Für die Mobilisierung der Economy of Things

Weeve Network

Eine Abhandlung zum Thema Token
(Teil 3/4)

Das Protokoll- und Token-Modell des Weeve Network

Sidd Bhasin und Sebastian Gajek
Weeve.network

Zusammenfassung

Es ist eine unbestreitbare Tatsache, dass Daten einen enormen Mehrwert darstellen, wenn sie tokenisiert und in einem Netzwerk eingesetzt werden, welches nach den Mechanismen und Grundsätzen einer Ökonomie funktioniert. Das Weeve Network mobilisiert die Economy of Things durch die Einführung einer Kommerzialisierungsschicht zwischen (IoT-)Geräten und der Blockchain. Im Weeve Network werden Daten von IoT-Geräten (oder „weeves“) indiziert, verarbeitet und gegen digitale Assets – wie etwa Kryptomünzen – eingelöst.
Die Vision von Weeve umfasst sowohl öffentliche als auch private Marktplätze, auf denen jede beliebige Art von digitalen Assets verkauft werden kann, so etwa Geodaten, Elektrizität oder Lieferstatus. Hier können Datenerzeuger und Datenkonsumenten (also Verkäufer und Käufer) ihr Angebot und ihre Nachfrage hinterlegen und ihre digitalen Assets zu fairen Preisen tauschen.
Um die Stabilität des Network in Anwesenheit von rationalen Spielern, die nicht unbedingt einer fairen Spielstrategie folgen, zu gewährleisten, nutzt das Netzwerk ein kryptoökonomisches Anreizmechanismus-Design. Spieler setzen ein Token ein, um für ihre Aktionen zu bürgen und so am Spiel (und damit am Netzwerk) teilnehmen zu können. Bei einer Netzwerk-Instabilität (z. B. Streit, ungerechter Austausch, Regelverstöße) kann die Community den Einsatz eines Teilnehmers anfechten. Die intrinsische Zusammensetzung des Weeve-Mechanismus-Designs gewährleistet, dass unehrliche oder unfaire Strategien durch Einsatzverlust bestraft werden und ehrliche Strategien durch Belohnungs-Mechanismen verstärkt werden.

Stichwörter: Spieltheorie, Kryptoökonomie, fairer Austausch, Stake-basiertes Mechanismus-Design, rationale Spieler

1 Einleitung

1.1 Begründung

Die IoT-Branche wächst mit schwindelerregender Schnelligkeit. Während das Marktforschungsunternehmen Gartner vor Kurzem noch prognostizierte, dass das Internet der Dinge im Jahr 2017 acht Milliarden Geräte miteinander verbinden würde, soll diese Zahl seinen neuesten Prognosen zufolge bis 2021 auf unglaubliche 28 Milliarden steigen. Damit einhergehen würde ein Anstieg des wirtschaftlichen Wertes dieses Netzwerks aus verbundenen Geräten: Bis 2025 soll hier der Umsatz auf 4–11 Billionen USD steigen.

Diese Vorhersagen beschreiben natürlich nur einen Idealfall. Damit IoT sich tatsächlich in diese Richtung weiterentwickeln kann, bedarf es einer entsprechenden Infrastruktur, auf der dieses wirtschaftliche Wachstum stattfinden kann. Denn ohne eine stabile Grundlage kann das beschriebene Potenzial nicht ausgeschöpft werden.
Blockchain-Technologien manifestieren sich seit Kurzem als ein innovatives Paradigma zur Erschaffung neuer Wirtschaftssysteme.

Diese Technologien bereiten den Weg für die vollständig automatisierte Vermarktung von Daten zwischen Geräten, und somit die Gestaltung einer Economy of Things (EoT) – einer Ökonomie der Dinge. In einer Economy of Things bieten IoT-Geräte die eigenen Daten im Namen ihrer Inhaber (Einzelpersonen, Unternehmen oder andere Rechtssubjekte) auf konzeptuellen Plattformen, sogenannten Höchstpreis- und Zweitpreis-Marktplätzen, an. Andere IoT-Geräte oder Subjekte können diese Daten ersteigern und dafür mit Kryptogeld oder anderen digitalen Assets (z. B. Austausch von Geodaten gegen Temperaturdaten) bezahlen. So könnte etwa die überschüssige Energie eines Solarpanels für eine Handvoll Kryptomünzen an ein Elektroauto verkauft werden. Über ein Strommessgerät am Solarmodul könnte die Stromentnahme nachverfolgt und durch ein elektrisches Relais gestoppt werden, sobald die vereinbarte Energiemenge transferiert wurde. Bei den verschiedenen Aktivitäten in diesem Prozess handelt es sich jeweils um Datensätze, die mit Token verknüpft werden können. Das Beispiel lässt erahnen, auf welch vielfältige Weise IoT-Geräte zukünftig oraclebasierte Blockchain-Wirtschaftssysteme befähigen könnten.

1.2 Herausforderungen

Damit eine Economy of Things sowie die Vermarktung und der Handel mit Daten überhaupt möglich sind, muss zuerst ein grundlegendes Problem gelöst werden:

> **Wie gestaltet man ein „vertrauensloses“[1] Netzwerk, in dem (anonyme) Entitäten die Regeln des Marktplatzes befolgen, dort also Nachfragen und Angebote mit fairen Preisen hinterlegen?**

---

[1] Unter „nicht vertrauenswürdig“ verstehen wir ein vollständig dezentrales, selbsttragendes Netzwerk, in dem sich Spieler gegenseitig misstrauen.

Der Erfolg von IoT-Interaktionen hängt wesentlich von der Qualität und der Herkunft der Gerätedaten ab. Nun treten bei Computern bekanntlich öfter Bugs und unerwartete Fehler auf. Und IoT-Geräte sind auch nur „einfache“ Computer mit Verbindung zum Internet, die in diesem Fall wertvolle Daten (digitale Assets) sammeln. Es muss also gewährleistet werden, dass über diese Geräte keine falschen Daten oder Daten, die nicht von den Geräten generiert wurden, angeboten werden. Falsch kalibrierten Geräten oder einer Manipulation durch unehrliche Anbieter muss demnach entgegengewirkt werden. Das ist umso wichtiger, da die Verwendung unauthentischer Daten oft schwerwiegendere Konsequenzen hat als ein Mangel an Daten. Auf einem anonymen Daten-Marktplatz, auf dem es keine Gewährleistungen ob der (kryptografischen) Geräteidentität, der Datenherkunft und der Datenintegrität gibt, könnten Käufer den angebotenen Daten allerdings nicht vertrauen.

Ein weiteres Problem bei IoT-Transaktionen ist der Mangel an einheitlichen Standards für IoT-Geräte. Eine einfache Google-Suche oder sogar ein Blick in verschiedene Branchenberichte bringt ein Wirrwarr an Protokollen und Standards ans Licht – auf dieser Basis kann keine Einheitlichkeit geschaffen werden. Weder die Marktplatz-Betreiber noch die Teilnehmer haben also eine Möglichkeit, die Zuverlässigkeit und Authentizität von Geräten und der bereitgestellten Daten zu beurteilen. Datensätzen wird – wie jeder anderen Ware auch – ein Wert zugeschrieben. Bei Daten basiert dieser Wert auf der Herkunft. Eine verlässliche Wertzuweisung kann bei einem Datensatz (oder einem kontinuierlichen Datenfluss) nur dann erfolgen, wenn die Daten vom Sensor bis zum Marktplatz zuverlässig nachverfolgt werden. Je höher das Risiko, dass die Daten auf ihrem Weg manipuliert werden, umso weniger können wir ihnen vertrauen. Dies sind Faktoren, mit denen wir Daten als digitalen Assets Wert zuschreiben.

1.3 Eine Übersicht des kryptoökonomischen Token-Mechanismus von Weeve

In Netzwerken mit mehreren Spielern verfolgen individuelle Akteure unterschiedliche Strategien, mit der Absicht, ihren persönlichen Nutzen zu vergrößern. Wann immer finanzielle Anreize mit im Spiel sind, ist die Wahrscheinlichkeit groß, dass einige Teilnehmer unfair spielen und sich nicht an die Regeln halten. Jemand könnte sich beispielsweise als legitimer Datenanbieter ausgeben, jedoch gefälschte Daten anbieten, und so das System für die eigenen Zwecke ausnutzen. Es besteht auch das Potenzial für Plagiate, Markenfälschungen und Patentrechtsverletzungen und die Entwicklung eines Schwarzmarktes. Diese Art von Problemen tritt unweigerlich in Systemen auf, die mit schlecht durchdachten Anreiz-Strategien unbeabsichtigt ein fehlerhaftes Verhalten fördern.

Entgegenwirken kann man diesem Verhalten, indem man ein robustes Netzwerk aufbaut, das Teilnehmern einen Anreiz gibt, sich fair zu verhalten und die Integrität des Systems aufrechtzuerhalten. Aus diesem Grund bedient sich das Weeve Network der Grundsätze der Kryptoökonomie – einer der bemerkenswerten Einsatzmöglichkeiten der modernen Blockchain-Technologien. Das Weeve Network setzt Marktplatz-Anwendungen und relevante Services zur Registrierung von Geräten, Asset-Validierung und Konfliktlösung auf die Blockchain auf. Die Blockchain bietet uns dabei zum einen eine Werteinheit, mit der Wert übertragen wird und sowohl positive als auch negative Anreize ausgegeben werden und zum anderen ein Toolkit zur Entwicklung von Prozessen mit bedingter Logik in Form von „Smart Contracts“ (intelligenten Verträgen). Fest verankert in der Blockchain erstellt das Weeve Network ein System aus Anreizen, das Teilnehmer kontinuierlich dazu motiviert, zur Aufrechterhaltung von Marktplätzen mit qualitativ hochwertigen Daten beizutragen.

Die Verwalter solcher Marktplätze müssen demnach eine Sicherheit in Form von Token hinterlegen, mit der sie für die hohe Qualität von Angebot und Nachfrage bürgen. Das Weeve-Network-Protokoll ermöglicht es Besitzern von Token, die Handlungen der Marktplatz-Verwalter anzufechten. Fällt ein Verwalter durch eine solche Prüfung durch, verliert er die als Sicherheit hinterlegten Token. Diese werden dann als Belohnung an die Token-Inhaber verteilt, die am Prüfungsprozess beteiligt waren. Ein ähnlicher Mechanismus wird im Weeve Network angewandt, um Geräte-Inhaber dazu zu motivieren, einen hohen Mitgliedsstandard zu erreichen, indem sie nur hochwertige Daten bereitstellen (und keine gefälschten Datenstreams). Geräte-Inhaber, die an einem Marktplatz teilnehmen möchten, müssen zunächst in ein Geräteregister eingetragen werden. Jedes Register steht dabei für einen Mitgliedsstandard, den das Gerät erfüllen muss. Diese Register haben indirekt auch die Aufgabe, die Qualität der Daten zu evaluieren. Kandidaten müssen eine im intrinsischen Token des Registers festgelegte Sicherheit hinterlegen, um sich überhaupt für die Aufnahme in dieses Register zu qualifizieren. Token-Inhaber können eine Prüfung des Geräts veranlassen. Wird das Gerät anschließend als „gut“ bewertet und in die Liste aufgenommen, verliert der Inhaber seine Sicherheit nicht und er kann sie jederzeit einlösen, wenn er das Register wieder verlassen möchte.

