Potenciando la economía de las cosas

# La Red Weeve

Informe sobre los token (parte 3/4)

# Protocolo de la red Weeve y el modelo de tokens

Sidd Bhasin y Sebastian Gajek
Weeve.network

# Resumen

Es un hecho indiscutible que los datos tienen un gran valor cuando se los tokeniza y se los incorpora a una red que apoya la mecánica y los principios de una economía. La red Weeve potencia la Economía de las Cosas al introducir una capa de comercialización entre los dispositivos (IoT) y Blockchain. En los equipos de red Weeve (o "Weeves", en adelante) indexan, procesan, tokenizan e intercambian datos cosechados contra activos digitales, especialmente monedas cifradas.

Weeve visualiza los mercados públicos o privados para cualquier forma de activo digital que abarque desde datos geográficos, electricidad, hasta estados de entrega, donde los productores de datos y los consumidores (compradores y vendedores) se unen, ponen en custodia su oferta y demanda, e intercambian sus activos digitales a los precios acordados.

Para establecer la estabilidad de la red en presencia de jugadores racionales que no necesariamente siguen una estrategia de juego limpio, la red utiliza un diseño de mecanismo de incentivo de la economía cifrada. Para participar en el juego (y por lo tanto en la red), los jugadores depositan un token como garantía para responder por sus acciones. En casos de inestabilidad de la red (por ejemplo, una disputa, un intercambio injusto, una infracción), la comunidad puede impugnar el depósito. Los ingredientes intrínsecos del diseño del mecanismo Weeve protegen a los usuarios, de forma que se castiguen las estrategias deshonestas o injustas mediante la pérdida de los depósitos, mientras que las estrategias honestas se alientan mediante mecanismos de premios.

Palabras clave: teoría de juegos, economía cifrada, intercambio justo, diseño de mecanismo basado en depósitos, jugadores racionales

# 1. Introducción

## 1.1 Motivación

La industria de la IoT se está acercando rápidamente a la masa crítica. Gartner estima que para el año 2017, habrá hasta 8 mil millones de dispositivos de IoT y ese número llegará a 28 mil millones en 2021. Con esta enorme cantidad de dispositivos conectados a Internet, se espera que el valor económico genere entre $ 4 y 11 billones por año hacia 2025.

Esta es, por supuesto, solo una gran promesa, ya que sin la infraestructura adecuada para apoyar este rápido crecimiento económico, su valor económico simplemente quedará rezagado a los vestigios de un pasado menos conectado.
Las tecnologías de Blockchain surgieron recientemente con un nuevo y poderoso paradigma para crear nuevas economías.

De hecho, constituyen un trampolín para una comercialización totalmente automatizada de datos entre dispositivos, potenciando lo que hemos denominado la Economía de las Cosas (EoT). En una Economía de Cosas, los dispositivos IoT ofrecen sus datos en nombre de sus propietarios (particulares, empresas o cualquier entidad legal) a través de conceptos conocidos como mercados de primer precio o de segundo precio, y otros dispositivos o entidades de IoT consumen los datos a cambio de monedas cifradas o activos digitales relacionados (como, geodatos comerciales para datos de temperatura). Imagine, por ejemplo, un panel solar que vende el exceso de energía a un vehículo eléctrico que requiere una carga a cambio de monedas cifradas. El panel solar equipado con un amperímetro podría medir el consumo de corriente e instruir a un relé eléctrico para que corte la electricidad cuando se haya entregado la cantidad pactada de energía. Todas las actividades son ejemplos de datos tokenizables y muestran el valor de los dispositivos IoT como habilitadores versátiles de las nuevas economías de Blockchain basadas en Oracle.

## 1.2 Impugnaciones

Antes de que podamos llegar a una Economía de las Cosas y antes de que los datos puedan ser económicamente útiles e intercambiables, se debe resolver un problema fundamental:

> **¿Cómo podemos habilitar una red[1] sin confianza en la que las entidades (anónimas) siguen los principios del mercado, es decir, ponen en custodia la oferta y la demanda, a un precio justo?**

La calidad y la procedencia de los datos tienen el impacto más significativo en las operaciones exitosas de IoT. Las computadoras habitualmente presentan errores y fallas inesperadas. Los dispositivos de IoT, que ahora recopilan datos valiosos (activos digitales), no son más que computadoras ágiles y livianas conectadas a Internet. Se debe tener mucho cuidado de que los dispositivos no ofrezcan datos que no son de su propiedad o que simplemente sean falsos, por el

---

[1] La referencia a "Sin confianza" se refiere a una red completamente descentralizada y autosustentable en la que los jugadores sienten desconfianza entre sí.

bien de un mejor precio. Con frecuencia, los dispositivos están mal calibrados y los vendedores sin ética tienen incentivos para manipular los resultados. El uso de información incorrecta a menudo resulta en peores resultados que al no usar la información. Sin garantías de identidad del dispositivo (cifrado) y del origen e integridad de los datos, muy pocos compradores potenciales de datos tendrían suficiente confianza para intercambiar libremente en un mercado centrado en los datos, donde la propiedad de éstos datos pudiera no ser clara.

Un problema de igual importancia es la ausencia de estándares de dispositivos. Una búsqueda rápida en Google, e incluso una inmersión profunda en los informes de la industria, revelarán un desorden de protocolos y estándares que ofrece poca claridad. Esto hace que sea difícil tanto para los operadores del mercado como para los participantes, evaluar la confiabilidad y fiabilidad del dispositivo, y su aprovisionamiento calificado de datos. Los datos, al igual que cualquier otro producto, se atribuyen a su valor en función de la fuente de origen. Para que un mercado realmente pueda atribuir valor a los datos (o una secuencia de los mismos), debemos entender el camino que tomó para llegar desde el sensor hasta el mercado. Mientras mayor sea la posibilidad de que se alteren estos datos, menos podremos confiar en ellos, y por lo tanto, menos valor le asignaremos. Estos son factores que utilizamos para asignar valor al activo digital de los datos.

## 1.3 Resumen del mecanismo de token de la economía cifrada de Weeve

En redes de múltiples jugadores, las partes persiguen diferentes estrategias para maximizar su utilidad. De hecho, cuando se otorgan incentivos financieros, debemos hacer frente a los jugadores desleales. Por ejemplo, se puede producir una infracción. Los productores de datos falsificados pueden imitar a los productores reales, manipulando el sistema de juego a su favor. Puede producirse cualquier forma de plagio, falsificación de marca o violación de patente y como resultado, la creación de mercados negros. Dichos problemas son inherentes a un sistema en el que los incentivos están mal diseñados y, por consiguiente, conducen a un comportamiento viciado involuntario.

Para construir una red estable que incentiva a todas las partes a actuar de manera justa y mantener el estado de honestidad del sistema, es necesario un diseño de mecanismo que premie dicho comportamiento. Con este fin, la red Weeve aprovecha los principios de la economía cifrada; uno de los inventos asombrosos de las tecnologías Blockchain contemporáneas. La red Weeve construye aplicaciones de mercado y servicios relacionados para el registro de dispositivos, validación de activos y resolución de disputas sobre la base de Blockchain. El Blockchain subyacente nos proporciona: (i) una unidad de valor que puede utilizarse para las transacciones de valores y para crear incentivos y penalizaciones, y (ii) un conjunto de herramientas con las que podemos diseñar una lógica condicional en forma de "contratos inteligentes". Al estar al interior de Blockchain, la red Weeve crea un sistema de incentivos que premia la curación de mercados con alta calidad de datos.

En pocas palabras, los curadores del mercado depositan tokens como garantía para determinar la calidad de la oferta y demanda de datos. El protocolo de red Weeve permite a los titulares de tokens impugnar a los curadores del mercado. En el caso de perder una impugnación, el depósito se pierde y se divide como una recompensa entre los titulares de tokens que participaron en el proceso de impugnación. El protocolo de red de Weeve aplica un diseño de mecanismo similar para incentivar a los propietarios de dispositivos a alcanzar un alto estándar de membresía, asegurándose de que

los datos provistos tengan un valor económico (y no un flujo de datos falso). Para participar en un mercado, los propietarios de dispositivos deben aparecer en la lista de registros de dispositivos. Cada registro representa un estándar de membresía, que el dispositivo debe cumplir. Implícitamente, un registro en la red Weeve sirve el propósito de evaluar la calidad de los datos. Para ser considerado para la lista, los candidatos deben hacer un depósito en la denominación del token intrínseco del registro. Los titulares de tokens pueden impugnar al dispositivo. Si el dispositivo es "bueno" y se encuentra aceptado en la lista, el propietario del dispositivo guarda su depósito y puede retirarlo en caso que desee abandonar el registro.

