ties.network

Plataforma descentralizada de negocio

Libro blanco

Dmitry Kochin, Alexander Neymark

Abril, 2017

TTabla de contenidos:

1. Introducción

1.1 Resumen

Las tecnologías modernas nos permiten redescubrir los temas de descentralización y libertad para millones de personas. La oleada de interés por las criptomonedas y la economía descentralizada es una prueba directa de la decepción de la gente en el sistema clásico de relaciones entre mercaderías y dinero y redes profesionales y su intento de escapar a la contra-economía.

Este documento presenta el proyecto Ties.Network - un nuevo "LinkedIn" para la cripto-comunidad, Una plataforma de negocio distribuida que permite a operadores, inversionistas, desarrolladores, consultores y entusiastas encontrar socios de negocios, ofrecer sus servicios, cerrar acuerdos basados en contratos inteligentes, contratar personal, anunciar sus propios servicios en un ambiente cómodo y seguro y también financiar proyectos (individualmente o como parte de una comunidad particular). La plataforma le permite obtener la máxima exposición a la cripto-comunidad a través de un sistema de calificaciones y revisiones. También le permite actuar de manera anónima mientras mantiene las transacciones con otros miembros de la comunidad seguras.

Ties.Network satisface la necesidad de la cripto-comunidad para conectarse y la necesidad de asegurar las transacciones de negocios P2P en una nueva contra-economía. Hoy la comunidad está fragmentada y las conexiones son frágiles por dos razones. Todavía es un mercado nuevo (aunque está creciendo rápidamente), y porque es tan nuevo, es difícil encontrar profesionales en los que uno pueda confiar inmediatamente y llegar a un acuerdo. **Ties.Network tiene como objetivo resolver la cuestión de la confianza para la cripto-comunidad en un nivel fundamental, dando a las personas la oportunidad de encontrarse y hacer negocios en un nuevo entorno seguro, de acuerdo con los principios de la economía descentralizada.**

La plataforma utiliza un sistema de **"calificación genuina"**, lo que significa que sólo aquellos que realmente hicieron negocios con un usuario tienen derecho a calificarlos como profesionales, basando sus revisiones en transacciones de negocios exitosas y no en suposiciones o información de marketing. Esto significa que las revisiones no pueden ser falsas y que la plataforma se convertirá en una fuente sólida y confiable de información sobre proyectos viables relacionados con cadenas de bloques globales, tecnologías descentralizadas, reportes reales de due diligence sobre los próximos eventos de generación de fichas y dará voz a un verdadero bloque de expertos que tienen un historial de acuerdos exitosos.

Usando Ties.Network **la gente puede conectarse y hacer negocios a través de contratos inteligentes**, lanzar proyectos, promover sus negocios, encontrar proyectos para invertir en, y grupos para unirse. Además, tal plataforma ayudaría en la contratación de colaboradores, la publicación de puestos de trabajo, así como CVS con todas las partes beneficiarse de estas características.

Actualmente, no existe una plataforma que proporcione esta gama de servicios. Es hora de introducir una red pública de gran escala basada en la tecnología de cadena de bloques (blockchain) que incluya un libro mayor descentralizado para fines de negocios y de redes sociales. Esto permitirá que la cripto-comunidad tenga acceso a una plataforma única, universal y pública que permita la cooperación y ofrezca oportunidades para discutir y hacer negocios en el mismo ambiente.

1.2 ¿Qué es Ties.Network?

Como una herramienta de negocios Ties.Network es una plataforma social descentralizada donde los profesionales de negocios pueden conectarse y hacer negocios a través de contratos inteligentes en poco tiempo. La plataforma utiliza un sistema de calificación confiable, asegurando así que todos los participantes pueden centrarse únicamente en los negocios y los beneficios de las relaciones beneficiosas, y dejar los problemas de verificación y confianza a las soluciones integradas de la plataforma.

Como un producto de TI (Tecnología de la información), Ties.Network se basa en TiesDB - una base de datos pública, descentralizada y distribuida noSQL que permite almacenar grandes cantidades de datos dinámicos y buscar dentro del contenido de los archivos. TiesDB es una solución pública de código abierto que puede ser utilizada por otros dApps y proyectos descentralizados relacionados con cadenas de bloques para facilitar su entrada en el mercado y la estructura de grandes cantidades de datos.

Ties.Network es el análogo de LinkedIn para la cripto-comunidad. Es una plataforma descentralizada para operadores, inversionistas, desarrolladores, consultores y entusiastas que permite encontrar y contratar socios, empleados y voluntarios, vender sus productos o servicios, asegurar negocios a través de contratos inteligentes, promocionarse y financiar sus proyectos, entre otros artículos. Las personas pueden trabajar individualmente o como equipos para lograr sus objetivos.

La calificación libre y las revisiones (colaboración abierta distribuida o externalización abierta de tareas) dan a cada participante oportunidades máximas de relaciones públicas, al mismo tiempo que les da la opción de anonimato. En todos los casos, todas las transacciones son 100% seguras.

En el registro, cada usuario recibe una calificación por defecto basada en observaciones objetivas de la actividad del usuario en la cripto-comunidad y basada en los documentos proporcionados. La comunidad modificará esta calificación con base en la revisión de los acuerdos que ya han sido procesados en la plataforma a través de un voto imparcial y descentralizado.

1.2.1 Claves principales de la plataforma

Ties.Network (véase el capítulo 3) la integración de los contratos inteligentes en una plataforma de negocios permite a sus usuarios hacer lo siguiente:

- Comercio de bienes y servicios
- Comercio de criptomonedas
- Contratar y reclutar especialista
- Participar en eventos de generación de fichas y proyectos de cadena de bloques
- Recibir retroalimentación para los eventos de inicializadores o de generación de fichas
- Promoción de eventos de generación de tókenes y creación de redes con inicializadores

1.2.2 El concepto de base de datos público noSql

Durante los últimos años, la comunidad de cadena de bloques ha crecido rápidamente. Hoy en día la cadena de bloques no sólo da a la gente la oportunidad de hacer transacciones financieras seguras, sino que también ofrece una amplia gama de otros servicios. Los contratos inteligentes se han convertido en un gran avance en este campo. El contrato inteligente es un programa que se ejecuta en el núcleo de la cadena de bloques permitiendo el procesamiento personalizado flexible de cada transacción. Los contratos inteligentes en Ethereum [2] son Turing-completos y permiten algoritmos de programación de cualquier

complejidad.

Es por eso que Ethereum ha creado un nuevo mercado de aplicaciones descentralizadas, aplicaciones que se ejecutan directamente en la cadena de bloques heredando su distribución, descentralización y seguridad. Sin embargo, este crecimiento del mercado está restringido por la ausencia de un almacenamiento de datos adecuado. Las aplicaciones serias requieren almacenamiento de datos grandes y rápidos y deben ser capaces de realizar una búsqueda compleja dentro de los archivos. Nos enfrentamos a nosotros mismos al diseñar la arquitectura de Ties.Network.

Existen algunas implementaciones de almacenes de datos descentralizados tales como IPFS (4.9.3), almacenamiento de archivos en la nube (4.9.4) o cadena de bloques especiales (4.9.6). Pero todos ellos tienen una desventaja significativa - no permiten la búsqueda compleja dentro de los datos almacenados. También hay bases de datos distribuidas (4.9.5), y tienen todas las características requeridas excepto la principal - Tolerancia a la Prueba Bizantina (4.9.1). Por lo tanto, no se pueden utilizar en entornos públicos no confiables.