Mit diesen Anreiz-Mechanismen soll von vornherein verhindert werden, dass Geräte, welche nicht die Mitgliedsstandards erfüllen, welche keine authentischen Daten generieren oder welche die Netzwerk-Verhaltensregeln nicht befolgen, sich überhaupt bei diesen Registern bewerben. Bei einer Bewerbung würden diese nämlich einen finanziellen Verlust riskieren. Darüber hinaus haben auch Marktplatz-Verwalter einen Anreiz, echte Angebote und Nachfragen qualitativ hochwertiger Daten bereitzustellen, eine faire Preissetzung für beide Seiten durchzusetzen und bei Regelverletzungen moderierend einzugreifen. Andernfalls würden auch sie den Verlust ihrer Stakes riskieren.

2 Die Vision von Weeve

Weeve hat sich zum Ziel gesetzt, die Economy of Things zu mobilisieren. In dieser Ökonomie der Dinge werden Daten von IoT-Geräten (oder weeves) indiziert, verarbeitet und gegen digitale Assets – wie etwa Kryptomünzen – eingelöst. Unsere Vision umfasst sowohl öffentliche als auch private Marktplätze, auf denen jede beliebige Art von digitalen Assets verkauft werden kann, so etwa Geodaten, Elektrizität oder Lieferstatus. Hier können Datenerzeuger und Datenkonsumenten (also Verkäufer und Käufer) ihr Angebot und ihre Nachfrage hinterlegen und ihre digitalen Assets zu fairen Preisen tauschen.

2.1 Die Ziele des Network-Designs

Mit dem Weeve Network beabsichtigen wir, eine Vertrauensbasis zwischen Geräten zu schaffen und die Weiterentwicklung und Anwendung von neuen Standards zu kultivieren, welche die Grundlage neuer Marktplätze für den fairen Handel von Assets zwischen IoT-Geräten darstellen sollen.

2.1.1 Die Qualität der Daten

Das primäre Ziel des Netzwerks ist die Gewährleistung der Datenqualität auf dem Marktplatz. Um die Datenqualität zu bestimmen, werden verschiedene Faktoren hinzugezogen: etwa die Reputation und die Authentizität der Entität, die diese Daten generiert; die Sicherheitsmaßnahmen, die während der Erfassung, der Verarbeitung und der Übermittlung der Daten getroffen werden; oder die Validierung durch vertrauenswürdige Drittparteien. Alternativ kann die Qualität der Daten auch durch ein demokratisch gewähltes Quorum bestimmt werden. Diese Mechanismen dienen der Authentifizierung der Daten. Eine der größten Barrieren, die eine umfangreichere Teilnahme an der EoT bislang verhindert hat, ist die Datenauthentifizierung. Weeve wird dieses Hindernis aus dem Weg räumen und damit eine Economy of Things ermöglichen, die auf zuverlässigen, authentischen Informationen basiert. Geräte werden dann mit Zeugnissen versehen, die ihnen verschiedene Eigenschaften belegen, wie etwa Besitzverhältnis des Geräts, Prüfhistorie und Ergebnisse automatischer Testdurchläufe in Echtzeit. Durch solche kontextschaffende Dokumentation wird die ordnungsgemäße Ausführung von Dienstleistungsvereinbarungen im Netzwerk gewährleistet. Diese Betrugsvorbeugung verbessert die Marktsicherheit und ermöglicht Teilnehmern zuversichtlich mit ihren digitalen Assets zu handeln.

2.1.2 Die Stabilität des Netzwerks

Wirtschaftsmärkte basieren auf der Annahme, dass alle Teilnehmer rational agieren[2]. Auf dem Weeve-Markt ist das nicht anders. Weeve-Spieler handeln immer auf eine Art, die ihren Nutzen maximiert.

Ein rationaler Spieler handelt nicht notwendigerweise im besten Interesse des gesamten Netzwerks. Im Gegenteil: Er ist egoistisch, unfair, und zögert nicht, andere Spieler zu betrügen. Diese Aktionen sind für das Netzwerk von entscheidender Bedeutung, da sie es destabilisieren können. Ist das Netzwerk instabil, sind Angebot und Nachfrage mangelhaft: Käufer könnten potenziell gefälschte oder überteuerte Daten erstehen, und Verkäufern würde jegliche Grundlage dafür fehlen, höhere Preise zu verlangen.

Im Weeve Network wird anhand von Marktmechanismen ein Gleichgewicht zwischen den Hauptakteuren und wichtigen Marktkräften hergestellt. Bei gutem Marktgleichgewicht verfolgt jeder Weeve-Spieler eine Nutzen-maximierende Strategie. Der Mechanismus des Weeve Network folgt einer Trigger-Strategie: Spieler, welche die Stabilität des Netzes unterstützen, werden dafür belohnt, während Spieler, die das Netzwerk sabotieren, bestraft werden. Dieser Belohnungsmechanismus gibt Spielern einen überzeugenden Anreiz dafür, dem Netzwerk beizutreten, mit Daten zu handeln und mit ihrem Wissen und ihrem Engagement zur Stabilität des Network beizutragen. Ohne geeignete Anreizmechanismen hat das Netzwerk keinen eigenständigen Antrieb. Marktplätze können aufgrund mangelnder Nachfrage und unzureichendem Angebot nicht florieren. Der Strafmechanismus wiederum wirkt Strategien entgegen, mit denen das

---

[2]Im Gegensatz zu Menschen, die manchmal irrational handeln, besteht das Weeve Network aus Maschinen, die meistens ein rechnerisches Mechanismus-Design ausführen. Da der Mechanismus als Protokoll implementiert ist und per Code fest in das Gerät integriert wird, sind irrationale Abweichungen unwahrscheinlich.

Network destabilisiert werden soll. Destabilisierungsstrategien wird durch negative Anreize vorgebeugt. Bestraft werden die jeweiligen Spieler durch Verluste.

2.1.3 Dezentrale Standards mit Community-Governance

Um eine umfangreiche Nutzung des Network zu ermöglichen, wird vorausgesetzt, dass sich Spieler verschiedenster Art, unabhängig der verwendeten Technologien (zumindest in der anfänglichen Bootstrapping-Phase des Netzwerks), mit dem Netzwerk verbinden können. Betreiber der Marktplätze haben die Möglichkeit, Interoperabilitäts- und Glaubwürdigkeitsstandards festzulegen; somit kann der Markt sich dezentral selbst regulieren.

Regulatorische Rahmenwerke können oft mit der kontinuierlichen technologischen Innovation nicht mithalten. Deshalb sind flexible Standards, die von der Community verwaltet werden, äußerst wichtig. IoT-Geräte werden von Unternehmen entwickelt, um bestimmte Zwecke zu erfüllen. Damit die verschiedenen Unternehmen für eine Interoperabilität zwischen den eigenen und anderen Geräten sorgen können, müssen sie den gleichen Standards und Verfahren folgen. Durch die (kryptografische) Durchsetzung dieser Standards erhalten Geräteinhaber einen wirtschaftlichen Anreiz, die gleichen Standards anzuwenden.

Durch Governance werden relevante Mitgliedschaftsstandards festgelegt und regelmäßig angepasst. Dadurch dass die eigentlichen Nutzer dieser Standards deren Form bestimmen können, werden Weeve-Network-Teilnehmer von kürzeren Feedback-Zyklen für Vorschläge und Beratungen in der Gruppe profitieren. Anstatt dass internationale Normungsgremien neue, übergreifende Standards bestimmen, entstehen neue Standards in kleineren, schnelllebigen Marktplätzen. Die flexible, kontinuierliche Anpassung dieser Standards trägt nebenbei auch zur stetigen Verbesserung der Datenqualität und Netzwerkstabilität bei.

2.1.4 Verfahren zur Streitbeilegung

Konflikte sind ein natürliches Phänomen in jeder Wirtschaft. So kann beispielsweise eine Streitigkeit entstehen, wenn ein Käufer behauptet, dass eine erstandene Ware nicht vom Verkäufer geliefert wurde. Für die Beilegung von Streitigkeiten gibt es drei mögliche Strategien. Bei einer Mediation etwa soll eine unbeteiligte Drittpartei den Streitparteien helfen, eine Lösung für ihr Problem zu finden.
Anstatt dass den Parteien eine Lösung aufgezwungen wird, werden bei der Mediation zunächst die einzelnen Standpunkte berücksichtigt. Bei einem Schiedsverfahren wiederum dient eine neutrale dritte Partei als Schiedsrichter, der für die Beilegung der Streitigkeit[3] verantwortlich ist. Der Schiedsrichter begutachtet alle Beweismittel und trifft dann eine verbindliche Entscheidung. Die dritte – und bekannteste – Art der Streitbeilegung ist die Prozessführung. Dabei stehen sich in der Regel ein Angeklagter und ein Kläger gegenüber, die ihren Fall vor einem Richter oder einer Jury vorbringen. Der Richter oder die Jury muss die Beweise abwägen und eine bindende Entscheidung treffen.
Die Teilnehmer des Weeve Network können für die Streitbeilegung auf die Hilfe von Schiedsrichtern zurückgreifen, sofern kein automatisierter Konsens durch ein (sagen wir mal) Konfliktbeilegungsprotokoll erreicht werden konnte. Es wäre auch möglich, ein gerichtliches

[3] z. B. https://jury.online/arbitration.

Verfahren für die Streitbeilegung anzustrengen. Die Blockchain-Technologien bieten eine interessante Infrastruktur für die Implementierung einer verteilten Prozessführung. Im Rahmen des Weeve Network soll das Potenzial einer solchen Streitschlichtung auch künftig gegeben sein.

2.2 Netzwerk-Teilnehmer und Knoten-Verwalter

Als einfaches Modell setzen wir eine endliche Menge an Knoten N = {1,…, n}, die mit dem Netzwerk (oder dem Graphen) verbunden sind. Ein Netzwerk ist ein Paar (N, g), wobei g die Paarmenge der Knoten ist. g sei eine der Standarddarstellungen von Netzwerken: durch ihre Adjazenz-Matrizen sowie durch die Auflistung der miteinander verbundenen Knotenpaare. Jeder Knoten repräsentiert einen Spieler (oder eine Menge davon) im Netz, der den Knoten besitzt, kontrolliert oder verwaltet (siehe Abb. 1).