La lógica detrás de estos mecanismos de incentivos es que los dispositivos que no cumplan con los estándares de membresía deseados, ni generen datos veraces, ni sigan las costumbres de la red, evitarán una solicitud de registro, ya que esto lleva a una pérdida económica. Además, los curadores de mercados están incentivados para proporcionar una oferta y demanda real de datos de calidad, garantizar un equilibrio de precios para los proveedores y demandantes, y para actuar como mitigadores de las infracciones. La penalización, por el contrario, es el riesgo de pérdida del depósito.

# 2 La visión de Weeve

La visión de Weeve es potenciar la Economía de las Cosas donde las máquinas de IoT (o sus Weeves) indexan, procesan y comercian los datos cosechados con los activos digitales, especialmente las monedas cifradas. Nosotros visualizamos mercados públicos o privados para cualquier forma de activo digital que abarca desde geodatos, electricidad, hasta estados de entrega, donde los productores de datos y los consumidores (compradores y vendedores) se unen, ponen en custodia su oferta y demanda, e intercambian equitativamente sus activos digitales a los precios acordados.

## 2.1 Objetivos de diseño de red

La red Weeve busca establecer confianza entre dispositivos y cultivar estándares emergentes para habilitar la creación de nuevos mercados para el comercio justo de activos entre dispositivos IoT.

### 2.1.1 Calidad de los datos

El objetivo principal de la red es garantizar la calidad de los datos en el mercado. La calidad de los datos se puede definir por la reputación y autenticidad de la entidad que genera los datos, mide el monitoreo y salvaguarda la recolección, procesamiento y transporte de los datos, la validación a través de terceros confiables o mediante un quorum votado democráticamente. Estos mecanismos sirven para el propósito de la certificación de los datos. Uno de los principales obstáculos para la adopción masiva de EoT es la certificación de los datos. Al eliminar este obstáculo, Weeve habilitará una Economía de las Cosas dependiente de información confiable y auténtica. Al vincular los dispositivos a certificaciones de propiedades como la propiedad del dispositivo, el historial de inspecciones y los resultados de las pruebas automatizadas en vivo, la red garantiza la seguridad de los acuerdos de nivel de servicio. Una vez que se implementan las garantías contra el

fraude, la seguridad del mercado mejora, permitiendo a los participantes intercambiar activos digitales con confianza.

### 2.1.2 Estabilidad de la red

Los mercados económicos suponen que todos los agentes son perfectamente racionales. En el mercado de Weeve, esto no es diferente. Los jugadores de Weeve siempre actúan de una manera que maximiza sus utilidades.[2]

Un jugador racional no necesariamente actúa con una estrategia que beneficia a la red. De hecho, un jugador racional es egoísta, juega de manera injusta y no duda en traicionar a sus pares. Estas acciones son críticas para la red, ya que la desestabilizan. Si la red es inestable, habrá una ausencia de una oferta y una demanda sustanciales: no se impedirá que los compradores compren datos falsos o sobrevalorados, mientras que los vendedores carecerán de la justificación para exigir precios más altos.

El diseño de los mecanismos de mercado de la red Weeve asegura que se alcance un equilibrio entre los actores clave y las fuerzas del mercado significativas. En una situación de equilibrio, cada jugador de Weeve buscará una estrategia de maximización de sus utilidades. La idea subyacente del mecanismo de red de Weeve sigue una estrategia de causalidad: los jugadores que apoyan la estabilidad de la red obtienen recompensas, mientras que los jugadores que se desvían de la red son castigados. El mecanismo de recompensa incentiva claramente a los jugadores a unirse a la red, intercambiar sus datos y aportar sus conocimientos y servicios a la estabilidad de la red. Sin mecanismos de incentivos adecuados, la red no subsistirá y los mercados no se fomentarán debido a una oferta y demanda marginales y sin importancia. Por otro lado, el mecanismo de castigo combate las estrategias de desestabilización de la red. Las estrategias desestabilizadoras de jugadores por parte de participantes de la red Weeve resultan en desincentivos y ganancias negativas.

### 2.1.3 Normas descentralizadas regidas por la comunidad

Para una amplia utilización de la red, debemos suponer que varios jugadores, independientemente de sus tecnologías subyacentes (al menos en la etapa inicial del arranque de red), pueden conectarse a la red. Al permitir que los propietarios del mercado establezcan estándares de interoperabilidad y credibilidad, el mercado puede autorregularse de forma descentralizada.

La innovación tecnológica frecuentemente avanza más rápido que los marcos regulatorios, por lo que la capacidad de contar con estándares flexibles y orientados a la comunidad es extremadamente importante. Los dispositivos IoT, al igual que cualquier dispositivo informático, son fabricados por muchas empresas por diversos motivos. Para permitir que empresas no relacionadas construyan

---

[2]En contraste con los seres humanos que actúan ocasionalmente de manera irracional, la red Weeve consiste en máquinas que ejecutan principalmente un diseño de mecanismo computacional. Debido a que el mecanismo se implementa como un protocolo y está codificado en el dispositivo, es poco probable que ocurra una desviación irracional.

dispositivos que operen entre sí, deben seguir los mismos estándares y procedimientos. Al asegurar (cifradamente) estos estándares, los operadores de dispositivos tienen un incentivo económico para seguir el mismo estándar.

La gobernanza se usa para decidir los estándares de membresía relevantes y para revisarlos a lo largo del tiempo. Al empoderar a los usuarios reales de los estándares para determinar el estado futuro de sus propios estándares, todos los participantes de la red Weeve disfrutarán de ciclos de retroalimentación más cortos para las propuestas y deliberaciones grupales. La aparición de estándares ocurrirá en mercados más pequeños y dinámicos, en contraste con los organismos actuales de normas internacionales que lo abarcan todo. Como efecto secundario, la adaptación flexible y contemporánea de los estándares contribuye al aumento gradual de la calidad de los datos y la estabilidad de la red.

### 2.1.4 Resolución de conflictos

Las disputas surgen de forma natural en las economías. Considere, por ejemplo, una disputa entre un comprador y un vendedor donde el comprador afirma que no ha obtenido el bien y el servicio contratado. Cuando se trata de resolución de disputas, existen tres tipos básicos de ellas. El objetivo de la mediación es que un tercero neutral ayude a los participantes a llegar a un consenso por sí mismos.
En lugar de imponer una solución, la mediación trabaja con las partes en conflicto para explorar los intereses que subyacen a sus posiciones. En el arbitraje, un tercero neutral sirve como juez responsable de resolver la disputa.[3] El árbitro analiza la evidencia relevante y luego llega a una decisión vinculante. El tipo resolución de disputas más conocido, el litigio, generalmente involucra a un acusado enfrentado contra un demandante ante un juez o un jurado. El juez o el jurado es responsable de sopesar la evidencia y tomar una decisión.
Los participantes de la red Weeve se aprovecharán de los árbitros para la resolución de disputas, en caso de que no sea posible alcanzar un consenso automático a través de (digamos) un protocolo de resolución de disputas. Observamos que la resolución de disputas también puede ocurrir con la ayuda de un litigio. Las tecnologías de Blockchain proporcionan una infraestructura atractiva para implementar litigios distribuidos y la red de Weeve dejará esta posibilidad abierta para el trabajo futuro.

## 2.2 Participantes de la red y curadores de nodos

A un alto nivel, consideramos un conjunto finito de nodos N = {1, ..., n} que están conectados a la red (o gráfico). Una red es un par (N, g), donde g es un conjunto en los nodos. Si g denota una de las formas estándar en que se representan las redes: por sus matrices de adyacencia y también enumerando los pares de nodos que están conectados. Cada nodo representa a un jugador (o un conjunto de ellos) en la red que posee, controla o cura el nodo (ver Fig. 1).

---

[3] Por ejemplo, https://jury.online/arbitration.

