Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)

18. Dezember 2019

Schlussbericht

„Blockchain-basierte Erfassung und Steuerung von Energieanlagen mithilfe des Smart-Meter-Gateways: Machbarkeitsstudie und Pilotkonzept“

Inhaltsverzeichnis

1. Management Summary

- Mit der Verknüpfung von Blockchain- und SMGW-Technologie, um eine öffentliche Anlagendatenbank automatisiert zu pflegen, könnte eine sichere, skalierbare und interoperable Grundlage für zukünftige dezentrale Geschäftsmodelle geschaffen werden.
- Im Mittelpunkt dieses Projekts steht daher die Frage, unter welchen technischen, rechtlich/regulatorischen und kaufmännischen Voraussetzungen eine Smart Meter Gateway-Plattform in Kombination mit dem Einsatz von Blockchain-Technologie geeignet ist, diese Erwartungen zu erfüllen. Dazu wurde zunächst eine Machbarkeitsstudie erstellt und darauf aufbauend ein Konzept für ein Pilotprojekt zur „Automatisierten Pflege einer öffentlichen Anlagendatenbank" erarbeitet.

Die Machbarkeitsstudie hat die folgenden Ergebnisse erbracht:

Technische Sicht

- In Bezug auf die technische Analyse kann festgehalten werden, dass das SMGW grundsätzlich dazu geeignet ist, als ausführende Instanz Akteure automatisiert zu registrieren und Anlagendatensätze automatisch an eine öffentliche Datenbank zu übertragen. Dies gilt auch für die vollständige und eindeutige Herstellung der Identität mittels einer Public Key Infrastructure für ‚digitale Identitätszertifikate'.
- Ergänzt wird die technische Architektur durch den Einsatz einer verteilten Blockchain-Datenbank. Beim Design dieser Datenbank erscheint es sinnvoll, sich auf eine private bzw. Konsortial-Blockchain zu beschränken. Für den datenschutzrechtlich sicheren Umgang mit personenbezogenen Daten, deren Speicherung ‚off-chain' erfolgen kann, ist ein Identitäts- und Zugriffsmanagement auf Basis eines universell anwendbaren Datenmodells erforderlich.
- Der Einsatz der Blockchain für eine öffentliche Anlagendatenbank vermeidet eine asynchrone, redundante und damit fehleranfällige Datenhaltung. Gleichzeitig wird die Ausfallsicherheit des Gesamtsystems erhöht und die Aktualität und Richtigkeit der ausgetauschten Daten sichergestellt. Letztlich bietet die Blockchain-Lösung als höherwertige digitale Infrastruktur auch eine skalierbare, interoperable und sichere Grundlage für zukünftige Anwendungsfälle zwischen dezentralen Marktakteuren, wie z.B. den direkten Peer-to-Peer-Handel.
- Die Architektur einer öffentlichen Anlagendatenbank muss weiterhin die Übernahme der Daten vom SMGW oder einem autorisierten Endgerät ermöglichen. Grundsätzlich sind die dazu benötigten technischen Komponenten bereits mit der SMGW-Technologie verfügbar.

Regulatorische und rechtliche Sicht

- Aus regulatorischer Sicht ist insbesondere die Einbindung von Blockchain und SMGW bei der Registrierung in der Anlagendatenbank unter den aktuellen regulatorischen Rahmenbedingungen des EnWG und der MaStRV zu ermöglichen. Hier besteht Gestaltungsspielraum für den Verordnungsgeber.
- Regulatorisch relevant ist auch, dass die Prozesse zur Registrierung und Übertragung der Daten mit den Vorschriften zur Datenkommunikation und dem Aufgabenkreis des Gateway-Administrators übereinstimmen. Hier zeigt sich, dass die Ausweitung der Funktionalität des SMGWs auf die hier untersuchte Funktion erfordert, einen passenden WAN-Anwendungsfall für das SMGW in den technischen Richtlinien zu entwickeln und umzusetzen.
- Darüber hinaus stellen sich bei der automatisierten Anmeldung in einer öffentlichen Datenbank vor allem auch datenschutzrechtliche Fragen. Hierbei geht es im Einzelnen darum,
    - ob für die Einbindung von Marktteilnehmern mit den Marktrollen Messstellenbetreiber (Gateway-Administrator) und Netzbetreiber entsprechende datenschutz-rechtliche Erlaubnistatbestände bestehen,

- ob der Prozess zur Registrierung und Übertragung der Daten den Anforderungen der Datenschutzgrundsätze, insbesondere dem Transparenzgebot, entspricht und
- ob die Betroffenenrechte hinreichend gewahrt werden.

- Eine rechtskonforme Gestaltung, welche die Grundsätze des Transparenzgebots, der Datenminimierung, der Betroffenheitsrechte und des Rechts auf Datenportabilität einhält, erscheint als lösbare Aufgabe.

Wirtschaftlichkeit

- Im hier betrachteten Anwendungsfall kommen in Bezug auf die reine Automatisierung einer Anlagendatenbank grundsätzlich auch andere Lösungen als die Blockchain in Betracht. Darüber hinaus bildet die Blockchain in Verbindung mit dem Vertrauensanker SMGW aber einen besonderen gesamtwirtschaftlichen Nutzen. So kann eine sichere, offene und flexible technische Plattform für zahlreiche (auch Blockchain-basierte) energiewirtschaftliche Anwendungsfälle der Gegenwart und der Zukunft bereitgestellt werden, z.B. auch den direkten Peer-to-Peer-Handel unter Letztverbrauchern:
  - Direkte Transaktionen zwischen Marktpartnern (Letztverbrauchern) durch sichere Authentifizierung – Intermediäre werden entbehrlich, Transaktionskosten sinken
  - Mehr Marktteilnehmer und mehr Wettbewerb durch vereinfachten Zugang zu plattformgebundenen Lösungsangeboten
  - Offene, interoperable Plattform ersetzt herstellerspezifische Technologien, dadurch mehr Anbieterwettbewerb und gestärkte Autonomie der Verbraucher
- Ein weiterer gesamtwirtschaftlicher Nutzenaspekt betrifft die erhöhte Versorgungssicherheit bei stark skalierenden Geschäftsmodellen (z.B. der Ladesäuleninfrastruktur) durch eine sichere, skalierbare und interoperable Stammdatenplattform.
- Auf Seiten der Akteure im Energiemarkt profitieren die Anlagenbetreiber durch reduzierte Ingangsetzungs- und Transaktionskosten. Für die Netzbetreiber werden eigene Anlagendaten verzichtbar. Investoren wird die Finanzierung von Energieanlagen durch die Verfügbarkeit gesicherter Daten erleichtert. Ein offener, interoperabler Standard befördert auch die Bereitschaft zu Entwicklungsinvestitionen auf Seiten der Technologieanbieter und fördert potenziell die Marktverbreitung der SMGWs. Koordinierende und regulierende Behörden können schließlich den Aufwand durch ‚analoge' Aufgaben reduzieren.

Konzeption des Pilotprojekts

- Die Konzeption des Pilotprojekts erfolgte für den konkreten Anwendungsfall „Automatisierte Pflege einer öffentlichen Anlagendatenbank" unter Einbeziehung von Experten der EY (SMGW, Blockchain, Recht) sowie unter Mitwirkung von externen Akteuren (Markt, Hersteller, Dienstleister) nach einem Projektrollen- und Partnerkonzept. Eine entsprechend intensive Kooperation wird auch in der Pilotumsetzung empfohlen.
- Im Pilotprojekt anzustreben ist eine vollständige technische Implementierung mit der Fähigkeit zur Pilotdurchführung im Rahmen einer Reallaborumgebung, auch um eine spätere marktliche Nutzung vorzubereiten. Das „Plug & Play" für den Anlagenbetreiber im Feld sollte dennoch eine Anforderung für die Umsetzung sein.
- Im technischen Fokus steht dabei die Verwendung eines aktuell verfügbares SMGW (ohne jede technische Anpassung) mit einem Erweiterungsmodul auf der HAN/CLS-Schnittstelle, zusammen mit dem Einsatz einer Konsortial-Blockchain.
- Als Zeitraum für die Pilotdurchführung ist gemäß der erstellten Projektskizze von ca. 18 Kalendermonaten auszugehen.

2. Auftrag und Auftragsdurchführung

Die fortschreitende Dezentralisierung des Energieversorgungssystems mit dem Ausbau der Erneuerbaren Energien, Speichermöglichkeiten und flexiblen Verbrauchern bzw. Erzeugern stellt alle Akteure der Energiewirtschaft vor erhebliche Herausforderungen. Gleichzeitig bieten aber digitale Technologien, wie intelligente Ortsnetzstationen, Data Analytics, steuerbare Wechselrichter etc. auch erhebliche Potenziale, die Umstellung des deutschen Energiesystems effizient und erfolgreich zu gestalten. Mit dem Inkrafttreten des Gesetzes zur Digitalisierung der Energiewende (GDEW) zum 2. September 2016 wurde eine wichtige Grundlage zur Nutzung der Potenziale digitaler Technologien in der Energiewirtschaft geschaffen.

Ein Grundgedanke des GDEW ist es, auf der Basis zertifizierter und den Vorgaben des Gesetzes entsprechender Messtechnik - intelligente Messsysteme unter Verwendung eines Smart Meter Gateways (SMGW) - eine Plattform für zahlreiche Anwendungsfälle zu schaffen - in den Bereichen Smart Metering und Smart Grid, aber auch darüber hinaus für Smart Mobility, Smart Home und Smart Facilities, sowie für datenbasierte Mehrwertdienste, die in der Zukunft denkbar sind.

Viele der entstehenden Anwendungsfälle und Geschäftsmodelle beruhen darauf, dass ein sicherer, zeitgerechter und kosteneffizienter Austausch von Daten und Informationen zwischen digitalen Komponenten und auch zwischen Transaktionspartnern erfolgen kann. Blockchain-Technologien sind in diesem Zusammenhang in den letzten Jahren vermehrt in den Mittelpunkt der Betrachtung gerückt.

Es wird in der nahen Zukunft darauf ankommen, dem gesetzlich vorgesehenen SMGW-Plattformkonzept auch in der Praxis Geltung zu verschaffen. Dies gilt auch und gerade vor dem Hintergrund der gegenwärtig noch verbreiteten proprietären, nicht standardisierten und nicht interoperablen Lösungen. Dabei ist es auch entscheidend zu verstehen, in welcher Weise die SMGW-Plattform offen ist, für die Kombination mit innovativen Technologien wie der Blockchain.

Im Mittelpunkt dieses Projekts steht daher die Frage, unter welchen technischen, rechtlich/regulatorischen und kaufmännischen Voraussetzungen eine Konstellation aus Smart Meter Gateway-Plattform in Kombination mit dem Einsatz von Blockchain-Technologie die Grundlage für erfolgreiche digitale Anwendungsfälle und Geschäftsmodelle in der Energiewirtschaft darstellen kann.

Der vorliegende Bericht fasst die Ergebnisse der Arbeiten zusammen:

In einem ersten Schritt haben wir gemeinsam mit der Auftraggeberin diese Projektidee konkretisiert, zwei verschiedene Anwendungsfälle beschrieben und auf ihre Machbarkeit hin untersucht. Die Überlegungen hierzu sind im Abschnitt 3.1.1 dargestellt.

Der naheliegende Anwendungsfall „Direkter Peer-to-Peer-Handel unter Letztverbrauchern“ unter Einsatz von SMGW wird als technisch machbar, aber derzeit rechtlich nicht sinnvoll realisierbar qualifiziert und für eine Pilotierung zum jetzigen Zeitpunkt verworfen. Für den zur weiteren Betrachtung ausgewählten Anwendungsfall „Automatisierte Pflege einer öffentlichen Anlagendatenbank“ haben wir auf der Grundlage der Aufnahme des Status Quo am Beispiel des Marktstammdatenregisters (3.1.2.1) und der Formulierung eines möglichen Zielprozesses (3.1.2.2) eine Beschreibung der technologischen Lösung vorgenommen (3.1.3).

Abschnitt 3.1.4 behandelt die rechtlichen und regulatorischen Fragestellungen in Bezug auf die untersuchten Anwendungsfälle. Dabei wird zunächst auf die rechtlichen und regulatorischen Herausforderungen bei der Umsetzung eines direkten Peer-to-Peer-Handels eingegangen. In einem zweiten Schritt werden die rechtlichen Anforderungen an eine automatisierte Übermittlung und Pflege von Anlagenstammdaten in einer Datenbank untersucht.

In Abschnitt 3.1.5 wird schließlich der Frage nachgegangen, welche wirtschaftlichen Vorteile die Realisierung eines entsprechenden Anwendungsfalls für die Akteure im Energiemarkt (Lösungsanbieter, Prosumer, Verteilnetz- und Messstellenbetreiber) sowie aus gesamtwirtschaftlicher Sicht potenziell hat.

In den Abschnitten des Kapitel 3.2 wird, auf Basis des zuvor identifizierten Anwendungsfalls ein konkretes Pilotprojekt skizziert, mithilfe dessen die Auftraggeberin die weitere Umsetzung im Rahmen der Blockchain-Strategie des Bundes verfolgen kann.

Wesentliches Element in der Vorgehensweise hierzu ist dabei die Plausibilisierung der Elemente des Pilotkonzeptes anhand zweier Workshops mithilfe weiterer, zusammen mit der Auftraggeberin ausgewählter Marktpartner.

3. Ergebnisse zu den Arbeitspaketen

3.1 Arbeitspaket 1: Machbarkeitsstudie zur Projektidee

3.1.1 Konkretisierung der Projektidee und des zu pilotierenden Anwendungsfalls

Für die Untersuchung der Machbarkeit einer technischen Aufgabenstellung wie der Vorliegenden (SMGW interagiert mit Blockchain) ist die Formulierung eines konkreten Anwendungsfalls erforderlich. Auf diese Weise können die technischen und rechtlich/regulatorischen Anforderungen am konkreten Sachverhalt beschrieben und modelliert werden. Da auch eine Pilotierung konzipiert werden soll, sollte der ausgewählte Anwendungsfall zukunftsgerichtet und an den absehbaren Interessen der Akteure im Energiemarkt ausgerichtet sein (Verbraucher, Anbieter sowie koordinierende/regulierende Behörden).

Die hier zu untersuchende Verbindung der beiden technischen Elemente SMGW und Blockchain erfordert einen Anwendungsfall, bei dem

- zwei oder mehrere Akteure über eine Blockchain miteinander in Verbindung treten und
- die beteiligten Akteure jeweils über ein Smart Meter Gateway mit der Blockchain kommunizieren.

Dieses technische Set-up definiert bereits weitgehend den Rahmen, in dem der Anwendungsfall zu beschreiben ist: Nach § 29 Gesetz zur Digitalisierung der Energiewende kommt ein SMGW als Bestandteil eines intelligenten Messsystems verpflichtend zum Einsatz bei

- Letztverbrauchern mit mehr als 6.000 kWh Jahresverbrauch
- Letztverbrauchern mit **steuerbaren Verbrauchseinrichtungen** gem. §14a EnWG
- Betreiber von **Erzeugungsanlagen** mit einer installierten Leistung von mehr als 7 kW

Die vom BMWi als Auftrag formulierte Projektidee hat damit zum Gegenstand, die im Energiesystem vorhandenen steuerbaren Anlagen (Erzeuger, Verbraucher/Lasten und Speicher) über eine Blockchain(-Technologie) zur Etablierung und Abwicklung von Teilnehmerbeziehungen zu verbinden.

Dabei sollen die Eigenschaften und Funktionen des am Anlagenort vorhandenen Smart Meter Gateways so eingebunden werden, dass dieses mit seinem integrierten Sicherheitsmodul als Vertrauensanker (Authentizität, Verbindlichkeit, Nicht-Abstreitbarkeit) dienen kann.

Auf dieser Grundlage wurden mögliche Anwendungsfälle diskutiert und betrachtet. Ziel der Diskussion war es, einen oder mehrere Anwendungsfälle zu identifizieren, welche technisch umsetzbar sind und auch unter gesetzlichen, regulatorischen Rahmenbedingungen realisierbar sind. Das Konzept für eine Pilotierung des ausgewählten Anwendungsfalls soll dann im AP2 des Projektes erstellt werden.

3.1.1.1 Direkter P2P-Handel von elektrischer Energie unter Letztverbrauchern

Entsprechend dieser Rahmensetzung ist es naheliegend, als Anwendungsfall zunächst den Austausch von elektrischer Energie unter Letztverbrauchern in Betracht zu ziehen, die als (flexible) Verbraucher und Einspeiser agieren (Peer-to-Peer-Handel mit einem Liefer-/Erzeugungs- und Abnahme-Szenario).

Zentrale Eigenschaft der Blockchain-Technologie ist die Verwendung von „Smart Contracts" für das gesicherte Daten-Management innerhalb eines Vertragskonstruktes zweier Vertragsparteien. Das zugehörige Akteurs- und Prozessmodell sowie eine Skizze des P2P-Szenarios wurden in der ersten Iteration aus Sicht der technischen Aufgabenstellung erstellt. Die Details hierzu wurden in Anhang A dargestellt unter „P2P Energie-Lieferung und -Bezug".

Die technische Betrachtung dieses Anwendungsfalls im Rahmen der Vorstudie führt zu dem Ergebnis, dass die Einbindung auch des SMGW in diese Struktur als Vertrauensanker als grundsätzlich technisch möglich und umsetzbar erscheint. Dabei sind insbesondere noch drei Fragestellungen zu lösen:

- Die Kompatibilität zwischen SMGW und Blockchain-Netzwerk
- Im Rahmen des Identitätsmanagements das Problem eines konstanten, kryptographisch sicheren Identifikationsmerkmals im System
- Die Zuordnung von public keys und Stammdaten im System (zentral/dezentral)

Die rechtliche und regulatorische Bewertung dieses Anwendungsfalls ist nachfolgend unter 3.1.4. ausführlicher dargestellt. Diese Bewertung kommt zu dem Schluss, dass der Umsetzung des Anwendungsfalls eines direkten Peer-to-Peer-Handels von Letztverbrauchern im öffentlichen Verteilnetz ohne Intermediär derzeit erhebliche rechtliche Restriktionen entgegenstehen.

Zudem zeigt die Praxis am Energiemarkt, dass bereits etablierte Pilotprojekte zur Nutzung der Blockchain-Technologie für Peer-to-Peer-Geschäfte bestehen, wobei die Transaktionen zwischen den Letztverbrauchern über einen Intermediär abgewickelt werden. Beispielhaft seien hier Tal.Markt der WSW Wuppertaler Stadtwerke oder die Marktplätze von Lition Energie und enyway genannt.

Die Erweiterung dieser bestehenden Anwendungen um den Aspekt der Verwendung des SMGW wäre – wie oben dargestellt – technisch grundsätzlich möglich, der darüber hinaus gehende Erkenntniswert wegen der bereits vorhandenen Praxiserfahrungen aber voraussichtlich begrenzt.

Auch sind im vom BMWi geförderten Technologieprogramm „Smart Service Welt 2, Cluster Energie" bereits mehrere Projekte beheimatet, die den Gedanken eines Peer-to-Peer-Handels mittels Blockchain aufgreifen (ETIBLOGG, Pebbles, SMECS und BloGPV).[1]

Unter Berücksichtigung der Zielsetzung, einen umsetzbaren Piloten mit hohem Erkenntnisgewinn zu modellieren, wurde in Abstimmung mit dem Auftraggeber von einer weiteren Verfolgung dieses Anwendungsfalls abgesehen.

[1] Vgl. bspw. https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Smart_Service_Welt/Projekte/Energie/Energie.html

3.1.1.2 Automatisierte Pflege einer öffentlichen Anlagendatenbank

Im Zuge der Überlegungen hat sich gezeigt, dass gerade der sichere und eindeutige Identitätsnachweis für jede Anlage im Netz sowie der automatisierte Zugriff auf technische Anlagendaten eine unverzichtbare Grundlage für marktliche Peer-to-Peer Geschäftsmodelle unter Prosumern darstellt. Dies gilt letztlich analog für jede denkbare Interaktion in der künftigen dezentralen IoT-Welt der Strom-Verteilnetze.

Im Rahmen der Untersuchung der technischen Ausgestaltung des P2P-Anwendungsfalls wurde ebenfalls deutlich, dass eine Nutzung von Blockchain-Technologie die Bereitstellung einer gesicherten Identität der Vertragspartner erfordert und dass die Verwendung eines Smart Contracts, z.B. P2P-Energiehandel, in einem automatisierten, technischen Verfahren nur bei Vorliegen von qualitätsgesicherten, authentischen Stammdaten möglich ist.

Dies wiegt umso schwerer, als davon auszugehen ist, dass die Erzeugungs- und Verbrauchsanlagen sowie die Speicher im Wege der Maschine-zu-Maschine Kommunikation zukünftig tatsächlich voll automatisiert interagieren werden. Grundlegend anzustreben wäre also eine ‚Plug-and-Play"-Lösung, mit der ein Anlagenbetreiber seine Anlage mit Anschluss an das Netz selbständig und sicher identifiziert und registriert. Damit könnten auch alle kaufmännischen (z.B. EEG) und technischen Anlagenstammdaten übermittelt und allen berechtigten Akteuren zur Verfügung gestellt werden.

Die Verfügbarkeit von Stammdaten der (EEG-)Anlagen ist bereits durch die Einführung des Marktstammdatenregisters (MaStR) rechtlich geregelt. Dieses stellt bereits eine erhebliche Weiterentwicklung gegenüber den vorher existierenden Registern (z.B. PV-Meldeportal) dar und vereinfacht durch Maschine-zu-Maschine-Schnittstellen sowie einer Webanwendung die Kommunikation zwischen den Marktteilnehmern. Allerdings ist der Prozess der Daten-Erhebung, -Pflege und Bereitstellung bislang wenig automatisiert. Ebenso ist die Verwendung der Daten aus dem MaStR sowie die Datenqualität nicht standardisiert. So führen viele Marktteilnehmer zusätzliche, eigene Stammdaten-Sammlungen (Datenbanken) um diese in den benötigten Prozessen, insbesondere in der Marktkommunikation zu verwenden.

Eine solche halbautomatische Lösung zum Vorhalten von Marktstammdaten kann daher nur ein erster Schritt auf dem Weg zu einer echten digitalen Integration und Verbindung solcher Anlagen mit der Netzinfrastruktur sein.

Diese Überlegung bildet nun die Grundlage für die Ausformulierung des hier zu betrachtenden Anwendungsfalls: Es wird untersucht, ob und wenn ja wie eine Blockchain in Verbindung mit der zertifizierten SMGW-Technologie geeignet ist, eine entsprechende **digitale Lösung zur eindeutigen Identifizierung und Übermittlung von Stammdaten von Anlagen im Verteilnetz** zu ermöglichen.

Konkret wird in Abstimmung mit der Auftraggeberin im Rahmen dieser Studie die **automatisierte Pflege einer öffentlichen Anlagendatenbank** unter Verwendung der SMGW- und Blockchain-Technologie untersucht.

Im Rahmen der Vertiefung dieses Anwendungsfalls wurden folgende Erfolgsfaktoren definiert:

Erfolgskriterien, Ziele der Marktbarkeitsstudie und Prämissen für den Anwendungsfall


Das Smartmeter Gateway fungiert als Vertrauensanker für die Messwerte und Daten im System


Es gibt ein durchgängiges Identitätskonzept vom SMGW bis zur Blockchain


Identitäten, Daten und Transaktionen sind unfälschbar nachvollziehbar


Initialkonfiguration ist automatisierbar („Plug & Play“)


Das Energiesystem darf nicht disruptiv verändert werden, Innovation soll im Einklang mit heutigen Grundprinzipien erfolgen


Eine Blockchain kann in das bestehende System integriert werden


Die Blockchain Technologie hat konkrete Vorteile gegenüber klassischer IT

3.1.2 Marktstammdatenregister

3.1.2.1 Der Status Quo der Anlagendatenhaltung

Seit dem 31.01.2019 steht allen Marktakteuren sowie der Öffentlichkeit das Marktstammdatenregister über das zugehörige Webportal gemäß § 111e des Energiewirtschaftsgesetzes (EnwG) und der Marktstammdatenregisterverordnung (MaStRV) vom 20.04.2017 zur Verfügung. Mit dem MaStR werden das Anlagenregister sowie das Photovoltaik-Meldeportal ersetzt und damit bisherige weitgehend analoge Meldewege in einem digitalen Verzeichnis für energiewirtschaftliche Daten in Obhut der Bundesnetzagentur (BNetzA) vereinigt.

Die Notwendigkeit zum Aufbau des MaStR ergab sich aus dem Wandel des zentralisierten Strommarktes hin zu einer Vielzahl von dezentralen Anlagen unterschiedlicher Technologien und Leistungsklassen auf der Erzeugungs- wie auch auf der Verbrauchsseite. Hieraus resultiert der Bedarf nach einem zentralen, behördlichen Register für den deutschen Strom- und Gasmarkt. Durch die zentrale Datenhaltung soll eine Erhöhung der Datenqualität und -aktualität erreicht und damit behördliche und privatwirtschaftliche Prozesse vereinfacht werden (z.B. Marktkommunikation). Hierzu enthält das MaStR wesentliche Akteure und Anlagen im Bereich Strom und Gas und ist weitestgehend öffentlich nutzbar. Durch die Vergabe von Marktstammdatennummern soll die Marktkommunikation sowie die Identifikation von Akteuren des Energiemarktes vereinfacht und beschleunigt werden um u.a. automatisierte Maschine-zu-Maschine-(M2M)-Kommunikation sowie die Einsichtnahme durch eine Webansicht zu ermöglichen.[2]

Um die Vollständigkeit des Registers zu gewährleisten, sind alle Akteure des Strom- und Gasmarktes nach § 3 Abs. 1 der MaStRV verpflichtet, sich selbst und ihre Anlagen im MaStR-Webportal zu registrieren. Eine automatisierte Schnittstelle besteht jedoch nicht. Die Registrierungspflicht umfasst beispielsweise Betreiber von Einheiten und Marktplätzen, Bilanzkreisverantwortliche, Messstellen- und Netzbetreiber, Lieferanten und Weitere. Ebenfalls zu nennen sind Letztverbraucher, wenn sie an ein Höchst- oder Hochleistungsnetz oder im Fall von Gas an ein Fernleitungsnetz angeschlossen sind sowie Unternehmen zur Direktvermarktung von Strom aus Erneuerbaren Energien. Weitere, nicht zur Registrierung verpflichtete Marktakteure können sich freiwillig registrieren. Werden durch einen Marktakteur ortsfeste Einheiten zur Erzeugung, Speicherung oder zum Verbrauch von Strom oder Gas, wie beispielsweise EEG- und KWK-Anlagen oder Großverbraucher betrieben, sind diese ebenfalls zu registrieren.

Die hierbei abzulegenden Daten umfassen im Kern die technischen Stammdaten, die Standortdaten, die Betreiberinformationen sowie technische Zuordnungen (bspw. Netzanschluss). Bewegungsdaten der Anlagen werden nicht im MaStR erfasst. Da das Ziel des MaStR die Veröffentlichung möglichst vieler technischer Anlagendaten ist, sind alle nicht geschützten bzw. nicht vertraulichen Daten öffentlich einsehbar.

Wird eine Anlage in Betrieb genommen, gilt nach § 13 MaStRV eine einmonatige Frist zur Registrierung der Anlage. Für die Richtigkeit und Aktualität der Daten im MaStR ist der jeweilige Marktakteur bzw. Anlagenbetreiber in jedem Fall verantwortlich. Es sind jedoch Prüfungs- und Plausibilisierungsmaßnahmen durch die BNetzA sowie Netzbetreiber definiert. [3]

[2] Vgl. hierzu https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/MaStR/Webservice/webservice_node.html

[3] Vgl. hierzu https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/MaStR/MaStR_node.html

Der aktuelle Prozess zur Registrierung eines Marktakteurs und einer EEG-Anlage (z.B. einer Solaranlage auf einem Einfamilienhaus) ist über zwei Wege möglich: Digital im Webportal des MaStR oder mittels eines Papierformulars. Vereinfacht erfolgt der Vorgang in vier Prozessschritten:

1. Anlegen des MaStR-Kontos durch den Marktakteur und Eingabe der Stammdaten
2. Registrierung des Marktakteurs als Anlagenbetreiber
3. Registrierung der Anlage und Eingabe der technischen Stammdaten
4. Validierung des Datensatzes und Zuweisung der technischen Lokation

Werden hierbei die ersten drei Schritte weitestgehend durch den Marktakteur durchgeführt, erfolgt die Validierung der Daten durch den Netzbetreiber, die BNetzA oder nach Aufforderung seitens der BNetzA durch weitere Marktakteure.

Neben der Anlage von neuen Datensätzen sind für die finale Ausgestaltung des Setups einer potenziellen, öffentlichen Anlagendatenbank weitere Prozesse zu beachten. Diese sind:

- Auskunft
  - Öffentliche Daten
  - Vertrauliche und geschützte Daten
- Bearbeitung
- Löschung

Im Folgenden wird der Fokus exemplarisch auf den Prozess zur Registrierung eines Marktakteurs sowie einer Anlage gelegt. Da der Registrierungsprozess weitgehend unabhängig von der genutzten Datenbank betrachtet werden kann, erfolgt die Betrachtung des Anwendungsfalls unter Einbezug der Blockchain-Technologie nachgelagert in Abschnitt 3.1.3.5 und bleibt bei der Betrachtung des Zielprozesses zunächst unberücksichtigt.

3.1.2.2 Anforderungen an ein mögliches Zielmodell

Aus dem im vorherigen Abschnitt beschriebenen Beispiel des MaStR - wie auch für die meisten manuell gepflegten Datenbanken - ergeben sich verschiedene Herausforderungen. Diese resultieren aus den umfangreichen manuellen Anlage- und Pflegetätigkeiten für dezentral erhobene Daten, die durch viele verschiedene Parteien teilweise asynchron zueinander durchgeführt und lediglich nachträglich validiert werden.

Hieraus entstehen im Zeitablauf unabhängig von der Verantwortung der zuständigen Akteure üblicherweise Datenbestände, die insbesondere im Hinblick auf Vollständigkeit, Aktualität und Richtigkeit der Daten nurmehr stichprobenhaft überprüfbar sind. Ebenfalls erfolgt keine Identitätsprüfung der Anlagenbetreiber.

