erfolgen können
A7		Schnittstellen	Strukturierte Daten sollten über Schnittstellen an andere Systeme übertragbar sein
A8		PDF Kompatibilität	Für einen Export neuer und alter Daten sollte das PDF Format unterstützt werden
A9	x	KMU Kompatibilität	Die Lösung muss für KMU umsetzbar sein
A10	x	Schutz der Betriebsgeheimnisse	Betriebsgeheimnisse dürfen nicht an Wettbewerber oder Spione geraten
A11		Nebenbestimmungs-Management	Nebenbestimmungen der Genehmigungs-bescheide sollen digital verwaltet werden
A12		Bezahlung	Die Bezahlung soll über das System automatisierbar sein
A13	x	Strukturierte Daten	Strukturierte Daten erleichtern die digitale Verarbeitung und sollten die Grundlage bilden
A14	x	Erweiter- und Wiederverwendbarkeit	Software-Lösungen sollten zukünftig erweiterbar und wiederverwendbar sein, um Kosten zu sparen
A15	x	Transparenz	Um den exakten Fortschritt eines Antrags zu ermitteln, sollten dafür relevante Daten transparent sein

6 Konzept: Blockchain-basierter Ansatz

In diesem Kapitel wird das Konzept und die Blockchain Architektur beschrieben. Zunächst wird ein Überblick zu den einzelnen Komponenten gegeben, welche im Anschluss genauer erklärt werden. Die Komponenten lassen sich in drei Schichten zuordnen, welche der Reihe nach besprochen werden. Zuletzt werden einige Abläufe beschrieben und mit Diagrammen dokumentiert.

6.1 Überblick über die Komponenten

Das Blockchain-basierte Konzept lässt sich in mehrere Komponenten mit unterschiedlichen Verantwortlichkeiten aufteilen. Zusätzlich lassen sich die Komponenten in verschiedene Schichten gruppieren. Abbildung 1 zeigt den Zusammenhang aller Komponenten. Die unterste Schicht basiert auf einer Ethereum-basierten Blockchain mit Smart Contracts. Darüber wird eine Middleware empfohlen, welche zusätzliche Verifizierungs- und Sicherheitsmechanismen beinhaltet. Die Blockchain-Schicht und die Middleware bilden hierbei die Grundlage, auf welche beliebige Endanwendungen aufgesetzt werden können (betr. A14).

Diese Modularisierung erlaubt eine saubere Trennung der Verantwortlichkeiten. Die Blockchain-Schicht übernimmt hierbei keinerlei Businesslogik sondern dokumentiert lediglich alle Informationen, die manipulationssicher aufbewahrt werden müssen (betr. A1, A5). Dies hat den Vorteil, dass die Endanwendung im Laufe der Zeit einfach angepasst und aktualisiert werden kann.

6.2 Blockchain Layer

Bei der Blockchain-Schicht müssen sowohl die Infrastruktur als auch die Smart Contracts betrachtet werden. In den folgenden beiden Unterkapiteln wird beides vorgestellt und eine Empfehlung ausgesprochen.

6.2.1 Infrastruktur

Für die Blockchain-Infrastruktur existieren zahlreiche Implementierungen, aus denen eine Auswahl erfolgen muss. Dabei lässt sich eine Untergruppe ableiten, welche alle Ethereum-basierten Blockchain Infrastrukturen zusammenfasst. In diesem Konzept wird eine Ethereum-basierte Infrastruktur zu grunde gelegt und empfohlen. Dies liegt daran, dass Ethereum die älteste Blockchain-Technologie ist, welche Smart Contracts ermöglicht. Durch die lange Historie von Ethereum existieren unzählige Entwickler-Tools und zusätzlich eine sehr große Entwickler-Community.

Jüngere Blockchain-Technologien sind oftmals spezialisiert für konkrete Anwendungsfälle, was die Wiederverwendbarkeit der Infrastruktur reduziert. Eine Ethereum-basierte Infrastruktur könnte über das Thema der Genehmigungsanträge hinaus weiter verwendet werden. Zudem

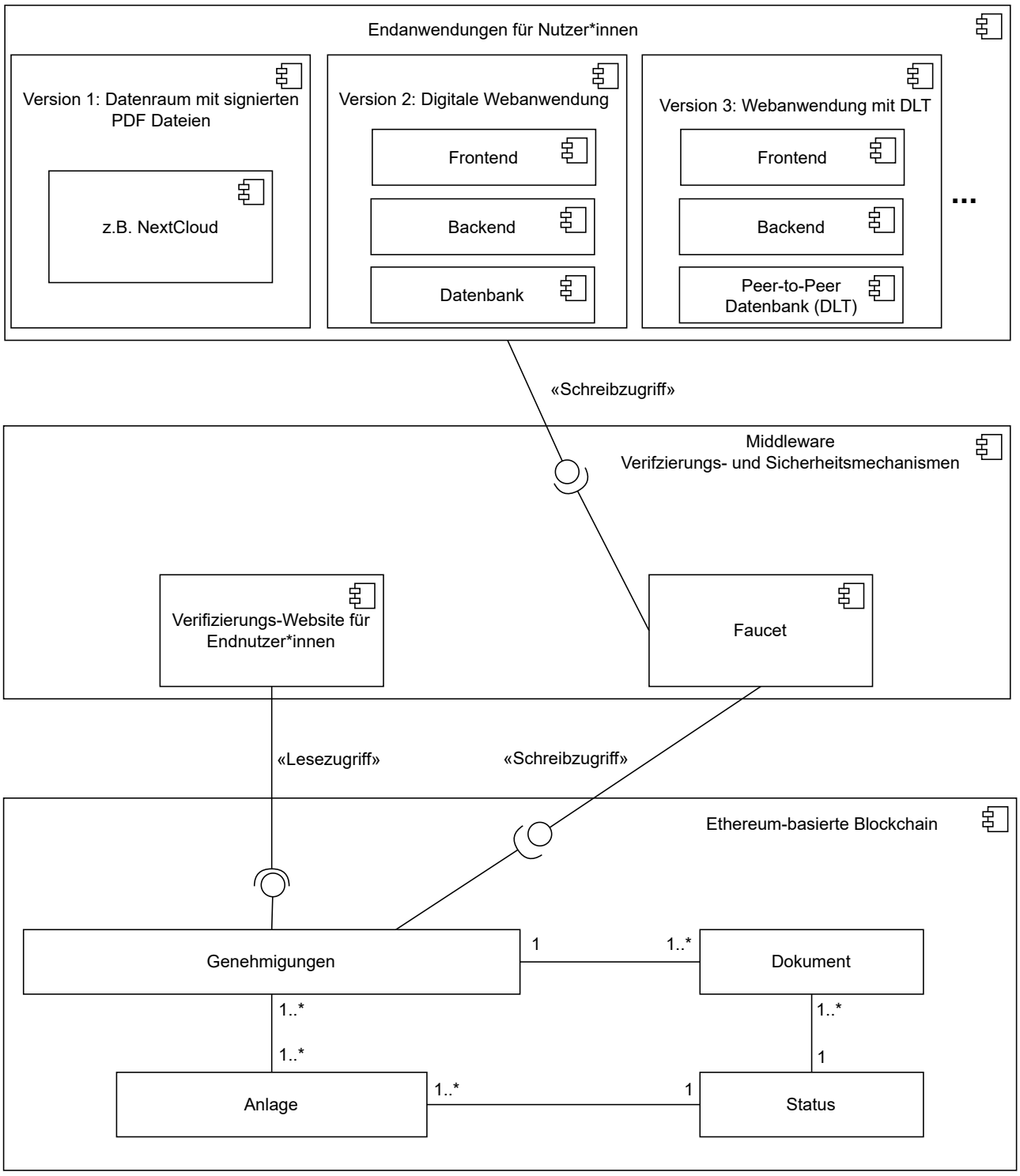

Abbildung 1: UML Komponentendiagram für das Blockchain-basierte Konzept

fällt der häufig zitierte Nachteil Ethereums – die Anzahl Transaktionen pro Sekunde – in einer konsortialen Blockchain weniger ins Gewicht. Dies liegt daran, dass im Fall von public- oder private-permissioned Blockchains andere Konsensmechanismen verwendet werden können, die einen höheren Durchsatz erlauben. Zudem kann bei der Wahl der Konsensmechanismen auch auf nachhaltige Mechanismen zurückgegriffen werden (betr. A4).

Die Nutzung einer Ethereum-basierten Blockchain reduziert ebenfalls die Probleme eines Vendor-Lock-Ins. Da es aktuell viele verschiedene Betreiber von Ethereum Blockchains gibt, wäre ein Wechsel – wenn auch nicht trivial – möglich. Dennoch bleibt ein Nachteil gegenüber anderer Blockchain-Technologien bestehen: Ethereum hat eine eigene Programmiersprache für die Entwicklung von Smart Contracts, welche von den Entwicklern neu gelernt werden muss. Andere Technologien verwenden hier oft Programmiersprachen, die bereits existieren, um eine größere Akzeptanz bei Entwicklern zu erzielen. Allerdings bietet die Ethereum Foundation zahlreiche Standards und Spezifikationen, um diesen Nachteil etwas auszugleichen. Hier kann also auf bereits bestehende Grund-Implementierungen zurückgegriffen werden, welche von hunderten Open-Source-Entwicklern bereits begutachtet und verbessert wurden. Zudem wird die Sprache direkt für Smart Contracts optimiert und die Verwendung der Sprache wird sehr stark in der Freiheit eingeschränkt, um möglichst wenig Sicherheitslücken zu verursachen.

Dieses Konzept empfiehlt die Nutzung einer Ethereum-basierten Infrastruktur aus den genannten Gründen, die in der folgenden Aufzählung nochmal zusammengefasst werden:

- Geringeres Risiko eines Vendor-Lock-Ins.
- Speziell für Smart Contracts optimierte Programmiersprache.
- Spezielle Entwickler-Tools für die Entwicklung, Qualitätssicherung und Wartung von Smart Contracts.
- Hohe Wiederverwendbarkeit für zukünftige andere Blockchain-Projekte (betr. A14).
- Größte Entwicklerbasis mit vielen Standards und Beispiel-Implementierungen.

Eine Infrastruktur basierend auf Hyperledger würde die genannten Vorteile und Kriterien erfüllen. Diese sollte als private-permissioned Blockchain aufgesetzt werden, so dass Lese- und Schreibzugriffe geschützt werden können (betr. A10). Sollen Lesezugriffe frei zugänglich sein, wäre auch eine public-permissioned Variante denkbar (betr. A15).

6.2.2 Design und Konzept der Smart Contracts

Tokenisierung von Anlagen und Dokumenten Token spielen im Bereich der Blockchain-Technologien eine sehr große Rolle. Assets, die tokenisiert werden können, werden früher oder später in Pilotprojekten mit Blockchain-Technologien digitalisiert. Im Anwendungsfall der Genehmigungsanträge können im Wesentlichen zwei Aspekte tokenisiert werden: die Industrie-

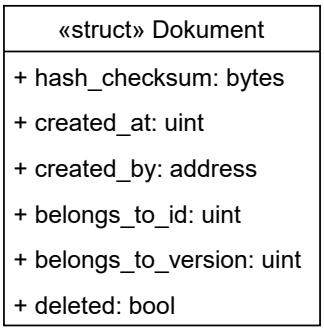

Abbildung 2: Objektdiagramm eines im Smart Contract abgesicherten Dokuments.

anlagen und deren zugehörigen Dokumente. Die drei größten existierenden Token-Standards wurden bereits in den Grundlagen (vgl. 3.3) vorgestellt. Da sowohl die Anlagen als auch die Dokumente eindeutig unterscheidbar und eher schlecht in beliebig kleine Stücke teilbar sind, bietet sich hier vor allem der ERC-721 Non-fungible Token Standard an (Entriken et al., 2018).

Jedes Dokument lässt sich als Asset repräsentieren und kann demnach als ein ERC-721 Token implementiert werden. Abbildung 2 zeigt die Attribute, die ein Dokument besitzen sollte (betr. A5). Da konkrete Inhalte und Dokumentennamen Hinweise zu Betriebsgeheimnissen geben könnten, werden diese nicht in der Blockchain abgespeichert (betr. A10). Der Hash wird verwendet, um den Inhalt eines Dokumentes zuverlässig abzusichern (betr. A1). Der Zeitstempel dokumentiert den Zeitpunkt, zu dem das Dokument hinterlegt wurde (betr. A5). Zusätzlich kann pseudonymisiert über das Wallet der Ersteller des Dokuments gespeichert werden. Da eine Löschung von der Blockchain nicht möglich ist, wird noch ein zusätzliches Flag angelegt, welches darstellt, ob das Dokument gelöscht und somit ungültig wurde.

An dieser Stelle kommt die Überlegung auf, ob ein Parent-Hash, also ein Hash auf das übergeordnete Verzeichnis sinnvoll wäre. Dies hätte allerdings zur Folge, dass jede Änderung am oder im übergeordneten Verzeichnis, zu einer Änderung des Hashes führen würde. Vor allem zum Zeitpunkt der Erstellung eines neuen Verzeichnisses mit neuen Dokumenten hätte dies sehr viele Transakationen zur Folge, da bei jedem weiteren Dokument alle vorherigen aktualisiert werden müssten. Aus technischer Sicht ist es ebenfalls komplex von einem gesamten Verzeichnis zuverlässige Hash-Werte zu ermitteln. Hier dürfen Attribute wie der Zeitpunkt der letzten Modifikation nicht mit einbezogen werden. Zusätzlich sortiert jedes Betriebssystem intern die Inhalte der Verzeichnisse unterschiedlich, hierdurch würde jedes Betriebssystem einen anderen Hash für das Verzeichnis berechnen – evtl. sogar jeder Rechner. Bei der Verifikation des gesamten Verzeichnisses auf der Blockchain würde also häufig Misstrauen bzgl. der erhaltenen Verzeichnisse entstehen. Zudem ist der Gedanke von Verzeichnissen sehr an Cloud-Lösungen angelehnt. In einem digitalen System mit strukturierten Daten sieht die Struktur unter Umständen anders aus, weshalb ein Parent-Hash auf der Ebene der Smart Contracts nicht empfohlen wird. So wird eine erhöhte Kompatibilität und Performance, ein geringerer Speicherbedarf und weni-

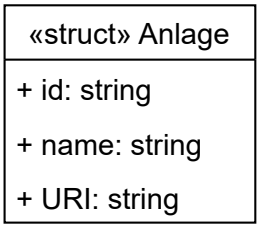

Abbildung 3: Objektdiagramm einer im Smart Contract hinterlegten Anlage.

ger Transaktionsgebühren benötigt. Für eine bessere Usability kann die Endanwendung, die auf die Blockchain zugreift, trotzdem Verzeichnis-basierte Strukturen anbieten, ohne dass die Blockchain selbst davon wissen muss (betr. A3).

Jede Anlage lässt sich ebenfalls als Asset repräsentieren und könnte demnach ebenfalls als ein ERC-721 Token implementiert werden (betr. A5). Da jedoch keine Betriebsgeheimnisse abgelegt werden können, fallen hier sehr viele Möglichkeiten weg. Abbildung 3 zeigt im Wesentlichen die minimalste Ausprägung eines ERC-721 Token. Die URI erlaubt einen blockchain-externen Link zu setzen, welcher bspw. in das Intranet eines Betreibers zeigen kann. Im Falle von BASF, Evonik und Wacker könnte hier ebenfalls ein Link auf die Anlage im hausinternen SAP-System zeigen. Die Zuordnung des Tokens zu einem Betreiber erfolgt in diesem Fall über die Zuordnung zu dessen Wallet. Diese Zuordnungen können dann nach Genehmigung in das ISA-B Register (oder vergleichbare) über Schnittstellen exportiert werden (betr. A7).

Um die Sinnhaftigkeit der Tokenisierung einer Anlage noch weiter zu steigern, kann die Gesamtheit aller Dokumente einer Anlage als Teil des ERC-721 Tokens betrachtet werden. Ein allgemeines Vorgehen wäre für jede Anlage einen eigenen ERC-721 Smart Contract zu deployen. Der Contract beinhaltet dann die Metadaten für eine Anlage und für jedes Dokument ein eigenes Token. Somit wäre die Zuordnung zu einer Anlage immer eindeutig und es wäre immer definiert, wer der zugehörige Betreiber ist. Die Dokumenten-Token selbst können dann vom Ersteller zur Behörde transferiert werden, um den Dokumentenübergang zu simulieren. Dies entspricht dann dem Briefkasten-Schlitz in der analogen Welt.

Mit diesem Ansatz würden eine Menge Contracts auf der Blockchain benötigt werden, da jede Anlage ihre eigene Menge an Dokumenten besitzt. Zudem müsste eine Lösung für Änderungsanzeigen einer Anlage gefunden werden, so dass die Dokumente eindeutig zugeordnet werden können. Um die Menge an Contracts zu verwalten, werden weitere Factory Contracts benötigt. Die Komplexität der Endanwendungen, die die Blockchain verwenden, würde ebenfalls enorm ansteigen, da diese tausende Contracts überwachen und prüfen müsste.

Diese Komplexität kann mit Hilfe des ERC-1155 Multi Token Standards gelöst werden (betr. A3) (Radomski et al., 2018). Der ERC-1155 Standard erlaubt die Kombination vieler verschiedener Token oder Assets in einen einzigen Smart Contract. Für den Anwendungsfall der

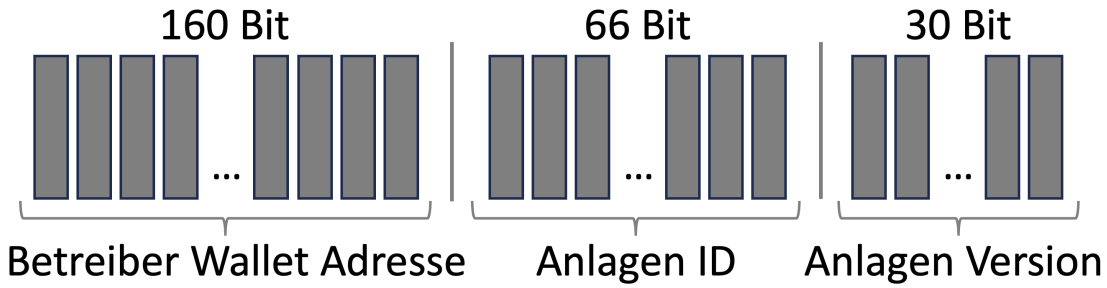

Abbildung 4: Aufteilung der 256 Bit einer ID im ERC-1155 Standard.

Genehmigungsanträge würden also alle Anlagen inkl. ihrer Dokumente in einem Smart Contract verwaltet werden. Dadurch benötigen Endanwendungen, die die Blockchain verwenden, lediglich eine Verbindung zu einem Contract. Zusätzlich wäre der gesamte Zustand und Speicher aller Genehmigungsanträge nur in einem einzigen Contract hinterlegt, was spätere Migrationen oder Upgrades der Logik vereinfachen würde.