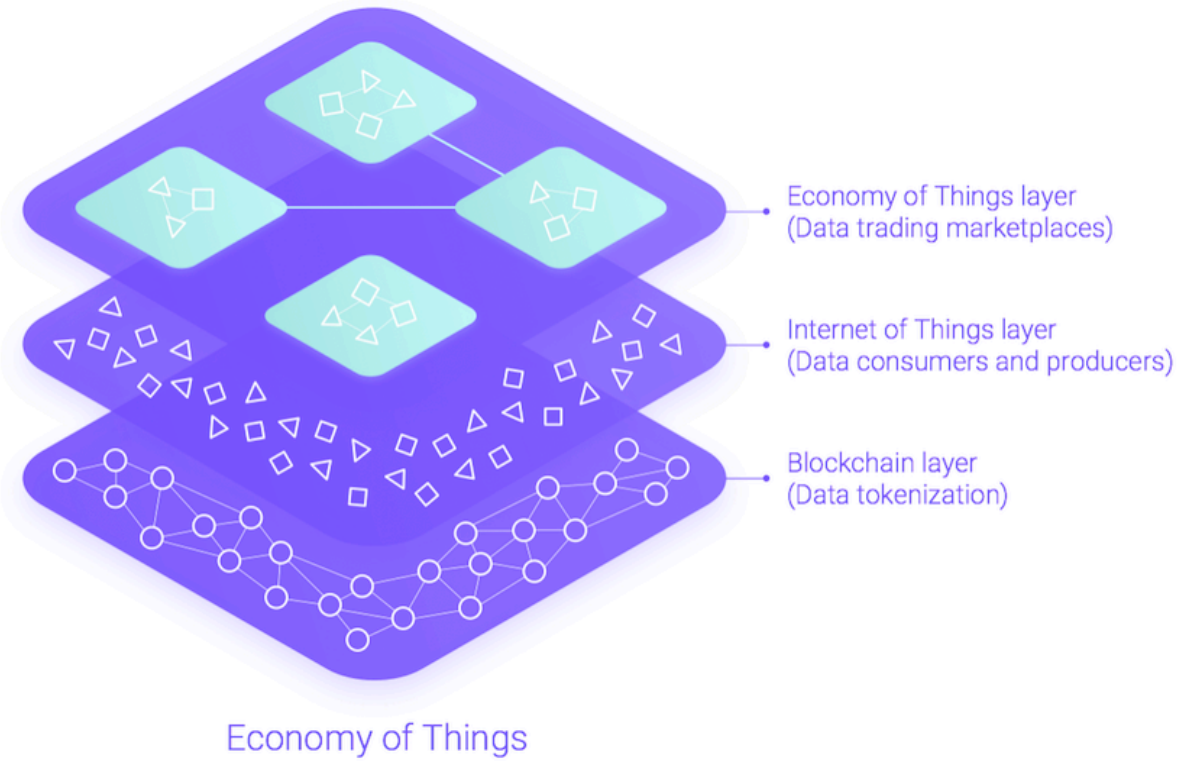


*Figura1: Una red Weeve que consiste en productores y consumidores de datos, mercados, validadores y árbitros.*

## 2.2.1 Nodos

Cada nodo en la red Weeve abstrae una de las siguientes funciones básicas sujetas a enmiendas futuras (ver Sección 5) como se resume en la Figura 2:

El nodo del dispositivo es la fuente y/o el receptor de activos digitales. Bajo su forma más simple, un nodo de dispositivo es una Internet de las Cosas con el propósito de suministrar o exigir activos. En general, es cualquier dispositivo informático que ofrece recursos a la red Weeve o que exige recursos de la misma. A veces nos referiremos a los vendedores como dispositivos que suministran activos y a los compradores como dispositivos que demandan activos. Un activo es cualquier forma de datos tokenizados con un valor potencial.

El Nodo de registro gestiona la propiedad y las propiedades de los dispositivos. Su propósito en la red Weeve es permitir la identificación y clasificación de los dispositivos. Un registro es una lista de dispositivos que se ajustan a ciertos estándares de membresía que mantienen criterios como la identidad del dispositivo, la identidad del propietario del dispositivo, los protocolos compatibles, las estrategias de las transacciones y las capacidades del dispositivo.

Un Nodo de mercado es una puerta de entrada a la actividad económica. Un mercado es un medio que permite a compradores y vendedores de un bien o servicio específico interactuar y facilitar un intercambio. Los bienes y servicios en la red Weeve se centran principalmente en datos tokenizados.

Propietario del dispositivo: realiza transacciones en la red por una tarifa.

Propietario del registro: propone y mantiene las reglas de registro aceptables, como los estándares de membresía, las tarifas de registro y los criterios de validación y políticas de arbitraje.

Propietario del mercado: propone y cura reglas de suscripción aceptables, como los estándares de los dispositivos, las tarifas de registro, los criterios de validación y las políticas de arbitraje.

Validador: evalúa y aplica los estándares de la membresía por una tarifa.

Árbitro: resuelva disputas por una tarifa.

Figura 2: Resumen de los principales jugadores de la red Weeve

El nodo de validación tiene una función de verificación en la red Weeve. La tarea de un nodo de validación es admitir el registro del dispositivo y los nodos de mercado en la clasificación del dispositivo. Los nodos de validación son auditores que evalúan y certifican las propiedades del dispositivo en correspondencia con los estándares de membresía. Examinan la idoneidad del mercado del dispositivo.

El Nodo de arbitraje cumple la función de resolución de disputas en la red Weeve.

### 2.2.2 Curadores y gobernanza

Los nodos cubren las funcionalidades esenciales de la red Weeve. En la práctica, cada uno de los nodos anteriores es de propiedad de, curado y orquestado por una entidad física o jurídica. La entidad puede ser una persona natural, una empresa, un gobierno, una organización sin fines de lucro o cualquier subconjunto de los mismos. Una entidad no solo puede implementarse a través de acciones tomadas por la persona jurídica, sino también a través de un contrato inteligente, un servidor web o cualquier otra interfaz programable. Este enfoque flexible permite un espectro de funcionalidades que va desde la centralización completa y la descentralización completa: las empresas pueden potar por controlar completamente sus nodos mientras que las comunidades o consorcios pueden desear un enfoque más equitativo. Los detalles del sistema de gobernanza se dejan a la implementación del nodo, sujeto al acuerdo de el o los curadores del nodo. Para facilitar la presentación, suponemos que la red de Weeve está compuesta por los siguientes curadores principales ( Figura 1):

- Los propietarios de registros operan registros de dispositivos y definen un estándar de la comunidad para evaluar la reputación de los propietarios de dispositivos y los criterios que respaldan la inclusión en la lista de sus dispositivos. Estos criterios pueden variar desde datos simples - como el monto del depósito - el historial de registros previos, la reputación del fabricante del dispositivo, hasta hechos concretos como una identificación de cifrado única, y soporte para hardware/software con garantías de alta seguridad. También definen los criterios para vetar un dispositivo del registro, así como un protocolo para resolver disputas con la ayuda de validadores y árbitros.

- Los propietarios de dispositivos que deseen utilizar la red y el mercado Weeve, deben unirse al registro de dispositivos. Un registro permite a los usuarios buscar las propiedades de un dispositivo y relacionar el dispositivo con su propietario. Para unirse a los registros de dispositivos, los propietarios de los dispositivos deben asegurarse de que sus dispositivos cumplan con los estándares de membresía establecidos por cada registro deseado. Para ser incluido en la lista, un validador designado por el registro debe evaluar la idoneidad de la membresía.

- Los propietarios del mercado curan los mercados. Al igual que los propietarios de registros, definen el estándar para evaluar la reputación de los propietarios del mercado y la calidad de los activos negociados en ese mercado. Para este fin, definen los criterios que respaldan la lista de dispositivos y la evaluación de la oferta y la demanda de los dispositivos de los activos. También definen los estándares para eliminar dispositivos del mercado y el conjunto de árbitros aptos para resolver disputas entre dispositivos o mercados competitivos. Además del mercado de administración de dispositivos, los curadores acuerdan los parámetros para establecer el mercado, lo que incluye, por ejemplo, el tipo de datos comercializables, el mecanismo de fijación de precios, el modelo de tarifas sujeto a su modelo de negocios (por ejemplo, por dispositivo, por transacción) y el método de pago.

- Los validadores son designados por los registros de dispositivos y verifican el cumplimiento de los miembros con los estándares de membresía. Su función es garantizar que solo los dispositivos de confianza y de alta calidad puedan realizar transacciones en los mercados. La red Weeve delega la designación de validadores y sus procesos a los propietarios del registro.

- Los árbitros resuelven las disputas. Los registros o mercados de dispositivos autorizan a los árbitros a resolver disputas para tipos de transacciones específicos, y en el caso de los tipos de transacciones entre registros, para respaldar la disputa todos los registros involucrados deben tener un conjunto común de árbitros para ese tipo de transacción.

Vale la pena mencionar que los curadores de la red abarcan desde personas naturales individuales hasta cualquier alianza de entidades legales. Específicamente, en ciertos casos, una sola entidad puede adoptar diferentes roles de curador. Por ejemplo, un fabricante de automóviles no solo puede curar automóviles, sino que también puede llevar un registro de los automóviles. Por lo tanto, los

fabricantes de automóviles pueden registrarse en diferentes mercados, como estacionamientos pertenecientes a diferentes operadores, siempre que los automóviles cumplan con los estándares de membresía del mercado. Remitimos al lector al documento de caso de uso para consultar análisis adicionales [1].

