White Paper de XYO Network: La red de ubicación criptográfica basada en el protocolo Proof of Origin

por Arie Trouw*, Markus Levin†, Scott Scheper‡

Janvier 2018

Reseña

Con la presencia creciente de tecnologías conectadas que se basan en la ubicación, nuestra privacidad y seguridad dependen en gran medida de la precisión y validez de la información sobre ubicación. Se han realizado distintos intentos de eliminar la necesidad de entidades centralizadas que controlan el flujo de los datos de ubicación, pero cada uno de ellos ha dependido de la integridad de los dispositivos que recopilan los datos en el mundo físico. Nuestra propuesta es una red de localización criptográfica independiente de la confianza mediante una novedosa formulación que depende de una cadena de pruebas de conocimiento cero para establecer un alto nivel de certeza de los datos de la información de ubicación. La red XYO Network (XY Oracle Network) es una abstracción que permite la comprobación de ubicación por capas en muchas clases de dispositivos y protocolos. Su núcleo es un conjunto de mecanismos criptográficos novedosos, denominados Proof of Origin y Bound Witness que combinan la potencia de la tecnología blockchain y la recopilación de datos del mundo real en un sistema con aplicaciones directas en la actualidad.

---

1 Introducción

Con el advenimiento de contratos inteligentes independientes de la confianza basados en blockchain, la necesidad de servicios de oráculo que arbitren el resultado de un contrato ha aumentado de manera significativa. Las implementaciones más actualizadas de contratos inteligentes dependen de un conjunto agregado o un único oráculo acreditado para resolver el resultado de un contrato. Esto es suficiente en los casos en que ambas partes acuerdan la autoridad e incorruptibilidad de un oráculo específico. Sin embargo, en muchos casos, no existe un oráculo apropiado o no puede considerarse como autoridad debido a la posibilidad de error o corrupción.

Los oráculos de ubicación se encuentran en esta categoría. La decisión de la ubicación de un objeto del mundo real depende de los componentes de generación, transmisión, almacenamiento y procesamiento de informes de un oráculo determinado; en todos ellos pueden producirse errores o pueden dañarse. Entre los riesgos se incluyen la manipulación, contaminación y pérdida de datos y la conspiración.

Por todo esto, nos encontramos frente al siguiente problema: la falta de un oráculo de localización descentralizado e independiente de la confianza influye negativamente en la certeza y precisión de la ubicación. Se han utilizado extensamente plataformas como Ethereum y EOS por su capacidad de mediar de manera segura en las interacciones en línea, cuyos casos de uso principales implican fideicomisos para recaudar fondos, en la forma de ICO. Sin embargo, hasta el momento, todas las plataformas se han centrado completamente en el mundo en línea y no en el físico, debido a la integridad de datos ruidosa y corruptible de los canales actuales de información.

La red XYO Network ha estado trabajando en el concepto de que los desarrolladores, como los que redactan contratos inteligentes para las plataformas de blockchain, puedan interactuar con el mundo físico como si

fuera una API. La red XYO Network es el primer protocolo de oráculo del mundo que permite a dos entidades realizar transacciones en el mundo real prescindiendo de un tercero centralizado. Nuestras abstracciones permiten a los desarrolladores verificar la ubicación, independientemente de la confianza, al crear un protocolo con casos de uso novedosos que no han sido posibles hasta hoy.

La red XYO Network se construirá sobre una estructura existente de más de 1 000 000 de dispositivos que circulan en el mundo distribuidos mediante su actividad de localización de objetos orientada a los clientes. Los dispositivos XY compatibles con Bluetooth y GPS hacen posible que los consumidores coloquen rastreadores físicos en los objetos a los que quieren seguir el rastro (como llaves, equipaje, bicicletas e incluso mascotas). Si extravían o pierden dicho objeto, pueden ver exactamente dónde está mediante una aplicación para teléfonos inteligentes. En solo seis años, la red XYO Network ha creado una de las mayores redes Bluetooth y GPS de consumidores del mundo.

---

2 Antecedentes históricos y enfoques anteriores

2.1 Prueba de ubicación

El concepto de ubicación comprobable ha estado manejándose desde 1960 e incluso puede remontarse hasta 1940 con los sistemas de navegación por radio basados en tierra, como LORAN [1]. En la actualidad, existen servicios de ubicación que apilan múltiples medios de comprobación uno sobre otro para crear una prueba de ubicación mediante la triangulación y los servicios GPS. No obstante, estos enfoques aún tienen que abordar el componente más crucial al que se enfrentan en la actualidad las tecnologías de ubicación: diseñar un sistema que detecte las señales fraudulentas y elimine los incentivos de falsificación de los datos de ubicación. Por este motivo, proponemos que la plataforma de criptolocalización más importante de la actualidad será la que se centre en comprobar el origen de las señales de ubicación física.

Sorprendentemente, el concepto de aplicar la comprobación de ubicación a las tecnologías blockchain surgió en septiembre de 2016, en DevCon 2 de Ethereum. Fue presentado por Lefteris Karapetsas, un desarrollador de Ethereum de Berlín. El proyecto de Karapetsas, Sikorka, permitía que los contratos inteligentes se implementaran en el momento mediante lo que denominó “Prueba de presencia”. Su aplicación para salvar la brecha entre la ubicación y el mundo del blockchain se centraba principalmente en casos de uso de realidad aumentada e introdujo conceptos novedosos como preguntas de comprobación para verificar la ubicación [2]

El 17 de septiembre de 2016, la comunidad de Ethereum acuño formalmente el término “Prueba de ubicación” [3]. Después, fue explicado en más detalle por el desarrollador de Ethereum Foundation, Matt Di Ferrante:

> “Honestamente, una prueba de ubicación confiable es una de las cosas más difíciles de implementar. Incluso si existen muchos participantes que puedan atestiguar la ubicación de cada uno de ellos, no existe garantía de que no se desdigan en el futuro y esto es una gran debilidad debido a que siempre se depende del informe de la mayoría. Se requeriría algún tipo de dispositivo de hardware especializado con tecnología antimanipulación, de manera que la clave privada se destruya cuando uno intente abrirlo o cambiar el firmware; solo entonces se podría tener mayor seguridad, pero, al mismo tiempo, no es imposible falsificar las señales de GPS. La correcta implementación de este concepto requiere tantas opciones alternativas y tantas fuentes de datos para garantizar su precisión que debería ser un proyecto adecuadamente financiado.” [3]
>
> — Matt Di Ferrante, Desarrollador, Ethereum Foundation

2.2 Prueba de ubicación: Limitaciones

Para resumir, la prueba de ubicación puede comprenderse como el aprovechamiento de las propiedades potentes del blockchain, como los sellos de tiempo y la descentralización, y su combinación con dispositivos conscientes de la ubicación fuera de la cadena que sean, con suerte, resistentes a la falsificación. Nos referimos al ámbito de la tecnología criptográfica de localización con el término “criptolocalización.” Además, en la misma medida en que la debilidad de los contratos inteligentes subyace en el hecho de que el oráculo utiliza una única fuente de la realidad (y, por lo tanto, una única fuente de fallos), los sistemas de criptolocalización enfrentan al mismo problema. La vulnerabilidad de las tecnologías actuales de criptolocalización gira alrededor de los dispositivos fuera de la cadena que informan la ubicación de los objetos. En los contratos inteligentes, la fuente de información externa a la cadena es un oráculo. En la red XYO Network, la fuente de información externa a la cadena se mueve en el mundo real como un tipo especializado de oráculo que denominamos Sentinel. La innovación principal de la red XYO Network es la prueba sin identidad basada en la ubicación que es la base de los componentes de nuestro sistema para crear un protocolo de criptolocalización independiente de la confianza.