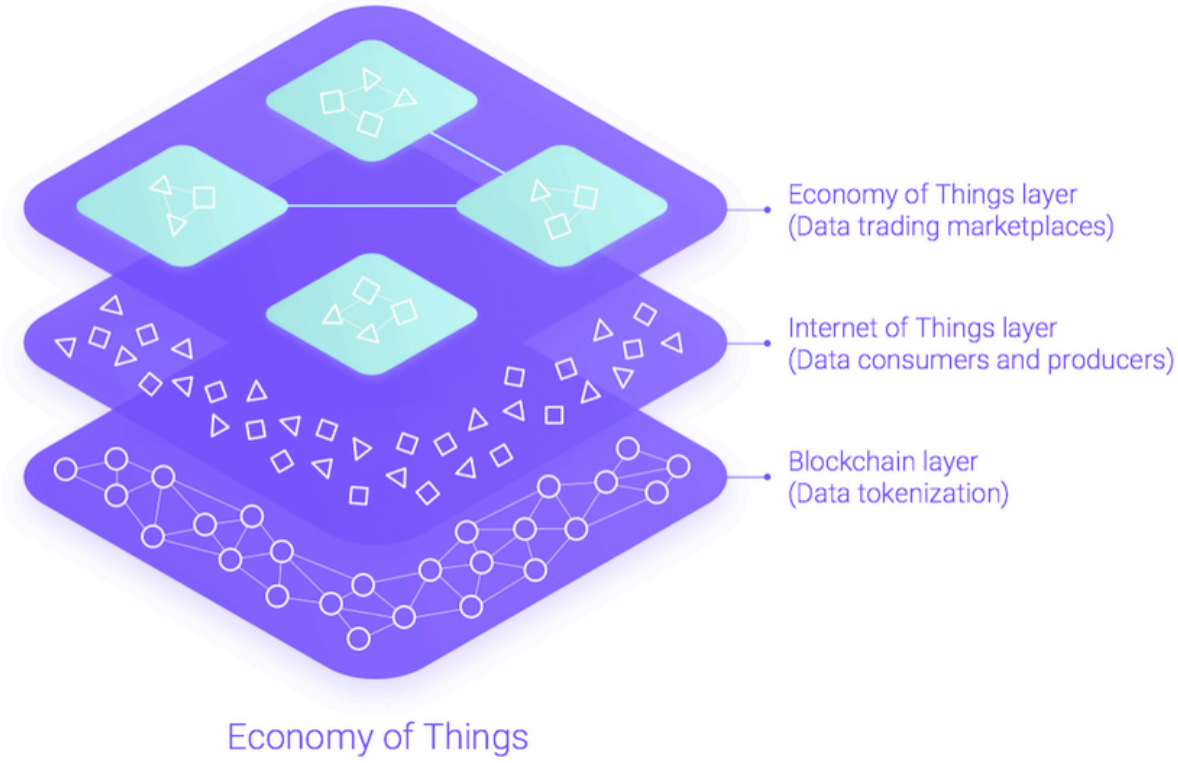

Abbildung1: Das Weeve Network, bestehend aus Datenerzeugern und -konsumenten, Marktplätzen, Validatoren und Schiedsrichtern.

2.2.1 Knoten

Jeder Knoten im Weeve Network stellt eine der folgenden Grundfunktionen, vorbehaltlich künftiger Änderungen (siehe Abschnitt 5), dar, wie in Abb. 2 zusammengefasst:

Geräteknoten sind Quellen und/oder Empfänger von digitalen Assets. In seiner einfachsten Form ist ein Geräteknoten ein IoT-Ding, welches Assets anbietet oder anfordert. Im Allgemeinen handelt es sich um ein beliebiges Computergerät, das im Weeve Network Ressourcen anbietet oder anfordert. Wir werden mitunter Verkäufer als Geräte bezeichnen, welche Assets bereitstellen, und Käufer als

Geräte, die Assets anfordern. Ein Asset ist jede beliebige Form tokenisierter Daten, die potenziell einen Wert haben.

Registerknoten verwalten Informationen zu den Eigentumsverhältnissen und Eigenschaften von Geräten. Ihre Aufgabe im Weeve Network besteht darin, die Identifizierung und Klassifizierung von Geräten zu ermöglichen. Bei einem Register handelt es sich um eine Auflistung von Geräten, die bestimmten Mitgliedschaftsstandards entsprechen. Durch diese Standards werden verschiedene Kriterien festgelegt, nach denen Geräte evaluiert werden, etwa Geräte-Identität, Identität des Geräte-Inhabers, kompatible Protokolle, Transaktionsstrategien und Gerätefunktionen.

Marktplatz-Knoten schaffen einen Ort für die wirtschaftliche Interaktion. Ein Markt ist ein Medium, das Käufern und Verkäufern ermöglicht, bezüglich eines spezifischen Produkts oder einer Dienstleistung zu interagieren, und das so den Verkauf erleichtert. Bei den Produkten und Dienstleistungen im Weeve Network handelt es sich in erster Linie um tokenisierte Daten.

Geräte-Inhaber: Handeln im Netzwerk gegen Zahlung einer Gebühr.

Register-Inhaber: Zuständig für die Unterbreitung und Durchsetzung von geeigneten Registerregeln wie etwa Mitgliedschaftsstandards, Registergebühren, Validierungskriterien und Schlichtungsrichtlinien.

Marktplatz-Inhaber: Zuständig für die Unterbreitung und die Verwaltung der Teilnahmeregeln wie etwa Gerätestandards, Registergebühren, Validierungskriterien und Schlichtungsrichtlinien.

Validatoren: Zuständig für die Überprüfung und Durchsetzung von Mitgliedschaftsstandards, gegen Erhalt einer Gebühr.

Schiedsrichter: Zuständig für die Beilegung von Streitigkeiten, gegen Erhalt einer Gebühr.

Abbildung 2: Übersicht der wichtigsten Akteure im Weeve Network

Validierungsknoten erfüllen eine prüfende Funktion im Weeve Network. Die Aufgabe der Validierungsknoten ist es, Geräteregister- und Marktplatz-Knoten bei der Geräteklassifizierung zu unterstützen. Validierungsknoten sind Prüfer, welche die Geräte-Eigenschaften entsprechend der Mitgliedschaftsstandards evaluieren und zertifizieren. Sie bestimmen die Marktplatzeignung von Geräten.

Schiedsrichter-Knoten sind verantwortlich für die Beilegung von Streitigkeiten im Weeve Network.

2.2.2 Verwalter und Governance

Knoten übernehmen wesentliche Funktionen des Weeve Network. In der Praxis gehört jeder der oben genannten Knoten einem Rechtssubjekt und wird von diesem verwaltet und organisiert. Es kann sich bei einem Subjekt um eine Privatperson, ein Unternehmen, eine Regierung, eine gemeinnützige Organisation oder eine beliebige Untergruppe davon handeln. Ein Knoten kann nicht nur durch die Aktionen des Subjekts agieren, sondern auch durch einen Smart Contract, Webserver oder eine andere programmierbare Schnittstelle. Diese flexible Herangehensweise ermöglicht vielfältige Implementierungsmöglichkeiten – von der vollständigen Zentralisierung bis zur vollständigen Dezentralisierung. Unternehmen könnten etwa ihre Knoten zentral kontrollieren, während Gemeinschaften oder Konsortien einen verteilten Ansatz wählen könnten. Die Einzelheiten des jeweiligen Governance-Systems sind dem Inhaber des Knoten überlassen, vorbehaltlich der Zustimmung des Verwalters/der Verwalter des Knotens. Zum Zwecke einer vereinfachten Darstellung gehen wir davon aus, dass das Weeve Network aus den folgenden primären Verwaltern besteht (siehe Abb. 1):

- Register-Inhaber verwalten Geräteregister und definieren einen Community-Standard, um die Reputation der Geräte-Inhaber und die für die Aufnahme in das Register geltenden Kriterien zu evaluieren. Diese Kriterien reichen von weichen Faktoren wie Einsatzbetrag, frühere Registerhistorien, Reputation des Geräteherstellers, bis zu harten Faktoren wie einer eindeutigen kryptografischen ID, Support für Hardware/Software mit hohen Sicherheitsgarantien. Sie definieren zudem die Kriterien für das Entfernen eines Geräts aus dem Register sowie ein Protokoll zur Beilegung von Streitigkeiten mit Hilfe von Validatoren und Schiedsrichtern.

- Geräte-Inhaber, die am Weeve Network und -Marktplatz teilnehmen möchten, müssen zunächst in das Geräteregister aufgenommen werden. In einem Register können Benutzer die Eigenschaften eines Geräts nachschlagen und den Besitzer des Geräts identifizieren. Um in ein Geräteregister aufgenommen zu werden, müssen Geräte-Inhaber sicherstellen, dass ihre Geräte den Mitgliedschaftsstandards entsprechen, die für das jeweilige Register gelten. Die Aufnahme setzt eine Evaluierung der Mitgliedschaftseignung durch einen vom Register ernannten Validator voraus.

- Marktplatz-Inhaber sind für die Verwaltung von Marktplätzen verantwortlich. Ähnlich wie Register-Inhaber definieren sie die Standards, um die Reputation der Geräte-Inhaber und die Qualität der auf dem Markt gehandelten Assets zu evaluieren. Zu diesem Zweck definieren sie die Kriterien für die Aufnahme von Geräten und für die Evaluierung der Assets, die Geräte anbieten oder anfordern. Sie definieren auch die Standards für das Entfernen von Geräten vom Marktplatz und bestimmen die Schiedsrichter, die Streitigkeiten zwischen Geräten oder konkurrierenden Marktplätzen beilegen sollen. Neben der Verwaltung der Geräte übernehmen die Verwalter der Marktplätze auch die Definition der Parameter zur Einrichtung des Markts, darunter beispielsweise die Art von Daten, mit denen

gehandelt werden kann, der Mechanismus zur Preisfestlegung, das ihrem Geschäftsmodell entsprechende Gebührenmodell (z. B. pro Gerät, pro Transaktion) und die Zahlungsmethode.

- Validatoren werden von Geräteregistern ernannt und prüfen die Einhaltung der Mitgliedschaftsstandards. Ihre Rolle besteht darin, sicherzustellen, dass nur vertrauenswürdige, hochwertige Geräte auf den Marktplätzen Transaktionen durchführen können. Das Weeve Network delegiert die Ernennung von Validatoren und ihrer Prozesse an die Register-Inhaber.

- Schiedsrichter legen Streitigkeiten bei. Geräteregister oder Marktplätze ermächtigen Schiedsrichter dazu, Streitigkeiten bezüglich bestimmter Transaktionsarten beizulegen. Für registerübergreifende Transaktionsarten müssen alle beteiligten Register gemeinsame Schiedsrichter bestimmen.

Bei Netzwerk-Verwaltern kann es sich um verschiedene Entitäten handeln – von einzelnen Privatpersonen zu einer Allianz von juristischen Personen. In bestimmten Fällen kann eine einzige Entität auch verschiedene Verwalter-Rollen übernehmen. Ein Automobilhersteller kann zum Beispiel gleichzeitig eine Autoflotte und ein Register für die Autos verwalten. Diese Hersteller können daher in die Register verschiedener Marktplätze aufgenommen werden (etwa Parkplätze verschiedener Betreiber), solange die Autos die Marktplatz-Mitgliedschaftsstandards erfüllen. Wir verweisen den Leser auf unsere Abhandlung zu den Anwendungsfällen für eine detailliertere Auseinandersetzung mit dem Thema [1].