Weiterhin führt die manuelle Pflege der Daten zu langen Bearbeitungszeiten und -fristen, was dem Ziel eines flexiblen, dezentralen Energiemarktes, auf dem ggf. auch Echtzeit-Transaktionen möglich sind, zuwiderläuft. Darüber hinaus ist nach der aktuellen Vorgehensweise ein durchgängiges Identitätskonzept für die Marktakteure nur eingeschränkt gewährleistet, was die Automatisierung möglicher Vertragskonstrukte erschwert. Dies führt dazu, dass viele Marktteilnehmer zusätzliche, eigene Daten-Sammlungen (Datenbanken) vorhalten, um diese in den eigenverantworteten Prozessen zu verwenden, insbesondere in der Marktkommunikation.

Um diesen Aspekten gerecht zu werden, ergeben sich folgende Anforderungen entlang des Prozesses ‚Aufnahme der Daten in eine öffentliche Datenbank':

- Minimierung manueller Tätigkeiten und automatisierte Datenübermittlung, möglichst nach dem „Plug & Play"-Prinzip

- Sichere und vollständige Identifizierung und Übermittlung von Akteurs- und Anlagenstammdaten
- Etablierung eines durchgehenden Identitätsmanagements des Marktakteurs unter Nutzung von SMGW und Public Key Infrastruktur (PKI) als Vertrauensanker (Authentizität, Verbindlichkeit und Nicht-Abstreitbarkeit)

Diese Aspekte werden im folgenden Abschnitt vertieft betrachtet und am Beispiel eines möglichen Zielmodells unter Einbezug von SMGW und Blockchain-Technologie aufgezeigt

3.1.2.3 Architekturvorschläge für ein Zielmodell

Zur Erreichung des Ziels, die manuellen Aufwände insbesondere für den Marktakteur (Anlagenbetreiber) zu verringern und die Qualität der Datenhaltung zu erhöhen, ergeben sich zwei Ansatzpunkte:

- Zum einen die automatisierte Registrierung des Akteurs an der Datenbank mittels SMGW und damit einhergehend die Herstellung der Identität mittels PKI.
- Zum anderen die automatische Übertragung des Anlagendatensatzes an die Datenbank. Für die Übertragung des Datensatzes ist es jedoch zunächst notwendig, dass die Daten erhoben und für die Übertragung zur Verfügung gestellt werden.

Beide Möglichkeiten können unter Nutzung des SMGW als ausführende Instanz erfüllt werden, da dieses als gesicherte Identität des Anlagenbetreibers und Vertrauensanker für seine Identität im Rahmen der PKI konzipiert ist und mit dem Ziel entwickelt wird, dieses als „Kommunikationsplattform des intelligenten Energienetzes zu ertüchtigen“[4].

Unter Zuhilfenahme der PKI und der Zertifikatstripel sind somit vom SMGW signierte und verschlüsselte Daten eindeutig der Urheberschaft des jeweiligen SMGW und somit dem Marktakteur zuzuordnen. Ebenfalls ist unter Berücksichtigung korrekter Provisionierung eine vollständige Automatisierung möglich, wodurch die manuellen Aufwände des Anlagenbetreibers minimiert werden können.

Die Registrierung des Akteurs kann somit durch das SMGW unter Nutzung der Cipher Suite ausgeführt werden. Durch die eindeutige Identifizierung ist es möglich,

- die Identitäten der Endkunden und somit der zugehörigen Anlagen eindeutig in der Anlagendatenbank zuzuordnen und damit Datenschiefstände zu vermeiden.
- eine Anmeldung in der Anlagendatenbank durch die SMGW Zugangsdaten des Endkunden (Zertifikat/ Login-Informationen) zu ermöglichen.

Hieraus folgt, dass die PKI zum Authentizitäts- und Identitätsanker zwischen Marktakteur/Anlagenbetreiber, SMGW und Datenbank als zentrale Elemente eines zukünftigen, digitalen Energiemarktes werden kann.

Aufbauend auf der automatisierten Akteurs-Registrierung wird die automatisierte Übertragung von Akteurs- und Anlagenstammdaten durch das SMGW an die Anlagendatenbank ermöglicht. Hierfür ist es notwendig, dass diese Daten vollständig erhoben und auf das SMGW provisioniert werden.

[4] Vgl. hierzu Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende (BMWi, BSI); https://www.bmwi.de/Redaktion/DE/Downloads/S-T/standardisierungsstrategie.pdf?__blob=publicationFile&v=4

Der zurzeit gültige Prozess zur Erhebung der Daten beruht wesentlich auf den manuellen Tätigkeiten des Marktakteurs, sowie der nachträglichen Validierung und Ergänzung der Daten. Dies führt zu Redundanzen in der Datenhaltung bei den Marktteilnehmern. Es existiert heute noch kein einheitlicher Prozess zur Agglomeration und gebündelten Übertragung der Daten an das MaStR. Diesem Punkt kann unter der Annahme begegnet werden, dass zum Zeitpunkt der Anlageninbetriebnahme alle (oder der Großteil) der benötigten Daten bei der Mehrzahl der beteiligten Instanzen zum Zeitpunkt der Errichtung und Inbetriebnahme der Anlage vorliegen (bspw. Anlagenbetreiber, Installateur, Netzbetreiber, MSB, …).

Zu erfüllende Kriterien für eine Instanz der Datenerhebung sind:

- Datenschutzrechtliches Einverständnis des Auftraggebers (Anlagenbetreiber) für die Erhebung und Verarbeitung der Daten
- Kenntnisse der bei der Datenerhebung zu berücksichtigenden Marktpartner
- Möglichkeit der Weiterleitung der Daten der SMGW
- Datenschutzrechtlich zulässige Verarbeitung der Daten bei den Beteiligten (Erhebung, Speicherung, Weiterleitung, Löschung)

Werden diese Punkte bei der Evaluierung der Marktteilnehmer als potenzielle Datenübermittler berücksichtigt, bietet sich der durch den Anlagenbetreiber gewählte (grundzuständige oder wettbewerbliche) Messstellenbetreiber als primäre Datenerhebungs- und Übermittlungsinstanz an:

- Der MSB hat Kenntnis von allen beteiligten Instanzen des Anlagenbetriebs.
- Der MSB erhebt wesentliche personenbezogene Daten (z.B. Anschrift für die Installation des SMGWs) im Zuge der Beauftragung zum Messstellenbetrieb. Aus diesem Grund wird die Zustimmung des Anlagenbetreibers zur Datenerhebung und Verarbeitung auch personenbezogener Daten in jedem Fall eingeholt und die Vereinbarung muss lediglich um ergänzende Informationen (z.B. technische Stammdaten) erweitert werden. Ebenfalls sind die notwendigen Richtlinien und Prozesse zur Datenhaltung und -verarbeitung bereits etabliert.
- Der Gateway-Administrator (GWA) ist rechtlich der Sphäre des MSB zugeordnet. Hiermit besteht die Möglichkeit der Provisionierung des SMGWs im Auftrag des MSBs durch den GWA.

Basierend auf der Annahme, dass der MSB einen Großteil der benötigten Daten bündeln kann, müssen prinzipiell zwei WAN-Anwendungsfälle für die Übermittlung der Daten mittels SMGW etabliert werden:

1. Übermittlung der Daten durch den GWA an das SMGW
2. Speicherung der Daten im SMGW und Übermittlung der signierten Daten aus dem SMGW an die Anlagendatenbank

Weiterhin muss ein, auf Basis der gewählten, technischen Implementierung geeignetes Headend-System auf Seiten der Anlagendatenbank zum Empfang der verschlüsselten und signierten Daten aus den SMGWs etabliert werden. Ist dies ermöglicht, folgt im Ergebnis, dass in der Datenbank durch das SMGW signierte und damit eindeutig zuordenbare Akteurs- und Anlagenstammdaten vorliegen.

Zudem ermöglicht die Provisionierung des SMGWs durch den GWA im Zuge der Inbetriebnahme, dass auch unvollständige Datensätze (beispielsweise bei nicht vorliegen einzelner Daten zum Zeitpunkt der Inbetriebnahme) an die Datenbank übertragen werden können und eine Art Basisdatensatz angelegt wird. Da auch dieser Teil-Datensatz signiert ist, ist er eindeutig zuzuordnen und die nachträgliche Befüllung kann bspw. durch die BNetzA (bspw. analog MaStRV) verlangt werden. Durch diese „Basisbefüllung“ bei Inbetriebnahme der Anlage wird die Grundlage für eine qualifizierbare Vollständigkeit der Datenbank geschaffen.

Eine exemplarische Ausbildung eines Prozesses zur Befüllung einer Datenbank ohne Anspruch auf Vollständigkeit ist in Anhang E dargestellt. Für die Machbarkeit der weiteren Prozesse im Datenmanagement, zur Beauskunftung bzw. Dritt-Verwendung, Bearbeitung und Löschung der

Datensätze liegt die Differenzierung nicht in der technischen Architektur, sondern im Konzept zum Identitäts- und Zugriffsmanagement und ist im Wesentlichen geprägt durch die Anforderungen und Rahmenbedingungen der einzelnen Marktakteure in diesem Bereich. Daher wird die Erarbeitung der zukünftigen Ausprägung nachgelagert im Rahmen der Pilotkonzeption im Arbeitspaket 2 berücksichtigt.

3.1.3 Technologische Betrachtung

Ziel dieses Abschnitts ist es, einen Überblick des aktuellen technologischen Stands im Hinblick auf die für den Anwendungsfall relevanten Systeme im Energiemarkt, Marktrollen und Blockchain-Technologie[5] zu geben.

3.1.3.1 High-Level Architektur

In seiner Gesamtheit besteht der Energiemarkt aus einer Vielzahl von Marktteilnehmern mit unterschiedlichen Systemen und Anforderungen (u.a. Energielieferanten, Letztverbraucher, Prosumer, Netz- und Messstellenbetreiber, Energiedienstleister, koordinierende und regulierende Behörden). Um ein einheitliches Verständnis dieser Landschaft von Akteuren zu ermöglichen, wird im Zuge dieses Kapitels die Beschreibung einer High-Level Architektur des bestehenden Systems „Energiemarkt" und einer möglichen zukünftigen Ausgestaltung in Bezug auf den hier untersuchten Anwendungsfall dargelegt.

Eine Übereinstimmung der Architekturen im Status Quo und in einem möglichen Zielbild ist die bestehende und zukünftige Rollenverteilung der einzelnen Marktteilnehmer im Zusammenhang mit der Smart Metering PKI (nachfolgend SM-PKI).

Eine Eingangsprämisse für diese Untersuchung ist, dass die grundlegende Funktionalität der SM-PKI und die dazugehörige Rollenverteilung im Sinne der Zertifikatsverwaltung als gegeben unterstellt wird. Das bedeutet, dass dieser Teil des Systems als konstant betrachtet wird. Aus diesem Grund wird diese im Folgenden nicht explizit betrachtet und nur verkürzt vorgestellt.

Die Root-CA wird vom Bundesamt für Sicherheit in der Informationstechnik (nachfolgend BSI) betrieben und stellt den hoheitlichen Vertrauensanker im System der SM-PKI dar. Sie bildet das Fundament für die Berechtigung zur Ausstellung und Nutzung der Zertifikate und ist Herausgeber der SM-PKI-Policy.[6] Dies bedeutet in weiterer Folge, dass die Root-CA die Sub-CA autorisiert Endnutzerzertifikate auszustellen.[7]

Die Sub-CA kann von einem Marktteilnehmer oder auch unternehmensübergreifend betrieben werden.[8] Diese Rolle kann von einem beliebigen registrierten Marktteilnehmer wahrgenommen

[5] Wesentliche Quellen im Abschnitt Blockchain

- Urbach et al. (2016). Blockchain: Grundlagen, Anwendungen und Potenziale
- Böhme, R., Pesch, P. (2017). Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie. In: DuD - Datenschutz und Datensicherheit 8-2017
- Sandner, P., Höfelmann, D. (2019). Entscheidungshilfe für den Einsatz von Blockchain-Technologien in Unternehmen: Vier Frameworks im Vergleich. FSBC Working Paper

[6] Certificate Policy der Smart Metering-PKI, Version 1.1.1, S. 12ff;

[7] Technische Richtlinie BSI TR-03109-4, Version 1.2.1, S. 11f;

[8] Siehe 4

werden. Die Aufgabe der Sub-CA ist es, die Zertifikate für alle Endnutzer zu erstellen. Dazu gehören Externe Marktteilnehmer (bspw. Messstellenbetreiber), Gateway Administratoren und Letztverbraucher.

Besondere Bedeutung kommt dabei dem Gateway Administrator zu. Neben dem Schlüssel/ Zertifikatsmanagement des Smart Meter Gateways gehören auch die Profilverwaltung, Bereitstellung von Firmware-Updates, Monitoring sowie die Unterstützung der Messwertverarbeitung zu dessen Aufgaben.[9] Die aktuelle sowie eine mögliche Ziel-Marktarchitektur sind im Folgenden dargestellt.

Status Quo

Der Status Quo am Beispiel des MaStR ist in Abschnitt 3.1.2.1 beschrieben. Die Beschreibung basiert auf der hier in Abbildung 1 dargestellten vereinfachten Marktarchitektur.
Demnach beauftragt der Kunde den Messstellenbetreiber mit dem Betrieb der Messstelle, der GWA provisioniert das SMGW und der Kunde registriert sich selbstständig im MaStR. Anschließend werden die Daten durch den Netzbetreiber validiert. Das Stammdatenregister wird zentral durch die BNetzA gehostet und den Marktteilnehmern zur Verfügung gestellt. Aufgrund der bestehenden Herausforderungen in Bezug auf Aktualität, Vollständigkeit und Korrektheit der Daten führt dies zu doppelter Datenhaltung bei den Marktteilnehmern und vermeidbaren Redundanzen.

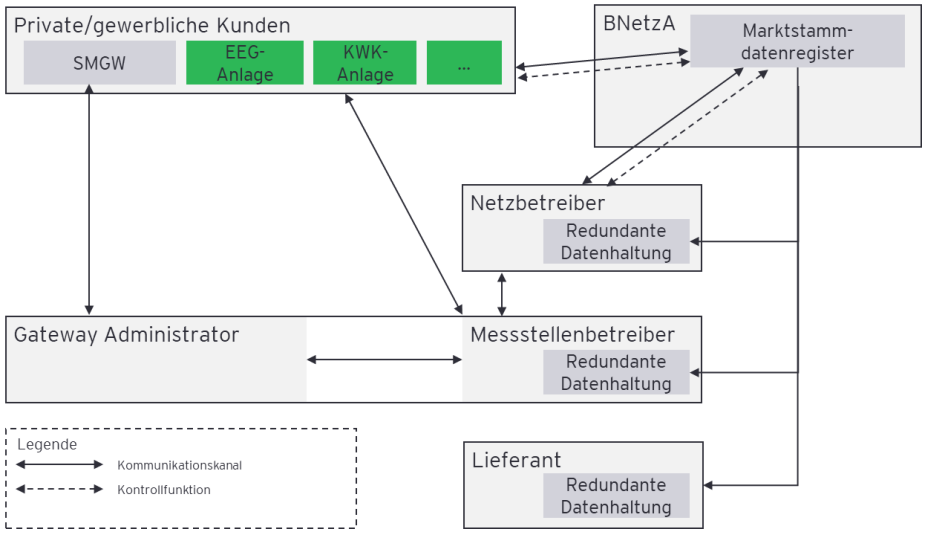


Abbildung 1: Vereinfachte Status Quo Architektur des Marktstammdatenregisters

Mögliches Zielbild

Ein mögliches Zielmodell basiert auf den in Abschnitt 3.1.2.3 dargestellten Ansätzen eines Zielmodells:

1. Identität des Anlagenbetreibers wird über das SMGW Zertifikat hergestellt
2. Datensatz des Anlagenbetreibers wird vom SMGW an die Anlagendatenbank übertragen

Damit kann die Identität über die PKI vollständig und eindeutig hergestellt werden. Weiterhin folgt durch die automatische Übermittlung der Daten aus dem SMGW, dass alle Anlagen, welche über ein SMGW verfügen, auch in der Datenbank angelegt sind. Für die Marktakteure Anlagenbetreiber und Netzbetreiber verbleibt lediglich, den angelegten Datensatz zu

- ergänzen,
- zu validieren
- und zu aktualisieren.

[9] Technische Richtlinie BSI TR-03109-6, Version 1.0, S.10;

Ergänzt wird dieser Aufbau durch den Einsatz einer verteilten Blockchain-Datenbank. Die Blockchain Nodes führen dazu, dass eine asynchrone, redundante und damit fehleranfällige Datenhaltung vermieden werden kann. Gleichzeitig wird die Ausfallsicherheit des Gesamtsystems erhöht und die Aktualität und Richtigkeit der Daten zwischen den Node-Betreibern sichergestellt. Die Daten in der Ankagendatenbank können wiederum um vertrauliche oder ergänzende Daten des jeweiligen Akteurs erweitert werden und somit individuelle Anwendungsfälle hierauf ermöglicht werden. Die Eigenschaften, mögliche technische Ausprägungen sowie Vor- und Nachteile dieser Technik werden in Abschnitt 3.1.3.5 eingehender betrachtet.

Ein wesentlicher zu beachtender Punkt ist dabei, wo welche Daten gespeichert werden. Im Blockchain Jargon wird zwischen on-chain und off-chain Daten unterschieden. Wie unter Punkt „3.1.3.5 Blockchain – on-chain vs. off-chain Datenhaltung“ erläutert, werden on-chain Daten auf allen Netzwerk-Knoten repliziert und damit hochredundant vorgehalten. In Kombination mit der Unverfälschlichkeit der Daten führt dies zu einem redundanten Bestand an unveränderbaren und damit „unlöschbaren“ Daten.

Daher bedarf es einer klaren Regelung, welche Daten auf der Blockchain abgelegt werden und welche anderweitig vorgehalten werden müssen. In dem Kontext einer verteilten Anlagendatenbank, ist es daher nicht sinnvoll personenbezogene Daten auf der Blockchain zu verarbeiten oder abzulegen, da diese damit unlöschbar und für alle Netzwerkteilnehmer einsehbar gemacht würden (siehe Punkt „3.1.4.2.2 Datenschutzrechtlicher Rechtsrahmen“). Diese müssten daher off-chain, mit einem klaren und gesetzeskonformen Identitäts- und Berechtigungsmanagement gespeichert werden.

Operativ notwendige Daten, wie Anlagenkapazität oder Einspeisungsvolumen zum Zeitpunkt X hingegen, könnten durchaus auf einer Blockchain abgelegt werden. Und damit, je nach genauer Implementierung, z.B. einen Echtzeitüberblick der in Betrieb genommenen Anlagen und Kapazität liefern. Das heißt, alle operativ notwendigen Daten, welche keine Assoziation zu personenbezogenen Daten zulassen (im Sinne der DSGVO und BDSG-Vorschriften), könnten auf einer Blockchain abgelegt und verarbeitet werden.

Welche Daten in welchem Format wo abgelegt werden, erfordert die Entwicklung eines für den Energiemarkt universell anwendbaren Datenmodells unter Berücksichtigung der Anforderungen der Regulierungsbehörden und Marktteilnehmer. Ein solches zu erstellen bzw. Anforderungen hierzu aufzunehmen wird ein fundamentaler Bestandteil eines zukünftigen Piloten sein.

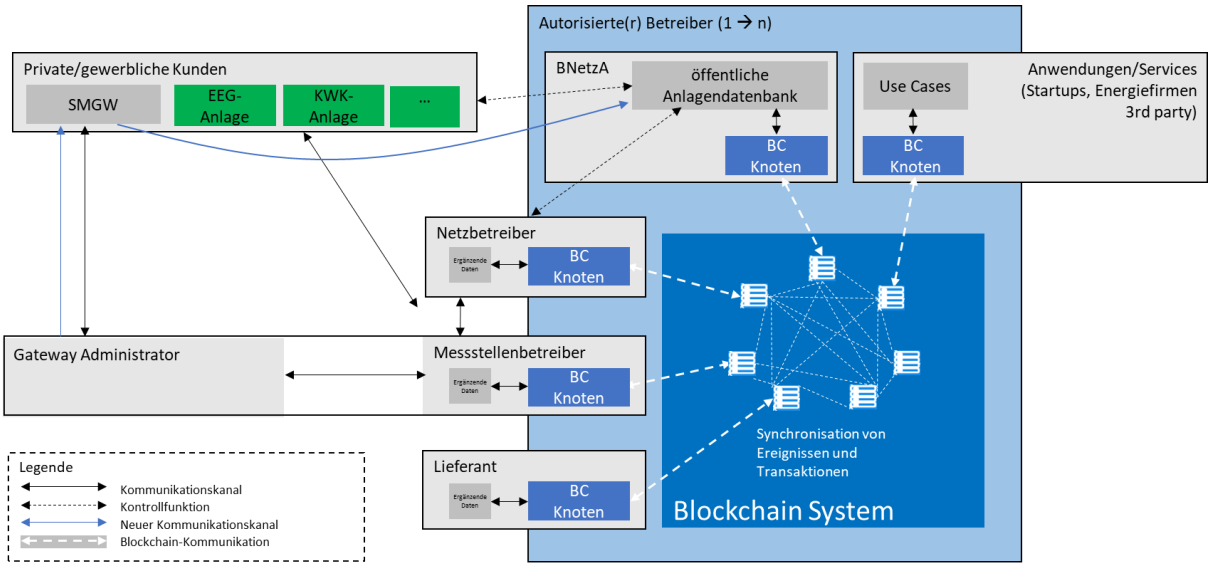


Abbildung 2: Vereinfachtes mögliches Zielmodell der Architektur der öffentlichen Anlagendatenbank

Ergänzend hierzu zu berücksichtigen sind die neuen Kommunikationskanäle zwischen GWA und SMGW (zur Provisionierung des SMGW) sowie der Übermittlung der Anlagendaten zwischen SMGW und Anlagendatenbank (BC-Knoten, Registrierung der Anlage und Übertragung der Daten in die Datenbank), wie in der Architekturskizze dargestellt.

3.1.3.2 Anlagendatenbank (technische Sicht)

Um die unter 3.1.2.3 aufgezeigten neuen Funktionen

1. Identität des Anlagenbetreibers wird über das SMGW Zertifikat hergestellt und
2. Datensatz des Anlagenbetreibers wird vom SMGW an der Datenbank übertragen

nutzen zu können, muss die Architektur der Datenbank entsprechend aufgestellt werden: Das SMGW kommuniziert gemäß Technischer Richtlinie (TR) mit Marktpartnern (bzw. deren Systemen) über einen Infokanal; dem GWA steht ein Adminkanal zur Verfügung. Der Zugriff auf die Anlagendaten durch den Anlagenbetreiber erfolgt über die HAN Schnittstelle. Die Architektur der Datenbank daher

- die technischen Voraussetzungen bieten, um die Daten vom GWA an das SMGW zu übertragen, dort zu speichern und zu signieren
- die technischen Voraussetzungen bieten, um die Kommunikations-Verbindung, entweder:
    - ausgehend vom SMGW selbst oder
    - ausgehend von einem autorisierten Endgerät (z.B. Dongle/Zusatzmodule) auf der HAN Schnittstelle

  zur Anlagendatenbank zu ermöglichen (siehe hierzu 3.1.3.3).
- auf Seiten der Datenbank eine Funktion implementieren, die
    - die Verbindung autorisiert
    - den Datenstrom/Datensatz empfängt und dabei
        - die Identität des Absenders authentifiziert
        - die Daten, wenn möglich validiert/plausibilisiert und
        - in der Anlagendatenbank unter der festgestellten Identität des Anlagenbetreibers speichert.

Grundsätzlich sind die hierfür benötigten technischen Komponenten bereits marktgängig mit der Einführung der SMGW-Technologie verfügbar (SMGW Head-End, PKI-Modul und Funktionen zum Datenempfang über Infokanal, z.B. für Messwerte in einem Meter Data Management System (MDMS), Zusatzmodule für die HAN Schnittstelle des SMGW).

Wie im Zielbild unter Abschnitt 3.1.2.3 dargestellt, kann durch den Einsatz einer Blockchain-basierten Datenbanktechnologie und einer entsprechend geänderte Architektur der Datenbank die redundante Datenhaltung vermieden werden.

3.1.3.3 Kommunikation zwischen Smart Meter Gateway und Blockchain

Grundsätzlich bestehen drei Möglichkeiten, um eine Kommunikation zwischen Smart Meter Gateway und einem Blockchain Netzwerk zu realisieren:

1. Das Smart Meter Gateway fungiert selbst als Knoten im Netzwerk
2. Das Smart Meter Gateway sendet Daten direkt an einen Blockchain Knoten
3. Das Smart Meter Gateway sendet die Daten an einen Intermediär, welcher diese dann an einen Blockchain Knoten weiterleitet

Dabei ist anzumerken, dass es sich bei den auszutauschenden Daten in erster Linie um im Zeitverlauf relativ unveränderliche Stammdaten (bspw. Anschrift, technische Stammdaten, etc.) handelt. Demnach ist bei der Synchronisation der Blockchain-Knoten nicht mit einer großen Menge an Daten zu rechnen, deren effektiver Durchsatz vom gewählten Blockchain Protokoll abhängt.

Des Weiteren ist festzuhalten, dass die gewählte Kommunikationsstruktur starken Einfluss auf die zu formulierenden Anforderungen des Identitätsmanagements hat (siehe 3.1.3.43.1.3.4 Identitätsmanagement).

Smart Meter Gateway als Knoten

Aufgrund der bestehenden technischen Begrenzungen und des eigentlichen Zwecks des SMGW ist Möglichkeit 1 aus heutiger Sicht als nicht umsetzbar einzustufen. Dies rührt im Wesentlichen daher, dass das Smart Meter Gateway laut derzeit gültiger Spezifikation auf einer hierarchischen PKI aufbaut und das Kommunikationsmodell, trotz der möglichen sternförmigen Kommunikation, im Grunde genommen in die Kategorie Point-To-Point einzuordnen ist. Konkrete Hürden für die Nutzung des Smart Meter Gateways als Blockchain-Knoten sind:

- Peer-to-Peer (P2P) Kommunikation: Neben dem Konsensusmechanismus ist die Fähigkeit einer reinen P2P Kommunikation (Peer-Discovery etc.) eine Grundvoraussetzung für die Gewährleistung der Konsistenz innerhalb des Netzwerks. So können sich Netzwerk-Knoten in einem traditionellen Blockchain-Netzwerk gegenseitig auffinden und ihren Datenbestand synchronisieren. Im Gegensatz dazu, kann das Smart Meter Gateway nur mit Parteien kommunizieren, für die ein Kommunikationsprofil appliziert wurde.
- Kryptographie: Um die Authentizität von Anfragen und Nachrichten in einem Blockchain-Netzwerk zu überprüfen bedient man sich meist einfacher kryptographischer Primitive, welche einheitlich im Netzwerk verwendet werden. So ist jeder Knoten in der Lage Nachrichten zu signieren, Signaturen zu überprüfen und Nachrichten zu empfangen, ohne den Sender bzw. Empfänger wirklich kennen zu müssen. Das System beruht auf einfachen Signaturen. Im Gegensatz dazu, bedient sich das Smart Meter Gateway einer PKI welche mehrere kryptographische Primitive beinhaltet und zertifikatsbasiert ist.
- Datenhaltung: Das Smart Meter Gateway ist darauf ausgelegt die eigenen Daten für einen Zeitraum von mehr als 10 Jahren vorzuhalten. In einem Blockchain-Netzwerk hält üblicherweise jeder Knoten die gesamte Historie des Netzwerks. Der lokale Speicherplatzbedarf des SMGW steigt dadurch deutlich.

Um also ein SMGW als Knoten verwenden zu können, müsste die Architektur des Geräts zu einem Großteil neu entwickelt werden und gleichzeitig müsste auch ein anforderungsgerechtes Blockchain Protokoll entwickelt, bzw. ein bestehendes adaptiert werden. Dies schränkt die Pilotierungs- und eine eventuell mögliche, nachfolgende Marktverfügbarkeit einer solchen Variante ein.

Smart Meter Gateway sendet direkt an Knoten

Eine andere Möglichkeit, die Kommunikation zwischen einem Smart Meter Gateway und einem Blockchain Netzwerk herzustellen, wäre der direkte Push der Nachrichten vom SMGW an einen Blockchain Knoten.

Hierbei ist die Notwendigkeit von kompatiblen Cipher Suites (TLS/Sign/Encryption) und Datenformaten zu beachten. Um diese Kompatibilität herzustellen, wäre unter Umständen die Realisierung eines neuen Blockchain Protokolls notwendig. Im Ergebnis würde das bedeuten, dass ein Blockchain Knoten - abgesehen von den P2P-Networking Fähigkeiten und dem Konsensus-Algorithmus - stark einem Head-end System für die Smart Meter PKI ähnelt.

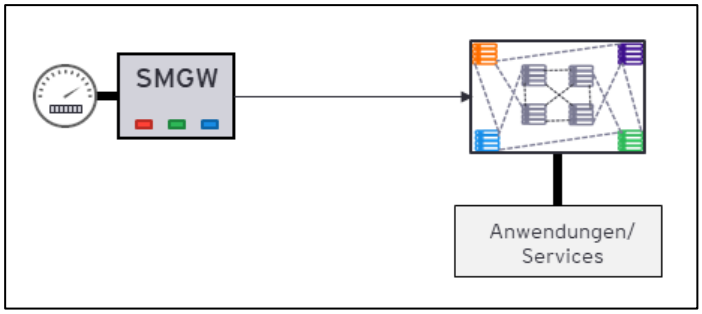


Abbildung 3: Direkte Kommunikation

Smart Meter Gateway sendet an Intermediär

Die dritte Möglichkeit der Kommunikation besteht in der Einbindung eines Intermediärs. Hierfür kommen mehrere Energiemarkt-Akteure in Frage. Das wesentliche Kriterium für das Intermediär-System ist die Fähigkeit, die Daten vom SMGW zu entschlüsseln und kompatible private Keys für das Blockchain Netzwerk zur Verfügung zu stellen. Folglich müsste das Intermediär-System eine Zuordnung von Public Keys aus der SM-PKI zu Private Keys für das Blockchain Netzwerk unter Einhaltung der PKI-Policy zur Verfügung stellen.