---

3 La red XY Oracle Network

> “Durante años, se ha reconocido la necesidad de un sistema que sea difícil de alterar para complementar al GPS. El GPS es sumamente preciso y confiable; a pesar de esto, la frecuencia y gravedad de las interferencias, falsificaciones, ataques cibernéticos y otras formas de interferencia parecen crecer. Esto podría tener efectos devastadores en nuestras vidas y nuestra actividad económica.” [4]
>
> — Dana Goward, Presidente, RNT Foundation

3.1 Introducción

El objetivo de la red XYO Network es crear un sistema de oráculo de localización descentralizado e independiente de la confianza, que sea resistente a los ataques y que ofrezca el mayor nivel de certeza posible cuando se le consulte la información disponible. Logramos esto mediante un conjunto de abstracciones que reducen en gran medida el riesgo de las falsificaciones de ubicación mediante una cadena de pruebas de conocimiento cero en todos los componentes del sistema.

3.2 Descripción general de la red

Nuestro sistema provee el punto de entrada a un protocolo de dispositivos conectados que brinda un gran nivel de certeza de los datos de ubicación mediante una cadena de pruebas criptográficas. Los usuarios podrán enviar transacciones, denominadas “consultas”, para recuperar datos de ubicación en cualquier plataforma de blockchain que incluya la función de contratos inteligentes.[1] A continuación, los agregadores de la red XYO Network escucharán estas consultas enviadas al contrato y buscarán las respuestas que tengan un alto nivel de precisión del conjunto descentralizado de dispositivos que transmiten pruebas criptográficas a estos agregadores. Después de acordar la respuesta con la mejor puntuación, los agregadores enviarán dichas respuestas a los contratos inteligentes. Esta red

[1] Ethereum, Bitcoin + RSK, Stellar, Cardano, IOTA, EOS, NEO, Dragonchain, Lisk, RChain, Counterparty, Monax y otras.

de componentes permite determinar si un objeto se encuentra en la coordenada XY específica en un momento determinado, con la mayor certeza posible comprobable e independiente de la confianza.

La red XYO Network tiene cuatro componentes principales: Sentinels (que recopilan los datos), Bridges (que transmiten los datos), Archivists (que almacenan los datos) y Diviners (los agregadores de respuestas). Los Sentinels recopilan información de ubicación mediante sensores, radios y otros medios. Los Bridges reciben los datos de los Sentinels y los transmiten a los Archivists. Los Archivists almacenan esta información para que los Diviners la analicen. Los Diviners analizan la heurística de la ubicación de los Archivists para generar respuestas a consultas y asignarles puntuaciones de precisión. A continuación, los Diviners transmiten estas respuestas al contrato inteligente (de esta manera, los Diviners cumplen la función de oráculos). La puntuación de precisión, denominada Origin Chain Score, se determina mediante un conjunto de pruebas de conocimiento cero denominado Proof of Origin Chain. La cadena garantiza que dos o más datos se originan en la misma fuente sin revelar ninguna información subyacente. Cada componente de la ruta de la consulta genera sus propios datos, que luego se encadenan a cada componente al que transmite dichos datos. Proof of Origin es una formulación novedosa que construye una cadena de garantías criptográficas en la ruta de los transmisores de la red para brindar un gran nivel de confianza a los datos del mundo real. Esta Proof of Origin Chain encapsula la confianza que merece un dato de ubicación hasta el primer dispositivo que recopiló lo datos. En la siguiente sección analizaremos en profundidad cómo funciona la Proof of Origin.

Para establecer un mecanismo de conceso descentralizado entre los Diviners, la red XYO Network dependerá de una blockchain pública e inmutable denominada XYOMainChain que almacena transacciones de consultas junto con la información recopilada por los Diviners y la puntuación de origen asignada. Antes de analizar en profundidad los detalles del funcionamiento de todo el sistema, definiremos claramente las responsabilidades de cada uno de los componentes de nuestra red.

3.2.1 Sentinels

Los Sentinels son los testigos de la ubicación. Observan la heurística de los datos y producen libros mayores temporales para dar fe de la certeza y precisión de la heurística. El aspecto más importante de los Sentinels es que los libros mayores que producen dan certeza al resto de los componentes de que provienen de la misma fuente. Esto se realiza al añadir la Proof of Origin a la cadena de transmisión de las pruebas criptográficas. Debido a que la red XYO Network es un sistema independiente de la confianza, se debe incentivar a los Sentinels para que proporcionen información de ubicación honesta. Esto se lleva a cabo al combinar dos componentes: reputación y pago. Se recompensa al Sentinel con tokens de XYO Network (XYO) cuando su información se utiliza para responder una consulta. Para aumentar la probabilidad de que se los recompense, deben crear libros mayores coherentes con los de sus pares y proporcionar Proof of Origin para identificarse como el origen de la información de ubicación.

3.2.2 Bridges

Los Bridges son los transcriptores de los datos de ubicación. Transmiten de manera segura los libros mayores de ubicación de los Sentinels a los Archivists. El aspecto más importante de un Bridge es que un Archivist puede estar seguro de que los libros mayores heurísticos que se reciben de un Bridge no han sido alterados. El siguiente aspecto más importante de un Bridge es que añaden una Proof of Origin adicional. Como la red XYO Network es un sistema independiente de la confianza, se debe incentivar a los Bridges para que transmitan heurísticas de manera honesta. Esto se lleva a cabo al combinar dos componentes: reputación y pago. Se recompensa al Bridge con tokens de XYO Network (XYO) cuando la información que han transmitido se utiliza para responder una consulta. Para aumentar las probabilidades de que se los recompense, deben crear libros mayores coherentes con los de sus pares y proporcionar Proof of Origin para identificarse como los transmisores de las heurísticas.

3.2.3 Archivists

Los Archivists almacenan la información de ubicación de los Bridges de manera descentralizada con el objetivo de guardar todos los libros mayores históricos. Incluso si parte de la información se pierde o no está disponible temporariamente, el sistema sigue funcionando solo que con menor precisión. Los Archivists también indexan los

libros mayores para poder devolver fácilmente una cadena de datos de libro mayor si fuera necesario. Los Archivists solo almacenan datos sin procesar y se los recompensa con tokens de la red XYO Network únicamente por la recuperación de los datos y su subsiguiente uso. El almacenamiento siempre es gratuito.

