



B2E2

Blockchain Based
Energy Ecosystem

Whitepaper:

Energy Token Model

Energieherkunft und Peer-to-Peer Handel:

Möglichkeiten dezentraler Energiemärkte auf Blockchain-Basis und deren technische Umsetzung

Veröffentlicht durch EnBW Energie Baden-Württemberg AG

b2e2@enbw.com

Autoren: Magnus Gödde, Alexander Kaiser, Christian Sander, Volker Seith, Matthias Stumpp, Klaus Winter

Version 1.0, 30.05.2020

LIZENZ

Das Whitepaper unterliegt der Creative Commons Public Licence: Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 International (CC – BY SA 4.0). Die Lizenzbedingungen sind diesem Whitepaper beigelegt.



Wir räumen Ihnen die im Rahmen der Lizenzbedingungen beschriebenen Rechte ein.

Bitte beachten Sie hierbei insbesondere die Bestimmungen zur Namensnennung und zum Haftungsausschluss.

Sofern die in den Lizenzbestimmungen genannten Voraussetzungen von Ihnen beachtet und eingehalten werden, können Sie dieses Whitepaper entsprechend ganz oder in Teilen vervielfältigen und weitergeben und abgewandeltes Material erstellen, vervielfältigen und weitergeben.

Gerne stehen wir Ihnen bei Fragen zur Nutzung dieses Whitepapers unter den eingeräumten Lizenzbedingungen zur Verfügung.

Inhalt

1	Motivation.....	5
2	Blockchain in der Energiewirtschaft	6
3	Beispiele für die Anwendung der Blockchain in der Energiewirtschaft.....	7
3.1	Erzeugungs-Share.....	7
3.2	Verbrauchs-Share	7
3.3	Absolute Bezugsrechte	7
3.4	Nachweis von Eigenschaften	7
3.5	Weitergabe von Energie	7
4	Anforderungen an eine auf Blockchain basierende Lösungsarchitektur	8
5	Authority-Modell	9
5.1	Market-Authority	9
5.2	Operative Authorities.....	10
5.2.1	Physical-Asset-Authority	10
5.2.2	Metering-Authority	11
5.2.3	Balance-Authority.....	11
5.2.4	Aufgaben aller operativen Authorities.....	11
6	Abbildung auf der Blockchain.....	11
6.1	Identitäten	11
6.2	Energie	13
6.3	Regeln des Energiemarktes	14
6.4	Verträge zwischen Marktteilnehmern.....	14
6.5	Teilnehmerkonzepte.....	15
6.5.1	Energiemarktteilnehmer als ungebundene BC- Teilnehmer.....	15
6.5.2	Dienstleister als Produkthanbieter für Endkunden (Trustee-Ansatz).....	15
7	Layer-Konzept der Umsetzung.....	15
8	Implementierung via Identity Contracts, Claims und Energy Token	18
8.1	Ethereum's Proof of Authority Protokoll.....	18
8.2	Abbildung von energiewirtschaftlichen Identitäten.....	19
8.3	Abbildung von Energie in Form von Token	22
9	Implementierung des Marktsetups	27
10	Implementierung eines „Absolute Forwards“ Szenario	33
10.1	Handel	33
10.2	Nachweis.....	34
10.3	Verteilung und Abrechnung	37
11	Implementierung eines „Generation-based Forwards“-Szenario	38
11.1	Handel.....	38
11.2	Nachweis.....	39
11.3	Verteilung und Abrechnung	40

12	Implementierung eines „Consumption-based Forwards“-Szenario.....	41
12.1	Handel.....	41
12.2	Nachweis.....	41
12.3	Verteilung und Abrechnung	43
13	Begriffserklärungen.....	45
14	Tabellen Verzeichnis	46
15	Abbildungsverzeichnis	46
16	Creative Commons Public Licence CC – BY SA 4.0	47

1 Motivation

Seit mehreren Jahren setzen wir uns bei EnBW mit dem Einsatz der Blockchain-Technologie in der Energiewirtschaft auseinander. Anlass dazu war das Versprechen der Technologie, Transaktionen zwischen beliebigen Partnern vertrauenswürdig zu dokumentieren, ohne dazu einen neutralen Dritten als Intermediär zu benötigen. Vereint mit der damit verbundenen Transparenz und der Möglichkeit, reale Werte über sogenannte Tokens in die Blockchain abzubilden, lag es nahe zu untersuchen, welche Möglichkeiten damit in der Energiewirtschaft entstehen und ob die Technologie hält, was sie verspricht.

Auf diesem Weg haben wir verschiedene Anwendungsfälle prototypisch umgesetzt und so praktische Erfahrungen gesammelt, um die technischen Möglichkeiten zu bewerten. So konnten wir u. a. in einem Proof of Concept den Nachweis der Qualität von Biogas auf der Strecke von Biogasanlage bis hin zum Blockheizkraftwerk mit Einsatz der Blockchain abbilden. Im Kontext der Elektromobilität realisierten wir in einem Prototyp die Interaktion von Fahrzeug und Ladesäule über Smart Contracts. In einem anderen Anwendungsfall führten wir den bilanziellen Nachweis von Strom aus einer dedizierten Erzeugungsanlage mit Hilfe von Tokens durch. Zudem standen wir im Austausch mit Universitäten, Industrieunternehmen und Startups und haben u. a. auch im Rahmen der Dena Multi Stakeholder Studie „Blockchain in der integrierten Energiewende“ an der Ausarbeitung von 11 Blockchain basierenden Anwendungsfällen mitgewirkt.

Aus den Erkenntnissen dieser und weiterer Anwendungsfälle haben wir das in diesem Whitepaper dargestellte Energiewirtschaftliche Tokenmodell entwickelt, in dem beschrieben wird, wie die Blockchain in der Energiewirtschaft eingesetzt werden kann. Dabei haben wir neben der technischen Machbarkeit auch auf die Anschlussfähigkeit an den bestehenden Energiemarkt geachtet.

Das Whitepaper stellt damit die Sicht der Autoren auf den aktuellen Stand der Technik dar und erhebt keinen Anspruch auf Vollständigkeit. So sind z. B. Fragestellungen, wie die Anwendbarkeit im geltenden regulatorischen Rahmen im Kontext konkreter Anwendungsfälle zu betrachten. Mit der Veröffentlichung dieses Whitepapers wollen wir einen Beitrag zur öffentlichen Diskussion der Einsatzmöglichkeiten der Blockchain in der Energiewirtschaft leisten. Wir erhoffen uns weitere Impulse aus der Diskussion des Whitepapers und freuen uns auf Feedback.

b2e2@enbw.com

2 Blockchain in der Energiewirtschaft

Blockchains und Distributed Ledger Technologien (DLT) sind in der Lage, hinsichtlich definierter Aktivitäten direkt und ohne Vermittler (Intermediär) Vertrauen zwischen Beteiligten zu schaffen, die sich in der Regel nicht kennen.

Auf dieser Basis entstehen Wirtschaftssysteme, in denen Menschen ohne zentrale Registrierung bei einem Plattformbetreiber den Austausch digitaler oder digitalisierter Güter durchführen können. Das Vertrauen auf die Korrektheit dieser Tauschverfahren übertragen die Teilnehmer den sogenannten Konsensmechanismen, bei denen letztlich die Gemeinschaft der Beteiligten die korrekte Ausführung von öffentlich implementierten Algorithmen überwacht. Dadurch können leistungsfähige Peer-to-Peer-Märkte (P2P) entstehen.

Wurde bis vor Kurzem die Blockchain als grundsätzliche Lösung und als Allheilmittel für alle möglichen Fragestellungen diskutiert, zeigt die aktuelle Ernüchterung, dass ein sinnvoller Einsatz nur für wirklich geeignete Anwendungsfälle angedacht werden sollte.

In der Energiewirtschaft ist der Einsatz der Blockchain sinnvoll, da

- › das zu tauschende Gut (Strom/Gas) sehr gut digitalisierbar ist (elektronische Zähler)
- › das zu tauschende Gut über ein vorhandenes Netz ausgetauscht wird, an dem jeder einen Anschluss hat und damit die Auslieferung des Gutes möglich ist
- › sie einen dezentralen Energiemarkt ermöglicht, auf dem Verbraucher und Erzeuger netzgebundene Energie und die zugehörigen Eigenschaften handeln können
- › auf Grund der Dezentralisierung der Energieerzeugung als Folge der Energiewende immer mehr Energiegemeinschaften entstehen, die die Energieverteilung unter den Teilnehmern vertrauensvoll organisieren müssen
- › sie ermöglicht, dass Verbraucher über Eigenschaften ihrer Energie selbst entscheiden können und diese verbürgt bekommen
- › sie eine einheitliche technische Basis und weiteres Potenzial zur Erhöhung des Standardisierungsgrades (z. B. durch Smart-Contracts) im Gesamtsystem mit sich bringt
- › sie die Möglichkeit zu selbst-souveränem Handeln bietet
- › sie perspektivisch eine praktikable Möglichkeit zur Abrechnung des zu tauschenden Gutes zur Verfügung stellt
- › sie einen weitgehend offenen und diskriminierungsfreien Zugang eröffnen kann
- › im regulierten bzw. stark reglementierten Teil der Energiewirtschaft per Definition Lösungsansätze für das „Oracle-Problem“ in Blockchain-Anwendungen existieren.

Tabelle 1: Vorteile des Blockchain Einsatz in der Energiewirtschaft

3 Beispiele für die Anwendung der Blockchain in der Energiewirtschaft

Neben dem Handel von Energiemengen, liegen weitere Anwendungsbeispiele im Nachweis von Eigenschaften wie Herkunft und Art der Erzeugung oder sogar in der Weitergabe bereits erworbener Energie ohne Intermediär.

In den Beispielen wird davon ausgegangen, dass sich Liefervereinbarungen auf einen Bilanzzeitraum beziehen und vor dem Bilanzzeitraum der Lieferung abgeschlossen werden. Pro Bilanzzeitraum werden die vereinbarten und später gelieferten Energiemengen saldiert und die Bilanz gebildet. Für die entstehende Über- oder Unterdeckung liegt die Verantwortung je nach Beispiel bei Erzeuger oder Verbraucher. Im deutschen Energiemarkt haben Bilanzzeiträume eine Länge von 15 min und orientieren sich am Stundenraster.

3.1 Erzeugungs-Share

Bei einem Erzeugungs-Share erwirbt der Verbraucher einen relativen Anteil an der Erzeugung einer Anlage. So kann ein Verbraucher beispielsweise 2 % an der Erzeugung einer größeren PV-Anlage erwerben. Das Risiko einer Über- oder Unterdeckung liegt hier auf der Verbraucherseite.

3.2 Verbrauchs-Share

Bei einem Verbrauchs-Share wird definiert, wieviel Prozent des Verbrauchs eines Verbrauchers durch einen Erzeuger abgedeckt werden. Die heute klassische Versorgung von Endkunden durch Energielieferanten entspricht einem Verbrauchs-Share von 100 % (Vollversorgung). Das Risiko einer Unterdeckung des Verbrauchers liegt hier auf der Erzeugerseite.

3.3 Absolute Bezugsrechte

Bei absoluten Bezugsrechte wird eine feste Energiemenge zur Übergabe zwischen Erzeuger und Verbraucher vereinbart. Dabei ist der Erzeuger in der Verantwortung, die vereinbarte Energie tatsächlich bereitzustellen. Der Verbraucher ist in der Pflicht, die vereinbarte Energiemenge dem Netz zu entnehmen.

3.4 Nachweis von Eigenschaften

Der Verbraucher erhält einen Nachweis darüber, dass Energie in einem bestimmten Bilanzzeitraum von einer bestimmten Erzeugungsanlage "für ihn" erzeugt wurde. Der Nachweis kann zusätzlich Eigenschaften dieser Erzeugungsanlage wie bspw. Art der Erzeugung (Sonne, Wind, Wasser) oder Ort der Anlage beinhalten.

3.5 Weitergabe von Energie

Ein wesentlicher Vorteil der Blockchain-Technologie ist es, dass sie Verfahren bereitstellt, mit denen die Eigentümerschaft von digitalen oder digitalisierten Gütern klar definiert ist und dass es ausschließlich in der Hand des Eigentümers liegt, diese Güter an einen anderen Eigentümer zu übertragen, sofern der neue Eigentümer dem zustimmt¹. Das bedeutet auf den Energiemarkt übertragen, dass die Teilnehmer digitale Güter ohne Vermittler untereinander übertragen können. Insbesondere die Weitergabe von Bezugsmengen durch den

¹ Die Zustimmung ist erforderlich, da der Preis der Energie im Bilanzzeitraum negativ sein kann.

Verbraucher bei Erzeugungs-Share und absoluten Energiemengen-Produkten, aber auch der Tausch von Energiemengen mit bestimmten Eigenschaften sind mögliche Szenarien.

4 Anforderungen an eine auf Blockchain basierende Lösungsarchitektur

Für einen Marktteilnehmer ist es wesentlich, Sicherheit über die Existenz und die Eigenschaften einer Erzeugungs- oder Verbrauchsanlage zu haben, für die er mit einem unbekanntem Partner ein Geschäft abschließt. Dazu genügt es nicht, auf die Vertrauen-erzeugenden Eigenschaften einer Blockchain zu verweisen, da sich diese auf die Transaktionen, nicht aber auf die initiale Existenz eines Gutes oder einer Eigenschaft beziehen. Wenn also Lisa an Moritz 10 kWh überträgt, dann ist die Transaktion jederzeit in der Blockchain nachvollziehbar. Woher weiß Moritz aber, dass Lisa überhaupt 10 kWh besitzt und weitergeben kann? Ziel muss also sein, die reale Situation so in die Blockchain zu überführen, dass keine Risiken hinsichtlich des Wahrheitsgehaltes der Aussagen bzgl. Existenz und Eigenschaften bestehen (Oracle Problem).

Um die beschriebenen Anforderungen zu erfüllen, arbeiten wir mit einem Authority-Modell, das einen Weg aufzeigt, wie Objekte aus der realen Welt (in diesem Fall Erzeugungs- und Verbrauchsanlagen mit ihren digitalen Eigenschaften und ihre gemessenen Erzeugungs- bzw. Verbrauchswerte) vertrauensvoll in digitaler Form auf eine Blockchain abgebildet werden können.

Gleichzeitig verfolgt das Authority-Modell das Ziel, den Souveränitätsanspruch des Marktteilnehmers zu berücksichtigen. Das bedeutet, dass er seine Identität auf der Blockchain frei bestimmen kann, indem er nach einem kryptographischen Verfahren Public-Private-Key-Paare generiert und verwendet.

Das bedeutet, dass Erzeugungs- oder Verbrauchsanlagen durch ihre Nutzer mit Identitäten auf der Blockchain versehen werden. Jede Anlage kann beliebig viele Identitäten besitzen, wobei in einem Bilanzzeitraum jede Anlage nur mit einer Identität verwendet werden darf. Durch diese Pseudonymisierung kann der Blockchain-Nutzer die zeitliche Nachvollziehbarkeit seines Verhaltens selbst steuern.

Die Existenz der Anlage hinter einer Identität und ihre Eigenschaften sowie die notwendige Einbindung in den Markt wird durch vertrauenswürdige Authorities bestätigt.

Durch das Authority-Modell sollte sichergestellt werden, dass

- (1) die Person, die für eine Energie-Anlage im Energiemarkt geschäftliche Aussagen tätigt, dies auch darf, weil sie z.B. als Besitzer bekannt ist
- (2) eine Energie-Erzeugungsanlage oder eine Energie-Verbrauchsanlage eines Energiemarkt-Teilnehmers tatsächlich existiert und an das öffentliche Netz angeschlossen ist
- (3) die Eigenschaften der Energieanlagen denen entsprechen, die in den Blockchain-Verträgen der Energiemarkt-Teilnehmer Verwendung finden
 - a. Erzeugungsart wie PV, Wind, Biomasse
 - b. Lokation der Anlage
 - c. Maximale Leistung der Anlage
- (4) die Messwerte, die von den Energie-Anlagen der Energiemarkt-Teilnehmer erhoben werden und für die Abwicklung der Blockchain-Verträge notwendig sind, auf der Blockchain bereitgestellt werden
- (5) die Anlage eines Energiemarkt-Teilnehmers gegen Abweichungen der Energiebilanz abgesichert ist; d.h. es existiert nachweislich ein Mechanismus, um fehlende oder überschüssige Energie auszugleichen
- (6) für eine real existierende Energie-Anlage ein Double-Spending in einem anderen Energiemarkt nicht oder nur transparent durchgeführt werden kann (z.B. in anderen Blockchains oder mit anderen Vermarktungsmechanismen wie z.B. Direktvermarktung)

Tabelle 2: Anforderungen an das Authority-Modell

Die Eintrittsschwelle für Nutzer ist somit gering. Sie besitzen die volle Souveränität über ihre verwendeten Identitäten. Informationen zu diesen Identitäten (z. B. Eigenschaften der Anlage) sind valide und nur durch den Eigentümer dieser Identität publizierbar. Geschäfte sind immer von beiden Seiten zu bestätigen.

5 Authority-Modell

Im Authority-Modell wird davon ausgegangen, dass über anerkannte Marktteilnehmer die Identitätsüberprüfung durchgeführt werden kann. Die Aufgaben des Energiemarktes sind durch Marktrollen abgedeckt und können aktuell auch nur über diese bedient werden. Diese Marktrollen werden daher in den Blockchain-Ansatz integriert, was bedeutet, dass Rolleninhaber als Authority mit einer eigenen Identität auf der Blockchain agieren. Auch für die Authorities wird der Souveränitätsanspruch berücksichtigt.

5.1 Market-Authority

Das Authority-Modell lebt von gemeinsamen Regeln, die in einem Markt gelten. Dieser Markt und seine Regeln werden durch eine Market-Authority definiert und bereitgestellt.

Die Market-Authority stellt sicher, dass alle Aktivitäten der Blockchain hinsichtlich der Bilanzzeiträume kompatibel sind und dass alle Blockchain-Teilnehmer, die sich als Inhaber einer definierten Marktrolle ausgeben, diese Marktrolle auch tatsächlich innehaben.

Durch diesen Ansatz wird es möglich, unterschiedliche Märkte aufzubauen. Ein Markt könnte definiert werden durch eine Energie-Gemeinschaft, welche die Blockchain als Abwicklungsplattform für die Aktivitäten ihrer Mitglieder nutzt oder einen Energiedienstleister, der seinen Kunden innerhalb der Kundengemeinschaft große Freiräume schaffen möchte. Es sind aber auch umfassende Märkte vorstellbar, in denen Verbände oder staatliche Organisationen die Aufgabe einer Market-Authority übernehmen. Im Folgenden wird der deutsche Energiemarkt mit den bekannten Marktrollen als Beispiel verwendet, um das Funktionsprinzip des Authority-Modells zu erläutern.

Die Market-Authority legt ein Zeitraster fest, in dem alle Aktivitäten stattfinden. Im heutigen Energiemarkt sind dies die Viertelstunde-Werte, auf denen nahezu alle Prozesse (Bilanzierung, Zählwerterfassung, Börsenpreise, ...) aufbauen. Dadurch ist sichergestellt, dass Handelsgeschäfte, aber auch z. B. Aussagen zu Anlagenexistenz und Zählwerte zueinander kompatibel sind.

Der Market-Authority sind – außerhalb der Blockchain – alle Inhaber von Marktrollen (z. B. MSB, Lieferant, VNB) bekannt. Ihr ist auch bekannt, mit welchen Blockchain-Identitäten der jeweilige Inhaber agiert. Dadurch ist sie in der Lage zu bestätigen, dass ein Marktteilnehmer eine bestimmte Marktrolle innehat und alle Aktivitäten dieser Marktrolle ausführen darf.

5.2 Operative Authorities

Die operativen Authorities ermöglichen einem Marktteilnehmer (Verbraucher und Erzeuger), auf der Blockchain zu agieren (Abbildung 1). Sie haben außerhalb der Blockchain einen klassischen Marktvertrag (z. B. als VNB, MSB, Lieferant/BKV) mit ihren Kunden und sind dadurch in der Lage,

- bestimmte Aussagen auf der Blockchain zu validieren („Ich habe eine Verbrauchsstelle“, „Ich habe eine Erzeugungsanlage“),
- zu treffen („Der Verbrauch der Anlage, die mit dem P2P-Teilnehmer xy verknüpft ist, war von 9:00 bis 9:15 am 3.5.2019 0,34 kWh)
- oder dem Energiemarkt zu garantieren, dass die Handelsaktivitäten des Marktteilnehmers physikalisch abgesichert sind („Die Energiemengen-Bilanz der Anlage, die mit dem P2P-Teilnehmer xy verknüpft ist, wird durch mich sichergestellt.“).

Dass eine operative Authority zugelassen ist, muss durch eine entsprechende Aussage der Market-Authority auf der Blockchain hinterlegt sein.

5.2.1 Physical-Asset-Authority

Die Physical-Asset-Authority kann bestätigen, dass ein Energiesystem tatsächlich existiert und am öffentlichen Netz angeschlossen ist. Nur dadurch ist gewährleistet, dass ein Handel mit Energie auch eine physikalische Entsprechung hat. Sie kann ebenfalls die Eigenschaften der Anlage (Verbraucher oder Erzeuger; Region, Art der Erzeugung usw.) validieren.

Im Energiemarkt könnte das die Marktrolle Verteilnetzbetreiber durchführen. Diese Authority nimmt die Aufgaben (2) und (3) wahr (vgl. Tabelle 2).