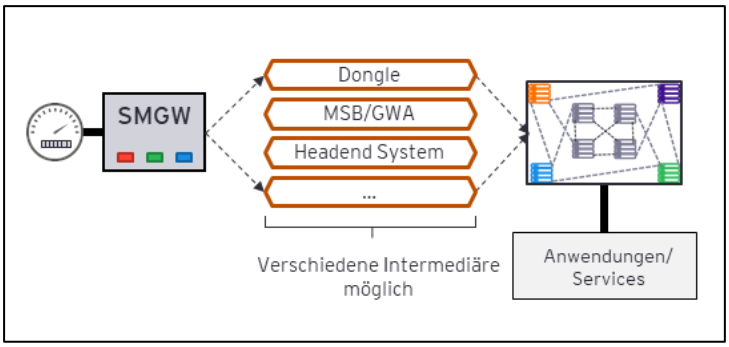


Abbildung 4: Indirekte Kommunikation

Conclusio

Während Variante 1 als Zukunftsperspektive einzustufen ist, wären Variante 2 und 3 unter bestimmten Annahmen (Wirtschaftlichkeit, Kooperation der Stakeholder etc.) bereits heute realisierbar. Ein wichtiges Unterscheidungsmerkmal ist die Definition von Intermediären in diesen Varianten.

Bei der direkten Kommunikation zwischen SMGW und einem Blockchain-Knoten wird die Nachricht vom Gerät direkt an den Knoten gesendet und im Netzwerk verteilt. Hier gibt es kein Intermediär-System im engeren Sinne, allerdings wäre die Bezeichnung Intermediär-Organisation, welche den Zugang zu dem Knoten verwaltet, treffend. Bei Variante 3, der Kommunikation mittels Intermediär, wird die Nachricht an ein Intermediär-System gesandt und von dort an einen Blockchain-Knoten weitergeleitet. Bei diesem System kann es sich bspw. um ein erweitertes Head-end System oder ein

Zusatzgerät im HAN des Endverbrauchers (Dongle) handeln. Somit besitzt diese Variante der Architektur immer ein Intermediär-System aber nicht in jedem Fall eine Intermediär-Organisation.

Im Ergebnis wird festgehalten, dass jede der genannten Varianten mit einem beträchtlichen Entwicklungsaufwand einhergeht, dessen genaues Ausmaß sich zu diesem Zeitpunkt nicht bestimmen lässt. Allerdings erfordert nicht jede Variante zwangsweise die Veränderung aller bestehenden Systeme (vgl. Tabelle 1: Kommunikationsvarianten und Entwicklungsbedarf in Systeme).

Entwicklungsbedarf der Kommunikationsvarianten					
	SMGW	**BC Protokoll**	**BC Knoten**	**Headend**	**Externe Hardware**
Variante 1	SEHR HOCH	SEHR HOCH	(Geht in SMGW auf)	---	---
Variante 2	---	HOCH	SEHR HOCH	(Geht in BC Knoten auf)	---
Variante 3	---	HOCH	MITTEL	MITTEL	HOCH bis SEHR HOCH

Tabelle 1: Kommunikationsvarianten und Entwicklungsbedarf von System

3.1.3.4 Identitätsmanagement

Die hierarchisch angelegte SM-PKI ist der integrale Bestandteil zur Wahrung der Daten-Authentizität und Zugriffskontrolle im heutigen System. Wie bereits unter 3.1.3.1 High-Level Architektur beschrieben, wird angenommen, dass die Struktur der SM-PKI konstant ist.

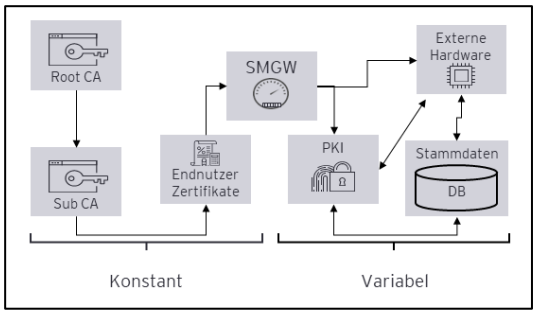


Abbildung 5: Komponenten für integriertes Identitätskonzept

Ein weiteres wesentliches Merkmal der hier verwendeten PKI ist die Notwendigkeit der Verwendung von Common Names (CN) auf den Zertifikaten der Marktteilnehmer (alle bis auf die Endverbraucher, sofern es sich um Privatpersonen handelt) und die Rollierung der zu verwendenden Zertifikate in rollenspezifischen Abständen.[10] Folglich gilt, dass es im derzeitigen System für Endverbraucher als Privatpersonen kein kryptographisch gesichertes Identitätsmerkmal gibt. Sollte ein Anwendungsfall nun die Identität eines Endnutzers benötigen (bspw. Kontrahierung eines neuen Liefervertrags und damit einhergehender Anbieterwechsel), sollte es im System die Möglichkeit geben, das Zertifikatsmaterial mit den notwendigen Stammdaten zu verknüpfen. Daraus ergibt sich die Notwendigkeit zur Vorhaltung der Stammdaten im System.

Grundsätzlich gibt es drei Möglichkeiten diese Daten im System zur Verfügung zu stellen:

Zentrale Speicherung

Die womöglich einfachste Lösung wäre die Etablierung eines zentralen Service, analog zum heutigen Marktdatenstammregister, welcher für die Verwaltung der PID und Stammdaten verantwortlich wäre. Vorteile dieser Lösung wären u. A. die Abwesenheit von Datenpartitionen und eine hohe Effizienz

[10] Certificate Policy der Smart Metering PKI, Version 1.1.1, S. 20ff;

durch mögliche Synergien mit dem Marktdatenstammregister. Nennenswerte Nachteile wären die Notwendigkeit eines dedizierten Betreibers sowie eines neuen Autorisierungskonzepts. Zusätzlich wäre eine solche Lösung als ein Single Point of Failure im System einzustufen.

Verteilte Speicherung

Bei der verteilten Speicherung werden Stammdaten an jenen Orten vorgehalten, wo sie bereits heute existieren, nämlich bei den Marktteilnehmern wie bspw. Netzbetreibern, Lieferanten und Messstellenbetreibern. Dies hätte den Vorteil, dass zum Großteil auf bereits vorhandene Dateninfrastruktur zurückgegriffen werden kann. Jedoch müsste auch hier ein neues Autorisierungskonzept geschaffen werden. Zudem wären die Daten in einem hohen Maße partitioniert, was einen gesonderten Service zur Auffindbarkeit relevanter Daten erfordern würde. Letztlich wäre noch die starke Abhängigkeit von den Marktteilnehmern als Betreibern des verteilten Systems zu nennen.

Dezentrale Speicherung

Eine weitere, oft außer Acht gelassene Möglichkeit wäre die Speicherung der Daten auf einem externen Hardwaregerät im HAN des SMGW-Endnutzers, also am ‚Rand' des Systems. Dieses Gerät könnte als eine Art Tresor für die PID des Endverbrauchers dienen und kann die Selbstverwaltung der Daten durch diesen selbst ermöglichen. Auch die Autorisierung für den Datenzugriff könnte vom Endnutzer selbst verwaltet werden.[11]
Hierbei sind allerdings zwei wesentliche Punkte zu beachten: Erstens liegen zu dieser Technologie noch keine Erfahrungen aus großen Anwendungsfällen vor und zweitens sollten eigene Richtlinien und Zertifizierungsprozesse für Hersteller solcher Geräte geschaffen werden.

3.1.3.5 Blockchain

Blockchain als digitale Infrastruktur

Der Begriff Blockchain beschreibt eine spezielle technische Realisierung der Integritätssicherung, bei der Einträge in Blöcke zusammengefasst und durch kryptographische Hash-Funktionen zu einer praktisch unveränderlichen Folge verkettet werden. Obwohl die Blockchain-Technologie ursprünglich zur technischen Umsetzung einer digitalen Währung konzipiert wurde, sind insbesondere modernere Ausprägungen als generisch nutzbare digitale Infrastruktur anzusehen. Diese Infrastruktur erlaubt es, ihre Eigenschaften wie bspw. Manipulationssicherheit über Schnittstellen für verschiedenartige Anwendungen nutzbar zu machen und diese zu verbreiten. Auf technischer Ebene interagiert die Blockchain dabei in der Regel mit herkömmlichen IT-Systemen und wird nicht als alleinstehende Infrastruktur genutzt.

Architekturempfehlungen

Im folgenden Abschnitt wird die Unterscheidung verschiedener technisch-konzeptioneller Modelle von Blockchain Systemen anhand mehrerer Designkriterien getroffen sowie konkrete Empfehlungen für den ausgewählten Anwendungsfall ausgesprochen.

Privat vs. Öffentlich

Zum einen können diese privat oder öffentlich sein. Ausschlaggebend dafür ist, durch wen sich die Systeme verwenden lassen, das heißt, wer Zugriff auf die Daten hat bzw. neue Dateninputs vorschlagen darf. Ist diese Verwendung jedermann gestattet, handelt es sich um ein öffentliches System; ist sie jedoch auf eine Organisation oder ein Konsortium beschränkt, ist das Blockchain-System als privat anzusehen.

[11] Eine Möglichkeit dies zu realisieren wären bspw. Decentralized Identifiers : https://w3c-ccg.github.io/did-spec/

Wird der Zugang eines Systems beschränkt und unterliegt der Kontrolle einzelner Teilnehmer bzw. einer beschränkten Anzahl von Akteuren, kann nicht per se von dem Erhalt der Attribute einer öffentlichen Blockchain ausgegangen werden. Die Unveränderlichkeit der Historie und die hohe Sicherheit gegen viele Angriffsvektoren ist in einem öffentlichen Blockchain stärker ausgeprägt. Siehe dazu auch die Ausführungen bezüglich des Konsens Algorithmus im weiteren Kapitel.

Empfehlung

Da in öffentlichen Blockchain-Systemen die Verkehrsdaten der Netzkommunikation beobachtet und gespeichert werden können, ist für den ausgewählten Anwendungsfall die Beschränkung auf private bzw. eine Konsortial-Blockchain sinnvoll. Öffentlicher Zugang sowie vollständige Transparenz wäre gemäß der definierten Erfolgskriterien nicht vereinbar mit den heutigen Grundprinzipien, bzw. dem Grundsatz, dass keine disruptive Veränderung erwünscht ist.

on-chain vs. off-chain Datenhaltung

Daten sind heterogen und unterschiedlich relevant. Daher ist eine Differenzierung, wo Daten gespeichert werden notwendig.

Bei der sogenannten **„on-chain" Datenspeicherung**, werden Daten direkt in der Blockchain gespeichert und somit auf jedem Knoten der Teilnehmer repliziert. Die vollständige und sofortige Replikation hat eine hohe Redundanz und somit eine garantierte Verfügbarkeit zur Folge. Folglich ist die Datendurchsatz limitiert und die Kapazität begrenzt.

Im Gegensatz dazu werden bei der sogenannten „**off-chain" Datenspeicherung** Daten außerhalb der Blockchain gespeichert. Dadurch entfallen Nachteile der on-chain Datenspeicherung wie die Einschränkung des Datendurchsatzes. Außerdem können Daten einfacher vor dem Zugriff weiterer Teilnehmer des Blockchain Systems geschützt werden. Allerdings können Daten nachträglich verändert werden, im Gegensatz zur on-chain Speicherung Unveränderbarkeit nicht gegeben ist. Eine Möglichkeit um die Nachteile teilweise zu kompensieren, ist es die Zugangsberechtigungen in der Blockchain zu speichern.

Empfehlung:

Nur Daten, die systemrelevant sind, wie etwa übergreifend benötigte Marktstammdaten sollten on-chain gespeichert werden. Dabei sind personenbezogene Daten durch kryptografische Verschlüsselung zu schützen. Alle Daten, die in großer Menge anfallen, wie etwa Transaktionsdaten, können mit dem heutigen Stand der Blockchain-Technologie nur off-chain gespeichert werden. Das Kriterium der unverfälschbaren Nachvollziehbarkeit von Daten und Transaktionen wird durch die Kombination des als Vertrauensanker agierenden SMGW, sowie der Blockchain sichergestellt. Die konkrete technische Implementierung ist im Zuge eines Piloten zu validieren.

Konsensalgorithmus und Skalierbarkeit

Die limitierte Anzahl von Transaktionen muss in Blockchain Systemen besonders berücksichtigt werden. Öffentliche Blockchains wie beispielsweise Ethereum oder Bitcoin, haben die höchstmögliche Integrität als Fokus. Da alle Daten synchronisiert werden müssen, geht dies zu Lasten des Datendurchsatzes. Dieser beträgt typischerweise nur wenige Transaktionen pro Sekunde.

Unterschiedliche Topologien (privat, konsortial, öffentlich) und hybride Mischformen können diese Herausforderungen adressieren. Indem nur Teilnehmer zugelassen werden, denen man bereits vertraut, kann der zugrundeliegende Konsensalgorithmus so adaptiert werden, dass dieser einen höheren Datendurchsatz ermöglicht.

Eine weitere Möglichkeit ist, eine „Sidechain" zu verwenden. Eine Sidechain ist eine Blockchain, die mit einer anderen Blockchain, der „Hauptchain" verbunden ist, wobei eine Hauptchain über mehrere

Sidechains verfügen kann. Ein großer Vorteil von Sidechains besteht darin, dass mit ihnen eine höhere Skalierbarkeit ermöglicht werden kann.

Empfehlung:

Um ein Blockchain System nachhaltig in das bestehende System integrieren zu können, muss dieses auch einen hohen Datendurchsatz bewältigen können (siehe Anforderungen des P2P-Anwendungsfalls, z.B. Speicherung von Messdaten). Durch die Beschränkung auf eine private bzw. Konsortial-Blockchain kann der Datendurchsatz im Vergleich zu öffentlich Blockchains erhöht werden. Je nach Menge der anfallenden Transaktionen ist der Einsatz von Sidechains gegebenenfalls sinnvoll. Da Sidechains sich in einem Stadium experimenteller Technologie befinden, ist es unerlässlich, diese in einem Piloten für den konkreten Anwendungsfall zu überprüfen.

Teilnehmer und Rollen

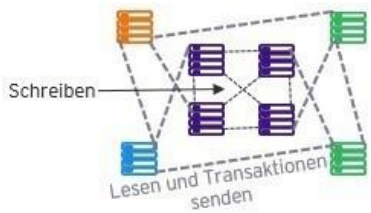
Grundsätzlich ist die Blockchain-Technologie so ausgelegt, dass diese nicht von der Existenz bzw. Verfügbarkeit von einzelnen Teilnehmern abhängt. Vielmehr können Teilnehmer jederzeit beitreten oder austreten ohne das System zu gefährden.

Empfehlung:

In Abgleich mit den unterschiedlichen Teilnehmern im heutigen Energiemarkt (Anlagenbetreiber, Messstellenbetreiber, Netzbetreiber, Lieferanten, Behörden) wird auch ein Blockchain-Netzwerk von mehreren Teilnehmern mit unterschiedlichen Rollen betrieben. Unterschiedliche Optionen für den Betrieb eines Netzwerks sind möglich. Einige dieser Konstellationen (nicht taxativ) sind:

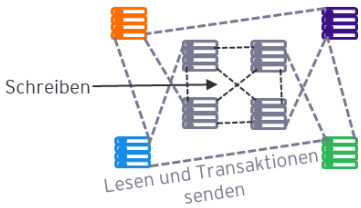
Option 1

- Alle Marktteilnehmer und Behörden betreiben Knoten
- Jeder Teilnehmer hat Lese- und Schreibrechte



Option 2

- Netzwerkknoten werden von Behörden betrieben mit vollen Schreibrechten
- Marktteilnehmer betreiben Knoten mit Leserechten



Option 3

- Netzwerkknoten werden von dedizierten Entitäten betrieben
- Alle Marktteilnehmer, Behörden und Endkunden können Leseknoten betreiben

Vorteile der Blockchain-Technologie

Im folgenden Abschnitt werden technische und wirtschaftliche Vorteile der Blockchain-Technologie beleuchtet. Dabei soll neben allgemeinen Aspekten besonders auf den ausgewählten Anwendungsfall eingegangen werden.

Integrität

Die Tatsache, dass bei Verwendung eines Blockchain Protokolls keine nachträglichen Änderungen stattfinden können, bedingt die Unveränderlichkeit von Daten. Technisch gesehen wird dies über den Einsatz sogenannter „Merkle-Trees" in den einzelnen Blöcken erreicht, in denen Hashes gespeichert werden. Durch die resultierende Garantie eines integren Systems kann Vertrauen unter allen Teilnehmern geschaffen werden. Dieses neu geschaffene Vertrauen kann die Grundlage für neue Formen der Zusammenarbeit sein und großes wirtschaftliches Potenzial ermöglichen.

Konsistenz

Ein zentraler Vorteil der Blockchain-Technologie ist, dass eine sogenannte „Single Source of Truth" garantiert wird. Somit hat jeder Teilnehmer die Sicherheit, dass für alle Teilnehmer genau ein und derselbe Datenbestand existiert. Die Energiewirtschaft profitiert somit klar durch Existenz eines verifizierten, bilanzkreisübergreifend korrekten Datensatz. Dieser kann unterschiedliche Auffassungen ausräumen bzw. im Falle eines Rechtsstreits zur schnellen Beilegung herangezogen werden.

Transparenz

Der Einsatz von Blockchain-Technologie bringt grundsätzlich eine erhöhte Transparenz. Somit sind systemkritische Daten für alle Teilnehmer verfügbar. Durch Sicherheitsmaßnahmen, wie etwa rollenbasierte Zugriffsrechte, ist gewährleistet, dass nur berechtigte Teilnehmer Einsicht in Daten erhalten können.

Aktualität

Zentrale Aufgabe eines Blockchain Systems ist die Synchronisation der Daten. Alle auf der Blockchain gespeicherten Daten werden somit in Echtzeit bei allen Teilnehmern synchronisiert vorgehalten. Somit kann aufwändiges Reporting zwischen den Teilnehmern des Systems stark reduziert werden bzw. entfallen. Dies bringt Potenzial für signifikante wirtschaftliche Einsparungen mit sich.

Nachvollziehbarkeit

Die ordnungsgemäße Durchführung aller Transaktionen wird durch Verwendung einer Blockchain sichergestellt. Somit existiert eine einsehbare Beweiskette, die belegt, dass die beteiligten Parteien ihren Verträgen nachgekommen sind. Dadurch können Streitfälle im Vorhinein vermieden werden, was ebenfalls zur Einsparung von Kosten beträgt.

Robustheit

Ausfallsicherheit wird dadurch gewährleistet, dass jeder Netzknoten einen gemeinsamen Status des Systems gespeichert hat. Dies impliziert, dass der Ausfall einzelner Rechner keinen Verlust des Systemstatus bedeutet. Ein Blockchain System kann als sicherere und robuste digitale Umgebung betrachtet werden, da kein isolierter Angriffspunkt existiert. Die Erreichung der Prämisse der Versorgungssicherheit wird dadurch gestärkt und mögliche wirtschaftliche Risiken durch Ausfälle im Vorhinein vermieden.

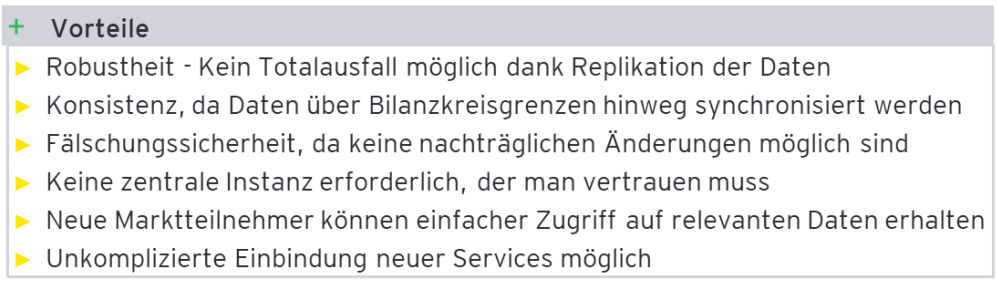


Abbildung 6: Übersicht von Vorteilen der Blockchain-Technologie

Nachteile der Blockchain-Technologie

Im folgenden Abschnitt werden den genannten Vorteilen der Blockchain-Technologie hinsichtlich des gewählten Anwendungsfalls etwaige Nachteile gegenübergestellt.

Ressourcenverbrauch

Je nach Auswahl des Konsensalgorithmus ist der Ressourcenverbrauch von Blockchain-Technologie im Vergleich zu konventionellen Technologien zu bewerten. So kommt es beim Einsatz eines sogenannten „Proof-of-Work" Algorithmus, wie etwa in der Bitcoin Blockchain, zu einer starken Mehrbelastung im Vergleich zu konventionellen Lösungen.

Bei modernen Blockchains, die alternative Konsensalgorithmen, wie etwa sogenannte „Proof-of-Stake" oder „Proof-of-Authority" Algorithmen einsetzen, tritt ein derartiger Mehrverbrauch an Ressourcen allerdings nicht auf. Diese Algorithmen sind insbesondere in privaten und konsortialen Blockchains Standard und gewährleisten ebenfalls die Stabilität und Sicherheit des Netzwerks.

Effizienz

Während die redundante Datenhaltung auf allen Blockchain Knoten eine höhere Ausfallsicherheit und Robustheit gewährleistet, wirkt sich diese negativ auf die Effizienz des Systems aus. Die Mehrkosten sind einer geringeren Ausfallrate und damit verbundenen Vorteilen gegenüberzustellen und in einem Piloten zu verifizieren.

Technische Komplexität

Für die optimale Erfüllung der Anforderungen des Anwendungsfalls muss ein bestehendes Blockchain Protokoll angepasst werden oder eine neue Form eines Blockchain Protokolls entwickelt werden. Geeignete Blockchain Protokolle, sowie notwendige Anpassungen sind im Rahmen der Pilotphase zu ermitteln, da diese von den Anforderungen der Marktteilnehmer abhängen. Wie bei jedem gemeinsam verwendeten Software-System, ist auch bei Verwendung einer Blockchain ein Mindestmaß an Koordination notwendig. Nur so kann die technische Weiterentwicklung im Einklang betrieben werden, sowie durch Updates die Blockchain Software bei allen Betreibern von Knoten auf demselben Stand gehalten werden.

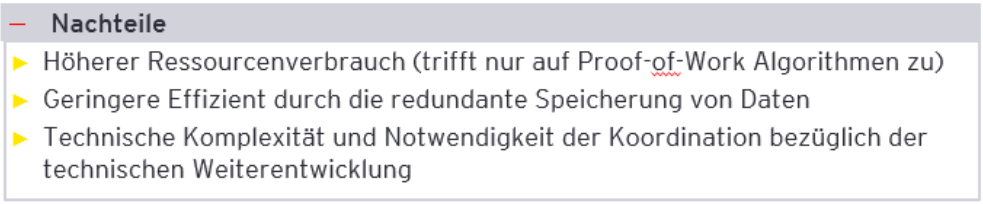


Abbildung 7: Übersicht von Nachteilen der Blockchain-Technologie

Fazit

Beim Status Quo handelt es sich um ein verteiltes System, wobei Netzbetreiber sowie Lieferanten Daten lokal speichern, aber keine automatisierte Austauschbarkeit möglich ist.

Aus rein technischen Gründen ist die Nutzung von Blockchain nur teilweise sinnvoll, da für die redundante Datenhaltung eine geringere Effizienz als bei zentralen Systemen gegeben ist. Vielmehr ist der Einsatz wirtschaftlich bzw. organisatorisch motiviert. So können bspw. Prozesse effizienter gestaltet werden, indem direktes Vertrauen ohne die Einbindung zentraler Betreiber hergestellt werden kann (Vermeidung von Intermediären).

Blockchain unterstützt dabei, organisationsübergreifende Prozesse abzuwickeln, ohne dass dafür eine zentrale Datenhaltung nötig sind.

Blockchain bietet grundsätzlich eine höherwertige, digitale Infrastruktur für effizientes Wirtschaften. Künftig können über diese neutrale Plattform vor allem auch innovative, neue Services angeboten werden und somit neue Geschäftsmodelle entstehen. Langfristig überwiegen somit die wirtschaftlich positiven Effekte, der erhöhten Ausfallsicherheit, der Kostenreduktion des aufwändigen Recordings, sowie von Streitfällen und damit verbundenen rechtlichen Kosten die Mehraufwände durch technisch ineffizientere Datenhaltung.

Die digitale Identität sowie die Integrität der Transaktionsdaten werden dabei durch das SMGW, welches als Vertrauensanker fungiert, sichergestellt. Dadurch ist es deutlich einfacher, neue Marktteilnehmer kontrolliert und sicher an diesem System teilnehmen zu lassen.

Auch der Export ausgewählter Daten und die öffentliche Bereitstellung dieser im Zuge der Open Data Initiative der Bundesregierung ist möglich.

Das System unterstützt die Energiewende: Die Verwendung von dezentralen, erneuerbaren Energieanlagen wird attraktiver für Unternehmer und Bürger. Kritische Marktteilnehmer werden weiterhin eingebunden und behalten die Kontrolle über das System.

Aus technischer Sicht erscheint die Umsetzbarkeit auf Basis des SMGW mit einem Erweiterungsmodul und die Verwendung einer Konsortial-Chain die vielversprechendste Variante und wird für die Ausarbeitung des Pilotkonzepts im Arbeitspaket 2 vorgeschlagen.

3.1.3.6 Datenerhebung

Die vorgeschlagene Zielarchitektur hat Anforderungen an das Informations-Modell, analog zu dem des MaStR.

Um den Nutzen der unter Abschnitt 3.1.2.3 aufgezeigten Funktionen des Zielmodells realisieren zu können, insbesondere für die zweite Funktion, aus

1. Identität des Anlagenbetreibers wird über das SMGW Zertifikat hergestellt
2. Datensatz des Anlagenbetreibers wird aus dem SMGW an die Anlagendatenbank übertragen

müssen die Daten im Prozess frühzeitig und möglichst vollständig erhoben und über das SMGW mit der Identität des Anlagenbetreibers signiert in die Datenbank übertragen werden.

Wie in Abschnitt 3.1.2 beschrieben, stammen die benötigten Daten aus diversen Quellen (bspw. Anlagenbetreiber, Anlagen-Hersteller und - Installateur, MSB, NB). Der (Teil-)Prozess mit dem Ziel der Erhebung der Daten liegt hier außerhalb der technischen Betrachtung der Aufgabenstellung, sollte aber im Rahmen der Evaluierung im Konzept des Piloten mit AP2 Berücksichtigung finden.

Die mit dem Anwendungsfall bereitgestellten authentischen Informationen sind einer Nachnutzung zugänglich. Für andere Anwendungsfälle wie zum Beispiel P2P-Handel sind aber weitere Informationsobjekte erforderlich, die aktuell nicht Bestandteil des Informationsmodells des MaStR sind. So können Informationen zum Messkonzept, Mess- und Abrechnungslokation, einer Nachnutzung in anderen Prozessen dienlich sein. Die Möglichkeit der gesicherten Prüfbarkeit der vertraulichen, in der Datenbank abgelegten, Informationen durch Dritte mittels der vom Anlagenbetreiber dafür freizugebenden, öffentlichen Identität (public key) ist ein weiterer Vorteil. Beide Szenarien erfordern eine Detailierung bzw. Erweiterung des Informations- und Service-Modells der Datenbank und sollten eine sinnvolle, erweiterte Nutzbarkeit zeigen – über den skizzierten Anwendungsfall hinaus, z.B. im Rahmen der Umsetzung des in AP2 zu konzipierenden Piloten.

3.1.4 Rechtliche und regulatorische Fragestellungen

Aus regulatorischer Sicht wurde zunächst der Anwendungsfall einer Peer-to-Peer Strombelieferung bewertet. Im Ergebnis bestehen derzeit große Herausforderungen, insbesondere im Zusammenhang mit dem Prozess des Lieferantenwechsels, dem Bilanzkreismanagement und den Verpflichtungen der einzelnen Marktakteure u. a. nach dem EnWG und EEG. Aktuell sind einzelne Lösungsansätze zur (vorübergehenden) Überbrückung der regulatorischen Herausforderungen zwar denkbar, auf lange Sicht dürfte eine unmittelbare „echte" Peer-to-Peer Strombelieferung jedoch eine (umfangreiche) Anpassung des regulatorischen Rahmens erfordern. Aus diesem Grund ist der Anwendungsfall derzeit nicht geeignet, die erfolgreiche Umsetzung eines Piloten in AP2 sicherzustellen.

Als ersten Schritt auf dem theoretisch möglichen Weg zu einer echten Peer-to-Peer Strombelieferung sieht der neu entwickelte Anwendungsfall die Einführung einer Plug & Play Lösung für eine öffentliche Datenbank vor.

3.1.4.1 Anwendungsfall Peer-to-Peer Strombelieferung

Bei der juristischen Bewertung des Anwendungsfalls einer Peer-to-Peer Strombelieferung ist zu beachten, dass der Strommarkt ein hoch regulierter Bereich ist. Hintergrund der Regulierung ist dabei insbesondere die Sicherstellung der Versorgungssicherheit, die Öffnung des Marktes für einen freien und fairen Wettbewerb sowie der Schutz des Letztverbrauchers. Um diese Kernziele des Energierechts abzusichern, knüpft der derzeitige regulatorische Rahmen an die verschiedenen Marktrollen gesetzliche Verpflichtungen und Vorgaben an. In diesem Rahmen ist eine unmittelbare „echte" Peer-to-Peer Strombelieferung nicht vorgesehen. Insbesondere aufgrund der Energiewende und der damit verknüpften Digitalisierung besteht jedoch der Wunsch, dem aktiven Letztverbraucher – dem Prosumer – mehr Gestaltungsspielraum bei der Energieversorgung zu lassen und somit auch die unterschiedlichen Prozesse zu beschleunigen. In diese Stoßrichtung versendet auch der europäische Gesetzgeber erste Signale, indem er in der Strombinnenmarktrichtlinie 2019[12] einen schnelleren Lieferantenwechsel vorsieht und den „aktiven Kunden" (Prosumer) als eigenen Marktakteur wahrnimmt. Dennoch führt die Peer-to-Peer Strombelieferung zu verschiedenen regulatorischen Herausforderungen.