# 3 Protocolo de red de Weeve y los tokens

## 3.1 Diseño del mecanismo

El diseño de mecanismos es un campo de la economía dedicado al estudio de mecanismos que incentivan y desincentivan las acciones. Las blockchains aseguran que a través del cifrado y los incentivos alineados adecuadamente, podamos diseñar protocolos de consenso seguros. Sin embargo, las blockchains tienen un significado mucho mayor, cuya utilidad para diseñar protocolos y aplicaciones de seguridad no se ha explorado en toda su magnitud y propósito. La red Weeve considera que Blockchain es un protocolo de capa base que no solo proporciona una tecnología para transferir monedas de una cuenta a
otra, o más en general, que se comunica para almacenar una entrada en una base de datos completamente distribuida y sin permisos, pero también proporciona una infraestructura para protocolos basados en incentivos.

### 3.1.1 Los principios de las decisiones curadas por tokens

Blockchain proporciona la funcionalidad para el uso de tokens. En esto, los tokens tienen utilidad. El aumento de la cantidad de tokens es ampliamente aceptado como recompensa mientras que la disminución de la cantidad de tokens se ve como una penalización. Uno puede usar el mecanismo de recompensa para incentivar las acciones consideradas como "positivas" y el mecanismo de castigo para desincentivar las acciones consideradas como "negativas". Aunque su ejecución es simple, este mecanismo sienta las bases para el diseño de incentivos criptoeconómicos, entre los cuales se encuentran los protocolos de consenso basados en la prueba de depósito, como Casper, aparentemente la aplicación más destacada. La idea clave se puede describir de la siguiente manera: los jugadores depositan tokens para respaldar sus acciones y el protocolo permite impugnar la acción del jugador (y por lo tanto su depósito de garantía). Un poco más concreto, el protocolo consiste en bloquear el depósito, anunciar la impugnación e iniciar una votación en la comunidad donde cada votante paga por un voto en el número de tokens proporcional al depósito. Los votantes ganadores comparten la recompensa proporcional a la participación de los votantes perdedores.

### 3.1.2 La votación cuadrática y los motivos por los cuales una participación mayoritaria no gobierna la red

El protocolo descrito anteriormente (votación) es un ejemplo de una decisión de mayoría curada por tokens. La norma de un voto por persona donde la mayoría gana, trata equitativamente a los titulares de tokens al darles a todos la misma oportunidad de influir en los resultados. En algunas decisiones, sin embargo,

la regla de la mayoría no es la elección correcta, ya que puede dar lugar a una tiranía de la mayoría. Es posible que algunos votantes no puedan participar en el protocolo, ya que no pueden pagar la cantidad de tokens supuestos. Específicamente, cuando la riqueza expresada en fichas se distribuye de manera desigual, una gran cantidad de titulares de fichas, a quienes les importa poco el resultado, prevalecen sobre una minoría que se preocupa apasionadamente, lo que resulta en una disminución del bienestar general.

La votación cuadrática es la idea más importante para las leyes y las políticas públicas que han surgido de la economía en (al menos) los últimos diez años. Cada votante puede comprar votos a favor o en contra de una propuesta, mediante el pago de tokens por el cuadrado de la cantidad de votos que él o ella compra. El depósito se devuelve a los votantes sobre una base individual. Weyl y Lalley demuestran que la decisión colectiva se aproxima rápidamente a la eficiencia a medida que aumenta el número de votantes [2]. Weyl prueba además que la votación cuadrática es bastante robusta ante la colusión, el fraude y el comportamiento "irracional" de los votantes; algunas propiedades que la votación por mayoría no proporciona [3].

La red Weeve considera que la votación cuadrática (o sus variantes, como el voto cúbico o exponencial) es una herramienta esencial en las decisiones curadas con tokens, específicamente en economías donde la distribución uniforme de tokens es improbable. Esta es una situación en la que las partes interesadas, como las empresas o las alianzas industriales, poseen una gran participación. (En el caso más extremo, tienen más del 51% de la cantidad total de tokens de los votantes). Los curadores de la red Weeve tienen la opción de seleccionar la regla de votación que mejor se adapte a su comunidad y su idea de un proceso de decisión democrático.

### 3.1.3 Incentivos de la generación de datos de alta calidad

La red de Weeve tiene como objetivo alentar a los propietarios de dispositivos a administrar sus dispositivos con mucho cuidado y diligencia. Los dispositivos son la fuente de la red Weeve. Recordemos que son los productores y consumidores de activos digitales y el motor de la oferta y la demanda. Los propietarios de los dispositivos tienen un incentivo inherente para unirse a la red Weeve: los productores están interesados en obtener ganancias, mientras que los consumidores buscan activos. Los mercados abordan estas motivaciones de manera ejemplar. Para facilitar el funcionamiento de los mercados y generar la tracción de los datos, la red Weeve comprende mercados con diferentes temas de activos (por ejemplo, geodatos, temperatura), calidad de datos y requisitos que los dispositivos deben cumplir para unirse.

El axioma de la red Weeve es que los propietarios de los dispositivos deben registrar sus dispositivos
en un registro de dispositivos que cumpla con el estándar de membresía del mercado. Debe tener en cuenta que cuando el dispositivo se incluye en un registro, puede conectarse a todos los mercados que respaldan los estándares de registro, o un subconjunto de los mismos. La decisión del diseño es facilitar la habilitación de la interconexión de dispositivos entre diferentes mercados. Los dispositivos deberán acceder e interactuar con mercados con estándares similares. Esto hace que todo el concepto sea más general y poderoso.

Los propietarios de dispositivos, por lo tanto, desean que la consideración se incluya en registros de alta calidad. Permiten la participación en mercados de alta calidad donde se espera que los activos digitales se negocien a un precio más alto, en lugar de la participación en mercados de baja calidad. Para convertirse en miembro de un registro, los propietarios de los dispositivos forman parte de una decisión curada por tokens. Es decir, depositan tokens por dispositivo sujetos al estándar de membresía y la política de registro.

Los validadores participan en la votación y corresponde a la política de registro designar validadores. Dependiendo del tipo de registro, los validadores pueden variar desde entidades distinguidas hasta cualquier titular de token, incluidos los propietarios del registro. Los validadores tienen el propósito de probar la conformidad del dispositivo con el estándar de membresía del registro. Su incentivo para participar en una decisión protegida por un símbolo es doble. Primero, reciben una remuneración por la votación, que equivale a la parte del depósito incautado. En segundo lugar, los validadores desean mantener alta la demanda del token que poseen, ya que esto aumenta su precio. Esto sucede si los validadores aseguran una red estable con registros y dispositivos de alta calidad.

Los propietarios de los dispositivos, que creen que serán rechazados, no se aplicarán al registro, ya que esto resultaría en una pérdida financiera para ellos. En caso de rechazo, su depósito se pierde y se divide como un premio entre los titulares de fichas que participaron en el proceso de impugnación. Si fueron aceptados, su depósito se bloquea, pero puede ser retirado en cualquier momento que el propietario del dispositivo desee abandonar el registro.

### 3.1.4 Incentivos de registros de dispositivos de alto estándar

Los registros de dispositivos juegan un papel crucial en la red. Se ha puesto un gran énfasis en el diseño del mecanismo de la red Weeve para cultivar registros de dispositivos significativos, ya que un registro con (muchos) dispositivos defectuosos daña la estabilidad de la red.

Para su creación, los propietarios de registros deben hacer un depósito proporcional a la cantidad de dispositivos registrados. En general, cualquier titular de token puede emitir un registro. Como los registros de alta calidad requieren una cantidad significativa de tokens, los registros son ante que nada, un instrumento
para empresas o alianzas de titulares de tokens. Al igual que en los grupos de interés más grandes, las decisiones se toman de forma democrática, con la expectativa de que la mayoría de los propietarios de los registros superará en número a los malos curadores. Para motivar aún más a los propietarios a orquestar registros "buenos", su depósito se utiliza como garantía en decisiones controladas por tokens.