Für alle Authorities gilt zudem, dass

- (7) es überprüfbar ist, dass sich alle Aktivitäten der verschiedenen operativen Authorities (VNB, MSB, BKV) die sich auf dieselbe Energie-Anlage (in Deutschland die Marktlokation) eines Marktteilnehmers beziehen sollen, dies auch tun. Sie sind in der Lage, die reale Identität einer Energie-Anlage (Marktlokation) für die Blockchain zu verschlüsseln, um die Bestimmbarkeit von Personen zu vermeiden
- (8) eine real existierende Energie-Anlage eines Marktteilnehmers in der Blockchain zu einem Zeitpunkt nur einmal referenziert wird. Konkret bedeutet dies, dass einer realen Anlage (z. B. Marktlokation) in einem Bilanzzeitraum nur eine digitale Blockchain-Identität zugeordnet sein darf
- (9) Authorities in der Lage sind, mit der souveränen Identität der Marktteilnehmer umzugehen (sie erfüllen die dargestellten Aufgaben ausschließlich auf den selbst gewählten Identitäten der Marktteilnehmer)

Tabelle 3: Anforderungen an das Authority-Modell

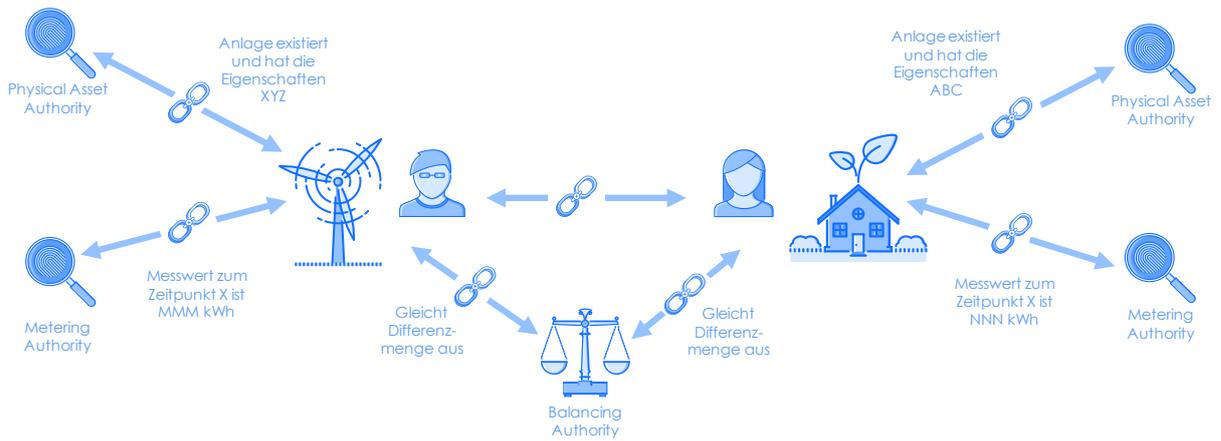


Abbildung 1: Operative Authorities bringen die Wahrheit in die Blockchain

5.2.2 Metering-Authority

Die Metering-Authority stellt sicher, dass die Zählwerte bzw. der Lastgang einer Anlage, die in der Blockchain abgelegt sind, auch vertrauenswürdig sind.

Im Energiemarkt könnte das die Markttrolle Messstellenbetreiber durchführen. Diese Authority nimmt die Aufgabe (4) wahr (vgl. Tabelle 2).

5.2.3 Balance-Authority

Die Balancing-Authority integriert den Marktteilnehmer in ihren Bilanzkreis und regelt den Netzzugang. Sie gleicht Differenzmengen für Marktteilnehmer als Verbraucher oder Erzeuger aus.

Sie hat mit dem Marktteilnehmer einen Stromliefervertrag (Verbrauch) oder einen Einspeisevertrag (Erzeugung), d. h. sie kennt die reale Identität ihres Kunden und seiner Anlage (die durch die Physical-Asset-Authority in ihrer Existenz bestätigt wurde).

Im Energiemarkt könnte das die Markttrolle Lieferant und Bilanzkreisverantwortlicher durchführen. Diese Authority nimmt die Aufgaben (5) und (6) wahr (vgl. Tabelle 2).

5.2.4 Aufgaben aller operativen Authorities

Für alle operativen Authorities gilt, dass sie sicherstellen müssen, dass nur der Verantwortliche für eine Anlage (Nutzer oder Eigentümer eines Netzzugangs) Vertragsaussagen für diese Anlage auf der Blockchain treffen darf (vgl. (1) Tabelle 2).

Da es sich um drei operative Authority-Rollen handelt, die gemeinsam alle Identitätsfragestellungen einer Anlage klären, müssen die Anforderungen (7)-[9] von allen operativen Authorities in einem definierten Verfahren erfüllt werden (vgl. Tabelle 3).

6 Abbildung auf der Blockchain

Die Umsetzung unterscheidet die Abbildung von Identitäten, Energie, Regeln des Energiemarktes und Verträgen zwischen Marktteilnehmern:

6.1 Identitäten

Identity-Contracts werden von den Marktteilnehmern und den Authorities genutzt, um ihre Identität bzw. die von Energieanlagen, die am Markt teilnehmen sollen, auf die Blockchain abzubilden. Um die Identitätsmechanismen in einem Markt anzuwenden, werden die Identity-Contracts mittels einer, von der Market-Authority bereitgestellten Contract-Facotory durch die Teilnehmer erstellt. Dabei kann das Selbstbestimmungsrecht über die eigene pseudonymisierte Identität für alle Teilnehmer gewahrt werden.

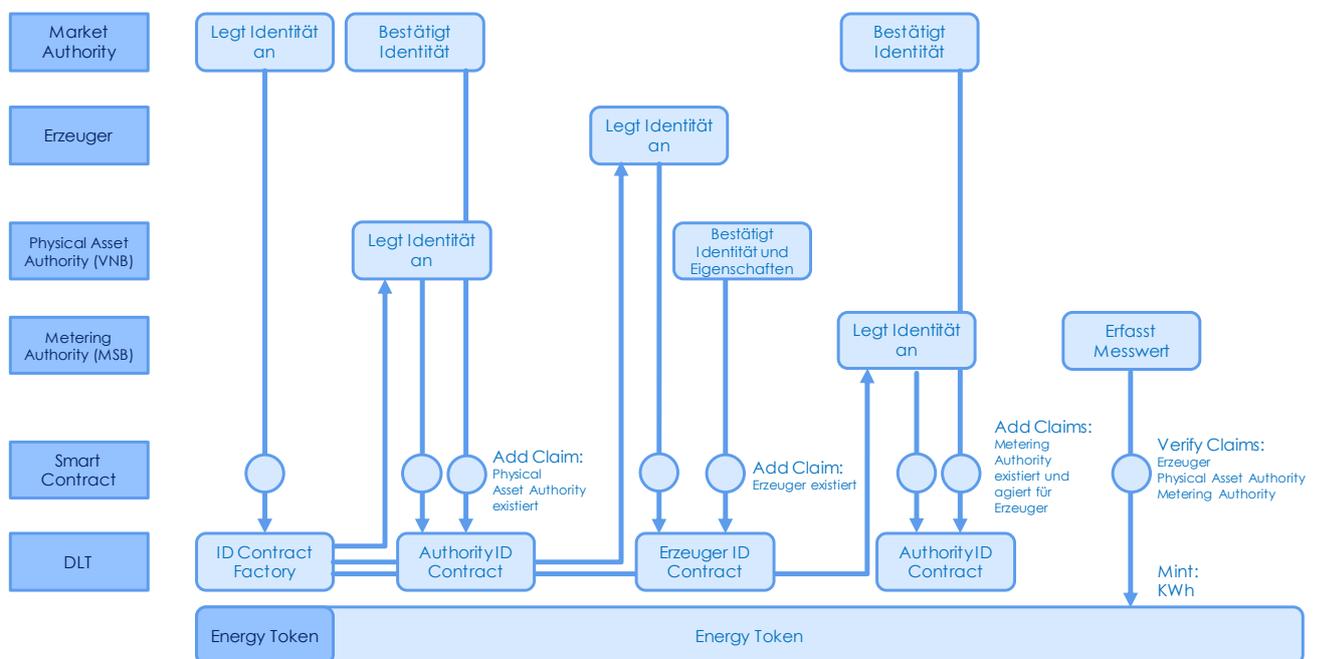


Abbildung 2: Beispiel für die Entstehung von Identitäten

Während der Identity-Contract dazu dient, die digitale Identität zu erzeugen, werden die relevanten Real-Welt-Aussagen zu dieser Identität (z.B. dass diese Anlage existiert und über welche Eigenschaften diese verfügt) durch sogenannte Claims sichergestellt.

Claims werden dabei von den Authorities ausgestellt, die operativ in der Lage sind, eine inhaltlich korrekte und vertrauenswürdige Aussage über ein Objekt der realen Welt zu treffen. Der Claim selbst wird von der Authority an den Marktteilnehmer übergeben und kann von diesem mit seinem Identity-Contract verbunden werden. Claims werden dabei von den Authorities ausgestellt, die operativ in der Lage sind, eine inhaltlich korrekte und vertrauenswürdige Aussage über ein Objekt der realen Welt zu treffen.

Um eine Aussage für ein Objekt treffen zu können, müssen Authorities in der Lage sein, die vom Teilnehmer vorgegebene digitale Identität z. B. einer Anlage mit der realen Identität verknüpfen zu können. Dazu benötigen sie einen sicheren Kommunikationskanal mit dem Marktteilnehmer, über den sie dessen digitale Identität empfangen und den Claim überreichen können. Dieser Kommunikationskanal ist eine übliche verschlüsselte Verbindung, wie sie bereits heute die meisten Energieversorger für ihre Kunden anbieten (z. B. Account mit Identifikation und Authentifizierung).

Die benötigten Aussagen über die reale Welt sind in mehrere Claims aufgeteilt, weil unterschiedliche Rollen im Markt jeweils Aussagen zu anderen Sachverhalten tätigen können und weil es dem Teilnehmer ermöglicht werden soll, seine Daten selbstbestimmt offenzulegen. Ein

Beispiel: Möchte ein Energieerzeuger Photovoltaik-Strom von seiner konkreten Anlage verkaufen, so muss er offenlegen, dass seine Anlage Photovoltaik-Strom erzeugt und durch genaue Geokoordinaten auffindbar ist. Möchte er nur Strom ohne Eigenschaften der Erzeugung anbieten, so genügt es, dass er die Existenz seiner Anlage offenlegt.

6.2 Energie

Im Energiemarkt ist es notwendig, Erzeugung und Verbrauch im Gleichgewicht zu halten. Ohne dieses Gleichgewicht kann ein stabiles Netz nicht gewährleistet werden. Aus diesem Grund werden Erzeugung und Verbrauch durch Bilanzkreisverantwortliche geplant und müssen sich bereits in der Planung im Gleichgewicht befinden.

Der tatsächliche Verbrauch bzw. die Erzeugung und damit die Bilanz wiederum kann erst mit einer Messung im Anschluss an die physikalische Belieferung ermittelt werden.

Entsprechend der fachlichen Notwendigkeit wird Energie in zwei Formen abgebildet. Zum einen als Angabe, wieviel Energie man verbrauchen bzw. erzeugen wird. Zum anderen als Energie, die nachgewiesenermaßen tatsächlich erzeugt oder verbraucht wurde:

Bezugsrechte- und Pflichten („Bestellung“)

Kauft ein Verbraucher eine Energiemenge bei einem Erzeuger ein, so entsteht er aus der Sicht des Verbrauchers Bezugsrechte aber, bilanziell relevant, natürlich auch Abnahmepflichten. Aus Sicht des Erzeugers besteht eine Belieferungspflicht oder – je nach bilanzieller Situation – ein Abgaberecht.

Nachweis der Lieferung („Lieferung/Abnahme“)

Mit der Messung an einer Erzeugungsanlage oder Verbrauchsstelle entsteht der Nachweis, welche Energiemengen tatsächlich erzeugt bzw. verbraucht wurden.

Tabelle 4: Zwei Formen zur Abbildung von Energie

Energie wird über Energie-Tokens auf der Blockchain repräsentiert. Diese sind genau einer Anlage und einem Bilanzzeitraum sowie einem Eigentümer zugeordnet und können zwischen Eigentümern auf der Blockchain nach geltenden Marktregeln ausgetauscht werden. Zum einen wird zwischen Energie-Token unterschieden, die Bezugsrechte, Abnahmepflichten und Belieferungspflichten auf die Blockchain abbilden. Sie werden als „Forwards“ bezeichnet. Diese unterscheiden sich wiederum je nach Anwendung in absolute Energiemengen-Token und relative Energiemengen-Token, welche sich wiederum dadurch unterscheiden, ob sie sich auf die Erzeugung oder den Verbrauch beziehen.

Auf der anderen Seite stehen den Forwards die „Certificates“ gegenüber. Sie implementieren den Nachweis einer Lieferung bzw. einer Abnahme von Energie (Messung).

Die Forwards werden von Erzeugungsanlagen bereitgestellt und können dann entsprechend gehandelt werden. Mit Erzeugung und Abgabe von Forwards entsteht für den Erzeuger eine Belieferungspflicht und für den Verbraucher eine Abnahmepflicht.

Die Certificates werden von der Metering-Authority jeweils bezogen auf die Anlagen-Identität gemintet (generiert). Die Certificates implementieren den Nachweis der Eigenschaften über die Herkunft.

Die Eigenschaften einer Anlage (Art der Erzeugung, Lokation, ...) können aus den Claims herausgelesen werden, die über die Anlagen-Identität und den Bilanzzeitraum referenziert werden können.

6.3 Regeln des Energiemarktes

Teile der Marktregeln werden in „Contract-Factories“ abgelegt. Dabei handelt es sich um Implementierungen von Smart-Contracts - also konkreten Code - die von den einzelnen Marktteilnehmern auf der Blockchain instanziiert werden müssen. So wird von der Market Authority eine Contract-Factory bereitgestellt, mit Hilfe derer die operativen Authorities und den Marktteilnehmer Identity Contracts „deployen“ können (Abbildung 2).

Die Implementierung der Energy-Token wird ebenfalls von der Market-Authority bereitgestellt. Weiterhin kann sie Regeln beschreiben, die nicht auf der Blockchain implementiert werden können (z. B. die Generierung von eindeutigen pseudonymisierten Identifikatoren von Real-Welt-Objekten wie die Ableitung von Identifikatoren aus Marktlokationen). Die Dokumente zur Beschreibung können mit freiem Zugriff abgelegt und zur Sicherstellung der Unveränderbarkeit der entsprechende Hash auf der Blockchain hinterlegt werden.

Damit sind alle Marktregeln auf der Blockchain hinterlegt, entweder als Implementierung oder als Dokumentationsverweis.

6.4 Verträge zwischen Marktteilnehmern

Die Implementierung der in Kapitel 3 genannten Anwendungsbeispiele unterscheidet sich vor allem in dem Verteilmechanismus der Certificates (vgl. Tabelle 5), also der Frage, wann ein Token gemintet wird bzw. wann und wie er verteilt wird.

Forwards

Forwards werden grundsätzlich von den Erzeugern erzeugt und bereitgestellt. Wie viele Token der Erzeuger minted und welche Eigenschaften von den Token repräsentiert werden, obliegt ausschließlich dem Erzeuger im Rahmen der Vereinbarungen mit der Balance-Authority (die aus Risikomanagement-Gründen Limiten aussprechen kann), den Eigenschaften der Anlage (maximale Erzeugungsleistung) und den bereitgestellten Claims. Die Forwards werden vom Erzeuger an den Verbraucher auf der Blockchain übertragen.

Certificates

Die Erzeugung der Certificates erfolgt durch die Metering-Authority, weil die Certificates auf den Zählwerten basieren. Der Verteilungsmechanismus von Certificates an die Bezieher von Energie hängt vom Anwendungsfall ab. Ein wesentliches Kriterium ist, ob die zu verteilenden Certificate-Token bereits vor (absolute Energiemengen-Token) oder erst nach (relative Energiemengen-Token) der Messung feststehen. Ein weiterer Aspekt des Verteilmechanismus liegt in der Unterscheidung, ob die relevante Messung zur Verteilung der relativen Certificate-Tokens beim Erzeuger oder beim Verbraucher stattfindet.

Tabelle 5: Forwards & Certificates

Dementsprechend werden auf der Blockchain drei Verteilungsalgorithmen (Absolute, GenerationBased, ConsumptionBased) implementiert. Eine Balance-Authority kann durch einen Claim definieren, welche Token-Distribution sie unterstützt.

6.5 Teilnehmerkonzepte

6.5.1 Energiemarktteilnehmer als ungebundene BC- Teilnehmer

Ein üblicher Blockchain-Ansatz ist es, dass die Teilnehmer mit einer sehr geringen Eintrittsschwelle und autark hinsichtlich ihrer digitalen Identität agieren können. Hierzu werden Authorities benötigt, die nicht auf die Energiehandels- und -Tausch-Aktivitäten ihrer Kunden Einfluss nehmen, und Vertrauen generieren, wo die Blockchain-Technologie dies nicht gewährleisten kann.

6.5.2 Dienstleister als Produktanbieter für Endkunden (Trustee-Ansatz)

Alternativ ist es auch möglich, klassische Intermediär-Geschäftsmodelle abzubilden. Hier übernimmt ein Dienstleister alle Aktivitäten - einschließlich der Identitätsgenerierung - für die Marktteilnehmer. Im Zusammenspiel mit der Möglichkeit, einen eigenen Energiemarkt zu generieren, kann die Blockchain hier als alternative Plattform zu konventioneller Technologie genutzt werden.

7 Layer-Konzept der Umsetzung

Um Komponenten und Technologien zu separieren und dadurch Entwicklungsgeschwindigkeit und Austauschbarkeit zu erhöhen, wird die Architektur in drei Layer gegliedert (Abbildung 3).

Unterschieden wird dabei zwischen dem Distributed-Ledger-Layer zur Abbildung des Blockchain-Protokolls, dem Smart-Contract-Layer zur Bearbeitung der fachlichen Fragestellungen auf der Blockchain und eines Layer, das den Zugang auf das Smart-Contract-Layer für unterschiedliche externe Sichten vereinfacht.

Das in diesem Artikel beschriebene Funktionsprinzip beschreibt Inhalte des Smart-Contract-Layers. Das Layer ist nach Überzeugung der Autoren offen für alle, um eine möglichst große Basis an Teilnehmern zur Generierung innovativer Produkte für den Energiemarkt zu erreichen.

Neben der Evaluierung des Smart-Contract-Layers im Rahmen dieser Anwendungsfälle arbeitet das EnBWTeam auch an Lösungen, den Zugang so einfach wie möglich zu gestalten. Hierzu wurde u. a. ein Application Interface (API) entwickelt, das es ermöglicht, bestehende Systemwelten schnell an das Smart-Contract-Layer anzubinden.

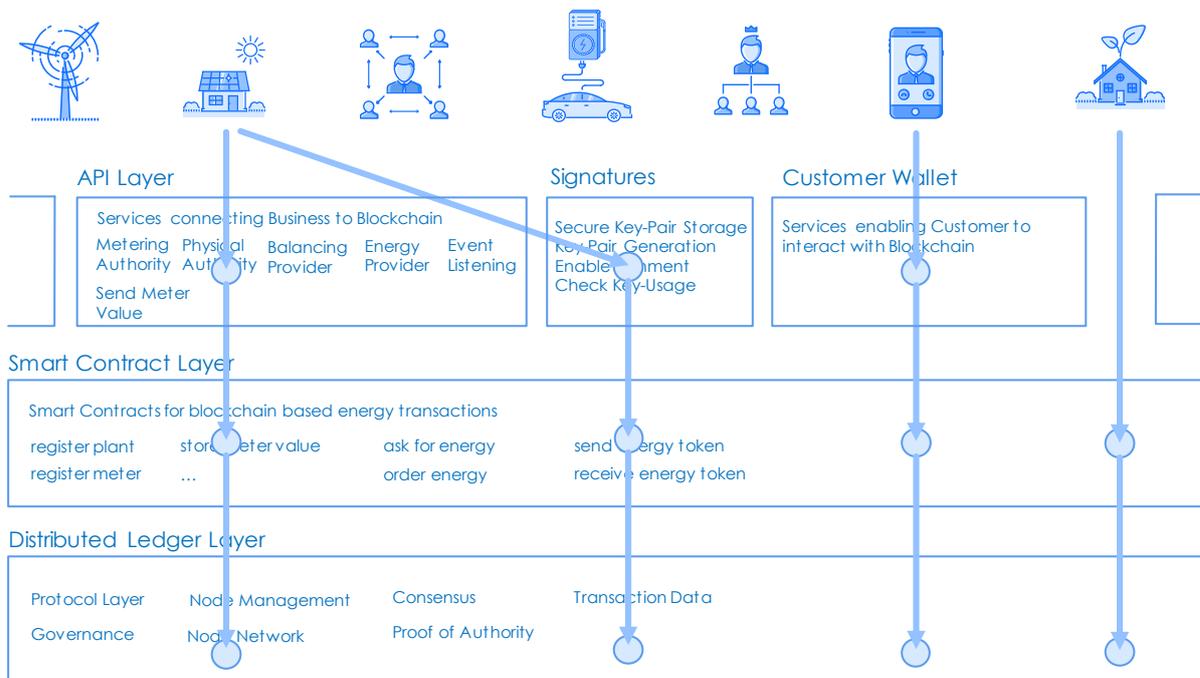


Abbildung 3: Schema der 3-Layer-Architektur

Wir hoffen, mit dem Artikel Denkanstöße geben zu können, wie die Blockchain in der Energiewirtschaft Anwendung finden kann. Auch in den kommenden Schritten bleibt die Auseinandersetzung mit dem Thema weiter spannend. Von kurz getakteten technologischen Entwicklungen bis hin zu regulatorischen Aspekten, die die Anwendung betreffen, bestehen noch zahlreiche Fragestellungen, mit denen es sich auseinanderzusetzen gilt.

Unterschieden wird dabei zwischen dem Distributed-Ledger-Layer zur Abbildung des Blockchain-Protokolls, dem Smart-Contract-Layer zur Bearbeitung der fachlichen Fragestellungen auf der Blockchain und einer Layer-Ebene zur Generierung von unterschiedlichen externen Sichten auf die Blockchain-Implementierung.

Die in diesem Papier skizzierte Lösung beschreibt in erster Linie die Implementierung auf der Ebene des Smart Contract Layers. Er ist als Open Source-Lösung entworfen, um eine möglichst große Basis an Teilnehmern zur Generierung innovativer Produkte für den Energiemarkt zu erreichen.