3.1.4.1.1 Aktuelle regulatorische Herausforderungen bei einer Peer-to-Peer Strombelieferung

Die aktuellen regulatorischen Herausforderungen liegen bei einer Peer-to-Peer Strombelieferung insbesondere bei den folgenden Aspekten:

- Lieferantenwechsel und GPKE
- Bilanzkreismanagement
- Verpflichtungen nach EnWG / EEG u. a.

Darüber hinaus ist ggf. das Doppelvermarktungsverbot nach § 80 EEG 2017 zu beachten.

[12] Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinien 2012/27/EU.

Lieferantenwechsel und GPKE

Der aktuelle regulatorische Rahmen ist auf eine konstante Strombelieferung über ein Elektrizitäts-/Energieversorgungsunternehmen („**EVU**“) ausgelegt und sieht keine sich kurzfristig ergebende und nur vorübergehende Peer-to-Peer Strombelieferung, wie im Anwendungsfall aufgezeichnet, vor. Dies ergibt sich u. a. aus den Regelungen zum Lieferantenwechsel (§ 20a EnWG, § 14 StromNZV) und der damit zusammenhängenden Prozessbeschreibung der Bundesnetzagentur „Geschäftsprozesse zur Kundenbelieferung mit Elektrizität“ („**GPKE**“).[13]

Eine kurzfristige Peer-to-Peer Strombelieferung stellt nach den genannten Regelungen einen Lieferantenwechsel dar und löst somit ein aufwendiges und standardisiertes Verfahren mit einer Umsetzungsfrist von bis zu drei Wochen aus.

Zwar ist in der Strombinnenmarktrichtlinie 2019 zukünftig eine Verkürzung des Lieferantenwechsels vorgesehen (Art. 12 Abs. 1), jedoch erst ab dem Jahr 2026. Der Lieferantenwechsel muss dann an allen Werktagen innerhalb von „nur noch“ 24 Stunden erfolgen. Im Ergebnis dürfte diese Regelung jedenfalls kurzfristig keine wesentliche Verbesserung für den geschilderten Use Case mit sich bringen, da dieser u.a. einen stündlichen Wechsel des Stromlieferanten vorsieht.

Unabhängig von der zeitlichen Komponente müsste der Prosumer als neuer Stromlieferant / EVU im vorgesehenen Anwendungsfall bei jeder neuen Strombelieferung die Vorgaben zum Lieferantenwechsel einhalten.

Bilanzkreismanagement

Zur Sicherstellung der Versorgungssicherheit wird die Ausgeglichenheit zwischen Einspeisung und Strombezug durch den jeweiligen Bilanzkreisverantwortlichen – i. d. R. ein EVU – und den jeweils zuständigen Übertragungsnetzbetreiber überwacht und sichergestellt (vgl. § 4 StromNZV). Jede Einspeise- oder Entnahmestelle wird zu diesem Zweck anhand entsprechender netzrelevanter Zählpunkte einem Bilanzkreis zugeordnet. Die Zuordnung des jeweiligen Zählpunktes sowie die Bewirtschaftung des Bilanzkreises erfolgt auf der Grundlage eines Vertrages mit dem Bilanzkreisverantwortlichen, i. d. R. auf der Grundlage eines Stromliefervertrages mit einem EVU, einem Bilanzkreisvertrag zwischen dem Bilanzkreisverantwortlichen und dem zuständigen Übertragungsnetzbetreiber und unter Anwendung der GPKE. Ein Lieferantenwechsel löst i. d. R. einen Bilanzkreiswechsel aus, d. h. die Abmeldung beim bisherigen Bilanzkreis und die Anmeldung beim neuen Bilanzkreis.

Bei einer wie im Anwendungsfall zunächst vorgesehenen Peer-to-Peer Strombelieferung würde (i) die Entnahmestelle des Letztverbrauchers punktuell ggf. dem Bilanzkreis des Prosumers zugeordnet werden, (ii) der Prosumer müsste daher auch vor diesem Hintergrund die GPKE zum Lieferantenwechsel einhalten und (iii) der Prosumer müsste das Bilanzkreismanagement, d. h. Ausgeglichenheit zwischen Einspeisung und Strombezug, sicherstellen.

Insofern ist auch in der Strombinnenmarktrichtlinie 2019, Art. 15 Abs. 2 lit. f, vorgesehen, dass grundsätzlich der „aktive Kunde“ (Prosumer) für im Stromnetz verursachte Ungleichgewichte finanziell verantwortlich und in dieser Hinsicht Bilanzkreisverantwortlicher ist – es sei denn, er delegiert die Bilanzkreisverantwortung.

[13] Anlage 1 zum BNetzA Beschluss BK6-16-200 vom 20.12.2016.

Verpflichtungen nach EnWG / EEG u. a.

Die Verpflichtungen, die mit den im Energierecht bekannten Marktrollen verknüpft sind, würden ebenfalls im Rahmen einer Peer-to-Peer Strombelieferung den Prosumer stark belasten.

Gemäß § 3 Nr. 18 EnWG und § 3 Nr. 20 EEG würde der Prosumer durch die – auch wenn nur kurzfristige – Stromlieferung an andere Letztverbraucher zum EVU werden. Diese Marktrolle wäre an umfangreiche Verpflichtungen geknüpft, die den Prosumer regelmäßig überfordern dürften. Beispielhaft seien zur Illustration die folgenden EVU-Verpflichtungen genannt:

- aus dem EEG:
  - (Erhebung und) Abführung der EEG-Umlage
  - Meldepflichten gegenüber dem ÜNB / der BNetzA
- aus dem EnWG:
  - Anzeigepflicht der Belieferung ggü. BNetzA
  - Anforderungen an Stromliefervertrag, Rechnungstellung und Stromkennzeichnung
  - Bei All-Inclusive-Verträgen: Abwicklung der Netznutzung durch den Letztverbraucher
- Sonstige Verpflichtungen
  - Registrierung im Marktstammdatenregister
  - Informations- und Beratungspflichten nach dem EDL-G.

3.1.4.1.2 Regulatorische Lösungsansätze für eine Peer-to-Peer Strombelieferung

Für die in Abschnitt 3.1.4.1.1 aufgezeigten regulatorischen Herausforderungen lassen sich erste Lösungsansätze im Sinne einer Überbrückung des aktuellen regulatorischen Rahmens finden. Auf lange Sicht dürfte eine unmittelbare „echte" Peer-to-Peer Strombelieferung jedoch eine (umfangreiche) Anpassung des regulatorischen Rahmens bedürfen. Denkbar sind dabei Lösungsansätze, die den bisherigen regulatorischen Rahmen durch Hinzuziehung eines Intermediärs unberührt lassen und solche, die den regulatorischen Rahmen anhand von Experimentierklauseln bzw. Ausnahmeregelungen modifizieren.

Perspektiven für den Use Case mit Intermediär

Der Einsatz eines Intermediärs ist eine in der Praxis bereits bestehende Abwandlung der Peer-to-Peer Strombelieferung, auch unter Einbindung von Blockchain-Technologien. Durch den Einsatz eines Intermediärs würde der Use Case abgewandelt werden müssen und zwar weg von einer unmittelbaren „echten" Peer-to-Peer Strombelieferung, hin zu einer mittelbaren Peer-to-Peer Strombelieferung. Die genaue Ausgestaltung dieses Ansatzes bedürfte einer tiefergehenden Prüfung.

Dabei sind zwei verschiedene Modelle denkbar:

- Der Intermediär als EVU kauft den erzeugten Strom ein und verkauft ihn an Letztverbraucher. In diesem Fall liegt im Falle des Wechsels des Stromerzeugers kein Lieferantenwechsel vor, da der Intermediär durchgehend der Lieferant, d. h. das EVU, bleibt.
- Der Intermediär als Dienstleister wird nicht EVU, übernimmt jedoch als Dienstleister die typischen EVU-Verpflichtungen wie Bilanzkreismanagement, Vertragsgestaltung, Abrechnung etc. In diesem zweiten Modell findet bei jedem Wechsel des Stromerzeugers ein Lieferantenwechsel statt, welcher die oben beschriebenen Prozesse auslöst.

Der hier anvisierte Anwendungsfall, mit im Einzelfall stündlich wechselndem Stromlieferanten, könnte daher unter Einschaltung eines Intermediärs nur dann umgesetzt werden, wenn der Intermediär auch als EVU agieren würde.

Perspektiven für den Use Case ohne Intermediär

Für die Umsetzung des Anwendungsfalls einer „echten" Peer-to-Peer Strombelieferung, ist eine Überbrückung der regulatorischen Herausforderungen anhand von Experimentierklauseln, Ausnahmevorschriften oder Verordnungsermächtigungen zugunsten von Kleinsterzeugern und Kleinstverbrauchern denkbar.

Entsprechende Vorschriften könnten z.B. folgendermaßen ausgerichtet werden:

- Der Prosumer wird durch eine Stromlieferung nicht zum EVU, z.B. solange die jährlich gelieferte Strommenge eine bestimmte Schwelle unterschreitet. Dieser Ansatz könnte sich z.B. an § 2 Nr. 12 EDL-G orientieren. Gem. § 2 Nr. 12 EDL-G wird die Eigenschaft als Energielieferant u. a. an dem Verkauf des Äquivalents einer jährlichen Energiemenge geknüpft bzw. an die Anzahl der beschäftigten Personen bzw. an den Jahresumsatz und die Jahresbilanz.
- Der Prosumer bleibt trotz Stromlieferung an einen anderen Letztverbraucher selbst Letztverbraucher bzw. wird mit diesem gleichgestellt. Dieser Ansatz könnte sich z.B. an § 3 Nr. 25 EnWG (Definition der Ladesäule) orientieren.

Der zeitliche und inhaltliche Aufwand für die Ausarbeitung solcher Vorschriften sollte nicht unterschätzt werden. Inhaltlich muss insbesondere größte Sorgfalt bei der Formulierung an den Tag gelegt werden, um sämtliche regulatorische Herausforderungen verschiedenster Gesetze abzudecken. Dies bedürfte einer tiefergehenden Überprüfung.

3.1.4.2 Anwendungsfall automatisierte Pflege einer öffentlichen Datenbank

Aus regulatorischer Sicht wird für den Anwendungsfall der automatisierten Pflege einer öffentlichen Datenbank insbesondere Folgendes zu beachten sein:

- Möglichkeit der Einbindung von Blockchain und SMGW bei der Registrierung in der Z öffentlichen Datenbank unter den aktuell regulatorischen Rahmenbedingungen des EnWG und der MaStRV
- Übereinstimmung des in Abschnitt 3.1.2.3 dargestellten Prozesses mit den Vorschriften zur Datenkommunikation sowie dem Aufgabenkreis des GWA.

Neben regulatorischen Aspekten stellen sich bei einer automatisierten Anmeldung in der öffentlichen Datenbank insbesondere datenschutzrechtliche Fragestellungen. Hierbei wird unter genauer Darstellung der einzelnen Datenprozesse darauf einzugehen sein,

- ob für die Einbindung von MSB, GWA und NB entsprechende datenschutzrechtliche Erlaubnistatbestände bestehen,
- ob der in Abschnitt 3.1.2.3 dargestellte Prozess den Anforderungen der Datenschutzgrundsätze, insbesondere dem Transparenzgebot, entspricht und
- ob die Betroffenenrechte hinreichend gewahrt werden.

3.1.4.2.1 Regulatorischer Rechtsrahmen

Der aktuelle regulatorische Rechtsrahmen stellt unterschiedliche Anforderungen an den Prozess der Registrierung im MaStR, welcher im EnWG (§§ 111e, f) sowie in der MaStRV geregelt ist, und an die Nutzung und Einbindung des SMGW (MsbG).

Zur Ausgestaltung der in §§ 111e, f EnWG geregelten Registrierungspflicht im MaStR hat das BMWi die MaStRV erlassen. Diese bestimmt:

- welcher Marktakteur und welche Anlage im MaStR zu registrieren sind (§§ 3, 5 MaStRV),
- welche Daten der Registrierungspflicht unterliegen (§ 6 i.V.m. Anlage 1, Tabelle 1 und 2 zur MaStRV),
- wann die Registrierung zu erfolgen hat (§§ 3 Abs. 2, 5 Abs. 5 MaStRV),
- wie die Registrierung zu erfolgen hat (§ 8) und
- welche Konsequenzen aus einem Verstoß gegen die Registrierungspflicht resultieren (§§ 21, 23).

Demnach ist die Pflicht zur Registrierung zunächst personengebunden und knüpft an die jeweilige Eigenschaft im Strom- und Gasmarkt. Zu den registrierungspflichtigen Akteuren zählen gem. § 3 MaStRV insbesondere Betreiber von EEG- und KWK-Anlagen, Netzbetreiber, Stromlieferanten, Bilanzkreisverantwortliche, Transportkunden und Betreiber bestimmter Verbrauchseinrichtungen. Neben den Marktakteuren selbst, ist jede Stromerzeugungsanlage, die unmittelbar oder mittelbar an ein Stromnetz angeschlossen ist, zu registrieren sowie Verbrauchsanlagen, wenn diese an das Hoch- bzw. Höchstspannungsnetz (Strom) oder an das Fernleitungsnetz (Gas) angebunden sind. Sollten verpflichtete Marktakteure der Verpflichtung zur Registrierung im MaStRV nicht nachkommen, werden etwaige Vergütungsansprüche von geförderten EEG- und KWK-Anlagen gehemmt (§ 23 MaStRV). Sollten verpflichtete Marktakteure der Verpflichtung zur Registrierung im MaStR nicht, nicht richtig, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig nachkommen, besteht außerdem die Gefahr der Verhängung eines Bußgeldes in Höhe von bis zu 50.000 EUR (§ 21 MaStRV i. V. m. § 95 Abs. 1 Nr. 5 lit. d, Abs. 2 Satz 1 EnWG).

Für die regulatorische Beurteilung des Anwendungsfalls sind die Vorgaben zum Registrierungsverfahren von entscheidender Bedeutung. Das Verfahren lässt sich unterteilen in die Erfassung von Stammdaten, sowie in die nachgelagerte Datenvalidierung. Beide Schritte werden dabei in ihrer genauen Ausgestaltung dem BMWi gem. §§ 111f Nr. 7, 7a EnWG überlassen, sodass dem Verordnungsgeber bei seiner Ausgestaltung ein großer Entscheidungsspielraum zusteht.

Derzeit ist das Verfahren zur eigentlichen Registrierung / Datenerhebung in § 8 MaStRV abschließend geregelt. Hiernach besteht, wie unter Abschnitt 3.1.2.1 dargestellt, die Verpflichtung zur Nutzung des Webportals, wenn nicht ausnahmsweise von der Möglichkeit der schriftlichen Übersendung der Daten auf der Grundlage standardisierter Formulare der BNetzA Gebrauch gemacht wird (§ 8 Abs. 1 Satz 2 MaStRV). Wie genau das Webportal zu benutzen ist, wird in § 8 Abs. 1 Satz 1 MaStRV hingegen nicht geregelt. Das Verfahren entspricht aber aufgrund der aktuellen technischen Ausgestaltung des Webportals dem unter Abschnitt 3.1.2.1 dargestellten Anwendungsprozess (Kontoeröffnung, Datenerfassung, Validierung). Bei der Beurteilung des Anwendungsfalls stellt sich mithin die Frage, ob die automatische Registrierung unter Anwendung des SMGW sowie der Blockchain-Technologie als Ausgestaltung des Webportals zu bewerten ist oder ein neues, bisher in der MaStRV nicht geregeltes Registrierungsverfahren darstellt, welches eine Anpassung der MaStRV erfordern würde. Ggf. stellt auch der Erlass von Allgemeinverfügungen durch die BNetzA in diesem Zusammenhang eine gangbare Maßnahme dar (§ 20 MaStRV).

Darüber hinaus bestehen zusätzliche Meldepflichten für Anlagenbetreiber nach § 18 MaStRV, die bei der Ausgestaltung des Piloten ggf. zu berücksichtigen sind.

Für die Validierung der im Marktstammdatenregister eingetragenen Daten sieht die MaStRV verschiedene Handlungsoptionen der BNetzA vor. Demnach ist diese zunächst berechtigt, die Daten

selbstständig anhand bestehender behördlicher sowie frei zugänglicher Quellen zu überprüfen (§ 10 Abs. 1 MaStRV). Unabhängig hiervon kann die BNetzA auch den registrierten Marktakteur verpflichten seine Daten zu validieren (§ 10 Abs. 2 MaStRV) oder den jeweiligen Netzbetreiber, an dessen Netz die registrierte Erzeugungsanlage angeschlossen ist (§ 13 MaStRV). Die Verantwortlichkeit für die Richtigkeit der Daten verbleibt hingegen bei den Marktakteuren (§ 10 Abs. 2 Satz 5 MaStRV).

Neben dem Registrierungs- und Validierungsprozess verpflichtet die MaStRV die jeweiligen Netzbetreiber zu überprüfen, ob und welche Einheiten miteinander unter den Voraussetzungen des § 14 Abs. 1 Nr. 1 – 4 MaStRV verbunden sind und in eine technische Lokation zusammengefasst werden können. Jede Lokation erhält gem. § 14 Abs. 3 MaStRV von der BNetzA eine eindeutige Identifikationsnummer.

Über die regulatorischen Vorgaben für die Benutzung und Verwendung des Marktstammdatenregisters hinaus ist aufgrund der geplanten Einbindung des SMGW im Einzelfall zu überprüfen, ob die unter Abschnitt 3.1.2.3 dargestellte Prozessbeschreibung mit den Vorschriften des MsbG vereinbar ist. Dieses bestimmt:

- Zuständigkeit und Aufgaben des GWA (§§ 3 Abs. 1 Satz 2, 25 MsbG)
- Technische Anforderungen zur Funktionalität und Interoperabilität des SMGW (§§ 22, 23 MsbG i.V.m. den technischen Richtlinien des BWI)
- Vorgaben zur Datenkommunikation (§§ 49ff. MsbG)
- Datenschutzrechtliche Vorgaben (§§ 49ff, 60ff. MsbG)

Unter Punkt 9) der in der der Anlage exemplarisch beigefügten Prozessbeschreibung wurde dabei bereits festgestellt, dass das SMGW gem. § 22 MsbG i.V.m. den entsprechenden technischen Richtlinien des BSI in seiner Funktionalität auf bestimmte vorab festgelegt WAF's beschränkt ist. Für den Anwendungsfall gibt es weder in den Vorgaben zur SMGW Generation 1 noch zur Generation 2 einen passenden WAF. Aus regulatorischer Sicht ist es somit erforderlich, einen passenden WAF zu entwickeln und in den technischen Richtlinien umzusetzen. Neben den technischen Voraussetzungen stellt das MsbG Anforderungen an die Art und Weise der Datenkommunikation sowie an die dabei beteiligten Marktakteure. Hier wird zu überprüfen sein, ob sich der unter Abschnitt 3.1.2.3 beschriebene Prozess bereits heute unter Beachtung dieser Vorgaben umsetzen lässt oder ob die Regularien dem Verfahren Grenzen setzen. In diesem Bereich überschneiden sich die regulatorischen Vorgaben zum SMGW, mit den nachfolgend darzustellenden datenschutzrechtlichen Anforderungen.

Die nachfolgenden Ausführungen zum Datenschutzrecht stehen unter der Maßgabe, dass die regulatorischen Vorgaben (insbes. §§49ff, 60ff MsbG, und MaStRV) die Vorgaben der Datenschutzgrundverordnung (VO EU 2016/679) (DSGVO) in europarechtlich zulässiger Weise präzisieren und insoweit klarstellende Regelungen darstellen. Die Vereinbarkeit der Gesetze mit der DSGVO, als höherrangigem europäischen Recht, wurde nicht geprüft. Nach heutigem Stand sind keine absoluten Datenschutzhindernisse ersichtlich, die die Datenverarbeitung im Rahmen des gegenwärtig skizzierten Anwendungsfalls grundsätzlich unzulässig erscheinen lassen. Die DSGVO ist noch eine verhältnismäßig neue Verordnung ist und noch nicht vollständig ausjudiziert, daher sollten relevante Entwicklungen der europäischen Rechtsprechung intensiv verfolgt werden.

3.1.4.2.2 Datenschutzrechtlicher Rechtsrahmen

Bei dem MaStR handelt es sich um ein öffentliches Register. Die Regelungen der DSGVO (VO EU 2016/679) (DSGVO) und auch des Bundesdatenschutzgesetzes (BDSG) sind auch in diesem Zusammenhang beachtlich, denn es werden im MaStR personenbezogene Daten verarbeitet. Eine Verarbeitung liegt vor, wenn „*Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann*" (Art. 4 DSGVO).

Die DSGVO ist ihrerseits technologieneutral, vgl. EG 15 DSGVO: „*Der Schutz natürlicher Personen sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung von personenbezogenen Daten, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen.*"

Für diesen Anwendungsfall konkret bedeutet dies, dass die Akteure die datenschutzrechtlichen Voraussetzungen erfüllen müssen. So müssen alle Beteiligten im Prozess die DSGVO und BDSG-Vorschriften beachten, die auf ihre Rolle im Datenschutzrecht (Verantwortlicher, Auftragsverarbeiter, betroffene Person) anwendbar sind. Jeder Verantwortliche ist für die Einhaltung der Datenschutzprinzipien und ihren Nachweis verantwortlich, Art. 5 DSGVO.

Weiterhin muss für jede Datenübermittlung der Akteure untereinander eine Rechtsgrundlage bestehen. In diesem Zusammenhang sind auch die Vorschriften §§ 49 ff MsbG beachtlich.

Das Einholen von Einwilligungen in die Datenverarbeitung durch die betroffenen Personen ist hierbei nicht zu empfehlen. Zum einen kann eine Einwilligung jederzeit widerrufen werden und hat zum anderen höhere Hürden als gesetzliche Erlaubnistatbestände.

Im Einzelfall wird sich die Übermittlung wohl regelmäßig auf Art. 6 lit. c), e) oder f) DSGVO stützen lassen. Die zutreffende Rechtsgrundlage muss für jede denkbare Übermittlungskonstellation individuell festgestellt und fallbezogen geprüft werden. Hierzu müssen die tatsächlichen und rechtlichen Verhältnisse aller Akteure noch weiter geschärft werden. Aus den §§ 49 ff MsbG und 60 ff MsbG lassen sich u.a. zulässige Übertragungswege anerkannter Akteure ableiten.

Die Sicherheit der Verarbeitung ist ebenfalls durch jeden einzelnen Verantwortlichen sicherzustellen. Auch hierzu enthalten die regulatorischen Vorschriften Angaben, die die Anforderungen der Angemessenheit zur Sicherheit der Verarbeitung, Art. 32 DSGVO, präzisieren.

Die nachfolgende kursorische Betrachtung beleuchtet weitere wichtige Fragestellungen, die sich direkt aus einer Automatisierung eines öffentlichen Registers in Form einer Datenbank und der Verwendung der Blockchain-Technologie ergeben können.

Die datenschutzrechtlichen Grundsätze und die Betroffenenrechte müssen bei diesen Anwendungsfällen insbesondere betrachtet werden.

Insbesondere sollte die Einhaltung der folgenden Grundsätze beachtet werden, denn das DSGVO-Leitmotiv, dass der Betroffene jederzeit Kontrolle und Entscheidungshoheit über seine Daten hat, als Ausdruck der Gewährleistung der Datensouveränität, darf nicht gefährdet werden:

Transparenzgebot

Je komplexer der Datenverarbeitungs- und Übermittlungsvorgang ist, desto wichtiger ist eine transparente Information, damit die betroffenen Personen jederzeit ein klares Bild davon haben, wann welche personenbezogenen Daten von welcher Stelle und an wen übermittelt werden. Hierbei wird gefordert, die Information *‚präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden. (…) Dies gilt insbesondere für Situationen, wo die große Zahl der Beteiligten und die Komplexität der*

dazu benötigten Technik es der betroffenen Person schwer machen, zu erkennen und nachzuvollziehen, ob, von wem und zu welchem Zweck sie betreffende personenbezogene Daten erfasst werden, wie etwa bei der Werbung im Internet." EG 58 DSGVO.

Die hier beschrieben teilautomatisierte Übermittlung muss sich an diesen Kriterien messen lassen. Aus derzeitiger Sicht ist die Wahrung des Transparenzgrundsatzes aus datenschutzrechtlicher Sicht eine große Herausforderung. Auch das Transparenzgebot wird, insbesondere durch die §§60 ff MsbG, in Hinblick auf die zu übermittelnden Informationen präzisiert.

Datenminimierung

Es dürfen nur so viele Daten übermittelt werden, wie dies zur Zweckerfüllung erforderlich ist. Die Grenzen, die durch das MaStR und MsbG und den weiteren Fachgesetzen im jeweiligen Fall gesetzt werden, sollten insoweit auch zwischen den weiteren Beteiligten als Richtschnur für die Menge der verarbeiteten Daten angesehen werden. Auch hier enthalten die regulatorischen Fachgesetze Präzisierungen.

Es darf wohl festgehalten werden, dass die Präzisierungen der regulatorischen Fachgesetze auch die Einhaltung der Grundsätze fördern können.

Betroffenenrechte

Als Ausfluss der Datenschutzgrundsätze des Art. 5 DSGVO und Ausdruck der Datensouveränität dienen die Betroffenenrechte. Auch hierbei muss noch Detailprüfung erfolgen.

Die nachfolgenden Rechte sollten insbesondere beachtet werden:

Recht auf Vergessenwerden, Art. 17 DSGVO

§ 9 Abs. 2 MaStrRV ist direkter Ausfluss des Gebots der Datenrichtigkeit und Sparsamkeit (Art. 5 Abs. 1 lit d) DSGVO). Zugleich wird hiermit Art. 17 DSGVO konkretisiert. Die Regeln zu Datenlöschung muss auch von allen weiteren Akteuren entsprechend beachtet und umgesetzt werden. Weiterhin führen die datenschutzrechtlichen Vorschriften, die u.a. in § 9 MaStrRV und in § 50 MsbG wiedergegeben sind, zu der Empfehlung, personenbezogene Daten lediglich off-chain zu speichern und die Zuordnung durch Pseudonyme zu gewährleisten. Weiterhin müssen die Daten, abhängig von den erhobenen Zwecken, zum Teil mit unterschiedlichen Fristen gelöscht werden. So müssen bei Datenspeicherung zu Finanz- und Zahlungszwecken längere Fristen beachtet werden.

Aufgrund der Eigenschaft der Unveränderlichkeit der Blockchain (Integrität, vgl. 3.1.3.5), muss die Zuordnung der auf der Blockchain liegenden Pseudonymen mit den off-chain gespeicherten Daten aufgehoben werden. Die datenschutzkonforme Löschung der außerhalb der Blockchain gehaltenen Zuordnungstabelle muss in der Form geschehen, dass es unmöglich ist, die Zuordnung wiederherzustellen, insbesondere nicht unter Zuhilfenahme weiterer Informationen. Hierbei muss sehr sorgfältig auf die zu löschenden Daten und die daraus folgende notwendige Unmöglichkeit der Wiederzuordnung geachtet werden. Eine dokumentierte und unwiederbringliche physische Datenlöschung der off-chain liegenden Zuordnungstabelle, die die on-chain liegenden Pseudonyme mit den off-chain gespeicherten Daten verknüpft, erscheint geboten.

Recht auf Datenportabilität

Gemäß Art. 20 DSGVO hat eine betroffene Person das Recht, seine personenbezogenen Daten *„(…) in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln (…)*".

In diesem Zusammenhang ist § 52 Abs. 2 MsbG zu beachten, der postuliert, dass die „(…) *Datenkommunikation hat in dem von der Bundesnetzagentur vorgegebenen, bundesweit einheitlichen*

Format zu erfolgen" hat. Bei einer Übernahme für alle Akteure dieses Prinzips kann das Recht auf Datenportabilität hierdurch positive Impulse erfahren.

Automatisierte Einzelfallentscheidung, Art. 22 DSGVO

Bei dem Verfahren muss beachtet werden, dass keine automatisierte Einzelfallentscheidung im Sinne des Art. 22 DSGVO vorliegen, da an diese hohen Anforderungen gestellt werden. Gegenwärtig sind hierfür jedoch keine Anhaltspunkte ersichtlich.

Weitere relevante Aspekte

Datenschutzfolgenabschätzung, Art 35 DSGVO

Um sicherstellen zu können, dass die Verarbeitung personenbezogener Daten gemäß der DSGVO erfolgt, ist eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO in Erwägung zu ziehen. Eine Datenschutzfolgenabschätzung (DSFA) ist notwendig, wenn bei der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht. Diese Voraussetzungen sind in der noch zu erfolgenden datenschutzrechtlichen Beurteilung im Detail zu überprüfen. Von besonderer Relevanz könnte in diesem Zusammenhang die Einbindung des SMGW sowie der Blockchain-Technologie als neue Technologien sein. Gegenwärtig gehen wir davon aus, dass DSFA erforderlich sein werden, diese aber wegen der hohen Regelungsdichte ebenfalls teilweise auf Standards zurückgegriffen werden kann.

Gemeinsame Verantwortliche, Art 26 DSGVO

Die Rechtsprechung des EUGH zur Frage des Vorliegens gemeinsamer Verantwortlichkeit ist derzeit im Fluss. Abhängig von der konkreten vertraglichen und tatsächlichen Ausgestaltung der jeweiligen Rechtsverhältnisse müssen die Voraussetzungen der jüngsten Rechtsprechung im Detail geprüft werden.

Gegenwärtig wird nicht davon ausgegangen, dass Fälle gemeinsamer Verantwortung vorliegen werden.

Weiterhin erwarten wir, dass auch hier, aufgrund der hohen Regelungsdichte, Standards geschaffen werden können.