Die Zusammenführung mehrerer Token in einem einzigen Contract wirkt zunächst so, als könnten hier irgendwann keine Anlagen oder Dokumente mehr verwaltet werden. Allerdings erfolgt die Zusammenführung über die Token-ID, welche aus 32 Byte also 256 Bit besteht. Somit können 2^{256} verschiedene Token bzw. in diesem Fall Anlagen, deren Ausbau-Versionen und deren Dokumente hinterlegt werden. Die 256 Bit können dann passend aufgeteilt werden, um verschiedene Informationen in die ID zu verpacken wie bspw. den Betreiber und die Anlagen-Version. Die maximale Anzahl der möglichen Token im Contract ist aus technischer Sicht nicht erreichbar, da die Festplatten der zugrundeliegenden Blockchain lange überlaufen würden.

Da die vollen 2^{256} Möglichkeiten also nicht benötigt werden, lässt sich die ID wie in Abbildung 4 etwas nützlicher aufteilen, um mehr Informationen aus ihr zu gewinnen: Wie bereits erwähnt, besteht eine ID aus 256 Bit. Um eine Milliarde Versionen pro Anlage zu garantieren, können 30 Bit für die Spezifikation der Version verwendet werden. 66 Bit werden für die Konkretisierung der Anlagen selbst genutzt, was über 70 Trillionen Anlagen pro Betreiber erlaubt. Die letzten 160 Bit repräsentieren die Wallet-Adresse des Betreibers, um immer eindeutig zuordnen zu können, wer die Anlage betreibt. Dieses komprimierte Verfahren erhöht die Performance und reduziert die Speicherkosten auf der Blockchain. Natürlich ist diese Aufteilung frei wählbar, allerdings sollten immer 160 Bit für die Wallet-Adresse reserviert werden. Jede Anlagen-Version kann dann beliebig viele Dokumente besitzen, solange die Gesamtkapazität von 2^{256} nicht überschritten wird.

Smart Contracts als digitaler Stempel Im aktuellen Prozess werden die Antragsunterlagen sowie der Genehmigungsbescheid von der zuständigen Behörde gestempelt, um die Echtheit der Unterlagen sicherzustellen. In einem digitalen System muss dieser Stempel ersetzt werden

(betr. A1). Die Blockchain kann mit Hilfe von Smart Contracts diese manipulationssicher herstellen. Wichtig ist hier allerdings zu bedenken, dass die Blockchain nicht verhindern kann, dass falsche Daten abgesichert werden. In der analogen Welt könnte der Mensch allerdings ebenfalls ein falsches Dokument versehentlich abstempeln. Der Unterschied bei der Blockchain ist aber, dass das fehlerhafte Dokument ebenfalls manipulationssicher hinterlegt werden würde. Dieses kann zwar als ungültig markiert oder sogar gelöscht werden, aber in der Historie der Blockchain wird der Fehler für immer dokumentiert bleiben.

Abbildung 5 zeigt die interne Struktur der Smart Contracts. Hierbei wurde das Konzept an der Spezifikation des ERC-1155 Standards angelehnt. Der Standard macht sich eine Maskierung und Komprimierung der IDs zu Nutzen. In diesem Konzept wird ein Antrag – unabhängig ob Änderung, oder Neu – über eine Anlagen-ID und eine Versionsnummer repräsentiert. Beide zusammen lassen sich zu einer kombinierten ID im Sinne des ERC-1155 zusammensetzen. Über die Anlagen-ID, die Versionsnummer und den Hash des Dokuments, gelangt man letztendlich zu den konkreten Informationen des Dokuments. Dies wird in Abbildung 5 über das verschachtelte Mapping dargestellt.

Da der ERC-1155 Standard einen Token-Standard repräsentiert, können diese Token auch zwischen Wallets versendet werden. Im Rahmen des Genehmigungsprozesses kann der Verbleib der Token auch den aktuellen Zuständigkeitsbereich während des Prozesses repräsentieren (betr. A5, A15). Sobald ein Unternehmen die Dokumenten-Token an eine Behörde transferiert, kann dies als Zeitpunkt der Einreichung interpretiert werden. Ab jetzt laufen Fristen los und der Token-Übergang repräsentiert den Briefkasten-Schlitz, in den Papierdokumente eingeworfen werden. Sobald der Antrag genehmigt oder abgelehnt ist, kann die Behörde die Dokumenten-Token inkl. Genehmigungsbescheid wieder zurück-transferieren. Egal in welchem Zuständigkeitsbereich sich die Token aktuell befinden, ist der Betreiber immer über die ersten 160 Bit der ID identifizierbar. Dadurch können sogar Sicherheitsmechanismen umgesetzt werden, die einen Transfer nur an den ursprünglichen Betreiber zulassen (betr. A10).

Jeder Token-Standard beinhaltet ebenfalls eine sogenannte Allowance-Logik. Darüber kann einer dritten Partei erlaubt werden, die Token zu transferieren. Somit kann ein Betreiber einer beliebigen Anzahl Mitarbeitenden die Erlaubnis geben, Dokumente in seinem Namen bei den Behörden einzureichen. Ebenso kann die Behörde einer beliebigen Anzahl Mitarbeitenden erlauben, die Dokumente inkl. Genehmigungsbescheid wieder an die Betreiber auszuhändigen. Diese Erlaubnis kann entweder pauschal erteilt werden für alle oder gezielt für einzelne Anlagen (betr. A3).

Zusätzlich zum ERC-1155 Standard kann eine ähnliche Logik wie die Allowance-Logik entwickelt werden, um Zugriffsrechte zu verwalten. Hierbei kann in der Blockchain hinterlegt werden, welche Institution Zugriffsrechte auf die unterschiedlichen Dokumente erhalten soll. Über die

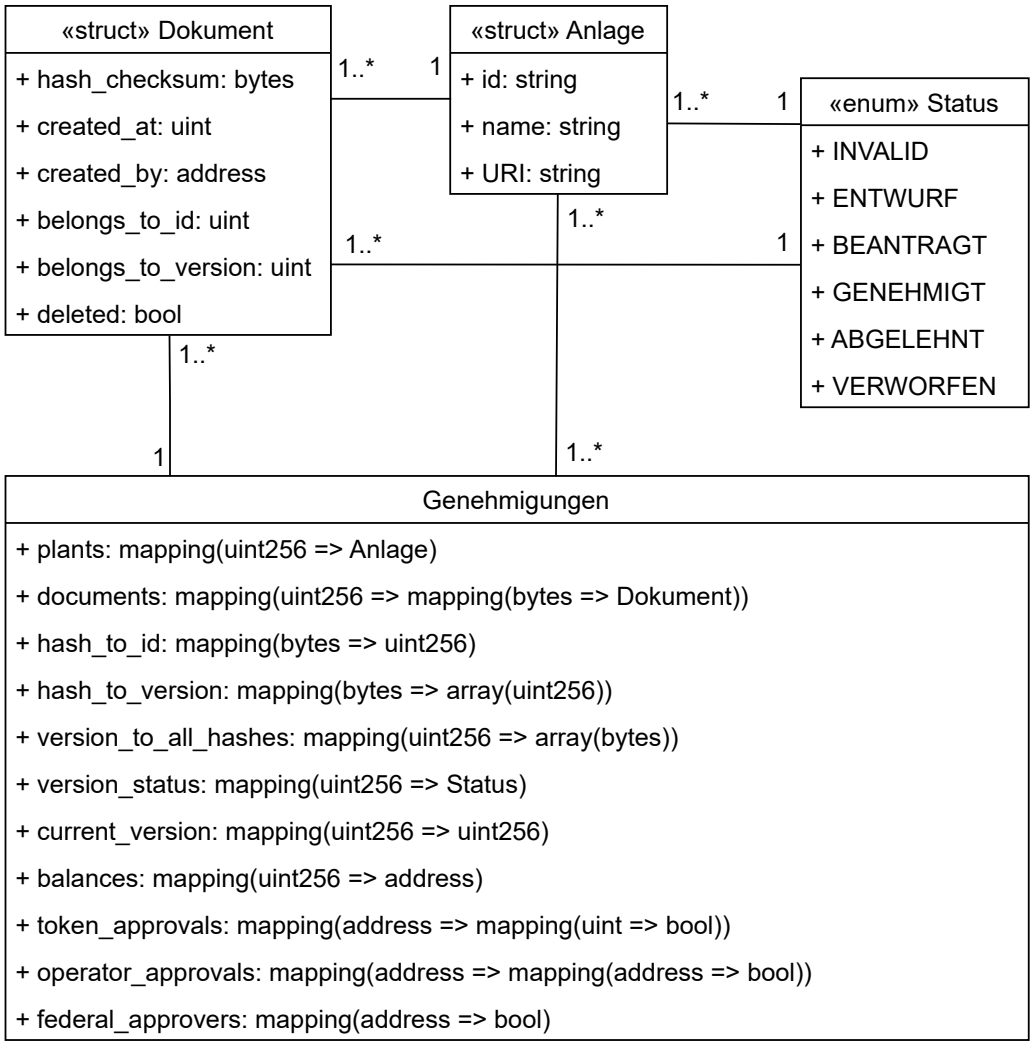

Abbildung 5: Klassendiagramm für die Smart Contract Struktur

Allowance-Logik lässt sich dann entscheiden, welche Mitarbeitenden konkret Zugriff erhalten sollen (betr. A10).

Bei der Programmierung mit Smart Contracts werden wichtige Ereignisse über Events signalisiert. Dies ermöglicht externen Software-Komponenten auf gewisse Ereignisse zu reagieren, ohne dass die Smart Contracts selbst über deren Logik Bescheid wissen müssen. Über diesen Ansatz können die Contracts generisch und wiederverwendbar implementiert werden. In diesem Konzept sollten Events emittiert werden, wann immer ein Transfer (Übergang des Zuständigkeitsbereichs), eine Allowance (Erlaubnis an Mitarbeitende) oder ein Zugriffsrecht erteilt wird. Zudem wäre auch bei der Erstellung neuer Anlagen, Versionen oder Dokumente ein Event hilfreich. So können die Endanwendungen mit Hilfe der Events prüfen, ob Fristen eingehalten wurden, oder wie weit der Prozess fortgeschritten ist (betr. A15).

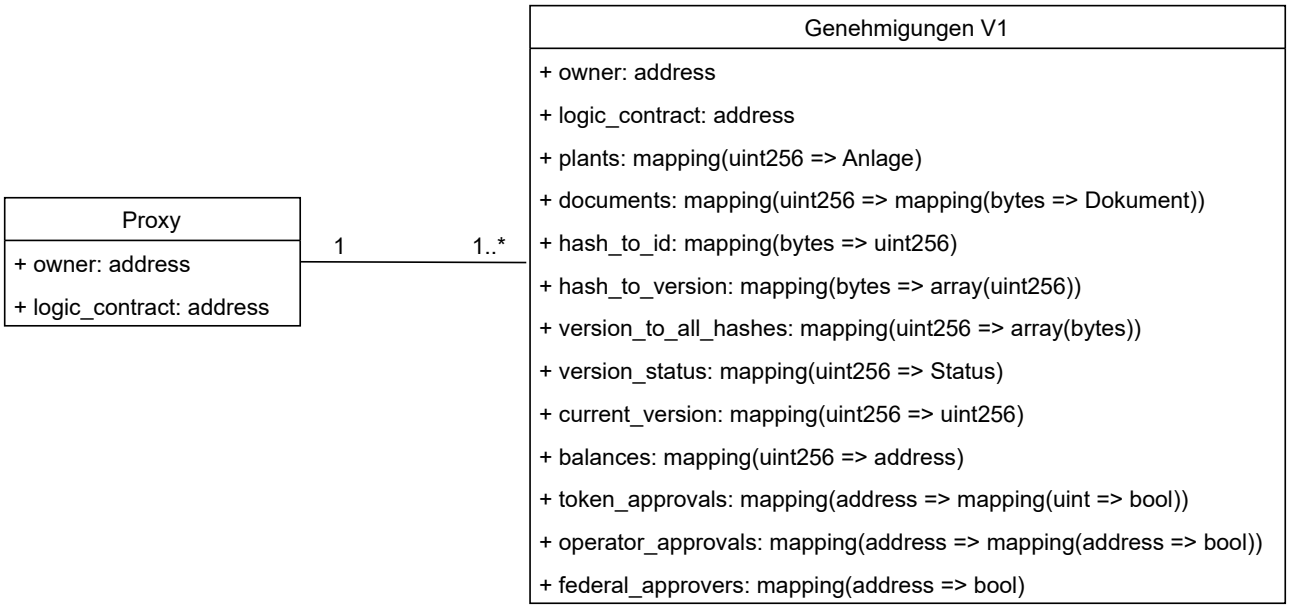

Abbildung 6: Klassendiagramm für das Proxy Pattern

Da bei Änderungsanzeigen nicht zwingend alle Dokumente erneuert werden, kann die letzte gültige, genehmigte Version eines Dokuments in mehreren Anlagen-Versionen relevant sein. Deshalb wird für jedes Dokument noch ein Statusfeld benötigt. Dieses repräsentiert, ob ein Dokument sich im Entwurf befindet, eingereicht, genehmigt oder verworfen bzw. gelöscht wurde. Bei der Überprüfung des Dokumenten-Hashes lässt sich so genau sehen, in welchen Versionen das Dokument gültig ist. Existiert das Dokument beispielsweise nur für die 1. Anlagen-Version, aber die Anlage befindet sich bereits in der zweiten Ausbaustufe, können die Nutzenden einfach identifizieren, ob das Dokument noch relevant ist (betr. A1). In Kapitel 6.3.1 wird dies genauer erläutert und anschaulich dargestellt.

Upgrades der Smart Contract Logik Smart Contracts gelten im Allgemeinen als unveränderbar, jedoch kann es im Laufe der Zeit nötig sein, die Logik eines Contracts zu verändern ohne deren Zustand und Speicher zu verlieren. Dies wird über sogenannte Upgradeability Patterns ermöglicht (Hajizadeh et al., 2023). Für diesen Anwendungsfall wird auf ein Proxy Pattern zurückgegriffen, da nur ein einziger ERC-1155 Contract zugrundeliegt. Abbildung 6 zeigt die Struktur, die dafür benötigt wird.

Solidity bietet die Möglichkeit sogenannte Delegate-Calls durchzuführen. Bei diesen erlaubt Contract A einem anderen Contract B seinen Zustand und Speicher zu modifizieren. Beim Proxy-Pattern wird ein Proxy-Contract eingesetzt, welcher keinerlei Logik besitzt und alle eingehenden Funktionsaufrufe direkt an einen Logik-Contract weiterleitet. Diese Weiterleitung erfolgt über einen Delegate-Call. Somit werden alle Speicher- und Zustandsänderungen im Bereich des Proxy-Contracts durchgeführt. Deshalb muss der Logik-Contract zu Beginn exakt genauso

aufgebaut werden wie der Proxy-Contract, da er sonst den Speicher des Proxys verfälschen würde. In Abbildung 6 wurde deshalb im Contract `Genehmigungen` sowohl das Attribut `owner` als auch `logic_contract` aufgenommen. Im Contract `Genehmigungen` werden beide allerdings irrelevant sein.

Sollte die Logik irgendwann geändert werden müssen, so wird lediglich ein neuer Logik-Contract benötigt (betr. A14). Im Proxy-Contract wird dann die Adresse des Logik-Contracts aktualisiert und ab dann werden alle Funktionsaufrufe an die neue Logik weitergeleitet. Somit hat der neue Logik-Contract direkt Zugriff auf den selben Speicher und Zustand im Proxy wie die veraltete Version. Abbildung 7 zeigt diese Zugriffsweiterleitung.

6.3 Middleware

Die Middleware wird eingeführt, um zusätzliche Sicherheitsmechanismen und -module einsetzen zu können. Für die erste Version werden zwei Module empfohlen: Ein Modul für die Verifikation der Dokumente, und ein Faucet, welches Schreibzugriffe absichert. Sollten zukünftig neue Sicherheitsmechanismen benötigt werden, können diese einfach in die Middleware-Schicht integriert werden.

6.3.1 Verifikation der Dokumente

Um ein empfangenes Dokument zu verifizieren, kann ein manueller Ansatz gewählt werden. Dieser Schritt ist vor allem relevant, um das nötige Vertrauen in einer nutzerfreundlichere Anwendung aufzubauen. Der Vorteil von Blockchain Anwendungen ist, dass alle Verifikationen auch manuell durchgeführt werden können und somit im Zweifelsfall geprüft werden kann, ob eine Manipulation – sei es am Dokument, oder an einer Softwarekomponente – stattgefunden hat.

Soll ein Dokument manuell verifiziert werden, muss zunächst der Hash des Dokuments berechnet werden. Üblicherweise erfolgt diese Berechnung mit Hilfe einer Checksumme. In diesem Anwendungsfall wird eine SHA-256 Checksumme als Hash verwendet (Hansen & Eastlake 3rd, 2011). Diese kann über die Powershell unter Windows oder mit dem Terminal unter Linux/Mac

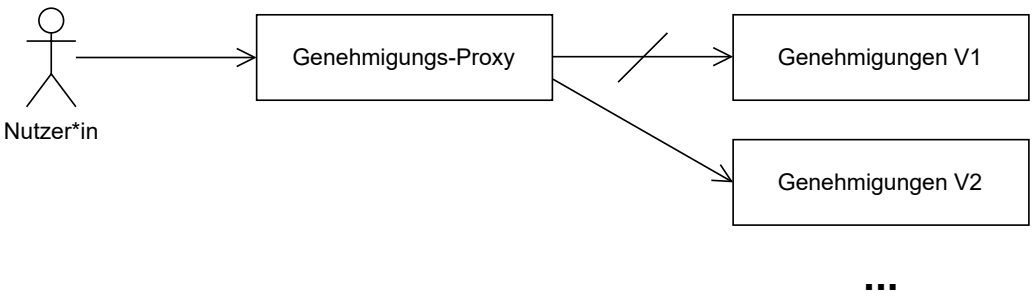

Abbildung 7: Weiterleitung der Zugriffe über den Proxy- an einen Logik-Contract.