Los Archivists están conectados en red; por ello, cuando se consulta a un Archivist, este se comunicará con otros Archivists para obtener información que no tiene. De manera opcional, un Archivist puede almacenar cualquier información de libro mayor que se le devuelva. El resultado serán dos tipos de Archivist: uno que está en el lado de producción de los datos de la "nube" y otro que está en el lado de consumo de los datos en la "nube". Los Archivists entre ellos serán híbridos. La opción de almacenamiento de datos no es obligatoria, pero puede implementarse fácilmente mediante IPFS u otra solución descentralizada de almacenamiento. Cada vez que los datos pasan de un Archivist a otro, se adjunta una Proof of Origin adicional para poder rastrear el pago, ya que se recompensa a todos los Archivists. En el caso de una recuperación, es posible establecer un nivel mínimo de Proof of Origin para aumentar la validez. Se deben alinear los intereses de los Sentinels, Bridges y Archivists para evitar que inflen los datos.

3.2.4 Diviners

Los Diviners constituyen la parte más compleja de la red XYO Network. El objetivo general de un Diviner es buscar la información más precisa para una consulta en la red XYO Network y transmitir dichos datos a quien envió la consulta. Los Diviners sondean la plataforma de blockchain correspondiente (es decir, Ethereum, Stellar, Cardano, IOTA, etc.) para responder las consultas emitidas por el contrato inteligente XYO. A continuación, interactúan directamente con la red de Archivists para encontrar la respuesta a la consulta y enviar aquella que tenga la mayor puntuación de precisión/confianza. Para asignar esta puntuación, evalúan al testigo con la mejor Proof of Origin Chain. Los Diviners que obtengan la respuesta con la mejor puntuación en el menor tiempo podrán crear un bloque en la blockchain XYO principal (XYOMainChain) mediante una Proof of Work. Las consultas se ordenan por prioridad en función del tamaño y la complejidad de la recompensa, es decir, cuantos más XYO se ofrezcan por la respuesta, mayor será la prioridad de la consulta.

Otros Diviners llegan a un consenso sobre la validez de un bloque y le adjuntan una firma digital. A continuación, el Divinier que haya sido la dirección coinbase de dicho bloque enviará una transacción al contrato inteligente con la respuesta junto con la puntuación de precisión. También envía una lista de firmas de otros Diviners para evitar que un atacante envíe información falsa al blockchain personificando al Diviner. Después, el contrato inteligente podrá comprobar la lista de firmas de la carga de trabajo para verificar la integridad de esta información.

3.3 Funcionalidad extremo a extremo

Una vez detalladas las responsabilidades de cada componente, presentamos un ejemplo integral de cómo funciona el sistema:

1. **Los Sentinels recopilan datos**
    - Los Sentinels recopilan la heurística de la ubicación en el mundo físico y preparan sus propias Proof of Origin que se encadenarán a los nodos superiores.
2. **Los Bridges recopilan datos de los Sentinels**
    - Los Bridges recopilan la información necesaria de los Sentinels en línea y adjuntan la Proof of Origin a su cadena. A continuación, los Bridges se ponen a disposición de los Archivists de la red.
3. **Los Archivists indexan/reúnen datos de los Bridges**
    - Los Bridges envían constantemente información a los Archivists que se conserva en repositorios descentralizados con un índice heurístico de ubicación.
4. **El Diviner investiga la consulta del usuario**
    - Los Diviners sondean las consultas enviadas al contrato inteligente de Ethereum y deciden comenzar el proceso de formulación de la respuesta.
5. **El Diviner recopila los datos de los Archivists**
    - A continuación, los Diviners deciden aceptar una consulta al buscar la información adecuada necesaria en la red de Archivists.
6. **El Diviner formula una respuesta**

- Los Diviners escogen, en la red de Archivists, la Best Answer a la consulta que tenga la mejor Origin Chain Score.

7. **El Diviner propone un bloque**
   - Después, los Diviners proponen bloques a la XYOMainChain que incluyen el contenido de la respuesta, la consulta y los tokens XYO (XYO) pagados mediante la Proof of Work. Otros Diviners de la red firman digitalmente el contenido del bloque y, una vez que se alcanza un consenso sobre la validez del bloque, el nonce de la cuenta de coinbase del Diviner se actualiza para plasmar su Proof of Work en el sistema.
8. **El Diviner devuelve el resultado al iniciador de la consulta**
   - Los Diviners empaquetan la respuesta, su Origin Chain Score y su conjunto de firmas digitales y la envían a un componente de adaptación que conecta de manera segura el contrato inteligente XYO. El adaptador tiene la responsabilidad de asegurarse de que no se haya comprometido la integridad del Diviner y envía el conjunto de respuestas con firma digital al contrato inteligente. Esto ocurre justo después del proceso de creación del bloque. A continuación, el coinbase del Diviner recibe el pago por el trabajo.
9. **Los componentes de la red XYO Network reciben una recompensa por su trabajo**
   - Los componentes de la Proof of Origin Chain reciben una recompensa por su trabajo de buscar la respuesta a la consulta. Tanto los Sentinels como los Bridges, Archivists y Diviners reciben una recompensa por su trabajo.

En el caso de que se formule una misma consulta más de una vez, es posible que se suministre más de una respuesta ya que la respuesta que se suministró en un momento determinado se basaba en la heurística disponible que el sistema podía ofrecer en dicho momento. El envío de una respuesta al blockchain tiene dos etapas. Primero, se debe realizar un análisis para determinar la Best Answer a la consulta. Si el sistema genera múltiples respuestas, los nodos las compararán y siempre escogerán la mejor. Este sería un ejemplo de una consulta simple: "¿Dónde se encontraba un nodo en la red en un momento específico?"

3.4 Blockchain como única fuente de la verdad

Básicamente, los Diviners simplemente transforman datos relativos en absolutos. Son capaces de explorar toda la red de Archivists para concretar una respuesta absoluta a la consulta de la red XYO Network. Los Diviners también son los nodos que proponen y añaden bloques a la XYOMainChain y obtienen una recompensa por su Proof-of-Work. Debido a que la red de Archivists es un repositorio de datos sin procesar y la blockchain es un repositorio de datos absolutos y procesados, la red puede, eventualmente, utilizar la información más reciente de la XYOMainChain para responder consultas futuras en lugar de depender de los cálculos computacionales costosos que realiza la red de Archivists.

Como los bloques de la XYOMainChain almacenan la Proof of Origin Chain y el gráfico de los componentes que se utilizaron para responder las consultas, los futuros Diviners pueden explorar estos datos absolutos para obtener resultados precisos con menor uso del ancho de banda. Como tal, la XYOMainChain se convertirá gradualmente en la fuente más importante de verdades del sistema. No obstante, aún se necesitará la red de Archivists para mantener la información más actualizada acerca de la heurística de ubicación recopilada por los Sentinels.

3.5 Marco de la red XYO Network para seleccionar la Best Answer

Definimos el término Best Answer como la respuesta única, entre una lista de respuestas posibles, que posee la mayor puntuación de validez y una puntuación de precisión más alta que la precisión mínima requerida. La puntuación de validez se basa en la Origin Chain Score. El sistema sabe cuál es la puntuación de origen más alta, que sería el 100 por ciento hasta que se alcance una puntuación mayor que, entonces, se convertiría en el nuevo 100 por ciento. La red XYO Network permite seleccionar el Best Answer Algorithm para determinar la Best Answer. Esto crea la posibilidad de investigaciones futuras de algoritmos alternativos.

Cuando se excluya información de una respuesta por ser incorrecta o errónea, se informará a los Archivists para que purguen los datos de sus repositorios descentralizados.