En el caso de que exista evidencia de una infracción a la norma de membresía, los propietarios del registro pueden ser impugnados por los mercados involucrados con el registro en caso de que exista evidencia de una infracción a la norma de membresía. En esencia, una infracción de membresía ocurre cuando un dispositivo registrado produce datos falsificados. En la práctica, los propietarios del mercado deben especificar términos más generales de la infracción. Además, los titulares de tokens, incluidos los propietarios de registros, pueden anunciar la impugnación de otros registros. La lógica aquí es prevenir cualquier forma de infracción. Supongamos que se produce una forma de plagio de dispositivos o datos, una infracción de marca registrada, una falsificación de marca y

una infracción de patente, como resultado de un registro "malo". La capacidad de impugnar el registro desincentiva a los propietarios del registro falsificado , ya que esto resultaría en una pérdida económica de su depósito.

Queda por ver por qué curar un registro es atractivo, ya que los propietarios pueden arriesgarse a perder su depósito. Los propietarios del registro establecen los cánones cuando se trata de hacer cumplir los estándares de membresía a través de la aceptación y el rechazo de las aplicaciones del dispositivo. Su incentivo es contribuir a la calidad de la red Weeve, ya que esto mantiene alta la demanda del token que poseen y aumenta su precio.

### 3.1.5 Incentivos de la curación de mercados

Dado el hecho que los mercados reciben una remuneración por cada transacción exitosa de activos digitales, sujeto al modelo de negocios del mercado, la oportunidad de obtener ingresos es una motivación obvia para administrar y organizar los mercados. Para operar un mercado, los propietarios del mercado hacen un depósito de garantía. La garantía es un depósito de seguridad y se utiliza en una decisión curada por tokens para incentivar a los propietarios a garantizar el comercio justo. Los dispositivos que intercambian activos digitales pueden impugnar al mercado en caso de disputa. Un mercado maligno puede emular la disponibilidad de datos de alta calidad, pero de hecho ofrece datos de baja calidad de dispositivos que no cumplen con el estándar de membresía propuesto. Del mismo modo, un mercado "malo" puede no maximizar la utilidad del proveedor y los demandantes, lo que da como resultado un precio no justificado para el activo negociado. En esos casos, el dispositivo o los propietarios de dispositivos pueden anunciar una impugnación contra el mercado por su depósito o garantía.

Es importante tener en cuenta que los tokens depositados se bloquean e inutilizan durante el período del garantía, incluso para la red Weeve. El protocolo no permitirá que ninguna entidad use estos tokens, e incluye a la red Weeve. Para que cualquiera pueda obtener acceso a estos tokens en garantía, uno necesitaría comprar el 51 por ciento de los mil millones de tokens en circulación y obtener acceso al protocolo en sí, lo cual es un escenario altamente improbable (consulte la Sección 3.1.2). La razón por la cual es altamente improbable, es que una vez que los demás usuarios de la red sepan que se está realizando una centralización intencional de la red Weeve (lo que se puede hacer fácilmente mediante un anuncio público virtual), el incentivo para permanecer en la red sería nulo. En este escenario, todos los usuarios honestos desbloquearían sus depósitos, cambiarían a la red bifurcada que se convertiría en la nueva red Weeve y por lo tanto quitarían todo el valor a la red original. Si no hubiera usuarios en la red centralizada deshonesta, el incentivo para que cualquier entidad obtenga acceso al protocolo sería cercana a cero. En esencia, cualquier jugador dominante gastaría muchos tokens Weeve para obtener el control de una red potencialmente inútil, ya que una vez que gana acceso mayoritario, el sistema honesto simplemente cambiaría a uno bifurcado, echando por tierra la iniciativa por carecer de utilidad.

### 3.1.6 Los token de Weeve y porqué son necesarios

El token de Weeve (WEEV) es el token nativo de la red Weeve y es necesario para la operación del protocolo de red. Tiene un suministro fijo sin una función de registro incorporada. Sus funciones principales se resumen en la Figura 3. El token WEEV es necesario para que la red para garantice que los participantes rindan cuentas de sus acciones y, por lo tanto, se alineen en el largo plazo. Una red con participantes de alta calidad y transacciones auténticas tiene un valor intrínseco más alto y esto debería reflejarse en el valor de los tokens y viceversa. Si, por ejemplo, se utilizara Ether en lugar de WEEV, entonces el valor de la red Ether probablemente eclipsaría enormemente al de la red Weeve, lo que significa que no hay un incentivo a largo plazo para que los participantes mejoren activamente su propia red y que no existe un incentivo de largo plazo para que los participantes eviten la destrucción de su propia red a través de actividades negativas como la especulación.

**Incentivos:** el token WEEV fomenta las acciones de red positivas.

- Los propietarios de dispositivos depositan tokens para registrar un dispositivo en el registro de dispositivos
- Los propietarios del registro depositan tokens para crear un nuevo registro de dispositivos
- Los propietarios del mercado depositan tokens para crear un nuevo mercado
- Se utiliza para el pago de pagos a validadores y árbitros

**Desincentivos:** el token WEEV desalienta las acciones de red defectuosas.

- Como garantía para penalizar a los dispositivos infractores que explotan los recursos de la red
- Como garantía para castigar los registros de dispositivos infractores que degradan la calidad de la red
- Como garantía para castigar a los mercados que realizan cualquier tipo de infracción

*Figura 3: Resumen de los mecanismos de incentivo de tokens WEEV*

En otras palabras, Ether o cualquier token relacionado no refleja la dinámica de la red Weeve. Puede haber situaciones en las que las fluctuaciones del precio de Ether sean completamente ortogonales respecto del rendimiento de la red Weeve. El token WEEV se desacopla de las fluctuaciones y brinda a los titulares de tokens una herramienta justa y confiable para evaluar el valor de la red. Esto se refleja en el precio de los tokens WEEV.

## 3.2 Protocolo de red de Weeve

El protocolo de red de Weeve (Figura 4) especifica la participación de alto nivel de los nodos en la red Weeve y la integración de servicios de terceros. Cada registro de dispositivos y propietario de mercado deposita el token WEEV como garantía. La regla general impuesta es que cuanto más valor deseen los propietarios, más depósitos se requerirán como garantía, sujetas a validación y arbitraje (detalles a continuación). Cada función en el protocolo tiene como objetivo aumentar la interoperabilidad, crear confianza, o ambos.

Para aumentar la interoperabilidad, el protocolo especifica estándares de membresía, tipos de transacción, listas de dispositivos, listas del historial de transacciones y la intermediación de nuevas transacciones. Estos componentes proporcionan suficiente información y herramientas para negociar un tipo de transacción compartido, comprometer el nuevo tipo de transacción e iniciar solicitudes de transacción con respuestas.

Para iniciar la confianza, el protocolo especifica pautas de validación, acceso a registros de actividad, listas de validadores y mecanismos de resolución de disputas. Estos elementos permiten a los registros proporcionar garantías razonables de que las transacciones serán genuinas y libres de errores.

El protocolo de red de Weeve no tiene como objetivo resolver el fraude de datos de forma directa. Sin embargo, permite que los individuos y los mercados acuerden qué define la confianza y dónde se debe establecer el límite.