3 Protokolle und Token des Weeve Network

3.1 Mechanismus-Design

Mechanismus-Design ist ein Bereich der Wirtschaftswissenschaften, der sich der Untersuchung positiver und negativer Anreiz-Mechanismen widmet. Blockchains gewährleisten, dass unter Verwendung von Kryptographie und richtig angeglichenen Anreizen sichere Konsens-Protokolle entworfen werden können. Blockchains haben jedoch noch weitaus größeres Potenzial, welches etwa bei der Gestaltung von (Sicherheits-)Protokollen und Anwendungen noch nicht im vollen Maße erforscht wurde. Für das Weeve Network ist die Blockchain ein Basis-Layer-Protokoll, das nicht nur die Technologie für die Übertragung von Kryptomünzen darstellt –
oder allgemeiner ausgedrückt das Speichern von Einträgen in einer vollständig verteilten, öffentlichen Datenbank –, sondern auch eine Infrastruktur für auf Anreizen basierende Protokolle bereitstellen kann.

3.1.1 Die Grundsätze der auf Token basierenden Entscheidungsfindung

Die Blockchain bietet die Grundlage für die Verwendung von Token. Es ist erst im Rahmen der Blockchain, dass Token sinnvoll eingesetzt werden können. Der Anstieg der Token-Menge wird allgemein als Belohnung anerkannt, während die Abnahme der Token-Menge als Strafe angesehen wird. Mithilfe des Belohnungsmechanismus werden Anreize für „gute“ Taten gegeben und mit dem

Bestrafungsmechanismus soll „schlechten“ Handlungen vorgebeugt werden. Obwohl dieser Mechanismus in seiner Ausführung recht simpel ist, bildet er dennoch die Grundlage für ein kryptoökonomisches Anreiz-Design. Proof-of-Stake-Konsens-Protokolle wie Casper scheinen dafür anscheinend die gängigsten Anwendungsfälle. Die zentrale Idee kann wie folgt beschrieben werden: Spieler setzen, um für ihre Aktionen zu bürgen, Token ein, und das Protokoll ermöglicht jedem, die Aktionen anderer Spieler (und somit deren Stake) anzufechten. Konkret bedeutet das, dass laut Protokoll der Stake eines Spielers zeitweilig unzugänglich wird, die Anfechtung angekündigt und eine Abstimmung in der Community initiiert wird, bei der jeder Wähler für seine Stimme mit einer Anzahl an Token proportional zum Stake bezahlt. Die Wähler, die gewinnen, teilen sich die Belohnung, bei der es sich um ein zum Stake der Wähler, die verlieren, proportionaler Betrag handelt.

3.1.2 Quadratic Voting: Wieso Teilnehmer mit mehrheitlichem Stake nicht die Kontrolle über das Network gewinnen

Das zuvor beschriebene (Abstimmungs-)Protokoll ist ein Beispiel für eine auf Token basierende Mehrheitsentscheidung. Bei Abstimmungen mit Mehrheitsregel, bei denen jeder Wähler nur eine einzige Stimme hat, hat jeder Teilnehmer eine gleichwertige Chance, das Endergebnis zu beeinflussen. Es gibt allerdings auch Entscheidungen,
bei denen eine Mehrheitsregelung nicht die beste Wahl ist, da sie zu einer Tyrannei der Mehrheit führen würde. Zudem könnten einige Wähler von einer Teilnahme am Protokoll ausgeschlossen werden, wenn sie die nötige Anzahl an Token nicht kaufen können. Vor allem wenn der als Token dargestellte Reichtum ungleich verteilt ist, kann sich leicht eine große Anzahl von Token-Inhabern, die nur mäßig an dem Ergebnis einer Abstimmung interessiert ist, gegen eine Minderheit durchsetzen, die leidenschaftlich an dem Thema interessiert ist. Dies führt zu einer Verringerung des allgemeinen Wohles.

Quadratic Voting ist die bedeutendste Idee für die Gesetzgebung und die öffentliche Ordnung, die in den letzten zehn Jahren aus der Wirtschaft entsprungen ist. Jeder Wähler kann gegen die Zahlung einer Token-Menge in Höhe des Quadrats der Anzahl an gekauften Stimmen für oder gegen einen Vorschlag abstimmen. Der Einsatz wird anschließend auf Pro-Kopf-Basis an die Wähler rückerstattet. Weyl und Lalley haben in diesem Zusammenhang bewiesen, dass sich die kollektive Entscheidung mit der steigenden Anzahl an Wählern schnell der Effizienz nähert [2]. Weyl hat weiterhin bewiesen, dass Quadratic Voting recht widerstandsfähig gegenüber Absprachen, Betrug und „irrationalem“ Wählerverhalten ist – einige Eigenschaften, welche die Mehrheitsabstimmung nicht bieten kann [3].

Das Weeve Network erachtet Quadratic Voting (oder Varianten davon wie Cubic oder Exponential Voting) als ein wesentliches Instrument bei auf Token basierenden Entscheidungsfindungen, vor allem in Wirtschaftssystemen, in denen eine gleichmäßige Verteilung der Token unwahrscheinlich ist. Das wäre etwa der Fall, wenn Akteure wie Unternehmen oder Branchenallianzen eine erhebliche Menge des Stakes halten. (In Extremfällen hielten sie mehr als 51 % der gesamten Token-Menge der Wählerschaft). Verwalter des Weeve Network können selbst die Abstimmungsregel wählen, die am besten für ihre Community geeignet ist und ihrem Verständnis eines demokratischen Entscheidungsprozesses entspricht.

3.1.3 Ein Anreiz-Mechanismus für die Erzeugung qualitativ hochwertiger Daten

Das Weeve Network hält Gerätebesitzer dazu an, ihre Geräte mit großer Sorgfalt und Gewissenhaftigkeit zu verwalten. Geräte sind das Herzstück des Weeve Network. Immerhin sind sie die Erzeuger und Konsumenten von digitalen Assets und verantwortlich für die kontinuierliche Bereitstellung von Angebot und Nachfrage. Geräte-Inhaber haben einen inhärenten Anreiz, dem Weeve Network beizutreten: Erzeuger können hier ihren gewinnorientierten Tätigkeiten nachkommen, während Konsumenten Assets kaufen können, nach denen sie gesucht haben. Marktplätze sind der beste Ort, um diese Interessen erfolgreich zu verfolgen. Um den Betrieb der Marktplätze zu erleichtern und den Austausch der Daten zu begünstigen, umfasst das Weeve Network Marktplätze mit verschiedenen Asset-Themen (z. B. Geodaten, Temperaturdaten), Datenqualitätsmerkmalen und Teilnahmevoraussetzungen.

Der Grundsatz des Weeve Network besagt, dass teilnehmende Geräte in einem Register aufgenommen werden müssen,
welches die Mitgliedschaftsstandards des jeweiligen Marktplatzes erfüllt. Wenn das Gerät in einem Register aufgeführt ist, kann es sich mit allen Marktplätzen verbinden, welche die Standards dieses Registers oder eine Teilmenge davon unterstützen. Diese Design-Entscheidung wurde getroffen, um das Zusammenwirken von Geräten zwischen verschiedenen Marktplätzen zu begünstigen. Geräte haben Zugang zu Marktplätzen mit ähnlichen Standards und können dort mit anderen Geräten interagieren. Auf diese Weise findet das Konzept eine allgemeinere und leistungsstärkere Anwendung.

Geräte-Inhaber haben daher großes Interesse daran, auf qualitativ hochwertigen Registern aufgeführt zu werden. Durch eine Aufnahme in „guten“ Registern können Inhaber an qualitativ hochwertigeren Marktplätzen teilnehmen, wo digitale Assets voraussichtlich zu höheren Preisen gehandelt werden. Um in ein solches Register aufgenommen zu werden, unterziehen sich Inhaber einer auf Token basierenden Entscheidungsfindung. Das heißt, sie setzen Token ein, um ihre Geräte gegen die Mitgliedschaftsstandards und Register-Richtlinien evaluieren zu lassen.

Bei den anderen Teilnehmern dieser Wahl handelt es sich um die Validatoren. Diese werden entsprechend der Register-Richtlinien nominiert. Wer als Validator agieren kann, hängt von der Art des Registers ab. Es kann sich etwa um bekannte Entitäten, individuelle Token-Inhaber oder Register-Inhaber handeln. Validatoren haben die Aufgabe, die Compliance der Geräte mit den Mitgliedschaftsstandards des Registers zu prüfen. Ihnen ist ein doppelter Anreiz dafür gegeben, an einer auf Token basierenden Entscheidungsfindung teilzunehmen. Sie werden erstens für die Teilnahme durch einen Anteil am Stake des Inhabers entlohnt. Zudem möchten Validatoren sicherstellen, dass die Nachfrage für ihr Token hoch bleibt, da dadurch auch dessen Preis steigt. Um das zu gewährleisten, müssen sie für ein stabiles Netzwerk mit qualitativ hochwertigen Registern und Geräten sorgen.

Verschiedene Geräte-Inhaber können anhand der festgelegten Standards selbst erkennen, ob ihre Geräte eine Chance haben, in das entsprechende Register aufgenommen zu werden. Stehen die Chancen schlecht, werden die Inhaber keine Aufnahme beantragen, da sie sonst finanzielle Verluste riskieren. Fällt ein Inhaber durch eine Prüfung seines Gerätes durch, verliert er die als Sicherheit hinterlegten Token. Diese werden dann als Belohnung an die Token-Inhaber verteilt, die am

Prüfungsprozess beteiligt waren. Bei einer erfolgreichen Prüfung würde der Einsatz des Geräte-Inhabers solange einbehalten, bis dieser sich dazu entscheidet, das Register wieder zu verlassen.

3.1.4 Ein Anreiz-Mechanismus für Geräteregister mit hohen Standards

Geräteregister sind ein zentrales Element des Netzwerks. So schaden etwa Register mit (vielen) schlechten Geräten der Netzwerkstabilität. Es wurde deshalb besonderen Wert darauf gelegt, dass das Mechanismus-Design des Weeve Network ordentliche Geräteregister hervorbringt.

Für die Erstellung eines neuen Registers müssen die zukünftigen Register-Inhaber einen Stake proportional zu der Anzahl der registrierten Geräte hinterlegen. Im Allgemeinen kann jeder Token-Inhaber Register erwirken. Da qualitativ hochwertige Register eine erhebliche Menge an Token benötigen, sind Register zunächst ein Instrument
für Unternehmen oder Allianzen von Token-Inhabern. Wie in größeren Interessengruppen üblich werden Entscheidungen auf demokratische Weise getroffen. Die Wahl dieser Methode basiert auf der Annahme, dass eine Mehrheit von Register-Inhabern schlechten Verwaltern zahlenmäßig überlegen ist. Ein weiterer Anreiz für Register-Inhaber, „gute“ Register zu organisieren, leitet sich davon ab, dass ihr Stake als Sicherheit eingesetzt wird, wenn auf Token basierende Entscheidungsfindungen abgehalten werden.