El problema Bizantino es un experimento destinado a ilustrar las dificultades y desafíos de diseño de intentar coordinar una acción mediante la comunicación sobre un vínculo poco fiable, donde los fallos de comunicación son posibles. **Con esto en mente, los programadores de Ties.Network desarrollaron una base de datos noSql descentralizada pública resistente, TiesDB, que puede ser construida en cualquier cadena de bloques con contratos inteligentes; Soporta replicación, sharding, índices secundarios, búsqueda de texto completo y permite a los usuarios modificar y eliminar datos.** La base de datos es pública en el sentido de que cualquiera puede establecer un nodo TiesDB y participar en la red procesando transacciones de usuarios y ganar dinero con esto. Igualmente, cualquiera puede usarlo para almacenar datos.

Al mismo tiempo, TiesDB mantiene el mismo poderoso sistema de procesamiento y velocidad que usted encuentra en las bases de datos privadas noSql (intra-corporativas). Debido a que TiesDB puede hacerse compatible con cualquier cadena de bloques que soporte contratos inteligentes Turing-completos, los miembros pueden usarlo para realizar transacciones en cualquier plataforma. Obtenga más información aquí (capítulo 4.4).

2. Aplicaciones

2.1 Contratos de negocio

Ties.Network se puede utilizar para hacer los siguientes contratos de negocio (dentro o fuera de la cripto-comunidad):

- Los trabajos de subcontratación (por ejemplo, programación, presentación de un libro blanco, traducción, diseño, asesoramiento, etc.), donde los términos y condiciones están regulados por la automatización de contratos inteligentes.
- Participar en trabajos freelance, temporales o de contratos, donde los contratos inteligentes regulan los términos y detalles del proyecto.
- Obtener retroalimentación de los expertos sobre la plataforma.

2.1.1 Haciendo conexiones

1. El usuario utiliza palabras clave para encontrar perfiles de posibles empleadores o conexiones de negocios.
2. Ambas partes discuten y negocian el acuerdo.
3. El usuario finaliza el acuerdo depositando el número acordado de fichas en la cartera de contrato inteligente, que actúa como garante del acuerdo. Si alguna de las partes falla, se devuelven las fichas.
4. Después de que se haya realizado el servicio o comercio, la cartera de contrato inteligente deposita las fichas al destinatario (o cliente) según lo contratado.
5. Los moderadores del sistema actúan como árbitros per-diem y usan los términos del contrato para resolver las disputas, cuando y si es necesario.

Los moderadores (capítulo 5) son recompensados por la compañía, ya que necesitan un incentivo financiero para regular el libro mayor de cadena de bloques y supervisar sus transacciones.

2.2 Inicializando un nuevo proyecto

Cualquier usuario puede subir su proyecto, detalles de la organización o perfil en Ties.Network. La plataforma puede ser utilizada para reclutar miembros del equipo del proyecto, para crear una cartera de proyectos para pagar a los miembros del equipo, o para recibir donaciones. Además, los usuarios pueden negociar los términos del acuerdo y compartir documentos y fotos con miembros de la comunidad

Los usuarios pueden agregar la siguiente información al perfil del proyecto:

- El Currículum Vitae del jefe de proyecto y su resumen biográfico
- Su información de contacto
- Enlaces a su sitio web y/o blog
- Información sobre empleo anterior, libros publicados, proyectos anteriores, cartera, etc.

También puede utilizar la plataforma para compartir su proyecto con personas u organizaciones

seleccionadas y bloquear las que desea excluir. Cuando inicie su propio proyecto, puede invitar a sus propios miembros del equipo, crear una cartera para el proyecto para pagar a los participantes relevantes y recibir donaciones, y compartir documentos y fotos con los miembros de su comunidad (o con el público) entre otros temas.

Ties.Network utiliza una plataforma automatizada de contrato inteligente, basada en Ethereum, donde las transacciones están codificadas en su libro mayor y donde las condiciones se ejecutan automáticamente una vez que se cumplen los términos del contrato. Los usuarios usan esta función para invertir, votar, recaudar fondos y financiación colectiva (crowdfunding).

2.3 La comunidad de expertos

La plataforma revalida todas las partes, registra y autentica todas las transacciones que utilizan la plataforma, rechazando datos ilegítimos o cuestionables. También se puede solicitar a los miembros expertos de Ties.Network que proporcionen retroalimentación sobre su proyecto o empresa, si lo desea.

El nivel de anonimato es opcional para los usuarios. La opción de permanecer en el anonimato hace que sea un ambiente seguro para cualquier persona que advierta a los inversores de financiar una estafa, para advertir a los participantes de las organizaciones ilegítimas, para advertir a alguien contra la contratación de un contratista determinado o aceptar un determinado trabajo. La comunidad de expertos puede utilizar esta plataforma para proporcionar retroalimentación profesional con respecto a los temas discutidos en la plataforma o señalar las limitaciones o deficiencias de cualquier transacción en particular.

2.4 Qué puede Ties.Network hacer por Ud.:

1. Ayudarle a participar en el comercio económico con entidades de cualquier país.
2. Proporcionar una plataforma transparente en tiempo real para realizar el comercio. Los beneficios incluyen: negocios de calificación, tecnología de contratos inteligentes, fondos bloqueados que sólo se liberan cuando se cumple el contrato.
3. Proporcionar seguridad: todas las transacciones pueden ser verificadas y supervisadas por expertos calificados que intervienen para resolver conflictos si así lo desea.
4. Proporcionarle una extensa red de miembros altamente profesionales de la cripto-comunidad, conectada a la industria de la cadena de bloques, a la cripto-economía y a las TI.
5. Darle una plataforma flexible para ampliar su red de conexiones profesionales y buscar especialistas en áreas completamente diferentes.
6. Dar transparencia al proceso de externalización.
7. Dar apertura y escalabilidad con un protocolo básico técnicamente ilimitado que puede manejar una cantidad creciente de almacenamiento, y que tenga el potencial de ser ampliado para acomodar el crecimiento del número de socios.

3. Aspectos de Ties.Network

3.1 Definiciones

3.1.1 Perfil

El perfil sirve como un punto de entrada único para el usuario a la comunidad. El registro denota el acuerdo con las reglas de la comunidad y se completa con la apertura de una cartera que contiene moneda TIE (fichas de plataforma Ties.Network) (capítulo 6).

Las claves de la cartera se adjuntan al perfil del usuario. Hay una opción para usar/restaurar la cartera de varios dispositivos. Al llenar el perfil, el usuario asigna el grado de anonimato que él o ella quiere. Incluso si el usuario selecciona el anonimato total, los mediadores de la plataforma todavía pueden investigar y regular la conducta del usuario (a través de la geografía, datos personales, fotos que contienen información personal, estilística, ortografía y puntuación de textos, etc.) para mantener la confianza de la plataforma. Además, la plataforma proporciona a un usuario una calificación multidistribución, implementa un sistema de revisión y permite a los anunciantes colocar y administrar anuncios.

3.1.1.1 Su perfil

Su perfil es una página que describe su historial de carrera, educación y otros contenidos relacionados que puede publicar.

La información del usuario incluye:

- Nombre y apellidos
- Fecha de nacimiento
- Información de contacto
- Ocupación o posición actual
- Una fotografía de rostro profesional
- Habilidades y experiencias
- Anuncios empresariales
- Palabras clave que se incluirán en la búsqueda
- Un formulario de calificación y revisión (que pueden ser rellenados por otros usuarios sobre la base de transacciones de negocios anteriores), así como un formulario de publicidad para sus productos y servicios.
- Chat – Se refiere a la comunicación entre los usuarios en tiempo real. Todo el historial de mensajes en las conversaciones se almacena en el lado del cliente (móvil/escritorio) y se cifra utilizando un protocolo de extremo a extremo. El contenido de los chats (fotos, vídeos, archivos) también se cifra y se almacena de la misma manera.