3.6 Integración inicial con blockchains públicas

La red XYO Network ha sido diseñada para ser una abstracción que pueda interactuar con cualquier blockchain pública que admita contratos inteligentes, como Ethereum, Bitcoin + RSK, EOS, NEO, Stellar, Cardano y otras. Para interactuar con XYO Network, los usuarios de Ethereum, por ejemplo, pueden enviar consultas a nuestro contrato inteligente XYO y pagar en tokens XYO (ERC20). Los nodos de nuestra propia blockchain XYO, denominados Diviners, sondearían constantemente Ethereum en búsqueda de estas consultas y recibirían su recompensa en la moneda nativa de nuestra propia blockchain XYO (también denominados tokens XYO). En el futuro, realizaremos conversiones uno a uno con los tenedores de nuestro token ERC20 en nuestra propia moneda nativa de blockchain para proveer a nuestras plataformas con tarifas de transacción compatibles con los micropagos necesarios para los casos de uso de IoT ampliables. En tales casos, permitiremos a los usuarios enviar consultas directamente a nuestra blockchain en lugar de interactuar mediante un contrato inteligente público.

---

4 Proof of Origin

Con una red física compuesta por nodos no confiables es posible determinar la certeza de los datos proporcionados por los nodos periféricos en base a la prueba de conocimiento cero de que dos o más datos tuvieron su origen en la misma fuente. Mediante estos conjuntos de datos, combinados con un número de conjuntos de datos similares y el conocimiento de la ubicación absoluta de por lo menos un nodo, es posible confirmar la ubicación absoluta del otro nodo.

4.1 Introducción a Proof of Origin

Los sistemas tradicionales independientes de la confianza se basan en una clave privada para firmar transacciones o contratos en un sistema. Esto funciona muy bien si su asume que el nodo de la red que firma los datos es física y virtualmente seguro. Sin embargo, si se compromete la clave privada, la capacidad de comprobar el origen se debilita.

Al aplicar los conceptos de independencia de la confianza a la Internet de las cosas, se debe asumir que los nodos periféricos de la red no son física ni virtualmente seguros. Esto trae aparejada la necesidad de identificar a los nodos periféricos sin utilizar ID exclusivas y evaluar, en cambio, si los datos que producen son honestos y válidos sin ningún conocimiento externo a la red.

4.2 El concepto central de Proof of Origin: Bound Witnesses

La Proof of Origin depende del concepto de Bound Witness. Debido a que para resolver un contrato digital no es útil una fuente de datos no confiable (un oráculo), es posible aumentar sustancialmente la certeza de los datos suministrados al establecer, primero, la existencia de una prueba de ubicación bidireccional. La principal heurística de ubicación bidireccional es la proximidad, ya que ambas partes pueden validar la instancia y el rango de la interacción al confirmarla. Esto brinda una prueba de conocimiento cero de que los dos nodos estaban en proximidad uno del otro.

A continuación, debemos determinar la certeza de que un nodo testigo del oráculo en un sistema independiente de la confianza ha recopilado los datos que comparte. En un sistema independiente de la confianza,

un nodo testigo puede producir datos falsos, ya sea por defecto o manipulación. Es posible detectar datos no válido y eliminarlos simplemente si no están dentro del rango permitido de dicha heurística. Los datos válidos pero incorrectos (es decir, datos falsos) son mucho más difíciles de detectar.

4.3 Heurística de ubicación unidireccional vs. bidireccional

La mayoría de los datos relacionados con el mundo físico (heurística) son unidireccionales. Es decir, el elemento que se mide no puede devolver la medición; esto hace que los datos heurísticos unidireccionales sean muy difíciles de validar. Una heurística bidireccional es aquella donde el elemento medido puede informar su propia medición a la otra parte; esto permite su validación. La ubicación es una heurística poco frecuente en el sentido de que puede ser bidireccional, con dos nodos periféricos informándose entre sí. Un ejemplo del mundo real serían dos personas que están una cerca de la otra y toman una selfie, imprimen una copia para cada una y ambas las firman. Este proceso otorgaría a ambas partes una prueba de proximidad. La única manera de que estas dos personas obtuvieran este "dato" es que estuvieran juntas en el mismo sitio.

Ahora, veamos los efectos en la red: imaginen un sistema donde se espera que cada uno de los nodos periféricos produzcan estas "selfies" mientras circulan y las guarden en una carpeta. También se espera que mantengan dicha carpeta en orden cronológico y que nunca puedan borrar ninguna. Esto establece un registro de proximidad de cada nodo periférico que puede comprobarse de manera cruzada con los registros de otros nodos periféricos.

4.4 Nodos centrales

Se considera a todos los nodos "testigos", incluso los Bridges y los nodos de transmisión, almacenamiento y análisis. Esto permite que los datos que se transmitan de un nodo al siguiente estén unidos. Este es el concepto de Bound Witness.

4.5 Referencia cruzada

Analizar todos los conjuntos de "selfies" que todos los nodos periféricos producen y encadenan permite al sistema producir la Best Answer a partir de la proximidad relativa de todos los nodos que componen la red. Si todos los nodos informan de manera honesta y precisa, al mapear todas las posiciones relativas de los nodos periféricos se logrará la máxima certeza y precisión posible: 100 por ciento. Contrariamente, si todos los nodos son deshonestos o fallan, la certeza y precisión pueden acercarse al mínimo de 0 por ciento.

Dado un conjunto de datos informados y una consulta sobre la posición relativa de uno de los nodos periféricos, es posible generar una aproximación de la posición junto con coeficientes de certeza y precisión.

Dado el mismo conjunto de datos y el mismo algoritmo de análisis, todos los cálculos deberían dar la misma aproximación de posición y los mismos coeficientes de certeza y precisión.

4.6 Diagrama

S’ y S” (Figura 1) son Sentinels (nodo periférico) que recopilan heurística. Al comunicarse entre sí, intercambian datos de heurística y claves públicas. Ambos construyen un registro completo de la interacción y firman la interacción resultante. A continuación, dicho registro firmado se convierte en la siguiente entrada en sus libros mayores (16 para S´ y 3 para S´´). Esta acción une a estos dos testigos como estando uno en proximidad del otro.