Neben der Open Source-Ebene der Smart Contracts liegt mit dem Blockchain Based Energy Ecosystem (B2E2) eine Plattform vor, die alle Fähigkeiten bereitstellt, um Teilnehmer den einfachen Zugang zu den Blockchain-Konstrukten des Energiemarktes zu ermöglichen. Insbesondere wendet sie sich an alle Unternehmen, die im Energiemarkt

- › als Authority ihre Kunden den Zugang zur Energie-Blockchain ermöglichen möchten
- › als professionelle Energielieferanten als P2P-Partner in einem freien Energiemarkt auftreten möchten
- › als Dienstleister den Energie-Blockchain-Teilnehmern komfortable und innovative Zugänge zu den Energie-Blockchain-Produkten bereitstellen möchten.

Ziel von B2E2 ist es, dass Unternehmen ihre meist vorhandenen Plattformen mit der Blockchain-Technologie verbinden können, ohne selbst intensives Blockchain-Know-How aufbauen

zu müssen. Um dies zu ermöglichen setzen wir uns im Kontext des API Layer u.a. mit folgenden Fragestellungen auseinander:

- > Anbindung an bestehende IT Systeme
- > Automatisierte Einstellung der Authority-Aussagen auf die Blockchain
- > Verwaltung von Marktteilnehmern für die Market-Authority
- > Durchführung von Blockchain-Aktivitäten als Treuhänder für Kunden (Customer Trustee)
- > Abgreifen relevanter Events von der Blockchain
- > Verwaltung der Public- und Private-Keys

8 Implementierung via Identity Contracts, Claims und Energy Token

Die folgenden Kapitel richten sich in erster Linie an Entwickler mit Erfahrung im Bereich des Ethereum Protokolls. Vorausgesetzt wird insbesondere das Verständnis der Funktionsweise des ERC 1155 Multi Token Standards², des ERC 725 Proxy Account Standards³ und des ERC 735 Claim Holder Standards⁴.

Die Entscheidung für die ERC 725 und 735 Standards sowie die Ausgestaltung der Repräsentation von Identitäten insgesamt sind wesentlich von den Kernzielen der W3C Decentralized Identifiers (DIDs)⁵ (insbesondere: Dezentralisierung und Selbstbestimmung) sowie den Kernkonzepten des W3C Verifiable Credentials Data Model⁶ (insbesondere: Claims) beeinflusst, weshalb eine Auseinandersetzung mit diesen Konzepten ebenso ratsam ist.

8.1 Ethereum's Proof of Authority Protokoll

Wir verwenden das Ethereum Protokoll wegen der Popularität und der Möglichkeit touring-vollständige Smart Contracts einzusetzen. Mit Smart Contracts können Erzeugungs- und Verbrauchsanlagen und ihre Eigenschaften auf der Blockchain repräsentiert werden. Die Popularität geht einher mit einem großen Ökosystem von Entwickler-Werkzeugen und anderen Applikationen. Das Ökosystem ist insbesondere wichtig, weil das Vertrauen der Nutzer nur gewonnen werden kann, wenn Sachverhalte auf der Blockchain mittels einer Vielzahl von einfach bedienbaren Applikationen "eigenständig" überprüft werden können.⁷

Des Weiteren besitzt Ethereum nach Bitcoin die zweithöchste Marktkapitalisierung⁸, was ein Indiz dafür ist, dass sich das Protokoll hinsichtlich Nutzbarkeit und Sicherheit bewährt hat. Für die Nutzbarkeit spricht ebenfalls die Tatsache, dass das Ethereum Protokoll die meisten Blockchain Entwickler besitzt.⁹ Zudem nutzt die Energy Web Foundation als eines der größten energiewirtschaftlichen Blockchain Konsortien ein Proof of Authority Ethereum Protokoll.¹⁰

Wir empfehlen den Einsatz eines Proof of Authority Konsens-Mechanismus, da hierbei nicht mit Rechenleistung über die Verarbeitung und chronologische Reihenfolge der Transaktionen abgestimmt wird, sondern durch anerkannte Validierer ("Authorities"). Im Vergleich zu einem offenen Proof of Work Protokoll wird folglich weniger Hardware und Energie benötigt. Zudem schafft ein Proof of Work Protokoll in der Energiewirtschaft gegenüber einem geschlossenen Proof of Authority Protokoll keinen Mehrwert an Vertrauen. Da in der Energiewirtschaft sowieso verschiedenen Authorities vertraut werden muss, erscheint es als sinnvoll auch einem Set an Authorities bei der Konsensfindung des Protokolls Vertrauen zu schenken.

Das Proof of Authority Protokoll sollte von möglichst vielen am System teilnehmenden Akteuren gemeinschaftlich betrieben werden.¹¹ Zudem müssen Anreize zur Kartellbildung ausgeschlossen sein, so dass die Anzahl der Angriffsvektoren und die Wahrscheinlichkeit für erfolgreiche Angriffe minimiert werden.

² Quelle: <https://github.com/ethereum/EIPs/issues/1155>

³ Quelle: <https://github.com/ethereum/EIPs/issues/725>

⁴ Quelle: <https://github.com/ethereum/EIPs/issues/735>

⁵ Quelle: <https://www.w3.org/TR/did-core/#design-goals>

⁶ Quelle: <https://www.w3.org/TR/vc-data-model/#claims>

⁷ Quelle: <https://github.com/ethereum/EIPs/issues/1155>

⁸ Quelle: <https://coinmarketcap.com/>

⁹ Quelle: <https://consensys.net/blog/blockchain-development/ethereum-has-4x-more-developers-than-any-other-crypto-ecosystem/>

¹⁰ Quelle: <https://www.energyweb.org>, "EWF is the world's largest energy blockchain ecosystem"

¹¹ Im besten Fall sollte auch der Staat zum Schutz kritischer Infrastrukturen am Konsensmechanismus teilnehmen.

8.2 Abbildung von energiewirtschaftlichen Identitäten

Um einen dezentralen Markt für Energie und ihre Eigenschaften zu realisieren, gilt es im ersten Schritt, energiewirtschaftliche Akteure auf einer Ethereum Blockchain zu authentifizieren, so dass sie Verbrauchs- und Erzeugungsanlagen und ihre Eigenschaften wahrheitsgemäß mit Ethereum Accounts verknüpfen können.

Energiewirtschaftliche Akteure werden durch sogenannte "Identity Contracts" auf der Blockchain repräsentiert. Die Identity Contracts implementieren den ERC 725 "Proxy Account", ERC 735 "Claim Holder" Standard und den ERC1155TokenReceiver Standard (Abbildung 4). Die Methoden des ERC 725 Standards werden genutzt, um beliebige Methoden von Smart Contracts aufrufen und somit insbesondere Energie und ihre Eigenschaften in Form von Token handeln zu können. Die "Claim" Funktionalität des ERC 735 Standards wird zur Authentifizierung und Autorisierung der energiewirtschaftlichen Akteure genutzt. Die Methoden des ERC1155TokenReceiver Standards werden für die Einwilligung von ERC1155 Token Transfers benötigt.

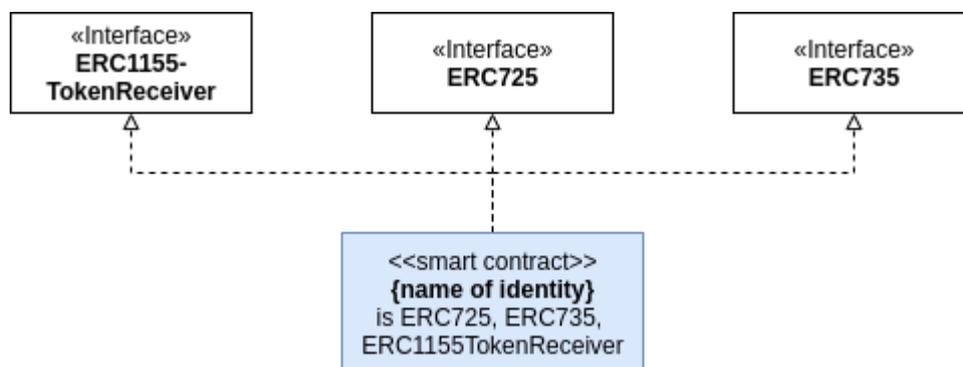


Abbildung 4: Identity Contract

Identity Contracts können von den energiewirtschaftlichen Akteuren durch eine Identity Contract Factory erstellt werden (Abbildung 5).^{12,13} Die Identity Contract Factory wird von der Market Authority erstellt. Der Zweck der Identity Contract Factory besteht darin, Komfort zu bieten. Identity Contracts können jedoch auch ohne die Identity Contract Factory erstellt werden.

¹² Zur grundlegenden Funktionsweise eines Factory Contracts: <https://medium.com/@i6mi6/solidty-smart-contracts-design-patterns-ecfa3b1e9784>

¹³ Beim ER-Model wurde die Martin-Notation für die Darstellung der Kardinalitäten verwendet und die Chen-Notation zur Beschreibung der Beziehungen: https://en.wikipedia.org/wiki/Entity%E2%80%93relationship_model

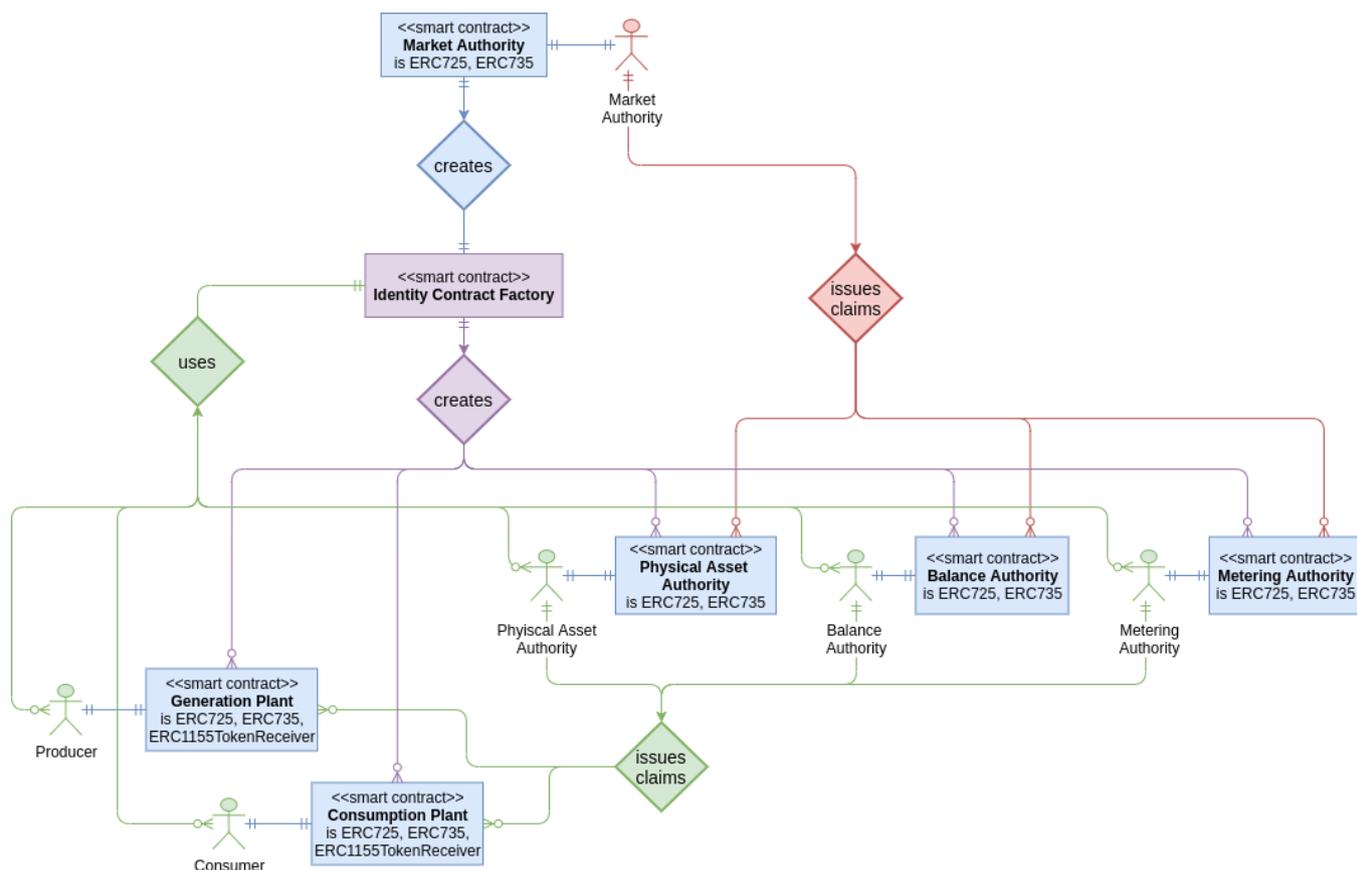


Abbildung 5: ER-Modell: Identity Contracts

Die Claims des ERC 735 Standards werden zwecks informationeller Selbstbestimmung zuerst an die Personen geschickt und anschließend von den Personen eigenständig ihren Identity Contracts hinzugefügt. Ein Claim besteht im Wesentlichen aus einer digital signierten Behauptung des "Issuers", dessen Adresse um selbige zu überprüfen sowie das verwendete Signaturschema. Die folgende Tabelle beinhaltet eine Übersicht aller Claims (Tabelle 6).

Claim Bezeichnung	"Issuer"	"Holder"	Zweck
"Is Balance Authority Claim"	Market Authority	Balance Authority	Market Authority authentifiziert und autorisiert den Identity Contract der Balance Authority.
"Is Metering Authority Claim"	Market Authority	Metering Authority	Market Authority authentifiziert und autorisiert den Identity Contract der Metering Authority.
"Is Physical Asset Authority Claim"	Market Authority	Physical Asset Authority	Market Authority authentifiziert und autorisiert den Identity Contract der Physical Asset Authority.
"Metering Claim"	Metering Authority	Consumption Plant, Generation Plant	Metering Authority bestätigt, dass sie die Messwerte der Anlage dem Blockchain Protokoll bereitstellt.

Claim Bezeichnung	"Issuer"	"Holder"	Zweck
"Balance Claim"	Balance Authority	Consumption Plant, Generation Plant	Balance Authority bestätigt, dass sie die Anlage in einem registrierten Bilanzkreis aufnimmt und bilanziell energetische Fehlmengen ausgleicht.
"Existence Claim"	Physical Asset Authority	Consumption Plant, Generation Plant	Physical Asset Authority bestätigt, dass die Anlage existiert und an das öffentliche Netz angeschlossen ist.
"Generation Type Claim"	Physical Asset Authority	Consumption Plant, Generation Plant	Physical Asset Authority bestätigt die Eigenschaften der Anlage (z.B. Verbraucher oder Erzeuger, Region, Art der Erzeugung).
"Location Claim"	Physical Asset Authority	Consumption Plant, Generation Plant	Physical Asset Authority bestätigt den Standort der Anlage.
"Identity Contract Factory Claim"	Market Authority	Market Authority	Market Authority veröffentlicht die Adresse der Identity Contract Factory.
"Energy Token Contract Claim"	Market Authority	Market Authority	Market Authority veröffentlicht die Adresse des Energy Token Contracts.
"Market Rules Claim"	Market Authority	Market Authority	Market Authority veröffentlicht den Teil der Regeln des Marktes, der nicht durch Smart Contracts festgelegt und durchgesetzt wird.
"Accepted Distributor Contracts Claim"	Balance Authority	Distributor	Balance Authority bestätigt, dass der entsprechende Distributor Contract von ihren "Balance Claim" Holder Kunden verwenden darf.

Tabelle 6: Claim Übersicht

Claims lassen sich zentral in Form von einem Claim Register Contract (Beispiel: ERC 1812¹⁴) oder dezentral in Form von Identity Contracts (Beispiel: ERC 735) ausgestalten. Wir haben uns für den dezentralen Ansatz entschieden, weil Claims somit direkt mit den Accounts verknüpft sind und über selbige ausgelesen werden können. Im Fall von einem zentralen Claim Register müsste zusätzlich die Adresse des Claim Register Contracts für die Überprüfung der Claims übermittelt werden.

Die Implementierung des Identity Contracts folgt den ERC 725, 735 und ERC1155TokenReceiver Standards. Im Folgenden werden zusätzliche Funktionen des Identity Contracts beschrieben, welche nicht durch die ERC Standards spezifiziert sind.

¹⁴ Quelle: <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1812.md>

constructor (IdentityContract marketAuthority, uint32 balancePeriodLength)	
Beschreibung	Die Methode ist ein Konstruktor und erstellt einen Identity Contract.
Aufrufer	Ethereum Accounts von den energiewirtschaftlichen Akteuren.
Aufrufparameter	IdentityContract marketAuthority: Beim Hinzufügen von den in diesem Dokument spezifizierten Claims wird überprüft, ob diese Claims entweder von der marketAuthority signiert wurden oder von einer Authority signiert wurden, welche als Authority von der marketAuthority durch einen entsprechenden Claim bestätigt wurde.
	uint32 balancePeriodLength: Länge vom Bilanzzeitraum, gemessen in Sekunden. Die Bilanzzeiträume fangen zu den Zeitpunkten 00:00:01 + i* balancePeriodLength an (mit i als Element der ganzen Zahlen). Sowohl der Energy Token Contract als auch der Distributor Contract liest diese Variable vom Identity Contract der Market Authority aus.

Tabelle 7: Konstruktor Identity Contract

8.3 Abbildung von Energie in Form von Token

Nachdem wir im ersten Schritt energiewirtschaftliche Identitäten auf die Blockchain abgebildet haben, gilt es im zweiten Schritt, Energie und ihre Eigenschaften in Form von handelbaren Token auf die Blockchain abzubilden.

Die Energie Token werden durch den Energy Token Contract auf die Blockchain abgebildet. Der Energy Token implementiert den ERC 1155 "Multi Token" Standard (Abbildung 6).¹⁵ Für jeden Bilanzzeitraum und für jede Erzeugungsanlage existieren unterschiedliche Token Arten. Die Anzahl der Token Arten ist folglich hoch. Der ERC 1155 "Multi Token" Standard wird verwendet um diese hohe Anzahl von Token Arten in einem Smart Contract zentral verwalten zu können. Im Vergleich zur Verwendung des ERC 20 Token Standards muss nur ein Contract erstellt und verwaltet werden. Das ist weniger komplex, erfordert einen geringeren Speicherbedarf und ist hinsichtlich Transaktionskosten günstiger.

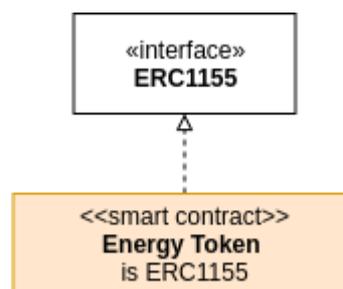


Abbildung 6: Energy Token Contract

Die unterschiedlichen Energie Token können in drei Dimensionen unterteilt werden (Abbildung 7: Systematische Unterteilung der Energie Token).

Die Dimension "Family" unterteilt die Energie Token zeitlich. Die Familie der Forwards bezieht sich auf zukünftige Energieflüsse, wohingegen die Familie der Certificates sich auf zu beweisende vergangene Energieflüsse bezieht.

Die Dimension "Genus" (im Deutschen "Gattung") unterteilt Energie Token zweckmäßig. Absolute Forwards werden gekauft, um eine absolute Energiemenge von einer

¹⁵ Quelle: <https://github.com/ethereum/EIPs/issues/1155>

Erzeugungsanlage zukünftig bilanziell beziehen zu können. Generation-based Forwards werden gekauft um einen relativen Anteil der Energiemenge von einer Erzeugungsanlage zukünftig bilanziell beziehen zu können. Consumption-based Forwards werden gekauft, um einen relativen Anteil des eigenen Verbrauchs von einer Erzeugungsanlage zukünftig bilanziell beziehen zu können.

Die Dimension "Species" (im Deutschen "Art") unterteilt Energie Token anlagen- und bilanzzeitraum-spezifisch. Jede Token Art besteht aus einer Menge von Token, welche sich alle auf denselben Bilanzzeitraum und dieselbe Erzeugungsanlage beziehen.

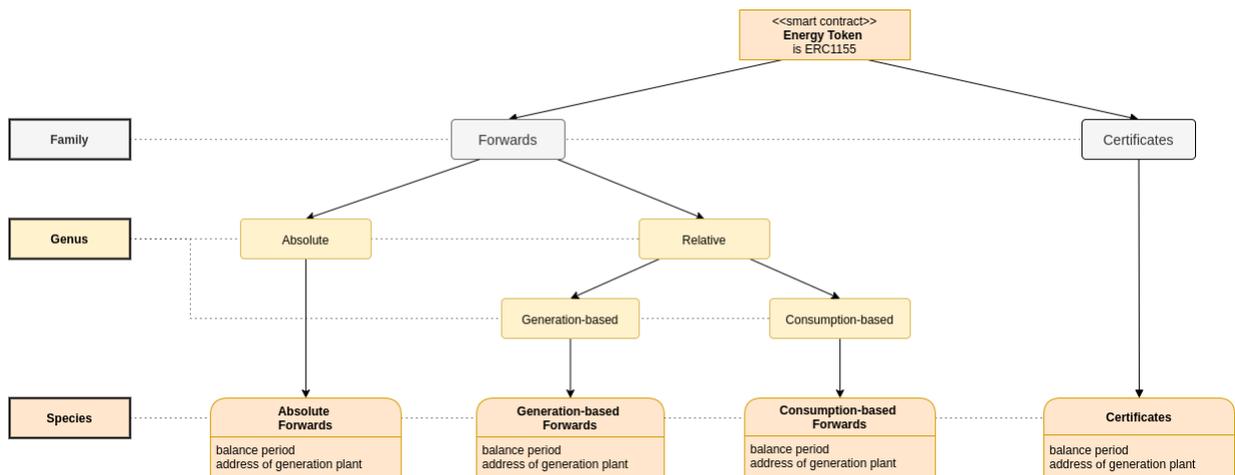


Abbildung 7: Systematische Unterteilung der Energie Token

Der Energy Token Contract wird von der Market Authority erstellt und bildet alle Token Arten ab (Abbildung 8: ER-Modell: Energy Token). Alle Token Arten werden sowohl von den Erzeugern als auch von den Verbrauchern gehandelt. Der Distributor Contract verteilt auf Basis der Forwards Token Kontostände die Certificates an die Besitzer der Forwards. Der Verteilungsmechanismus ist abhängig von der Forwards Gattung. Ein Verbraucher mit bspw. 30E18 Absolute Forwards hat eine Forderung in Höhe von 30 kWh gegenüber einer bestimmten Erzeugungsanlage für einen bestimmten Bilanzzeitraum. Ein Verbraucher mit bspw. 1E14 Relative Generation-based Forwards hat eine Forderung in Höhe von 0,0001% der erzeugten Energie gegenüber einer bestimmten Solar- oder Windkraft-Erzeugungsanlage für einen bestimmten Bilanzzeitraum. Ein Verbraucher mit bspw. 100E18 Relative Consumption-based Forwards hat eine Forderung in Höhe von 100% seiner verbrauchten Energie gegenüber einer bestimmten Erzeugungsanlage für einen bestimmten Bilanzzeitraum (entspricht einer bedingten Vollversorgung).¹⁶

¹⁶ Generation-based Forwards dürfen ausschließlich von Windkraftanlagen oder Solaranlagen Besitzern erstellt werden, deren Energieerzeugung nicht steuerbar ist.