3.1.2 Acuerdos

Esto se refiere a un acuerdo en la que dos o más partes entran para su beneficio mutuo en Ties.Network. En nuestro caso, un “acuerdo” denota el intercambio económico de fichas TIE para algunos productos, bienes, servicios o monedas de cualquier forma. También implica invertir en inicializadores, proyectos y participar en eventos de generación de ficha.

3.1.2.1 Invoice (Factura)

Una lista de bienes enviados o servicios prestados, con una declaración de la suma adeudada por éstos. En referencia a Ties.Network:

- Un usuario llamado A contrata un acuerdo con la parte B para completar un trabajo o un servicio. B entonces se presenta a A con un formulario que demuestra que el trabajo/servicio se completó y solicita el pago.
- A acepta la factura y paga a B con moneda TIE.

3.1.2.2 Garantía y disputas

El pago se transfiere a una garantía de contrato inteligente, que sólo se libera cuando los resultados de la transacción son aceptados por todas las partes involucradas. Cuando y sólo sea necesario, los árbitros de Ties.Network intervendrán para resolver disputas (para más información, véase más adelante “Auto-organización y motivación”).

3.1.2.3 Criptomoneda y cambio de moneda fiduciaria para fichas TIE

La esencia de la plataforma indica comercio e intercambio, dar y recibir, y compra y venta con fichas TIE. La plataforma permitirá el intercambio P2P de ficha TIE a otras monedas y moneda fiduciaria.

3.1.3 Búsqueda de resultados

Los usuarios pueden buscar perfiles de empleadores, servicios, organizaciones, individuos y similares. Los resultados de búsqueda se presentan como una lista con filtros (por ejemplo, individuos, proyectos, conexiones, calificaciones).

3.1.4 Proyecto

Un proyecto sobre Ties.Network es un instrumento para la colaboración de los usuarios dentro de una determinada industria permitiendo a los usuarios discutir/compartir sus ideas, realizar transacciones financieras P2P entre los miembros del equipo del proyecto y recopilar fondos de otros usuarios de la plataforma.

3.1.4.1 Atributos básicos de un proyecto:

- La existencia de un propietario del proyecto (público o anónimo).
- La existencia de un moderador del proyecto (rol dentro del proyecto).
- La existencia de múltiples propietarios de firmas de la cartera de proyectos.
- La existencia de una idea sólida y una descripción del proyecto.
- Posibilidad de crear un nombre corto para el proyecto para promocionarlo fuera de la red.
- Posibilidad de crear proyectos públicos y privados.
- Posibilidad de crear proyectos temporales o permanentes.
- Posibilidad de publicar materiales de proyectos (fotos, vídeos, documentos, texto, comentarios).
- Posibilidad de discutir los materiales del proyecto.
- Posibilidad de cerrar el proyecto.
- Posibilidad de añadir nuevas personas al proyecto y crear un canal para la entrada.

- Instrumentos de financiación colaborativa del proyecto (recaudación de fondos en la cartera del proyecto).
- Posibilidad de crear derivados para financiar diferentes partes del proyecto.

3.2 Ejemplo del proceso de trabajo

1. El acceso a la plataforma se proporciona a través de un cliente móvil (Android, iOS, Windows Phone), así como versiones de escritorio de la plataforma para todos los principales sistemas operativos (Windows, MacOS, Linux).
2. El proceso de registro implica la creación de una cartera (personal o pública con firmas) y una cuenta (con o sin datos personales).
3. El usuario elige una industria/campo determinado y crea un proyecto o se une a uno existente para fines de discusión, participación o inversión.
4. La plataforma ayuda a encontrar contactos o clientes, realizar ofertas y emitir facturas.
5. Los usuarios compran TIE (la ficha usada para ofertas y facturas) a través de un proceso de registro simplificado.
6. Las carpetas TIE están disponibles para transacciones P2P instantáneas usando pagos por Internet o para pagar en persona (usando NFC o códigos QR).
7. TIE se puede negociar para la moneda fiduciaria u otras criptomonedas de intercambio en la plataforma o un intercambio exterior.

3.3 Economía

La plataforma Ties.Network no toma una comisión de dinero recibido de bienes o servicios, ni toma una parte de cualquier proyecto. En su lugar, Ties.Network impone impuestos y comisiones sobre los servicios para pagar a los moderadores y mantener su servicio.

3.3.1 Fuentes de ingreso de la plataforma

Ties.Network obtiene sus ingresos de los siguientes procesos:

- Publicidad (auto-publicidad por los usuarios de la plataforma)
- Impuesto de depósito
- Cambio monetario

Cada uno de estos ingresos se utilizará para pagar a los moderadores y garantizar la eficacia óptima de la plataforma (para más información, véase “autoorganización y motivación”).

3.3.2 Fuentes de ingreso para los nodos

Ties DB obtiene sus ingresos de las siguientes fuentes:

- Almacenaje de contenido en el servidor de nodo
- Recuperar contenido del servidor de nodo

Cuando el usuario coloca el contenido en la base de datos en el servidor de nodos, paga la tarifa de servicio del nodo para almacenar y procesar el contenido. El sistema no sólo motiva a los propietarios de nodos a utilizar el proceso, sino que también evita que los atacantes desborden la base de datos. Posteriormente, la plataforma reembolsa los gastos del usuario en caso de que los usuarios no muestren

signos de actividad maliciosa y no haya colusión entre el participante y el nodo (para más información, véase más adelante “Autoorganización y motivación”). Los costos de usuario para el almacenamiento, así como para la recuperación de contenido, provienen del presupuesto de la plataforma.