Gibt es Hinweise auf eine Verletzung der Mitgliedschaftsstandards, können Register-Inhaber von Marktplätzen infrage gestellt werden, die mit dem Register in Verbindung stehen. Im Wesentlichen liegt eine Mitgliedschaftsverletzung vor, wenn sich herausstellt, dass ein registriertes Gerät gefälschte Daten produziert. In der Praxis müssen Marktplatz-Inhaber allgemeinere Bedingungen für solche Verstöße festlegen. Token-Inhaber, einschließlich Register-Inhaber, haben die Möglichkeit, andere Register anzufechten. Damit soll jede Form von Regelverstoß verhindert werden. Nehmen wir an, jede Form von Geräte- oder Daten-Plagiat, wie Markendiebstahl, Markenpiraterie und Patentrechtsverletzung tritt als Folge eines „schlechten“ Registers auf. Dadurch, dass alle Teilnehmer die Möglichkeit haben, Register anzufechten, erhalten Inhaber gefälschter Register den negativen Anreiz eines finanziellen Verlustes (ihres Stakes).

Bleibt uns nun noch zu erläutern, welchen positiven Anreiz die Verwaltung eines Registers bietet – immerhin laufen Inhaber stets die Gefahr, ihren Stake zu verlieren. Register-Inhaber bestimmen selbst, nach welchen Kriterien und mit welcher Strenge die Durchsetzung der Mitgliedschaftsstandards erfolgt, indem sie Anträge von Geräten entweder annehmen oder ablehnen. Register-Inhaber haben einen Anreiz, für ein qualitativ hochwertiges Netzwerk zu sorgen, da dadurch die Nachfrage für ihr Token hoch bleibt, und dessen Preis steigt.

3.1.5 Ein Anreiz-Mechanismus für die Verwaltung fairer Marktplätze

Angesichts der Tatsache, dass Marktplätze – abhängig von dem jeweiligen Geschäftsmodell – eine Gebühr für jeden erfolgreich abgeschlossenen Deal mit digitalen Assets erhalten, ist die Möglichkeit finanzieller Einnahmen natürlich ein überzeugender Anreiz für die Verwaltung und Organisation von Marktplätzen. Um einen Markt zu betreiben, hinterlegen Marktplatz-Inhaber

eine Kaution. Dieser Stake ist eine Sicherheitskaution und wird in auf Token basierenden Entscheidungsfindungen eingesetzt, um Anreize für die Inhaber zu schaffen, einen fairen Handel zu gewährleisten. Geräte, die digitale Assets austauschen, können den Marktplatz im Streitfall anfechten. Ein „bösartiger“ Marktplatz kann die Verfügbarkeit von qualitativ hochwertigen Daten simulieren, aber in Wirklichkeit minderwertige Daten von Geräten anbieten, die den vorgeschlagenen Mitgliedschaftsstandards nicht gerecht werden. Ebenso könnte ein „schlechter“ Marktplatz den Nutzen der Erzeuger und Konsumenten nicht maximieren, wodurch ein nicht gerechtfertigter Preis für die gehandelten Assets entsteht. In solchen Fällen können das Gerät oder die Geräte-Inhaber den Marktplatz und dessen Stake herausfordern.

Es ist wichtig, zu beachten, dass Token, die als Stake hinterlegt wurden, in diesem Zeitraum selbst für das Weeve Network gesperrt und unbrauchbar sind. Das Protokoll verhindert, dass diese Token verwendet werden können. Weder Teilnehmer des Marktplatzes noch das Weeve Network haben darauf Zugriff. Um tatsächlich Zugriff auf diese Token zu erhalten, müsste man 51 Prozent der eine Milliarde Token im Umlauf kaufen und Zugriff auf das Protokoll selbst gewinnen – ein höchst unwahrscheinliches Szenario (vgl. 3.1.2). Es ist auch deshalb so unwahrscheinlich, da, sobald andere Benutzer im Netzwerk herausfinden, dass eine vorsätzliche Zentralisierung des Weeve Network stattfindet (was leicht durch eine virtuelle öffentliche Bekanntmachung geschehen kann), kein Anreiz mehr bestünde, im Netzwerk zu bleiben. Alle ehrlichen Benutzer würden dann nämlich ihre Stakes entsperren und zu der Netzwerk-Fork wechseln, die dann zum neuen Weeve Network werden würde. Das ursprüngliche Netzwerk wäre dann wertlos. Wenn es in dem zentralisierten, unehrlichen Netzwerk keine Nutzer mehr gibt, gibt es auch fast gar keinen Anreiz für den Zugriff auf das Protokoll. Im Wesentlichen würde ein dominierender Spieler viele Weeve-Token ausgeben, um die Kontrolle über ein potentiell unbrauchbares Netzwerk zu gewinnen – denn sobald er sich den mehrheitlichen Zugriff verschafft hat, würde das ehrliche System einfach zu einer Fork wechseln, wodurch die gesamte „schlechte“ Initiative sinnlos wird.

3.1.6 Das Weeve-Token

Das Weeve-Token (WEEV) ist das native Token des Weeve Network und ist erforderlich für den Betrieb des Netzwerkprotokolls. Es hat einen fixen Bestand und besitzt keine integrierte Funktionalität zum Verbrennen. Die Hauptfunktionen des Tokens werden in Abbildung 3 zusammengefasst. Das WEEV-Token ist wichtig für das Netzwerk, um sicherzustellen, dass Teilnehmer für ihre Handlungen zur Rechenschaft gezogen werden, und ihre Interessen deshalb langfristig aufeinander ausgerichtet sind. Ein Netzwerk mit hochwertigen Teilnehmern und authentischen Transaktionen hat einen höheren intrinsischen Wert, was sich dementsprechend auf den Token-Wert auswirken sollte, und umgekehrt. Wenn beispielsweise Ether anstatt WEEV verwendet werden würden, würde der Wert des Ether-Netzwerks wahrscheinlich den des Weeve Network um einiges übertreffen. Das würde bedeuten, dass Teilnehmer keinen langfristigen Anreiz haben, ihr eigenes Netzwerk aktiv zu verbessern, und die Zerstörung ihres Netzwerks durch negative Aktivitäten wie etwa Spekulationen zu verhindern.

Positive Anreize: Das WEEV-Token fördert Aktionen mit positiven Ergebnissen für das Netzwerk.

- Geräte-Inhaber hinterlegen Token, damit ihre Geräte in Geräteregister aufgenommen werden.
- Register-Inhaber hinterlegen Token, um neue Geräteregister zu erstellen.
- Marktplatz-Inhaber hinterlegen Token, um neue Marktplätze zu erstellen.
- Token werden auch verwendet, um Gebühren an Validatoren und Schiedsrichter auszuzahlen.

Negative Anreize: Das WEEV-Token hält Teilnehmer davon ab, Aktionen mit negativen Ergebnissen für das Netzwerk zu starten.

- Es dient als Sicherheit, um nichtkooperative Geräte zu bestrafen, welche Netzwerkressourcen für ihre Zwecke ausnutzen.
- Es dient als Sicherheit, um Geräteregister zu bestrafen, welche die Qualität des Netzwerks verschlechtern.
- Es dient als Sicherheit, um Marktplätze zu bestrafen, welche gegen die Regeln verstoßen.

Abbildung 3: Eine Übersicht der WEEV-Token-Anreizmechanismen

Das heißt, dass Ether oder ähnliche Token eine andere Dynamik verfolgen als das Weeve Network. Es kann etwa vorkommen, dass Preisschwankungen des Ether statistisch vollkommen unzusammenhängend zur Performance des Weeve Network erfolgen. Das WEEV-Token entkoppelt sich von diesen Schwankungen und gibt Token-Inhabern ein faires und verlässliches Werkzeug, um den Wert des Netzwerks zu beurteilen. Dies spiegelt sich im Preis der WEEV-Token wider.

3.2 Weeve-Network-Protokoll

Das Weeve-Network-Protokoll (Abb. 4) beschreibt die allgemeine Beteiligung der Knoten im Weeve Network und die Integration der Dienste von Drittanbietern. Jedes Geräteregister und jeder Marktplatz-Inhaber setzt das WEEV-Token als Sicherheit ein. Als Faustregel gilt: Je höher der Wert der beabsichtigten Transaktionen, desto höhere Sicherheitskautionen müssen Inhaber hinterlegen vorbehaltlich der Validierung und Schiedsverfahren (Details folgen). Jede Funktion im Protokoll versucht, die Interoperabilität zu erhöhen, Vertrauen zu schaffen, oder beides.

Um die Interoperabilität zu erhöhen, definiert das Protokoll Mitgliedschaftsstandards, Transaktionsarten, die Auflistung der Geräte, die Auflistung der Transaktionshistorien und die Vermittlung von neuen Transaktionen. Diese Komponenten bieten ausreichend Informationen und Tools, um eine gemeinsame Transaktionsart zu bestimmen, die neue Transaktionsart verbindlich zu machen und Transaktionsanforderungen mit Antworten zu initiieren.

Damit von vornherein eine Vertrauensgrundlage besteht, definiert das Protokoll außerdem Validierungsrichtlinien, Zugang zu Aktivitätslogs, Auflistungen von Validatoren und Mechanismen zur Streitbeilegung. Mit diesen Elementen können Register angemessene Garantien geben, dass die Transaktionen authentisch und frei von Fehlern sind.

Das Weeve-Network-Protokoll zielt nicht darauf ab, Datenbetrug direkt zu lösen. Einzelpersonen und Marktplätze können selbst mitbestimmen, was Vertrauenswürdigkeit ist, und wo die Grenze gezogen werden soll.