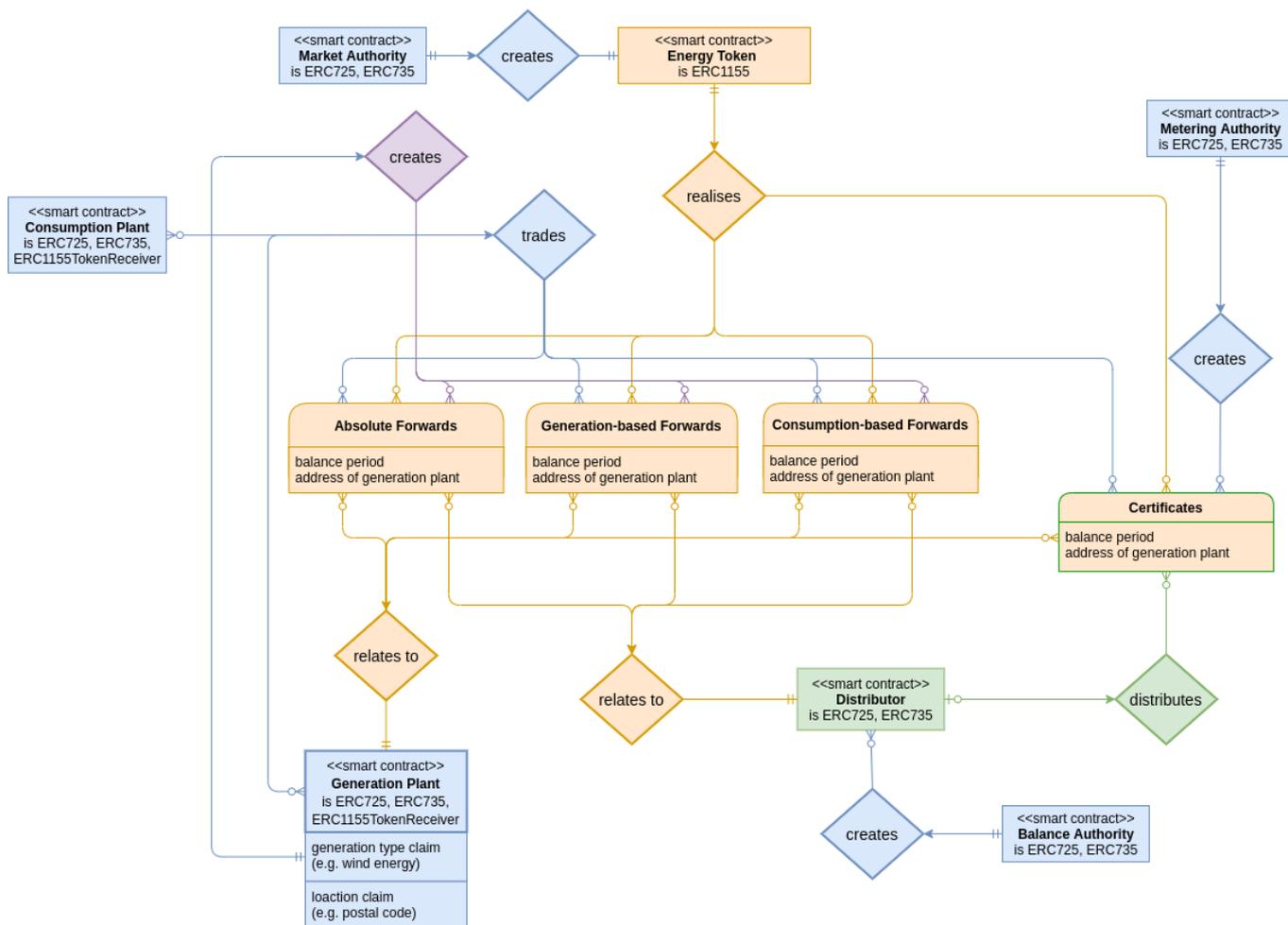


Abbildung 8: ER-Modell: Energy Token

Die Implementierung des Energy Token Contract folgt dem ERC 1155 Multi Token Standard. Im Folgenden werden zusätzliche Funktionen des Energy Token Contract beschrieben, welche nicht durch den ERC 1155 Multi Token Standard spezifiziert sind.

Der Energy Token beinhaltet folgende zwei Methoden zur Token-Erstellung.

createForwards (uint64 balancePeriod, TokenKind tokenKind, address distributor) onlyGenerationPlants returns(uint256 tokenID)	
Beschreibung	Die Methode erstellt eine bilanzzeitraum-spezifische Forward-Art. Dieser Forwards Art wird ein Distributor Contract zugeordnet. Im Fall der generation-based Forwards wird zusätzlich eine konstante Menge von 100E18 Token (\Leftrightarrow 100% der zukünftig erzeugten Energie) für die Erzeugungsanlage des aufrufenden Identity Contracts erstellt.
Aufrufer	Identity Contracts von Erzeugungsanlagen, welche mit allen notwendigen Claims verknüpft sind.
Aufrufparameter	uint64 balancePeriod: Beginn vom Bilanzzeitraum, gemessen in Unixzeit. Die Bilanzzeiträume fangen zu den Zeitpunkten 00:00:01 + i*balancePeriodLength an (mit i als Element der ganzen Zahlen).
	TokenKind tokenKind: Spezifiziert die Gattung der Forwards Art.
	address distributor: Adresse des Distributor Contracts, welcher auf Basis der Forwards die Certificates nach dem Energiefluss verteilt.
Rückgabeparameter	uint256 tokenID: Eindeutige Kennung der Forwards Art.

Tabelle 8: Methode „createForwards“

mint (uint256 tokenID, address[] to, uint256[] quantities) returns(uint256 tokenID)	
Beschreibung	Die Methode schöpft eine oder mehrere Mengen von Token einer bestimmten Token Art für eine oder mehrere Adressen. Generation-based Forwards können mit dieser Methode nicht geschöpft werden.
Aufrufer	Die Ersteller der Token Art.
Aufrufparameter	uint256 tokenID: Eindeutige Kennung der Token Art, von welcher Token geschöpft werden.
	address[] to: Empfänger Adressen der zu schöpfenden Token.
	uint256[] quantities: Mengen der für die Empfänger Adressen zu schöpfenden Token (1 kWh \Leftrightarrow value = 1E18).
Rückgabeparameter	uint256 tokenID: Eindeutige Kennung der Token Art, von welcher Token geschöpft wurden.

Tabelle 9: Methode „mint“

Die folgenden zwei Funktionen sind Teil des Identity Contracts und werden im Zuge des Token-Transfers für einen 2-Wege-Handschlag vom Energy Token genutzt. Empfänger von Energy Token müssen im Zuge des 2-Wege-Handschlags dem Empfang von Energy Token zustimmen, sofern der Sender weder eine Metering Authority noch ein DistributorContract ist. Der Token-Empfänger ruft dabei im ersten Schritt in seinem Identity Contract die „approveSender“ oder „approveBatchSender“ Methode auf, um einen oder mehrere Token Sender(n) die Erlaubnis zu geben, ihm eine bestimmte Anzahl von Token oder weniger zu senden. Anschließend transferiert der Token Sender im zweiten Schritt die Token zum Empfänger durch Aufruf der „safeTransferFrom“ oder „safeBatchTransferFrom“ Methode im Energy Token Contract.

Energy Token der Forwards Familie berechtigen und verpflichten den Tokenbesitzer, Energie zu beziehen. Die Pflicht begründet den 2-Wege-Handschlag zwischen Sender und Empfänger beim Transfer von Forwards. Certificates können, abhängig von dem was nachgewiesen wird, einen positiven oder negativen Nutzen für den Token Besitzer aufweisen. Der potentiell negative Nutzen begründet den 2-Wege-Handschlag beim Transfer von Certificates.

approveSender (address sender, uint64 expiryDate, uint256 value, uint256 tokenID) onlyOwner returns(bool success)	
Beschreibung	Ein Empfänger erlaubt es einem Token Sender, ihm eine bestimmte Anzahl an Token einer bestimmten Art zuzuschicken. Diese Erlaubnis ist befristet.
Aufrufer	Alle Accounts.
Aufrufparameter	address sender: Adresse des Token Sender, welcher die Erlaubnis zum Zusenden von Token bekommen soll.
	uint64 expiryDate: Frist der Erlaubnis, gemessen in Unixzeit.
	uint256 value: Anzahl der Token, welche der Token Sender zusenden darf (1 Token entspricht 1E-18 kWh).
	uint256 tokenID: Kennung der Token Art, welche der Token Sender zusenden darf.
Rückgabeparameter	bool success: Das Argument ist „true“, wenn die Methode erfolgreich ausgeführt wurde.

Tabelle 10: Methode "approveSender"

approveBatchSender (address sender, uint64 expiryDate, uint256[] values, uint256[] tokenIDs) onlyOwner	
Beschreibung	Analog zur Methode "approveSender" mit dem Unterschied, dass der Empfänger mit <u>einem</u> Methoden-Aufruf es dem Empfänger erlauben kann, ihm mehrere unterschiedliche Mengen unterschiedlicher Token Arten zu senden.
Aufrufer	Alle Accounts.
Aufrufparameter	address sender: Adresse des Token Sender, welcher die Erlaubnis zum Zusenden von Token bekommen soll.
	uint64 expiryDate: Frist der Erlaubnis, gemessen in Unixzeit.
	uint256[] values: Anzahl der Token, welche der Token Sender zusenden darf (1 Token entspricht 1E-18 kWh).
	uint256[] tokenIDs: Kennung der Token Art, welche der Token Sender zusenden darf.

Tabelle 11: Methode "approveBatchSender"

Der Energy Token erweitert den ERC 1155 Standard um zwei Methoden zur Dokumentation von Energie-Messwerten. Die Messwerte des Energie-Verbrauchs werden vom Consumption-based Distributor Contract benötigt. Die Messwerte des Energie-Verbrauchs und der Energie-Erzeugung werden vom jeweiligen Balancer für die Abrechnung gebraucht.

addMeasuredEnergyConsumption (address plant, uint256 value, uint64 balancePeriod, bool corrected) onlyMeteringAuthorities() onlyGenerationPlants() returns(bool success)	
Beschreibung	Dokumentiert für eine Verbrauchsanlage die Energiemenge für einen bestimmten Bilanzzeitraum.
Aufrufer	Identity Contracts von Metering Authorities, welche mit allen notwendigen Claims verknüpft sind.
Aufrufparameter	address plant: Adresse des Identity Contracts der Verbrauchsanlage.
	uint256 value: Verbrauchte Energiemenge (1 kWh \leftrightarrow value = 1E18).
	uint64 balancePeriod: Beginn vom Bilanzzeitraum, gemessen in Unixzeit. Die Bilanzzeiträume fangen zu den Zeitpunkten 00:00:01 + i*balancePeriodLength an (mit i als Element der ganzen Zahlen).
	bool corrected: Falls das Argument "true" ist, werden die ursprünglich hinzugefügten Messwerte um die korrigierten Messwerte erweitert.
Rückgabeparameter	bool success: Das Argument ist "true", wenn die Methode erfolgreich ausgeführt wurde.

Tabelle 12: Methode "addMeasuredEnergyConsumption"

addMeasuredEnergyGeneration (address plant, uint256 value, uint64 balancePeriod, bool corrected) onlyMeteringAuthorities() onlyGenerationPlants() returns(bool success)	
Beschreibung	Analog zur Methode "addMeasuredEnergyConsumption". Dokumentiert für eine Erzeugungsanlage die Energiemenge für einen bestimmten Bilanzzeitraum.
Aufrufer	Identity Contracts von Metering Authorities, welche mit allen notwendigen Claims verknüpft sind.
Aufrufparameter	address plant: Adresse des Identity Contracts der Verbrauchsanlage.
	uint256 value: Verbraachte Energiemenge (1 kWh \leftrightarrow value = 1E18).
	uint64 balancePeriod: Beginn vom Bilanzzeitraum, gemessen in Unixzeit. Die Bilanzzeiträume fangen zu den Zeitpunkten 00:00:01 + i*balancePeriodLength an (mit i als Element der ganzen Zahlen).
	bool corrected: Falls das Argument "true" ist, werden die ursprünglich hinzugefügten Messwerte um die korrigierten Messwerte erweitert.
Rückgabeparameter	bool success: Das Argument ist "true", wenn die Methode erfolgreich ausgeführt wurde.

Tabelle 13: Methode "addMeasuredEnergyGeneration"

9 Implementierung des Marktsetups

In den Kapiteln 10ff wird die beispielhafte Verwendung der drei verschiedenen Token Gattungen ("Absolute Forwards", "Generation-based Forwards" und "Consumption-based Forwards") in Form von Sequenzdiagrammen beschrieben. Hierzu ist es jeweils erforderlich, im Vorfeld ein Set von Smart Contracts, welche den Rahmen für die energiewirtschaftlichen Anwendungsfälle bilden, zu deployen. Im Folgendem wird dieser Initialisierungsschritt als "Marktsetup" bezeichnet. In diesem Kapitel wird dargestellt, wie ein Marktsetup durchgeführt werden kann.

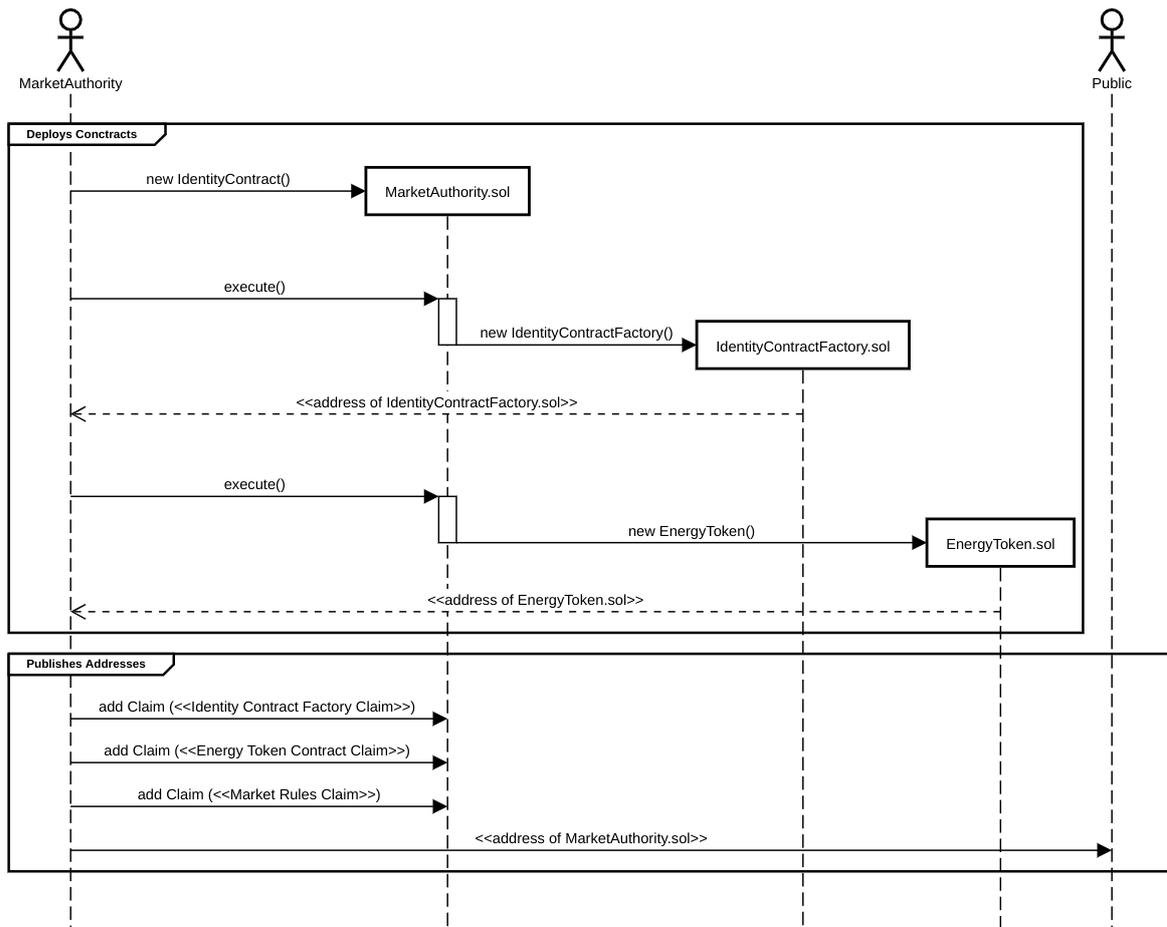


Abbildung 9: Marktsetup, Teil 1

Die Market Authority legt im Blockchain Netzwerk grundlegende Funktionen und Regeln für ihren Energie-Markt fest. Dafür erstellt die Market Authority Smart Contracts, welche diese grundlegenden energiewirtschaftlichen Funktionen im Blockchain Netzwerk bereitstellen. Anschließend macht die Market Authority die Adressen der Contracts bekannt, indem sie die Adressen als Claims ihrem Identity Contract hinzufügt und die Adresse ihres Identity Contracts (bspw. auf ihrer Website) veröffentlicht. Auf gleiche Weise werden diejenigen Marktregeln, welche nicht durch Smart Contracts forciert werden können, veröffentlicht (Abbildung 9).

Die operativen Authorities nutzen die von der Market Authority bereitgestellten Funktionen, um sich Identitäten im Blockchain Netzwerk zu beschaffen. Dafür erstellen die operativen Authorities sich mit Hilfe der Identity Contract Factory Identity Contracts. Im vorliegenden Prozess existiert eine Balance Authority für den Verbraucher ("BalanceAuthority_C") und eine Balance Authority für den Erzeuger ("BalanceAuthority_P") (Abbildung 10).

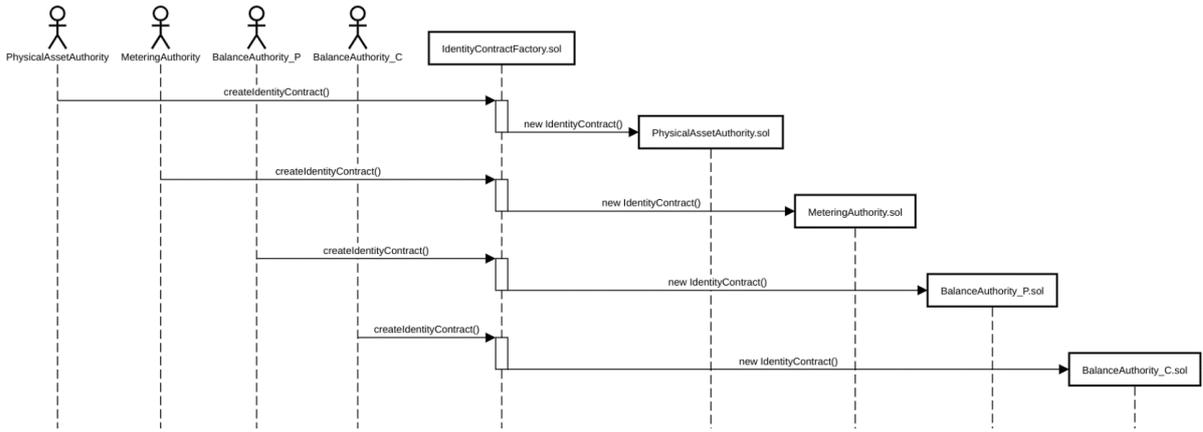


Abbildung 10: Marktsetup, Teil 2

Erzeuger und Verbraucher nutzen die von der Market Authority bereitgestellten Funktionen, um sich Identitäten im Blockchain Netzwerk zu beschaffen. Dafür erstellen sie sich mit Hilfe der Identity Contract Factory Identity Contracts (Abbildung 11).