3.1.4.2.3 Vertragsrecht und sonstige zivilrechtliche Aspekte

Die angestrebte Plug & Play Lösung zur teilautomatisierten Registrierung von EEG-/KWK-Anlagen in einer öffentlichen Anlagendatenbank wirft am Rande schließlich die Frage auf, wer verantwortlich ist für eine fehlerhafte Datenübertragung oder für eingetretene Datenverluste, etwa aufgrund technischer Fehler oder aufgrund von Cyberangriffen. Nach der gegenwärtigen Regulatorik ist der Betreiber einer EEG-/KWK-Anlage grundsätzlich in Persona verpflichtet, diese unter den Voraussetzungen der MaStRV über das Webportal zu registrieren. Der Bundesnetzagentur bzw. den Netzbetreibern obliegt die Überprüfung der übermittelten Daten. Nicht geregelt ist demgegenüber die Verantwortlichkeit für die Datenübertragung bzw. für die gespeicherten Daten selbst. Denkbar wäre – als Auffangtatbestand – die Heranziehung allgemeiner zivilrechtlicher Grundsätze, um im Schadensfall zu einem interessengerechten Ausgleich zu gelangen. Unseres Erachtens bietet sich jedoch insbesondere an, die Verantwortlichkeiten für die Daten sowie die Haftung für etwaige Vermögenseinbußen wegen nicht ordnungsgemäßer Anmeldung der EEG/KWK-Anlage (Geldbuße, Vergütungsansprüche) aus Gründen der Rechtssicherheit vertraglich ausdrücklich zu regeln. Nahe liegt hier, die bestehenden bzw. gebräuchlichen Verträge, zum Beispiel mit dem Messstellen- oder Netzbetreiber, um entsprechende Klauseln zu ergänzen. Die Ausgestaltung der Klauseln ist abhängig vom Einzelfall. Eine tiefergehende Prüfung der Haftungsrisiken, die einer vertraglichen – oder

gesetzlichen – Regelung zugeführt werden sollten, wird gemeinsam mit einer Empfehlung im Abschlussbericht aufgenommen.

3.1.5 Wirtschaftliche Potenziale im Energiemarkt und gesamtwirtschaftliche Sicht

Bei der Betrachtung der generellen wirtschaftlichen Potenziale einer kombinierten SMGW/Blockchain-Lösung erscheint es sinnvoll, sich zunächst bewusst zu machen, dass die **Smart Meter Gateway Technologie** eine sichere und interoperable Grundlage für zahlreiche mögliche Anwendungsfälle im Zuge der Digitalisierung der Energiewirtschaft darstellt.

Abbildung 8: Mögliche Anwendungsfälle auf der Grundlage der SMGW-Technologie

Diese Übersicht stellt nur die Möglichkeiten aus heutiger Sicht dar. Insbesondere in den Bereichen Smart Mobility, Smart Home und Smart Services ist für die Zukunft mit der Entwicklung weiterer zahlreicher Geschäftsmodelle rund um Energielösungen zu rechnen.

Grundsätzlich erscheint auch das Anwendungspotenzial der **Blockchain-Technologie** in der Energiewirtschaft groß: Die dena hat in einer aktuellen Studie elf Anwendungsfälle in den Bereichen Asset- und Datenmanagement, Marktkommunikation, Energiehandel und Finanzierung von Investitionen beschrieben, darunter auch der in dieser Studie untersuchte Anwendungsfall der automatisierten Anmeldung von Anlagen im Marktstammdatenregister.[14]

Dabei ist zu berücksichtigen, dass die Blockchain zwar unveränderbare, sichere und transparente Informationsprotokolle für die Interaktion zwischen energiewirtschaftlichen Akteuren bietet, als Technologie aber nicht alternativlos ist. So kommen für viele Anwendungsfälle auch (erweiterte) Datenbanklösungen in Betracht. So ist diese Lösung nicht per se gesetzt, sondern kommt nur zum

14 Deutsche Energie-Agentur GmbH (dena): „Blockchain in der integrierten Energiewende", Berlin, 2019

Einsatz, wenn die Kosten-Nutzen-Abwägung im spezifischen Anwendungsfall und im Vergleich zu konkurrierenden Alternativlösungen zu Gunsten der Blockchain ausfällt.

Gesamtwirtschaftlicher Nutzen

Im hier betrachteten Anwendungsfall kommen in Bezug auf die reine Automatisierung eine Anlagendatenbank grundsätzlich auch andere Lösungen als die Blockchain in Betracht. Darüber hinaus aber bildet die Blockchain in Verbindung mit dem Vertrauensanker SMGW eine sichere, offene und flexible technische Plattform für zahlreiche (auch Blockchain-basierte) energiewirtschaftliche Anwendungsfälle der Gegenwart und Zukunft, z.B. auch den direkten Peer-to-Peer-Handel unter Letztverbrauchern, wie oben dargestellt.

Der gesamtwirtschaftliche Nutzen einer solchen energiewirtschaftlichen Anwendungsplattform lässt sich an Hand von drei wesentlichen Aspekten beschreiben:

- Zum einen macht die sichere Authentifizierung von Anlagen und die Blockchain direkte Transaktionen zwischen Marktpartnern (Letztverbrauchern) technisch möglich. Nach entsprechender Anpassung der rechtlichen/regulatorischen Grundlagen werden für diese Transaktionen potenziell **keine Intermediäre mehr** benötigt. Intermediäre werden durch den technischen Vertrauensanker ersetzt, die **Transaktionskosten sinken**, die Märkte für den Austausch von Energie und Energiedienstleistungen werden effizienter.
- Durch den vereinfachten, automatisierten Zugang über eine einheitliche Plattform wird sich potenziell die **Anzahl der Marktteilnehmer** auf Anbieter- wie auch auf Nachfragerseite für plattformgebundene Lösungsangebote **vergrößern** und damit das Wettbewerbselement in der Preisbildung auf den entsprechenden Märkten für Energiedienstleistungen weiter gestärkt.
- Zum dritten schafft die technologische Plattform eine **offene, interoperable** Grundlage für Anbieter und Verbraucher. Die Verbreitung und Nutzung der SMGW-Blockchain-Basis hat das Potenzial, proprietäre (anbieterspezifische) Technologien zu ersetzen, dadurch den Wettbewerb unter den Anbietern auf einer interoperablen Plattform zu befördern und damit die Rolle der Verbraucher als Nachfrager von Lösungsangeboten am Markt zu stärken.

Ein weiterer wichtiger gesamtwirtschaftlicher Nutzenaspekt betrifft die **Versorgungssicherheit bei stark skalierenden Geschäftsmodellen**, wie z.B. im Bereich der Elektromobilität, wenn gleichgerichtetes Handeln von Netzkunden (Prosumern) auf physikalische Engpasssituationen trifft - insbesondere im Verteilnetz.

Bereits heute ist erkennbar, dass unterschiedliche Anbieterstandards im Bereich Ladeinfrastuktur und Bezug von Ladestrom e-Mobility-Kunden zwingen, zahlreiche Smartphone-Apps verschiedener Anbieter und ggf. auch mehrere Ladekabel mit sich zu führen, um ein bundesweites Laden für ihr batterieelektrisches Fahrzeug zu ermöglichen.

Um weitergehende Probleme auch im netzdienlichen Lademanagement und beim Austausch von Flexibilitäten im Bereich Ladeinfrastruktur unter den Marktteilnehmern zu vermeiden, erscheint die Nutzung der oben beschriebenen standardisierten Plattform als eine vielversprechende Lösung - im Verein mit der Schaffung der technischen und regulatorischen Voraussetzungen.

Wirtschaftliche Vorteile auf Seiten der Akteure im Energiemarkt

Bei einer automatisierten Registrierung, Verwaltung und Bereitstellung von Anlagenstammdaten reduziert potenziell den Meldeaufwand (An-, Ab- und Ummeldungen) von dezentralen Anlagen im Netz erheblich. Für den **Anlagenbetreiber** reduziert das die Ingangsetzungs- und Transaktionskosten. Angesichts der hohen Zahl bereits vorhandener und potenziell zukünftiger Anlagen im Netz entsteht ein erhebliches Einsparpotenzial. Allein die Zahl von 1,7 Mio. installierten EEG-Anlagen (Deutschland,

2017)[15] illustriert das vorhandene Potenzial. Hinzu kommen steuerbare Verbraucher (§14a-Anlagen), deren Zahl durch den absehbaren massiven Ausbau der Ladeinfrastruktur in den nächsten Jahren noch deutlich zunehmen wird.

Auf Seiten der **Verteilnetzbetreiber** ergeben sich analog Einsparpotenziale, weil separate, eigene Anlagendatenbanken verzichtbar werden. Hinzu kommt, dass die Netzbetreiber mit einem zentralen, aktuellen und standardisierten Datenbestand zu Anlagen in ihrem Netz über eine bestmögliche Grundlage für Netzplanung und -betrieb verfügen. Gerade um den Ausbau der Stromnetze in einem volkswirtschaftlich vertretbaren Rahmen zu halten, ist die Schaffung der Voraussetzungen für eine höhere Auslastung der vorhandenen Netze unabdingbar. Dazu gehört ein netzdienliches Management von volatilen Einspeisern und flexiblen Lasten. Eine der Voraussetzungen ist eben die zuverlässige und vollständige Erfassung aller entsprechenden, an das Netz angeschlossenen Anlagen.

Die sichere Anlagenidentifikation und der automatisierte Nachweis von Anlagenleistungsdaten kann auch die Finanzierung entsprechender Assets durch **Investoren** erleichtern und beschleunigen, insbesondere wenn es sich um dislozierte Anlagenparks handelt, die z.B. als virtuelles Kraftwerk betrieben werden.

Für die **Technologieanbieter** erhöht sich die Planbarkeit und reduziert sich das Risiko für ihre Investitionen, wenn eine technologische Plattform als Standard definiert ist und in ihren Funktionalitäten entsprechend einer transparenten Roadmap weiterentwickelt wird. Weiterhin kann der hier untersuchte Anwendungsfall dazu beitragen, dass sich die **Marktverbreitung der SMGW Technologie** über die Pflichteinbaufälle hinaus erhöht und damit auch die Zahl der Geräte steigt. Dies wiederum erhöht die Motivation der Technologieanbieter, in den deutschen Messwesen-Markt zu investieren.

Auf Seiten der **koordinierenden und regulierenden Behörden** besteht durch ein automatisiertes oder teilautomatisierte, öffentliche Anlagendatenbank perspektivisch die Möglichkeit, ‚analoge' Aufgabenerfüllung zu reduzieren und Personalkapazität für höherwertige Tätigkeiten zu gewinnen.

15 Bundesnetzagentur, „EEG in Zahlen" 2017

3.2 Arbeitspaket 2: Konzept Pilotprojekt „Automatisierte Pflege einer öffentlichen Anlagendatenbank“

Nachdem der Anwendungsfall im Arbeitspaket 1 identifiziert wurde, erfolgte mit der Aufstellung eines Pilotkonzeptes für den konkreten Anwendungsfall die weitere Ausarbeitung im Arbeitspaket 2.

3.2.1 Vorgehen zur Definition des Pilotkonzepts

Die Hauptanforderung des Pilotkonzeptes besteht in der Fähigkeit zur unmittelbaren technischen Umsetzung des in AP1 beschriebenen Anwendungsfalls. Hierbei wird insbesondere Wert auf die vollständige Implementierung und Fähigkeit zur Pilotdurchführung gelegt. Die in der Umsetzung des Konzeptes aus AP2 vorzunehmende Pilotierung soll darüber hinaus auch als Grundlage für eine spätere marktliche Nutzung dienen können.

Der zeitliche Rahmen für die Umsetzung des Piloten wurde von der Auftraggeberin mit zwei Jahren angesetzt (2020 bis 2021) Wir gehen davon aus, dass das hier beschriebene Vorhaben mit einer Netto-Umsetzungszeit von ca. 18 Kalendermonaten realisierbar sein wird und haben diese Projektdauer für die Pilotkonzeption entsprechend zu Grunde gelegt.

Die inhaltliche Grundlage für die Ausarbeitung des Konzeptes bildet die Architekturskizze des AP1. Im technischen Fokus steht dabei die Verwendung eines SMGW (ohne jede technische Anpassung) mit einem Erweiterungsmodul auf der HAN/CLS-Schnittstelle und die Verwendung einer Konsortial-Blockchain. Ein direkter, öffentlicher Feldtest ist nicht erforderlich; der technische Aufbau und die Evaluierung können in einem Real-Labor erfolgen. Das „Plug & Play“ für den Anlagenbetreiber im Feld sollte dennoch eine Anforderung für die Umsetzung sein.

Die Erstellung der Konzeption erfolgte unter Einbeziehung von Experten der EY (Organisation, SMGW, Blockchain, Recht) sowie unter Mitwirkung von externen Akteuren nach einem Projektrollen- und Partnerkonzept: Marktpartner (Marktrolle MSB sowie Gatewayadministrator) und Technologiepartner für SMGW und Erweiterungen, Blockchain, Cloud IoT Services und Übertragungstechnik. Hierdurch wurde die Verankerung des Machbarkeits- und Umsetzbarkeitsgedankens im Pilotkonzept gestärkt und mögliche Risiken sowie Notwendigkeiten bei besonderen Rahmen- und Umsetzungsbedingungen erkannt und berücksichtigt.

Die beiden Kernergebnisse der Studie im AP2 sind insofern die Aufstellung einer Rahmenstruktur für die strukturierte Aufplanung des Pilotprojektes, sowie die Ableitung und Verprobung der konkreten Projektinhalte entlang der erarbeiteten Projektstruktur. Diese wurden in zwei Workshops mit den EY Experten und den externen Akteuren ausgearbeitet.

3.2.2 Projektstruktur für das Pilotkonzept

Als Grundlage für die Entwicklung der Projektstruktur des Pilotkonzepts wurde die standardmäßige Aufstellung eines Umsetzungsprojektes genutzt. Diese Struktur bietet den Vorteil, einzelne Elemente in Form von Aufgaben oder Aktivitäten ziel- und ergebnisorientiert anordnen zu können. Gleichzeitig können die Form der Umsetzung und der organisatorischen Abläufe für die Durchführung selbst offengehalten werden (z.B. agiles Vorgehen gegenüber Wasserfall-Modell).

Die Projektstruktur gliedert sich in die Phasen Planung, Implementierung, Nutzung und Evaluierung (plan, build, run, evaluate).

Die nachfolgende Abbildung zeigt die im Konzept vorgeschlagene Struktur und die erwartete Verteilung der Projektphasen auf der Zeitachse auf Basis der Workshop-Ergebnisse und der geplanten Projektdauer von 18 Monaten.

Phase	Monate	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
PMO	18																		
PLAN	7																		
BUILD	10																		
RUN	3																		
EVAL	5																		

Abbildung 9: Grobskizze und Phasenmodell des Piloten

3.2.3 Projektrollen- und Partnerkonzept

Basierend auf den im AP1 identifizierten Rollen der Akteure für die Umsetzung des Anwendungsfalls wurde für die Plausibilisierung des Konzepts mithilfe externer Partner eine Marktsichtung potentieller Projektpartner durchgeführt und eine Kandidatenliste für eine erste Ansprache mit der Auftraggeberin abgestimmt.

Neben den potentiellen Marktpartnern für die Umsetzung des Anwendungsfalls wurden ebenfalls potentielle Technologie- und Implementierungspartner für Geräte, Komponenten und Infrastruktur (Rollen Technologiepartner SMGW und HAN/CLS-Erweiterungen, Technologiepartner Blockchain, Technologiepartner Erweiterungen, Implementierungspartner Cloud- und IoT-Dienste, Implementierungspartner Übertragungstechnik und Marktpartner Energiewirtschaft) identifiziert.

3.2.4 Workshop-Konzept

Für die Plausibilisierung des Pilotkonzepts wurden zwei Workshops vorbereitet und mit den Marktpartnern durchgeführt.

3.2.4.1 Workshop 1: Projektinhalte

Die Aufgabe im ersten Workshop bestand in der Konzeption und Plausibilisierung der Inhalte der einzelnen Projektphasen.

Die Aufgabenstellung des Pilotprojektes „Automatisierte Pflege einer öffentlichen Anlagendatenbank“ muss dabei unter funktionalen und nicht-funktionalen Anforderungen aus den Perspektiven Prozesse und Technik, sowie organisatorischen Rahmenbedingungen und Regulatorik behandelt werden.

Hierfür wurde die allgemeine Projektstruktur mit den Phasen

- Planung
- Umsetzung
- Betrieb
- Evaluierung

weiter detailliert. Jede Phase wiederum beinhaltet Aktivitäten und Subaktivitäten. Für jede Subaktivität wurden im Zuge des Workshops konkrete Anforderungen definiert.

Auf Basis der technischen Architektur wurden konkrete Aktivitäten abgeleitet und mit den Projektpartnern verprobt.

Wesentliche Erkenntnisse zu Rahmenbedingungen daraus waren:

- Die technische Anpassung des SMGW selbst zur Implementierung der Stammdaten und Verknüpfung mit einer Blockchain ist nicht zielführend unter den gegebenen Rahmenbedingungen des Piloten (Problem der potentiellen Verfügbarkeit eines SMGW mit

diesen Funktionen im vorgegeben Zeitverlauf und kurzfristige Anwendbarkeit außerhalb/nach dem Piloten).

- Bei der Integration und Erweiterung von einzelnen Funktionen des SMGW ist aus o.a. Grund auch unbedingt darauf zu achten, dass das TOE des SMGW nicht angetastet bzw. verändert wird. Präferiert wird eine Umsetzung ohne jede technische Anpassung (Firmware) des SMGW. Idealerweise sollte die Implementierung über ein Zusatzmodul auf der HAN/CLS-Schnittstelle erfolgen.
- Bei der Kopplung eines Zusatzmoduls an ein SMGW muss zwingend ein Gatewayadministrator (GWA) mitwirken. Da im Rahmen des Prozess- und Technologie-Designs neue Anforderungen an den GWA gestellt werden, müssen Erweiterungen oder Anpassungen an das IT-System des GWA aufgestellt und im Rahmen des Piloten umgesetzt werden können. Daher ist die Mitwirkung eines (zertifizierten) GWA mit den Fähigkeiten zur flexiblen und erweiterbaren Gestaltung und Umsetzung von GWA-Prozessen und -Systemen im Piloten als wichtige Voraussetzung anzusehen.

Die Details der einzelnen Aktivitäten und Anforderungen an die Umsetzung des Piloten sind in *Anhang B: AP2 – Detaillierte Projektskizze* dargestellt.

3.2.4.2 Workshop 2: Verprobung der Umsetzbarkeit und Einhaltung der Projektziele

Die Aufgabe im zweiten Workshop bestand in der Plausibilisierung der Umsetzbarkeit, der im ersten Workshop identifizierten Projektinhalte.

Hierbei wurden insbesondere Abhängigkeiten und Rahmenbedingungen für den zeitlichen Verlauf des Pilotprojektes und zur Machbarkeit/Einhaltung der Projektziele erarbeitet und mit den Workshop-Teilnehmern verprobt.

Wesentliche Erkenntnisse zu Rahmenbedingungen daraus sind:

- Die Umsetzung des Pilotprojektes erfordert keinen vollumfänglichen Feldversuch, da eine öffentliche Anlagendatenbank nicht über zahlreiche, echte Instanzen verfügen muss, um eine variantenreiche Evaluierung der Eignung durchzuführen. Daher kann ein Pilot in einem Real-Labor umgesetzt werden, wobei gilt:
  - Die Nutzbarkeit für den Anwender (Plug & Play für den Anlagenbetreiber) im Feld sollte dennoch ein konkreter Teil der Anforderung, Implementierung und Evaluierung sein.
  - Anforderungen an Skalierbarkeit und Performance in einem ausreichend gehärteten Pilot-System müssen auch im Labor durch geeignete Maßnahmen implementiert und evaluiert werden
- Bei der Umsetzung werden zahlreiche, komplexe Abhängigkeiten bei Prozessen, Technik und Recht- bzw. Regulatorik-Aspekten über eine Vielzahl von betroffenen Akteuren und Komponenten zutage treten.
  Die Bildung einer entsprechenden Governance Struktur für die jeweiligen Themenbereiche und die übergreifende Koordination im Projekt ist zu berücksichtigen.

3.2.5 Erfolgsfaktoren

Das Ziel des Pilotprojektes ist die Umsetzbarkeit der skizzierten Blockchain-Lösung zu beweisen. Doch wann wird dieses Ziel als erreicht erachtet? Es wurden hierzu definierte Erfolgsfaktoren erarbeitet, die das Ziel des Projektes konkreter beschreiben und als (Abnahme-)Kriterien gelten können, wann das Pilotprojekt als erfolgreich angesehen werden kann.

- **Technischer ‚Durchstich' erfolgreich im Labor betreibbar und reproduzierbar:**
  Mit ‚technischer Durchstich' ist gemeint, dass einige Transaktionen tatsächlich von Anfang bis Ende durchgeführt werden. Von der (Erst-)Installation einer Anlage über die Registrierung bis zum Zugriff auf diese Daten durch einen berechtigten Dritten. Es ist nicht ausreichend Teilaspekte getrennt zu testen.
  Mit ‚im Labor betreibbar' ist gemeint, dass es ausreichend ist, die Systeminfrastruktur (Anlage, Smartmeter Gateway, Blockchain etc.) in einem abgeschirmten Bereich, unabhängig von tatsächlich im Feld befindlichen Smartmetergateways zu testen.
- **Ein Konzept zum Datenmanagement ist erarbeitet und ein echter Anlagenbetreiber erzeugt seinen vollständigen Datensatz:**
  Die erfassten Daten in der Datenbank sind entsprechend rechtlicher und technologisch sinnvoller Aspekte auf die Blockchain und traditionelle Datenspeicher produktionsreif aufgeteilt („on-/off-chain") und wurden über einen tatsächlichen Anlagenbetreiber erzeugt.
- **Der Netzbetreiber des Anlagenbetreibers ist enthalten**:
  Der für den Anlagenbetreiber verantwortliche Netzbetreiber ist ebenfalls Teil der Transaktion, um das Szenario realistisch abzubilden.
- **Andere Knotenbetreiber können die Existenz der Anlage und relevanten Anlagendaten gesichert feststellen (über Blockchain und PKI):**
  Ein berechtigter Dritter kann über die neu geschaffene Sicherheitsinfrastruktur ebenfalls auf die erzeugten Daten zugreifen, um den gesicherten Austausch systemkritischer Daten zu beweisen.
- **Die wirtschaftliche Evaluierung ist abgeschlossen**:
  Es wurden Kosten & Nutzen für die unterschiedlichen Teilnehmer (Anwender, Netzbetreiber, Behörden, etc.) analysiert und eine gesamtwirtschaftliche Betrachtung aus Sicht der Energiewirtschaft erarbeitet.
- **Etwaige notwendige Anpassungen an Rechtsrahmen und Regulatorik sowie der relevante Rechtsrahmen sind identifiziert:**
  Die Grundannahme des Piloten ist, dass die regulatorische Basis derzeit vorhanden ist. Dies wird jedoch detailliert überprüft und etwaige notwendige Anpassungen des Rechtsrahmen identifiziert.
- **Ein „generischer Kern" des BC-SMGW Systems ist vorhanden und eine Anwendung über den Piloten hinaus ist möglich:**
  Der Pilot soll nicht nur eine Einmalentwicklung für exakt diesen Use Case darstellen, sondern soll als Basis für spätere – auf den Stammdaten aufbauende – Use Cases dienen können, wie z.B. Peer-2-Peer Stromhandel etc.
  Potentielle Kandidaten für diesen „Kern" können sein:
  - generisches, standardisiertes Verfahren für die Kopplung von SMGW und Zusatzmodulen verschiedener Hersteller und der Blockchain
  - generisches Verfahren für das Datenmanagement (z.B. potentiell auch Messwerte), inkl. on-/off-chain Strategie in der Blockchain und das zugehörige Identitäts- und Zugangsmanagement für diese Daten.
- **Die Systemintegrität zwischen BC und SMGW ist gewährleistet (Sicherheit des Gesamtsystems):**
  Das Smart-Meter-Gateway bietet eine ausgeklügelte Sicherheitsarchitektur auf Basis von Zertifikaten. Die Blockchain bietet ein sicheres Konzept auf Basis von Identitäten und privaten und öffentlichen Schlüssel. Während die Annahme besteht, dass beide Systeme als sehr sicher einzustufen sind, muss gewährleistet sein, dass diese beiden Welten auch in Kombination dieselbe Sicherheit bieten.

- **Es wurde ein nutzerzentrierter Ansatz verwendet, um die Usability für den Endverbraucher sicherzustellen**:
  Anlagenbetreiber sind Privatpersonen oder Firmenkunden, die sehr leicht in das neue System einbettet werden müssen. Benutzerfreundlichkeit und niedrigste Einstiegshürden nach dem „Plug-And-Play" Prinzip sind ein wesentliches Kriterium, damit so ein System akzeptiert wird am Markt.
- **Ein Betriebskonzept ist erarbeitet:**
  Das System soll nicht nur lauffähig sein, sondern es muss ein Konzept erstellt sein, welches betriebliche Aspekte, Verantwortlichkeiten, Supportstrukturen, Weiterentwicklungen, Verfügbarkeiten, etc. vorschlägt, so dass ein solches System auch in einen professionellen Produktionsbetrieb übergehen werden kann.

3.2.6 Ergebnisse des Pilotkonzepts

Das erarbeitete Pilotkonzept wird im weiteren Verlauf dargestellt.

Die tabellarische Struktur findet sich in *Anhang B: AP2 – Detaillierte Projektskizze*

Nachfolgende Darstellung zeigt den vorgeschlagenen Projektverlauf über 18 Monate, über die Projektphasen und den darin enthaltenen Arbeitspaketen:

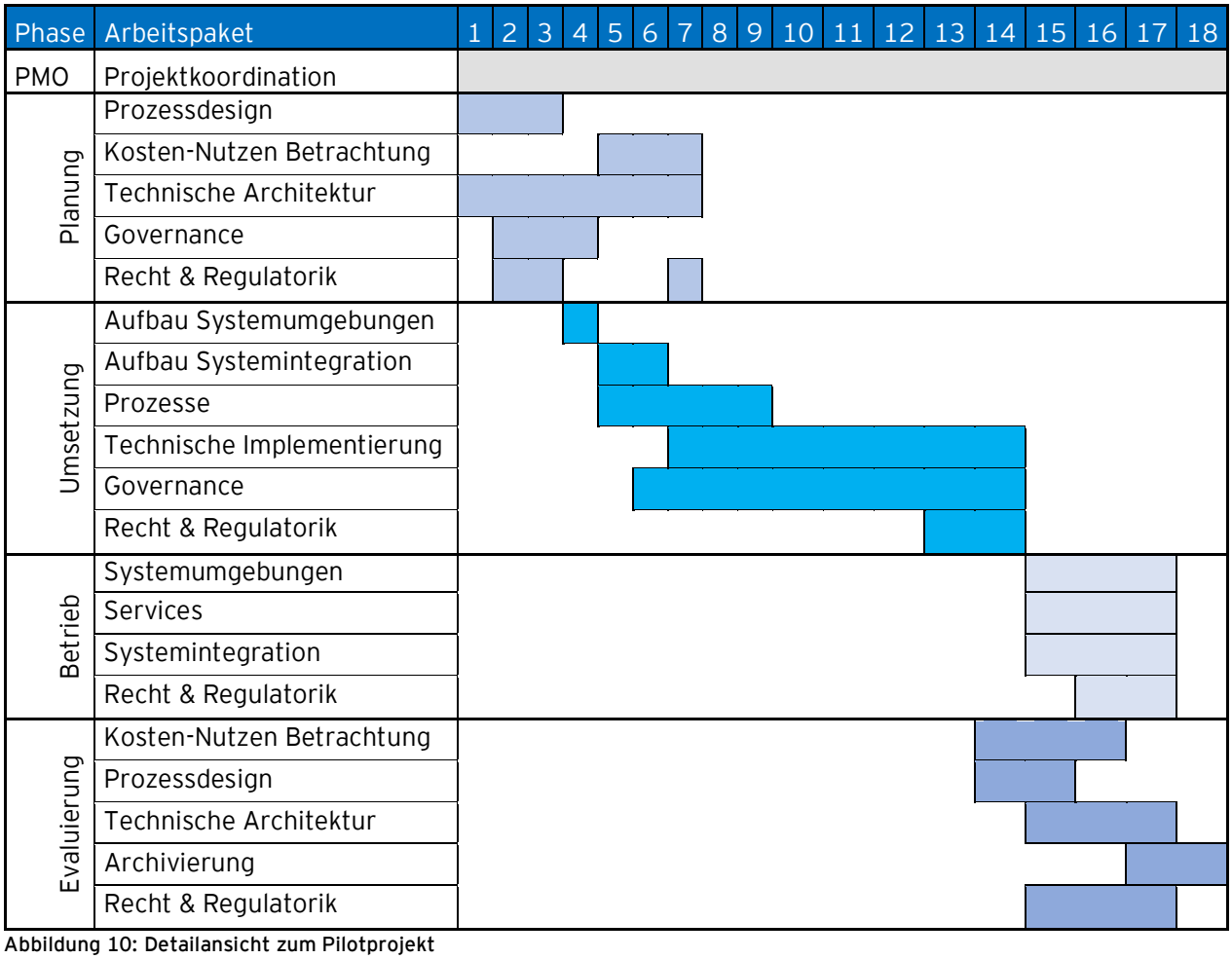


Abbildung 10: Detailansicht zum Pilotprojekt

3.2.6.1 Projektkoordination

Im Rahmen der Projektkoordination sind geeignete Formen des Projektmanagements zu planen und zu etablieren. Für die Umsetzung des Projektes ist die zur Verfügungstellung von Projektinfrastruktur und die Berechnung von KPIs zur Überwachung des Projektfortschritts maßgeblich. Im Zuge des Projektmarketings ist Darstellung der Projektergebnisse in der Öffentlichkeit zu gewährleisten. Die Resonanz ist anschließend zu evaluieren und die Ergebnisse zu dokumentieren.