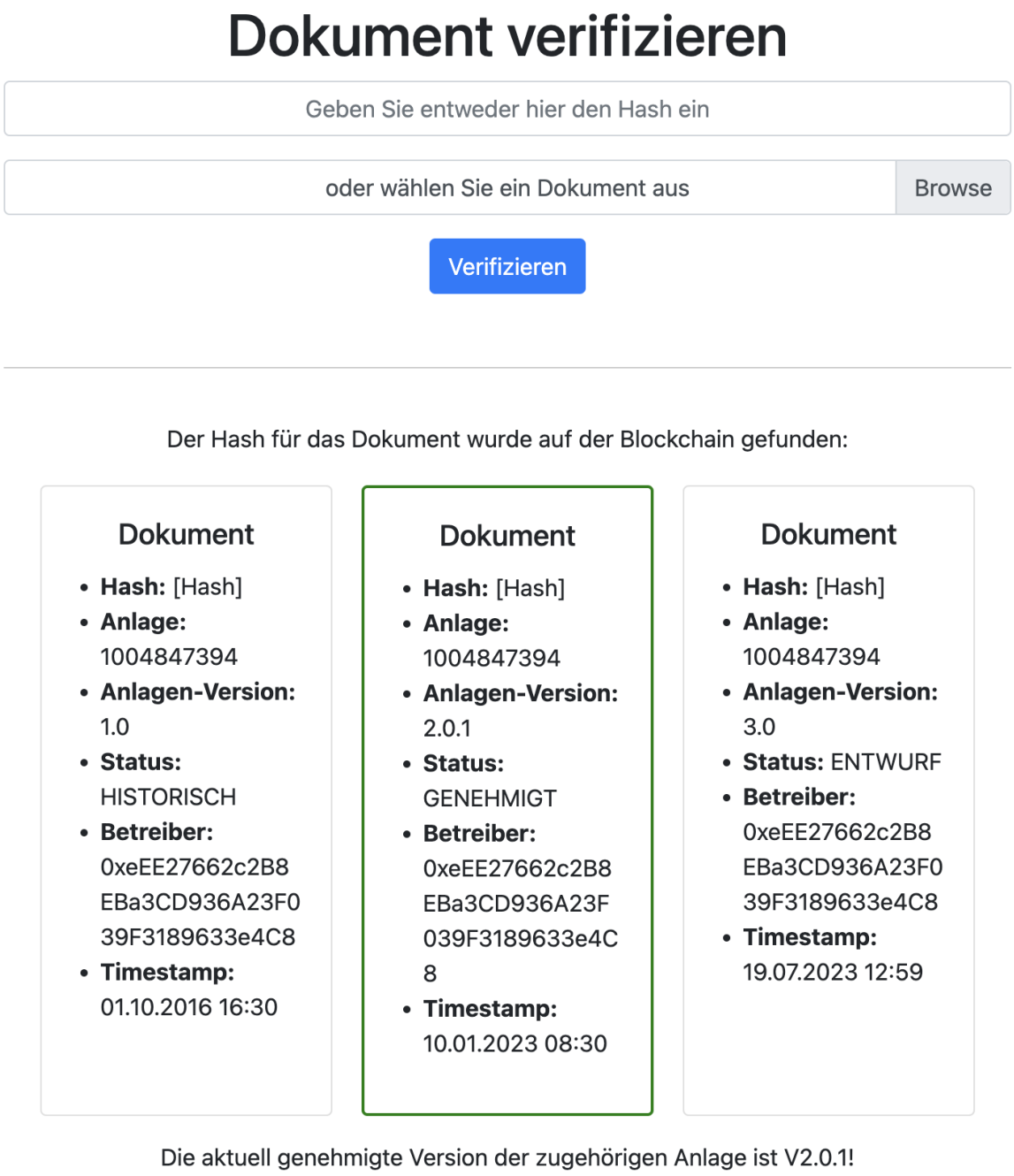

Abbildung 8: Beispiel-Darstellung der Verifikations-Webseite mit erfolgreichem Abgleich.

berechnet werden. Das Kommando für die Linux oder Mac Terminals lautet `shasum -a 256 <PFAD_UND_DATEINAME>`. Unter Windows wäre das Kommando für die Powershell `CertUtil -hashfile <PFAD_UND_DATEINAME> SHA256`. Das Ergebnis ist ein Hashwert in hexadezimaler Darstellung mit einer Länge von 64 Zeichen.

Der Hashwert kann dann genutzt werden, um auf der Blockchain im Smart Contract zu überprüfen, ob dieses Dokument hinterlegt ist (betr. A1). Befindet sich auf der Blockchain der Hashwert, werden die zugehörigen Informationen zum Dokument geladen. In diesem Anwendungsfall also die zugehörige Anlage inkl. der Version und des Status – also ob das Dokument sich im Entwurf befindet bzw. eingereicht, genehmigt oder verworfen wurde. Sollte das Dokument nicht auf der Blockchain existieren, werden keine Informationen angezeigt.

Da nicht für jeden Fall der manuelle Weg benötigt wird, kann mit Hilfe einer Verifikations-Webseite der Prozess effizienter gestaltet werden (betr. A3). Die Webseite kann sehr simpel aufgebaut werden, so dass entweder ein Hashwert oder ein Dokument angegeben werden kann. Wird ein Hashwert angegeben, wird dieser direkt auf der Blockchain verifiziert. Wird ein Dokument angegeben, dann berechnet die Webseite selbst den Hash mithilfe der Checksumme und verifiziert dies dann auf der Blockchain. Wichtig ist hierbei, dass die Webseite so implementiert wird, dass das Dokument nicht auf einen Server hochgeladen wird. Die Berechnung sollte lokal im Browser des Nutzenden stattfinden, so dass hier keine Dokumente mit Betriebsgeheimnissen unnötig auf einen Server geladen werden.

Abbildung 8 zeigt exemplarisch wie die Webseite aussehen könnte. In diesem Fall ist ein Dokument zu sehen, welches für drei verschiedene Anlagen-Versionen relevant ist (betr. A5). Die erste Version ist dabei nur noch historisch, die zweite aktuell genehmigt und die dritte gerade beantragt. Wäre kein Dokument mit einer aktuell genehmigten Version zu finden, so handelt es sich um ein Dokument, welches durch eine Änderung an der Anlage irrelevant wurde und nur noch von historischer Bedeutung ist. Abbildung 9 zeigt eine beispielhafte Darstellung, wenn kein passendes Dokument auf der Blockchain gefunden werden kann.

6.3.2 Datenprüfung beim Schreibvorgang

Bei nationalen oder konsortialen Blockchains gelten zusätzliche Bestimmungen, was den Umgang mit illegalen Daten betrifft. Werden bspw. Links zu Kinderpornographie oder Hitler-Grüße auf eine solche Blockchain gespeichert, kann die Löschung dieser Daten gefordert werden. Da eine Löschung allerdings nicht möglich ist, müsste die Blockchain abgeschalten werden oder ein Fork auf einen Stand vor diesen Daten zurückgesetzt werden. Dadurch können wichtige Daten verloren gehen, oder eine Lücke entstehen, welche Manipulationen zulässt. Das Eliminieren dieser illegalen Daten würde zudem Zeit beanspruchen und Aufwand verursachen. Angreifer könnten danach den Vorgang wiederholen und das System so dauerhaft lahmlegen, weshalb

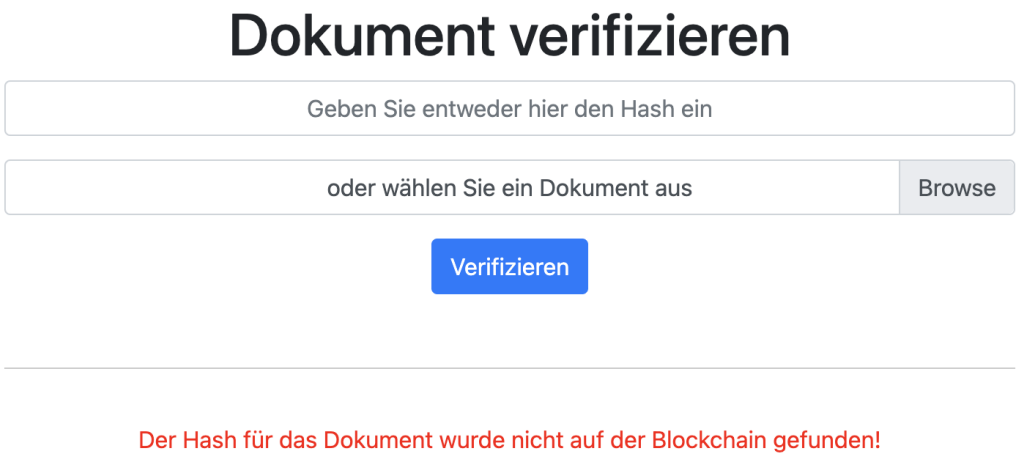

Abbildung 9: Beispiel-Darstellung der Verifikations-Webseite ohne zutreffendes Dokument.

hier Sicherheitsmechanismen eingeplant werden sollten, um das Risiko möglichst minimal zu halten (betr. A3).

Das Risiko für illegale Daten entsteht nur während des Schreibprozesses und dieser benötigt Ether für die Bezahlung der Transaktionsgebühren. Wenn alle Teilnehmer jederzeit über Ether auf ihrem Wallet verfügen, erhöht sich das Risiko für illegale Schreibprozesse. So könnte theoretisch das Wallet missbraucht werden, um beliebige Transaktionen auszuführen. Zwar würde anhand der Wallet-Adresse nachvollziehbar sein, wer für diese illegalen Daten verantwortlich ist, jedoch würde dies nichts daran ändern, dass die Daten wieder entfernt werden müssen. Deshalb sollten die Teilnehmer kein Ether zur freien Verfügung besitzen, sondern immer nur die Menge, die aktuell für den nächsten Schreibvorgang benötigt wird.

Für diesen Ansatz wird die Verwendung eines Faucets empfohlen. Ein Faucet im Allgemeinen ist eine Software-Komponente, welche Ether besitzt und auf Anfrage dieses kostenlos ausgibt. Üblicherweise wird diese Komponente vor allem für Testnetze im Blockchain-Bereich verwendet, um Test-Ether bei Bedarf an Entwickler zu verteilen. Allerdings kann im Anwendungsfall der Genehmigungsprozesse ein Faucet genutzt werden, um Schreibzugriffe zu verifizieren.

Abbildung 10 zeigt den Prozess, der intern mit einem Faucet abläuft. Die drei Zuständigkeitsbereiche markieren, welcher Teil durch ein Faucet gegenüber einer Anwendung ohne Faucet hinzukommt. Sobald der Nutzende das gewünschte Dokument in die Anwendung hochlädt, wird dort der Hash für das Dokument berechnet und eine Transaktion vorbereitet, welche diesen Hash und zugehörige Metadaten auf die Blockchain speichern möchte. Diese Transaktion wird in Abbildung 10 mit dem Kürzel `D` gekennzeichnet. In einer Anwendung ohne Faucet würde diese Transaktion direkt an die Blockchain übermittelt, dort ausgeführt und die Transaktionsgebühr bezahlt werden. Mit Faucet wird die Transaktion zunächst an das Faucet geschickt. Zusätzlich erhält das Faucet das Dokument, für welches der Hash auf die Blockchain geschrieben werden

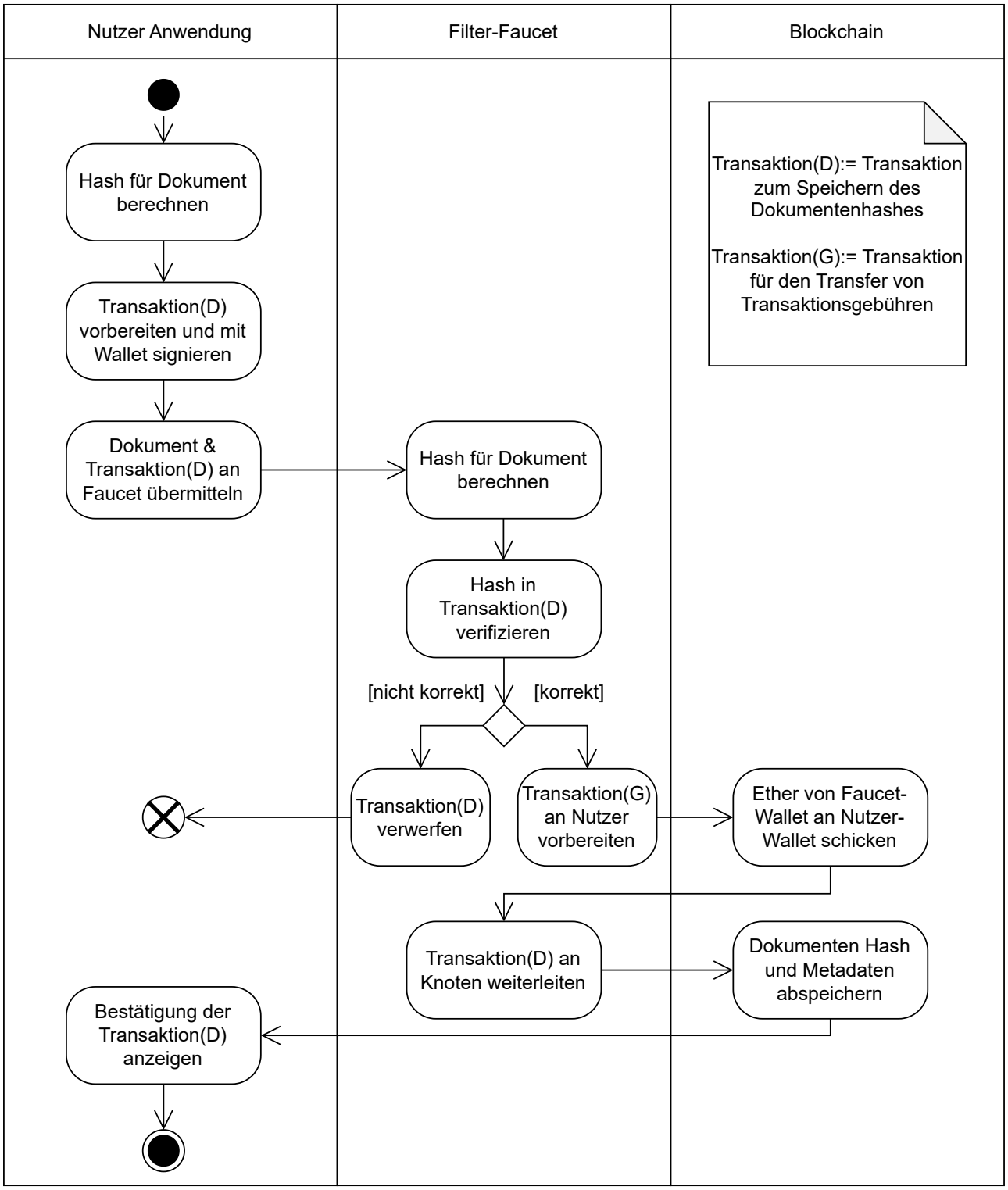

Abbildung 10: Ablauf eines Schreibprozesses mit Faucet-Anbindung.

soll. Das Faucet kann nun erneut den Hash für das Dokument berechnen und prüfen, ob dieser Hash wirklich in der Transaktion `D` zu finden ist. Ist alles wie erwartet, transferiert das Faucet die

benötigte Menge Ether zur Bezahlung der Transaktionsgebühr an das Nutzer-Wallet. Danach wird die ursprüngliche Transaktion an die Blockchain weitergeleitet.

Das Faucet ermöglicht so eine Inhaltsprüfung, welche zukünftig auch beliebig erweitert werden kann (betr. A14). Hier muss nur immer der Aspekt der Zensur beachtet werden. Das Faucet sollte also nicht zu stark in die Inhalte eingreifen und lediglich illegale Daten verhindern. Das Faucet könnte aber auch um zusätzliche Sicherheitsmechanismen erweitert werden, wie bspw. eine Prüfung, an wen die ERC-1155 Token eines Dokuments übermittelt werden. So ist bspw. denkbar, dass das Faucet prüft, ob die Behörde die Dokumente an den richtigen Betreiber zurückschickt, damit nicht versehentlich Betriebsgeheimnisse an falsche Betreiber übermittelt werden (betr. A10). Diese Überprüfung könnte allerdings auch in der Endanwendung selbst stattfinden – das Faucet wäre dann nur noch eine zusätzliche Sicherheit direkt vor dem Schreibvorgang in die Blockchain.

Ein weiterer Vorteil des Faucets ist, dass der Absender einer Transaktion geprüft werden kann. So können nur Transaktionen von bekannten Teilnehmern erlaubt werden. Der Allowance-Mechanismus des ERC-1155 Standards, über den Betreiber oder Behörden den Mitarbeitenden die Erlaubnis geben können in ihrem Namen Dokumente anzulegen und einzureichen, kann das Faucet dabei berücksichtigen. Eine Transaktion wird also dann erlaubt, wenn der Absender ein Betreiber, eine Behörde oder ein dem Faucet unbekanntes Wallet mit Erlaubnis ist. Um die Ausfallsicherheit des Faucets zu erhöhen, kann das Faucet auch dezentral mehrfach deployed werden (betr. A6). Prinzipiell könnte pro Teilnehmer – also Betreiber oder Behörde – ein eigenes Faucet deployed werden, wodurch die Übertragung der Dokumente mit Betriebsgeheimnissen nicht über das öffentliche Internet erfolgen müsste (betr. A10).

6.4 Applikationsschicht

Da die Blockchain-Schicht mit den Smart Contracts nur Hashwerte, Zugriffe, Berechtigungen und Zeitpunkte manipulationssicher verwaltet, ist es aus Sicht der Blockchain egal, welche Endanwendung ihr diese Daten übermittelt. Die Endanwendung kann also im Lauf der Zeit angepasst oder komplett ausgetauscht werden, ohne dass die zugrundeliegende Blockchain davon betroffen ist (betr. A14). In den Stakeholder-Gesprächen wurden unterschiedliche bereits existierende Ansätze ermittelt. Zudem wurden auch die Wünsche und Anforderungen erhoben. Die folgenden drei Beispiele beschreiben einen möglichen Weg, welcher in Zukunft bestritten werden kann, um zu einer vollkommen digitalen Endanwendung zu gelangen.