4. La arquitectura de Ties.Network

4.1 Características de la arquitectura

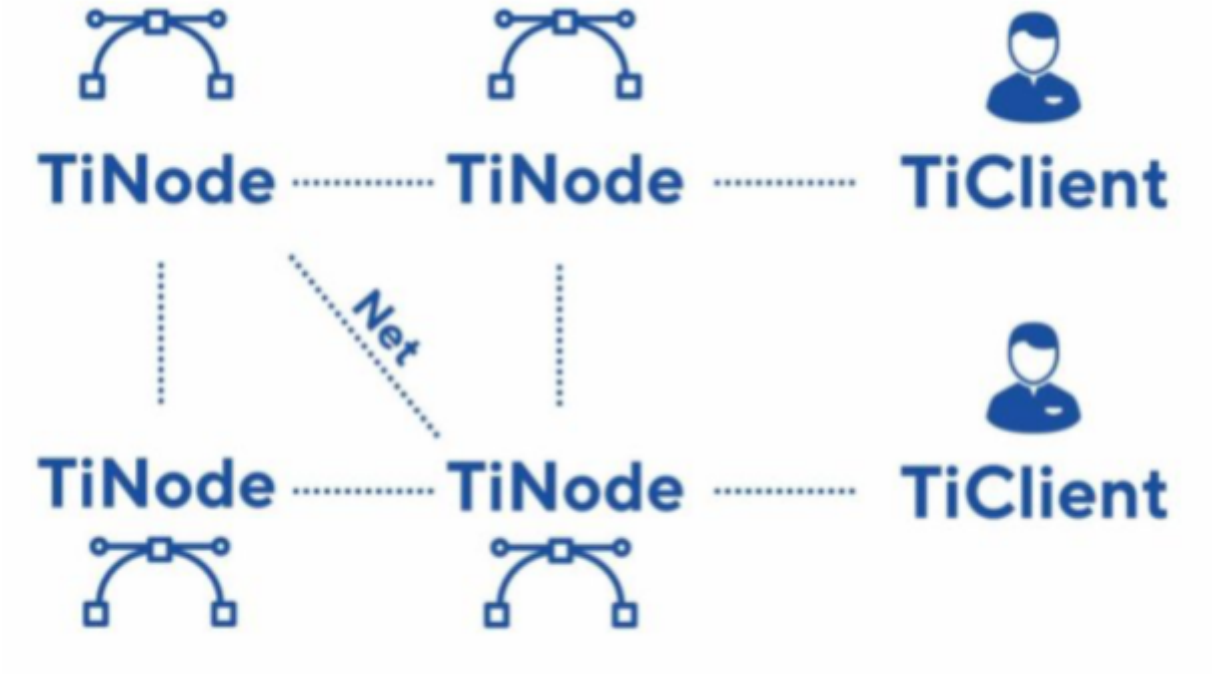

Fig. High level overview of the platform architecture

Fig. Vista general de alto nivel de la arquitectura de la plataforma

Ties.Network, como una plataforma adecuada para hacer negocios, cumple con los siguientes requisitos:

1. **Descentralización.** La plataforma Ties.Network representa una red descentralizada de servidores (nodos). Las aplicaciones cliente se conectan a los nodos dentro de la red. En el corazón de cada TiNode está la cadena de bloque que alimenta la descentralización. Por el momento, varias versiones de cadena de bloques pueden ser utilizadas para Ties.Network. Ethereum [2] se utilizará para la etapa inicial, pero podemos transferir a otra cadena de bloques con contratos inteligentes, por ejemplo, RChain [3], si es necesario, para satisfacer el crecimiento de la red y otros requisitos como escalamiento y velocidad, si Ethereum no puede abordar problemas de escalabilidad.

2. **Estabilidad.** La plataforma es resistente a las actividades maliciosas de los participantes (estabilidad a los ataques de Sybil, el Problema de los Generales Bizantinos, etc.). La cadena de bloques resiste intrínsecamente el comportamiento malicioso de los miembros individuales de la red. Sin embargo, si hay algo más que la cadena de bloque en el sistema, se requieren esfuerzos adicionales para asegurar la sostenibilidad. Volveremos a esta cuestión cuando consideremos el

almacenamiento de datos (capítulo 4.4).

3. **Anonimato** de servidores y usuarios individuales, así como privacidad de las comunicaciones entre servidores y usuarios. Tradicionalmente, el enmascaramiento de IP y los métodos de cifrado de tráfico como TOR [4] o I2P [5] se han utilizado para proporcionar el anonimato y la privacidad para los clientes de la plataforma y los nodos individuales ocultando su dirección IP. Sin embargo, estos métodos son demasiado lentos y los datos sincronizados por el servidor requieren un procesamiento de velocidad mucho más potente. Para resolver el problema, se utiliza una red de malla Hyperboria [6] que utiliza el protocolo cjdns [7].

4. **Almacenamiento de datos.** La capacidad de almacenar datos y realizar una búsqueda a través de una gran cantidad de datos estructurados.

5. **Escalabilidad.** La capacidad de la plataforma para manejar una cantidad creciente de trabajo para acomodar el crecimiento del miembro.

6. **Fuente abierta.** Todos los componentes de la plataforma tienen código abierto y se publican con una licencia abierta.

7. **Publicidad.** Cualquiera puede unirse al sistema de soporte de red instalando el software abierto del sistema.

8. **Rentabilidad.** Los usuarios pueden beneficiarse de la plataforma.

9. **Velocidad.** La plataforma incluye procesamiento rápido para lograr la computación en tiempo real y superar el retraso causado por los actuales modelos basados en la nube.

10. **Posibilidades de expansión.** La plataforma soporta aplicaciones de terceros (dapps) y proporciona un nuevo modelo para la creación de aplicaciones exitosas y masivamente escalables.

4.2 Capas de la arquitectura

A un nivel alto podemos distinguir las siguientes capas de la plataforma.

1. TiClient – aplicación cliente
2. TiesDB - base de datos pública descentralizada
3. Contratos inteligentes
4. Cadena de bloques
5. Red Hyperborea

Los usuarios interactúan con Ties.Network con la aplicación cliente TiClient. TiClient se conecta a TiesDB y a cadena de bloques. TiesDB se utiliza para almacenar y recuperar datos de usuario. TiClient y TiesDB utilizan contratos inteligentes en cadena de bloque para transacciones financieras y para asegurar la estabilidad de operaciones críticas. Todos los nodos están conectados a través de la red Hyperboria para proporcionar velocidad, anonimato y encriptación de extremo a extremo de todas las comunicaciones.

4.3 Almacenamiento de datos

Ties.Network se ocupa de una gran cantidad de datos, por lo que debemos elegir el lugar adecuado para almacenarlo. El depósito de datos distribuidos debe estar disponible para las aplicaciones que se ejecutan en la parte superior de la cadena de bloques con las siguientes cualidades:

1. Distribución
2. Publicidad
3. Resistencia al problema de los Generales Bizantinos y otras formas de ataque en una red pública
4. Soporte Sharding (la capacidad de duplicar sólo una parte de los datos en cada nodo con el fin de aumentar la capacidad de almacenamiento de datos)
5. Velocidad
6. Capacidad para almacenar datos estructurados
7. Capacidad para borrar datos

El problema es que actualmente no hay implementación que cumpla con todos estos requisitos. Hay algunos almacenamientos de archivos descentralizados, pero tienen inconvenientes. La principal es que ninguna solución proporciona herramientas para buscar los archivos por su contenido, lo cual es crítico para la mayoría de las aplicaciones. Examinaremos las soluciones actuales en el capítulo 4.9 y subrayaremos sus limitaciones. Y en el próximo capítulo presentamos nuestra propia solución universal para el almacenamiento de datos estructurados descentralizados - TiesDB.

4.4 TiesDB

4.4.1 TiesDB: Información general

Existen muchas implementaciones de bases de datos distribuidas que cumplen todos los requisitos anteriores, excepto una - Tolerancia de fallas Bizantinas (véase 4.9.5). Por lo tanto, no pueden ser públicas. Así que proponemos TiesDB, que trae BFT a bases de datos distribuidas noSQL y conserva sus otras cualidades.

TiesDB es una base de datos descentralizada de nueva generación con las siguientes interfaces innovadoras:

1. **Distribución**
   TiesDB soporta un número ilimitado de réplicas, cada una de las cuales puede ser un coordinador (ver 4.4.4). Al solicitar cualquiera de ellos, el usuario obtiene acceso a todos los datos.
2. **Publicidad**
   TiesDB se crea para operar en la esfera pública. Pueden añadirse nuevos nodos a la red y tomarán parte de la carga en cualquier momento.
3. **Resistencia al Problema de los Generales Bizantinos** y otros tipos de ataques en una red pública Todos los datos colocados en TiesDB están firmados por el propietario (ver 4.4.2), por lo que los nodos no pueden cambiar los datos de forma arbitraria, ni corromper datos al replicar otros

nodos. Los intentos de sustitución se detectan inmediatamente a través de cambios en la firma electrónica. Cualquier participante que lo haga, o intente hacerlo, será instantáneamente eliminado de la red. La cadena de bloque externa (para TiesDB) se utiliza para depósitos de TIE, estableciendo derechos de acceso y asentamientos mutuos entre los nodos.