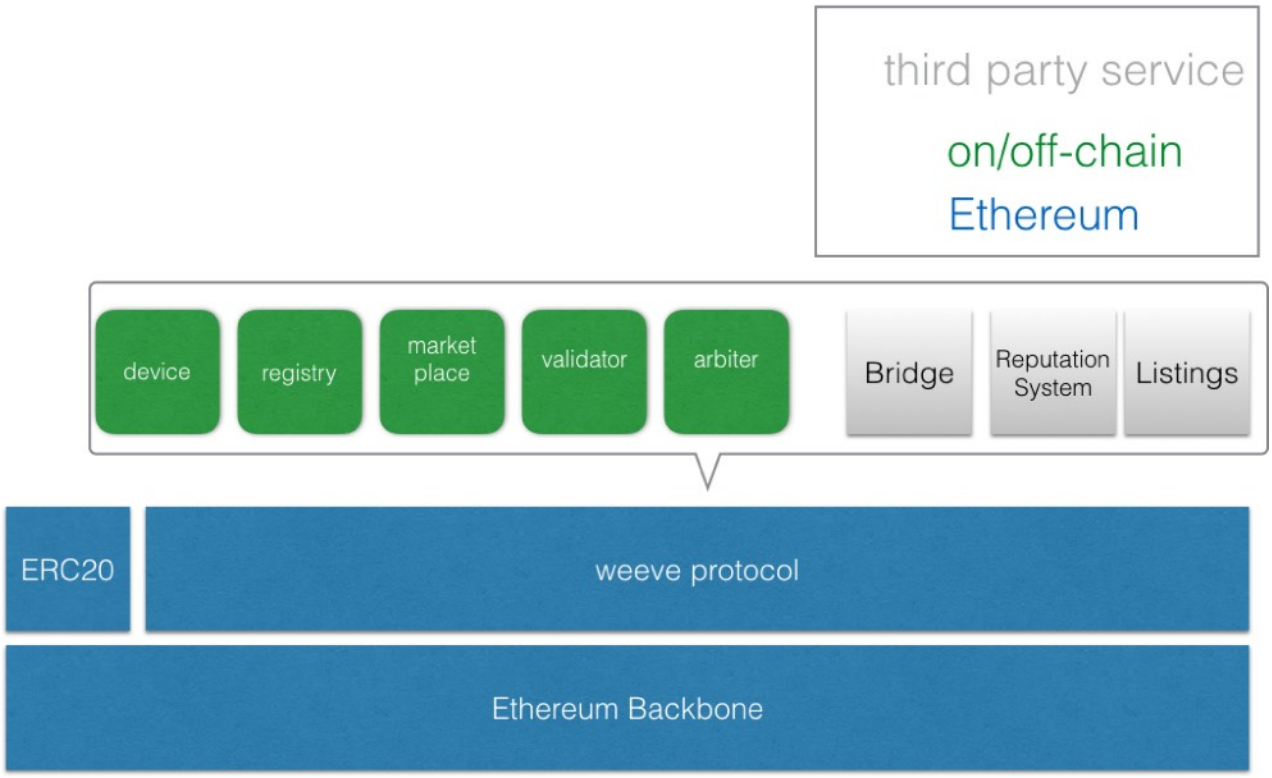


*Figura 4: Descripción general del protocolo Weeve*

### 3.2.1 Estándares de membresía

La especificación de los estándares de membresía debe priorizar:

- Especificaciones y razonamiento amigables con humanos

- Estructura general y secciones estándar
- Acceso para las partes relevantes
- Detalles técnicos para realizar implementaciones cuando corresponda, tales como estructuras de datos
- Un formato simple
- Un contacto con el autor actualizado
- Fechas, horas e historial de actualización de documentos

Debido a la gran cantidad de posibles tipos de registro de dispositivos, actualmente no se conoce el mejor formato individual para la especificación de los estándares de membresía, pero debiera surgir uno o más estándares viables a medida que se adquiera experiencia. Las conversaciones con socios potenciales de IoT en todas las industrias han revelado requisitos muy diferentes para los estándares de membresía, lo que da más crédito al dilema de la interoperabilidad de IoT. Por este motivo, es mejor evitar las recomendaciones excesivas ante la incertidumbre.

Los documentos digitales que contienen los estándares de membresía para un registro pueden ser bastante voluminosos, como cuando contienen archivos adjuntos con detalles y especificaciones técnicas y tablas de datos incorporadas. Por lo tanto, los estándares de membresía deben almacenarse fuera de la cadena con entramados en la cadena, como en un clúster IPFS[6] o en un proveedor de almacenamiento inmutable y descentralizado.

Los cambios en los estándares de registro deben ser legitimados por los criterios de gobernanza de los registros de dispositivos y se deben registrar de forma inmutable para que los miembros del registro y los miembros del mercado los revisen. Los creadores del mercado deben aplicar un conjunto similar de estándares. Se debe reiterar que los estándares de membresía variarán drásticamente dependiendo de los registros de dispositivos específicos y de los creadores del mercado; un registro de dispositivos para teteras conectadas no requiere los mismos estándares estrictos de membresía que un registro para un equipo militar.

### 3.2.2 Pautas de validación y arbitraje

Como documentos complementarios a los estándares de membresía, los propietarios de registros y mercados proporcionan pautas de validación y arbitraje como herramientas de evaluación de validadores y árbitros designados. Las pautas de validación, que pueden verse como un estándar de auditoría, sirven como contrato de trabajo entre el registro/mercado y sus validadores, delineando acuerdos tales como evaluaciones automatizadas (por ejemplo, a través de un protocolo de atestación remota [4]), evaluaciones manuales (como inspección del hardware), líneas de tiempo, criterios de aceptación y resolución de disputas para los validadores. Una vez que un dispositivo ha iniciado su solicitud a un mercado, estas pautas de validación sirven como fuente. Un propósito similar a la búsqueda de pautas arbitrarias. En esencia, permiten especificar el árbitro en caso de una disputa y hacer uso de interfaces de funciones similares a las de los validadores.

[6]https://ipfs.io/

Estos documentos de directrices debieran ser similares en su estructura a las plantillas y pautas de evaluación del Programa FedRAMP[47], que son, por ejemplo, utilizadas por el Gobierno Federal de EE.UU. para proporcionar a la industria un enfoque estandarizado de la evaluación de seguridad, la autorización y monitoreo continuo de los productos y servicios en la nube. Además, el sitio web del programa proporciona una lista de asesores autorizados, del mismo modo que cada registro de dispositivos contiene listas de validadores designados. Las pautas de validación deben priorizar:

- Directrices y razonamiento amigables con humanos
- Puntos de anclaje de documentos referenciables por máquina para admitir la comprobación automatizada y los formatos de elaboración de informes digitales
- Acceso para validadores y árbitros
- Detalles técnicos para implementaciones cuando corresponda, incluido el código fuente o los servicios de terceros utilizados para la evaluación
- Puntos de anclaje de documentos referenciables por máquina para admitir la comprobación automatizada y los formatos de elaboración de informes digitales
- Listas de verificación y rúbricas de calificación para las validaciones deseadas
- Retroalimentación cualitativa y cuantitativa que incluye una alineación general con los estándares de membresía, fortalezas y debilidades sobresalientes, historial del solicitante con respecto a los estándares de membresía
- Información de contacto del autor actualizada
- Fechas, horas e historial de actualización de documentos

### 3.2.3 Registros de actividad

Se alienta a los propietarios de registros y mercados a mantener registros de actividad de transacciones para los eventos que ocurren en el registro y el mercado. Los árbitros podrán acceder a un subconjunto de registros de actividad para resolver disputas con los datos relevantes. Si un árbitro intenta resolver una disputa y no se dispone de los registros de actividad de transacciones de una de las partes, es probable que el árbitro falle a favor de la parte que presenta la evidencia. Por lo tanto, los propietarios de los mercados tenderán a mantener buenos registros para mejorar los resultados de sus disputas.

Específicamente, es posible que los propietarios de mercados deseen verificar los registros de actividad de las transacciones relevantes de sus partes de la transacción para garantizar la

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

coherencia e integridad de los historiales de transacciones o de las validaciones del dispositivo. Estos también son útiles en una fase de impugnación cuando se evalúa la confiabilidad de un dispositivo.

Los registros de actividad deberían poder filtrarse, al menos, por:

- Fecha
- Tipo de actividad
- ID del participante

Se recomienda encarecidamente que los siguientes eventos produzcan entradas de registro detalladas:

- Cambios de gobernanza
- Cambios de propuestas y referencias
- Resultados de votaciones
- Transacciones
- Cambios a los estándares de la calidad
- Cambios a las pautas de validación
- Cambios a los tipos de transacción
- Cambios a la lista de dispositivos
- Cambios en los metadatos del dispositivo

En algunas situaciones, puede ser relevante la privacidad de los registros de actividad. En ese caso, la red Weeve sugerirá tecnologías para mejorar la privacidad, como el cómputo de múltiples partes o el cifrado funcional.

### 3.2.4 Tipos de transacciones

Los propietarios del registro y del mercado tendrán la capacidad de especificar tipos de transacción a través de documentos de estilo RFC, bibliotecas y código de muestra. Estas bibliotecas de transacciones deben registrar los datos relevantes para fines de disputa y arbitraje en el registro de

actividad. Este requisito permite a los árbitros contar con los hechos relevantes al determinar los resultados de los casos y resulta esencial para un mercado seguro.

Los estándares de membresía pueden incluir requisitos que fomentan aún más la interoperabilidad de los dispositivos, como los URI de dispositivos, el soporte de protocolos específicos de transacciones, los puntos de conexión de servicio, los proveedores de almacenamiento de datos, las unidades de medida de datos y más. Estos requisitos sirven como la base que permite el intercambio entre dispositivos, ya sea simplemente de datos sin procesar o transacciones más complejas como subastas, negociaciones de precio y capacidades avanzadas de consulta. Los estándares de membresía otorgan a los tipos de transacción una base sobre la cual pueden operar.

Para determinar las capas de transporte en los tipos de transacciones, se recomienda a los registros de dispositivos que utilicen el protocolo MQTTS[8], diseñados específicamente por el equipo Weeve, que admiten comunicaciones seguras del dispositivo de IoT como el direccionamiento, la gestión de sesiones, la transferencia de datos y la confirmación. Para determinar las capas de pago en los tipos de transacción, se recomienda a los registros de dispositivos que utilicen protocolos justos de intercambio[9]. Estos respaldan el depósito en garantía de la oferta y la demanda, la negociación de precios y el reconocimiento de entrega. Otras capas de servicio pueden agregarse de manera similar a los tipos de transacción.