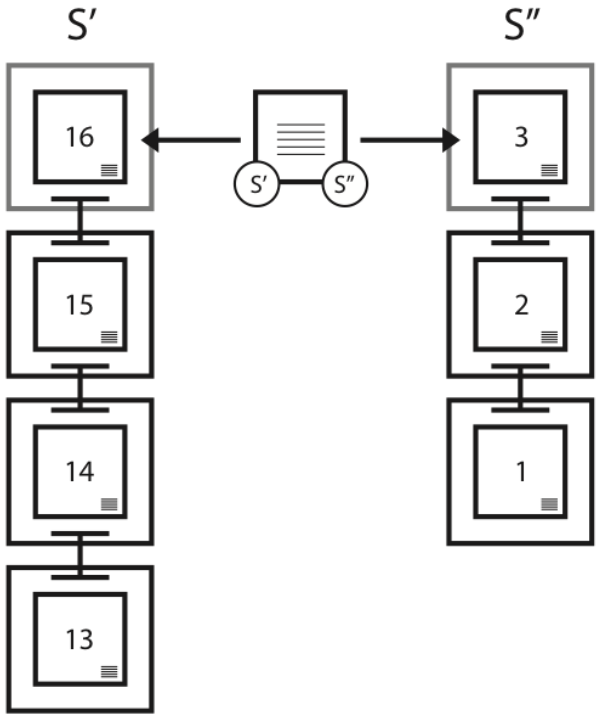

Figura 1 Ejemplo de unión de testigos entre dos Sentinels

4.7 Cadenas de origen

Cada uno de los orígenes conserva su propio libro mayor y lo firma para crear una Proof of Origin Chain. Una vez compartida la información acerca de la Proof of Origin Chain, esta será efectivamente permanente. Esto se debe a que la bifurcación que ocurre después de compartir los datos finaliza la cadena y todos los datos futuros del testigo se considerarán como creados por un nuevo testigo. Para generar un eslabón en la Proof of Origin Chain, el origen genera un par de claves pública/privada. A continuación, firma los bloques anterior y siguiente con el mismo par después de incluir la clave pública en ambos bloques. Inmediatamente después de la firma, la clave privada se elimina. Al eliminarla inmediatamente, el riesgo de robo o reutilización de la clave privada se reduce en gran medida.

Las Proof of Origin Chains son la clave para comprobar que los libros mayores que ingresan a la red XYO Network sean válidos. Las ID exclusivas para la fuente de los datos no son prácticas ya que pueden falsificarse. La firma con claves privadas no es práctica debido a que la mayoría de los componentes de la red XYO Network son difíciles, sino imposibles, de proteger físicamente, por esto la posibilidad de que un impostor robe una clave privada es demasiado grande. Para resolver esto, la red XYO Network utiliza Transient Key Chains. El beneficio es que es imposible falsificar una cadena de origen de los datos. No obstante, una vez que se ha roto la cadena, está rota para siempre y no puede continuarse, lo que la convierte en una isla.

Cada vez que se transmite un libro mayor heurístico en la red XYO Network, el receptor adjunta su propia Proof of Origin, esto alarga la Proof of Origin Chain y genera una intersección de Proof of Origin. Las Proof of Origin Chains y la Proof of Origin Intersections son los principales indicadores que utilizan los Diviners para comprobar la

validez de los libros mayores. La ecuación de reputación de un libro mayor es, en efecto, qué porcentaje de la red XYO Network participó en crear la serie de Proof of Origin asociada. En teoría, si el 100 por ciento de los registros de la red XYO Network está enlazado con la Proof of Origin y analizado en su totalidad, la probabilidad de que sean válidos es del 100 por ciento. Si el 0 por ciento de los registros de la red XYO Network está disponible para análisis, la validez cae al 0 por ciento.

Para mayor seguridad, la clave pública de un eslabón de la cadena no se suministra hasta que no esté disponible la segunda entrada. Esto también permite que transcurra un lapso entre entradas o que se almacenen más datos en el eslabón anterior o el siguiente.

4.8 Origin Chain Score

El Origin Chain Score se calcula de la siguiente manera (algoritmo predeterminado):

- PcL = Longitud de Proof of Origin Chain
- PcD = Dificultad de Proof of Origin Chain
- Pc' Pc" O = Superposición de Proof of Origin Chain para Pc' y Pc"

$$Score = \prod_{i=0}^{i=n} \frac{PcL * PcD}{Pc' Pc'' O}$$

4.9 Origin Tree

El Origin Tree se utiliza para calcular la validez aproximada de una respuesta. Utiliza los datos recopilados para generar un árbol ideal, que es el árbol que mejor se adapta a dichos datos para una respuesta confirmada determinada. Si el nodo N está ubicado en X, Y, Z, T, el error entre todos los datos del conjunto debe tener un determinado valor. Para calcular este error, deberíamos calcular la distancia MÍN, MÁX, MEDIA, MEDIANA y PROMEDIO DESDE LA MEDIA.

Dado un conjunto S de todas las puntuaciones s, un PcD de dificultad de Proof of Origin Chain y un error de factor de error, la Best Answer se determina de la siguiente manera:

$$BestAnswerScore = \max_{\forall s \in S_j} [PcD * (1 - error)]$$

Es decir, la respuesta confirmada que tiene la mayor Best Answer Score es la mejor respuesta. Mediante el Proof of Origin Tree, es posible identificar y podar ramificaciones imposibles (valores atípicos).

4.10 Encadenado transitorio de claves

Es posible encadenar una serie de paquetes de datos al utilizar claves privadas temporarias para firmar paquetes sucesivos. Cuando se incluye en los paquetes de datos la clave pública junto con la clave privada, el receptor puede comprobar que ambos paquetes fueron firmados por la misma clave privada. No es posible alterar los datos incluidos en el paquete sin romper la firma; esto garantiza que los paquetes firmados no fueron alterados por un tercero, como un Bridge o un nodo de almacenamiento.

4.11 Profundidad de los eslabones

Como mínimo, un nodo genera un nuevo par de claves pública/privada para cada eslabón de la Proof of Origin Chain con una profundidad de eslabón de 1. Pueden existir N entradas en la tabla de eslabones para una entrada de libro mayor determinada, cada una de ellas especifica la distancia hacia el futuro cuando se añadirá la parte dos del eslabón. Ningún par de eslabones puede tener el mismo orden de magnitud en una escala de base 2. Por ejemplo, se permitirá la entrada [1, 3, 7, 12, 39] pero no [1, 3, 7, 12, 15].

El eslabón de profundidad 1 se crea, utiliza y elimina cuando se publica el eslabón anterior. No obstante, en el caso de los eslabones cuya profundidad sea mayor de 1, su par se genera cuando se firma el bloque anterior y la segunda firma no se produce hasta N bloques más tarde, después de lo cual se elimina la clave privada. Por este motivo, siempre se considera a los eslabones con profundidad mayor de 1 menos seguros que los de profundidad 1, pero pueden utilizarse para mejorar el rendimiento y reducir la pérdida de datos en detrimento de dicha seguridad.

4.12 Orden fijo

El elemento clave para determinar la secuencia de los libros mayores es el orden en que se informan. Debido a que no es posible que un dispositivo cambie el orden de ningún libro mayor de la Proof of Origin firmado, es posible establecer un orden absoluto al analizar todos los libros conjuntamente.

4.13 Penúltima publicación

El método principal para establecer la Proof of Origin se basa en el hecho de que un Sentinel siempre informa su penúltimo bloque sin informar el último. Esto permite que el último bloque tenga el eslabón a su antecesor firmado como prueba del enlace.

4.14 Eslabones vacíos

Para que la Proof of Origin Chain sea más segura, se requiere que la cadena se actualice no más de una vez cada diez segundos y no menos de una vez cada sesenta minutos. Cuando no existen nuevos datos disponibles, se añadirá un eslabón vacío a la cadena.

4.15 Diagrama

A medida que el tiempo transcurre de izquierda a derecha (Figura 2), la Proof of Origin Chain que se está construyendo se alarga. En cualquier momento dado, el productor de la cadena solo suministrará a quien llama las entradas con bordes oscuros y esperará a la segunda firma de la entrada para ponerla a disposición. Por ejemplo, en la 3a columna, solo las entradas 2 y 1 se devolverán como parte de la cadena.