6.4.1 Version 1: Datencloud für PDFs

Die erste Version soll eine Zwischenlösung darstellen, um möglichst schnell von der Papier-Version zu einer elektronischen Version wechseln zu können (betr. A8). BASF nutzt hier bereits erfolgreich eine Cloud-Lösung auf Basis von NextCloud zusammen mit dem zuständigen Landratsamt. Nach dem Vorbild von BASF kann eine ähnliche Lösung etabliert werden. Dafür wird

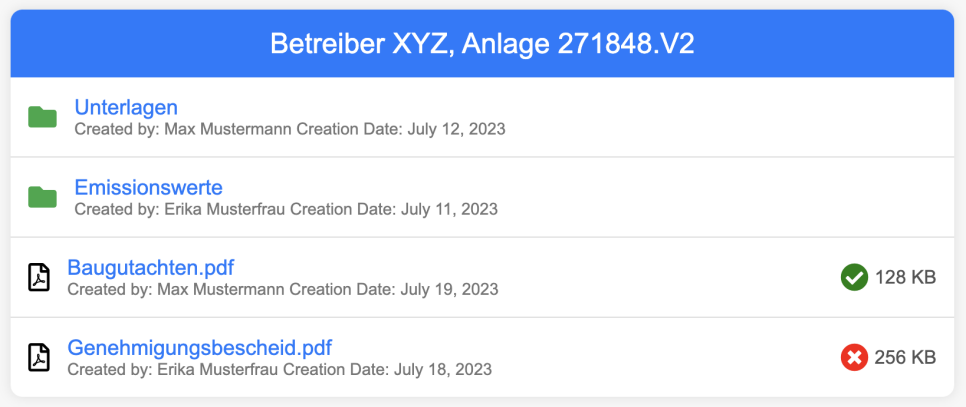

Abbildung 11: Beispiel-Darstellung eines Cloud-Verzeichnisses mit Verifikation der Hashwerte.

eine Open-Source-Cloud-Lösung empfohlen, welche für diesen Anwendungsfall etwas erweitert werden kann.

Abbildung 11 zeigt wie eine angepasste Cloud-Lösung aussehen könnte. Für jedes Dokument könnte hier ein Icon angezeigt werden, welches signalisiert, ob der Hash des Dokuments auf der Blockchain hinerlegt ist.

Der Vorteil dieses Ansatzes ist, dass die Nutzenden den Umgang mit Cloud-Lösungen heutzutage meistens gewohnt sind. Zudem deckt die Cloud-Lösung von sich aus viele relevante Anforderungen ab, wie bspw. Zugriffsberechtigungen und den Dokumentenübergang in den Zuständigkeitsbereich der Behörden. Der Nachteil ist, dass dieser Ansatz nur mit Dokumenten realisierbar ist, hier sind also strukturierte Daten zur digitalen Weiterverarbeitung noch nicht möglich (betr. A13). Deshalb stellt diese Version nur den ersten Schritt dar.

6.4.2 Version 2: Digitale Webanwendungen

Für die zweite Version soll eine voll digitale Webanwendung entwickelt werden. Diese basiert komplett auf strukturierten Daten und nicht mehr nur auf PDF-Dokumenten (betr. A13). Die Inhalte werden ebenfalls über die Smart Contracts der Blockchain abgesichert. Die Webanwendung besitzt die üblichen Bestandteile inkl. einer eigenen Datenbank, ein eigenes Backend und das Frontend.

Wie genau die Usability und das Frontend aufgebaut werden sollen, muss in zukünftigen Studien definiert werden. Wichtig ist allerdings, dass hier die Wünsche an die Prozessoptimierung umgesetzt werden. So müssen nicht nur die Einreichung der Daten umgesetzt werden, sondern im Idealfall auch wiederverwendbare Bausteine und automatische Befüllung von Formularen basierend auf den Stammdaten (betr. A3). Eine digitale Verwaltung der Nebenbestimmungen bei genehmigten Anträgen ist ebenfalls möglich und sinnvoll (betr. A11).

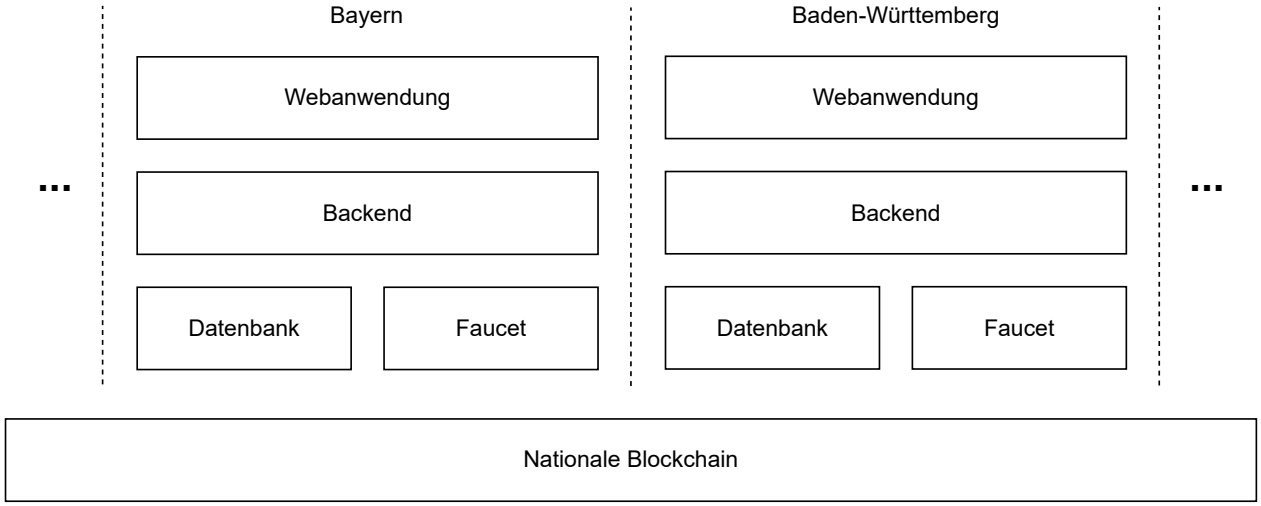

Abbildung 12: Schichtenarchitektur der digitalen Webanwendung.

Die Anwendung kann dann ebenfalls verhindern, dass genehmigte Daten verändert werden können (betr. A1). Sollte ein Änderungsantrag gestellt werden, müssen die Daten zunächst dupliziert werden und danach erst können diese angepasst werden. Natürlich wäre eine Manipulation in der Datenbank immer noch möglich, aber dies würde mit einem Abgleich auf der Blockchain auffallen.

Abbildung 12 zeigt eine mögliche Architektur, die für diese Version denkbar wäre. Das Backend hat dabei Zugriff auf eine Datenbank in der neben den strukturierten Daten auch personenbezogene Daten gespeichert werden könnten (betr. A2). Zusätzlich erhält das Backend direkten lesenden Zugriff auf die nationale Blockchain, und indirekten schreibenden Zugriff über das in Abschnitt 6.3.2 erklärte Faucet. Dabei kann das Backend und die Datenbank auch dezentral zur Verfügung gestellt werden (betr. A6). So kann bspw. jedes Bundesland seine eigene Version mit eigenen spezifischen Anpassungen verwenden. Die Datenbanken könnten auch jeweils in jedem Bundesland separat betrieben werden. So wären die Daten von Bayern bspw. nicht mit denen von Baden-Würtemberg gemischt. Je nach Wunsch, kann die Dezentralisierung noch weiter verstärkt werden und bis auf einzelne Behörden verteilt werden. Alle Systeme interagieren aber mit derselben nationalen Blockchain, wodurch ein Dokument, welches bspw. von einer Behörde in Bayern an ein anderes Bundesland übermittelt wird, auch dort verifizierbar ist (betr. A1).

6.4.3 Version 3: Peer-to-Peer Datenbank

Bei dieser Version wird die Idee von Herrn Lux, eine Peer-to-Peer Datenbank zu verwenden aufgegriffen. Um den dezentralen Charakter auch in der Endandwendung weiter aufzugreifen, kann anstelle einer herkömmlichen Datenbank auch eine Peer-to-Peer Datenbank in Form eines Distributed Ledger (DL) verwendet werden. Hierbei würde der DL so konfiguriert werden, dass die Daten nur in dem Knoten gespeichert werden, welcher diese auch benötigt. Die Knoten der

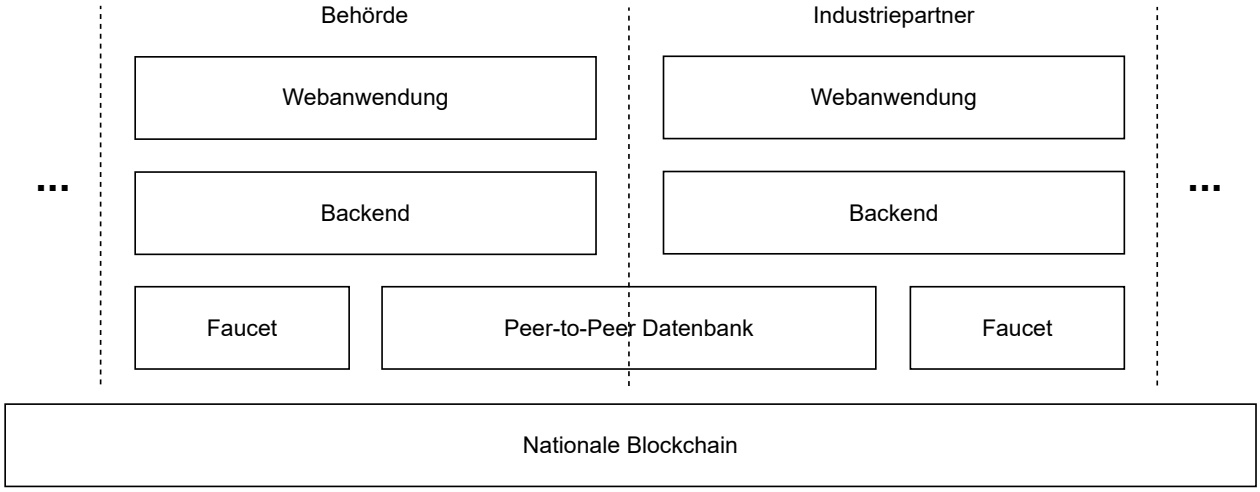

Abbildung 13: Schichtenarchitektur der digitalen Webanwendung mit Peer-to-Peer Datenbank.

Behörden hätten demnach den größten Datenbestand – nämlich alle Daten, die von Betreibern bei dieser Behörde eingereicht wurden. Die Betreiber selbst hätten aber ausschließlich die Daten, der Anlagen, die sie selbst betreiben. Dieser dezentrale Charakter würde die Betriebsgeheimnisse weiter absichern (betr. A10). Der Angriffsvektor bei den Behörden bleibt allerdings trotzdem bestehen, weshalb das System sehr sorgfältig betrieben werden muss.

Abbildung 13 zeigt die Architektur mit einer Peer-to-Peer Datenbank. Bei dieser Variante liegt die größte Dezentralität vor, allerdings ist dies auch mit dem höchsten Aufwand an Ressourcen verbunden (betr. A3, A4). Ein ähnliches Prinzip wird allerdings bereits zwischen Evonik und BASF eingesetzt, um dort Finanzflüsse effektiver zu gestalten. Die Erkenntnisse der beiden Stakeholder könnten bei der Umsetzung dieser Version berücksichtigt werden.

6.4.4 Weitere Ideen

Da eine vollkommen digitale Anwendung mit zahlreichen Schnittstellen interagieren und verknüpft werden kann, existieren ab Version 2 unzählige Möglichkeiten. So könnten bspw. Schnittstellen zu einem digitalen Euro geschaffen werden, welcher die Bezahlprozesse am Ende eines Genehmigungsantrages automatisiert (betr. A7, A12). Hierbei wären sogar Rabatte oder Zusatzgebühren denkbar, sollten Fristen nicht eingehalten worden sein. Alle relevanten Informationen könnten aus den abgesicherten Daten in der zugrundeliegenden Blockchain gewonnen werden und wären somit nicht manipulierbar (betr. A1).

Ebenfalls könnten Schnittstellen geschaffen werden, um alle relevanten Informationen für das ISA-B Register – oder vergleichbare – automatisch zu exportieren. Hier würde der manuelle Aufwand wegfallen, der derzeit nach Erteilung der Genehmigung anfällt (betr. A3).

6.5 Abläufe und Interaktionen

In diesem Abschnitt werden diverse Abläufe und Interaktionen mit dem System technisch dokumentiert. Hierfür wurden diverse UML-Diagramme erstellt. Alle Abläufe betreffen vorrangig die Interaktionen mit dem Smart Contract, da die Interaktionen mit der digitalen Anwendung ab Version 2 zukünftig noch genau geprüft werden müssen. In den Abläufen werden unter Umständen Nutzer*innen dargestellt, wobei deren Aktivitäten auch durch die Cloud aus Version 1 oder die Webanwendung ab Version 2 unterstützt oder ersetzt werden können.

6.5.1 Anlegen eines neuen Dokuments

Bevor ein Dokument in der Blockchain angelegt werden kann, muss dieses natürlich zuvor erstellt worden sein. Ab Version 2 werden dann nur noch strukturierte Daten über die Webanwendung erstellt, aber der Ablauf zur Absicherung auf der Blockchain bleibt identisch: Wird ein neues Dokument im Smart Contract angelegt, muss zunächst geprüft werden, ob die zugehörige Anlage oder Anlagenversion bereits existiert. Abbildung 14 zeigt den exakten Ablauf. Ist das Dokument das erste einer neuen Anlage oder Anlagenversion, so muss zunächst ein zugehöriges Token erstellt werden. Dafür kann bspw. der Link ins Intranet für die Anlage hinterlegt werden.

Sobald die Anlage oder Anlagenversion existiert, kann das zugehörige Dokumenten-Token angelegt werden. Die zugehörigen Metadaten werden dann auf die Blockchain gespeichert und mit dem Hash verknüpft. Die dargestellten Mapping-Einträge repräsentieren die Zuordnungen zu Anlagenversionen, Status und Zuständigkeitsbereichen. Zuletzt können noch passende Zugriffsberechtigungen vergeben werden. In Abbildung 14 sieht man, dass insgesamt drei Aufrufe getätigt werden. Diese drei Aufrufe entsprechen den drei benötigten Transaktionen.

6.5.2 Löschen eines Dokuments

Um ein Dokument zu löschen, muss lediglich eine einzige Transaktion ausgeführt werden. Diese markiert im Struct `Dokument` das jeweilige Dokument anhand seines Hash-Werts als gelöscht. Der Hash-Wert und die Metadaten bleiben aber Teil der Blockchain, da eine komplette Löschung nicht möglich wäre. Ein fehlerhaft gespeichertes Dokument behält also seinen digitalen Stempel auch nach dem Löschvorgang. Allerdings wird dieser ohne das Dokument nur schwer auffindbar sein.

Abbildung 15 zeigt den kompakten Löschvorgang als Sequenzdiagramm. Wenn gewünscht, könnten zusätzliche Zugriffsprüfungen erfolgen, so dass Dokumente bspw. nur von den Institutionen gelöscht werden dürfen, welche für deren Erstellung verantwortlich waren. Zudem kann sichergestellt werden, dass Dokumente nach Genehmigung nicht mehr gelöscht werden können.

6.5.3 Aktualisieren eines Dokuments

Wird ein Dokument aktualisiert, so wird für die neue Version ein neuer Hash angelegt. Da der Hash der vorherigen Version nur bekannt ist, wenn die vorherige Version vorhanden ist,

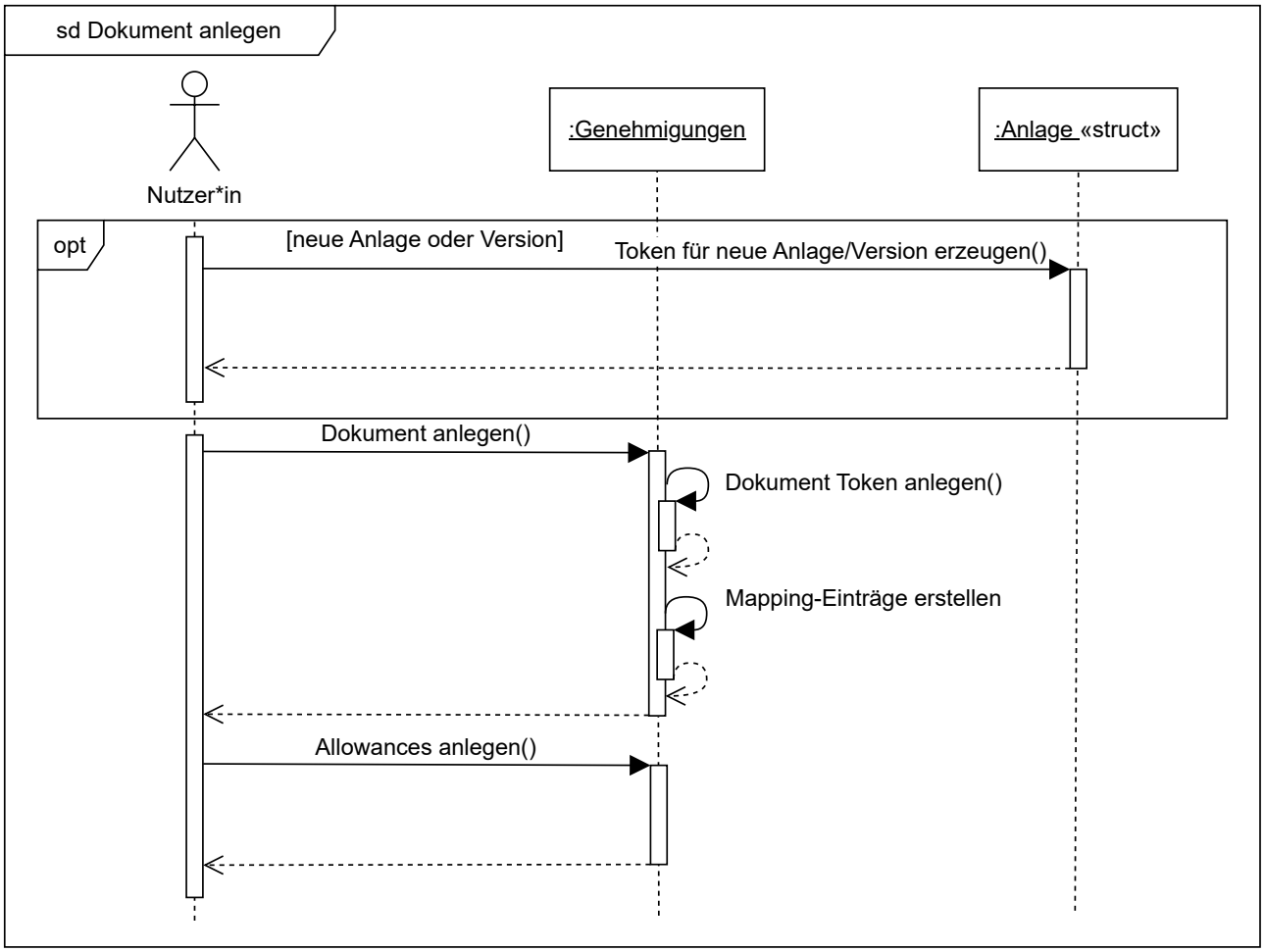

Abbildung 14: Sequenzdiagramm über das Anlagen eines Dokuments.

kann der Datensatz der vorherigen Version nicht immer ohne Weiteres identifiziert werden. Für diesen Fall wird empfohlen eine Aktualisierung immer mit zwei Schritten durchzuführen: zunächst wird die ursprüngliche Version gelöscht und danach die neue Version angelegt. Die ursprüngliche Version wird auf der Blockchain aber lediglich als gelöscht markiert und sollte diese noch im Umlauf sein, wird dies dadurch von Nutzenden erkannt.