[8]Consulte la sección 2.2, http://papers.weeve.network/weeve_whitepaper.pdf
[9]Consulte la sección 2.5, http://papers.weeve.network/weeve_whitepaper.pdf

Los propietarios del registro y del mercado pueden especificar parámetros, según el tipo de transacción, relacionados con el proceso de arbitraje, en donde una o más partes disputan una transacción y requieren una resolución. Estos parámetros incluyen, pero no están limitados a:

- Marcos de tiempo para las disputas
- Montos mínimo y máximo de disputas
- Pautas de resolución
- Pautas de selección de árbitros
- Elección del sistema de arbitraje modular

### 3.2.5 Transacciones

Cada transacción debe tener un identificador de transacción único, un identificador de dispositivo único, un tipo de transacción y los metadatos de transacción correspondientes registrados y autenticados, o certificados en la cadena. Este requisito garantiza que las transacciones sean atómicas, de modo que en caso de disputas y arbitrajes, estén acompañadas con los mejores datos posibles de las transacciones y sus participantes. Las transacciones sin registros en cadena no disfrutarán de una protección completa de la red Weeve en caso de una disputa.

### 3.2.6 Interfaces de metadatos

Los metadatos para dispositivos y transacciones pueden y deben representarse en una diversidad de formatos, incluidos JSON, XMLS, protocolos de cable y blobs binarios, según su caso de uso. Por ejemplo, los formatos de metadatos utilizados en las máquinas comerciales de alta frecuencia pueden requerir paquetes de datos mucho más compactos que los formatos utilizados para las casetas de peaje de las autopistas. Por lo tanto, no es razonable requerir ningún formato particular de representación de metadatos. Sin embargo, en aras de la interoperabilidad, debe haber al menos un método común para acceder a estos metadatos. Por lo tanto, el registro y el mercado requerirán funcionalidades básicas de lista, filtrado, creación y acceso para que se encuentren disponibles para los contratos inteligentes. Estos requisitos se implementarán inicialmente como una especificación de interfaz para contratos inteligentes, e incorporarán también componentes de autenticación y autorización.

## 3.3 Interfaz del protocolo Weeve

Es posible implementar un nodo Weeve utilizando una variedad de tecnologías subyacentes, desde servidores centralizados administrados por empresas tradicionales hasta contratos inteligentes completamente descentralizados gobernados por una comunidad de entusiastas de dispositivos IoT. Esta flexibilidad permite el intercambio entre cualquier grupo de personas, ya sea que se trate de grandes entidades corporativas o individuos muy involucrados. Un contrato inteligente implementa las interfaces de protocolo y satisface varios requisitos de firma de función, tal como se describe en un nivel general en las secciones a continuación.

En resumen, cada nodo debe implementar funciones que admitan:

- El depósito de garantía y la eliminación de éste en el contrato inteligente de la red Weeve (el depósito y la eliminación del depósito se haría en múltiples niveles, es decir, en el registro, en el mercado, etc., para los dispositivos que deseen participar en la red weeve)
- La recuperación de estándares de membresía
- La recuperación de pautas de validación
- La recuperación de tipos admitidos de transacciones
- La consulta de registros de actividad
- Las listas de dispositivos y metadatos
- Las listas de historiales de transacciones y metadatos
- Las listas de validadores (Registros y Mercados)
- Las listas de árbitros (Registros y Mercados)

### 3.3.1 Inclusión y exclusión de listas

Los posibles propietarios pueden depositar una cantidad significativa de tokens WEEV, proporcional a sus volúmenes de transacción deseados y previstos, a la cantidad de dispositivos en lista, etc. (el mecanismo se ha dejado abierto por ahora para permitir su flexibilidad) con el objetivo de crear nuevos registros de dispositivos y mercados, respectivamente. Como parte del proceso de creación, el depósito se debe realizar a través del registro del dispositivo y (resp. mercado) que contiene al menos un dispositivo de inicialización conforme a los estándares de membresía. Esto sirve como demostración de que los estándares son, de hecho, alcanzables.

Recordemos, necesitamos depósitos de los propietarios del registro para prevenir la ofensas entre registros. Utilizando mecanismos de incentivo de la teoría de juegos, ningún creador de registro tendría incentivos engañar el sistema, o sacarlo de su estado de honestidad, sin enfrentar el riesgo de perder su depósito y ser reconocido como deshonesto en el sistema. Este mecanismo de depósito está profundamente arraigado en el sistema en todos los niveles, desde la creación de registros y la creación de mercados, hasta la inclusión en listas de dispositivos en registros y mercados.

Si el dispositivo de inicialización se elimina de la lista sin que aparezca ningún otro dispositivo válido en el registro, el registro del dispositivo (resp. mercado) se libera y el propietario puede destruir el registro (resp. mercado) retirando el depósito. La red Weeve puede entonces, eventualmente, implementar un proceso de recolección de basura mediante el cual se requiera que registros y mercados pasen por simples controles de vigencia para permanecer en buen estado. El dispositivo de inicialización no tiene un estado especial en el registro (resp. mercado) más allá de servir como demostración inicial de los estándares de membresía alcanzables. Estas medidas de depósitos y demostración buscan desalentar la creación de nodos de baja calidad en la red Weeve y facilitar su eliminación. Inicialmente, todos los registros nuevos estarán sujetos a la aprobación de validadores elegidos por la red para proteger al ecosistema naciente de la contaminación, sin embargo,

el objetivo a largo plazo de los proyectos es la gobernanza descentralizada impulsada por la comunidad, que posiblemente imite los sistemas de impugnación del solicitante de ciertos nodos.

### 3.3.2 Recuperación de estándares de membresía

Es necesario que los nodos puedan acceder a los estándares de membresía de otros registros. Por lo tanto, todos los nodos deben admitir consultas desde la red. En la implementación de la interfaz, la función devuelve estándares de membresía firmados para autenticar datos confidenciales.

### 3.3.3 Recuperación de las pautas de validación

Al igual que con los estándares de membresía, un nodo también debe poder acceder a las pautas de validación y arbitraje de otros registros/mercados. En la implementación de la interfaz, la función pasa por el registro firmado y el origen del dispositivo para permitir las restricciones adecuada de las pautas de validación/arbitraje devueltas con el objetivo de proteger los datos sensibles.

### 3.3.4 Recuperación de tipos de transacciones admitidos

Durante la creación de los registros, los propietarios del registro podrán especificar los tipos de transacciones admitidas por el registro, incluidos los detalles del protocolo por tipo de transacción, tales como convenciones de llamadas, tiempos, cálculos de precios, estructuras de datos relevantes y requisitos de entrega. Estos tipos de transacciones deben ponerse a disposición para su inclusión en la lista por medio de una implementación de la interfaz y pueden estar protegidos por controles de permisos.

### 3.3.5 Registros de actividad de consulta

Los registros de actividad son una vía para que los registros de dispositivos y los mercados brinden transparencia a los posibles creadores del mercado. Al proporcionar una interfaz que expone los registros de validación y el historial de gobernanza, un posible mercado puede tener más certeza de que un dispositivo dentro del registro del dispositivo entregará según lo prometido.

### 3.3.6 Listas de dispositivos y metadatos

Los dispositivos y sus metadatos pueden solicitarse a pedido. La función de lista de dispositivos en el contrato inteligente es utilizada por los registros y mercados para encontrar otros dispositivos. Todas las consultas pueden ser autenticadas y autorizadas por el sistema de seguridad de cada registro de dispositivos.

### 3.3.7 Lista de transacciones y metadatos

Las transacciones y sus metadatos pueden solicitarse a pedido. La función de lista de transacciones en el contrato inteligente es utilizada por otros dispositivos para verificar transacciones históricas y hacer referencia a otros. Todas las consultas pueden ser autenticadas y autorizadas por el sistema de seguridad de cada registro de dispositivos.

### 3.3.8 Lista de validadores

Los propietarios del registro pueden designar validadores para cumplir los criterios de validación de los estándares de membresía, que pueden ser una combinación de tareas automáticas y manuales. Debe exponerse una interfaz para proporcionar una lista de validadores activos.

### 3.3.9 Lista de árbitros

Los propietarios de registros y de mercados pueden designar árbitros como terceros independientes e imparciales para resolver disputas. Debe exponerse una interfaz para proporcionar una lista de árbitros activos. Estas listas contienen metadatos, como información de la cuenta, y se usan para autenticar y autorizar a los árbitros a ver ciertos registros de actividad en todos los Registros de dispositivos. Esto se usa con el propósito de resolver disputas.