4. **Soporte Sharding**
   Cada nodo es responsable de almacenar un cierto rango de claves de datos primarias. La replicación de datos tiene escalabilidad, por lo que puede crecer con la red.
5. **Velocidad**
   Debido a los principios de almacenamiento de datos (ver 4.4.2), la velocidad de lectura/escritura en TiesDB será casi idéntica a bases de datos privadas similares, como Apache Cassandra.
6. **Capacidad para almacenar datos estructurados**
   Los datos almacenados en Ties.Network complementan su plataforma. Puede ser un documento JSON con una estructura, que es útil para una aplicación particular.
7. **Capacidad para borrar datos**
   La eliminación de datos está soportada en TiesDB. Aunque la eliminación de datos instantánea no puede garantizarse, los datos se eliminarán si los nodos actúan de forma no maliciosa. Un nodo malicioso nunca puede eliminar los datos sin embargo no puede almacenar todo, ya que sólo ciertos intervalos de clave primaria pueden ser enviados a ella.
8. **Lenguaje de consulta con una capacidad para llevar a cabo la búsqueda utilizando más de la clave primaria**
   Utilizamos índices secundarios similares a los métodos de integración de elasticsearch con Cassandra en el proyecto Elassandra, que permitan la búsqueda de clave secundaria así como una búsqueda de texto completo.

Además del proyecto Ties.Network, TiesDB también puede utilizarse para otros proyectos. Se basa en una cadena de bloques, que soporta contratos inteligentes de Turing completos. Por lo tanto, puede ser utilizado para otras cadenas de bloques distribuidas como Ethereum, RChain, y otros.

4.4.2 TiesDB: Principios de organización de datos

Dado que la base de datos necesita satisfacer una amplia gama de aplicaciones de cadena de bloques, ser flexible para un poder de procesamiento rápido, ser resistente al comportamiento malicioso de otros nodos DB, proporcionar un nivel de replicación suficiente y tener mecanismos para motivar a los participantes a apoyar la red, DB está diseñado con las siguientes propiedades:

1. La base de datos es pública, el usuario (cliente) de la base de datos es identificado por su clave pública. La clave pública es el ID de usuario.
2. Cada usuario puede enviar transacciones a la base de datos. Y cada transacción debe ser firmada por este usuario.
3. El nuevo registro firmado por el propietario es creado por el usuario.
4. Solamente el propietario (o el usuario para quien la confianza se instala a través del mecanismo de permisos implementado como un contrato inteligente en la cadena de bloques) puede cambiar el registro después de su creación.
5. Todos pueden leer todas las grabaciones.
6. Cada único código de identificación de usuario crea registros separados.
7. Más permisos complejos pueden ser instalados mediante un contrato inteligente en la cadena de

bloque (por ejemplo, la confianza entre Usuarios específicos, derechos para crear o borrar tablas, etc.)

8. Todos los permisos deben ser verificados para transacciones y replicaciones.

La firma criptográfica obligatoria de cada registro garantiza que ningún registro malicioso puede cambiar o eliminar un registro sin conocer la clave privada. El almacenamiento de datos sigue siendo resistente al ataque de los Generales bizantinos, incluso sin un mecanismo de consenso, mientras que la velocidad sigue siendo la misma que la de las bases de datos noSql.

Por otro lado, un atacante puede generar un ataque Sybil, donde un solo adversario controla múltiples nodos en una red, ya que es desconocido para la red, que los nodos están controlados por la misma entidad adversaria. Podemos resolver este problema con “motivación” o nuestro sistema de incentivos.

4.4.3 TiesDB Sistema incentivador

Una red pública es un tipo de red en la que cualquiera tiene acceso y puede conectarse a otras redes o Internet. Los incentivos se suelen dar para motivar a los participantes y para fomentar la participación ética.

TiesDB es similar a Ethereum Swarm [26] ofrece los siguientes incentivos:

- Premio por la extracción de datos
- Premio por el almacenamiento de datos

Los premios se asignan a partir de los fondos del usuario que hace consultas. Dado que los pagos a través de la cadena de bloques son lentos, se pueden utilizar dos métodos para pagos rápidos: transacciones fuera de cadena y “chequeras”. En transacciones fuera de cadena, el usuario debe crear un canal fuera de cadena con cada nodo de la base de datos o utilizar canales intermedios entre nodos. Dado que dicho canal requiere su propio repositorio de financiación, tal enfoque puede ser muy costoso, por lo que se prefiere el enfoque de “chequera”. Antes de acceder a la base de datos, el usuario deposita parte de sus fondos en un contrato inteligente - 'chequera', y los fondos pueden ser utilizados como pago o premio.

The chequebook contract assumes the following:

- The contract monitors the total amount issued to each recipient at the time of the connection.
- When sending a cheque, the owner must memorize the total amount sent to each recipient.

Un cheque se cobra si:

- La dirección del contrato corresponde a la dirección en el cheque.
- El cheque es firmado por el propietario (ID de usuario - llave pública).
- El monto total en el cheque es mayor que el monto en el cheque anterior dado al mismo destinatario.

Los participantes usan “cheques” para recompensar nodos. El nodo receptor sólo puede guardar el último cheque recibido de cada usuario y lo cobra depositándolo en la “chequera”.

4.4.4 Premio por la extracción de datos

Los datos de los nodos DB tienen cierto nivel de replicación. Específicamente, los datos con una clave específica se almacenan sólo en una parte de los nodos, por ejemplo, en *N* de ellos. Sin embargo, el usuario puede referirse a cualquier nodo para los datos, que luego actúa como un "coordinador".

En una solicitud del usuario, el coordinador determina estos *N* nodos por las claves de datos y las rutas de la solicitud a ellos. Los datos devueltos por los nodos son verificados por el coordinador para el cumplimiento con las firmas electrónicas y comparadas con la marca de tiempo, después de lo cual el registro más reciente se devuelve al usuario.

Para que esto funcione, el incentivo debe cumplir las siguientes condiciones:

1. Los nodos más rápidos reciben más pagos.
2. Los nodos que devuelven datos antiguos recibirían menos pagos.
3. Los nodos tardíos (que no devuelven los datos en absoluto) no reciben pago.
4. El coordinador recibe una cuota fija.

El coordinador emite una factura con los datos, que incluye información sobre los nodos utilizados. Posteriormente, el usuario escribe un cheque para cada uno. A continuación, el coordinador envía las comprobaciones a los nodos. También envía la actualización de los datos a los nodos que no han devuelto datos válidos.

Para protegerse contra los coordinadores maliciosos y los usuarios delincuentes, cada nodo mantiene una lista de usuarios de los que espera el pago. Si el nivel de deuda excede un determinado umbral, el nodo puede dejar de aceptar solicitudes de estos usuarios y coordinadores delincuentes. Y las listas se actualizan a medida que se reciben los cheques.

4.4.5 Premio por el almacenamiento de datos

El premio por la extracción indirecta incentiva el almacenamiento de datos, pero lo hace sólo para los datos populares y a menudo solicitados. Para fomentar el almacenamiento de datos a largo plazo, especialmente si los datos son raramente solicitados, algún tipo de incentivo de almacenamiento de datos es necesario.

Esta pieza de Ethereum Swarm [26] describe el sistema de premios para el almacenamiento. Los nodos entran en un contrato de almacenamiento de datos con el propietario de la información durante un período de tiempo. El almacenamiento se puede pagar en el momento del almacenamiento de datos (actualización) o después de un cierto período de tiempo, siempre que los datos se almacenan realmente. En el caso de que se detecte una pérdida de datos durante la duración del contrato, el nodo puede ser penalizado, ya que cada nodo requiere un registro inicial con un depósito de seguridad.