Da vor allem in der ersten Version mit Cloud-Lösung nicht garantiert werden kann, dass alle bei einer Aktualisierung immer die Dateien überschreiben, ist dieser Ansatz auch sinnvoll für die Konsistenz. Nutzende könnten auch manuell eine Datei zunächst löschen bevor eine neue hochgeladen wird. Ebenfalls könnte eine neue Version einen neuen Namen besitzen, wodurch das Update auch nicht mehr automatisch zuordenbar wäre. Wenn eine Aktualisierung generell als Löschen und Erstellen gehandhabt wird, ist die Logik der Software immer konsistent.

Sollte ein Dokument aktualisiert werden, nachdem dieses genehmigt wurde, darf eine Löschung der genehmigten Version sowieso erst erfolgen, wenn die neue Version genehmigt wurde. Demnach wäre auch eine Aktualisierung nicht zulässig. In diesem Fall wird die neue Version einfach

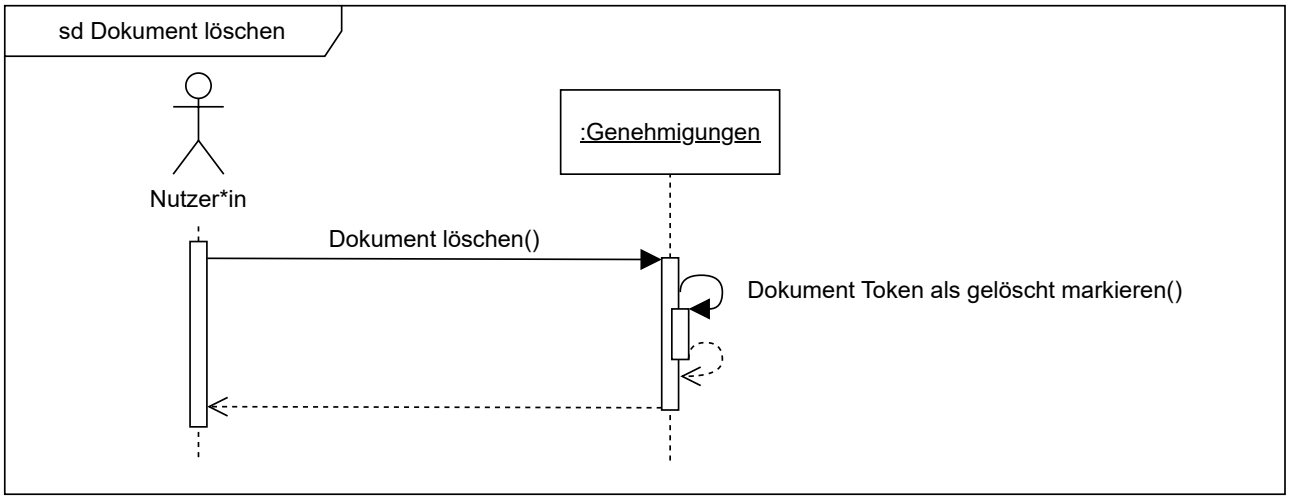

Abbildung 15: Sequenzdiagramm über das Löschen eines Dokuments.

neu angelegt und die alte bleibt weiterhin als letzte gültige Version auf der Blockchain gespeichert.

6.5.4 Aktualisieren des Status einer Anlage

Sobald eine neue Anlagenversion genehmigt wurde, wird die aktuell genehmigte Version der jeweiligen Anlage aktualisiert. Somit ist immer eindeutig erkennbar, ob sich ein Dokument auf die zuletzt genehmigte Anlagenversion bezieht.

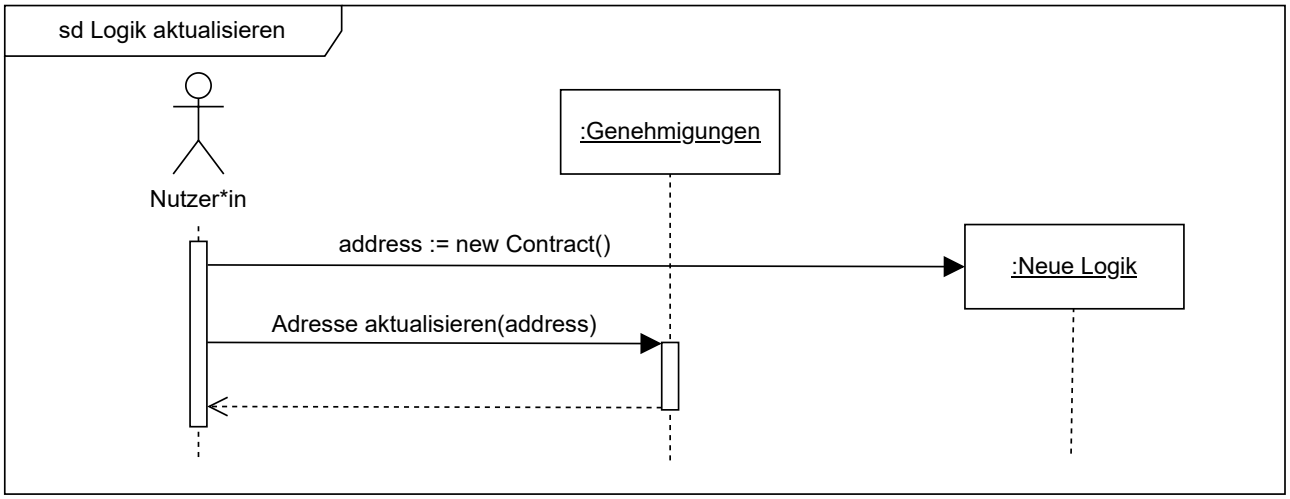

Abbildung 16: Sequenzdiagramm über das Aktualisiern des Logik-Contracts.

6.5.5 Durchführung eines Upgrades der Smart Contract Logik

Muss irgendwann der Logik-Contract aktualisiert werden, so kann dies mithilfe des angewandten Proxy-Delegation Patterns durchgeführt werden. Dafür muss zunächst der neue Logik-Contract auf der Blockchain initialisiert werden. Anschließend wird im Proxy-Contract die Adresse des

Logik-Contracts auf die neue Adresse, des zuvor initialisierten Contracts abgeändert. Abbildung 16 zeigt diesen Ablauf in Form eines Sequenzdiagramms. Sofern der vorherige Logik-Contract eine Funktion zum Löschen besitzt, kann dieser nun gelöscht werden. Da die Ethereum Foundation von einer Löschfunktion abrät und dies in Zukunft auch deaktivieren möchte, sollte darauf verzichtet werden (Ballet et al., 2022). In diesem Fall sind also zwei Transaktionen nötig.

7 Bewertung und Handlungsempfehlungen

Um eine Bewertungsmatrix über die Vorteilhaftigkeit bzw. Nachteiligkeit von Blockchain Technologien zu erstellen, muss das erarbeitete Konzept mit herkömmlichen Ansätzen verglichen werden. In diesem Fall wird sowohl der IST-Zustand als auch eine digitale Lösung betrachtet. Der IST-Zustand bezieht sich dabei immer auf den aktuell meist gelebten Ansatz mit Papier-Anträgen und -Archivierungen. Für den Vergleich mit herkömmlichen digitalen Systemen wird eine digitale Webanwendung zu Grunde gelegt. Diese basiert auf klassischen SQL-Datenbanken mit XML-Schnittstellen und gegenbenenfalls für die PDF-Dokumente passende Dokumentenenmanagement-Systeme. Um die Inhalte zusätzlich abzusichern werden digitale Signaturen verwenden – ähnlich dem Vorgehen bei BASF, wo die PDF-Dokumente digital signiert werden, bevor sie in einer Cloud abgelegt werden.

Wichtig zu bedenken ist, dass die Blockchain Technologie ein herkömmliches System nicht komplett ersetzt, sondern nur ergänzt, um zusätzliche Möglichkeiten zu erhalten. Die Vorteile, die eine herkömmliche SQL-Datenbank besitzt, lassen sich also auch im Blockchain-Konzept anwenden. Diese Bewertungsmatrix soll also darstellen, ob der zusätzliche Aufwand, der durch den Einsatz von Blockchain Technologien entsteht, zu rechtfertigen ist. Dafür wird nun geprüft, in welchen Punkten die Blockchain-Lösung Vorteile bietet, welche ein herkömmliches System alleine nicht bieten kann.

Tabelle 2 zeigt die Anforderungen aus Abschnitt 5.2.3, mit den Punktzahlen, welche die verschiedenen Konzepte erzielen. Die erreichbaren Punktzahlen sind $2, 1, 0, -1$, und -2, wobei 2 viele Vorteile und -2 viele Nachteile repräsentiert. Diese Punkteverteilung erfolgt zunächst ohne Gewichtung und alle Entscheidungen werden begründet. Danach erfolgt eine beispielhafte Gewichtung, um einen Eindruck zu vermitteln, ob der Einsatz von Blockchain-Technologien vorteilhaft ist.

Bezüglich der Manipulationssicherheit gewinnt ganz klar das Blockchain-Konzept. Die Blockchain Technologie ist für seine Manipulationssicherheit bekannt und in Kombination mit Smart Contracts lassen sich Dokumente und Daten eindeutig absichern. Eine Manipulation wird sofort bemerkt, da der hinterlegte Hash nicht mehr übereinstimmen würde. Dies schreckt ab vor potentiellen Manipulationsversuchen und bedarf einer Übernahme von mindestens 50% der Blockchain-Knoten, um erfolgreich zu sein. Selbst dann wüssten allerdings die noch nicht gekaperten Knoten über die Manipulation Bescheid. Der Papier-Ansatz ist hier auf dem zweiten Platz, da die Verwendung von zwei exakten Ausfertigungen an unterschiedlichen Archiv-Orten, eine Manipulation stark erschwert. Lediglich im Falle von Naturkatastrophen und Verlust eines der beiden Dokumente wäre eine Manipulation einfacher durchzuführen. Beim digitalen Ansatz kann eine Manipulation – bspw. durch Administratoren der Software – nur schwer verhindert werden.

Tabelle 2: Bewertungsmatrix anhand der definierten Anforderungen.

ID	Kurzform	Blockchain	Digital	Papier
A1	Manipulationssicherheit	2	0	1
A2	Datenschutz	-1	1	2
A3	Reduzierung Verwaltungsaufwand	0	2	-2
A4	Nachhaltigkeit	1	2	-2
A5	Rechtliche Dokumentation	2	0	0
A6	Verfügbarkeit	2	1	-2
A7	Schnittstellen	2	2	-2
A8	PDF Kompatibilität	2	2	2
A9	KMU Kompatibilität	1	2	1
A10	Schutz der Betriebsgeheimnisse	0	0	2
A11	Nebenbestimmungs-Management	1	1	-2
A12	Bezahlung	2	0	-1
A13	Strukturierte Daten	2	2	-2
A14	Erweiter- und Wiederverwendbarkeit	2	0	-2
A15	Transparenz	2	1	-2
	Summe	**20**	**16**	**-9**

Datenschutz ist bei der Papier-Version am einfachsten, da die Dokumente nur auf Papier archiviert werden und nicht automatisch durchsuchbar sind. Natürlich erfolgen hier teilweise elektronische Scans, die dann natürlich wieder abgesichert werden müssen. Bei der digitalen Version können jegliche personenbezogenen Daten gespeichert aber auch wieder gelöscht werden, was einen Vorteil gegenüber der Blockchain Technologie darstellt. Bei Blockchain-Technologien muss auf personenbezogene Daten verzichtet werden, da diese nach informationellen Selbstbestimmungsrecht jederzeit löschbar sein müssen. Da dies nicht möglich ist, ist dies als Nachteil zu werten, da hier extra auf die manipulationssichere Speicherung verzichtet werden muss.

Ein digitales System reduziert den Verwaltungsaufwand gegenüber Papier enorm, da hier aufwändige Post-Zeiten wegfallen und keine Digitalisierung durch Einscannen mehr erfolgen muss. Zudem können die Daten teilweise automatisiert weiterverarbeitet werden, was wiederum vorteilhaft ist. Das digitale System mit Blockchain-Technologien zu erweitern behält zwar diese

Vorteile bei, allerdings steigt der Verwaltungsaufwand wieder etwas durch den zusätzlichen Hardware-Betrieb, der für die Blockchain notwendig wird. Somit wird die Blockchain-Lösung hier neutral bewertet.

Die Nachhaltigkeit wäre bei einem digitalen System am besten, da hier am wenigsten Hardware-Kosten und Betriebszeiten anfallen. Zudem fallen die Papier-, Druck- und Lagerkosten weg. Die Blockchain-Technologie schneidet minimal schlechter ab, da durch die zusätzliche Infrastruktur ein etwas höherer Energiekonsum erzeugt wird. Allerdings lässt sich dieser durch die Wahl passender Konsensmechanismen wie bspw. Proof-of-Authority in Grenzen halten. Die höheren Anschaffungskosten für die zusätzliche Hardware bleibt allerdings bestehen.

Bei der rechtlichen Dokumentation hat die Blockchain Technologie die meisten Punkte. Durch die Manipulationssicherheit und die Kombination diverse Kryptografieverfahren lässt sich diese rechtssichere Dokumentation korrekt umsetzen. Fristen, Zeitpunkte und Inhalte können hier sauber digital gespeichert werden und sind somit jederzeit verfügbar und überprüfbar. Ein Datums-Stempel auf einem Papier-Dokument lässt sich einfach ändern, ebenso wie die Änderung eines Zeitstempels in einer herkömmlichen SQL-Datenbank, weshalb sowohl das digitale System als auch die Papier-Variante hier neutral bepunktet werden.

Bei der Verfügbarkeit liegt die Blockchain-Technologie durch ihre hohe Dezentralität vorn. Selbst wenn die darüberliegende Cloud- oder Webanwendung ausfallen sollte, können Dokumente immer verifiziert werden. Dass die komplette Blockchain Infrastruktur ausfällt ist sehr unwahrscheinlich. Gegenüber einer Papier-Version hat eine digitale Anwendung den Vorteil, dass die Daten schneller verfügbar sind und einfacher gefunden werden können. Allerdings bleibt hier das Ausfallrisiko der Webanwendung selbst bestehen.

Bei den Schnittstellen bieten alle digitalen Systeme ähnliche Vorteile. Jedes digitale System kann Schnittstellen anbieten, um Daten zur Verfügung zu stellen. Bei der Papier-Version können hierbei nur Nachteile festgestellt werden.

Die PDF-Kompatibilität ist bei allen Ansätzen identisch. Die digitalen Daten können – sofern implementiert – einfach als PDF exportiert werden. Für die Papier-Version existieren üblicherweise sowieso schon PDF-Dokumente, die gedruckt wurden. Falls nicht, kann durch ein Scan ebenfalls ein PDF erstellt werden.

Bei der KMU-Kompatibilität hat die digitale Webanwendung die meisten Vorteile. Diese kann einfach von den Behörden betrieben werden und alle Institutionen – auch KMU – können diese verwenden. Da laut den Stakeholder-Gesprächen die Papier-, Druck- und Lagerkosten durchaus höher ausfallen können, hat die Papier-Version für KMU einen Nachteil gegenüber der digitalen Variante. Die Blockchain-Variante kann genauso gut abschneiden, wie ein digitales System, sollen allerdings alle Teilnehmer einen eigenen Knoten betreiben, so sind KMU hier

leicht benachteiligt oder benötigen unter Umständen einen Dienstleister. Deshalb wurden hier beim Blockchain-Konzept Punkte abgezogen.

Den größten Schutz der Betriebsgeheimnisse bietet die Papier-Version. Die Betreibenden können die Dokumente selbst zur zuständigen Behörde transportieren und dort werden die Papiere dann sorgfältig aufbewahrt. Im Falle einer Öffentlichkeitsbeteiligung liegen die Dokumente dann bei der zuständigen Behörde aus und können nicht digital eingesehen werden. Hier birgt sowohl die digitale Anwendung als auch die Blockchain-Lösung die gleichen Gefahren. Da in der Blockchain die Inhalte lediglich abgesichert, aber nicht direkt gespeichert werden, gibt es hier bei der Bepunktung keinen Unterschied. Ein digitales System, welches mit Bedacht implementiert wurde, kann allerdings Vorteile gegenüber eingescannten Papier-Dokumenten bieten.

Die Industriepartner wünschten sich ebenfalls Möglichkeiten für das Management von Nebenbestimmungen. Dies ist bei der Papier-Version garnicht möglich. Hier müssen die Nebenbestimmungen eingescannt oder anderweitig digitalisiert und in Zusatz-Systemen verwaltet werden. Ein digitales System kann hierbei Unterstützung leisten. Allerdings kann im Rahmen dieses Konzeptes nicht genau bewertet werden, ob weitere Vorteile abgesehen von einer Schnittstelle dafür geschaffen werden können.

Bezüglich der Bezahlung bietet der Blockchain-basierte Ansatz die Möglichkeit mit anderen Blockchains – wie bspw. dem digitalen Euro – kombiniert zu werden. So könnte eine Bezahlung mithilfe von Smart Contracts automatisiert werden. Dabei können bspw. auch versäumte Fristen in Form von Rabatten berücksichtigt werden. Die Papier-Version hat den Nachteil, dass die Rechnung auf dem Postweg deutlich länger dauert und dann unter Umständen für Finanzsysteme noch digitalisiert werden muss. Ein digitales System wurde hierbei neutral bepunktet, da es keine besonderen Vorteile über eine Automatisierung hinaus bzgl. Bezahlungen bietet.

Bei der Anforderung für strukturierte Daten unterscheiden sich Blockchain und herkömmliche digitale Systeme nicht. Welche Art von Daten auf der Blockchain abgesichert werden, spielt hierbei keine Rolle. Somit können sowohl unstrukturierte, semi-strukturierte als auch strukturierte Daten abgesichert werden. Ein herkömmliches digitales System unterstützt diese Art von Daten ebenfalls. Lediglich die Papier-Version kann nicht für strukturierte Daten genutzt werden.

Die Papier-Version bietet bzgl. der Erweiter- und Wiederverwendbarkeit ausschließlich Nachteile. Natürlich lässt sich ein Dokument zukünftig anders gestalten, allerdings bleiben die Daten immer unstrukturiert und können nicht über Schnittstellen mit digitalen Systemen verbunden werden. Die digitale Version lässt sich wie jeder andere Software ebenfalls erweitern, aber eher schlecht für andere Anwendungsfälle wiederverwenden. Bei der Blockchain-Lösung kann die Infrastruktur zusätzlich für andere Anwendungsfälle wiederverwendet werden. Somit wäre der Folge-Aufwand für weitere Blockchain-Projekte deutlich geringer. Das Proxy-Pattern lässt zu-

dem eine Erweiterung der Smart Contract Logik in Zukunft zu. Hierdurch bietet die Blockchain die Möglichkeit der Manipulationssicherheit inkl. der Flexibilität zukünftiger Erweiterungen wie herkömmliche digitale Anwendungen.