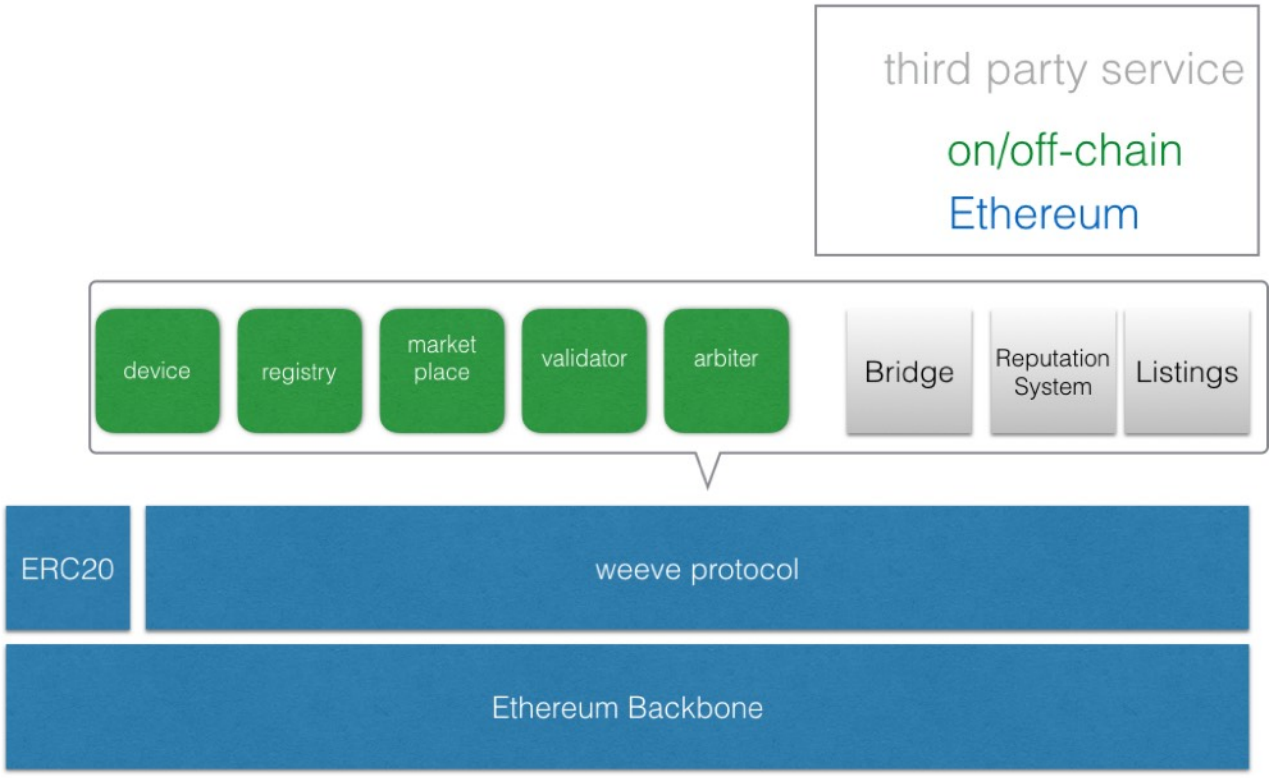

Abbildung 4: Eine Übersicht des Weeve-Protokolls

3.2.1 Mitgliedschaftsstandards

Bei der Bestimmung der Mitgliedschaftsstandards sollte auf folgende Punkte besonderen Wert gelegt werden:

- Benutzerfreundliche Spezifikationen und Argumentation
- Standardmäßige allgemeine Struktur und Abschnitte
- Zugänglichkeit für alle Beteiligten
- Technische Details für konforme Implementierungen falls zutreffend, wie Datenstrukturen
- Einfache Formatierung
- Aktuelle Kontaktinformationen der Autoren
- Daten, Zeitpunkte und Verlauf der Dokumentupdates

Aufgrund der außergewöhnlich hohen Anzahl der möglichen Geräteregistertypen gibt es zurzeit kein einziges bestes Format für die Spezifikation der Mitgliedschaftsstandards. Wir erwarten allerdings, dass sich mit der Zeit ein oder mehrere praktikable Standards hervortun werden. In Gesprächen mit potentiellen IoT-Partnern aller Branchen konnten wir völlig unterschiedliche Anforderungen für Mitgliedschaftsstandards identifizieren. Dies verschlimmert wiederum das Dilemma der Interoperabilität von IoT-Geräten. Angesichts dieser Unsicherheiten ist es vorerst am besten, nicht mit übermäßig detaillierten oder strengen Richtlinien aufzuwarten.

Digitale Dokumente, in denen die Mitgliedschaftsstandards angeführt werden, können recht umfangreich sein, beispielsweise wenn sie Anlagen mit technischen Details und Spezifikationen mit eingebetteten Datentabellen enthalten. Daher sollten Mitgliedschaftsstandards nicht direkt auf der Blockchain gespeichert liegen – also besser Off-Chain – und nur mit dieser verbunden sein, wie beispielsweise auf einem IPFS [6]-Cluster oder einem dezentralen, unveränderlichen Speicheranbieter.

Änderungen an den Registerstandards müssen durch die Governance-Kriterien des Geräteregisters legitimiert sein und für die Prüfung durch Register- und Marktplatz-Mitglieder gespeichert werden. Ähnliche Standards sind von Erstellern von Marktplätzen anzuwenden. An diesem Punkt möchten wir noch einmal betonen, dass Mitgliedschaftsstandards abhängig vom spezifischen Geräteregister und den Marktplatz-Erstellern enorm variieren können. Ein Geräteregister für Kaffeemaschinen etwa erfordert nicht die gleichen strikten Mitgliedschaftsstandards wie ein Register für militärisches Gerät.

3.2.2 Richtlinien für Validierung und Schlichtung

Richtlinien für die Validierung und Schlichtung werden von Register- und Marktplatz-Inhabern als Begleitdokumente für die Mitgliedschaftsstandards bereitgestellt und fungieren als Prüf-Tools für Validatoren und Schiedsrichter. Richtlinien für die Validierung, die als Prüfstandard angesehen werden können, dienen als Arbeitsvereinbarung zwischen dem Register/Marktplatz und seinen Validatoren und beschreiben Vereinbarungen wie automatisierte Prüfungen (z. B. über ein Remote-Authentifizierungsprotokoll [4]), manuelle Prüfungen (wie die Inspektion der Hardware), Zeitrahmen, Akzeptanzkriterien und die Streitschlichtung für Validatoren. Sobald ein Gerät seine Anfrage an einen Marktplatz gestellt hat, dienen diese Validierungsrichtlinien als Quelle. Einen ähnlichen Zweck verfolgen die Schlichtungsrichtlinien. Im Grunde erlauben sie es, im Streitfall den Schiedsrichter anzugeben und Funktionsschnittstellen in ähnlicher Art wie Validatoren zu verwenden.

[6]https://ipfs.io/

Diese Richtliniendokumente sollten ähnlich aufgebaut sein wie die vom US-amerikanischen FedRAMP-[4]Programm bereitgestellten Vorlagen[7] und Richtlinien, die zum Beispiel von der US-Regierung verwendet werden, um der Branche einen standardisierten Ansatz zur Sicherheitsprüfung, Autorisierung und kontinuierlichen Überwachung für Cloud-Produkte und -Services bereitzustellen. Außerdem befindet sich auf der Website des Programms eine Liste mit

[4] https://www.fedramp.gov/templates/

autorisierten Prüfern, so wie es für jedes Geräteregister eine Liste mit ernannten Validatoren gibt. Die Validierungsrichtlinien sollten die folgenden Punkte priorisieren:

- Benutzerfreundliche Richtlinien und Argumentation
- Maschinell referenzierbare Ankerpunkte im Dokument, um automatische Prüfungen und digitale Berichtsformate zu unterstützen
- Zugänglichkeit für Validatoren und Schiedsrichter
- Technische Details für konforme Implementierungen falls zutreffend, einschließlich Quellcode oder Drittanbieter-Services, die für die Prüfung verwendet werden
- Maschinell referenzierbare Ankerpunkte im Dokument, um automatische Prüfungen und digitale Berichtsformate zu unterstützen
- Checklisten und Bewertungsrubriken für gewünschte Validierungen
- Qualitatives und quantitatives Feedback, einschließlich der Gesamtausrichtung an den Mitgliedschaftsstandards, deutlicher Stärken und Schwächen sowie einer Historie des Antragstellers hinsichtlich der Mitgliedschaftsstandards
- Aktuelle Kontaktinformationen des Autors
- Daten, Zeitpunkte und Verlauf der Dokumentupdates

3.2.3 Aktivitätsprotokolle

Register- und Marktplatz-Inhaber sollten Protokolle mit Transaktionsaktivitäten für Ereignisse, die im Register und auf dem Marktplatz stattfinden, aufbewahren. Schiedsrichter bitten eventuell um Zugriff auf einen Teil der Aktivitätsprotokolle, um Streitfälle mithilfe der relevanten Daten zu lösen. Wenn ein Schiedsrichter versucht, einen Streit beizulegen und für eine Partei fehlen die Transaktionsaktivitätsprotokolle, wird der Schiedsrichter wahrscheinlich zugunsten der Partei entscheiden, die Beweise vorlegen kann. Deshalb tendieren Marktplatz-Inhaber dazu, alles gut zu dokumentieren, um ihre Position im Fall von Streitigkeiten zu verbessern.

Marktplatz-Inhaber sollten insbesondere die relevanten Transaktionsaktivitätsprotokolle der Parteien prüfen, die Transaktionen durchführen, um die Einheitlichkeit und Richtigkeit der Transaktionsverläufe oder Geräte-Validierungen sicherzustellen. Diese sind auch in der Prüfphase hilfreich, wenn ermittelt wird, wie vertrauenswürdig ein Gerät ist.

Aktivitätsprotokolle sollten mindestens nach den folgenden Kriterien gefiltert werden können:

- Daten

- Aktivitätstyp
- Teilnehmer-IDs

Es wird unbedingt empfohlen, dass die folgenden Ereignisse detaillierte Protokolleinträge erzeugen:

- Governance-Änderungen
- Änderungsvorschläge und Hinweise
- Abstimmungsergebnisse
- Transaktionen
- Änderungen an Mitgliedschaftsstandards
- Änderungen an Validierungsrichtlinien
- Änderungen an Transaktionstypen
- Änderungen am Geräte-Listing
- Änderungen an Geräte-Metadaten

Manchmal unterliegen die Aktivitätsprotokolle dem Datenschutz. In solchen Fällen wird das Weeve Network entsprechende Technologien zur Verbesserung des Datenschutzes (wie Mehrparteienberechnung oder funktionale Verschlüsselung) vorschlagen.

3.2.4 Transaktionstypen

Register- und Marktplatz-Inhaber können Transaktionstypen mithilfe von Dokumenten, Bibliotheken und Beispielcode im RFC-Format angeben. Diese Transaktionsbibliotheken sollten relevante Daten für Streitfälle und Schiedsverfahren im Aktivitätsprotokoll aufzeichnen. Aufgrund dieser Vorgabe haben Schiedsrichter später Zugriff auf relevante Fakten, wenn sie den Ausgang eines Falls bestimmen sollen. Deshalb sind sie wichtig für einen sicheren Marktplatz.

Mitgliedschaftsstandards können Anforderungen enthalten, die die Interoperabilität zwischen Geräten noch weiter fördern, darunter Geräte-URIs, transaktionsspezifischer Protokoll-Support, Service-Endpunkte, Datenspeicheranbieter, Datenmaßeinheiten und mehr. Diese Anforderungen dienen als Grundlage für den geräteübergreifenden Austausch, ganz egal, ob es unverarbeitete Daten oder komplexere Transaktionen wie Auktionen, Preisverhandlungen und erweiterte Abfragemöglichkeiten sind. Mitgliedschaftsstandards geben Transaktionstypen eine Basis, auf die sie sich stützen können.