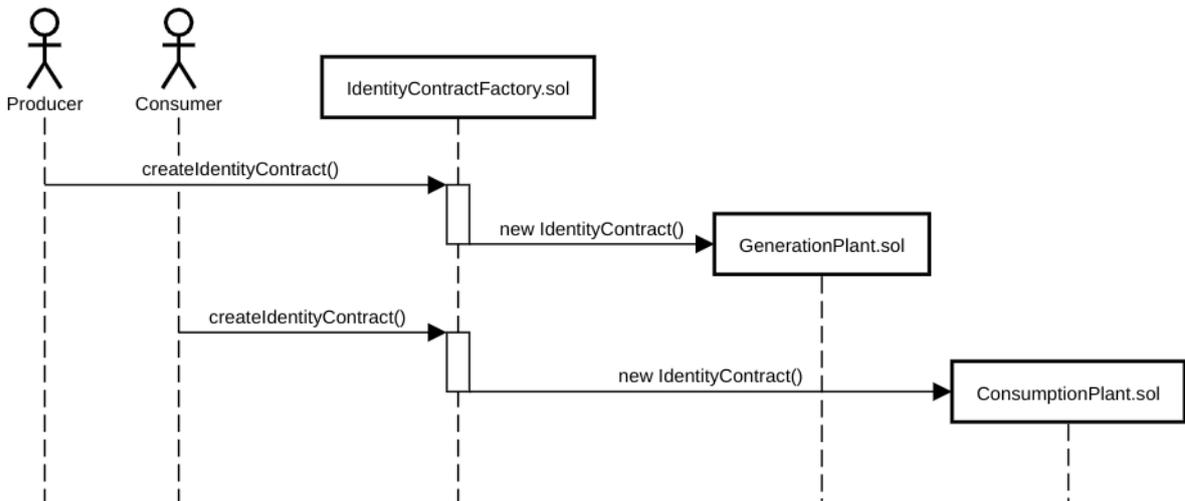


Abbildung 11: Marktsetup, Teil 3

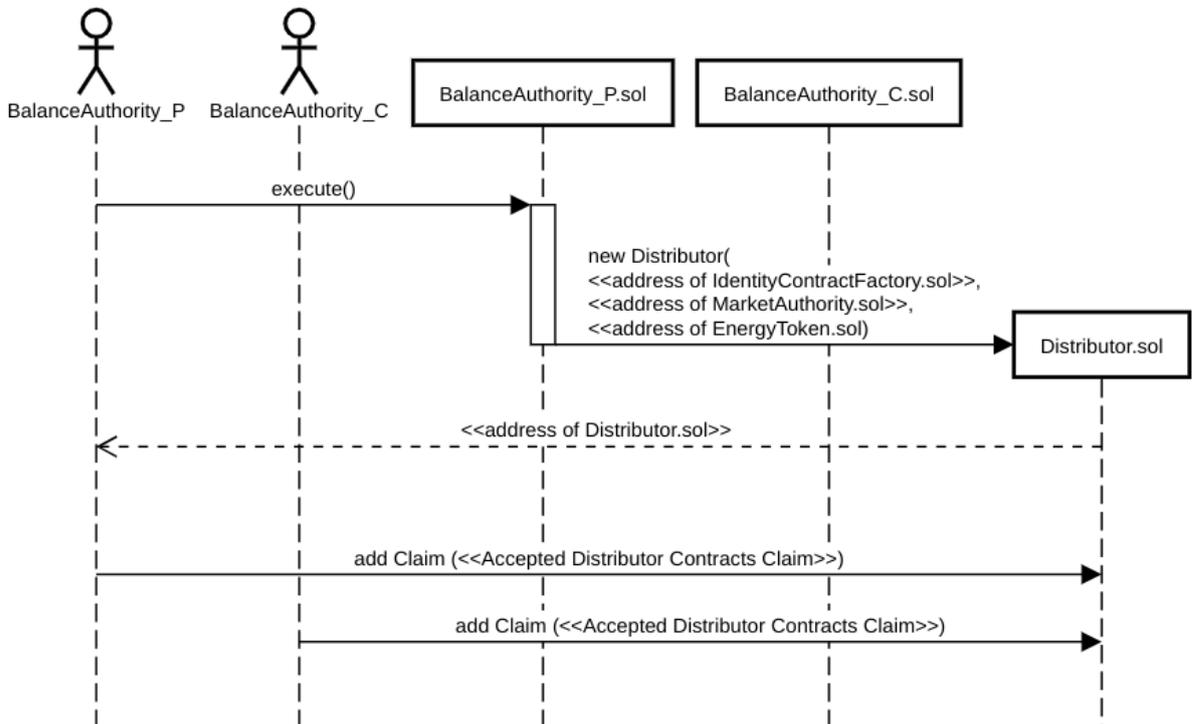


Abbildung 12: Marktsetup, Teil 4

Die Balance Authorities geben in Form von einem Distributor.sol Contract bekannt, welche Vertragstypen ihre Kunden beim Handel von Energie im Blockchain Netzwerk verwenden dürfen. Dafür erstellt die Balance Authority vom Erzeuger einen Distributor Contract, welcher für jede der drei Forwards Gattungen einen Verteilmechanismus implementiert. Anschließend geben beide Balance Authorities durch einen Claim bekannt, dass der erstellte Distributor Contract von all ihren "Balance Claim" Holder Kunden verwendet werden darf (Abbildung 12).

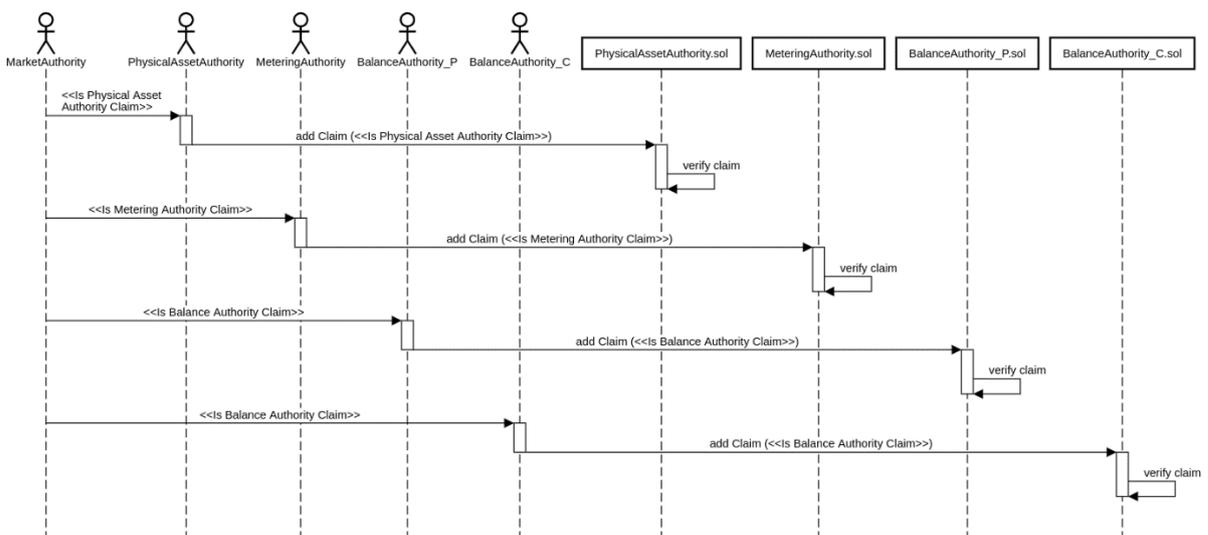


Abbildung 13: Marktsetup, Teil 5

Die Market Authority bestätigt im Blockchain Netzwerk die operativen Authorities in ihrer Rolle. Dafür schickt die Market Authority off-chain Claims zu den operativen Authorities, welche sich

diese dann an ihre Identity Contracts anhängen. In den Identity Contracts wird überprüft, ob die Signatur der Claims korrekt ist und vom öffentlichen Schlüssel der Market Authority erstellt wurde. Zum einen authentifiziert die Market Authority mit den Claims die operativen Authorities im Blockchain Netzwerk. Zum anderen autorisiert sie mit den Claims die operativen Authorities zur Nutzung des Energy Token Contracts (Abbildung 13).

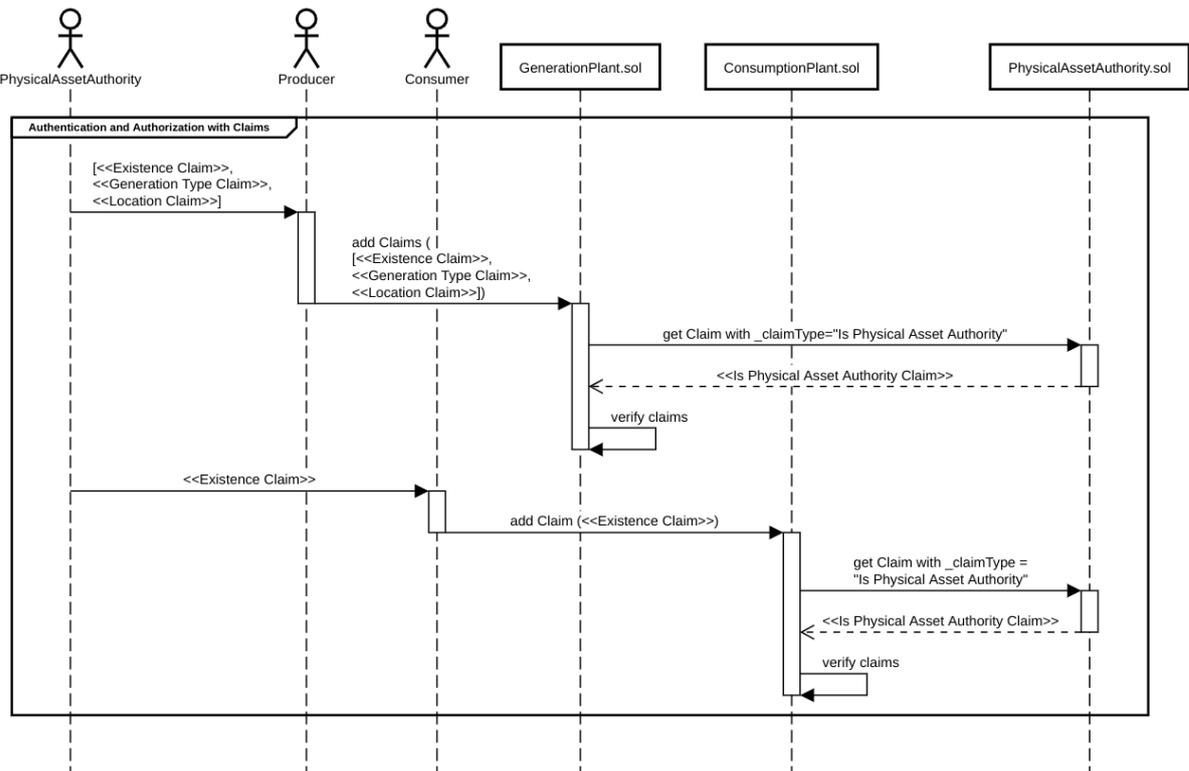


Abbildung 14: Marktsetup, Teil 6

Die Physical Asset Authority beglaubigt im Blockchain Netzwerk die Existenz und Eigenschaften der Verbrauchs- und Erzeugungsanlagen. Dafür stellt die Physical Asset Authority dem Erzeuger und Verbraucher Claims aus, welche sich diese dann an die Identity Contracts ihrer Anlagen anhängen. In den Identity Contracts wird überprüft, ob die Signatur der Claims korrekt ist und ob sie zum öffentlichen Schlüssel der entsprechenden Physical Asset Authority gehört. Zudem wird überprüft, ob die Physical Asset Authority in ihrer Rolle von der Market Authority durch einen Claim bestätigt wurde (Abbildung 14).

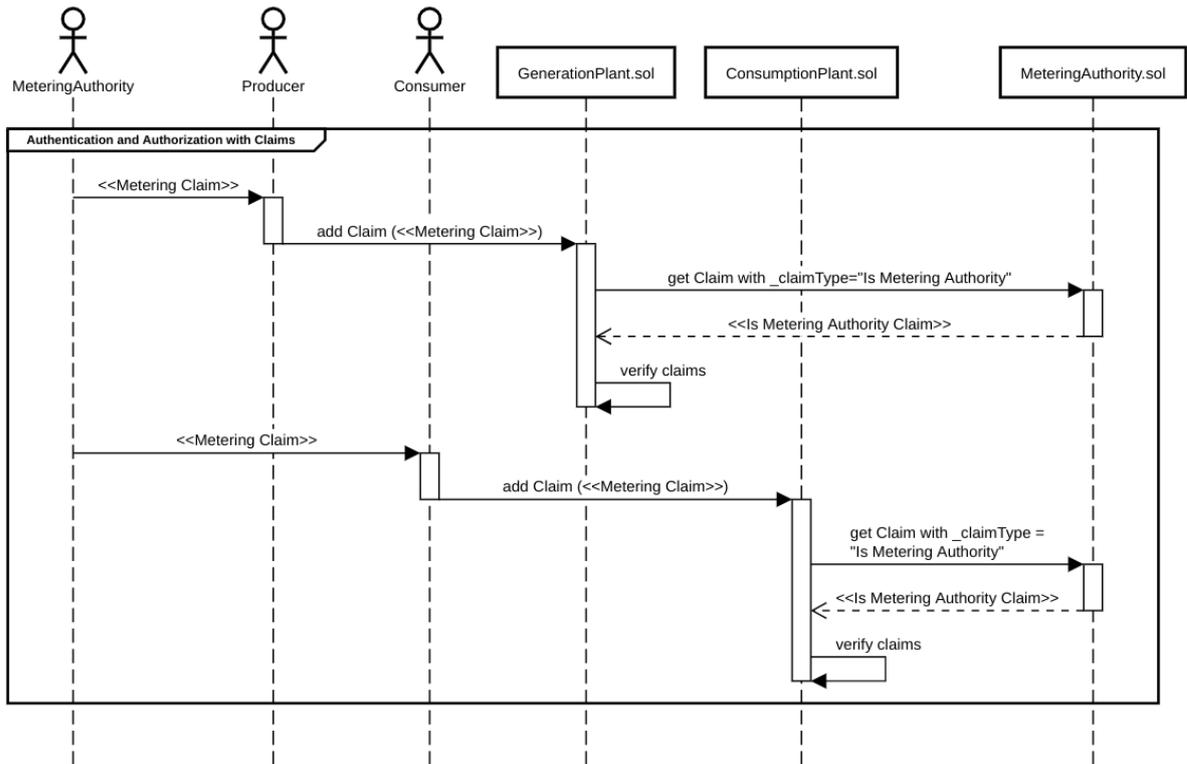


Abbildung 15: Marktsetup, Teil 7

Die Metering Authority bestätigt, dass sie die Messwerte der Anlagen dem Blockchain Protokoll bereitstellt (Abbildung 15).

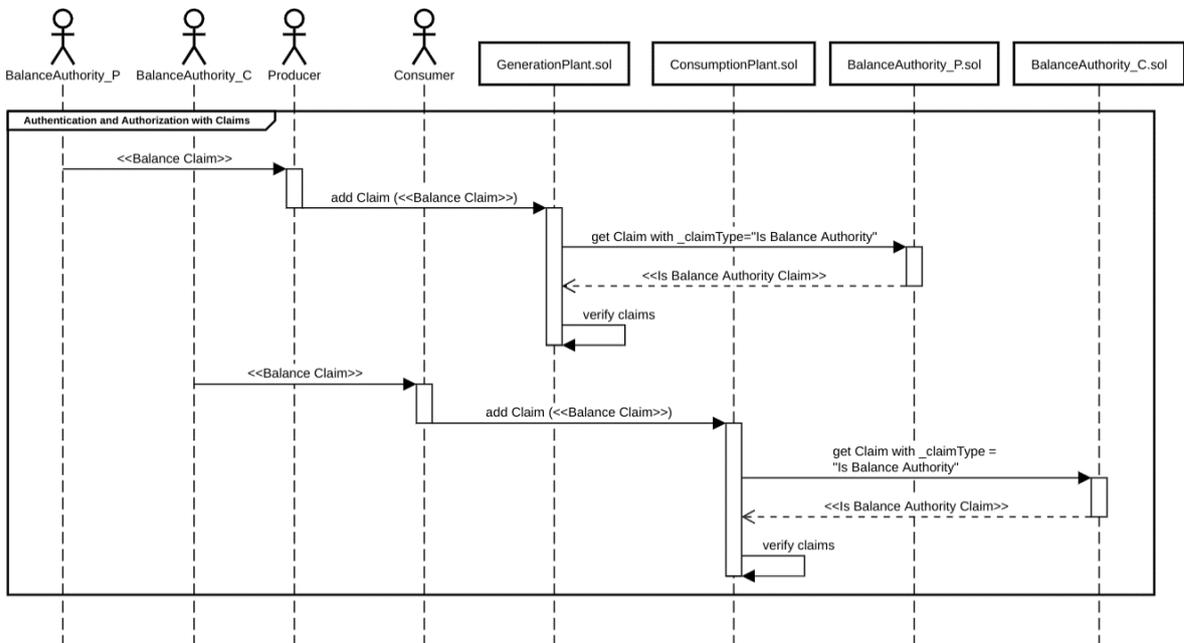


Abbildung 16: Marktsetup, Teil 8

Die Balance Authority bestätigt, dass sie die Anlage in einen registrierten Bilanzkreis aufnimmt und energetische Fehlmengen im Bilanzkreis ausgleicht (Abbildung 16).

10 Implementierung eines „Absolute Forwards“ Szenario

10.1 Handel

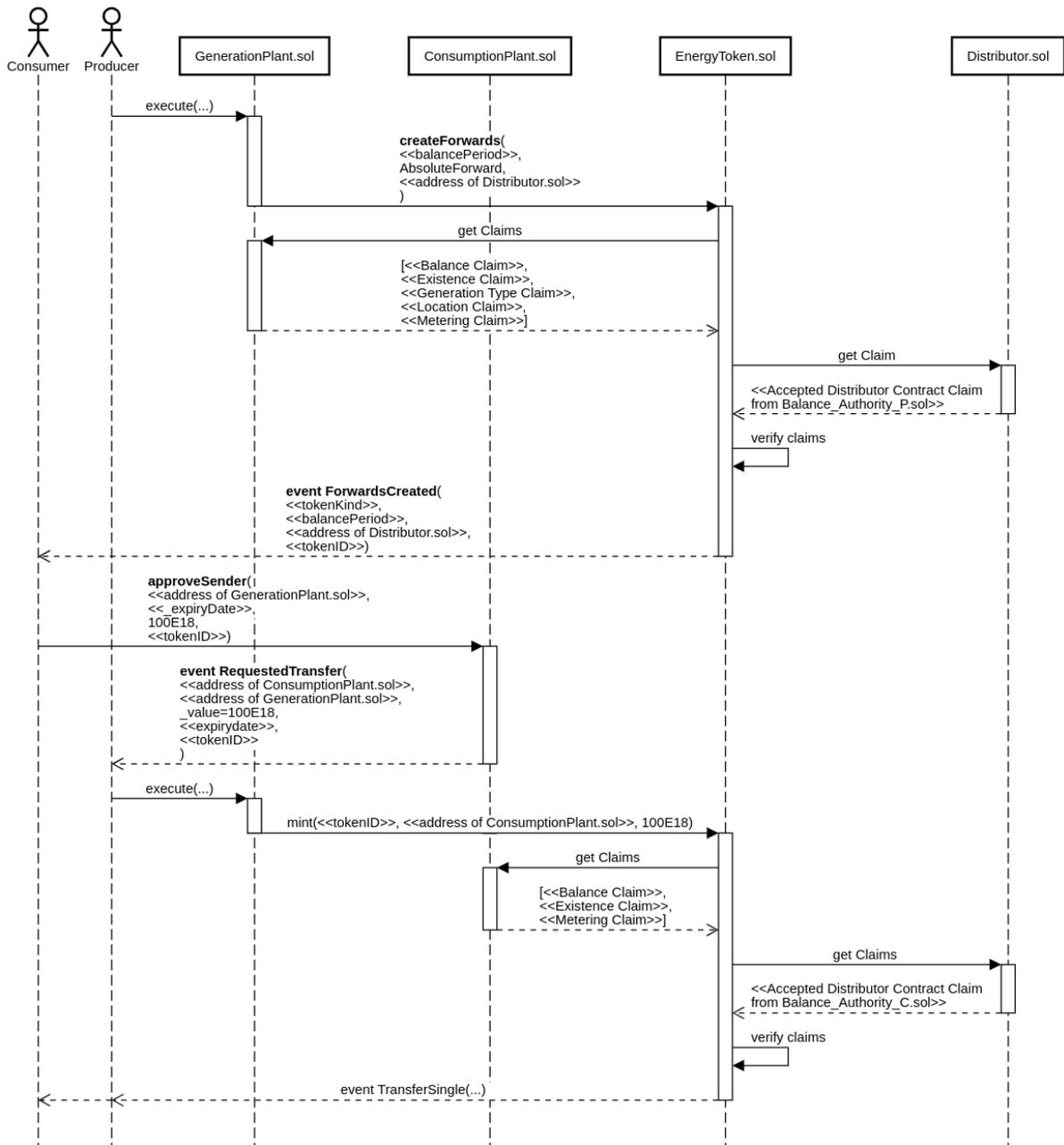


Abbildung 17: Absolute Forwards (Trading)

Der Erzeuger beschließt, eine fixe Menge Energie seiner Anlage für einen bestimmten Bilanzzeitraum zu verkaufen. Dafür verschickt er unter Zustimmung des Verbrauchers 100 kWh in Form von 100E18 Absolute Forward Token an den Verbraucher. Die tokenID ergibt sich aus der Token Gattung, dem Bilanzzeitraum und dem Identity Contract der Erzeugungsanlage. Hierbei werden sowohl die Claims der Verbrauchsanlage als auch die der Erzeugungsanlage überprüft (Abbildung 17).