Die Transparenz ist ein Vorteil der Blockchain-Technologie, weshalb hier am meisten Punkte vergeben wurden. Zu gewissen Teilen lässt sich die Transparenz zwar auch in herkömmlichen Anwendungen nachahmen, allerdings wird sie durch den dezentralen Charakter der Blockchain Technologie fast schon erzwungen und kann auch zukünftig nicht entfernt werden. Papier bietet hier gar keine Transparenz, da das Papier beliebig innerhalb der Institutionen vervielfältigt und verteilt werden kann.

Tabelle 3 zeigt eine beispielhafte Gewichtung und deren Auswirkung auf die Gesamtpunktzahl. Dabei wurden vor allem die Anforderungen der Manipulationssicherheit, der Wahrung der Betriebsgeheimnisse und der Berücksichtigung von KMU sehr hoch gewichtet. Diese drei Anforderungen wurden in allen Stakeholder-Gesprächen sehr stark fokussiert, weshalb die Gewichtung so gewählt wurde. Natürlich ist die Gewichtung beliebig anpassbar und diese soll hier nur als Beispiel dienen.

Tabelle 3: Gewichtete Bewertungsmatrix anhand der definierten Anforderungen.

ID	**Kurzform**	**Gewichtung**	**Blockchain**	**Digital**	**Papier**
A1	Manipulationssicherheit	12	2	0	1
A2	Datenschutz	6	-1	1	2
A3	Reduzierung Verwaltungsaufwand	6	0	2	-2
A4	Nachhaltigkeit	5	1	2	-2
A5	Rechtliche Dokumentation	10	2	0	0
A6	Verfügbarkeit	7	2	1	-2
A7	Schnittstellen	4	2	2	-2
A8	PDF Kompatibilität	4	2	2	2
A9	KMU Kompatibilität	11	1	2	1
A10	Schutz der Betriebsgeheimnisse	12	0	0	2
A11	Nebenbestimmungs-Management	2	1	1	-2
A12	Bezahlung	1	2	0	-1
A13	Strukturierte Daten	8	2	2	-2
A14	Erweiter- und Wiederverwendbarkeit	7	2	0	-2
A15	Transparenz	5	2	1	-2
	Summe	**100**	**128**	**96**	**-22**

Sowohl die einfache als auch die gewichtete Bewertung zeigen, dass die Papier-Version in ihren Nachteilen überwiegt, weshalb hier dringend Abhilfe geschaffen werden muss. Gegenüber einer herkömmlichen digitalen Lösung bietet die Blockchain-Variante einige Vorteile, die den zusätzlichen Aufwand rechtfertigen. Der Ausbau und die Entwicklung einer passenden Infrastruktur stellt hierbei den größten Aufwand dar, welcher durch die Wahl eines geeigneten Dienstleisters erheblich reduziert werden kann. Vor allem die Manipulationssicherheit kann durch eine Blockchain-Lösung sehr stark erhöht werden, weshalb dies den Nachteil des erhöhten Aufwands aufwiegen kann. Die sehr hohe Wiederverwendbarkeit einer vorhandenen Infrastruktur relativiert dann im Laufe der Zeit die initialen Kosten. Durch die flexiblen Smart Contracts kann nahezu jeder Anwendungsfall von der Manipulationssicherheit profitieren.

8 Diskussion

Um die Forschungsfragen zu beantworten, wurde zunächst der IST-Zustand mittels Stakeholder-Gesprächen erhoben. Den Gesprächen lag ein semi-strukturierter Leitfaden mit offenen Fragen zu Grunde und je nach Gesprächsverlauf wurden zusätzliche vertiefende Fragen gestellt. Anhand der Gespräche wurde dann der IST-Zustand ermittelt aber auch die jeweiligen Anforderungen des Stakeholders erhoben. Hierbei wurde auf die Auflistung üblicher Softwareentwicklungs-Anforderungen verzichtet, um den Fokus auf die für diesen Anwendungsfall wesentlichen Anforderungen zu behalten. Diese Anforderungen wurden dann während der Konzipierung berücksichtigt.

Allgemein lassen sich zwei Modelle unterscheiden: ein dokumentenbasierter Dialog und ein datenbasierter Dialog. Ein dokumentenbasierter Dialog, welcher lediglich PDF-Dokumente austauscht, sollte nicht als Digitalisierung betrachtet werden, weshalb dies auch immer als elektronischer Ansatz bezeichnet wurde. Dies liegt unter anderem an den entstehenden Medienbrüchen. Ein datenbasierter Dialog würde den Medienbruch eliminieren, führt aber zu Herausforderungen im Bezug auf Manipulationssicherheit. In dieser Machbarkeitsstudie wurde allerdings dargestellt, wie mit Hilfe von Blockchain und DL-Technologien die Manipulationssicherheit gewährleistet werden kann.

Generell kann die Blockchain-Technologie für eine langfristige, rechtsverbindliche und vertrauliche Speicherung verwendet werden (F1)). Allerdings muss die DSGVO berücksichtigt werden, welche eine Löschung personenbezogener Daten erzwingt, sollten Betroffene Personen dies wünschen. Da eine vollständige Löschung innerhalb einer Blockchain nicht möglich ist, muss komplett auf die Speicherung personenbezogener Daten verzichtet werden. Zudem müssen Betriebsgeheimnisse zwingend geschützt werden, weshalb eine direkte Speicherung der Betriebsgeheimnisse ebenfalls nicht möglich ist (F2)). Dennoch können sowohl personenbezogene Daten als auch Betriebsgeheimnisse mit Hilfe der Blockchain abgesichert werden (F1), F2)). Hierfür werden Hash-Verfahren eingesetzt, welche nicht umkehrbar sind (vgl. Abschnitt 3.5.2). Somit können Daten immer verifiziert werden, indem der Hash geprüft wird, aber der Hash alleine erlaubt keinerlei Rückschlüsse auf das ursprüngliche Dokument.

Die Vermeidung der Speicherung von Betriebsgeheimnissen oder personenbezogenen Daten hat zur Folge, dass zusätzlich zur Blockchain noch andere Software-Systeme verwendet werden müssen, um die Daten abzuspeichern. Zur Sicherheit dieser Datenspeicher kann die Blockchain selbst keinen Beitrag leisten. Die Blockchain dient dann lediglich der manipulationssicheren Verifikation von Daten und Dokumenten. Sollte der Zugriff auf die richtigen Daten und Dokumente verloren gehen, kann auch mittels der Blockchain nicht mehr auf diese Daten zugegriffen werden. Die Implementierung eines sicheren und redundanten Datenspeichers ist also zwingend notwendig. Dieser Datenspeicher kann aber wie in Abschnitt 6.4.3 auf der DL Technologie ba-

sieren und mit einer Peer-to-Peer Datenbank gesichert werden (F2)). Der Vorteil wäre dann, dass die zugrundeliegende Blockchain volle Transparenz zur Verifizierung der Daten bietet, wohingegen die Daten selbst in der Peer-to-Peer Datenbank gespeichert werden. Die Peer-to-Peer Datenbank verteilt dabei die Daten nur auf die Knoten, die diese Daten benötigen oder besitzen, wodurch die Betriebsgeheimnisse nur beim jeweiligen Betreiber und den zuständigen Behörden verfügbar sind. Dadurch, dass immer eindeutig ist, wo sich die Daten befinden, können diese dann auch wieder gelöscht werden, was der wesentliche Unterschied zur Blockchain-Technologie ist.

Im Vergleich mit herkömmlichen Softwarelösungen wie bspw. SQL-Datenbanken und XML-Schnittstellen bietet die Blockchain-basierte Lösung erheblichen Mehrwert bei der Manipulationssicherheit (F3)). Wird das Gesamtbild betrachtet, so kann der Einsatz einer Blockchain auch für andere Anwendungsfälle Vorteile bringen. Prinzipiell kann jeder Anwendungsfall, der eine manipulationssichere Verifikation von Daten benötigt, profitieren. Somit muss auch die Wiederverwendbarkeit und Erweiterbarkeit einer Blockchain-Lösung bei der Entscheidung über den Mehrwert betrachtet werden. Im Gegensatz zu herkömmlichen Ansätzen kann die Blockchain Infrastruktur problemlos für viele verschiedene Anwendungsfälle gleichzeitig verwendet werden. Hier muss nicht für jeden Anwendungsfall eine eigene Infrastruktur geschaffen werden. Die Kosten für die Einrichtung einer solchen Infrastruktur werden also im Laufe der Zeit immer günstiger, umso mehr Anwendungsfälle umgesetzt werden. Durch den Einsatz von Smart Contracts kann für jeden Anwendungsfall immer eine passende Lösung geschaffen werden – natürlich unter Berücksichtigung der zuvor erläuterten Randbedingungen bzgl. der DSGVO. Diese Wiederverwendbarkeit relativiert die höheren intialen Aufwände.

Ein häufig diskutierter Nachteil, dass Smart Contracts nicht geändert werden können und somit keine Anpassung der Logik bei Gesetzesänderungen möglich ist, wurde durch das Proxy-Pattern umgangen (vgl. Abschnitt 6.2.2). Somit bleibt die Logik der Smart Contracts erweiterbar und anpassbar an zukünftige Anforderungen. Hierbei muss nur bedacht werden, dass die interne Struktur der Contracts identisch bleiben muss, um Daten-Überlappungen zu verhindern. Im schlechtesten Fall wären bei einer Logik-Änderung also ein paar nicht länger nutzbare Daten im Contract gespeichert.

Im Vergleich zu digitalen Signaturen bietet die Blockchain-Lösung ebenfalls erheblichen Mehrwert (F3)). Adobe Sign könnte bspw. auch über Schnittstellen mit herkömmlichen SQL-Datenbanken verbunden werden, allerdings können Datenbank-Inhalte immer durch System-Administratoren manipuliert werden. Auch wenn solch ein Manipulations-Szenario unwahrscheinlich wirken mag, können bspw. aufgrund extremer persönlicher Situationen solche Handlungen durchgeführt werden. Aber auch die Gefahr durch Malicious Insider muss bedacht werden (Weber et al., 2020). Durch den Einsatz von Blockchain-Technologien und Smart Contracts können keine Manipulationen erfolgen, selbst wenn ein Malicious Insider dies in Erwägung zieht. Für

eine Manipulation müssten dann über 50% der Blockchain unter Kontrolle des Angreifenden sein – und selbst dann wüsste die restliche Minderheit, dass eine Manipulation erfolgt ist. Einen Manipulationsversuch komplett unbemerkt durchzuführen, wäre nur möglich, wenn alle Knoten der gesamten Infrastruktur gekapert werden. Deshalb ist eine gute, dezentrale Infrastruktur besonders wichtig. Für den Aufbau dieser sollten möglichst viele Industriepartner, als auch Behörden einen Knoten in ihrem Rechenzentrum zur Verfügung stellen. Hierfür wäre auch eine konsortiale Blockchain Infrastruktur denkbar, welche aus vielen verschiedenen und unabhängigen Partnern besteht.

Die mangelnde Möglichkeit Daten von der Blockchain zu löschen, stellt eine Herausforderung bei konsortialen oder nationalen Blockchains dar. Sollten illegale Daten auf der Blockchain gespeichert werden, kann dies im schlimmsten Fall zur Abschaltung dieser führen. Deshalb müssen hier zusätzliche Sicherheitsmechanismen implementiert werden. Das Faucet aus Abschnitt 6.3.2 schafft hierbei Abhilfe und ermöglicht eine Datenprüfung vor der Speicherung. Bei zukünftigen weiteren Anwendungsfällen für die Blockchain, können jeweils für die einzelnen Fälle individualisierte Faucets implementiert werden. Die Faucets können dann auch sicherstellen, dass nur Smart Contracts des eigenen Anwendungsfalls beschrieben werden können. Der Faucet-Mechanismus bietet auch unzählige Möglichkeiten für Erweiterungen.

Der Aspekt integrierter Finanzflüsse und Bezahlmöglichkeiten wird ebenfalls durch Blockchain-Technologien ermöglicht. Entweder können auf der zugrundeliegenden Blockchain passende Smart Contracts implementiert werden, über welche eine Bezahlung umgesetzt wird. Oder zusätzliche externe Blockchains, welche zukünftig für Bezahlungen etabliert werden, können über Schnittstellen angeschlossen werden. Hier kann dann über Cross-Chain-Systeme anhand der Informationen in den Smart Contracts eine Bezahlung automatisiert werden.

Dennoch bleiben ein paar Nachteile und Limitierungen beim Einsatz von Blockchain-Technologien bestehen: Personenbezogene Daten und Betriebsgeheimnisse dürfen nicht direkt in einer Blockchain gespeichert werden, wegen der fehlenden Löschbarkeit. Fehlerhafte Inhalte können ebenfalls nicht vollständig gelöscht werden, sie sind immer in der Transaktionshistorie gespeichert. Ohne die zugehörigen Original-Daten sind Hashwerte allerdings nutzlos, wodurch zusätzlich zur Blockchain ebenfalls redundante – und im Idealfall dezentrale – Services geschaffen werden müssen, welche die Daten und Dokumente ausfallsicher aufbewahren. Die Manipulationssicherheit der Blockchain kann nur gewährleistet werden, wenn die Infrastruktur genügend dezentral aufgebaut wurde, wodurch die Hardware-Kosten insgesamt steigen. Die Kosten können durch geeignete Konsensmechanismen und häufige Wiederverwendung bezogen auf den Anwendungsfall wieder gesenkt werden.

Wenn eine Analyse des Schutzbedarfs von Anfang an einen hohen Bedarf an Manipulationssicherheit ergibt, dann ist der Einsatz einer Blockchain von Anfang an mit zu berücksichtigen. Besitzt die Anwendung einen geringeren Bedarf kann die Entwicklung der Anwendung herkömmlich

erfolgen und die Blockchain kann an den entsprechenden Stellen nachträglich eingebunden werden. Infrastruktur-Dienstleister können hierbei den Aufwand reduzieren: Werden bereits bestehende Blockchain-Infrastrukturen verwendet, fallen weniger zusätzliche Hardware-Kosten an und die gesamte Infrastruktur profitiert von der Wiederverwendung. Zudem spielt die Einführung einer Blockchain-Infrastruktur auch für das strategische Ziel Bayern als führendes Land im Bereich der Blockchain-Technologie zu etablieren, eine entscheidende Rolle.

9 Ausblick

Mit dieser Machbarkeitsstudie wurde der aktuelle IST-Zustand erhoben und Anforderungen aller beteiligten Stakeholder ermittelt. Dies bietet den Vorteil, dass ein umfassendes Gesamtbild kreiert werden konnte, für welches ein passendes Software-Konzept erstellt wurde. Mithilfe des Konzepts kann im Anschluss ein Demonstrator implementiert werden, welcher die Funktionsweise der Smart Contracts zeigt. Durch die Flexibilität der Nutzung dieser Contracts können im Anschluss beliebige Endanwendungen ergänzt werden, um den Prozess möglichst nutzerfreundlich zu unterstützen. Deshalb wird die Entwicklung des Demonstrators sehr empfohlen.

Mithilfe des Demonstrators lässt sich dann eine passende Infrastruktur auswählen. Hierfür sollten verschiedene Dienstleister ermittelt werden, um einen Vergleich mit den Kosten bei einem Neuaufbau zu ermöglichen. Viele Dienstleister betreiben die Infrastruktur allerdings in ihren eigenen Rechenzentren, was zu einer geringen Dezentralität führt. Deshalb sollten vor allem konsortiale oder nationale Blockchain Infrastrukturen wie bspw. die Hyperledger Besu Chain der govdigital berücksichtigt werden. Alle betrachteten Infrastrukturen sollten zudem Ethereum-basiert sein, um einen Vendor-Lock-In zu vermeiden.

Wurde eine passende Infrastruktur gefunden, müssen die Smart Contracts des Demonstrators für diese Infrastruktur noch einmal angepasst werden. Anschließend können die Smart Contracts dann dort eingesetzt werden. Als nächstes sollte nach weiteren Anwendungsfällen gesucht werden, welche von einer Absicherung der Daten und Dokumente profitieren. Der Demonstrator kann dafür dann als Vorlage genutzt werden, um andere Anwendungsfälle ebenfalls manipulationssicher umzusetzen.

Die einzelnen Teilnehmer müssen Wallets besitzen, um eine Blockchain-basierte Anwendung nutzen zu können. Dafür muss zunächst an die Betreiber und Behörden ein Wallet vergeben werden. Die einzelnen Institutionen können danach selbstständig für die Mitarbeitenden weitere Wallets generieren und die nötigen Allowances setzen. Hierfür muss die Endanwendung Unterstützung bieten, da eine manuelle Durchführung der nötigen Schritte nicht nutzerfreundlich ist.

Sobald die Entwicklung des digitalen Euros spezifiziert ist, kann dann ebenfalls über eine Integration nachgedacht werden. Durch die gute Wiederverwendbarkeit kann diese Integration dann für alle bereits etablierten Anwendungsfälle genutzt werden. Eine weitere Möglichkeit ist die Schaffung zusätzlicher Schnittstellen, um die benötigten Daten für das ISA-B Register und vergleichbare automatisiert zu extrahieren. Dies reduziert die manuellen Aufwände und vereinfacht die Prozessabläufe.

Quellenverzeichnis

Ballet, G., Buterin, V., & Feist, D. (2022). *EIP-4758: Deactivate SELFDESTRUCT* (Ethereum Request for Comments Nr. 4758). Ethereum Foundation. https://eips.ethereum.org/EIPS/eip-4758

Bogner, A., Littig, B., & Menz, W. (Hrsg.). (2009). *Interviewing Experts*. Palgrave Macmillan UK.

Braun, V., & Clarke, V. (2021). *Thematic Analysis: A Practical Guide*. SAGE.

BSI. (2023). Was ist der Prüfsummencheck? https://www.bsi.bund.de/dok/6599444

Cockburn, A. (2006). *Agile Software Development: The Cooperative Game (2nd Edition)*. Addison-Wesley Professional.

Entriken, W., Shirley, D., Evans, J., & Nastassia, S. (2018). *ERC-721: Non-Fungible Token Standard* (Ethereum Request for Comments Nr. 721). Ethereum Foundation. https://eips.ethereum.org/EIPS/eip-721

Fertig, T., & Schütz, A. (2019). *Blockchain für Entwickler: Grundlagen, Programmierung, Anwendung*. Rheinwerk Verlag.