3.2.6.2 Planung

Prozessdesign

Als Grundlage der Implementierung des Piloten sind die notwendigen Geschäftsprozesse zur Erfassung und Verwaltung von Stammdaten zu erarbeiten. Dabei ist ein Akteursmodell sowie die institutionelle Aufstellung des Systems zu etablieren. Weiters soll ein Usability Konzept sowie ein fachliches Datenmodell aufgestellt werden. Zuletzt soll ein System zur Einholung von Feedbacks konzipiert werden.

Kosten-Nutzen Betrachtung

Im Zuge des Pilotprojektes soll die kommerzielle Machbarkeit evaluiert werden. Hierzu ist ein Business Case zu erarbeiten, wobei der gesamtwirtschaftliche Nutzen zu berücksichtigen ist. Außerdem sind Make-or-Buy Entscheidungen zu treffen.

Technische Architektur

Die technische Konzeptionierung bildet die Grundlage für alle weiteren Arbeitsschritte. Es sollen die technische Umsetzung des Plug-&Play/Usabilitykonzepts erarbeitet werden, sowie Datenmanagementkonzept, Identitätskonzept, Sicherheitskonzept, Skalierbarkeitskonzept, Testkonzept und ein Kommunikationsinfrastrukturkonzept. Weiters ist ein Domain Model als UML Diagramm aufzustellen und Risiken frühzeitig im Rahmen eines Change-Management Konzepts zu vermeiden. Außerdem soll die vorläufige Technologieauswahl der Geräte sowie der Technologien für Backend Systeme, Frontend und des Blockchain Protokolls getroffen werden. Zuletzt sollte ein klarer Kommunikationsprozess etabliert werden, um eine mit dem BSI abgestimmte Lösung zu erreichen.

Governance

Es sollen Gremien nach Entscheidungsbereichen mit den relevanten Projektpartnern etabliert werden, die Abstimmungen und Entscheidungen zwischen den Projektteilnehmern herbeizuführen und nachhaltige Strukturen für die Entscheidungsfindung innerhalb des Projektes schaffen.

Recht & Regulatorik

Zunächst müssen die Marktakteure, insbesondere diejenigen, die direkt am Blockchain-Netzwerk teilnehmen, identifiziert werden. Parallel dazu erfolgt die Bestimmung der rechtlich relevanten Prozesse und Klärung von Grundsatzfragen, namentlich ob das geltende Recht, aufgrund der geplanten technischen Umsetzung oder zur Vereinbarkeit mit europäischem Recht, angepasst werden muss. Darauf aufbauend kann das Compliance Konzept geplant werden. Nach Herausarbeitung der rechtlichen Stellung und der damit einhergehenden Pflichten und Rechte der Marktakteure, unter anderem aus MsbG, MaStRV und DSGVO, ist zu prüfen in welcher Art und Weise eine Einhaltung bestmöglich erzielt werden kann. Gleichzeitig müssen die Haftungsrisiken bewertet und Schritte zur Bewältigung etwaiger neuer Risiken vorgenommen werden, zum Beispiel hinsichtlich einer fehlerhaften Datenübertragung bzw. bei vorsätzlichen Datenmanipulationen oder auch Datendiebstahl. Hier kommt – abhängig von den konkreten Umständen des Einzelfalles – neben der Verantwortlichkeit des Anlagenbetreibers auch eine Verantwortlichkeit des Messstellenbetreibers oder des Herstellers des Smart-Meter-Gateways in Betracht.

3.2.6.3 Umsetzung

Aufbau Systemumgebungen

Bevor die Einzelkomponenten implementiert werden können, ist der Aufbau entsprechender Systemumgebungen notwendig. Dazu zählen neben dem Cloud Hosting auch die physischen Räumlichkeiten für die Installation der Geräte sowie die Einrichtung einer Entwicklungs- sowie Laufzeitumgebung für das Blockchain Netzwerks.

Aufbau Systemintegration

Die zuvor etablierten Systemumgebungen der Einzelkomponenten müssen miteinander verbunden werden, damit diese ordnungsgemäß kommunizieren können.

Prozesse

Die im vorhergehenden Projektabschnitt definierten Rollen und Rechte, sowie die Geschäftsprozesse zur automatischen Erfassung und Verwaltung von Stammdaten sind entsprechend zu implementieren. Außerdem sind Usability Konzepte umzusetzen und das zuvor definierte Feedbacksystem umzusetzen.

Technische Implementierung

Die zuvor in der Planungsphase definierten Komponenten und Konzepte (Plug & Play, Domain Model, Testkonzept, Identitätskonzept, Datenmodell) müssen entsprechend umgesetzt werden. Dazu zählt die Inbetriebnahme des SMGW und des CLS Geräts, der Aufbau von Blockchain Knoten, sowie des Frontends. Weiters muss die Kommunikationsinfrastruktur aufgebaut werden und Schnittstellen implementiert werden. Außerdem ist die Dokumentation zu erstellen und laufend zu erweitern.

Governance

Die definierten Autoritäten und Gremien zur Abstimmung und Entscheidungsfindung sollen etabliert werden. Abstimmung und übergreifende Festlegungen für kritische Themen der Architektur und der Anwendung sind herbeizuführen.

Recht und Regulatorik

In der Build-Phase werden u.a. Vertrags- und Informations-Templates zur Regelung der Rechte und Pflichten der Akteure entworfen und Maßnahmenpakete und Handlungsabläufe zur Sicherstellung eines funktionierenden Compliance Konzeptes, unter Zuhilfenahme geeigneter Tools, umgesetzt.

Sofern eine Anpassung der gesetzlichen Rahmenbedingungen identifiziert worden ist, werden mögliche Handlungsoptionen geprüft und ggf. Gesetzesänderungen formuliert.

Es ist ein Reporting-Prozess zu implementieren, um die juristische Bewertung zu sichern und, darauf aufbauend, in einem Prozess der kontinuierlichen Verbesserung, die Erkenntnisse in dem Projekt einfließen lassen zu können.

3.2.6.4 Betrieb

Systemumgebungen

Der reibungslose Betrieb der Einzelkomponenten und deren Systemumgebungen muss während des Betriebs sichergestellt werden.

Systemintegration

Die Verbindungen der Systemkomponenten müssen während des Betriebs überwacht und aufrechterhalten werden.

Services

First- und Second-Level Support soll bereitgestellt werden und via Ticketing technische Unterstützung und Störungsbehebung anbieten.

Recht & Regulatorik

Durch effektive Kommunikationsmittel werden die im Laufe der praktischen Umsetzung des Projekts aufkommenden ad-hoc Rechtsfragen in angemessener Form, z.B. schriftlichen Stellungnahmen, beantwortet.

3.2.6.5 Evaluierung

Prozessdesign

Die Prozesse sind nach dem Testbetrieb im Hinblick auf die Umsetzung und die Zielerreichung des Planungsstadiums sowie die Erfolgsfaktoren des Projektes zu bewerten und zu dokumentieren. Weiter soll von den Projekt-Stakeholdern Feedback eingeholt werden.

Kosten-Nutzen Betrachtung

Nach der Betriebsphase ist die kommerzielle Machbarkeit zu evaluieren und ein Business Case auf Basis der Planung zu erstellen. Zusätzlich sollen durch eine unabhängige Partei eine volkswirtschaftliche Betrachtung der entwickelten Technologien und Prozesse sowie identifizierter Potenziale durchgeführt werden.

Technische Architektur

Die gesamte technische Architektur soll einer umfassenden technischen Überprüfung unterzogen werden und Abweichungen festgehalten werden. Externe Parteien sollen technische Unterstützung bei der Evaluierung des Piloten erhalten. Weiters soll das Sicherheitskonzept überprüft werden, die Kommunikation und das Validierungstool getestet sowie die Skalierbarkeit zu prüfen. Zuletzt ist eine finale Entscheidung bezüglich der Empfehlung des am besten geeigneten Blockchain Protokolls abzugeben.

Recht & Regulatorik

Die Funktionalität und Vollständigkeit des Konzeptes werden rechtlich geprüft und in Form eines juristischen Abschlussberichts dokumentiert.

Archivierung

In der Abschlussdokumentation sollen sämtliche erarbeiteten Ergebnisse gesamtheitlich dokumentiert und dem Auftraggeber zur Verfügung gestellt werden. Weiters sind die Artefakte zu konservieren und Lessons learned festzuhalten. Sämtliche personenbezogene Daten, z.B. der Projektteilnehmer in den Testsystemen sind DSGVO-konform zu löschen.

4. Zusammenfassung und Ausblick

Der bereits in vollem Gang befindliche Wandel des Deutschen Energiesystems mit dem Ausbau dezentraler und erneuerbarer Erzeugung, Speicherung und mit einer Vielzahl an flexiblen Verbrauchern kann erfolgreich und effizient nur mit dem Einsatz digitaler Technologien gestaltet werden.

Eine wichtige Voraussetzung für die Realisierung der neuen Energiewelt ist dabei die Verknüpfung und Steuerung der dezentralen Energieanlagen zum marktlichen Ausgleich von Erzeugung und Verbrauch und auch zur optimalen Ausnutzung verfügbarer Netzkapazitäten.

Die bisherige Praxis zeigt, dass hierzu neben den zahlreichen innovativen und proprietären Lösungen auch bundesweite Standards gebraucht werden, um die Sicherheit der kritischen Infrastruktur und das Vertrauen der Marktakteure in die Zuverlässigkeit des Gesamtsystems und die Verlässlichkeit der ausgetauschten Informationen zu sichern.

Mit dem Inkrafttreten des Gesetzes zur Digitalisierung der Energiewende (GDEW) 2016 wurde eine wichtige Grundlage zur Nutzung der Potenziale digitaler Technologien in der Energiewirtschaft geschaffen: Das Gesetz gibt u.a. den Einsatz zertifizierter Messtechnik vor - intelligente Messsysteme mit Smart Meter Gateways (SMGW) als gesicherter Vertrauensanker für die Identität der gespeicherten und übertragenen Messdaten. Das SMGW ist zudem ausgelegt als technische Plattform für die Realisierung zukünftiger Anwendungsfälle und Geschäftsmodelle.

Seit einiger Zeit kommt im Energiemarkt auch die Blockchain als potenzielle Basistechnologie der Digitalisierung zum Einsatz: In Pilotprojekten wird die Verknüpfung von Marktteilnehmern über die Blockchain realisiert, u.a. um einen Peer-to-Peer-Handel von Letztverbrauchern zu erproben. Auch wenn die aktuellen rechtlichen und regulatorischen Rahmenbedingungen einem direkten Handel und Austausch von Energie unter Letztverbrauchern noch entgegenstehen, so sind es diese und andere dezentrale Anwendungsfälle, die das Energiesystem der Zukunft prägen werden.

Letztlich sind aber alle hier zukünftig entstehenden Geschäftsmodelle darauf angewiesen, dass ein sicherer, zeitgerechter und kosteneffizienter Austausch von Daten und Informationen zwischen digitalen Komponenten und auch zwischen den Transaktionspartnern erfolgen kann.

Mit der Verknüpfung von Blockchain und SMGW Technologie zum Zweck der automatisierten Pflege einer öffentlichen Anlagendatenbank könnte eine sichere, skalierbare und interoperable Grundlage für zukünftige dezentrale Geschäftsmodelle geschaffen werden.

Im Mittelpunkt dieses Projekts steht daher die Frage, unter welchen technischen, rechtlich/regulatorischen und kaufmännischen Voraussetzungen eine Konstellation aus Smart Meter Gateway-Plattform in Kombination mit dem Einsatz von Blockchain-Technologie geeignet ist, diese Erwartungen zu erfüllen. Dazu wurde zunächst eine Machbarkeitsstudie erstellt (Arbeitspaket 1), deren Ergebnisse im Abschnitt 3.1 dargestellt sind. Darauf aufbauend wurde ein Konzept für ein Pilotprojekt zur „Automatisierten Pflege einer öffentlichen Anlagendatenbank“ erarbeitet (Arbeitspaket 2), das in Abschnitt 3.2 dieses Berichts ausgeführt wird.

Im Rahmen der Machbarkeitsstudie wurden zusammenfassend die folgenden Ergebnisse erarbeitet:

Technische Sicht

Als Ergebnis in Bezug auf die technische Analyse kann festgehalten werden, dass das SMGW als ausführende Instanz für eine automatisierte Registrierung von Akteuren, sowie eine automatische Übertragung von Anlagendatensätzen an eine öffentliche Datenbank grundsätzlich geeignet ist, einschließlich der vollständigen und eindeutigen Herstellung der Identität mittels PKI. Die hierfür bestehenden Voraussetzungen sind abhängig von der gewählten technischen Implementierung und in diesem Bericht skizziert und näher beschrieben.

Dabei geht es nicht nur um die Anforderungen an die technische Architektur, sondern auch um das Konzept zum Identitäts- und Zugriffsmanagement, das geprägt ist von den Anforderungen der beteiligten Marktakteure.

Ergänzt wird die technische Architektur durch den Einsatz einer verteilten Blockchain-Datenbank. Dieser Bericht enthält erste Empfehlungen zu den Designkriterien. So erscheint die Beschränkung auf eine private bzw. Konsortial-Blockchain sinnvoll. Eine wichtige konzeptionelle und auch datenschutzrechtlich relevante Frage ist dabei, wie der Umgang mit personenbezogenen Daten, deren Speicherung ‚off-chain' erfolgen kann, mit einem klaren und gesetzeskonformen Identitäts- und Berechtigungsmanagement. Letztlich ist die Entwicklung eines universell anwendbaren Datenmodells erforderlich, das den Anforderungen der Regulierungsbehörden und Marktteilnehmer gerecht wird.

Der Einsatz der Blockchain für die öffentlichen Anlagendatenbank vermeidet eine asynchrone, redundante und damit fehleranfällige Datenhaltung. Gleichzeitig wird die Ausfallsicherheit des Gesamtsystems erhöht und die Aktualität und Richtigkeit der ausgetauschten Daten sichergestellt. Letztlich bietet die Blockchain-Lösung als höherwertige digitale Infrastruktur auch eine skalierbare, interoperable und sichere Grundlage für zukünftige Anwendungsfälle zwischen dezentralen Marktakteuren, wie z.B. dem Peer-to-Peer-Handel.

Die Architektur der Anlagendatenbank muss weiterhin die Voraussetzungen bieten, die Übernahme der Daten vom SMGW oder einem autorisierten Endgerät zu ermöglichen. Grundsätzlich sind die hierfür benötigten technischen Komponenten bereits marktgängig mit der Einführung der SMGW-Technologie verfügbar.

Regulatorische und rechtliche Sicht

Aus regulatorischer Sicht ist für den Anwendungsfall der automatisierten Pflege einer öffentlichen Anlagendatenbank insbesondere Folgendes zu beachten:

- Die Möglichkeit der Einbindung von Blockchain und SMGW bei der Registrierung in der Datenbank unter den aktuellen regulatorischen Rahmenbedingungen des EnWG und der MaStRV. Hier besteht Gestaltungsspielraum für den Verordnungsgeber.
- Die Übereinstimmung der Prozesse zur Registrierung und Übertragung der Daten mit den Vorschriften zur Datenkommunikation sowie dem Aufgabenkreis des GWA. Hier zeigt sich u.a., dass es notwendig sein wird, dass die Ausweitung der Funktionalität des SMGWs auf den hier darzustellenden Anwendungsfall die Entwicklung eines passenden WAFs und dessen Umsetzung in den technischen Richtlinien erfordert.

Weiterhin stellen sich bei einer automatisierten Anmeldung in der Anlagendatenbank vor allem auch datenschutzrechtliche Fragen. Hierbei geht es im Einzelnen darum,

- ob für die Einbindung von Marktteilnehmern mit den Marktrollen Messstellenbetreiber, (Gateway-Administrator) und Netzbetreiber entsprechende datenschutzrechtliche Erlaubnistatbestände bestehen,
- ob der Prozess zur Registrierung und Übertragung der Daten den Anforderungen der Datenschutzgrundsätze, insbesondere dem Transparenzgebot, entspricht und
- ob die Betroffenenrechte hinreichend gewahrt werden.
- Aufgrund der Eigenschaft der Unveränderlichkeit der Blockchain ist bei der Implementierung auf die korrekte Umsetzung des Prozesses für eine datenschutzkonforme Löschung von Daten zu achten.

Unter Einhaltung der Grundsätze des Transparenzgebots, der Datenminimierung, der Betroffenheitsrechte und des Rechts auf Datenportabilität erscheint eine rechtskonforme Gestaltung der datenschutzrechtlichen Anforderungen insgesamt jedoch als lösbare Aufgabe.

Wirtschaftlichkeit

Im hier betrachteten Anwendungsfall kommen in Bezug auf die reine Automatisierung einer Anlagendatenbank grundsätzlich auch andere Lösungen als die Blockchain in Betracht. Darüber hinaus aber bildet die Blockchain in Verbindung mit dem Vertrauensanker SMGW eine sichere, offene und flexible technische Plattform für zahlreiche (auch Blockchain-basierte) energiewirtschaftliche Anwendungsfälle der Gegenwart und Zukunft, z.B. auch den direkten Peer-to-Peer-Handel unter Letztverbrauchern:

- Direkte Transaktionen zwischen Marktpartnern (Letztverbrauchern) durch sichere Authentifizierung – Intermediäre werden entbehrlich, Transaktionskosten sinken
- Mehr Marktteilnehmer und mehr Wettbewerb durch vereinfachten Zugang zu plattformgebundenen Lösungsangeboten
- Offene, interoperable Plattform ersetzt proprietäre Technologien, dadurch mehr Anbieter-Wettbewerb und gestärkte Autonomie der Verbraucher

Ein weiterer gesamtwirtschaftlicher Nutzenaspekt betrifft die erhöhte Versorgungssicherheit bei stark skalierenden Geschäftsmodellen (z.B. der Ladesäuleninfrastruktur) durch eine sichere, skalierbare und interoperable Stammdatenplattform.

Auf Seiten der Akteure im Energiemarkt profitieren die Anlagenbetreiber durch reduzierte Ingangsetzungs- und Transaktionskosten. Für die Netzbetreiber werden eigene Anlagendaten verzichtbar. Investoren wird die Finanzierung von Energieanlagen durch die Verfügbarkeit gesicherter Daten erleichtert. Ein offener, interoperabler Standard befördert auch die Bereitschaft zu Entwicklungsinvestitionen auf Seiten der Technologieanbieter und fördert potenziell die Marktverbreitung der SMGWs. Koordinierende und regulierende Behörden können schließlich den Aufwand durch ‚analoge' Aufgaben reduzieren.

Konzeption des Pilotprojekts

Die Konzeption des Pilotprojekts erfolgte für den konkreten Anwendungsfall „Automatisierte Pflege einer öffentlichen Anlagendatenbank". Die Erstellung der Konzeption erfolgte unter Einbeziehung von Experten der EY (SMGW, Blockchain, Recht) sowie unter Mitwirkung von externen Akteuren nach einem Projektrollen- und Partnerkonzept: Marktpartner (Marktrolle MSB sowie

Gatewayadministrator) und Technologiepartner für SMGW und Erweiterungen, Blockchain, Cloud IoT Services und Übertragungstechnik.

Die Hauptanforderung des Piloten soll darin bestehen, eine vollständige technische Implementierung mit der Fähigkeit zur Pilotdurchführung zu schaffen, auch als Vorbereitung für eine spätere marktliche Nutzung.

Grundlage für den Piloten ist die Architekturskizze aus Arbeitspaket 1. Im technischen Fokus steht dabei die Verwendung eines SMGW (ohne jede technische Anpassung) mit einem Erweiterungsmodul auf der HAN/CLS-Schnittstelle und die Verwendung einer Konsortial-Blockchain. Ein direkter, öffentlicher Feldtest ist nicht erforderlich; der technische Aufbau und die Evaluierung können in einem Real-Labor erfolgen. Das „Plug & Play" für den Anlagenbetreiber im Feld sollte dennoch eine Anforderung für die Umsetzung sein.

Mit Blick auf diese Umsetzung sind zahlreiche und zum Teil komplexe Abhängigkeiten bei Prozessen, Technik- und Rechts- bzw. regulatorischen Fragen zu erwarten, und das über eine Vielzahl von betroffenen Akteuren und Komponenten. Dies erfordert eine gut definierte Projekt-Governance und Verantwortlichkeit für die Umsetzungsfelder und eine integrierende Projektkoordination.

Für den Ablauf des Pilotprojekts wurde eine Aufstellung in Projektphasen nach dem Standard eines Umsetzungsprojektes genutzt (Planung, Umsetzung, Betrieb und Evaluierung). Zur Beschreibung der einzelnen Projektphasen wurde eine detaillierte Projektskizze erstellt. Als Zeitraum für die Pilotdurchführung ist von ca. 18 Kalendermonaten auszugehen.

5. Anhang

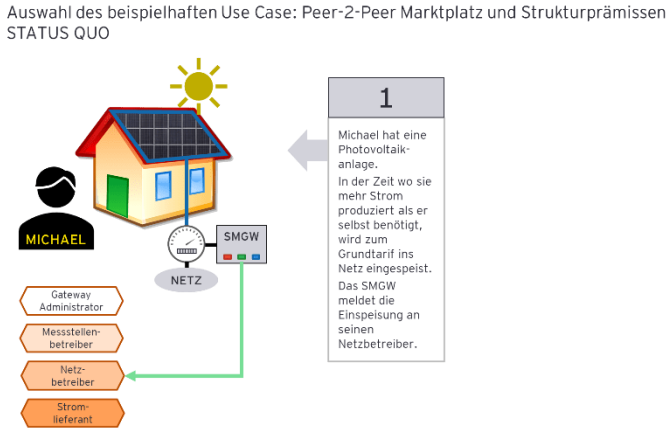
5.1 Anhang A: AP1 - P2P Energie-Lieferung und -Bezug

Dieser Anwendungsfall wurde, aufgrund der Analyse (siehe 3.1.4.1) zu den rechtlichen und regulatorischen Rahmenbedingungen, nach Abstimmung mit der Auftraggeberin nicht weiter vertieft.

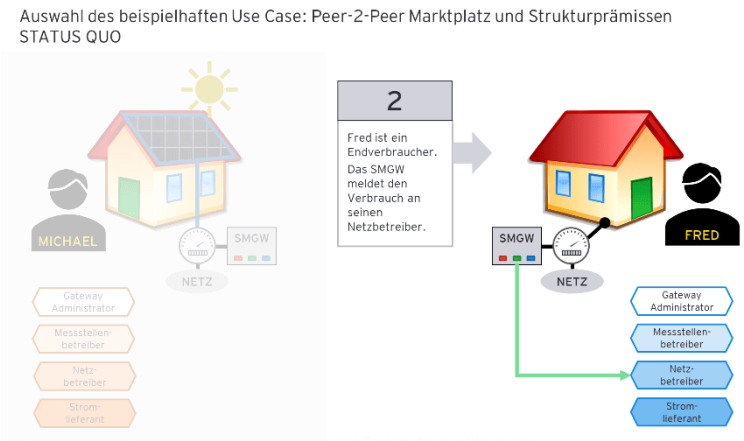
In diesem Anhang finden sich nachfolgend die weiteren Arbeitsergebnisse aus der ersten Iteration des AP1 zum Anwendungsfall P2P-Energie-Lieferung und -Bezug.

5.1.1 Schematische-Darstellung des Use Case

Schritt 1:

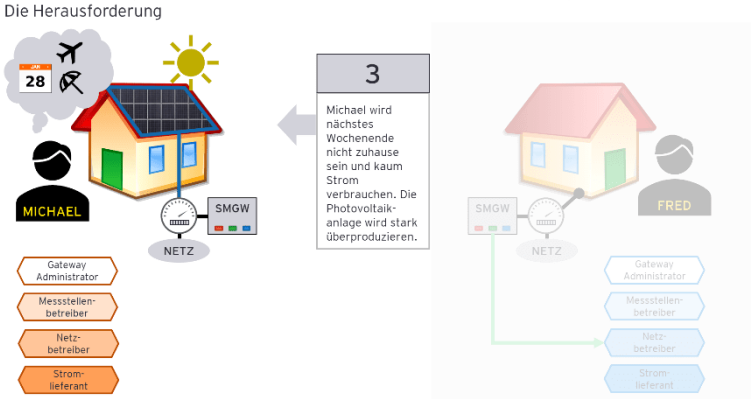


Schritt 2:



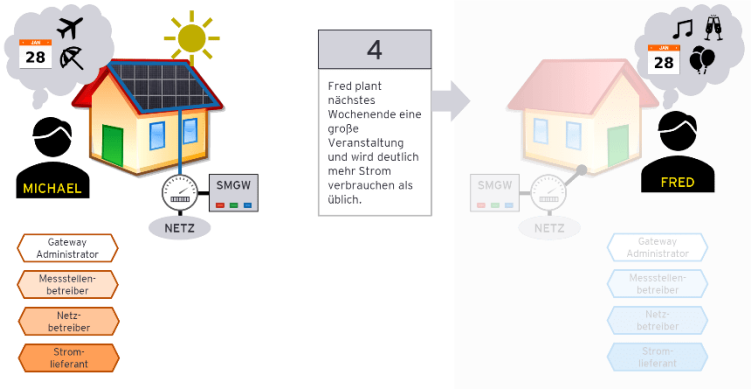
Schritt 3:

Auswahl des beispielhaften Use Case: Peer-2-Peer Marktplatz und Strukturprämissen
Die Herausforderung



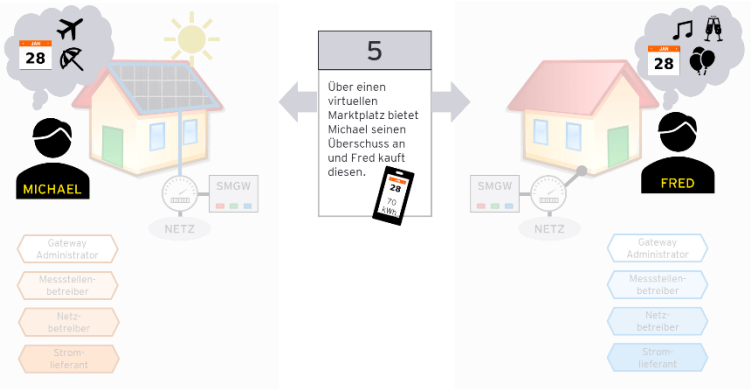
Schritt 4:

Auswahl des beispielhaften Use Case: Peer-2-Peer Marktplatz und Strukturprämissen
Die Herausforderung



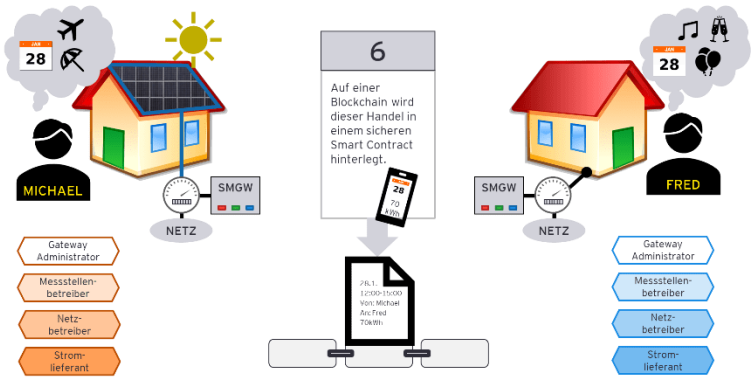
Schritt 5:

Auswahl des beispielhaften Use Case: Peer-2-Peer Marktplatz und Strukturprämissen
Der Marktplatz



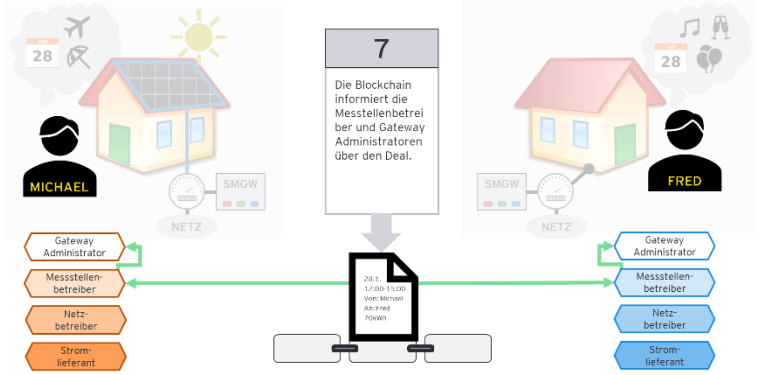
Schritt 6:

Auswahl des beispielhaften Use Case: Peer-2-Peer Marktplatz und Strukturprämissen
Der Marktplatz



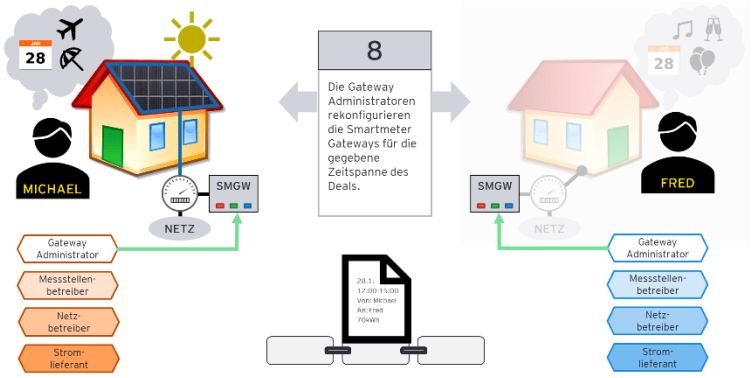
Schritt 7:

Auswahl des beispielhaften Use Case: Peer-2-Peer Marktplatz und Strukturprämissen
Der Marktplatz



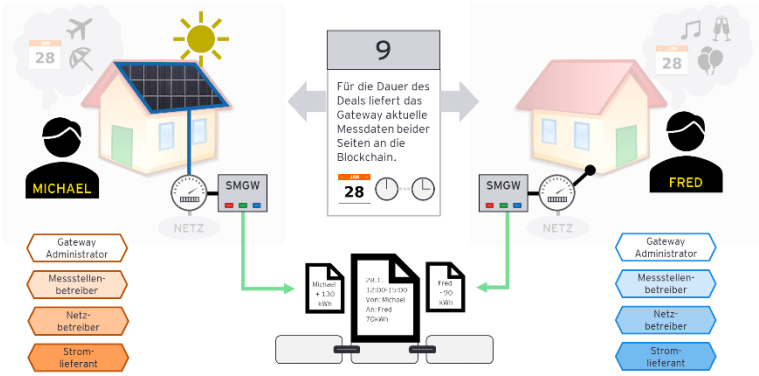
Schritt 8:

Auswahl des beispielhaften Use Case: Peer-2-Peer Marktplatz und Strukturprämissen
Der Marktplatz



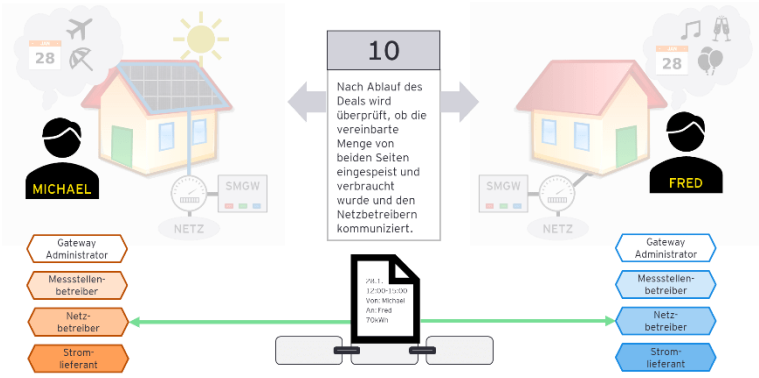
Schritt 9:

Auswahl des beispielhaften Use Case: Peer-2-Peer Marktplatz und Strukturprämissen
Die Ausführung



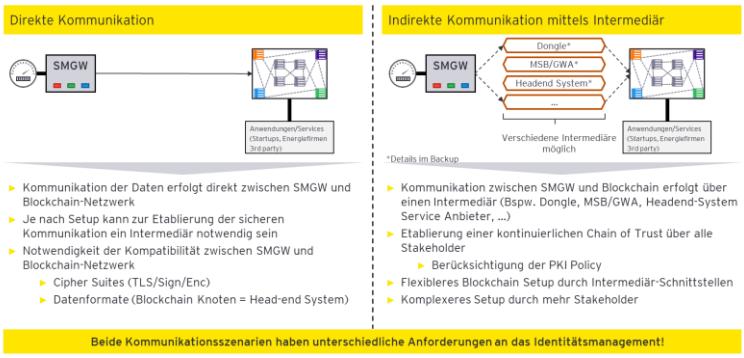
Schritt 10:

Auswahl des beispielhaften Use Case: Peer-2-Peer Marktplatz und Strukturprämissen
Die Ausführung



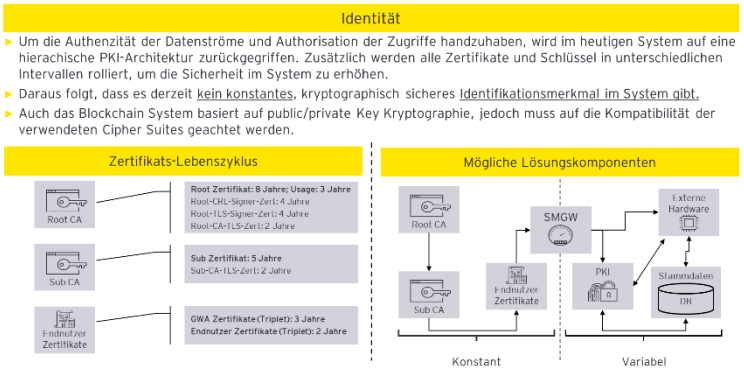
5.1.2 Detailbetrachtung – Kommunikation des SMGW

Detailbetrachtung – Kommunikation Smartmeter Gateway

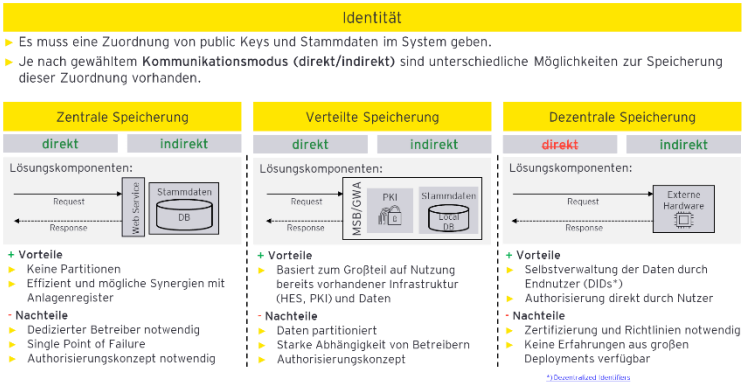


5.1.3 Detailbetrachtung – Identitätsmanagement

Detailbetrachtung – Identitätsmanagement 1/2

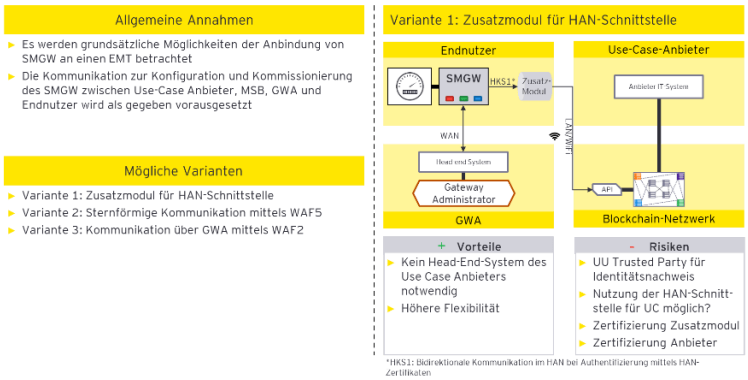


Detailbetrachtung – Identitätsmanagement 2/2

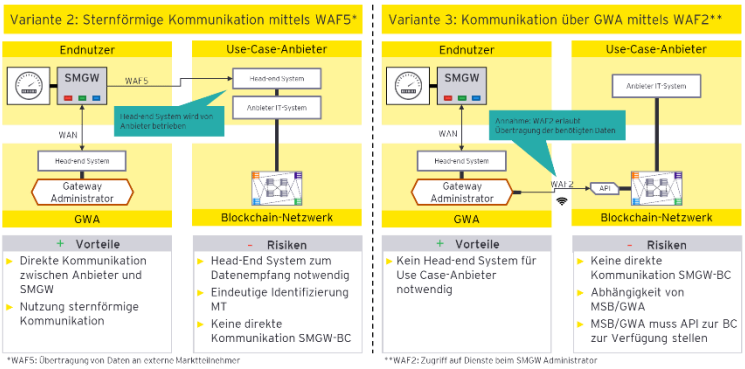


5.1.4 Detailbetrachtung – Möglichkeiten der SMGW-Anbindung

Möglichkeiten der Anbindung SMGW-Blockchain 1/2



Möglichkeiten der Anbindung SMGW-Blockchain 2/2



5.2 Anhang B: AP2 – Detaillierte Projektskizze

5.2.1 PMO

Anforderung	Beschreibung
Reporting- / Dokumentationspflichten definieren	Die Erarbeitung von Reporting- und Dokumentationspflichten ist ein grundlegender Bestandteil des Projektmanagements. Hierbei sind sowohl die Berichtsempfänger als auch die während des Projektes durchzuführenden Anforderungen an das Reporting sowie die Dokumentation durchzuführen.
Projektkoordination planen und etablieren	Um einen geregelten Projektablauf zu gewährleisten ist die Konzeption und Etablierung einer Projektkoordination erforderlich. Aufgabe der Projektkoordination ist insbesondere ▶ Definition und Dokumentation der Projektplanung ▶ Definition und Nachverfolgung von Zielvorgaben ▶ Aufsatz und Durchführung von Abstimmungsterminen ▶ Aufsatz und Durchführung von Lenkungsausschüssen und Stakeholder-Terminen ▶ Aufsatz und Durchführung des Projektcontrollings ▶ Aufsatz und Durchführung des Projektrisikomanagements
Systemunterstützung / Projektinfrastruktur planen	Für die Umsetzung des Projektes ist die zur Verfügungstellung der Projektinfrastruktur zu planen. Dies beinhaltet sowohl die Beschaffung von Hard- und Software als auch bspw. notwendige Infrastruktur wie z.B. Räumlichkeiten oder des Projektmanagementhandbuches. Ebenfalls sind Verfahrensweisen für Beschaffungsvorhaben zu etablieren.
Projektmarketing planen	Um die Darstellung des Projektes sowohl gegenüber der Öffentlichkeit als auch gegenüber interessierten Stakeholdern sowie der Öffentlichkeit zu gewährleisten, ist das Projektmarketing zu planen. Dies beinhaltet nicht nur das Marketing als solches, sondern auch die Identifizierung und Einbeziehung der Stakeholder in das Projekt. Ziel des Projektmarketings ist sowohl die Darstellung der Projektergebnisse als auch die Erhöhung von Verständnis und Akzeptanz für diese. Hierfür ist die Darstellung des Projektes in der Öffentlichkeit zu gewährleisten, bspw. durch die Veröffentlichung von Pressemitteilung, Newsletter, Social Media oder einer Projekt-Homepage.
Projektkoordination umsetzen	Aufgabe des der Aktivität ist die Umsetzung der konzipierten Projektkoordination unter zu Hilfenahme der etablierten Tools, Methoden und Prozesse. Dies beinhaltet u.a. ▶ Die Überwachung des Projektfortschrittes ▶ Die Aktualisierung von Statuskennzahlen

	Die Planung und Durchführung von Statusmeetings und Abstimmungsterminen (Jour Fixes, Lenkungsausschüsse, Gremien
Systemunterstützung / Projektinfrastruktur bereitstellen	Um die Projektbearbeitung zu ermöglichen muss eine Projektinfrastruktur erstellt werden. Dies beinhaltet sowohl Hard- und Software als auch weitere Ressourcen. Für die Beschaffung müssen Anforderungen definiert, Ausschreibungen durchgeführt und evaluiert werden sowie Verträge abgeschlossen. Ebenfalls müssen die Zuständigkeiten für die Ressourcen nach der Beschaffung definiert werden.
Projektkommunikation umsetzen	Diese Aktivität beinhaltet die Umsetzung der in der Planungsphase definierten Projektkommunikation sowohl zur Öffentlichkeit als auch zu den Stakeholdern.
Dokumentation (Templates, Exchange, Sharepoints etc.) bereitstellen	Aufgabe des Arbeitspaketes ist es, die benötigten Ressourcen bereitzustellen, um die in der Phase Plan definierten Projekttätigkeiten und Dokumentationspflichten zu erfüllen. Hierbei werden sowohl technische Ressourcen als auch Templates berücksichtigt und die Durchführung der notwendigen Tätigkeiten etabliert.
Reporting- / Dokumentationspflichten ausführen	Reporting- und Dokumentationspflichten sind als grundlegender Bestandteil des Projektmanagements ordnungsgemäß auszuführen. KPIs zur Überwachung des Projektfortschritts sind entsprechend anzupassen und auszuwerten.
Projektmarketing Resonanz erfassen	Nach Abschluss der Betriebsphase ist die Projektkommunikation nach außen mit einem Fokus auf die erreichten Projektergebnisse weiter fortzusetzen. Darüberhinausgehend ist das Vorgehen der Projektkommunikation im Hinblick auf die erreichte Resonanz zu evaluieren und die Ergebnisse zu dokumentieren.

5.2.2 Planung

5.2.2.1 Prozessdesign

Anforderung	Beschreibung
Institutionelle Aufstellung des Systems definieren	Als Grundlage für die Zusammenarbeit der beteiligten Parteien des Pilotprojektes ist ein Akteursmodell sowie die institutionelle Aufstellung des Systems zu erarbeiten. Das Gesamtergebnis des Arbeitspaketes muss sowohl das Akteursmodell inkl. Rollen, Rechten und Pflichten der beteiligten Parteien enthalten als auch die vertraglichen Grundlagen der Zusammenarbeit reflektieren. Ebenfalls ist eine enge Schnittstelle zur technischen Ausprägung des Piloten bei der Definition der Rollen zu berücksichtigen, da Wechselwirkungen der Rollendefinitionen mit der technischen Umsetzung bestehen (bspw. die kleinste wirtschaftliche Einheit mit einer eigenen Identität).
Geschäftsprozesse zur automatischen Erfassung und Verwaltung von Stammdaten definieren	Als Grundlage der Implementierung des Piloten sind die notwendigen Geschäftsprozesse zur Erfassung und Verwaltung von Stammdaten zu erarbeiten. Als Ausgangspunkt können die Geschäftsprozesse des MaStR herangezogen werden, jedoch ist der Anwendungsfall explizit unabhängig hiervon und unter besonderer Berücksichtigung der technischen Lösung (SMGW/Blockchain) zu betrachten. Möglichen Geschäftsprozesse sind bspw.: ▶ Anmeldung der Anlage ▶ Abmeldung ▶ Änderungsmeldung Weitere notwendige Geschäftsprozesse über den reinen Anwendungsfall hinaus können bspw. sein.: ▶ Verwaltung der Infrastruktur in Form eines Betriebsmodells (z.B. Antrag auf Betrieb eines Blockchain Nodes) ▶ Daten von MSB System ins GWA System bringen ▶ Zentrale Bewirtschaftung der Daten ▶ DSGVO-Prozesse
Usability Konzept erarbeiten	Anhand der definierten Akteure, Rollen und Geschäftsprozesse ist ein Usability Konzept zu erarbeiten. Hierfür sollen Personas und User Stories in Abhängigkeit des Anwendungsfalls erarbeitet werden. Anhand dieser ist ein Konzept der Nutzersicht zu erarbeiten. Das Konzept ist mit Vertretern der jeweiligen Akteure Rolle zu verproben.
Plug & Play Konzept	In Abhängigkeit mit dem Usability Konzept, der technischen Architektur sowie dem Identitätskonzept ist ein Plug & Play Konzept für den Endanwender zu arbeiten.

	Im Fokus soll minimaler Installationsaufwand sowie minimales Fehlerpotenzial beim Endanwender während Installation und Betrieb stehen.
fachliches Daten- / Informationsmodell erarbeiten	Ausgehend vom Anwendungsfall „ öffentliche Anlagendatenbank“ ist ein fachliches Datenmodell zu erarbeiten. Als Ausgangspunkt des Datenmodells können die Anforderungen des MaStR dienen, jedoch ist die Erweiterbarkeit des Datenmodells für weitere Anwendungsfälle eine Anforderung. In dieses Arbeitspaket inbegriffen ist die Definition der Herkunft der Daten sowie der Zeitpunkt der Datenaufnahme in die Datenbank. Ebenfalls ist die Vereinbarkeit der Datenhaltung mit der DSGVO und dem Ansatz der Datensparksamkeit bei der Definition des Datenmodells zu berücksichtigen. Hierbei ist der Ort der Datenhaltung und die Abhängigkeit zu Akteuren, Berechtigungen und Pflegeprozessen zu berücksichtigen.
Feedbacksystem konzipieren	Für die Validierung der Projektergebnisse und Zielsetzungen ist ein Feedbacksystem zu konzipieren. Ziel des Systems ist die Überprüfung der Erfolgskriterien anhand von Umfragen/Bewertungen der Stakeholder. Hierfür muss ein System zur Einholung des Feedbacks konzipiert, die zu befragenden Stakeholder bestimmt und ein Ablauf des Feedbackprozesses bestimmt werden.

5.2.2.2 Kosten-Nutzen Betrachtung

Anforderung	Beschreibung
kommerzielle Machbarkeit erarbeiten	Im Zuge des Pilotprojektes soll die kommerzielle Machbarkeit evaluiert werden. Hierzu ist ein Business Case zu erarbeiten in dessen Zuge die spezifischen Nutzen der Stakeholder, mögliche Anreize für beteiligte (bspw. HES, BC-Knoten-Betreiber) Parteien, regulatorische Preisobergrenzen (bspw. Messstellenbetrieb) sowie Hardwarekosten zu berücksichtigen sind. Weiterhin sollten mögliche Fördergelder für die Entwicklung sowie den Rollout berücksichtigt werden. Ein Teil des Business Cases ist ebenfalls ein betriebswirtschaftliches Vergütungssystem für alle beteiligten Parteien. Der Business Case hat direkte Schnittstellen zur Evaluierung des gesamtwirtschaftlichen Nutzens, welche im Zuge der Bearbeitung der Aktivität berücksichtigt werden sollten.
Make-or-Buy Entscheidungen treffen	In Abstimmung mit den technischen Arbeitspaketen sind Make-or-Buy Entscheidungen zu treffen. Hierfür ist es erforderlich Anforderungen an Technologie-Auswahlprozesse zu definieren, Optionen für Managed Services zu erarbeiten, Anforderungen an das Kostenstabilität zu definieren (bspw. im Falle von Skalierung von Datenübertragung, Hosting usw.).

	Ebenfalls sind im Zuge dieser Überlegungen Lifecycle Modelle zu erarbeiten sowie Ersatzkosten und die Nachhaltigkeit der Lösungen zu berücksichtigen.
Sinnhaftigkeit Verwendung Blockchain eruieren	Die Verwendung von Blockchain-Technologie im Zuge der Pilotierung ist eine externe Vorgabe an die Architektur. Dennoch ist die Sinnhaftigkeit der Verwendung von Blockchain im Zuge des Projektes zu evaluieren. Besonderes Augenmerk sollte hierbei auf den Vergleich der Datenbanklösung mit einer konventionellen Datenhaltung bei ähnlicher Einbindung des SMGWs gelegt werden. Zu berücksichtigende Aspekte können beispielsweise Eigenschaften wie ökologische Auswirkungen, Ausfallsicherheit und Mehrwerte durch verteilte BC-Knoten sein.

5.2.2.3 Technische Architektur

Anforderung	Beschreibung
Kommunikation mit BSI	Um eine mit dem BSI abgestimmte Lösung zu erreichen, ist zeitgerechte Kommunikation unabdinglich. Insbesondere die Frage, ob für den Piloten ein eigener Anwendungsfall geschaffen werden soll, spielt eine Rolle. Daneben muss auch geklärt werden, welche Daten und Funktionen im ToE gespeichert werden können, sowie welches Zertifikatsmaterial für die Kommunikation des SMGW mit CLS Devices verwendet werden darf. Zentral für die spätere Nutzung im späteren Produktivbetrieb ist die garantierte Rückwirkungsfreiheit. Der Entwurf einer Wunschspezifikation muss ein detailliertes Konzept beinhalten.
Datenmodell/-Managementkonzept erstellen	Um kohärente Daten zu gewährleisten, muss ein Datenmodell sowie ein umfassendes Datenmanagementkonzept geschaffen werden. Ein solches Konzept inkludiert Zugriffsberechtigungen zu Daten sowie ein detailliertes Sichtbarkeitskonzept um Daten vor unberechtigtem Zugriff zu schützen. Dieses soll in einem Rollenmodell klar ersichtlich sein. Weiters ist auszuarbeiten, welche Daten on-chain (im Blockchain System) sowie off-chain (außerhalb des Blockchain Systems) gehalten werden sollen. Außerdem ist die Konzeptionierung der Sicherstellung der Authentizität der Stammdaten erforderlich.
Domain Modell erarbeiten	Um eine saubere, zukunftssichere Architektur zu erhalten, soll ein Domain Model erarbeitet werden. Kernfrage dabei ist die

	trennscharfe Abgrenzung von logischen Grenzen. Weiters muss definiert werden, in welchen Komponenten Business Logik enthalten ist. So kann beispielsweise ein Teil der Logik in den Smart Contracts der Blockchain stecken. Das Ergebnis muss als UML Diagramm dokumentiert werden.
Identitätskonzept erarbeiten	Um eine reibungslose Integration der Identitäten zu gewährleisten, soll bestehendes ID Management eruieren werden und neu zu schaffende ID Management Prozesse definiert werden. Derzeit gibt es bereits Identitätsmanagement bei PKI und Blockchain, daher muss ein Konzept erstellt werden, wie das Zusammenspiel funktionieren kann.
SMGW Technologieauswahl treffen	Das SMGW stellt das Herzstück des Piloten dar, da es den Vertrauensanker bildet. Damit die im Piloten zu verwendenden Geräten den Anforderungen genügen, sind vorab Hardwareanforderungen zu definieren. Anschließend muss eruiert werden, ob für den Piloten ein bestehendes SMGW verwendet werden kann oder Anpassungen erforderlich sind. Weiters muss festgehalten werden, ob die Produktiv-PKI verwendet werden soll, oder eine Test-PKI genutzt wird.
GWA System & MSB Backend auswählen	Damit das SMGW für den Use Case verwendet werden kann, muss es zuvor von einem GWA konfiguriert werden. Damit der GWA diese Aufgaben wahrnehmen kann, ist ein leistungsfähiges System erforderlich. Dieses System muss anpassbar bzw. erweiterbar sein um Prozessanforderungen umsetzen zu können. Weiters soll die Anbieteränderbarkeit gegeben sein. Basierend auf diesen Anforderungen, ist ein geeignetes GWA System sowie ein MSB Backend System auszuwählen. Alle Anforderungen für etwaige Änderungen, die für die Kompatibilität erforderlich sind, sind festzuhalten.
CLS-Gerät Technologieauswahl treffen	Um mit einer externen Ressource kommunizieren zu können, ist die Verwendung eines CLS Geräts von Vorteil. Damit die im Piloten zu verwenden Geräte den Anforderungen genügen, sind vorab Hardwareanforderungen zu definieren. Anschließend muss eruiert werden, ob für den Piloten ein bestehendes CLS Gerät verwendet werden kann oder Anpassungen erforderlich sind. Zusätzlich ist das SDK des CLS Geräts auf Tauglichkeit zu evaluieren und Anpassungen, die gegebenenfalls notwendig sind, festzuhalten.
Blockchain-Technologie Auswahl treffen	Die Auswahl der Blockchain-Technologie muss zahlreiche Kriterien berücksichtigen. Zuvor muss eruiert werden, welche Teilnehmer Blockchain Knoten benötigen und in welcher Ausführung (Full / Light) diese sinnvoll wären. Der zu wählende Konsensalgorithmus muss dem Kriterium der

	Umweltfreundlichkeit entsprechen, muss die nötige Performance erreichen und muss Sicherheit bei der voraussichtlichen Anzahl der Knotenbetreiber erreichen.
Sicherheitskonzept erarbeiten	Als Grundlage für die Gewährleistung von Sicherheit des neu zu schaffenden Systems ist ein umfassendes Sicherheitskonzept zu erstellen. Dieses muss sowohl die Sicherheit der Teilsysteme, als auch des Gehaltssystems aus Frontend, Backend, Blockchain, CLS sowie SMGW berücksichtigen.
Kommunikationsinfrastrukturkonzept erstellen	Um ein reibungsloses Zusammenspiel der Komponenten zu ermöglichen, ist eine zuverlässige Kommunikationsinfrastruktur unabdinglich. Dazu zählt eine stabile WAN Verbindung zwischen SMGW und GWA, wobei wenn möglich ein Tunnel aufrechterhalten werden soll. Weiters muss eine sichere Kommunikation der einzelnen Komponenten untereinander sichergestellt werden. Insbesondere das CLS Gerät und die Blockchain Knoten müssen auf eine zuverlässige Netzwerkinfrastruktur zurückgreifen können.
Validierungstool definieren	Da Verwendung einer Blockchain zwar die Unveränderbarkeit von Daten garantiert, diese aber nur schwer für Laien überprüfbar ist, soll ein benutzerfreundliches Validierungstool geschaffen werden. Um die Anforderungen vollständig zu erfassen, ist es von Vorteil, mehrere Szenarien für mögliche Dispute erarbeiten, die mittels Blockchain aufgeklärt werden können. Weiters soll ein umfassendes Konzept für Auditierbarkeit eruiert werden.
Skalierbarkeitskonzept erarbeiten	Skalierbarkeit ist ein Erfolgskriterium des Piloten. Um diese zu gewährleisten, ist die Durchführung von Stresstests ein geeignetes Mittel. Um realistische Annahmen für die Definition der Stresstests zu erhalten, sollen im Vorfeld mehrere Szenarien erarbeitet werden. Basierend darauf ist eine Spezifikation der Stresstests zu erstellen.
Risikomanagement definieren	Um dem Erfolgskriterium der Nachhaltigkeit im Sinne der Weiterverwendbarkeit des Piloten gerecht zu werden, ist es wesentlich, ein System zu schaffen, das möglichst größtmögliche Flexibilität zulässt und frei von sogenannter „technischer Schuld“ (technical debt) ist. Dazu ist es erforderlich, von Beginn an Risikomanagementprozesse zu definieren, die sich der Identifikation, der Vermeidung sowie dem Management von möglichen Risiken annehmen.
Change Management Konzept erarbeiten	Um eine reibungslose Transition vom Piloten zum Produktivbetrieb sicherzustellen, soll ein Change-Management Konzept ausgearbeitet werden. Dieses soll eine umfassende Planung der Mechanismen zur Migration,

	Einhaltung von Kompatibilität und Zukunftssicherheit beinhalten.
Technische Umsetzung des Plug-&Play/Usabilitykonzepts erarbeiten	Ein zentrales Erfolgskriterium des Piloten ist die Benutzerfreundlichkeit für Endanwender. Um die technische Umsetzbarkeit dieses zuvor definierten Plug & Play Konzepts sicherzustellen, soll diese im Detail erarbeitet werden. Dazu zählt etwa die Fragestellung, wie ein Private Key eines Anlagenbetreibers benutzerfreundlich und sicher ins SMGW eingebracht werden kann. Weiters ist die Spezifikation eines Frontends zu erarbeiten sowie ein modernes Frontend Framework auszuwählen, das den Anforderungen gerecht wird.
Testkonzept erarbeiten	Ein wesentliches Mittel zur Sicherstellung von Funktionalität und Qualität ist der Einsatz von Tests. Im Sinne der „Test Driven Design“ Methodik sind Tests bereits im Vorfeld zu spezifizieren. Dabei kommen sowohl Unit Tests der einzelnen Komponenten, sowie Integration Tests zum Einsatz. In der Design Phase soll ein umfassendes Konzept diesbezüglich erarbeitet werden.
Dokumentationsschema festlegen	Um eine vollständige Dokumentation zu gewährleisten, ist es erforderlich, die Anforderungen klar und rechtzeitig zu definieren. Zu einer ordnungsgemäßen Dokumentation zählen sowohl eine umfassende technische Dokumentation, als auch ein benutzerfreundliches Anwenderhandbuch und eine Support Guideline.

5.2.2.4 Governance

Anforderung	Beschreibung
Abstimmung und übergreifende Festlegung im Projekt herbeiführen	Die Governance des Projektes hat starke Nähe zur Projektkoordination. Die Aufgabe der Aktivität besteht darin Abstimmungen und Entscheidungen zwischen den Projektteilnehmern herbeizuführen und nachhaltige Strukturen für die Entscheidungsfindung innerhalb des Projektes zu schaffen. Hierfür sind Gremien nach Entscheidungsbereichen mit den relevanten Projektpartnern zu etablieren, welche grundlegen Entscheidungen zu bestimmten Bereichen abstimmen und fällen. Entscheidungsbereiche können unter anderem sein ▸ PKI ▸ Usability ▸ Standards, Algorithmen, Protokolle und Schnittstellen ▸ Rechtliche Verantwortlichkeiten ▸ Datenmodell

	▶ Anwendungsfall Interoperabilität Ebenfalls ist ein Gremium zur Schlichtung bei Interessenkonflikten sowie bei der Veränderung der Projektpartnerschaft zu etablieren. Des Weiteren sind Prozesse zu definieren, über die Entscheidungsvorlagen an die Gremien übermittelt werden.

5.2.2.5 Recht & Regulatorik

Anforderung	Beschreibung
Akteure	Um im Folgenden definieren zu können, u. a. welche Pflichten und welche vertraglichen Verhältnisse bestehen sowie um welche Prozesse es im Laufe des Pilotprojektes geht, müssen zunächst die betroffenen Akteure identifiziert werden. In einem zweiten Schritt ist die Frage zu klären, wer Zugriff auf die Blockchain-Daten zu welchem Zweck bzw. in welcher Rolle und ggf. In welchem Umfang erhält; es geht daher um die direkten Teilnehmer an der Blockchain. In datenschutzrechtlicher Hinsicht müssen die Akteure richtig zugeordnet werden (Verantwortlicher, Auftragsverarbeiter, Gemeinsame Verantwortliche) und die entsprechenden gesetzliche geforderten Verträge und Übermittlungsgrundlagen definiert.
Definition der Prozesse	Parallel zur Identifikation der Akteure / Teilnehmer gilt es, die einzelnen Prozesse, die im Rahmen des Pilotprojekts durchgeführt werden, zu identifizieren und zu definieren. Dazu gehören u. a. die folgenden Prozesse: ▶ An- und Abmeldung ▶ Änderungsmeldung ▶ Zeitpunkt der Meldung ▶ Umfang der Daten nach MaStRV ▶ Prüfung der datenschutzrechtlichen Erfordernisse an die Prozesse (insb. Gestaltung, Beteiligte und Dokumentation) ▶ Datenschutzfreundliche Ausgestaltung (Art.5, 25 DSGVO), insbesondere datenschutzfreundliche Voreinstellung des SMGW ▶ Soweit erforderlich, Prozessbeschreibung zu und Definition der Durchführung von Datenschutzfolgeabschätzungen ▶ Abschluss der richtigen datenschutzrechtlichen Verträge bei den Akteuren inkl. der BNetzA

Klärung von Systemfragen	Bevor mit der rechtlichen Ausgestaltung des Pilotprojektes begonnen werden kann, sind weitere grundsätzliche Fragen zu klären, die den rechtlichen Rahmen betreffen: Dazu gehören u. a. die folgenden Fragenstellungen: ► Ist das geltende Recht anzupassen? o Zum einen stellt sich die Frage bzgl. Des Registrierungsverfahrens nach § 8 MaStRV. Danach besteht grundsätzlich die Verpflichtung zur Nutzung des Webportals. In der "Plan"-Phase des Pilotprojektes wird mithin die Frage zu klären sein, ob die automatische Registrierung unter Anwendung des SMGW sowie der Blockchain-Technologie als Ausgestaltung des Webportals zu bewerten ist oder ein neues, bisher in der MaStRV nicht geregeltes Registrierungsverfahren darstellt, welches eine Anpassung der MaStRV erfordern würde. o Darüber hinaus wird zu prüfen sein, ob die im MsbG festgelegten Preisobergrenzen (§ 31 MsbG) insbesondere aufgrund von Erweiterungen von Daten-Speicherkapazitäten gemäß § 34 MsbG angepasst werden sollten. In diesem Rahmen ist auch zu prüfen, ob die in § 34 MsbG anvisierte früheste Anpassungsmöglichkeit der Preisobergrenzen ab 2027 anzupassen ist. ► Ist das System freiwillig oder verpflichtend auszugestalten? Es ist zu prüfen, ob die anvisierte Plug-and-Play-Lösung verpflichtend auszugestalten ist oder auf freiwilliger Basis umgesetzt werden soll. In letzterem Fall würden daher der Status Quo sowie die anvisierte Plug-and-Play-Lösung nebeneinander bestehen und ggf. aufeinander abgestimmt werden müssen. ► Prüfung der europarechtlichen Vereinbarkeit der MaStRV, insbesondere der Aufbewahrungsfristen (in Hinblick auf die DSGVO die Öffnungsklauseln) ► Verantwortlichkeiten und Haftung u.a. für fehlerhafte Datenübertragungen oder Datenmanipulationen
Compliance Konzept erarbeiten	Zunächst muss für die Verarbeitungen die Rechtsgrundlage identifiziert und ggf. eine Interessenabwägung vorgenommen werden. Angemessene Methoden zur Sicherstellung der Dokumentationspflichten der DSGVO sind zu identifizieren. Zur Wahrung von Transparenz und der Betroffenenrechte, vor allem der Informationsrechte, sind, auf Basis der identifizierten Akteure, Kommunikationskonzepte zur Sicherstellung der Verpflichtungen aus Art. 12, 13 und 14 DSGVO zu erarbeiten.