## 4 Disputas y arbitrajes

El arbitraje se vuelve necesario cuando al menos una parte de una transacción inicia una disputa. La inicialización de la disputa debe recopilar automáticamente todos los detalles relevantes de la transacción almacenados en la cadena o fuera de ella y recopilar datos adicionales de las partes de la transacción, según sea necesario. Las disputas sobre transacciones de origen humano deben recibir un tratamiento diferente a las disputas derivadas de transacciones originadas en la máquina. Por ejemplo, la resolución de disputas para millones de transacciones de dispositivos en milisegundos puede requerir agregación, análisis y deliberación por parte de agentes humanos, de forma similar a los procesos de descubrimiento electrónico experimentados por empresas en litigio.

Por ejemplo, en un mercado de vehículos eléctricos que buscan estaciones de carga, los estándares de membresía pueden requerir que los vehículos eléctricos tomen instantáneas de la carga de la batería del vehículo, el kilometraje, la presión de los neumáticos, etc. Esta información podría usarse para determinar si un vehículo eléctrico recibió la cantidad total de carga que se le otorgó, con pruebas que corroboren la manipulación. De esta forma, los árbitros están completamente equipados con la mejor información disponible para tomar una decisión.

## 4.1 Él dijo, ella dijo

Al igual que en las plataformas con múltiples caras existentes, se puede utilizar un sistema de reputación para ayudar a resolver disputas en el caso de visiones en conflicto y sin fundamentos de un evento. Los sistemas de reputación están fuera del alcance del Protocolo de red Weeve, pero son posibles y se fomentan por registro de dispositivos, o entre ellos.

## 4.2 Almacenamiento

Inicialmente, cada registro y mercado de dispositivos proporcionará recursos para acceder, almacenar y administrar las estructuras de datos para fines de disputas y arbitrajes. A largo plazo, se admitirán para que los registros descentralizados de validadores y árbitros puedan

realizar una validación cruzada en un dominio similar o confiar en un servicio descentralizado que proporciona administración de validación (kleros, delphi, etc.).

## 4.3 Servicios de terceros

Varios proyectos en el ecosistema de Blockchain ya están trabajando en sistemas abiertos y equitativos para la adjudicación, incluyendo Delphi y Kleros, y se han realizado esfuerzos durante la implementación del contrato inteligente para admitir la compatibilidad total con estos servicios de arbitraje conectables a petición de propietarios de registros y mercados. Muchos de estos servicios aún requieren el nombramiento legítimo de árbitros equitativos, por lo que en estos casos, la selección del árbitro seguirá siendo responsabilidad de los propietarios. Además, las variables relacionadas con el arbitraje, como el marco de tiempo de la disputa, los importes mínimos y máximos de la disputa y las tarifas del árbitro ya han sido establecidos por los propietarios en los tipos de transacción.

## 4.4 Arbitraje entre registros

Para el arbitraje en múltiples registros, es posible que se permita a los árbitros certificados por todos los registros y mercados participantes para tipos de transacciones específicos, arbitrar las disputas correspondientes por una tarifa. En el futuro, podemos imaginar a varios árbitros, cada uno en representación de los intereses de su registro, llegar a un consenso, a diferencia de los ajustadores de reclamos actuales.

# 5 Funcionalidad de la capa superior

Así como las capas de las aplicaciones residen encima de las capas de sesión en el modelo OSI, los servicios importantes para garantizar la estabilidad de la red pueden existir utilizando primitivas provistas por el protocolo de red de Weeve. Las siguientes secciones describen características que no forman parte del protocolo de red de Weeve, pero están profundamente interconectadas y consideramos su integración como un aporte viable de la red en el futuro.

### 5.1 Listas de registros de dispositivos y mercados

Los registros de dispositivos y mercados pueden incluirse en listas en la plataforma Weeve y, finalmente, etiquetarse con atributos como la geografía, el tipo de registro y los estándares de membresía públicamente disponibles. La evaluación y aprobación de listas puede incluir inicialmente todos los registros de dispositivos depositados que aceptan, pero a largo plazo, la decisión final sobre esta actividad debe dejarse a la comunidad. Es posible usar un registro de dispositivos para que contenga la membresía de otros registros, pero esta estructura recursiva es compleja y se considera fuera del alcance de las implementaciones iniciales de contratos inteligentes. Estas listas estarán disponibles para las partes relevantes a través de un sitio web mantenido por la plataforma Weeve y, eventualmente, también a través de dApps, a medida que

ecosistemas como Blockstack[5] alcancen la madurez. Se admitirá el inicio de sesión a través de una cartera de monedas cifradas, para permitir el acceso autorizado a las listas de registros de dispositivos.

## 5.2 Sistemas de reputación

Los sistemas de reputación garantizan la seguridad del mercado al permitir que los participantes del mercado sepan con quién están realizando transacciones. Si bien los sistemas de reputación no serán parte del Protocolo de registro de dispositivos Weeve, constituyen no obstante, construcciones importantes que aportan significativamente a habilitar nuevas formas de comercio. Por lo tanto, la plataforma Weeve proporcionará libremente bloques de construcción para que los Propietarios de registros implementen sistemas de reputación encima del protocolo.

Estos sistemas se implementarán como contratos inteligentes anclados a los identificadores de dispositivos y Registros de dispositivos. Actualizarán los perfiles individuales al leer historiales de transacciones y registrar los resultados de arbitrajes y disputas. El sistema debe ser altamente personalizable ya que las diferentes formas de comercio justificarán diferentes resultados para las reputaciones de dispositivos.

Por ejemplo, los mercados impulsados por participantes humanos requerirán interfaces de usuario para
comunicar completamente la semántica de una reputación con el fin de que los humanos tomen mejores decisiones. Por el contrario, cerca de los mercados completamente automatizados en los que los dispositivos se involucran en operaciones de alta frecuencia, pueden usar métodos estadísticos para analizar datos en busca de actualizaciones algorítmicas de reputaciones y clasificar automáticamente a los socios comerciales deseables sin intervención humana.

## 5.3 Transacciones al interior de Blockchain ("Puente")

La tecnología de Blockchain es incipiente y pueden haber muchas blockchains que compiten y que sirven como infraestructura para los protocolos. La primera iteración de la red Weeve se creará sobre el blockchain Ethereum, pero debe adaptarse a evoluciones futuras o competidores que proporcionan bases subyacentes de facto. Por lo tanto, es importante adoptar un enfoque flexible que sea razonablemente independiente de la implementación subyacente de Blockchain.

Para lograr la interoperabilidad de Blockchain entre transacciones, un mercado puede requerir que sus miembros cumplan con las especificaciones estándar de los URI que puedan representar registros de dispositivos en diferentes blockchains. Las transacciones se pueden reenviar a través de diferentes blockchains utilizando tecnologías de retransmisión que están alcanzando rápidamente la madurez y la adopción masiva. El principal beneficio para la red es la capacidad de hacer uso de las ventajas únicas de blockchains específicos, como el procesamiento de alto rendimiento o garantías de anonimato.

# 6 Conclusión

[5] https://blockstack.org/

En la actualidad, la industria de la IoT adolece de costosos problemas de interoperabilidad y seguridad. La red Weeve tiene como objetivo resolver este problema proporcionando a la comunidad un software de código abierto de alta calidad que incluye weeveOS, un sistema operativo IoT a Blockchain seguro por diseño, y la plataforma de curación de mercado de Weeve. El token WEEV permite un mercado basado en estas primitivas, abierto a cualquier participante en el mundo, y lo suficientemente flexible para satisfacer las exigencias de las empresas tradicionales de cadena de mando y los defensores de un futuro descentralizado para los dispositivos IoT.

Con su protocolo, la red weeve aborda problemas de interoperabilidad y confianza complejos utilizando estándares de membresía, pautas de validación y tipos de transacciones. La infraestructura subyacente de Blockchain cierra la brecha entre las partes que no son de confianza, y la ficha WEEV puede incentivar la actividad de negociación segura entre dispositivos en la que los participantes se sientan seguros. La red Weeve permitirá un futuro descentralizado en el que los nuevos mercados para las transacciones entre dispositivos irrumpirán en un orden emergente a voluntad de su comunidad.

*Referencias*

[1] Informe de caso de uso
[2] Steven P. Lalley y 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) Edición Especial: 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 Mayo de 2004, Berkeley, CA, EUA, IEEE Computer Society (2004).