10.2 Nachweis

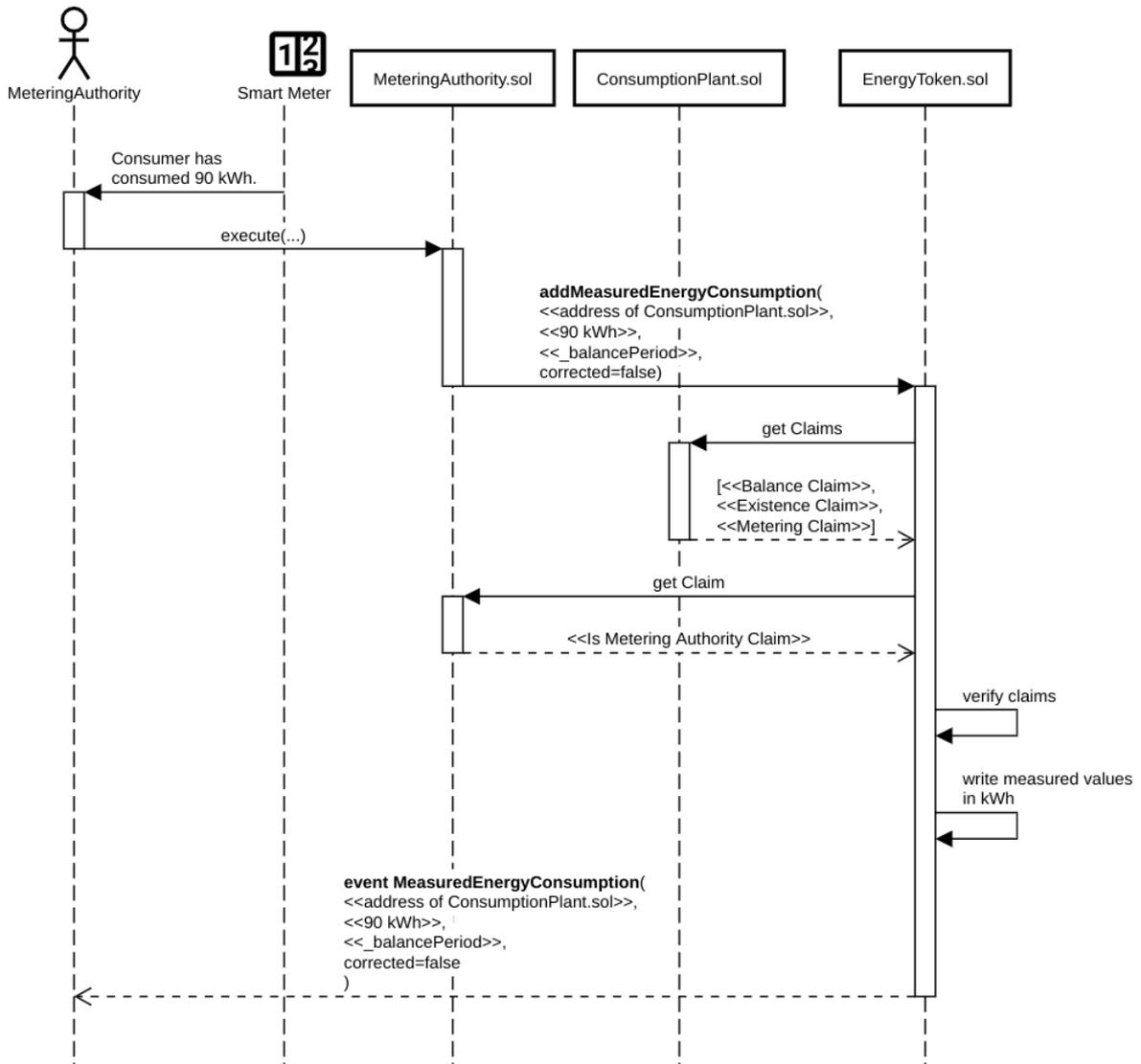


Abbildung 18: Certificates, Teil 1

Die Metering Authority dokumentiert auf der Blockchain die Messwerte der Verbrauchsanlage. Dafür speichert die Metering Authority durch Aufruf der "addMeasuredEnergyConsumption" Methode im Energy Token Contract die Messwerte der Verbrauchsanlage ab. Dabei werden zum einen die Claims der Metering Authority überprüft und zum anderen die Claims der Verbrauchsanlage (Abbildung 18).

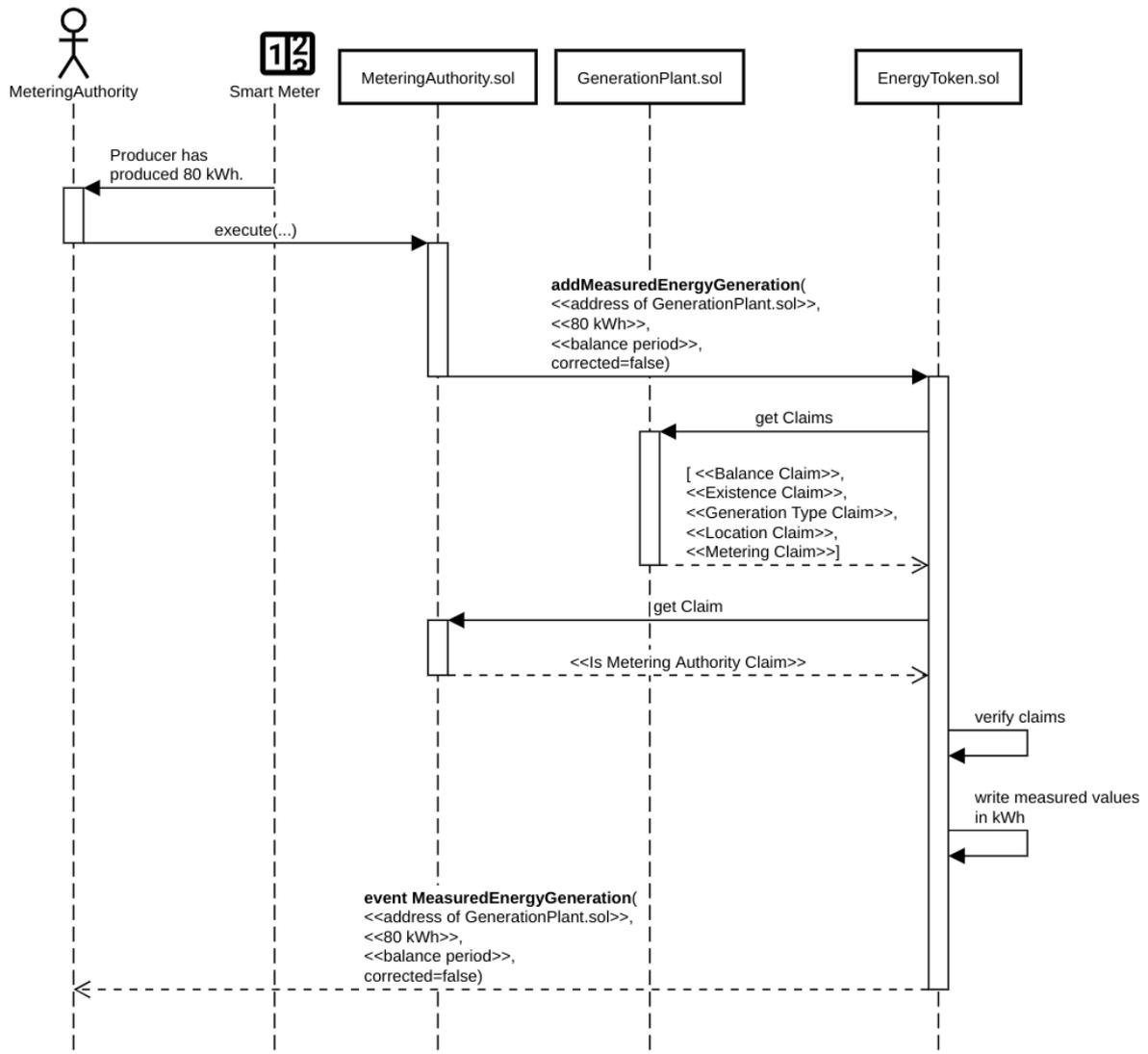


Abbildung 19: Certificates, Teil 2

Die Metering Authority dokumentiert auf der Blockchain die Messwerte der Erzeugungsanlage (Abbildung 19).

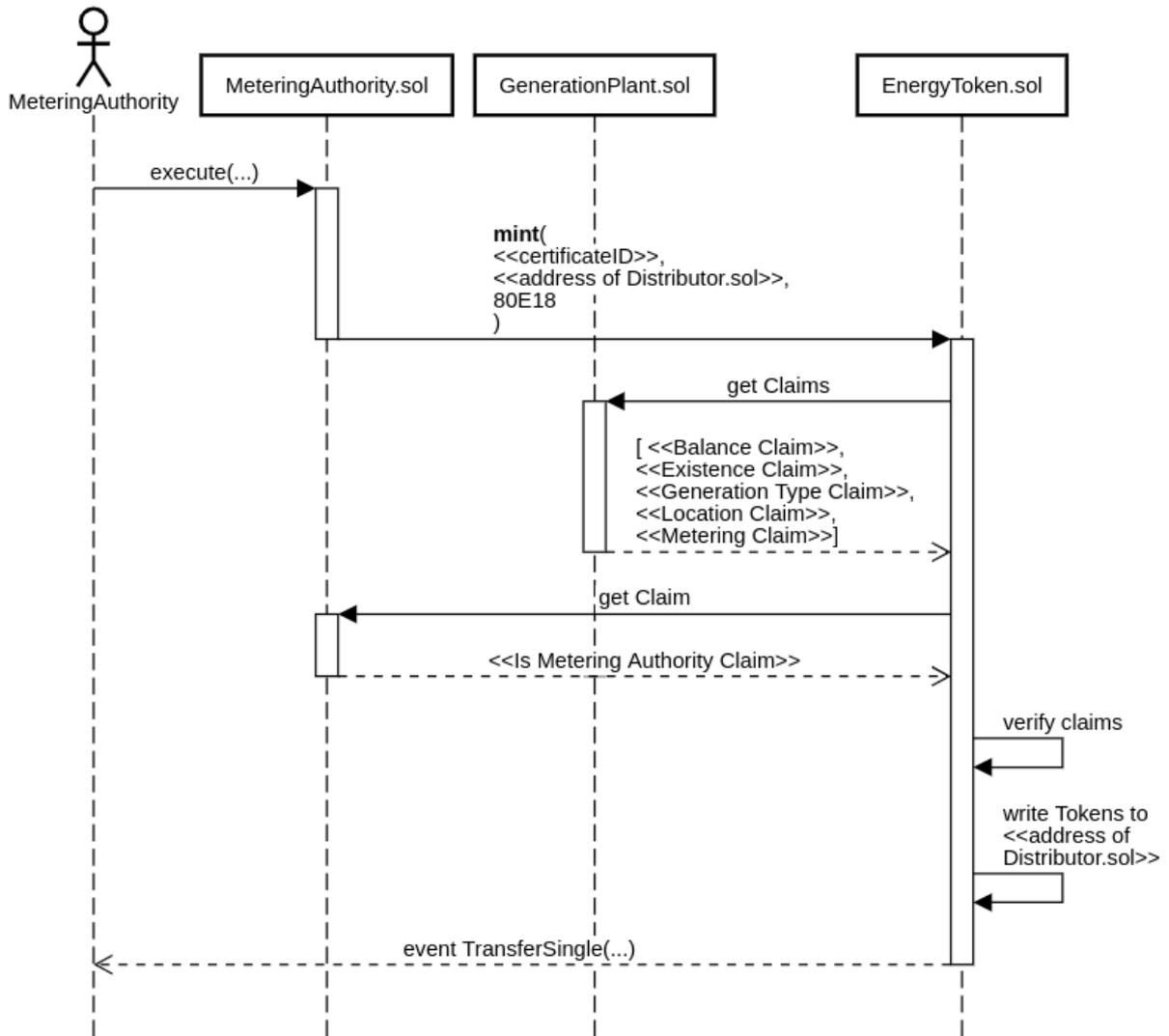


Abbildung 20: Certificates, Teil 3

Die Metering Authority schöpft 80E18 bilanzzeitraum-spezifische Certificate Token, welche im weiteren Verlauf an die Forward Token Besitzer verteilt werden. Die Metering Authority bildet somit die geflossene Energie samt Eigenschaften der Erzeugungsanlage auf die Blockchain in Form von handelbaren Token ab (Abbildung 20).

10.3 Verteilung und Abrechnung

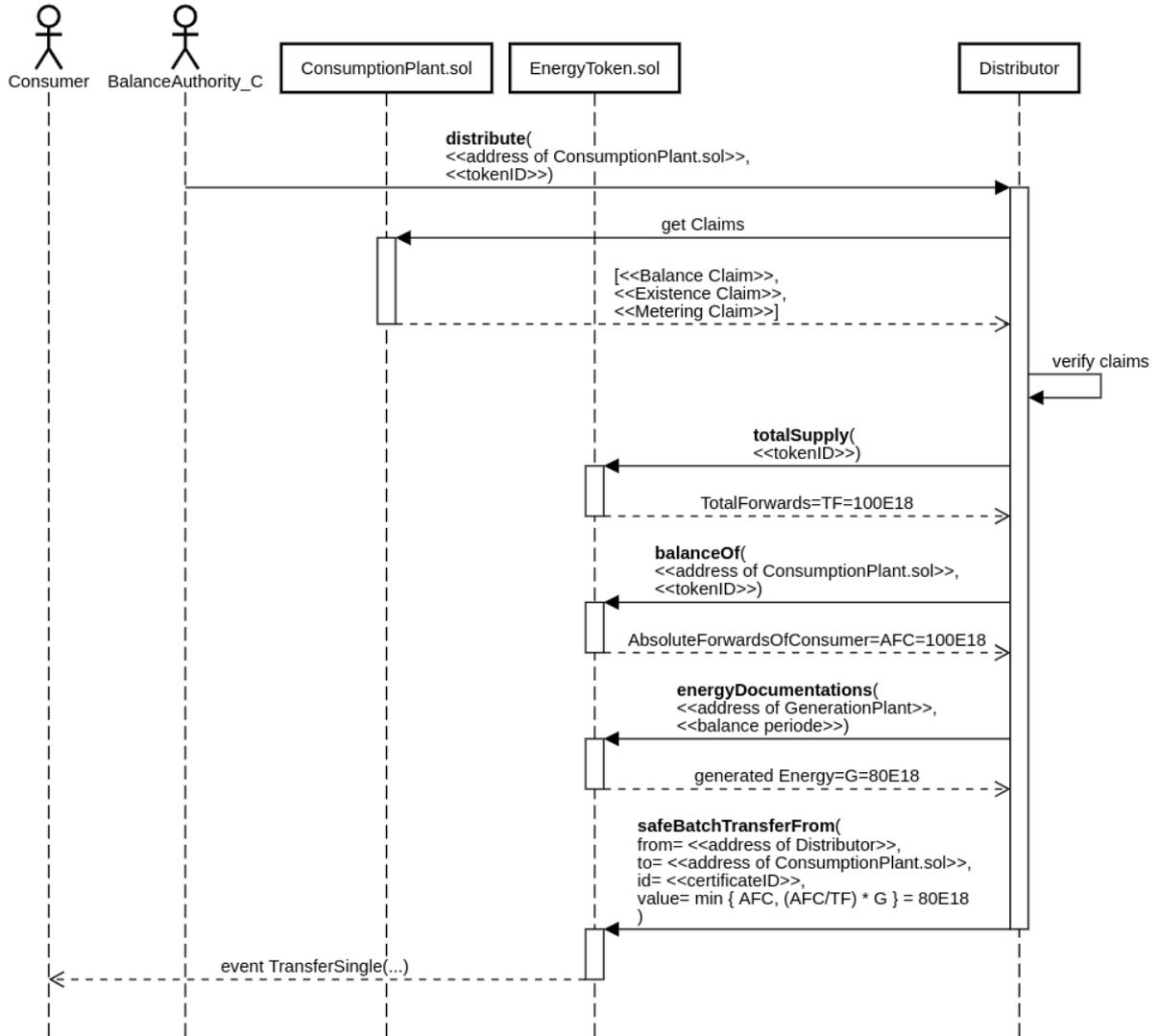


Abbildung 21: Absolute Forwards (Distribution & Billing), Teil 1

Die Balance Authority des Verbrauchers beschafft diesem die ihm zustehenden Certificates. Dafür führt die Balance Authority des Verbrauchers durch Aufruf der "distribute" Methode die Verteillogik im Distributor Contract aus, welcher die Certificates an die Verbrauchsanlage schickt. Hierbei werden die Claims von der Verbrauchsanlage überprüft (Abbildung 21).

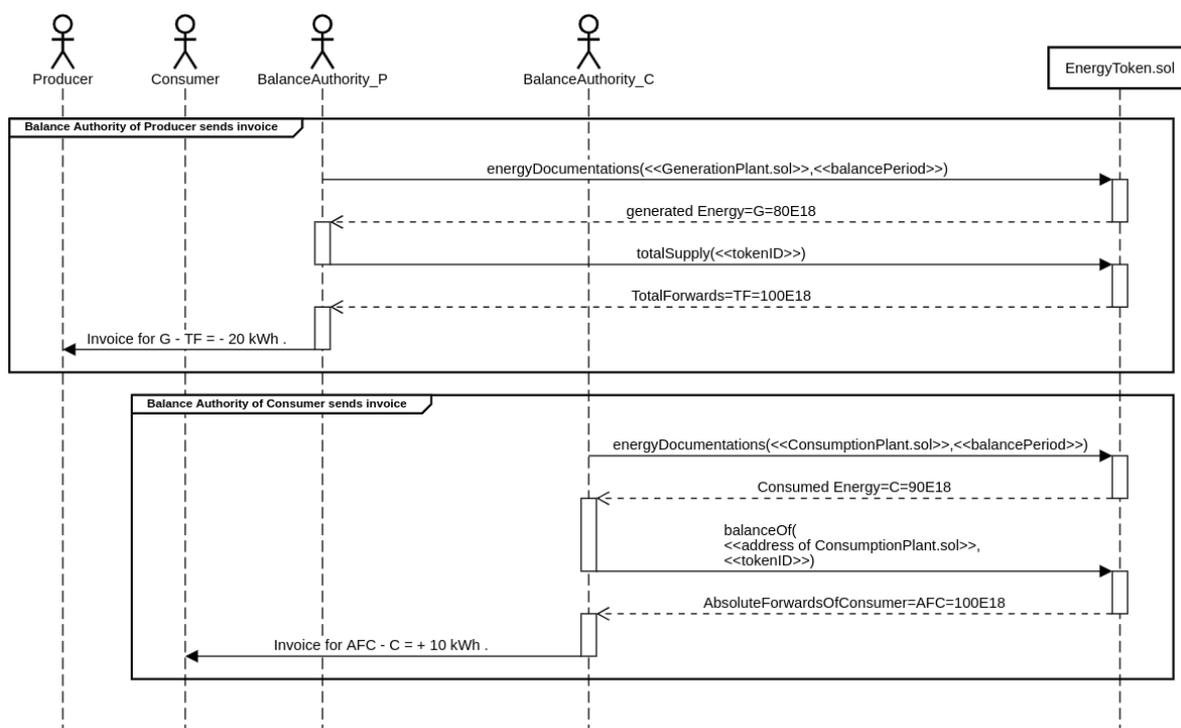


Abbildung 22: Absolute Forwards (Distribution & Billing), Teil 2

Die Balance Authority des Erzeugers stellt die Fehlmenge zwischen vereinbarter und tatsächlich erzeugter Energiemenge dem Erzeuger in Rechnung. Die Balance Authority des Verbrauchers stellt die Fehlmenge zwischen vereinbarter und tatsächlich verbrauchter Energiemenge dem Verbraucher in Rechnung. Die Rechnung kann auch eine Gutschrift für den Verbraucher oder Erzeuger darstellen (Abbildung 22).

11 Implementierung eines „Generation-based Forwards“-Szenario

Die technische Funktionsweise ist analog zum Fall der Implementierung eines „Absolute Forwards (vgl. Kapitel 10) und wird daher in diesem Kapitel nicht nochmals erläutert.

11.1 Handel

Der Erzeuger verspricht dem Verbraucher, ihm 30% seiner erzeugten Energie bilanziell zukommen zu lassen. Dazu schickt der Erzeuger 30E18 Generation-based Forward Token der zuvor erstellten Token Art an den Verbraucher (Abbildung 23).

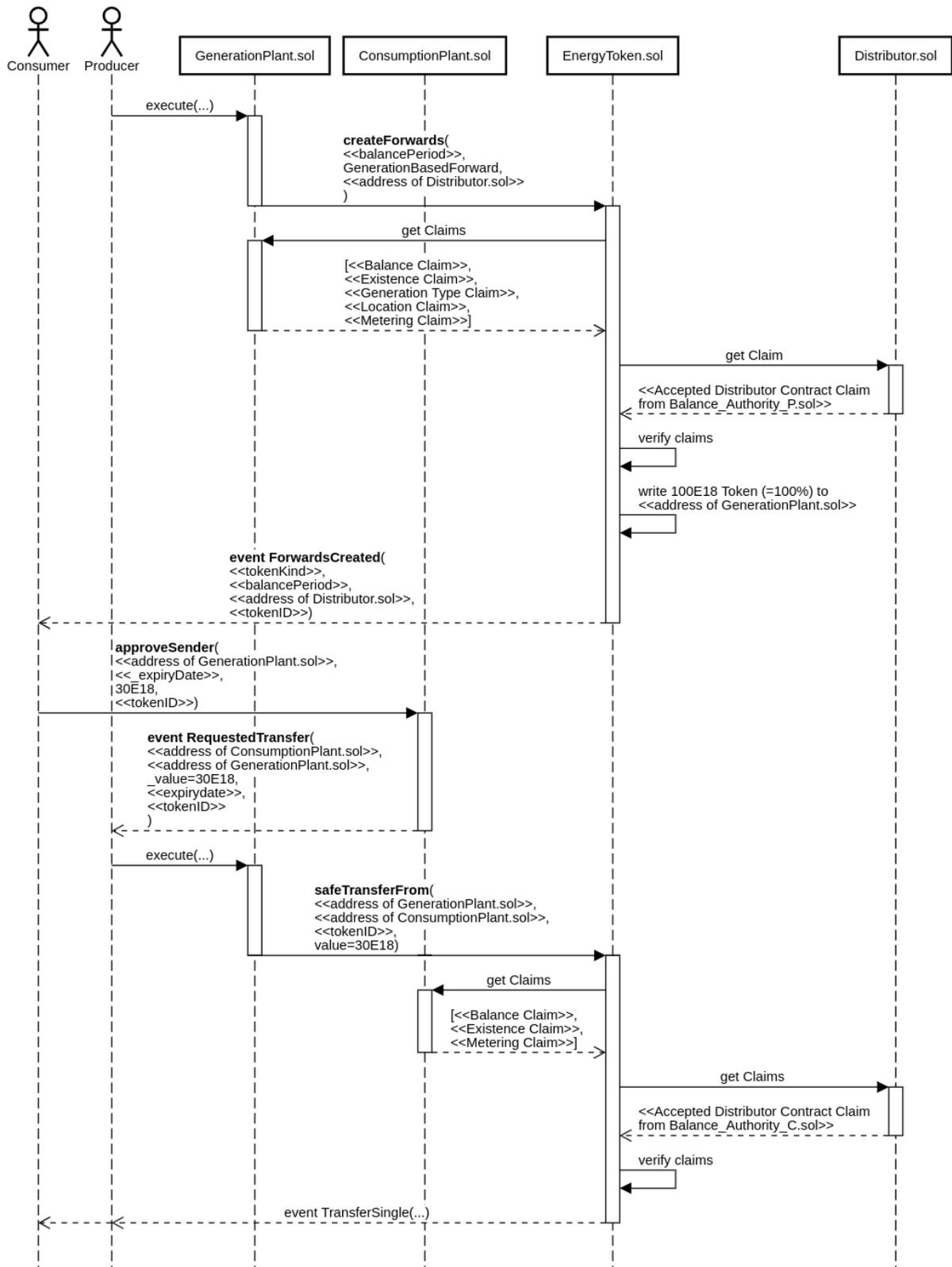


Abbildung 23: Generation-based Forwards (Trading)

11.2 Nachweis

Der Prozess des Nachweises funktioniert analog zu Kapitel „10.2 Nachweis“.