	Aufgrund neuster Entwicklungen, ist mittlerweile wohl davon auszugehen, dass die Marktakteure, die direkt am Blockchain-Netzwerk teilnehmen, als gemeinsame Verantwortliche klassifiziert werden. In der Plan-Phase sind daher die Verpflichtungen, die sich aus der Teilnahme ergeben, zu spezifizieren. Diese können zur Erarbeitung von Vertragstemplates dienen. Nach derzeitigen Erkenntnissen (Sachverhalt, Rechtslage, etc.) ist der Nutzer (privater/gewerbliche Kunde) eines SMGW nur als Betroffener zu qualifizieren, denn dieser nimmt nicht am Blockchain-Netzwerk teil, sendet nur seine Daten an die Marktakteure und empfängt keine personenbezogenen Daten. Aufgrund der möglichen Einordnung als Auftragsverarbeiter der Marktakteure zueinander in den verschiedenen Modellen, ist neben der Identifizierung von Gemeinsamkeiten zur Erarbeitung eines Auftragsverarbeitungsvertragstemplates, auch die Erstellung eines Vertragsmanagementtools zu prüfen. Um insbesondere den Grundsatz der Datensparsamkeit gerecht zu werden ist die Entwicklung differenzierter Konzepte – Lösch- und Zugriffsberechtigung – notwendig. Dabei sind die Fristen zu identifizieren zu denen die Daten off-chain gelöscht werden müssen, ebenso wie Akteure und die Daten, auf die in bestimmten Situationen zugegriffen werden kann. Für eine etwaige Datenverarbeitung außerhalb der EU/EWR müssen geeignete Garantien zur Sicherung der datenschutzrechtlichen Anforderungen identifiziert und geprüft werden, alternativ sollte konzeptionell der Export außerhalb der EU/des EWR ausgeschlossen werden. Um einen datenschutzrechtlichen Mindeststandard bei allen Marktakteuren zu erreichen kann bsp. die Erstellung von Handreichungen, Informationsblättern, Musterverträgen und Templates zur angemessenen Dokumentation geprüft werden. Neben den datenschutz- und lizenzrechtlichen Verpflichtungen sind die einzuhaltenden energierechtlichen Verpflichtungen u. a. aus MsbG und MaStRV zu identifizieren. In der Plan-Phase wäre zu prüfen, in welcher Form die Einhaltung dieser Pflichten sichergestellt / vereinfacht werden kann, ggf. durch Erstellung eines Leitfadens.
Klärung von Verpflichtungen und Haftungsfragen	Die MaStRV beinhaltet Regelungen dazu, welcher Marktakteur verpflichtet ist, welche Informationen und in welcher Form zu melden. Verstöße gegen die Registrierungspflicht werden sanktioniert. Vor dem Hintergrund der Plug&Play-Lösung sollte zum einen der Status Quo der Verpflichtungen sowie der Haftungsregelungen bzgl. möglicher Verstöße identifiziert werden. Zum anderen sollte geprüft werden,

	▶ inwiefern die bestehenden Verpflichtungen und die damit einhergehende Haftung im Rahmen der geplanten Plug&Play-Lösung noch Bestand haben kann, ▶ ob ggf. gesetzliche Anpassung für eine Verschiebung der Haftungsregelungen notwendig wird, ▶ welche (neuen) Haftungsrisiken ggf. auf die einzelnen Akteure / Teilnehmer zukommen (z. B. aufgrund von technischen Fehlern), ▶ wie die einzelnen Akteure / Teilnehmer sich ggf. gegen diese jeweiligen Haftungsrisiken absichern können und ▶ welche Schritte bei einem Data Breach einzuleiten sind. Es sollte identifiziert werden, ob Materialien, z.B. Handreichungen zur Dokumentation und Haftung, insbesondere Bußgeldberechnung und -praxis von Datenschutzbehörden, den Marktteilnehmern bei der datenschutzrechtlichen Haftungsvermeidung helfen kann.
Vertragskonzept	Nachdem die einzelnen Akteure / Teilnehmer, deren jeweilige Verpflichtungen und Haftungsrisiken sowie mögliche Gesetzesanpassungen identifiziert wurden, gilt es, die vertraglichen Verhältnisse bzw. notwendigen Verträge zwischen den einzelnen Akteuren / Teilnehmern zu identifizieren sowie deren wesentliche Inhalte, z. B. in Form von “Term Sheets”, festzulegen.

5.2.3 Umsetzung

5.2.3.1 Aufbau Systemumgebungen

Anforderung	Beschreibung
Systemumgebungen der Einzelkomponenten aufbauen	Bevor die Einzelkomponenten implementiert werden können, ist der Aufbau entsprechender Systemumgebungen notwendig. Zum einen muss das Cloud Hosting den Anforderungen entsprechend provisioniert werden. Weiters sind die physischen Räumlichkeiten zu schaffen, in denen SMGWs sowie CLS Geräte aufgebaut und in Betrieb genommen werden können. Zusätzlich müssen MSB sowie GWA Backend Systeme installiert werden. Die Einrichtung einer Entwicklungs- sowie Laufzeitumgebung für das Blockchain Netzwerks bzw. die Blockchain Knoten ist zu bewerkstelligen. Weiters müssen Entwicklungsumgebungen für das Backend System sowie das Frontend System aufgebaut werden.

5.2.3.2 Aufbau Systemintegration

Anforderung	Beschreibung
Systemumgebungen der Einzelkomponenten verbinden	Nachdem die Systemumgebungen der Einzelkomponenten aufgebaut wurden, müssen diese verbunden werden. Die Cloud muss von außen für Berechtigte erreichbar sein. Der GWA muss eine Netzwerkanbindung zwischen dem MSB sowie GWA Backend und dem SMGW sicherstellen. Das SMGW muss mit dem CLS Gerät ordnungsgemäß kommunizieren können. Die Blockchain Knoten müssen sowohl untereinander kommunizieren können, als auch für das Backendsystem erreichbar sein. Das Backendsystem muss für ein Frontend ansprechbar sein. Das Frontend muss für Endgeräte aufrufbar sein. Der Erfolg soll durch simple Integrationstests (z.B. „ping“) laufend überprüft werden.

5.2.3.3 Prozess

Anforderung	**Beschreibung**
Rollen- und Rechtekonzept in den Systemen umsetzen	Aufgabe des Arbeitspaketes ist es die im Projektabschnitt Plan definierten Rollen und Rechte zu implementieren. Dies beinhaltet sowohl die Umsetzung des Konzeptes im Hinblick auf Zugriffsberechtigungen, aber auch die Implementierung von Prozessen zur Rechteverwaltung (Authentifizierung, Autorisierung, Anpassung von Rechten, Anlegen neuer Akteure, ...). Die Umsetzung des Rollen- und Rechtekonzeptes ist eng mit der technischen Implementierung der Lösung abzustimmen, da Auswirkungen auf alle beteiligten Akteure und Prozesse bestehen. Ebenfalls ist zu berücksichtigen, ob verschiedene Rollen Anpassungen des Frontends erfordern.
Geschäftsprozesse zur automatischen Erfassung und Verwaltung von Stammdaten implementieren	In diesem Arbeitsschritt sind die Geschäftsprozesse zur automatischen Erfassung und Verwaltung von Stammdaten zu implementieren, welche in der Phase Plan definiert wurden. Bei der Implementierung sind ebenfalls die Ergebnisse der Usability sowie des Plug & Play Konzeptes sowie der Umsetzung dieser Ergebnisse zu berücksichtigen.
Usability Konzept umsetzen	Ziel des Arbeitsschrittes ist die Umsetzung des erarbeiteten Usability Konzepte in Form des Frontends. Hierzu sind Mockups zu erstellen und zu testen. Die Einbindung des Frontends in die Geschäftsprozesse ist zu gewährleisten um somit eine End-to-End User Experience entlang der Geschäftsprozesse für die beteiligten Akteure zu ermöglichen.
Feedbacksystem aufbauen	Das in der Phase Plan definierte Feedbacksystem ist betriebsbereit umzusetzen und zu etablieren. Die erfordert einen vorhandenen Feedback Prozess, definierte KPIs und definierte Stakeholder.

5.2.3.4 Technische Implementierung

Anforderung	Beschreibung
Datenmodell/-Managementkonzept implementieren	Das in der Designphase erstellte Datenmodell, sowie das Datenmanagementkonzept, welches Zugriffsberechtigungen, Rollenmodell und einen Prozess zur Sicherstellung der Authentizität enthält, soll in diesem Arbeitspaket umgesetzt werden. Weiters ist auch die on-chain (im Blockchain System) sowie off-chain (außerhalb des Blockchain Systems) Datenspeicherung zu implementieren.
Domain Modell umsetzen	Das in der vorhergehenden Design Phase definierte UML-Modell soll nun ordnungsgemäß umgesetzt werden. Die Business Logik soll dabei je nach Definition im Modell teilweise im Backend, sowie teilweise als Blockchain Smart Contract implementiert werden.
Schnittstellen / Integration umsetzen	Um die einzelnen Systemkomponenten zu integrieren, sind entsprechende Schnittstellen zu implementieren. Wie in der Design Phase festgelegt, sollen entsprechende APIs sowie Services (Identity, Files, etc.) umgesetzt werden.
Identitätskonzept umsetzen	Wie im Konzept für Identitätsmanagement zuvor festgehalten, soll das reibungslose Zusammenspiel der unterschiedlichen Identitäten (private Keys, Tokens, etc.) implementiert werden.
SMGW in Betrieb nehmen	Das SMGW muss eingebaut und in Betrieb genommen werden. Der GWA muss unter Verwendung der korrekten PKI das SMGW initialisieren und sicherstellen, dass es für die weitere Verwendung korrekt konfiguriert ist.
CLS Gerät in Betrieb nehmen	Bevor am CLS Gerät Software installiert werden kann, muss dieses ebenfalls in Betrieb genommen werden. Die notwendige Firmware, sowie das SDK muss installiert werden und ein Zugang für den Upload von weiteren Programmteilen eingerichtet werden.
Blockchain Knoten aufbauen	Je nach Typus des in der Design Phase ausgewählten Blockchain Protokolls, ist das Blockchain Netzwerk entsprechend aufzubauen. Im Falle der Verwendung eines privaten Konsortialnetzwerks, ist ein initiales Bootstrapping durchzuführen, bei dem alle Knoten verbunden werden.
Frontend implementieren	Wie im Konzept zuvor festgelegt, soll in diesem Arbeitspaket die Programmierung des Frontends umgesetzt werden. Dabei sind die zuvor erstellten Mockups maßgeblich, wobei regelmäßig Feedback eingeholt und eingearbeitet werden soll.
Sicherheitskonzept umsetzen	Unter Berücksichtigung neuer Erkenntnisse und Änderungen während der Implementierung von einzelnen

	Systemkomponenten soll das in der Planungsphase erstellte Sicherkeitskonzept entsprechend umgesetzt werden.
Kommunikationsinfrastruktur aufbauen	Um dem GWA die Inbetriebnahme und Konfiguration des SMGW zu ermöglichen, ist eine stabile WAN Verbindung herzustellen. Dazu ist ein permanenter Tunnel zwischen dem SMGW und dem Head End System des MSB aufzubauen. Weiters ist die ordnungsgemäße Verbindung zwischen dem SMGW und dem CLI Gerät sicherzustellen.
Validierungstool implementieren	Das zuvor in der Design Phase erstellte Konzept für ein Validierungstool, welches die Daten der Blockchain benutzerfreundlich ausliest und damit Audit Prozesse vereinfacht, soll in diesem Arbeitspaket technisch umgesetzt werden.
Skalierungs-/Performancetests implementieren	Stresstests sowie Performance Tests sind wie zuvor festgelegt zu programmieren. Änderungen in den jeweiligen Systemkomponenten sind entsprechend zu berücksichtigen.
Usabilitykonzept umsetzen	Die Umsetzung des in der Design Phase erstellten Plug & Play Konzepts umfasst die Implementierung des Frontends sowie der Schaffung von Möglichkeiten zur einfachen Handhabung des privaten Schlüssels durch Anlagenbesitzer. Die Umsetzung muss durch User Feedback nach jedem Sprint evaluiert werden und Feedback entsprechend umgesetzt werden.
Testkonzept implementieren	Die zuvor festgelegten Modalitäten des Unit- sowie Integration Testing sollen in diesem Arbeitspaket ordnungsgemäß durchgeführt werden. Die Tests sind mit wachsendem Umfang laufend zu erweitern und die volle Abdeckung einzuhalten.
Dokumentation erstellen	Um die Weiterverwendbarkeit des Piloten sicherzustellen, ist darauf zu achten, alle technischen Komponenten bestmöglich zu dokumentieren. Gemäß des zuvor in der Design Phase erarbeiteten Konzepts, soll die technische Dokumentation sowohl direkt im Code erfolgen, als auch als eigenes Handbuch exportiert werden. Das Anwenderhandbuch sowie die Support Guideline sind ebenfalls zu erstellen. Dabei ist darauf zu achten, für die unterschiedlichen Zielgruppen die passende Sprache sowie den optimalen Detailgrad zu wählen.

5.2.3.5 Governance

Anforderung	Beschreibung
Abstimmung und übergreifende Festlegung für kritische Themen der Architektur und der Anwendung herbeiführen	Ziel des Arbeitspakets ist der Aufsatz sowie die Gremienarbeit der definierten Autoritäten und Gremien zur Abstimmung und Entscheidungsfindung. Ebenfalls ist sicherzustellen, dass Prozesse für die Übermittlung von Entscheidungsvorlagen an die entsprechenden Gremien etabliert und das Ergebnis der Entscheidungen an die relevanten Stakeholder kommuniziert wird.

5.2.3.6 Recht und Regulatorik

Anforderung	Beschreibung
Aufsetzen von Verträgen, Gesetzesänderungen etc.	Sofern in der Plan-Phase ermittelt wurde, dass eine Anpassung des geltenden Rechts notwendig ist, insbesondere das Registrierungsverfahren nach § 8 MaStRV und die Preisobergrenzen nach § 31 MsbG angepasst oder ergänzt werden müssen, beinhaltet die Build-Phase auch die Prüfung von rechtlichen Handlungsoptionen und ggf. das Entwerfen von Formulierungen für Gesetzesänderungen. Die in der Plan-Phase z.B. in Form von „Term-Sheets“ festgelegten wesentlichen Inhalte der vertraglichen Verhältnisse zwischen den einzelnen Akteuren/Teilnehmern sind in der Build-Phase in Form von Vertragsentwürfen umzusetzen.
Aufsetzen von Tools/Reporting zur Überprüfung der Compliance	Die Einhaltung der rechtlichen Vorgaben u.a. aus dem MsbG, der MaStRV und der DSGVO, die im Compliance-Konzept identifiziert worden sind, ist fortlaufend zu gewährleisten. Dabei sind die vorgenannten erarbeiteten Gesetzesänderungen und Verträge sowie das in der Plan-Phase erarbeitete Compliance-Konzept und die darin identifizierten Maßnahmen zu berücksichtigen. Um juristischen Experten die Auswertung des Prozesses zu ermöglichen, ist ein entsprechendes Reporting zu implementieren (z.B. PDF-Reports). Die Rohdaten des Blockchain Transaktionen sind dazu in ein entsprechendes Format zu bringen, sodass diese für nicht technisch versierte Personen auswertbar sind.
Compliance überprüfen	Die Einhaltung der rechtlichen Anforderungen, ggfs. unter Berücksichtigung der vorgenannten erarbeiteten Gesetzesänderungen und Vertragsentwürfe, ist mithilfe des

	bestehenden Compliance-Konzepts und den dafür eingerichteten Tools fortlaufend zu kontrollieren. Hierzu gehört auch der Prozess zur kontinuierlichen Verbesserung (KVP) Prozess. Die Prüfung und Einhaltung des Compliance-Konzepts ist in geeigneter Weise zu dokumentieren. Es ist stetig zu prüfen, ob die Notwendigkeit einer Anpassung der inhaltlichen und formalen Dokumentation besteht. Optional wird ein Compliance Managementsystem / Datenschutzmanagementsystem implementiert, um die Prüfung zu erleichtern.

5.2.4 Betrieb

5.2.4.1 Systemumgebungen

Anforderung	Beschreibung
Systemumgebungen der Einzelkomponenten betreiben	Während des Betriebs muss der reibungslose Betrieb der Einzelkomponenten und deren Systemumgebungen sichergestellt werden. Dazu zählen die in der Cloud betrieben Server, die Kommunikationsinfrastruktur, die physische Umgebung der Geräte (SMGW, CLS), sowie die Blockchain Knoten, in denen Smart Contracts ausgeführt werden.

5.2.4.2 Systemintegration

Anforderung	Beschreibung
Verbindung der Systemkomponenten aufrecht erhalten	Die Aufrechterhaltung der Netzwerkanbindung zwischen dem MSB sowie GWA Backend und dem SMGW soll sichergestellt werden. Die Verbindung zwischen SMGW und CLS Gerät muss aufrechterhalten werden. Die Blockchain Knoten müssen sowohl untereinander kommunizieren können, als auch für das Backendsystem erreichbar sein. Das Backendsystem muss für ein Frontend ansprechbar sein. Das Frontend muss für Endgeräte aufrufbar sein. Der Erfolg soll durch ständiges Monitoring überprüft werden.

5.2.4.3 Services

Anforderung	Beschreibung
Onboarding/ Offboarding/ Data Management durchführen	Notwendige Support Services für die Entwickelten Funktionen und Prozesse sind zu etablierten. Dies bedeutet zum einen technischen Support (First- und Second-Level) aber auch Unterstützung, aber auch Störungsbehebung, Stammdatenmanagement und weitere Unterstützungsleistungen. Zu berücksichtigen ist eine Verwaltung der Tätigkeiten (Ticketing) sowie Priorisierungen und Eskalationen.

5.2.4.4 Recht & Regulatorik

Anforderung	Beschreibung
Ad hoc Beratung	Die Durchführung des Pilotprojekts wird Fragen aufwerfen, die ad hoc beantwortet werden müssen. Die Services im Bereich Support beim Betrieb des Pilotprojekts umfassen deswegen die rechtliche Prüfung und Beantwortung etwaiger während des Betriebs auftretender Rechtsfragen, abhängig von Umfang und Komplexität der Fragestellung jeweils etwa in Form einer schriftlichen Stellungnahme, eines Kurzgutachtens oder einer anderen geeigneten und angemessenen Kommunikationsform.

5.2.5 Evaluierung

5.2.5.1 Prozessdesign

Anforderung	Beschreibung
Soll-Ist Erhebung & Bewertung durchführen	Die Prozesse sind nach dem Testbetrieb im Hinblick auf die Umsetzung und die Zielerreichung des Planungsstadiums sowie die Erfolgsfaktoren des Projektes zu bewerten. Wesentliche Bewertungskriterien können Usability, Fit-for-Purpose, Security, Skalierbarkeit und Performance sein. Darüber hinaus ist ebenfalls die Zielerreichung des Plug & Play Ansatzes zu bewerten. Die Ergebnisse sind zu dokumentieren.
Feedback	Von den verschiedenen Projektstakeholdern ist Feedback zu Projektdurchführung, Zielerreichung und erwarteten Perspektiven einzuholen. Die Ergebnisse sind auszuwerten und zu dokumentieren.

5.2.5.2 Kosten-Nutzen Betrachtung

Anforderung	Beschreibung
kommerzielle Machbarkeit evaluieren & überarbeiten	Im Anschluss an Entwicklung und Betriebsphase ist die kommerzielle Machbarkeit zu evaluieren und ein Business Case auf Basis der Planung zu erstellen und nach Bewertung der Betriebsphase zu aktualisieren.
Volkswirtschaftliche Betrachtung	Auf Basis des Business Cases sollte eine volkswirtschaftliche Betrachtung der entwickelten Technologien und Prozesse sowie identifizierter Potenziale durchgeführt werden. Die Evaluierung sollte durch einen unabhängigen, nicht mit der Projekt-Implementierung eingebunden Dritten erfolgen.

5.2.5.3 Technische Architektur

Anforderung	Beschreibung
Externe Evaluierung begleiten	Um die externe Evaluierung zu ermöglichen und den Parteien (z.B. BSI, GWA, BNetzA) so einfach wie möglich zu gestalten, soll diese technisch unterstützt werden.
Erfüllung Architekturkonzepte evaluieren	Im Rahmen einer umfassenden technischen Überprüfung soll überprüft werden, ob sämtliche Architekturkonzepte korrekt und vollständig nach Plan umgesetzt wurden. Dazu zählen neben dem Domain Model das Daten- und Rollenmodell, das Identitäts- und Zugriffskonzept sowie das Interoperabilitätskonzept (Systemumgebungen, PKI, APIs). Abweichungen sind schriftlich festzuhalten.
Blockchain-Technologie Auswahl finalisieren (Empfehlung / Entscheidung)	Die Entscheidung, welches Blockchain Protokoll am besten für den Anwendungsfall geeignet ist, ist im Rahmen des Piloten zu treffen. Basierend auf den Erfahrungen, die während der Pilotphase gesammelt wurden, ist eine endgültige Empfehlung abzugeben. Dabei soll nicht nur der Typ der Blockchain berücksichtigt werden, sondern auch begründete Vorschläge unterbreitet werden, welchen Typ von Knoten von welchen Marktteilnehmern sinnvollerweise betrieben werden sollten. Die Empfehlungen sind schriftlich festzuhalten.
Sicherheitskonzept überprüfen	Die im Sicherheitskonzept festgelegten Mechanismen zur Überprüfung (z.B. Penetration Testing, Simulation des Ausfalls von Blockchain-Knoten) sind soweit auszuführen, sodass diese ein realistisches Bild zeichnen, aber nicht den laufenden Betrieb gefährden. Die Erkenntnisse über Schwachstellen im System sind den betreffenden Parteien mitzuteilen, die für die Entwicklung und den Betrieb jeweilige Komponenten zuständig sind. Jedenfalls sind nicht nachweislich beseitigte Sicherheitslücken schriftlich im Endbericht festzuhalten.
Kommunikationsinfrastruktur testen	Gegenstand der Evaluierung der Kommunikationsinfrastruktur sind die Zuverlässigkeit der WAN Verbindung (Tunnel) zwischen SMGW und MSB, die Kommunikation des SMGW mit dem CLI-Device, sowie der Blockchain Knoten untereinander. Weiters ist die Verbindung der einzelnen Softwarekomponenten untereinander zu überprüfen. Erkenntnisse sind im Endbericht festzuhalten.
Validierungstool testen	Um die technische und inhaltliche Funktion des Validierungstools zu testen, sind die zuvor definierten Szenarien für mögliche Dispute nachzuspielen. Dabei soll eruiert werden, ob das Tool eine sachgemäße Auditierbarkeit ermöglicht. Technische sowie fachliche Erkenntnisse sind im Endbericht festzuhalten.

Skalierbarkeit- / Performance evaluieren	Um die Möglichkeit der Ausweitung des Piloten auf den Produktivbetrieb zu evaluieren, sind die zuvor definierten Stresstests durchzuführen und anschließend auswerten. Dabei soll der laufende Betrieb nicht gefährdet werden. Das Ergebnis ist schriftlich festzuhalten.

5.2.5.4 Recht & Regulatorik

Anforderung	Beschreibung
Abschlussdokumentation erstellen	Die rechtliche Evaluierung umfasst die Überprüfung von Funktionalität und Vollständigkeit des Compliance- und Vertragskonzepts sowie der rechtlichen Hürden aus der Run-Phase. Das Ergebnis der juristischen Abschlussbewertung der Überprüfung, z.B. des rechtlichen Anpassungsbedarfs und Hinweise für eine rechtssichere Umsetzung, ist schriftlich zu dokumentieren.

5.2.5.5 Archivierung

Anforderung	Beschreibung
Abschlussdokumentation	Die erarbeiteten Ergebnisse müssen gesamtheitlich dokumentiert und dem Auftraggeber zur Verfügung gestellt werden.
Artifakte konservieren	Die im Projekt beschafften und erarbeiteten Artefakte (bspw. Hardware, Software, Laborausrüstung, Dokumente, Kommunikation) sind durch die Projektpartner in angemessener Weise zu konservieren.
Lessons Learned festhalten	Die gewonnenen organisatorischen, technischen und kaufmännischen Erkenntnisse sind angemessen zu dokumentieren und im Rahmen der Projektpartner sowie mit dem Auftraggeber zu teilen.
Löschung von Daten	Beim Rückbau der Pilotinfrastruktur und vor Beendigung des Projektes sind sämtliche personenbezogenen Daten DSGVO konform zu löschen.

5.3 Anhang C: Abbildungsverzeichnis

5.4 Anhang D: Tabellenverzeichnis

5.5 Anhang E: Glossar

Begriff / Abkürzung	Erläuterung
AP	Arbeitspaket
BMWi	Bundesministerium für Wirtschaft und Energie
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CLS	Controllable Local System
EEG	Erneuerbare Energien Gesetz
GWA	Gateway-Administrator
HAN	Home Area Network-S
MaStR	Marktstammdatenregister
MaStRV	Marktstammdatenregisterverordnung
MDMS	Meter Data Management System
MSB	Messstellenbetreiber
NB	Netzbetreiber
P2P	Peer zu Peer (aus dem englischen Peer to Peer), direkte Beziehung und Ausübung von Interaktion/Prozessabwicklung zweier (Vertrags-) Partner ohne den Einsatz eines Mittelsmanns/Intermediär
PKI	Public Key Infrastructure (aus dem Englischen) bezeichnet ein kryptografisches Verfahren mittels dessen digitale Zertifikate ausgestellt, verteilt und geprüft werden. Anhand dieser Zertifikate können die Teilnehmer der PKI eine „digitale Identität" verwenden und rechnergestützt die Authentizität, Unversehrtheit und Vertraulichkeit von Informationen herstellen oder verifizieren
PMO	Projektmanagement & Organisation
PV	Photovoltaik (-Anlage) zur Energieerzeugung
Smart Contract	Smart Contracts (dt. intelligente Verträge) sind digitale Verträge, die auf Computerprotokollen basieren und der Blockchain-Technologie aufbauen[16]
SMGW	Smart Meter Gateway
TAF	Tarifanwendungsfall: Anwendungsfälle für Tarifierung, Bilanzierung und Netzzustandsdatenerhebung
TOE	Target of Evaluation - im Rahmen der Zertifizierung und Anerkennung der SMGW Produkte der einzelnen Hersteller
TR	Technische Richtlinie
WAF	WAN-Anwendungsfall (SMGW)
WAN	Wide Area Network

[16] Vgl. hierzu https://blockchainwelt.de/smart-contracts-vertrag-blockchain/

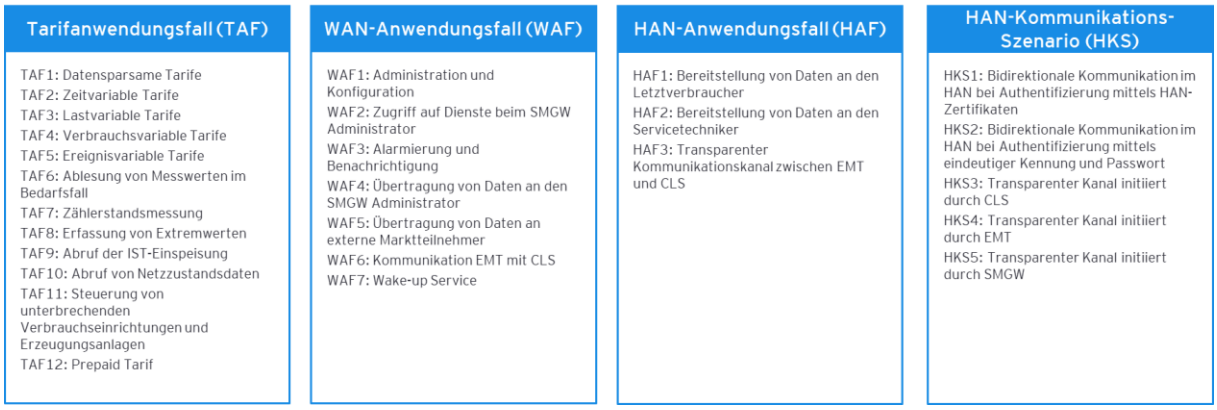


Abbildung 11: Glossar Kommunikationsszenarien