Grigg, I. (2004). The Ricardian Contract. *Proceedings. First IEEE International Workshop on Electronic Contracting, 2004.*, 25–31. https://doi.org/10.1109/WEC.2004.1319505

Hajizadeh, M., Apostolou, D., Park, D., & Smith, C. (2023). Upgrading Smart Contracts. https://ethereum.org/en/developers/docs/smart-contracts/upgrading/

Hansen, T., & Eastlake 3rd, D. E. (2011). *US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)* (Request for Comments RFC 6234). Internet Engineering Task Force. https://doi.org/10.17487/RFC6234

Moriarty, K., Kaliski, B., Jonsson, J., & Rusch, A. (2016). *PKCS #1: RSA Cryptography Specifications Version 2.2* (Request for Comments RFC 8017). Internet Engineering Task Force. https://doi.org/10.17487/RFC8017

Radomski, W., Cooke, A., Castonguay, P., Therien, J., Binet, E., & Sandford, R. (2018). *ERC-1155: Multi Token Standard* (Ethereum Request for Comments Nr. 1155). Ethereum Foundation. https://eips.ethereum.org/EIPS/eip-1155

Rivest, R. L. (1992). *The MD5 Message-Digest Algorithm* (Request for Comments RFC 1321). Internet Engineering Task Force. https://doi.org/10.17487/RFC1321

Schlatt, V., Schweizer, A., Urbach, N., & Fridgen, G. (2016). Blockchain: Grundlagen, Anwendungen und Potenziale. https://publica.fraunhofer.de/entities/publication/dc9322f0-3063-4792-b69a-b2006982d857/details

Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets. *Extropy: Journal of Transhumanist Thought*, *16*.

Vogelsteller, F., & Buterin, V. (2015). *ERC-20: Token Standard* (Ethereum Request for Comments Nr. 20). Ethereum Foundation. https://eips.ethereum.org/EIPS/eip-20

Weber, K., Schütz, A. E., & Fertig, T. (2020). Insider Threats – Der Feind in den eigenen Reihen. *HMD Praxis der Wirtschaftsinformatik*, *57*(3), 613–627. https://doi.org/10.1365/s40702-020-00616-9

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungen

BImSchG	Bundes-Immissionsschutzgesetz
DL	Distributed Ledger
ERC	Ethereum Request for Comments
FT	Fungible Token
ICO	Initial Coin Offering
KMU	kleine und mittlere Unternehmen
KVB	Kreisverwaltungsbehörden
LfU	Bayerische Landesamt für Umwelt
MD5	Message-Digest Algorithm 5
NFT	Non-fungible Token
SHA	Secure Hash Algorithm
StMD	Bayerisches Staatsministerium für Digitales
StMUV	Bayerisches Staatsministerium für Umwelt und Verbraucherschutz
VCI	Verband der chemischen Industrie e.V.

Glossar

Allowance	Beschreibt die Erlaubnis eine Transaktion im Namen eines anderen Wallets durchführen zu dürfen. 12, 31, 32, 39, 57
Angriffsvektor	Der Weg oder die Methode, die Angreifer nutzen, um in Computersysteme einzudringen. 22, 42
AngularJS	Ein Javascript-basiertes Framework für die Implementierung von Web-Anwendungen. 19
Best-Practice	Optimal erprobte Methode oder Herangehensweise für effektive Ergebnisse. 23
Bug	Ein Fehler in einer Software, welcher jederzeit eintreten kann, sollte die entsprechende Stelle im Programm-Code aktiv werden. 11
Cross-Chain	Die Fähigkeit, Interaktionen oder Transfers von Werten zwischen verschiedenen unabhängigen Blockchain-Netzwerken zu ermöglichen. Dies kann den Datenaustausch und die Nutzung von Funktionen über verschiedene Blockchains hinweg erleichtern. 55
DSGVO	EU-Verordnung zum Schutz personenbezogener Daten, gültig seit Mai 2018. Regelt Datennutzung, Transparenz und Datenschutzstandards. 53, 54
ERC-721 Token	Standard für nicht-fungible Token (NFTs) auf der Ethereum-Blockchain. Ermöglicht die eindeutige Identifizierung und Darstellung individueller digitaler Vermögenswerte, wie z.B. digitale Kunstwerke oder Sammlerstücke. 12, 28, 29

Ether — Die native Kryptowährung der Ethereum-Blockchain. Wird für Transaktionen, Smart-Contract-Ausführung und Gebühren verwendet.. 37, 39

Faucet — Eine Software-Komponente, welche Zugriff auf ein Wallet mit Kryptowährungen besitzt und diese auf Anfrage – unter Einhaltung definierbarer Kritieren – automatisiert verteilt. 34, 37–39, 55, 60

Flag — Ein Flag bezeichnet einen Datentypen, welcher die Werte „Wahr" oder „Falsch" annehmen kann, um zu signalisieren, ob eine bestimmte Bedingung oder ein Zustand gilt. 28

Fork — Eine 1:1 Kopie des Zustands einer Blockchain bis zu einem bestimmten Zeitpunkt – definiert über die Blocknummer. 36

Gerichtsstand — Der rechtliche Ort, an dem ein Gerichtsverfahren stattfindet. Hier werden rechtliche Streitigkeiten behandelt und Urteile gefällt, basierend auf den geltenden Gesetzen und Zuständigkeiten.. 11

Hack — Eine unbefugte, oft illegale Handlung, bei der ein Angreifer Sicherheitsmechanismen überwindet, um auf Computersysteme, Netzwerke oder Software zuzugreifen. Dies kann zur Datenmanipulation, Informationsdiebstahl oder Beeinträchtigung der Systemintegrität führen. 11

Hyperledger	Ein Open-Source-Projekt und ein Dachverband für verschiedene Blockchain-Technologien und -Plattformen, die für Unternehmensanwendungen entwickelt wurden. 8, 27, 57
ISA-B	Das Register in Bayern, in welchem Anlagen, die von BImSchG betroffen sind, dokumentiert werden. 18, 19, 29, 42, 57
Java	Eine sehr weit verbreitete Programmiersprache, welche prinzipiell für alle Plattformen (Windows, Linux, etc.) verwendet werden kann. 19
Konsensmechanismus	Regelwerk oder Algorithmus in einer Blockchain, um Einigkeit über Transaktionen zu erzielen und dies ohne zentrale Kontrolle. 27, 49, 55
Lokalitätsprinzip	Alle relevanten Informationen zum Verständnis eines Zusammenhangs sollen an einer Stelle des Systems lokalisiert und möglichst ohne Kenntnis des Kontexts nachvollziehbar sein.. 22
Malicious Insider	Ein internes Individuum, das bösartig handelt und in einer Organisation, einem Unternehmen oder einer Einrichtung tätig ist. Dies kann dazu führen, dass sensible Informationen gestohlen, Systeme sabotiert oder andere schädliche Aktivitäten ausgeführt werden. 54

Mapping	Ein Datentyp der Programmiersprache Solidity, welcher ein Key-Value Paar darstellt. Der Value kann wiederrum ein Mapping sein. 31, 43
Metadaten	Daten, die Informationen über andere Daten liefern. Sie beschreiben Eigenschaften wie den Erstellungszeitpunkt, den Autor, den Dateityp und vieles mehr. Metadaten bieten Kontext und ermöglichen eine bessere Verwaltung und Organisation von Informationen, ob in Dateien, in Kommunikation oder in digitalen Ressourcen. 37, 43
Middleware	Eine Software-Zwischenschicht, die die Kommunikation und Interaktion zwischen verschiedenen Anwendungen oder Systemen erleichtert. Sie bietet standardisierte Schnittstellen und Dienste, um die Integration von Softwarekomponenten zu ermöglichen. 25, 34
Nebenbestimmung	Zusätzliche Regeln oder Bedingungen zur Verfeinerung einer Hauptvereinbarung. 19, 23, 24, 40, 50
NextCloud	Open-Source-Plattform für persönliche Cloud-Speicherung und -synchronisierung mit Dateifreigabe, Kalender und Kontaktfunktionen. 39
Off-Chain	Datenverarbeitung oder Transaktionen, die außerhalb der Hauptblockchain abgewickelt werden. Dies reduziert die Belastung der Blockchain und kann die Skalierbarkeit verbessern, indem Vorgänge außerhalb der Blockchain erfolgen. 11

Open-Source Ein Ansatz für Softwareentwicklung, bei dem der Quellcode öffentlich zugänglich ist. Dies ermöglicht es Entwicklern, den Code zu überprüfen, anzupassen und zu teilen. Open-Source-Software fördert die Zusammenarbeit, Transparenz und Innovation, da sie von einer Gemeinschaft von Entwicklern weltweit unterstützt und erweitert werden kann.. 27, 40

Peer-to-Peer Direkte Kommunikation und Ressourcenteilung zwischen Geräten ohne zentrale Serverinstanz. 9, 41, 42, 54, 60

Powershell Microsofts Skriptsprache für Systemautomatisierung und Befehlszeileninteraktion auf verschiedenen Plattformen. 34, 36

Proxy Vermittler zwischen zwei Komponenten, welcher Anfragen weiterleitet und die Sicherheit oder Leistung erhöht.. 33, 34, 45, 50, 54

REST API Kommunikation zwischen Software über standardisiertes HTTP, um Daten und Aktionen auszutauschen. 19

SQL Strukturierte Abfragesprache zur Verwaltung und Abfrage von Datenbanken. Ermöglicht das Erstellen, Ändern und Abrufen von Daten in relationalen Datenbanken durch klar definierte Anweisungen. 54

Terminal Eine textbasierte Benutzerschnittstelle in einem Computersystem, die es Benutzern ermöglicht, Befehle einzugeben und Textausgaben zu erhalten. Mit dem Terminal können Benutzer direkt mit dem Betriebssystem interagieren, Befehle ausführen, Programme starten und Systeminformationen abrufen. 36

Testnetz	Ein Experimentier- und Entwicklungsumfeld in der Blockchain, das risikofreies Testen von Anwendungen ermöglicht, ohne echte Kryptowährungen zu verwenden. 37
Token	Digitale Einheit auf einer Blockchain, repräsentiert bspw. Vermögen oder Rechte, verwaltet durch Smart Contracts. 12–14, 27, 28, 30, 31, 43
Transaktionsgebühr	Kosten für die Durchführung einer Transaktion in einer Blockchain, deckt Verarbeitungs- und Validierungskosten ab. 29, 37, 39
UML	Ist die Unified Modelling Language. Eine semi-formelle Notation für die Erstellung technischer Software-Diagramme. 26, 43, 60
Upgradeability	Beschreibt die Möglichkeit, die Logik eines Smart Contracts zu aktualisieren ohne seinen Zustand und Speicher zu verlieren.. 33
URI	Kennzeichnung zur Identifizierung von Ressourcen im Internet, wie Webseiten oder Dateien. 29
Vendor-Lock-In	Eine Situation, in der ein Kunde aufgrund von technischen oder vertraglichen Abhängigkeiten an einen bestimmten Anbieter gebunden ist. Dadurch kann es schwer sein, zu einem anderen Anbieter zu wechseln, was die Flexibilität einschränkt und langfristige Kosten erhöhen kann. 27, 57
Wallet	Eine digitale Anwendung oder Dienst, um Kryptowährungen sicher zu speichern, zu verwalten und zu übertragen. 28–31, 37, 39, 57
XML	Textbasierte Sprache für strukturierte Datendarstellung, ermöglicht maschinenlesbare und menschenverständliche Informationen. 54

Öffentlichkeitsbeteiligung	Ab einer gewissen Menge von Auswirkungen muss die Öffentlichkeit bei einer Anlagen-Genehmigung beteiligt werden, bevor eine Entscheidung getroffen werden darf. 19, 50

Einführung eines strukturierten Nachrichtenformats

Da im Rahmen der Digitalisierung von Genehmigungsanträgen strukturierte Daten empfohlen werden, muss eine passende Vorgehensweise definiert werden, um diese Strukturierung zu etablieren. Nachfolgend wird beispielhaft aufgezeigt, wie dies erreicht werden kann. Hierbei wurden die Vorgaben von XÖV[2] berücksichtigt.

Motivation Die Nutzung strukturierter Nachrichten ermöglicht eine weitergehende Automatisierung der Prozesse. Die damit einhergehende Automatisierungsmöglichkeit führt zu mehr Effizienz und damit schnelleren Prozessen. Zusätzlich werden die Daten Prüfbar bzgl. ihrer Plausibilität. Die verwendeten Datentypen können automatisiert geprüft und damit Fehler erkannt werden. Das erhöht die Zuverlässigkeit sowie Stabilität der Prozesse und führt zu einer Beschleunigung der Prozesse. Fehler werden oftmals schon beim Verursacher erkannt und können dort behoben werden.

Allgemeines Vorgehen Prinzipiell gibt es zwei Szenarien:

- Fachgesetzgebung: Im Falle z. B. von XMeld ist es der Normengeber, der die Standardisierung durchführt und den erzeugten Standard durchsetzt. Die Verpflichtung zur Nutzung eines Standards ist das stärkste und effizienteste Mittel zur flächendeckenden Nutzung eines Standards.
- Interessensgemeinschaft: In anderen Fällen wird ein Standard von einer Gruppe initiiert, die durch die gemeinsame Nutzung eines Standards effizienter zusammenarbeiten wollen. Eine Nutzung eines solchen Standards basiert auf Freiwilligkeit.

Ein Nachrichtenformat soll die Prozesse optimal unterstützen. Die Qualität des Standards entscheidet damit über seinen Nutzen. Daher empfiehlt es sich eine Expertengruppe zu bilden, in der Wissensträger aus allen relevanten Bereichen und Institutionen mitarbeiten. Somit sollten sowohl Rechtsexperten als auch technische Experten mitarbeiten. Eine Analyse der Stakeholder kann bei der Bildung der Expertengruppe hilfreich sein. Bereits in dieser frühen Phase ist es wichtig „über den Tellerrand" zu schauen. Gibt es bisher nicht betrachtete Stellen, an die zumindest ein Teil der Daten weitergeleitet werden sollten? Nur wenn möglichst alle Interessierten an der Entwicklung mitarbeiten, können spätere Anpassungen weitgehend vermieden.

Nach der Bildung der Expertengruppe gilt es ein Pflegekonzept (auch Betriebskonzept genannt) auszuarbeiten. Dieses Konzept soll sicherstellen, dass eine dauerhafte Pflege und Weiterentwicklung organisatorisch und finanziell gesichert sind. Damit ist ein erste Schritt getan, wie er in den Regeln zur XÖV konformen Standardisierung beschrieben wird:

[2] http://xoev.de/

K-1 (MUSS) Standard der öffentlichen Verwaltung: „Eigentümerin" des XÖV-Standards muss die öffentliche Verwaltung sein, d.h. sie bestimmt seine Inhalte und hat alle Rechte am Standard inne. Weiter entscheidet sie über Entwicklung und Pflege sowie über die Verwendung des Standards.

K-2 (MUSS) Freie Verwendung: Der XÖV-Standard muss frei von Rechten Dritter sein. Er muss innerhalb der öffentlichen Verwaltung der Bundesrepublik Deutschland und für die Nutzer ihrer Dienstleistungen uneingeschränkt und unentgeltlich verwendbar sein und bleiben.

K-3 (MUSS) Dokumentation: Ein XÖV-Standard muss alle Informationen bereitstellen, die erforderlich sind, um eine standardkonforme Schnittstelle für IT-Verfahren zu entwickeln. Er ist in Form von XML-Schema-Dateien und deren konsistenter Dokumentation an seine Nutzer auszuliefern.

K-4 (MUSS) Veröffentlichung: Die Zertifizierung ist ausschließlich über das XRepository zu beantragen. Der Standard muss mit seiner Dokumentation als PDF-Datei, seinen XML-Schema-Dateien, einer XMI-Repräsentation seines XÖV-UML-Modells sowie seinem Pflegekonzept nach erfolgter Zertifizierung unverzüglich im XRepository veröffentlicht werden.

K-5 (MUSS) Nachhaltigkeit des Standards: Für den XÖV-Standard muss ein Pflegekonzept vorliegen, aus dem erkennbar ist, dass ein langfristige Wartung und Fortschreibung gewährleistet wird.

Auskunftspflichten beziehen sich auf Kriterien, bei denen die Verantwortlichen eines Standards Informationen zu ihrem Vorhaben aufbereiten und an die XÖV-Koordination übermitteln. Diese Informationen dienen im Wesentlichen der Transparenz zu Inhalten und Rahmenbedingungen des Standardisierungsvorhabens für die XÖV-Koordination, aber auch für Dritte, um die Wiederverwendung fachlicher Datenschnittstellen zu fördern.

K-6 (SOLL) Anzeige der Entwicklungsabsicht: Der Beginn der Entwicklung eines Standards soll der XÖV-Koordination so früh wie möglich nach der Identifizierung des Bedarfs angezeigt werden.

K-7 (MUSS) Informationen zum Status Quo des Standards: Die für die Entwicklung und die Pflege des Standards zuständige Stelle (Organisationseinheit der öffentlichen Verwaltung) muss den Projektsteckbrief ausfüllen und an die XÖV-Koordination übermitteln. Bei relevanten Änderungen muss die zuständige Stelle den Steckbrief aktualisieren.

Die technischen Kriterien der XÖV-Konformität beziehen sich auf das XÖV-UML-Modell – D.h. Prozesse und Datenstrukturen in UML 2.x Notation – und seine Darstellung in XML-Schema. Diese Kriterien sind weitestgehend automatisiert überprüfbar. Die XÖV-konforme Generierung

der XML-Schemata aus dem XÖV-UML-Modell und die automatisierte Überprüfung der technischen Kriterien sind in dem XÖV-Produktionszubehör – insbesondere im XGenerator und den XÖV-XSD-Vorlagen – implementiert, das in die Produktionsumgebung eines jeden XÖV-Vorhabens zur Erstellung eines XÖV-Standards integriert sein muss.

K-8 (SOLL) Modellierung der Prozesse in UML: Die verteilten Datenverarbeitungsprozesse, in denen die durch den XÖV-Standard spezifizierten Nachrichten ausgetauscht werden, sollen unter Verwendung von UML 2.x als Aktivitätsdiagramme beschrieben werden.

K-9 (MUSS) Modellierung der Datenstrukturen in UML: Die Modellierung der Datenstrukturen des XÖV-Standards muss unter Verwendung von UML 2.x als Modellierungssprache erfolgen.

K-10 (MUSS) Einhaltung der XÖV-Namens- und Entwurfsregeln: Für XÖV-Standards müssen die von der XÖV-Koordination herausgegebenen XÖV-Namens- und Entwurfsregeln entsprechend ihrer Verbindlichkeit verwendet werden. Das schließt die Verwendung des von der XÖV-Koordination veröffentlichten XÖV-Profils für UML in der zum Zeitpunkt der Konformitätsprüfung jeweils aktuellen Fassung ein.