Cuando almacena datos, el nodo devuelve un recibo que demuestra que ha aceptado el archivo para el almacenamiento. Este recibo le permite comprobar la situación de almacenamiento de los datos asociados y, si es necesario, iniciar un contrato inteligente legal para penalizar el nodo ofensor.

Como los datos no son estáticos, un registro con la misma clave se puede volver a escribir varias veces. Esto significa que no sólo puede corresponder el registro original al recibo presentado, sino que también puede corresponder a un registro con la misma clave que es más reciente para la marca de tiempo.

Cuando el usuario inicia una operación de eliminación de datos, en lugar de borrar datos físicamente, los datos son sustituidos por un registro especial “cero”. El registro se puede eliminar físicamente después de la expiración de su contrato de almacenamiento.

4.4.6 TiesDB: Búsqueda completa de texto

En bases de datos simples de noSql, una búsqueda rápida con un número pequeño de nodos es posible solamente con la llave primaria. Una búsqueda exhaustiva de palabras clave es difícil de lograr sin índices secundarios y capacidades de búsqueda de texto completo. En este sentido, TiesDB difiere de las bases de datos noSql. Sugerimos una solución similar a Elassandra [27], que utiliza los índices de texto completo local de ElasticSearch [28] en cada nodo de la base de datos distribuida noSql Cassandra. Las consultas de texto completo son enviadas por el coordinador (ver 4.4.4) a todos los nodos, para ser mezclados y devueltos al cliente. Dado que los índices adicionales se crean localmente e independientemente en cada nodo, el problema de los Generales Bizantinos ya no es una preocupación aquí.

4.4.7 Conclusión

Construido de acuerdo con los principios anteriores TiesDB resuelve el problema del almacenamiento rápido de datos públicos para las aplicaciones descentralizadas, que necesitan realizar búsquedas avanzadas en los datos almacenados. Esta es una solución única por el momento. TiesDB es público y puede ser utilizado por cualquier aplicación descentralizada de Ethereum. En el futuro TiesDB puede ser portado a cualquier cadena de bloques con contratos inteligentes Turing completos.

4.5 Cjdns y la red Hyperboria

Para resolver el anonimato y el requisito de privacidad, utilizamos la red Hyperboria. Cjdns (Caleb James Delisle Network Suite) es un protocolo de red e implementación de referencia, basado en la idea de que las redes deben ser fáciles de configurar, los protocolos deben escalarse sin problemas y la seguridad debe ser omnipresente. La página de proyecto de Cjdns se jacta de que implementa 'una red cifrada de IPv6 usando criptografía de clave pública para la asignación de direcciones y una tabla de hash distribuida para enrutamiento'. Esencialmente, la aplicación crea una interfaz de túnel en un equipo host que actúa como cualquier otra interfaz de red y es potente en la medida en que permite que cualquier servicio existente que desee hacer frente a una red para ejecutar, siempre y cuando ese servicio ya sea compatible con IPv6.

Todo el tráfico sobre Hyperboria está encriptado de extremo a extremo, deteniendo a los intrusos que operan nodos rogue. Cada nodo de la red recibe una dirección IPv6 única, que se deriva de la clave pública de ese nodo después de generar el par de claves público/privado. Esto elimina la necesidad de una configuración de cifrado adicional y crea un entorno con suficientes direcciones IP para una expansión sustancial de la red. A medida que la red crece en tamaño, la calidad del enrutamiento también mejora. Con nodos más activos, el número de rutas potenciales aumenta para mitigar el fallo (piense en “generales maliciosos”) y optimice la ruta más rápida desde el emisor al receptor.

En general, Cjdns no es anónimo, ni pretende serlo. Más bien, los usuarios usan pseudónimos para ocultar sus identidades. Para ocultar mejor su identidad, puede cambiar periódicamente los seudónimos para que no esté claro si las solicitudes provienen de una o varias fuentes.

Ventajas de la red de malla Hyperboria:

1. Es agnóstico hacia la forma en que el anfitrión se conecta a sus compañeros. Es decir, no importa mucho si el par con el que necesitamos conectarnos es a través de Internet o en un punto de acceso físico.
2. Se codifica de extremo a extremo, deteniendo a los intrusos que operan nodos rogue.
3. Cada nodo de la red recibe una dirección IPv6 única. Esto elimina la necesidad de una configuración de cifrado adicional y crea un entorno con suficientes direcciones IP para una amplia expansión de red.
4. Las direcciones IPv6 asignadas a los nodos no están relacionadas con su ubicación, lo que hace imposible conocer la ubicación física del nodo IP.
5. Alto poder de procesamiento.

Desventajas de la red de malla Hyperboria:

1. Los nodos comunicantes sólo conocen el IP del otro, no los de otros nodos con los que no están conectados directamente.
2. El tráfico se realiza a través de la ruta más corta, por lo que todos los nodos intermedios saben qué nodos se comunican pero no saben cuáles y dónde están.

El primer inconveniente puede ser evitado por lo siguiente:

1. Un nodo conectado a una red se comunica con túneles solamente con nodos de confianza, si existen.
2. El nodo intermedio propio de Hyperboria es creado, y el nodo está enlazado por el túnel al sistema. En lugar de su propio sitio, puede utilizar uno de confianza, si existe. Los usuarios de red pueden utilizar este método para conectarse a la red.

El segundo inconveniente puede reducirse alterando el identificador IPv6 y el par de claves de su propio nodo.

A pesar de estos inconvenientes, **Hyperboria es compatible para vincular los nodos de Ties.Network en una red, ya que permite a los usuarios mostrar su dirección IP real sólo a los nodos de confianza o a un nodo de confianza Hyperboria de terceros**. En otras palabras, el hecho de que cualquier tráfico en la red se cifre automáticamente hace innecesario conectar nodos a través de túneles directos. Al mismo tiempo, la velocidad de conexión sigue siendo alta, y la plataforma le da la seguridad para publicar direcciones de nodo IPv6 para conectar clientes y para equilibrar la carga.

Los usuarios que desean anonimato pueden beneficiarse de conectividad adicional a los nodos donde algunos de los nodos se publican como TOR Hidden Service y el acceso a ellos sólo se logra a través de TOR. Para mayor anonimato, puede utilizar TOR con la VPN. Por lo tanto, el anonimato de la plataforma se realiza colocándolo en Hyperboria, y la privacidad se proporciona mediante el cifrado obligatorio de todo el tráfico, independientemente de los servicios de superposición. Los clientes más exigentes pueden utilizar TOR + VPN para la conexión con nodos.