11.3 Verteilung und Abrechnung

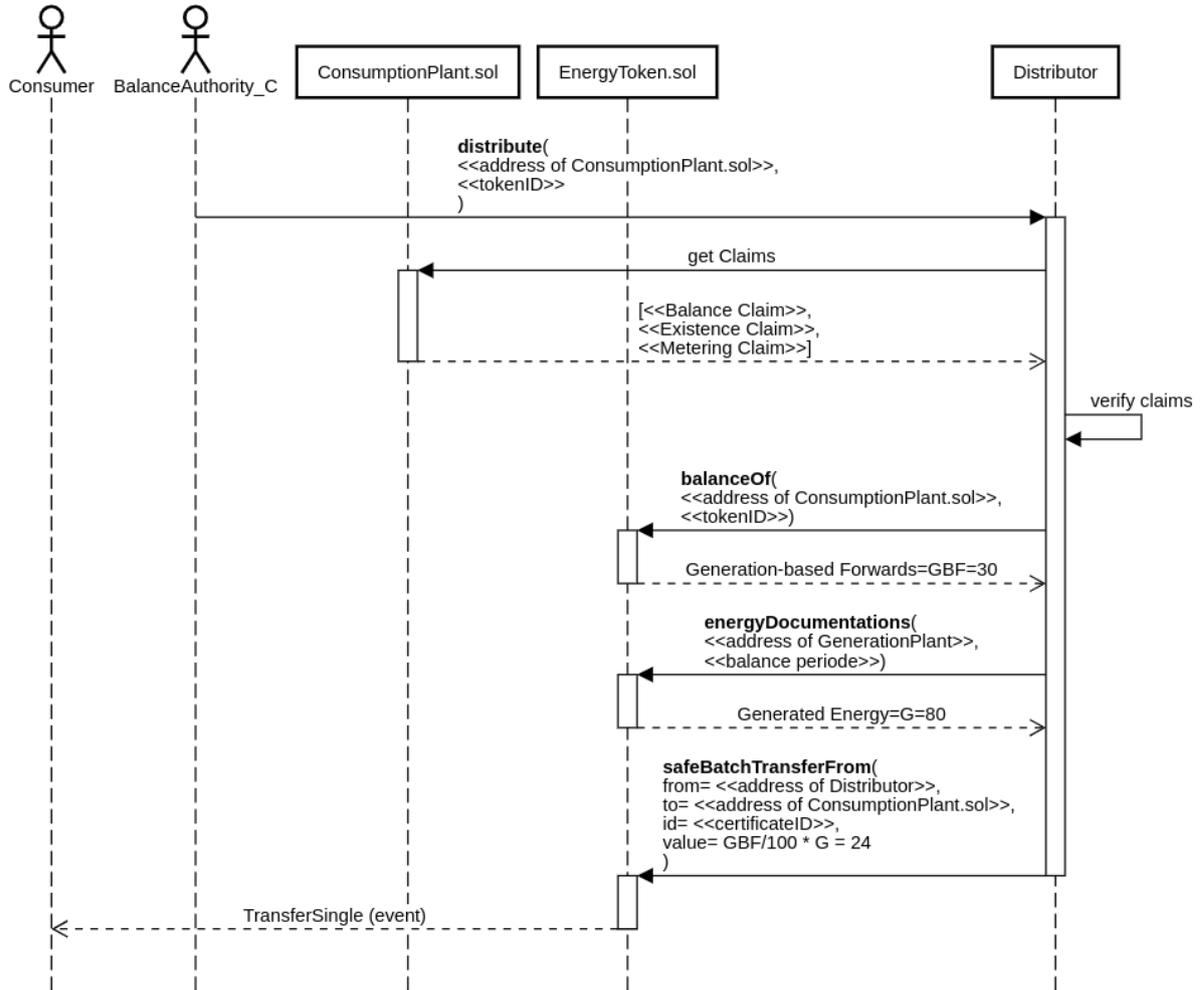


Abbildung 24: Generation-based Forwards (Distribution & Billing), Teil 1

Die Balance Authority des Verbrauchers beschafft dem Verbraucher die ihm zustehenden Certificates (Abbildung 24).

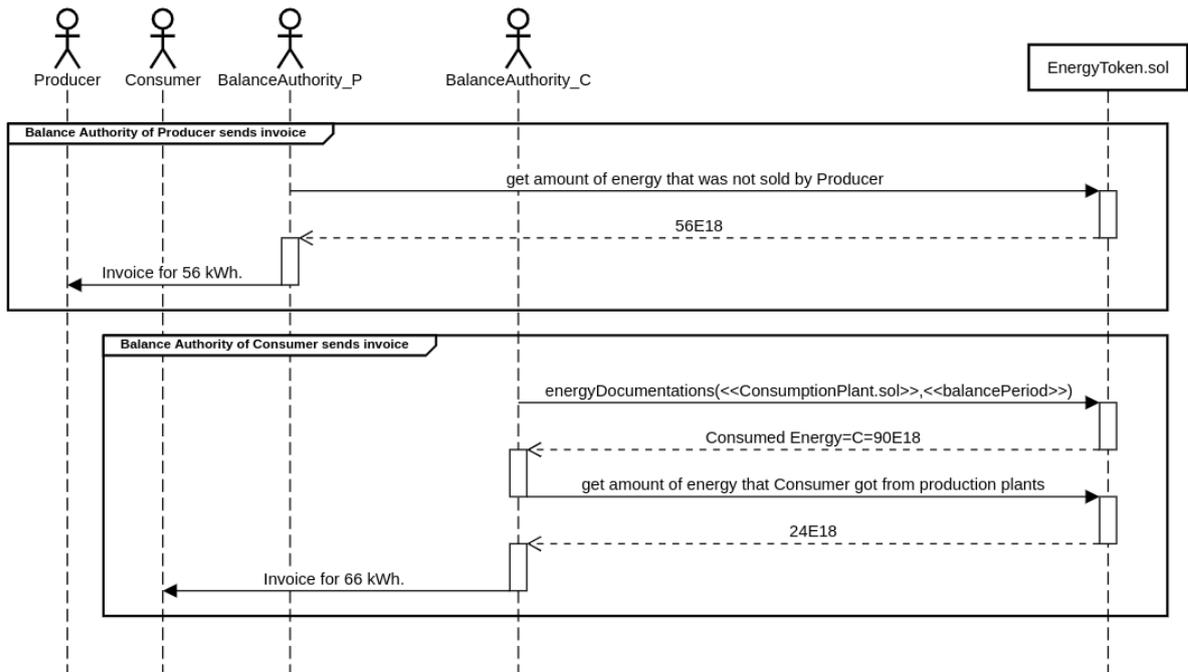


Abbildung 25: Generation-based Forwards (Distribution & Billing), Teil 2

Die Balance Authority des Erzeugers stellt dem Erzeuger die Fehlmenge zwischen vereinbarter und tatsächlich erzeugter Energiemenge in Rechnung. Die Balance Authority des Verbrauchers stellt dem Verbraucher die Fehlmenge zwischen vereinbarter und tatsächlich verbrauchter Energiemenge in Rechnung (Abbildung 25).

12 Implementierung eines „Consumption-based Forwards“-Szenario

Die technische Funktionsweise ist analog zum Fall der Absolute Forwards und wird daher in diesem Kapitel nicht nochmals erläutert.

12.1 Handel

Der Erzeuger verspricht dem Verbraucher Vollversorgung, indem er dem Verbraucher 100E18 Consumption-based Forward Token zuschickt (Abbildung 26).

12.2 Nachweis

Der Prozess des Nachweises funktioniert analog zu Kapitel „10.2 Nachweis“

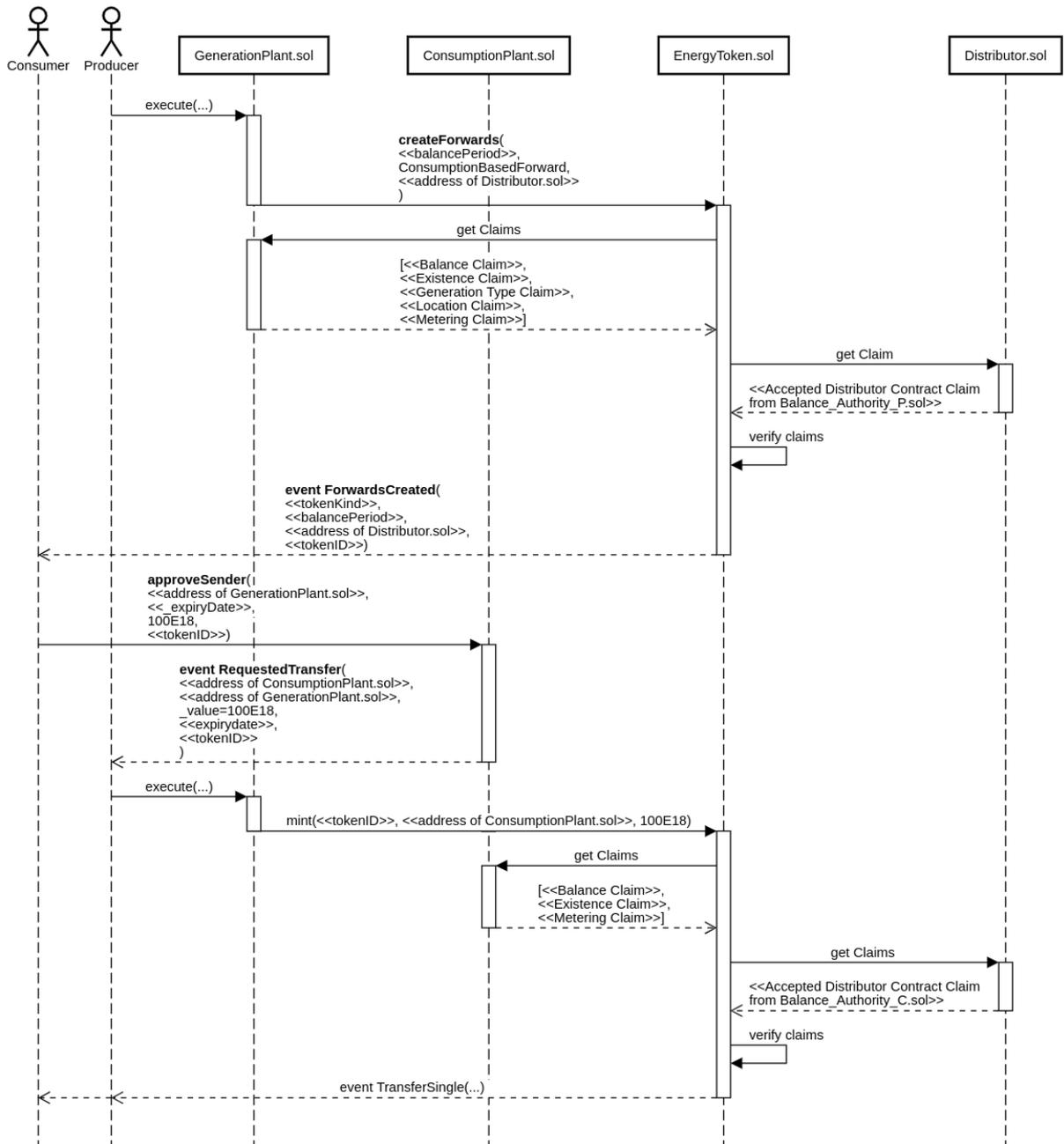


Abbildung 26: Consumption-based Forwards (Trading)

12.3 Verteilung und Abrechnung

Die Balance Authority des Verbrauchers beschafft diesem die ihm zustehenden Certificates (Abbildung 27).

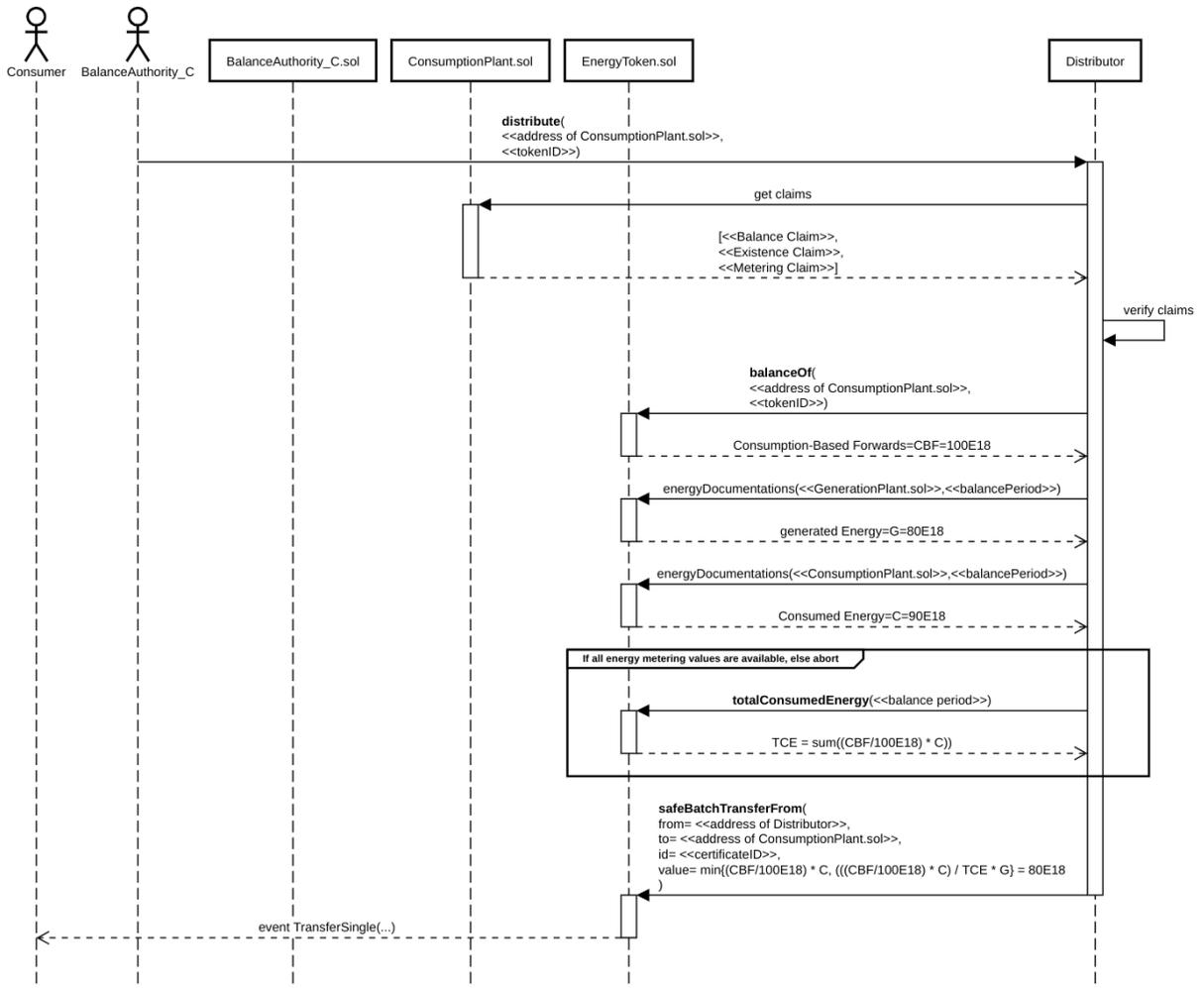


Abbildung 27: Consumption-based Forwards (Distribution & Billing), Teil 1

Die Balance Authority vom Erzeuger stellt die Fehlmenge zwischen vereinbarter und tatsächlich erzeugter Energiemenge dem Erzeuger in Rechnung (Abbildung 28).

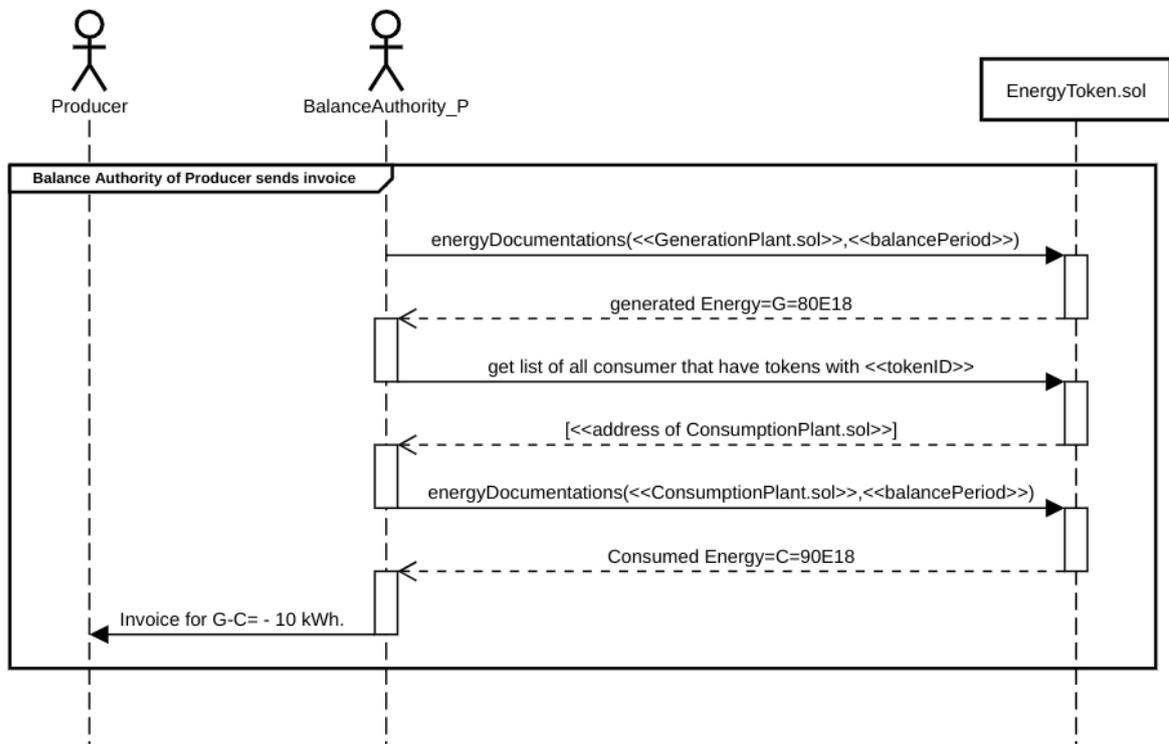


Abbildung 28: Consumption-based Forwards (Distribution & Billing), Teil 2

13 Begriffserklärungen

„Energiewirtschaftliche Akteure“: Authorities, Erzeuger und Verbraucher.

“Authority“: Vertrauensschaffender energiewirtschaftlicher Akteur mit besonderen Befugnissen, welcher insbesondere dafür zuständig ist, reale Sachverhalte wahrheitsgetreu auf die Blockchain abzubilden.

“Token Contract“: Ein Smart Contract, welcher jeder Adresse einen oder mehrere Kontostände von Token Arten zuweist und eine Menge von Funktionen zum Erstellen und Transferieren von einer oder mehreren Token Arten bereitstellt.

“Token Art“: Endliche Menge von vermengbaren Token, welche insbesondere dieselben Eigenschaften haben.

“Token“: Ein Token repräsentiert die kleinste transferierbare Einheit, welche durch einen Token Contract realisiert wird. 1 Token entspricht 1E-18 kWh.

“Claim“: Eine signierte Behauptung in digitaler Form. Der Verteilnetzbetreiber schickt bspw. einem Erzeuger eine digital signierte Urkunde, welche bestätigt, dass seine Erzeugungsanlage ordnungsgemäß funktioniert.

“off-chain“: Nicht mittels Blockchain Protokoll.

“Generation Plant“: Erzeugungsanlage.

“Consumption Plant“: Verbrauchsanlage.

“Balance Period“: Bilanzzeitraum.

“Consumption-based“: Verbrauchsabhängig.

“Generation-based“: Erzeugungsabhängig.

“Forwards“: “Ein Forward ist eine Vereinbarung, einen Vermögenswert zu einem bestimmten Preis und zu einem bestimmten Zeitpunkt in der Zukunft zu kaufen bzw. zu verkaufen.”¹⁷

“Claim Issuer“: Der Ersteller eines Claims.

“Claim Holder“: Energiewirtschaftlicher Akteur, über den ein Claim etwas aussagt. Der Claim Holder ist insbesondere Besitzer des ERC 735 Identity Contracts, mit welchem der Claim verknüpft ist.