K-11 (SOLL) Nutzung von XÖV-Kern- und Fachkomponenten: Die durch die XÖV-Koordination im XRepository veröffentlichten XÖV-Kern- und Fachkomponenten sollen im XÖV-UML-Modell wiederverwendet werden.

K-12 (SOLL) Nutzung der XÖV-Basisdatentypen: Die von der XÖV-Koordination herausgegebenen XÖV-Basisdatentypen sollen im XÖV-UML-Modell verwendet werden.

K-13 (SOLL) Nutzung von Codelisten: Die von der XÖV-Koordination empfohlenen und im XRepository bereitgestellten Codelisten sollen verwendet werden.

K-14 (MUSS) Erfolgreiche Verarbeitung des XÖV-UML-Modells durch das XÖV-Produktionszubehör: Das XÖV-UML-Modell muss fehlerfrei durch das von der XÖV-Koordination herausgegebene XÖV-Produktionszubehör in der zum Zeitpunkt der Konformitätsprüfung jeweils aktuellen Fassung verarbeitet werden können. Dies beinhaltet die fehlerfreie Erzeugung der XML-Schemata.

K-15 (SOLL) Nutzung einer sicheren Infrastruktur für den elektronischen Datenaustausch: Die öffentliche Verwaltung entwickelt und betreibt Infrastrukturkomponenten, die sich an sicheren elektronischen Diensten (Secure Web Services) orientieren. Neben der dafür erforderlichen Standardisierung elektronischer Dienste auf fachlicher Ebene ist vor allem auch die Sicherheit bei der Inanspruchnahme und Erbringung der Services zu gewährleisten. Methodische und technische Grundlagen der fachlichen Standardisierung und der Infrastrukturkomponenten sind aufeinander abgestimmt.

Die Wirtschaftlichkeit von Infrastrukturkomponenten ist umso höher, je größer die Zahl der Nutzer ist. Aus diesem Grunde, und wegen der abgestimmten Weiterentwicklung fachlicher und sicherheitstechnischer Standards im Sinne sicherer elektronischer Dienste, empfehlen die OSCI-Leitstelle Bremen und das Bundesministerium des Innern (BMI) die angemessene Nutzung der von der öffentlichen Verwaltung entwickelten Infrastrukturkomponenten. Ein XÖV-Standard soll daher, zur Erfüllung der in dem jeweiligen fachlichen Kontext notwendigen Sicherheitsanforderungen, die von der öffentlichen Verwaltung entwickelten Lösungen in angemessenem Umfang berücksichtigen:

- Public-Key Infrastruktur PKI-1 Verwaltung
- Übertragungsstandard OSCI-Transport
- Service-Registry DVDV

Detaillierte Überlegungen zur Anwendung von DLT

Heinz-Günter Lux von Evonik Digital GmbH hat bereits im Vorfeld dieser Machbarkeitsstudie einige DLT Projekte durchgeführt. Seine Erfahrungen und Empfehlungen sind in die folgenden Überlegungen eingeflossen. Diese Überlegungen können zur Umsetzung von "Version 3: Peer-to-Peer Datenbank" verwendet werden und sollen nochmal etwas anschaulicher darstellen, wie diese Version gestaltet werden kann.

Herr Lux betrachtete dabei folgende drei Bausteiner einer Blockchain: die Verschlüsselung, das Hashen und die dezentrale Validierung (Proof Mechanismus). Die DLT kann ebenfalls Verschlüsselung und Hashen anbieten. Im Business-to-Business (B2B) Bereich spielt die dezentrale Validierung eine untergeordnete Rolle, weil zwischen den Organisationen alles auf Grundlage von Verträgen oder Gesetzen geregelt wird. Die Vertraulichkeit ist hier allerdings besonders wichtig und wird durch geeignete Verschlüsselung der relevanten Daten ermöglicht. Dabei sollten die Daten auch nur auf den Knoten der beteiligten Parteien liegen und nicht dezentral auf allen Knoten.

Überträgt man diese Überlegung auf den Bereich der Genehmigungsverfahren, so bleiben Betriebsgeheimnisse durch Verschlüsselung nach außen hin geschützt und durch die ausschließliche Speicherung in den beteiligten Knoten deutlich weniger exponiert. Dennoch spielt im Fall der Genehmigungsverfahren die Manipulationssicherheit und deren Überprüfbarkeit durch dritte Parteien eine große Rolle. Behörden müssen bspw. sicherstellen, dass keine Manipulation vorleigt. Deshalb werden die Inhalte zusätzlich auf unterster Ebene mit Hilfe einer Blockchain abgesichert. Somit kümmert sich DLT um die Verschlüsselung der konkreten Daten und die Blockchain um die dezentrale Validierung und Inhaltssicherung.

Herr Lux befürwortet grundsätzlich den Datendialog gegenüber einem Dokumentendialog. Der Ablauf wurde folgendermaßen beschrieben:

- Die Zentralbehörde stellt den Smart Contract auf der Blockchain zur Verfügung und kümmert sich um dessen Wartung.
- Der Smart Contract ersetzt somit das Antrags-Formular.
- Die Datenfelder werden funktionalisiert und die Daten werden kategorisiert: Betriebsgeheimnis, Öffentlich, Teilbar mit anderen Behörden, etc.
- Das Need-to-Know Prinzip wird eingehalten und die Daten liegen verschlüsselt nur in den Knoten der Beteiligten. Zudem wird ein technisches Vier-Augen-Prinzip angewandt, so dass registrierte Daten niemals einseitig geändert oder gelöscht werden können.
- Der Genehmigungsdialog erfolgt mittels strukturierter Daten über den Smart Contract.
- Zur Echtheitsprüfung der Daten zusätzliche Hashwert-Validierung in einer Blockchain.

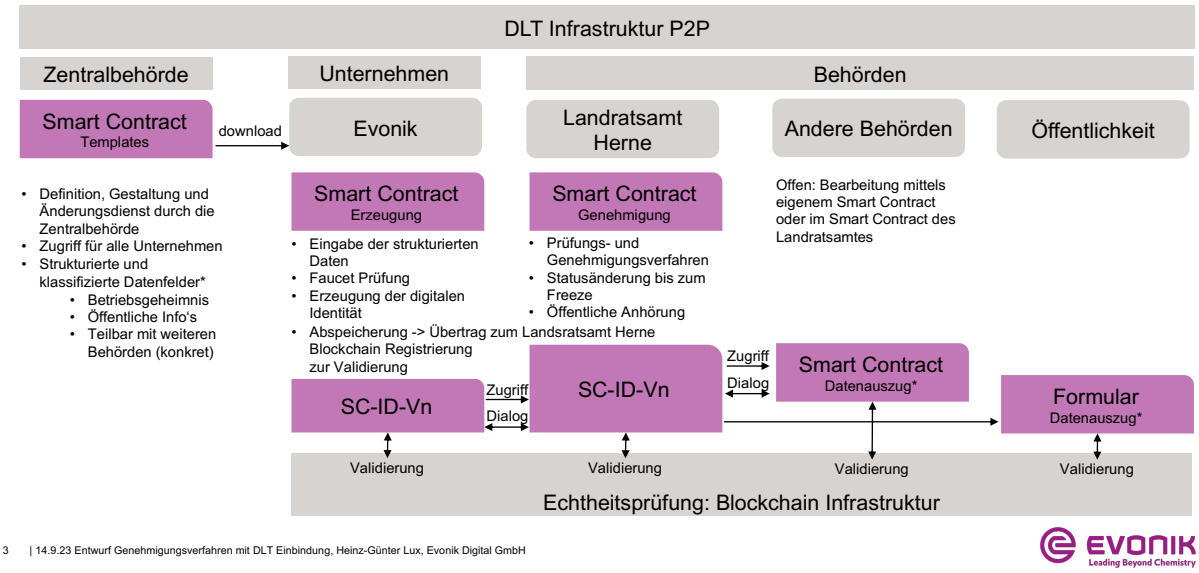

Abbildung 17: Genehmigungsverfahren mit DLT Einbindung

- Teilen der Daten getriggert durch die funktionalisierten Datenfelder.
- Veröffentlichung mittels definierter Fomulare, deren Inhalte aus der DLT gefüttert werden basierend auf den Kategorien. Dadurch entfällt das manuelle Schwärzen.

Abbildung 17 zeigt die Zusammenhänge noch einmal in visueller Form. Der beschriebene Ansatz wurde in der Mail vom 18.09.2023 von Herrn Lux in der Arbeitsgruppe zu den Genehmigungsverfahren geteilt. Zur vollständigen Dokumentation dieses Projekts, wurden die Inhalte aufgegriffen und in diesem Anhang eingearbeitet.

Entwicklung des Demonstrators

Im Rahmen des Projekts wurde ein Demonstrator implementiert, welcher die Machbarkeit des vorgestellten Konzepts aufzeigen soll. Der Demonstrator stellt dabei keine vollfunktionsfähige Lösung dar, sondern lediglich ein Proof-of-Concept. Um den Fokus zu gewährleisten, wurden lediglich kleine Workflows für den Demonstrator ausgewählt und das Hauptaugenmerk auf die Interaktion mit der Blockchain und dem Smart Contract gelegt. Für den Demonstrator wurde der Dokumentenbasierte Dialog gewählt, auch wenn die Arbeitsgruppe im Allgemeinen die Implementierung eines Datenbasierten Dialogs befürwortet. Der dokumentenbasierte Dialog ermöglicht allerdings jeder Person, einfach und übersichtlich die Machbarkeit auszuprobieren und Hashwerte im Smart Contract abzusichern. Die Ausrichtung des Demonstrators ist also komplett auf eine gute Veranschaulichung abgestimmt.

Der Demonstrator besteht aus insgesamt fünf Komponenten:

- Ein Smart Contract, welcher die Inhalte absichert.
- Eine Landingpage von der aus die Nutzerinteraktion startet und durch die einzelnen Ansichten leidet.
- Eine Ansicht für die Rolle des Betreibers von Anlagen zum Erstellen von Anlagen, Versionen und Dokumenten.
- Eine Ansicht für die Verifikation von Dokumenten, welche prüft, ob diese im Smart Contract hinterlegt sind.
- Eine Ansicht für die Rolle von Genehmigern und Genehmigerinnen, um Genehmigungsbescheide hochzuladen und zu sichern.

Bei der Entwicklung des Smart Contracts wurde darauf geachtet, alle vorgestellten Funktionalitäten des Konzepts testweise zu implementieren, um eine Aussage über die Machbarkeit treffen zu können. Ein paar Dinge mussten ergänzt oder angepasst werden – das Konzept wurde anschließend aktualisiert. Insgesamt lässt sich allerdings sagen, dass der Smart Contract wie geplant umgesetzt werden kann. Von Seiten der Blockchain-Technologie ist die Machbarkeit somit erfüllt. Es gilt allerdings zu beachten, dass die Proxy-Logik noch nicht umgesetzt wurde und das einige Standard-Interfaces, etc. vor einem produktiven Einsatz, umgesetzt werden müssen. Der Fokus war wie definiert nur auf ein Proof-of-Concept ausgelegt, nicht um den vorhandenen Contract produktiv zu schalten. Testfälle und Deployment-Skripte wurden ebenfalls angefertigt.

Das Frontend übernimmt die Logik, um Anlagen anzulegen, Versionen anzulegen und Dokumente auf der Blockchain abzusichern. Es werden keine Dokumente auf andere Server geladen, die Berechnungen finden alle lokal im Frontend statt. Dadurch müssen bei der Benutzung des

Demonstrators keine Bedenken vor Informationsverlust bestehen. Die berechneten Hashwerte werden aber korrekt in der Test-Blockchain der GovDigital abgesichert.

Um den Verwaltungsaufwand gering zu halten, wurde komplett auf ein Backend mit Serveranbindung verzichtet. Alle Daten liegen lokal im Browser. Werden die Daten im Browser gelöscht, bleiben lediglich die Hashwerte auf der Blockchain erhalten, die allerdings nicht umkehrbar sind und somit keine Rückschlüsse auf die durchgeführten Tests zulassen.

Der Demonstrator ist unter https://www.demonstrator-genehmigungswesen.h-d-gmbh-demo.de/ erreichbar und benötigt Basic Auth Zugangsdaten, welche beim Termin zum Projektabschluss verteilt werden. Werden die Zugangsdaten später benötigt, können diese bei Tobias Fertig (tobias.fertig@h-d-gmbh.de) erfragt werden.

Zusätzlich wurde im Projekt ein Block-Explorer angelegt, über welchen die Transaktionen eingesehen werden können. Dieser ist unter https://www.gdexplorer.h-d-gmbh-demo.de/ erreichbar und genötigt ebenfalls Basic Auth Zugangsdaten.

Interview-Leitfaden

Hier wird der Fragebogen, der den Stakeholder-Gesprächen zugrundelag dokumentiert. Der Fragebogen wurde nicht erzwungen sondern diente als grobe Orientierung. Wenn das Gespräch einen anderen Verlauf nahm, wurden spontan andere passende und ergänzende Fragen gestellt. Dabei wird im Fragebogen zwischen Kurzfragen (KF), Schlüsselfragen (SF) und Ergänzungsfragen (EF) unterschieden. EF wurden dabei nur gestellt, sollten sie bei der Beantwortung der SF nicht schon beantwortet worden sein.

Kurzfragen zum Stakeholder

KF1) Name, Position, Vertretung welches Stakeholders

KF2) Wie wird das System zum Genehmigungsprozess in der Organisation verwendet?

Prozess: IST-Zustand

SF1) Wie läuft der bisherige Prozess ab?

EF1) Ist der Prozess einheitlich für alle Arten von Anlagen?

EF2) Ist der Prozess nur für Chemie-Industrie einheitlich?

EF3) Was ist ein Minimalbeispiel?

EF4) Was ist ein Maximalbeispiel?

SF2) Welche Systeme sind im Prozess involviert?

EF5) Gibt es zusätzliche externe Abhängigkeiten?

SF3) Welche Akteure sind am Prozess beteiligt?

EF6) Was sind passive Akteure, die benachrichtigt werden?

EF7) Was sind aktive Akteure, die beteiligt sind?

Prozess: Wunsch-Zustand

SF4) Gibt es Änderungswünsche zum bisherigen Prozessablauf?

SF5) Welche Punkte des Prozesses sollten manipulationssicher abgelegt werden?

EF8) Sollen weitere externe Abhängigkeiten geschaffen werden?

EF9) Sollen weitere Systeme involviert werden?

EF10) Werden weitere Akteure benötigt?

Use Case

SF6) Beschreiben Sie die Use Cases, die vom System abgedeckt werden sollen.

EF11) Wird nur eine Dokumentation durch die Blockchain gewünscht?

EF12) Gibt es weitere Funktionalitäten, die wünschenswert sind?

SF7) Ist eine integrierte Bezahlung gewünscht? (Kryptowährung, Stable Coin, etc.)

SF8) Müssen zusätzliche Prozesse neben der Genehmigung beachtet werden?

EF13) Spielt die Wartung und Instandhaltung ebenfalls eine Rolle?

SF9) Soll das System für Genehmigungen maßgeschneidert werden?

Governance

SF10) Was muss bei einer Änderung des Prozesses beachtet werden?

EF14) Wird eine Anpassung des Contracts gewünscht?

SF11) Wie soll der Zugriff auf ältere Versionen ermöglicht werden?

Vertrauen

SF12) Gibt es Vertrauensprobleme bei der Eingabe der Daten?

SF13) Gibt es Vertrauensprobleme bzgl. rückwirkender Manipulation?

SF14) Bzgl. welchen Daten des Prozesses liegen Vertrauensprobleme vor?

Transparenz

SF15) Wer soll welche Daten lesen können?

SF16) Wer soll welche Daten schreiben können?

Zugriffsverwaltung

SF17) Wer soll an Versions-Updates berechtigt sein?

EF15) Wer kümmert sich um die Wartung der Server/Knoten?

EF16) Wer trägt die Verantwortung für den Betrieb?

Datensicherung und Datenschutz

SF18) Welche Anforderungen an die Datensicherung bestehen?

EF17) Wie lange ist die Aufbewahrungspflicht?

EF18) Wie viele Anträge werden im Schnitt pro Jahr gestellt?

SF19) Was soll mit den bisherigen Anträgen geschehen?

EF19) Müssen die Anträge ebenfalls in das neue System aufgenommen werden?

SF20) Gibt es datenschutzrechtliche Bedenken bzgl. Konkurrenz oder Spionage?

SF21) Müssen personenbezogene Daten abgespeichert werden?

Betrieb

SF22) Gibt es technische Anforderungen zum Deployment, Hosting, etc.?

EF20) Gibt es technische Einschränkungen?

SF23) Gibt es spezielle Anforderungen an die Wahl der Technologie/Programmiersprache

Termine

Hier wird eine Übersicht über die erfolgten Termine gegeben. Diese Übersicht dient lediglich der wissenschaftlichen Dokumentation. Alle Termine fanden Remote mit diversen Telekonferenz-Tools statt.

Tabelle 4: Übersicht über die Termine mit Involvierung von Stakeholdern.

Anlass	**Stakeholder**	**Zeitpunkt**
Vorbesprechung	StMUV	11.04.2023 13:30
Kick-Off	Alle	04.05.2023 14:00
Interview	VCI	08.05.2023 13:00
Interview	Evonik	08.05.2023 14:30
Interview	VCI	11.05.2023 13:00
Interview	Evonik	16.05.2023 14:00
Interview	LfU	17.05.2023 13:00
Interview	Gruppe Luftreinhaltung/Reg. Oberfr.	17.05.2023 14:30
Abstimmung	StMUV	24.05.2023 10:00
Infrastruktur	Govdigital	24.05.2023 12:00
Interview	BASF	26.05.2023 09:00
Interview	Wacker	02.06.2023 09:00
Abstimmung	StMUV	05.06.2023 13:00
Blockchain Talk	Alle & Gäste	07.06.2023 14:00
Ergebnisrunde 1/3	Verschiedene	14.06.2023 14:00
Ergebnisrunde 2/3	Verschiedene	16.06.2023 13:00
Abstimmung	StMUV	03.07.2023 13:00
Ergebnisrunde 3/3	Verschiedene	05.07.2023 10:00
Smart Contract Diskussion	Govdigital, Evonik	12.07.2023 13:00
Abgabe Projektbericht	Alle	25.08.2023 11:00
Abstimmung	StMUV	05.09.2023 10:00
Fragerunde Projektbericht	Alle	18.09.2023 14:00
Abstimmung	StMUV	19.09.2023 15:00
Präsentation Demonstrator	StMUV	29.11.2023 12:00
Abstimmung	StMUV	11.12.2023 09:15
Finales Deployment	-	22.12.2023 12:00
Finale Abgabe Projektbericht	Alle	29.12.2023 17:00