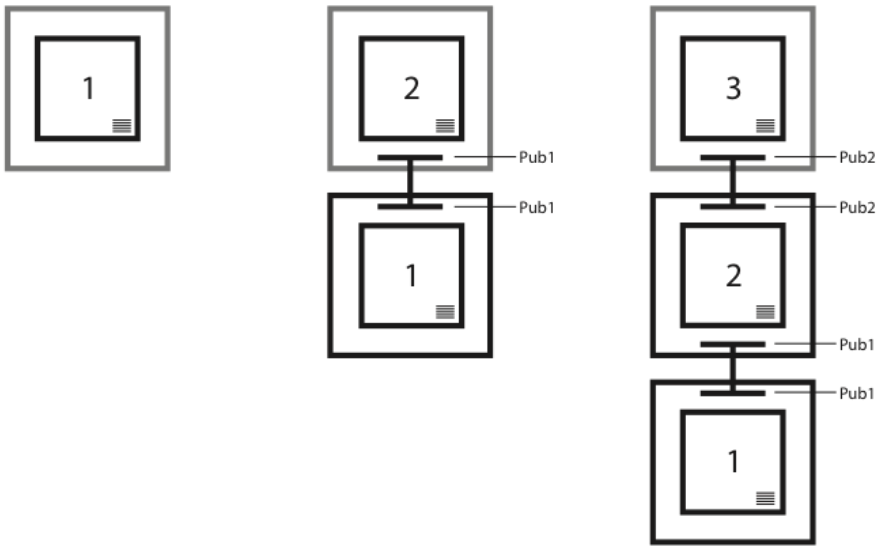

Figura 2 Ejemplo de inclusión de eslabones en una Proof of Origin Chain

4.16 Resumen

Dada una serie de paquetes de datos firmados en pares secuenciales con claves privadas temporarias que incluyen claves públicas emparejadas, es posible determinar con certeza absoluta que los paquetes provinieron del mismo origen.

---

5 Consideraciones de seguridad

5.1 Ataque de Diviner falso

Se envía al contrato inteligente XYO un conjunto de firmas digitales porque el contrato debe comprobar la integridad del Diviner que envió la respuesta. A continuación, el contrato puede comprobar el resto de los Diviners que firmaron

la lista dentro de un intervalo con gran nivel de confianza. Sin esto, el oráculo transmisor sería la única fuente de fallas y riesgos del sistema.

5.2 Ataque DDoS a los Sentinels

Otro ataque que debe considerarse es la denegación de servicio distribuido (DDoS) entre nodos Sentinel de una determinada región. Un atacante podría intentar establecer una gran cantidad de conexiones con los Sentinels para impedirles que transmitan la información correcta o que transmitan información al Bridge. Es posible eludir este problema al requerir a cualquiera que intente conectarse a un Sentinel que resuelva un pequeño acertijo criptográfico. Como una consulta no implicará una gran cantidad de conexiones a los Sentinels, esto no sería una gran carga en el sistema de transmisión XYO y un atacante debería gastar una gran cantidad de recursos para ejecutar un DDoS con éxito en nuestra red. En cualquier momento dado, cualquiera puede comprobar una Proof of Origin Chain ya que está almacenada en la XYOMainChain. Esto garantiza que si una única entidad de la cadena fue comprometida, la precisión de la respuesta a la consulta (Origin Chain Score) caerá a 0.

---

6 Economía de tokens de XYO

Los oráculos son una porción importante de las necesidades de potencia e infraestructura de las aplicaciones descentralizadas, la mayor parte se relaciona con la conectividad y la adición de oráculos acreditados. Creemos que para que las aplicaciones descentralizadas alcancen su máximo potencial, se necesita un sistema de oráculos descentralizado e independiente de la confianza.

6.1 Criptoeconomía de la red XYO Network

Utilizamos tokens XYO para incentivar el comportamiento deseado de proporcionar heurística de ubicación precisa y confiable. Los tokens XYO pueden considerarse como el "combustible" necesario en la interconexión con el mundo real para comprobar la coordenada XY del objeto especificado.

El proceso sería el siguiente: primero, el titular de un token envía a la red XYO Network una consulta (por ejemplo, “¿Dónde se encuentra mi paquete ordenado a eCommerce con dirección XYO 0x123456789…?”). A continuación, la consulta se envía a la cola donde espera para ser procesada y respondida. En el momento de crear la consulta, el usuario puede establecer el nivel de confianza y el precio del combustible XYO que desea. Además de la dinámica del mercado, el costo de la consulta (en tokens XYO) se determina según la cantidad de datos necesarios para proporcionar una respuesta a la consulta. Cuantos más datos se necesiten, mayor será el precio de la consulta y mayor el precio del combustible XYO. Las consultas a la red XYO Network tienen el potencial de ser muy grandes y costosas. Por ejemplo, una empresa de transporte y logística podría consultar a la red XYO lo siguiente: “¿Cuál es la ubicación de cada uno de los vehículos de nuestra flota?”

Una vez que el titular de tokens XYO consulta a la red XYO Network y paga el combustible solicitado, todos los Diviners que intervienen en la tarea se comunican con los Archivists correspondientes para recuperar los datos

pertinentes necesarios para responder la consulta. Los datos se obtienen de los Bridges, que originalmente recopilaron los datos de los Sentinels. Los Sentinels son, esencialmente, los dispositivos o señales que comprueban la ubicación de los objetos. Entre ellos se encuentran rastreadores Bluetooth, rastreadores GPS, dispositivos de geolocalización incorporados a dispositivos IoT, tecnologías de seguimiento satelital, escáneres de código QR, escáneres RFID y muchos otros. XY Findables es pionera en el sector de Bluetooth y GPS para consumidores, esto le ha permitido probar o procesar heurística de ubicación en el mundo real. Todos los esfuerzos del desarrollo del sector de consumidores de XY Findables han contribuido en gran medida en el diseño del Protocolo de blockchain de XYO Network. Si la información proporcionada por un dispositivo Sentinel (como una baliza Bluetooth) se utiliza para responder una consulta, los cuatro componentes involucrados en la transacción reciben una parte del combustible XYO que pagó el tenedor del token: el Diviner (que buscó la respuesta), el Archiver (que almacenó los datos), el Bridge (que transmitió los datos) y el Sentinel (que registró la información de la ubicación). La distribución del combustible entre 3 de los 4 componentes de la red XYO Network se otorga siempre en la misma proporción. La excepción son los Diviners, cuyo trabajo en el proceso de proporcionar una respuesta es más amplio. Dentro de cada componente, el combustible se distribuye equitativamente.

6.2 Recompensas por independencia

Los dispositivos que recopilan información son los bloques constitutivos de la red; un mismo dispositivo puede actuar como uno o más de los cuatro componentes del sistema. No obstante, es poco frecuente, especialmente un una red XYO Network grande, que los dispositivos cumplan la función de más de dos de estos componentes. Además, se otorgaría mayor puntuación al libro mayor de la blockchain que tuviera una Proof of Origin más independiente; por este motivo, existe una penalización criptoeconómica para los dispositivos que actúen como componentes múltiples.