Für die Bestimmung von Transportschichten in Transaktionstypen werden Geräteregister dazu angehalten, das MQTTS-Protokoll[8] zu nutzen, das speziell vom Weeve-Team entwickelt wurde und grundlegende IoT-sichere Geräte-Kommunikationen wie die Adressierung, die Session-Verwaltung, den Datentransfer und die Bestätigung unterstützt. Für die Bestimmung der Zahlungsschichten in Transaktionstypen werden Geräteregister dazu angehalten, faire Austauschprotokolle zu verwenden[9]. Diese unterstützen die Treuhanddienste bei Angebot und Nachfrage, die Preisverhandlung und die Lieferbestätigung. Andere Service-Schichten können in ähnlicher Form zu den Transaktionstypen hinzugefügt werden.

[8]Vgl. Abschnitt 2.2, http://papers.weeve.network/weeve_whitepaper.pdf
[9]Vgl. Abschnitt 2.5, http://papers.weeve.network/weeve_whitepaper.pdf

Die Register- und Marktplatz-Inhaber können für jeden Transaktionstyp Parameter in Zusammenhang mit dem Schiedsverfahren festlegen, bei dem eine oder mehr Parteien eine Transaktion anfechtet und eine Lösung verlangt. Diese Parameter umfassen unter anderem:

- Zeitfenster für Streitfälle
- Minimale und maximale Streitbeträge
- Lösungsrichtlinien
- Richtlinien für Schiedsrichterauswahl
- Auswahl eines modularen Schiedssystems

3.2.5 Transaktionen

Für jede Transaktion müssen eine eindeutige Transaktions-ID, eine eindeutige Geräte-ID, ein Transaktionstyp und entsprechende Transaktions-Metadaten aufgezeichnet und authentifiziert oder On-Chain bestätigt werden. Diese Anforderung stellt sicher, dass Transaktionen nicht mehr teilbar sind, sodass im Falle von Streitigkeiten und Schiedsverfahren die bestmöglichen Daten über die Transaktionen und ihre Teilnehmer verfügbar sind. Transaktionen ohne On-Chain-Aufzeichnungen genießen nicht den vollen Schutz vom Weeve Network, falls es zu einem Streitfall kommt.

3.2.6 Metadaten-Schnittstellen

Metadaten für Geräte und Transaktionen können und sollten in einer Vielzahl von Formaten vorliegen, einschließlich JSON, XMLS, Wire-Protokolle und Binärblobs (je nach Anwendungsfall). So verlangen zum Beispiel Metadaten-Formate, die in hoch frequentierten Trading-Maschinen verwendet werden, eine kompaktere Datenkomprimierung als Formate, die für Mautstellen auf Autobahnen genutzt werden. Daher ist es nicht sinnvoll, ein bestimmtes Darstellungsformat für die Metadaten zu fordern. Doch aus Gründen der Interoperabilität muss es mindestens eine gemeinsame Methode geben, um auf diese Metadaten zuzugreifen. Daher müssen für das Register und den Marktplatz grundlegende Listen-, Filter-, Erstellungs- und Zugriffsfunktionen für Smart

Contracts bereitgestellt werden. Diese Anforderungen werden zunächst als eine Schnittstellenspezifikation für Smart Contracts implementiert, und enthalten Authentifizierungs- sowie Autorisierungskomponenten.

3.3 Weeve-Protokoll-Schnittstellen

Ein Weeve-Knoten kann mit einer Vielzahl von zugrundeliegenden Technologien implementiert werden, von zentralen Servern, die von traditionellen Unternehmen betrieben werden, bis hin zu komplett dezentralen Smart Contracts, die von einer Community aus IoT-Geräte-Enthusiasten geregelt werden. Diese Flexibilität ermöglicht es allen Gruppen von Menschen zu handeln, seien es große Kapitalgesellschaften oder stark engagierte Einzelpersonen. Ein Smart Contract implementiert die Protokoll-Schnittstellen, was mehrere Signatur-Anforderungen erfüllt, die in den folgenden Abschnitten allgemein beschrieben werden.

Kurz gesagt: Jeder Knoten muss Funktionen implementieren, die Folgendes unterstützen:

- Staking und Unstaking für den Smart Contract des Weeve Network (Staking und Unstaking erfolgen auf mehreren Ebenen, d. h. im Register, auf dem Marktplatz usw. für Geräte, die am Weeve Network teilnehmen möchten)
- Abrufen von Mitgliedschaftsstandards
- Abrufen von Validierungsrichtlinien
- Abrufen von unterstützten Transaktionstypen
- Abfragen von Aktivitätsprotokollen
- Listing von Geräten und Metadaten
- Listing von Transaktionsverlauf und Metadaten
- Listing von Validatoren (Register & Marktplätze)
- Listing von Schiedsrichtern (Register & Marktplätze)

3.3.1 Listing und Entfernen von Listings

Zukünftige Inhaber können einen großen Teil des WEEV-Token proportional zu ihrem erwarteten und gewünschten Transaktionsvolumen, der Anzahl an gelisteten Geräten usw. einsetzen (der Mechanismus wird vorerst offen gelassen, damit das System flexibel bleibt), um neue Geräte-Register bzw. Marktplätze zu erstellen. Im Rahmen des Erstellungsprozesses muss der Stake über das Geräte-Register (bzw. den Marktplatz) eingesetzt werden, wobei mindestens ein Erstgerät enthalten sein muss, das den Mitgliedschaftsstandards entspricht. Dies dient als Beweis dafür, dass die Standards auch wirklich erreichbar sind. Zur Erinnerung: Wir brauchen Stakes von Register-Inhabern, um Verstöße zwischen Registern zu umgehen. Bei der Verwendung von Anreizmechanismen der Spieltheorie hätte kein Register-Ersteller den Anreiz, das System zu manipulieren oder dessen vertrauenswürdigen Ruf zu gefährden, ohne das Risiko einzugehen, seinen eingesetzten Stake zu verlieren und im System als unehrlich zu gelten. Dieser Staking-Mechanismus ist auf allen Ebenen tief in das System eingebettet und erstreckt sich von der Register-Erstellung über die Marktplatz-Erstellung bis hin zum Geräte-Listing in Registern und auf Marktplätzen.

Wenn das Listing für das erste Gerät ohne weitere gültige Geräte aus dem Register entfernt wird, wird der Stake für das Geräte-Register (bzw. den Marktplatz) freigegeben, und es kann passieren, dass der Inhaber damit das Register (bzw. den Marktplatz) zerstört, indem er den Stake

zurückzieht. Das Weeve Network führt schließlich vielleicht eine Speicherbereinigung durch, wobei Register und Marktplätze einfache Lebendigkeitstests bestehen müssen, um weiterhin in einem guten Zustand zu bleiben. Das initialisierende Gerät hat keinen Sonderstatus im Register (bzw. Marktplatz), nachdem es als erste Demonstration für die erreichbaren Mitgliedschaftsstandards diente. Diese Staking- und Demonstrationsmaßnahmen haben den Zweck, der Erstellung von qualitativ minderwertigen Knoten im Weeve Network entgegenzuwirken und deren Entfernung zu vereinfachen. Anfangs müssen alle neuen Register von den vom Netzwerk gewählten Validatoren geprüft werden, um das entstehende Ökosystem vor Verschmutzung zu schützen, aber das

langfristige Ziel der Projekte ist eine dezentrale und von der Community gesteuerte Governance, die möglicherweise die Antragstellerprüfsysteme bestimmter Knoten selbst nachahmt.

3.3.2 Abrufen von Mitgliedschaftsstandards

Ein Knoten muss in der Lage sein, auf die Mitgliedschaftsstandards der anderen Register zuzugreifen. Daher muss jeder Knoten Abfragen aus dem Netzwerk unterstützen. Bei der Implementierung der Schnittstelle gibt die Funktion signierte Mitgliedschaftsstandards zurück, um sensible Daten zu authentifizieren.

3.3.3 Abrufen von Validierungsrichtlinien

So wie bei Mitgliedschaftsstandards muss ein Knoten in der Lage sein, auf die Richtlinien für die Validierung und Schlichtung von anderen Registern/Marktplätzen zuzugreifen. Bei der Implementierung der Schnittstelle wird die Funktion mit einer Register- und Geräteherkunft versehen, um angemessene Einschränkungen bei der Ausgabe von Validierungs-/ Schlichtungsrichtlinien zum Schutz sensibler Daten zu ermöglichen.

3.3.4 Abrufen von unterstützten Transaktionstypen

Während der Register-Erstellung können die Register-Inhaber die Transaktionstypen angeben, die das Register unterstützt, darunter Protokolldetails pro Transaktionstyp wie Anrufkonventionen, Zeitpunkte, Preisberechnungen, relevante Datenstrukturen und Bereitstellungsanforderungen. Diese Transaktionstypen müssen über eine Schnittstellen-Implementierung für das Listing verfügbar gemacht werden und können durch Berechtigungskontrollen geschützt werden.

3.3.5 Abfragen von Aktivitätsprotokollen

Aktivitätsprotokolle sind eine Möglichkeit für Geräte-Register und Marktplätze, um Transparenz für potenzielle Marktplatz-Ersteller zu schaffen. Durch die Bereitstellung einer Schnittstelle, die Validierungsdatensätze und Governance-Verläufe zur Verfügung stellt, hat ein potenzieller Marktplatz mehr Sicherheit, dass ein Gerät im Geräte-Register wie versprochen liefert.

3.3.6 Listing von Geräten und Metadaten

Geräte und ihre Metadaten können auf Anfrage zur Verfügung gestellt werden. Die Funktion für das Listing von Geräten im Smart Contract wird von Registern und Marktplätzen verwendet, um andere Geräte zu finden. Alle Abfragen müssen eventuell erst durch das Sicherheitssystem eines Geräteregisters authentifiziert und autorisiert werden.

3.3.7 Listing von Transaktionen und Metadaten

Transaktionen und ihre Metadaten können auf Anfrage zur Verfügung gestellt werden. Die Funktion für das Listing von Transaktionen im Smart Contract wird von anderen Geräten verwendet, um historische Transaktionen zu prüfen und auf andere zu verweisen. Alle Abfragen müssen eventuell erst durch das Sicherheitssystem eines Geräteregisters authentifiziert und autorisiert werden.

3.3.8 Listing von Validatoren

Register-Inhaber können Validatoren bestimmen, um die Validierungskriterien für Mitgliedschaftsstandards zu erfüllen, die eine Kombination aus automatisierten und manuellen Aufgaben sein können. Es muss eine Schnittstelle zur Verfügung gestellt werden, um eine Liste mit aktiven Validatoren bereitzustellen.

3.3.9 Listing von Schiedsrichtern

Register- und Marktplatz-Inhaber können Schiedsrichter ernennen, die als anerkannte faire und unabhängige Dritte dazu beitragen, Streitfälle zu lösen. Eine Schnittstelle muss zur Verfügung gestellt werden, um eine Liste mit aktiven Schiedsrichtern bereitzustellen. Diese Listen enthalten Metadaten (wie Kontoinformationen) und werden verwendet, um Schiedsrichter zu authentifizieren und zu autorisieren, damit diese bestimmte Aktivitätsprotokolle in Geräte-Registern einsehen können. Zweck dieser Daten ist es, Streitfälle beizulegen.