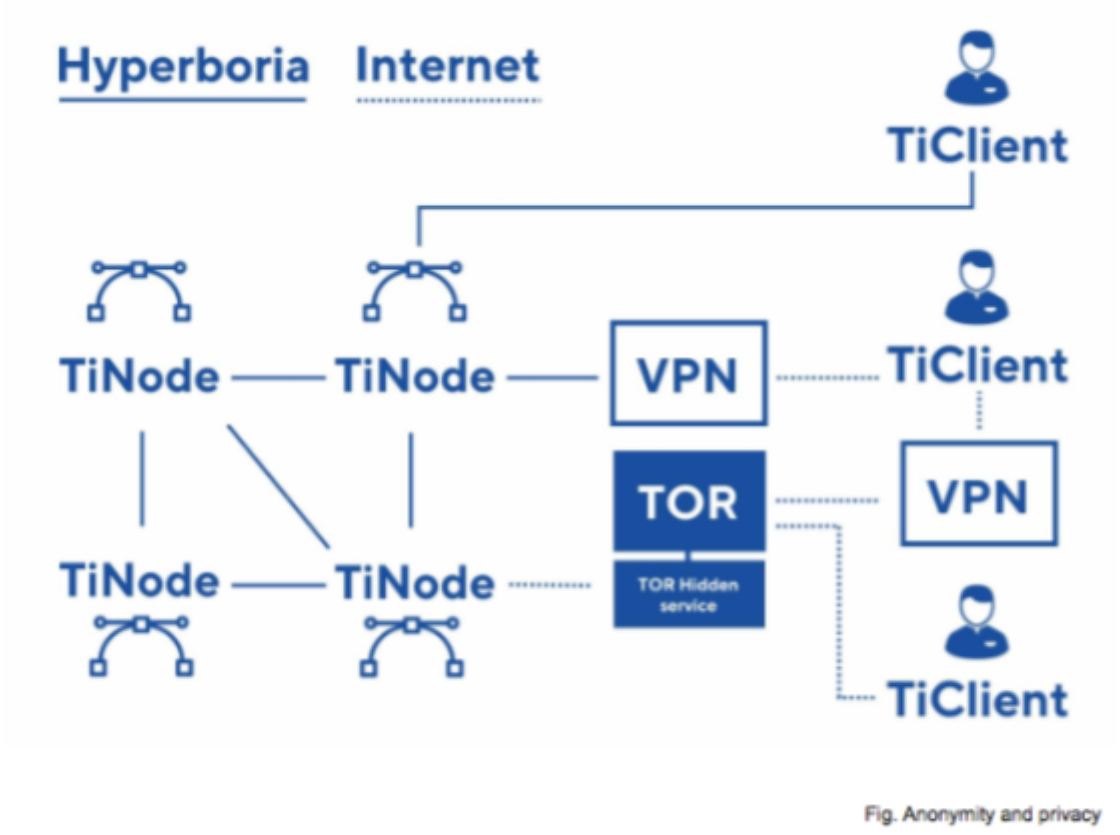

Fig. Anonymity and privacy

Fig. Anonimato y privacidad

4.6 Cliente

Los usuarios interactúan con el sistema utilizando el programa TiClient. El cliente suministra la interfaz de usuario, almacena las claves, interactúa con los nodos de cadena de bloqueo y de TiNode, así como con otros clientes a través de protocolos de chat.

4.7 Chats

Para resumir las cosas, una aplicación de software de chat es necesaria para la comunicación empresarial y una colaboración mejorada. En Ties.Network, se implementará un chat utilizando cifrado de extremo a extremo, como BitMessage, para conectar a los usuarios de la red.

4.8 Nodo y esquema de interacción del cliente

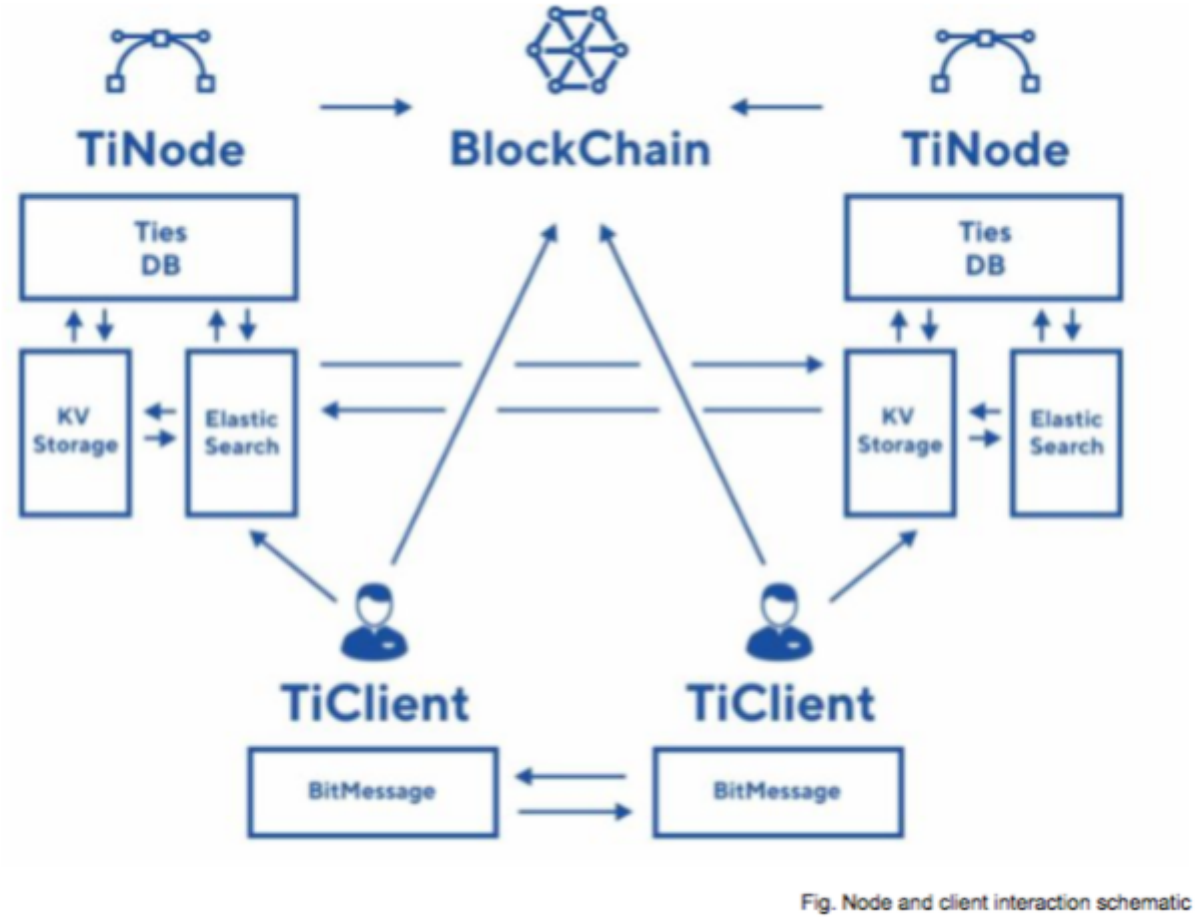

Fig. Nodo y esquema de interacción del cliente

4.9 Factores de determinación para las soluciones utilizadas

En este capítulo consideramos las tecnologías disponibles y justificamos nuestros esfuerzos para hacer un mejor acercamiento al almacenamiento descentralizado público de datos. Aunque no usamos las soluciones revisadas en este capítulo, las consideramos a fondo y las encontramos inadecuadas para ser utilizadas en Ties.Network. Aquí explicamos por qué.

4.9.1 Problema de los Generales Bizantinos

Las plataformas de código abierto engendran ciertos desafíos, el primero de los cuales es el llamado problema Bizantino (o "El problema de los Generales Bizantinos") [1]. Los sistemas informáticos fiables deben manejar componentes que funcionan incorrectamente y que dan información contradictoria a diferentes partes del sistema. Esta situación puede expresarse de manera abstracta en términos de un grupo de generales del ejército Bizantino acampado con sus tropas alrededor de una ciudad enemiga. Comunicándose sólo por mensajero, los generales deben ponerse de acuerdo sobre un plan de batalla

común. Sin embargo, uno o más de ellos pueden ser traidores que tratarán de confundir a los demás. El problema es encontrar un algoritmo para asegurar que los generales leales lleguen a un acuerdo.

El “Problema de los Generales Bizantinos”, también conocido como “fracasos Bizantinos”, se considera la clase más general y más difícil de los fracasos entre los modos de falla. El llamado modo de fallo-parada de falla ocupa el extremo más simple del espectro. Mientras que el modelo fallo-stop de falla simplemente significa que la única manera de fallar es un fallo de nodo, detectado por otros nodos, los fallos bizantinos no implican restricciones, lo que significa que el nodo fallido puede generar datos arbitrarios, pretendiendo ser correctos, haciendo difícil la tolerancia de fallo.