6.3 Recompensas por integridad estacionaria

A los Sentinels de la red XYO Network se les asigna un coeficiente de estacionariedad por la magnitud de su movimiento en toda su vida útil. Cuando menos se mueva un Sentinel en un lapso, mayor será la confianza en sus datos. Los Archivists realizan un seguimiento y analizan estos coeficientes de estacionariedad al considerar a cuáles Sentinels enviar las consultas.

6.4 Uso de tokens de incentivo

Un sistema en el cual no se incentiva a los tenedores de tokens a utilizarlos crea un problema a largo plazo en la economía subyacente. Crea un ecosistema con muy escasas reservas de valor y activa el impulso natural de inventar motivos para no utilizar el token en lugar de estimular las utilidades y la liquidez.

El principal problema de la mayoría de los incentivos criptoeconómicos es que se centra demasiado en los mineros de tokens (por ejemplo, Sentinels, Bridges, Archivists, Diviners) y muy poco en los usuarios de tokens. El token XYO tiene ambos aspectos en cuenta.

El modelo de tokens XYO incentiva a los mineros no solo a suministrar datos precisos si no a reconocer, también, cuando no suministrar ningún dato. Se recompensa al usuario final para que realice más transacciones cuando la liquidez de la red es baja en comparación a cuando esta es alta. De esta manera, el ecosistema de los tokens XYO tiene la capacidad de permanecer equilibrado, fluido y saludable.

6.5 Especificaciones de los tokens XYO

La venta pública de tokens posee una estructura de precios escalonada que comienza en 1 ETH: 100 000 XYO con un máximo de 1 ETH: 33 333 XYO. La información relacionada con nuestro volumen y estructura de precios temporal se anunciará en breve.

Plataforma de contratos inteligentes: Ethereum

- Tipo de contrato: ERC20
- Token: XYO
- Nombre del token: token utilitario XYO Network
- Dirección del token: 0x55296f69f40ea6d20e478533c15a6b08b654e758
- Emisión total: finita y limitada a la cantidad que se alcance después de la venta principal de tokens
- Límite proyectado para participaciones digitales (Tokens) de XYO: $48 Millones
- Tokens no vendidos ni asignados: se destruirán después de la venta. No se generarán más tokens XYO después de finalizada la venta principal.

---

7 Casos de uso de la red XYO Network

El uso de la red XYO Network tiene enormes aplicaciones que abarcan múltiples sectores. Por ejemplo, consideremos una empresa de comercio electrónico que podría ofrecer a sus clientes premium servicios de pago contra entrega. Para poder ofrecer este servicio, dicha empresa aprovecharía la red XYO Network (que utiliza tokens XYO) para redactar contratos inteligentes (es decir, en la plataforma Ethereum). A continuación, la red XYO Network podría rastrear la ubicación del paquete que se envía en todas las etapas hasta el consumidor, desde el estante del almacén hasta el correo que realiza el envío, todo el trayecto hasta la casa del consumidor y todos los sitios por lo que pase. Esto permitiría a las empresas y sitios web de comercio electrónico comprobar, independientemente de la confianza, que el paquete no solo ha llegado al domicilio del cliente sino que este lo ha recibido de manera segura. Una vez que el paquete llegue al domicilio del cliente (definido y comprobado mediante una coordenada XY específica), el envío se considerará entregado y se liberará el pago al proveedor. De esta manera, la integración del comercio electrónico con la red XYO Network brinda la capacidad de proteger al comerciante contra fraude y garantiza a los consumidores que solo pagarán por los artículos que lleguen a su domicilio.

Consideremos una integración totalmente distinta de la red XYO Network a un sitio de reseñas de hoteles, cuyo problema actual es la falta de confianza en sus reseñas. Obviamente, los propietarios de hoteles tienen interés en mejorar sus reseñas a cualquier costo. ¿Qué ocurriría si pudiéramos decir con suma certeza que alguien estaba en San Diego, voló a Bali y se alojó en un hotel durante dos semanas, volvió a San Diego y allí escribió una reseña sobre su estancia en el hotel de Bali? La reputación de la reseña sería muy alta, especialmente si fue escrita por alguien que publica reseñas habitualmente y ha escrito muchas de ellas con datos de ubicación comprobados.

---

8 Ampliación de la red XYO Network

Somos afortunados al contar con un sector de consumidores exitoso basado en una red del mundo real con más de un millón (1 000 000) de dispositivos Bluetooth y GPS. La mayoría de las redes de ubicación no alcanzan esta fase ni logran la masa crítica necesaria para construir una red tan extensa. La red de Sentinels que hemos creado es solo el punto de partida. La red XYO Network es un sistema abierto al que cualquier operador de dispositivos de ubicación puede conectarse y comenzar a ganar tokens XYO.

Por lo general, cuanto mayor sea la cardinalidad de un Sentinel de la red XYO Network, más confiable es. Para seguir haciendo crecer la red, XYO Network está asociándose con otras empresas para ampliar su red de Sentinels más allá de su propia red de balizas XY Findables.

---

9 Agradecimientos

Este informe es el producto del esfuerzo de un equipo estimulante y su redacción fue posible debido a la convicción en nuestra visión de las siguientes personas: Raul Jordan (Harvard College, Thiel Fellow y asesor de XYO Network); por su contribución en sintetizar nuestro informe y ayudarnos a comunicar con elegancia los detalles técnicos. Agradecemos a Christine Sako su excepcional ética de trabajo y precisión en la revisión de este informe. La coherencia en la estructura y mejores prácticas de nuestro informe son el fruto de sus esfuerzos. Agradecemos a Johnny Kolasinski su investigación y recopilación de los casos de uso correspondientes. Por último, agradecemos a John Arana su cuidadosa revisión y comentarios creativos.

Referencias

[1] Blanchard, Walter. Hyperbolic Airborne Radio Navigation Aids. Journal of Navigation, 44(3), septiembre de 1991.

[2] Karapetsas, Lefteris. Sikorka.io. http://sikorka.io/files/devcon2.pdf. Shanghai, 29 de septiembre de 2016.

[3] Di Ferrante, Matt. Proof of Location. https://www.reddit.com/r/ethereum/comments/539o9c/proof.of.location/. 17 de septiembre de 2016

[4] Goward, Dana. Testimonio de RNT Foundation ante el Congreso, audiencia de la Cámara de Representantes de EE. UU.: “Finding Your Way: The Future of Federal Aids to Navigation,” Washington DC, 4 de febrero de 2014.

Glosario

precisión Medida de la confianza que tiene un punto o heurística de datos dentro de un margen de error específico

Archivist Un Archivist almacena heurística como parte de un conjunto de datos descentralizado con el objetivo de almacenar libros mayores históricos pero sin este requisito. Incluso si parte de la información se pierde o no está disponible temporariamente, el sistema sigue funcionando solo que con menor precisión. Los Archivists también indexan los libros mayores para poder devolver una cadena de datos de registro si es necesario. Los Archivists almacenan datos sin procesar y se les recompensa únicamente por la recuperación de los datos. El almacenamiento siempre es gratuito.

Best Answer Definimos el término Best Answer como una respuesta única, entre una lista de respuestas posibles, que posee la mayor puntuación de validez y una puntuación de precisión más alta que la precisión mínima requerida.