4 Streitigkeiten und Schiedsverfahren

Schiedsverfahren sind notwendig, wenn mindestens eine Partei einer Transaktion einen Streitfall eröffnet. Die Eröffnung eines Streitfalls sollte automatisch alle relevanten Transaktionsdetails sammeln, die On- oder Off-Chain gespeichert werden. Bei Bedarf sollten weitere Daten von den Parteien, die die Transaktion durchgeführt haben, erfasst werden. Streitfälle in Bezug auf Transaktionen, die zwischen Menschen stattfanden, müssen anders behandelt werden, als Streitfälle, deren Ursprung in maschinellen Transaktionen liegen. Beispielsweise ist bei einer Streitbeilegung für Millionen von Gerätetransaktionen, die in einer Geschwindigkeit von Millisekunden durchgeführt werden, eine Zusammenführung, Analyse und Beratung durch menschliche Agenten notwendig, ähnlich wie bei E-Discovery-Prozessen, die Unternehmen im Fall von Rechtsstreitigkeiten durchlaufen.

Zum Beispiel erfordern die Mitgliedschaftsstandards auf einem Marktplatz für Elektrofahrzeuge, die nach Ladestationen suchen, dass die Elektrofahrzeuge Schnappschüsse des Akkuladestands, des Kilometerstands, des Reifendrucks usw. vornehmen. Diese Daten können verwendet werden, um zu bestimmen, ob das Elektrofahrzeug die volle Ladungsmenge erhalten hat, die ihm gewährt wurde, wodurch ein Nachweis gegen Manipulation erbracht werden kann. So sind Schiedsrichter hervorragend mit den besten Informationen ausgerüstet, um eine Entscheidung zu treffen.

4.1 Aussage gegen Aussage

Wie auf anderen bestehenden Plattformen mit mehreren Seiten kann auch ein Reputationssystem verwendet werden, um Streitfälle im Fall einer abweichenden, unbegründeten Darstellung eines Ereignisses beizulegen. Reputationssysteme liegen außerhalb des Zuständigkeitsbereichs für das Weeve-Network-Protokoll, sind aber möglich und werden für jedes Geräteregister oder übergreifend empfohlen.

4.2 Speicherung

Anfangs stellt jedes Geräte-Register und jeder Marktplatz die Mittel für den Zugriff, die Speicherung und die Verwaltung von Datenstrukturen bereit, um Streitigkeiten beizulegen und Schiedsverfahren durchzuführen. Auf lange Sicht wird ein Support für dezentrale Register mit Validatoren und Schiedsrichtern implementiert werden, die

die Validierung übergreifend für ein ähnliches Gebiet übernehmen oder sich auf einen dezentralen Service verlassen, der Validatoren verwaltet (Kleros, Delphi usw.).

4.3 Drittanbieter-Services

Mehrere Projekte im Blockchain-Ökosystem basieren bereits auf offenen und fairen Systemen für die Urteilsfindung (z. B. Delphi und Kleros). Während der Implementierung von Smart Contracts wurde auf Veranlassung von Register- und Marktplatz-Inhabern versucht, volle Kompatibilität für diese zuschaltbaren Schiedsverfahren zu gewährleisten. Für viele dieser Services müssen noch faire Schiedsrichter ernannt werden, sodass in diesen Fällen die Schiedsrichterauswahl weiterhin in der Verantwortung der Inhaber liegt. Darüber hinaus werden Variablen in Zusammenhang mit dem Schiedsverfahren – wie das Zeitfenster für den Streitfall, die Mindest- und Maximalbeträge für den Streitfall und die Gebühren für den Schiedsrichter – von den Inhabern in den Transaktionstypen festgelegt.

4.4 Registerübergreifendes Schiedsverfahren

Für Schiedsverfahren, an denen mehrere Register beteiligt sind, können Schiedsrichter, die von allen betroffenen Registern und Marktplätzen für bestimmte Transaktionstypen zertifiziert sind, berechtigt sein, entsprechende Streitfälle gegen eine Gebühr zu schlichten. Für die Zukunft können wir uns mehrere Schiedsrichter vorstellen, wobei jeder die Interessen seines Registers vertritt, um zu einem Konsens zu kommen, also nicht anders als die Schiedsrichter von heute.

5 Mehrschichtige Funktionalität

Genauso wie sich Anwendungsschichten auf Session-Schichten im OSI-Modell befinden, können wichtige Services zur Gewährleistung der Netzwerkstabilität vorhanden sein, die Primitive verwenden, die vom Weeve-Network-Protokoll bereitgestellt werden. Die folgenden Abschnitte beschreiben Funktionen, die nicht Teil des Weeve-Network-Protokolls sind, aber trotzdem eng damit zusammenhängen. Wir betrachten deren Integration als nützliche zukünftige Bereicherung für das Netzwerk.

5.1 Listings von Geräte-Registern und Marktplätzen

Geräte-Register und Marktplätze können auf der Weeve-Plattform gelistet und anschließend mit Attributen wie Geographie, Register-Typ und öffentlich verfügbaren Mitgliedschaftsstandards getaggt werden. Die Prüfung und Genehmigung von Listings kann anfangs alle eingesetzten Geräte-Register umfassen, die zustimmen, aber auf lange Sicht sollte die Community das letzte Wort für diese Aktivität haben. Es ist möglich, ein Geräte-Register zu verwenden, um die Mitgliedschaft anderer Register einzuschließen, aber diese rekursive Struktur ist komplex und liegt außerhalb des Zuständigkeitsbereichs der anfänglichen Smart-Contract-Implementierungen. Diese Listings werden für die relevanten Parteien über eine Website zur Verfügung gestellt, die

von der Weeve-Plattform verwaltet wird, und erreichen letztendlich über DApps als Ökosysteme wie Blockstack[5] die entsprechende Reife. Die Anmeldung über ein Kryptowährungs-Wallet wird unterstützt, um den genehmigten Zugriff auf Listings mit Geräte-Registern zu ermöglichen.

5.2 Reputationssysteme

Reputationssysteme gewährleisten die Sicherheit des Marktes, indem Marktplatz-Teilnehmer wissen, mit wem sie Transaktionen durchführen. Obwohl Reputationssysteme kein Teil des Geräte-Registerprotokolls von Weeve sind, handelt es sich dabei dennoch um wichtige Konstrukte, die einen großen Beitrag dazu leisten, neue Handelsformen zu ermöglichen. Deshalb bietet die Weeve-Plattform kostenlose Building-Blocks für Register-Inhaber an, um Reputationssysteme auf das Protokoll zu implementieren.

Diese Systeme werden als Smart Contracts implementiert und mit Geräte-Identifikatoren und Geräte-Registern verankert. Sie aktualisieren einzelne Profile, indem sie Transaktionsverläufe auslesen und die Ausgänge von Schiedsverfahren und Streitigkeiten aufzeichnen. Das System sollte hochgradig anpassbar sein, da unterschiedliche Handelsformen unterschiedliche Ausgänge für Geräte-Reputationen zur Folge haben.

Zum Beispiel brauchen Marktplätze mit menschlichen Teilnehmern Benutzerschnittstellen, die komplett mit den Semantiken einer Reputation für Menschen kommunizieren können, um bessere Entscheidungen zu treffen. Auf der anderen Seite können nahezu vollständig automatisierte Marktplätze, auf denen Geräte in hoher Frequenz Handel treiben, statistische Methoden nutzen, um Daten für algorithmische Updates der Reputationen zu verwenden und gewünschte Handelspartner automatisch in Rankings aufzuführen, ohne dass menschliches Zutun erforderlich ist.

5.3 Intra-Blockchain-Transaktionen („Brücke“)

Blockchain-Technologie ist im Entstehen und es kann viele konkurrierende Blockchains geben, die als Infrastruktur für Protokolle dienen. Der erste Durchlauf des Weeve Networks wird auf der Ethereum-Blockchain aufgebaut, muss sich aber an zukünftige Entwicklungen oder Wettbewerber anpassen, die de facto die Grundlage dafür bilden. Deshalb ist ein flexibler Ansatz wichtig, der von der zugrundeliegenden Blockchain-Implementierung unabhängig ist.

Um die Blockchain-Interoperabilität zwischen Transaktionen zu ermöglichen, muss ein Marktplatz dafür sorgen, dass seine Mitglieder sich an Standardspezifikationen für URIs halten, die die Geräte-Register in verschiedenen Blockchains darstellen können. Transaktionen können mithilfe von Relais-Technologien an verschiedene Blockchains weitergeleitet werden. Diese Technologien entwickeln sich gerade immer schneller weiter und kommen immer häufiger zum Einsatz. Der Hauptvorteil des Netzwerks ist die Fähigkeit, einzigartige Vorteile spezifischer Blockchains zu nutzen, darunter die Hochdurchsatzverarbeitung oder die Anonymitätsgarantie.

6 Schlussfolgerungen

[5] https://blockstack.org/

Die IoT-Branche leidet heute unter kostspieligen Interoperabilitäts- und Sicherheitsproblemen. Das Weeve Network möchte dieses Problem beheben, indem eine Community mit qualitativ hochwertiger Open-Source-Software bereitgestellt wird, zu der auch das weeveOS – ein IoT-to-Blockchain Operating System, das „secure by design“ ist – und die Weeve-Marktplatz-Verwaltungsplattform gehören. Das WEEV-Token ermöglicht einen Marktplatz, der auf diesen Primitives basiert, für alle Teilnehmer auf der Welt offen ist und flexibel genug ist, um die Anforderungen von traditionellen Chain-of-Command-Unternehmen und Befürwortern einer dezentralen Zukunft für IoT-Geräte gleichermaßen zu erfüllen.

Mit seinem Protokoll kümmert sich das Weeve Network unter Nutzung von Mitgliedschaftsstandards, Validierungsrichtlinien und Transaktionstypen um schwierige Interoperabilitäts- und Vertrauensprobleme. Die zugrunde liegende Blockchain-Infrastruktur bildet die Brücke zwischen nicht vertrauenswürdigen Parteien und das WEEV-Token kann ein Anreiz für sichere Handelsaktivitäten zwischen Geräten sein, damit sich Teilnehmer sicher fühlen. Das Weeve Network ermöglicht eine Zukunft der Dezentralität, in der durch eine neue Aufstellung nach dem Willen der Community innovative Märkte für Transaktionen zwischen Geräten entstehen.

Quellenangaben

[1] Whitepaper mit Anwendungsfall
[2] Steven P. Lalley und Glen Weyl: „Quadratic Voting: How Mechanism Design Can Radicalize Democracy“ American Economic Association Papers and Proceedings, 2018, 1(1).
[3] Glen Weyl: „The Robustness of Quadratic Voting“ Public Choice, 2017, 172(1-2) Special Issue: Quadratic Voting and the Public Good: 75-107.
[4] A. Seshadri, A. Perrig, L. van Doorn, P.K. Khosla: SWATT: SoftWare-based ATTestation for embedded devices. IEEE Symposium on Security and Privacy, S&P 2004, 9–12 May 2004, Berkeley, CA, USA, IEEE Computer Society (2004).