¹⁷ Quelle: [https://de.wikipedia.org/wiki/Forward_\(Wirtschaft\)](https://de.wikipedia.org/wiki/Forward_(Wirtschaft))

14 Tabellen Verzeichnis

Tabelle 1: Vorteile des Blockchain Einsatz in der Energiewirtschaft.....	6
Tabelle 2: Anforderungen an das Authority-Modell.....	8
Tabelle 3: Anforderungen an das Authority-Modell.....	10
Tabelle 4: Zwei Formen zur Abbildung von Energie.....	13
Tabelle 5: Forwards & Certificates.....	14
Tabelle 6: Claim Übersicht.....	21
Tabelle 7: Konstruktor Identity Contract.....	22
Tabelle 8: Methode „createForwards“.....	24
Tabelle 9: Methode „mint“.....	25
Tabelle 10: Methode "approveSender".....	25
Tabelle 11: Methode "approveBatchSender".....	26
Tabelle 12: Methode "addMeasuredEnergyConsumption".....	26
Tabelle 13: Methode "addMeasuredEnergyGeneration".....	27

15 Abbildungsverzeichnis

Abbildung 1: Operative Authorities bringen die Wahrheit in die Blockchain.....	11
Abbildung 2: Beispiel für die Entstehung von Identitäten.....	12
Abbildung 3: Schema der 3-Layer-Architektur.....	16
Abbildung 4: Identity Contract.....	19
Abbildung 5: ER-Modell: Identity Contracts.....	20
Abbildung 6: Energy Token Contract.....	22
Abbildung 7: Systematische Unterteilung der Energie Token.....	23
Abbildung 8: ER-Modell: Energy Token.....	24
Abbildung 9: Marktsetup, Teil 1.....	28
Abbildung 10: Marktsetup, Teil 2.....	29
Abbildung 11: Marktsetup, Teil 3.....	29
Abbildung 12: Marktsetup, Teil 4.....	30
Abbildung 13: Marktsetup, Teil 5.....	30
Abbildung 14: Marktsetup, Teil 6.....	31
Abbildung 15: Marktsetup, Teil 7.....	32
Abbildung 16: Marktsetup, Teil 8.....	32
Abbildung 17: Absolute Forwards (Trading).....	33
Abbildung 18: Certificates, Teil 1.....	34
Abbildung 19: Certificates, Teil 2.....	35
Abbildung 20: Certificates, Teil 3.....	36
Abbildung 21: Absolute Forwards (Distribution & Billing), Teil 1.....	37
Abbildung 22: Absolute Forwards (Distribution & Billing), Teil 2.....	38
Abbildung 23: Generation-based Forwards (Trading).....	39
Abbildung 24: Generation-based Forwards (Distribution & Billing), Teil 1.....	40
Abbildung 25: Generation-based Forwards (Distribution & Billing), Teil 2.....	41
Abbildung 26: Consumption-based Forwards (Trading).....	42
Abbildung 27: Consumption-based Forwards (Distribution & Billing), Teil 1.....	43
Abbildung 28: Consumption-based Forwards (Distribution & Billing), Teil 2.....	44

Creative Commons Public Licence: Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 International (CC – BY SA 4.0)

Durch die Ausübung der lizenzierten Rechte (wie unten definiert) erklären Sie sich rechtsverbindlich mit den Bedingungen dieser Creative Commons Namensnennung – Share Alike 4.0 International Public License ("Public License") einverstanden. Soweit die vorliegende Public License als Lizenzvertrag anzusehen ist, gewährt Ihnen der Lizenzgeber die in der Public License genannten lizenzierten Rechte im Gegenzug dafür, dass Sie die Lizenzbedingungen akzeptieren, und gewährt Ihnen die entsprechenden Rechte in Hinblick auf Vorteile, die der Lizenzgeber durch das Verfügbarmachen des lizenzierten Materials unter diesen Bedingungen hat.

Abschnitt 1 – Definitionen

- a. Abgewandeltes Material bezeichnet Material, welches durch Urheberrechte oder ähnliche Rechte geschützt ist und vom lizenzierten Material abgeleitet ist oder darauf aufbaut und in welchem das lizenzierte Material übersetzt, verändert, umarrangiert, umgestaltet oder anderweitig modifiziert in einer Weise enthalten ist, die aufgrund des Urheberrechts oder ähnlicher Rechte des Lizenzgebers eine Zustimmung erfordert. Im Sinne der vorliegenden Public License entsteht immer abgewandeltes Material, wenn das lizenzierte Material ein Musikwerk, eine Darbietung oder eine Tonaufnahme ist und zur Vertonung von Bewegtbildern verwendet wird.
- b. Abwandlungslizenz bezeichnet die Lizenz, die Sie in Bezug auf Ihr Urheberrecht oder ähnliche Rechte an Ihren Beiträgen zum abgewandelten Material in Übereinstimmung mit den Bedingungen der vorliegenden Public License erteilen.
- c. BY-SA-kompatible Lizenz bezeichnet eine unter creativecommons.org/compatiblelicenses genannte Lizenz, die Creative Commons als der vorliegenden Public License im Wesentlichen gleichwertig anerkannt hat.
- d. Urheberrecht und ähnliche Rechte bezeichnet das Urheberrecht und/oder ähnliche, dem Urheberrecht eng verwandte Rechte, einschließlich insbesondere des Rechts des ausübenden Künstlers, des Rechts zur Sendung, zur Tonaufnahme und des Sui-generis-Datenbankrechts, unabhängig davon, wie diese Rechte genannt oder kategorisiert werden. Im Sinne der vorliegenden Public License werden die in Abschnitt 2(b)(1)-(2) aufgeführten Rechte nicht als Urheberrecht und ähnliche Rechte angesehen.
- e. Wirksame technische Schutzmaßnahmen bezeichnet solche Maßnahmen, die gemäß gesetzlichen Regelungen auf der Basis des Artikels 11 des WIPO Copyright Treaty vom 20. Dezember 1996 und/oder ähnlicher internationaler Vereinbarungen ohne entsprechende Erlaubnis nicht umgangen werden dürfen.
- f. Ausnahmen und Beschränkungen bezeichnet Fair Use, Fair Dealing und/oder jegliche andere Ausnahme oder Beschränkung des Urheberrechts oder ähnlicher Rechte, die auf Ihre Nutzung des lizenzierten Materials Anwendung findet.
- g. Lizenzelemente bezeichnet die Lizenzeigenschaften, die in der Bezeichnung einer Creative Commons Public License aufgeführt werden. Die Lizenzelemente der vorliegenden Public License sind Namensnennung und Share Alike.
- h. Lizenziertes Material bezeichnet das Werk der Literatur oder Kunst, die Datenbank oder das sonstige Material, welches der Lizenzgeber unter die vorliegende Public License gestellt hat.
- i. Lizenzierte Rechte bezeichnet die Ihnen unter den Bedingungen der vorliegenden Public License gewährten Rechte, welche auf solche Urheberrechte und ähnlichen Rechte beschränkt sind, die Ihre Nutzung des lizenzierten Materials betreffen und die der Lizenzgeber zu lizenzieren berechtigt ist.
- j. Lizenzgeber bezeichnet die natürliche(n) oder juristische(n) Person(en), die unter der vorliegenden Public License Rechte gewährt (oder gewähren).
- k. Weitergabe meint, Material der Öffentlichkeit bereitzustellen durch beliebige Mittel oder Verfahren, die gemäß der lizenzierten Rechte Zustimmung erfordern, wie zum Beispiel Vervielfältigung, öffentliche Vorführung, öffentliche Darbietung, Vertrieb, Verbreitung, Wiedergabe oder Übernahme und öffentliche Zugänglichmachung bzw. Verfügbarmachung in solcher Weise, dass Mitglieder der Öffentlichkeit auf das Material von Orten und zu Zeiten ihrer Wahl zugreifen können.
- l. Sui-generis Datenbankrechte bezeichnet Rechte, die keine Urheberrechte sind, sondern gegründet sind auf die Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken in der jeweils gültigen Fassung bzw. deren Nachfolgeregelungen, sowie andere im Wesentlichen funktionsgleiche Rechte anderswo auf der Welt.
- m. Sie bezeichnet die natürliche oder juristische Person, die von lizenzierten Rechten unter der vorliegenden Public License Gebrauch macht. Ihr bzw. Ihre hat die entsprechende Bedeutung.

Abschnitt 2 – Umfang

- a. Lizenzgewährung
 - 1. Unter den Bedingungen der vorliegenden Public License gewährt der Lizenzgeber Ihnen eine weltweite, vergütungsfreie, nicht unterlizenzierbare, nicht-ausschließliche, unwiderrufliche Lizenz zur Ausübung der lizenzierten Rechte am lizenzierten Material, um:
 - A. das lizenzierte Material ganz oder in Teilen zu vervielfältigen und weiterzugeben; und
 - B. abgewandeltes Material zu erstellen, zu vervielfältigen und weiterzugeben.
 - 2. Ausnahmen und Beschränkungen. Es sei klargestellt, dass, wo immer gesetzliche Ausnahmen und Beschränkungen auf Ihre Nutzung Anwendung finden, die vorliegende Public License nicht anwendbar ist und Sie insoweit ihre Bedingungen nicht einhalten müssen.
 - 3. Laufzeit. Die Laufzeit der vorliegenden Public License wird in Abschnitt 6(a) geregelt.
 - 4. Medien und Formate; Gestattung technischer Modifikationen. Der Lizenzgeber erlaubt Ihnen, die lizenzierten Rechte in allen bekannten und zukünftig entstehenden Medien und Formaten auszuüben und die dafür notwendigen technischen Modifikationen vorzunehmen. Der Lizenzgeber verzichtet auf jegliche und/oder versichert die Nichtausübung jeglicher Rechte und Befugnisse, Ihnen zu verbieten, technische Modifikationen vorzunehmen, die notwendig sind, um die lizenzierten Rechte ausüben zu können, einschließlich solcher, die zur Umgehung

wirksamer technischer Schutzmaßnahmen erforderlich sind. Im Sinne der vorliegenden Public License entsteht kein abgewandeltes Material, soweit lediglich Modifikationen vorgenommen werden, die nach diesem Abschnitt 2(a)(4) zulässig sind.

5. Nachfolgende Empfänger
 - A. Angebot des Lizenzgebers – Lizenziertes Material. Jeder Empfänger des lizenzierten Materials erhält automatisch ein Angebot des Lizenzgebers, die lizenzierten Rechte unter den Bedingungen der vorliegenden Public License auszuüben.
 - B. Zusätzliches Angebot des Lizenzgebers – Abgewandeltes Material. Jeder, der abgewandeltes Material von Ihnen erhält, erhält automatisch vom Lizenzgeber ein Angebot, die lizenzierten Rechte am abgewandelten Material unter den Bedingungen der durch Sie vergebenen Abwandelungslicenz auszuüben.
 - C. Keine Beschränkungen für nachfolgende Empfänger. Sie dürfen keine zusätzlichen oder abweichenden Bedingungen fordern oder das lizenzierte Material mit solchen belegen oder darauf wirksame technische Maßnahmen anwenden, sofern dadurch die Ausübung der lizenzierten Rechte durch Empfänger des lizenzierten Materials eingeschränkt wird.
 6. Inhaltliche Indifferenz. Die vorliegende Public License begründet nicht die Erlaubnis, zu behaupten oder den Eindruck zu erwecken, dass Sie oder Ihre Nutzung des lizenzierten Materials mit dem Lizenzgeber oder den Zuschreibungsempfängern gemäß Abschnitt 3(a)(1)(A)(i) in Verbindung stehen oder durch ihn gefördert, gutgeheißen oder offiziell anerkannt werden.
- b. Sonstige Rechte
1. Urheberpersönlichkeitsrechte, wie etwa zum Schutz vor Werkentstellungen, werden durch die vorliegende Public License ebenso wenig mitlizenziert wie das Recht auf Privatheit, auf Datenschutz und/oder ähnliche Persönlichkeitsrechte; gleichwohl verzichtet der Lizenzgeber auf derlei Rechte bzw. ihre Durchsetzung, soweit dies für Ihre Ausübung der lizenzierten Rechte erforderlich und möglich ist, jedoch nicht darüber hinaus.
 2. Patent- und Kennzeichenrechte werden durch die vorliegende Public License nicht lizenziert.
 3. Soweit wie möglich verzichtet der Lizenzgeber auf Vergütung durch Sie für die Ausübung der lizenzierten Rechte, sowohl direkt als auch durch eine Verwertungsgesellschaft unter welchem freiwilligen oder abdingbaren gesetzlichen oder Pflichtlizenzmechanismus auch immer eingezogen. In allen übrigen Fällen behält sich der Lizenzgeber ausdrücklich jedes Recht vor, Vergütungen zu fordern.

Abschnitt 3 – Lizenzbedingungen

Ihre Ausübung der lizenzierten Rechte unterliegt ausdrücklich folgenden Bedingungen

- a. Namensnennung
1. Wenn Sie das lizenzierte Material weitergeben (auch in veränderter Form), müssen Sie:
 - A. die folgenden Angaben beibehalten, soweit sie vom Lizenzgeber dem lizenzierten Material beigefügt wurden:
 - i. die Bezeichnung der/des Ersteller(s) des lizenzierten Materials und anderer, die für eine Namensnennung vorgesehen sind (auch durch Pseudonym, falls angegeben), in jeder durch den Lizenzgeber verlangten Form, die angemessen ist;
 - ii. einen Copyright-Vermerk;
 - iii. einen Hinweis auf die vorliegende Public License;
 - iv. einen Hinweis auf den Haftungsausschluss;
 - v. soweit vernünftigerweise praktikabel einen URI oder Hyperlink zum lizenzierten Material;
 - B. angeben, ob Sie das lizenzierte Material verändert haben, und alle vorherigen Änderungsangaben beibehalten; und
 - C. angeben, dass das lizenzierte Material unter der vorliegenden Public License steht, und deren Text oder URI oder einen Hyperlink darauf beifügen.
 2. Sie dürfen die Bedingungen des Abschnitts 3(a)(1) in jeder angemessenen Form erfüllen, je nach Medium, Mittel und Kontext in bzw. mit dem Sie das lizenzierte Material weitergeben. Es kann zum Beispiel angemessen sein, die Bedingungen durch Angabe eines URI oder Hyperlinks auf eine Quelle zu erfüllen, die die erforderlichen Informationen enthält.
 3. Falls der Lizenzgeber es verlangt, müssen Sie die gemäß Abschnitt 3(a)(1)(A) erforderlichen Informationen entfernen, soweit dies vernünftigerweise praktikabel ist.
- b. Share Alike

Zusätzlich zu den Bedingungen in Abschnitt 3(a) gelten die folgenden Bedingungen, falls Sie abgewandeltes Material weitergeben, welches Sie selbst erstellt haben.

1. Die Abwandelungslicenz, die Sie vergeben, muss eine Creative-Commons-Lizenz der vorliegenden oder einer späteren Version mit den gleichen Lizenzelementen oder eine BY-SA-kompatible Lizenz sein.
2. Sie müssen den Text oder einen URI oder Hyperlink auf die von Ihnen gewählte Abwandelungslicenz beifügen. Diese Bedingung dürfen Sie in jeder angemessenen Form erfüllen, je nach Medium, Mittel und Kontext in bzw. mit dem Sie abgewandeltes Material weitergeben.
3. Sie dürfen keine zusätzlichen oder abweichenden Bedingungen anbieten oder das abgewandelte Material mit solchen belegen oder darauf wirksame technische Maßnahmen anwenden, sofern dadurch die Ausübung der Rechte am abgewandelten Material eingeschränkt wird, die Sie unter der Abwandelungslicenz gewähren.

Abschnitt 4 – Sui-generis-Datenbankrechte

Soweit die lizenzierten Rechte Sui-generis-Datenbankrechte beinhalten, die auf Ihre Nutzung des lizenzierten Materials Anwendung finden, gilt:

- a. es sei klargestellt, dass Abschnitt 2(a)(1) Ihnen das Recht gewährt, die gesamten Inhalte der Datenbank oder wesentliche Teile davon zu entnehmen, weiterzuverwenden, zu vervielfältigen und weiterzugeben;
- b. sofern Sie alle Inhalte der Datenbank oder wesentliche Teile davon in eine Datenbank aufnehmen, an der Sie Sui-generis-Datenbankrechte haben, dann gilt die Datenbank, an der Sie Sui-generis-Datenbankrechte haben (aber nicht ihre einzelnen Inhalte) als abgewandeltes Material, insbesondere in Bezug auf Abschnitt 3(b); und
- c. Sie müssen die Bedingungen des Abschnitts 3(a) einhalten, wenn sie alle Datenbankinhalte oder wesentliche Teile davon weitergeben.

Es sei ferner klargestellt, dass dieser Abschnitt 4 Ihre Verpflichtungen aus der vorliegenden Public License nur ergänzt und nicht ersetzt, soweit die lizenzierten Rechte andere Urheberrechte oder ähnliche Rechte enthalten.

Abschnitt 5 – Gewährleistungsausschluss und Haftungsbeschränkung

- a. Sofern der Lizenzgeber nicht separat anderes erklärt und so weit wie möglich, bietet der Lizenzgeber das lizenzierte Material so wie es ist und verfügbar ist an und sagt in Bezug auf das lizenzierte Material keine bestimmten Eigenschaften zu, weder ausdrücklich noch konkludent oder anderweitig, und schließt jegliche Gewährleistung aus, einschließlich der gesetzlichen. Dies umfasst insbesondere das Freisein von Rechtsmängeln, Verkehrsfähigkeit, Eignung für einen bestimmten Zweck, Wahrung der Rechte Dritter, Freisein von (auch verdeckten) Sachmängeln, Richtigkeit und das Vorliegen oder Nichtvorliegen von Irrtümern, gleichviel ob sie bekannt, unbekannt oder erkennbar sind. Dort, wo Gewährleistungsausschlüsse ganz oder teilweise unzulässig sind, gilt der vorliegende Ausschluss möglicherweise für Sie nicht.
- b. Soweit wie möglich, haftet der Lizenzgeber Ihnen gegenüber nach keinem rechtlichen Konstrukt (einschließlich insbesondere Fahrlässigkeit) oder anderweitig für irgendwelche direkten, speziellen, indirekten, zufälligen, Folge-, Straf- exemplarischen oder anderen Verluste, Kosten, Aufwendungen oder Schäden, die sich aus der vorliegenden Public License oder der Nutzung des lizenzierten Materials ergeben, selbst wenn der Lizenzgeber auf die Möglichkeit solcher Verluste, Kosten, Aufwendungen oder Schäden hingewiesen wurde. Dort, wo Haftungsbeschränkungen ganz oder teilweise unzulässig sind, gilt die vorliegende Beschränkung möglicherweise für Sie nicht.
- c. Der Gewährleistungsausschluss und die Haftungsbeschränkung oben sollen so ausgelegt werden, dass sie soweit wie möglich einem absoluten Haftungs- und Gewährleistungsausschluss nahe kommen.

Abschnitt 6 – Laufzeit und Beendigung

- a. Die vorliegende Public License gilt bis zum Ablauf der Schutzfrist des Urheberrechts und der ähnlichen Rechte, die hiermit lizenziert werden. Gleichwohl erlöschen Ihre Rechte aus dieser Public License automatisch, wenn Sie die Bestimmungen dieser Public License nicht einhalten.
- b. Soweit Ihr Recht, das lizenzierte Material zu nutzen, gemäß Abschnitt 6(a) erloschen ist, lebt es wieder auf:
 1. automatisch zu dem Zeitpunkt, an welchem die Verletzung abgestellt ist, sofern dies innerhalb von 30 Tagen seit Ihrer Kenntnis der Verletzung geschieht; oder
 2. durch ausdrückliche Wiedereinsetzung durch den Lizenzgeber.Es sei klargestellt, dass dieser Abschnitt 6(b) die Rechte des Lizenzgebers, Ausgleich für Ihre Verletzung der vorliegenden Public License zu verlangen, nicht einschränkt.
- c. Es sei klargestellt, dass der Lizenzgeber das lizenzierte Material auch unter anderen Bedingungen anbieten oder den Vertrieb des lizenzierten Materials jederzeit einstellen darf; gleichwohl erlischt dadurch die vorliegende Public License nicht.
- d. Die Abschnitte 1, 5, 6, 7 und 8 gelten auch nach Erlöschen der vorliegenden Public License fort.

Abschnitt 7 – Sonstige Bedingungen

- a. Der Lizenzgeber ist nicht an durch Sie gestellte zusätzliche oder abweichende Bedingungen gebunden, wenn diese nicht ausdrücklich vereinbart wurden.
- b. Jedwede das lizenzierte Material betreffenden und hier nicht genannten Umstände, Annahmen oder Vereinbarungen sind getrennt und unabhängig von den Bedingungen der vorliegenden Public License.

Abschnitt 8 – Auslegung

- a. Es sei klargestellt, dass die vorliegende Public License weder besagen noch dahingehend ausgelegt werden soll, dass sie solche Nutzungen des lizenzierten Materials verringert, begrenzt, einschränkt oder mit Bedingungen belegt, die ohne eine Erlaubnis aus dieser Public License zulässig sind.
- b. Soweit wie möglich soll, falls eine Klausel der vorliegenden Public License als nicht durchsetzbar anzusehen ist, diese Klausel automatisch im geringst erforderlichen Maße angepasst werden, um sie durchsetzbar zu machen. Falls die Klausel nicht anpassbar ist, soll sie von der vorliegenden Public License abgeschieden werden, ohne dass die Durchsetzbarkeit der verbleibenden Bedingungen tangiert wird.
- c. Auf keine Bedingung der vorliegenden Public License wird verzichtet und kein Verstoß dagegen soll als hingenommen gelten, außer der Lizenzgeber hat sich damit ausdrücklich einverstanden erklärt.
- d. Nichts in der vorliegenden Public License soll zu einer Beschränkung oder Aufhebung von Privilegien und Immunitäten führen, die dem Lizenzgeber oder Ihnen insbesondere aufgrund rechtlicher Regelungen irgendeiner Rechtsordnung oder Rechtsposition zustehen, oder dahingehend interpretiert werden.