Best Answer Algorithm Algoritmo que se utiliza para generar las Best Answer Scores cuando un Diviner escoge una respuesta. La red XYO Network admite la adición de algoritmos especializados y permite al cliente especificar cuál algoritmo utilizar. Se requiere que dicho algoritmo proporcione el mismo resultado cuando cualquier Diviner lo ejecute en el mismo conjunto de datos.

Bound Witness Bound Witness es un concepto al que se llega gracias a la existencia de heurística bidireccional. Debido a que no es útil usar una fuente de datos no confiable (un oráculo) para la resolución de contratos digitales, hay un aumento sustancial en la certeza de los datos proporcionados al establecer dicha heurística. La principal heurística de ubicación bidireccional es la proximidad, ya que ambas partes pueden validar la instancia y el rango de la interacción al cofirmarla. Esto brinda una prueba de conocimiento cero de que los dos nodos estaban en proximidad uno del otro.

Bridge Un transcriptor heurístico. Transmite de manera segura los libros mayores heurísticos de los Sentinels a los Diviners. El aspecto más importante de un Bridge es que un Diviner puede estar seguro de que los libros mayores heurísticos que recibe de un Bridge no han sido alterados. El siguiente aspecto más importante de un Bridge es que añade metadatos de Proof of Origin adicionales.

certeza Medida de la probabilidad de que un punto o heurística de datos no haya sido dañado ni manipulado.

criptolocalización Ámbito de la tecnología criptográfica de localización

criptoeconomía Disciplina formal que estudia los protocolos que rigen la producción, distribución y consumo de bienes y servicios en una economía digital descentralizada. La criptoeconomía es una ciencia práctica que se centra en el diseño y la caracterización de estos protocolos.

Diviner Un Diviner analiza datos históricos almacenados en la red XYO Network para responder a una consulta determinada. La heurística almacenada en la red XYO Network debe tener un alto nivel de Proof of Origin para determinar su validez y precisión. Un Diviner evalúa al testigo en base a su Proof of Origin para obtener y entregar las respuestas. Como la red XYO Network es un sistema independiente de la confianza, se debe incentivar a los Diviners para que suministren análisis honestos de la heurística. A diferencia de los Sentinels y Bridges, los Diviners utilizan la Proof of Work para añadir respuestas a la blockchain.

heurística Punto de datos acerca del mundo real relativo a la posición de un Sentinel
(proximidad, temperatura, luz, movimiento, etc…).

oráculo Parte de un sistema de DApp (aplicación descentralizada) responsable de proporcionar una respuesta con precisión y certeza para resolver un contrato digital. El término "oráculo" tiene su origen en la criptografía, donde indica una fuente realmente aleatoria (por ejemplo, un número aleatorio). Proporciona la puerta necesaria desde la ecuación criptográfica al mundo. Los oráculos envían información a los contratos inteligentes desde fuera de la cadena (el mundo real, sistema fuera de la cadena). Los oráculos son interfaces entre el mundo digital y el real. Si tomamos un ejemplo macabro, consideremos un contrato de Última voluntad y testamento. Las cláusulas del testamento se ejecutan cuando se confirma que el testador ha fallecido. Es posible construir un servicio de oráculo para activar un testamento al compilar y agregar datos relevantes de fuentes oficiales. El oráculo se usaría como feed o punto final de un contrato inteligente a donde consultar para comprobar si la persona ha fallecido.

Origin Chain Score Puntuación asignada a una Origin Chain para determinar su credibilidad. Esta evaluación tiene en cuenta longitud, vueltas innecesarias, superposición y redundancia.

Origin Tree Conjunto de datos de entradas de libro mayor extraídas de distintas Origin Chains para establecer el origen de la entrada heurística con un nivel especificado de certeza.

Proof of Origin La Proof of Origin es la clave para comprobar que los libros mayores que ingresan a la red XYO Network son válidos. Las ID exclusivas para la fuente de los datos no son prácticas ya que pueden falsificarse. La firma con claves privadas no es práctica debido a que la mayoría de los componentes de la red XYO Network son difíciles, sino imposibles, de proteger físicamente; la posibilidad de que un impostor robe una clave privada es demasiado grande. Para resolver esto, la red XYO Network utiliza Transient Key Chains. Su beneficio es que es imposible falsificar la cadena de origen de los datos. No obstante, una vez que se ha roto la cadena, está rota para siempre y no puede continuarse, lo que la convierte en una isla.

Proof of Origin Chain Una Transient Key Chain que enlaza una serie de entradas heurísticas de libro mayor de los Bound Witness.

Proof of Work Proof of Work son datos que reúnen determinados requisitos y que son difíciles de producir (es decir, costosos y que llevan mucho tiempo) pero sencillos de comprobar por terceros. La producción de una Proof of Work puede ser un proceso aleatorio con baja probabilidad de generación por lo que, en promedio, se requiere un proceso riguroso de prueba y error antes de que se cree una Proof of Work válida.

Sentinel Un Sentinel es un testigo heurístico. Observa la heurística y da fe de su certeza y precisión al producir libros mayores temporales. El aspecto más importante de los Sentinels es que producen libros mayores que otorgan certeza a los Diviners que provienen de la misma fuente al añadirles la Proof of Origin.

smart contract Protocolo acuñado por Nick Szabo antes de Bitcoin, supuestamente en 1994 (por lo que algunos creen que es Satoshi Nakamoto, el místico y desconocido inventor de Bitcoin). La idea de los contratos inteligentes es codificar un acuerdo legal en un programa y que las computadoras descentralizadas ejecuten sus condiciones en lugar de que los seres humanos interpreten y ejecuten los contratos. Los contratos inteligentes reúnen al dinero (por ejemplo, Ether) y a los contratos en el mismo concepto. Debido a que los contratos inteligentes son deterministas (como los programas de computación) y totalmente transparentes y legibles, son una manera potente de reemplazar a los intermediarios y los agentes.

Transient Key Chain Una Transient Key Chain eslabona una serie de paquetes de datos mediante criptografía de clave transitoria.

independiente de la confianza Característica mediante la cual todas las partes del sistema pueden alcanzar el consenso sobre cuál es la verdad canónica. El poder y la confianza se distribuyen (o comparten) entre los participantes de la red (por ejemplo, desarrolladores, mineros y consumidores) en lugar de concentrase en un único

individuo o entidad (por ejemplo, bancos, gobiernos e instituciones financieras). Es un término común que puede comprenderse fácilmente. Las blockchains no eliminan realmente la confianza. Lo que hacen es minimizar la cantidad de confianza necesaria de cualquier actor individual del sistema. Lo hacen al distribuir la confianza entre distintos actores del sistema mediante un juego económico que los incentiva a cooperar según las reglas definidas en el protocolo.

XY Oracle Network XYO Network

XYO Network XYO Network significa "XY Oracle Network.” Está compuesta por todo un sistema de componentes/nodos que admiten XYO que incluye Sentinels, Bridges, Archivists y Diviners. La función principal de la red XYO Network es actuar como un portal mediante el cual los contratos inteligentes digitales pueden ejecutarse gracias a las confirmaciones de geoubicación del mundo real.

XYOMainChain Blockchain inmutable de la red XYO Network que almacena transacciones de consulta junto con los datos recopilados por los Diviners y su puntuación de origen asociada.