En este problema, varias facciones del ejército rodean un castillo que esperan saquear. Un general conduce cada facción y un general es el líder general. Sólo un ataque simultáneo garantiza la victoria. Además, dado que las facciones rodean el castillo, se dispersan, haciendo difícil el control centralizado. Los generales deben enviar mensajes entre las facciones para retransmitir el tiempo de ataque. Sin embargo, algunos generales son traidores y no obedecerán el comando o transmitirán el tiempo de ataque equivocado a los otros generales. Los generales no saben quién es leal y quién es un traidor y no hay forma de averiguarlo.

Problemas: ¿Cómo podemos asegurar un ataque coordinado para saquear el castillo?

Implicaciones

En un sistema distribuido, cualquier entrada (mensajes) al sistema (el tiempo acordado del ataque) debe ser de confianza. Las redes digitales suelen tener millones de miembros (los generales) que se dispersan a nivel mundial y puesto que no hay un mando centralizado (no hay gobierno central), es imposible para usted conocer a cada uno de los miembros. Entonces, ¿cómo puede usted confiar en los otros miembros de la red y asegurarse de que las entradas al libro mayor distribuido son exactas y que el libro mayor sí tiene la información correcta?

La arquitectura TiesDB resuelve este problema y regula un exitoso “ataque coordinado” proporcionando una red descentralizada y autónoma que asegura todas las transacciones entrantes y utiliza criptografía segura para mantener la confianza a pesar de la falta de gobierno central (ver 4.4.2 y siguientes).

4.9.2 Cadena de bloques como una base de datos

La cadena de bloques ya es un repositorio de datos distribuido. Entonces, ¿por qué no almacenar los datos directamente en la cadena de bloques?

Nuevas implementaciones de la cadena de bloques, como Ethereum, le permiten almacenar también contratos inteligentes, entre otros datos. Los contratos inteligentes permiten aplicaciones distribuidas (por ejemplo, dApps en Ethereum), que también almacenan información de usuario. Actualmente, la mayoría de las aplicaciones simples almacenan todos sus datos en cadena de bloques.

Sin embargo, la cadena de bloques como almacenamiento de datos tiene inconvenientes significativos:

1. **La cadena de bloques es inmutable.** Todo lo almacenado en la cadena de bloques permanece allí por siempre y no se puede quitar. Este es un grave inconveniente dado que la mayor parte de la información de la interacción de los usuarios es temporal y se puede eliminar más adelante. El almacenamiento eterno de información también funciona en contra del anonimato.
2. **La capacidad de datos es limitada.** Cada nodo es una réplica completa de otros nodos. Como resultado, una aplicación popular puede causar el rápido inflado de la cadena de bloques de

tamaño en todos los nodos simultáneamente. En algún momento, la cadena de bloques puede llegar a ser demasiado grande en tamaño y superar la capacidad de los discos duros producidos en masa. Si esto ocurre, necesitaría un equipo costoso que podría conducir a la centralización no deseada.

3. **Es lento.** El rendimiento de la cadena de bloques Ethereum, la cadena de bloques más lista para la producción en el mercado, es de sólo 15 TPS. No es absolutamente suficiente para una aplicación popular descentralizada.
4. **Almacenamiento de valores clave primario sin capacidad para realizar una búsqueda compleja dentro de los datos de los usuarios.**

Por lo tanto, las implementaciones actuales de cadenas de bloque tienen varias desventajas que hacen que su uso como almacenamiento de datos sea ineficaz. Son lentas (una docena de transacciones por segundo para una red total), tienen capacidad limitada debido a la excesiva replicación e inmutabilidad y son primitivas en funcionalidad (son simples bases de datos de valor-clave sin capacidad para realizar búsquedas complejas). Por lo tanto, la cadena de bloques no cumple con los requisitos para el almacenamiento de datos descentralizados que estamos buscando.

4.9.3 IPFS

IPFS [8] (Sistema de Archivo Interplanetario) es un sistema de archivos distribuido, basado en DHT [9] (Tabla Hash Distribuida) y el protocolo BitTorrent [10]. Utiliza el direccionamiento de contenido para combinar e integrar diferentes sistemas de archivos.

Ventajas:

1. Los dispositivos sólo almacenan los archivos necesarios.
2. No hay necesidad de confiar en (pares) peers, ya que el direccionamiento se realiza a través del hash de los contenidos.
3. IPFS proporciona resistencia a la 'inundación' (es decir, cargar archivos inútiles en la red) por pares (peers) descargar sólo los archivos necesarios.
4. Una alta tasa de transferencia (gracias a BitTorrent).

Desventajas:

1. IPFS sólo almacena archivos (datos no estructurados, sin búsqueda de contenido).
2. Un usuario solo puede salir de la red una vez que la distribución del archivo esté completa.
3. Otros participantes deben estar en línea para garantizar el almacenamiento de datos.
4. Los archivos son estáticos (es decir, no cambiables).
5. IPFS no elimina archivos.

Tanto las redes sociales basadas en IPFS, AKASHA (Ethereum + IPFS) [11] como la plataforma comercial OpenBazaar [12], tienen todas las desventajas del sistema IPFS, incluyendo las limitaciones de almacenamiento, y los usuarios sólo pueden salir de la red una vez que la distribución de archivos es completada. No encontramos IPFS adecuado para nuestro almacenamiento de datos y tenemos que encontrar una mejor solución.

4.9.4 Almacenamientos descentralizados de archivos en la nube

Estos repositorios le permiten combinar dispositivos individuales en un almacenamiento en una nube común, similar a Dropbox [13], pero con costos más bajos. Los propietarios de estos servicios (también llamados "agricultores"), proporcionan un lugar para almacenar los archivos de otras personas por un

cierto costo. Ellos usan pruebas criptográficas para medir ciertos datos como prueba de almacenamiento o prueba de recuperabilidad. Tanto el negociante como el 'granjero' usan la criptomoneda como medio para el negocio. Estos proyectos se crean principalmente con la tecnología DHT y el direccionamiento de contenidos. Algunos empresarios también usan cadena de bloques y contratos inteligentes.

Los protocolos de almacenamiento distribuido más prominentes son Sia [14], Storj [15], Ethereum Swarm [16], MaidSAFE [17]. Todos ellos están construidos con principios similares, mientras que Ethereum Swarm es una plataforma descentralizada para aplicaciones que también alberga dApps.

Ventajas:

1. Los archivos se almacenan en la nube y están disponibles si el propietario está en línea o no.
2. Transferencia alta de tasa.
3. Garantía de seguridad de almacenamiento y extracción de archivos.
4. Puede eliminar archivos no deseados.

Desventajas:

1. Almacenamiento sólo de archivos (datos no estructurados, sin búsqueda compleja).
2. Los archivos son estáticos.
3. El almacenamiento es una opción de pago.

Los repositorios de archivos distribuidos no son aptos, bien para almacenar la información dinámica estructurada (tal como datos del usuario de una red social) porque las capacidades de búsqueda de datos son muy limitadas. Por ejemplo, en dichos repositorios, no podemos buscar por palabra clave, por ubicación o por una publicación específica del usuario.

4.9.5 Información general de las bases de datos distribuidas

El teorema CAP [18] hace que sea imposible obtener la base de datos totalmente distribuida que garantice la coherencia, disponibilidad y tolerancia de partición.

En nuestro caso, necesitamos una base de datos distribuida resistente al particionamiento pero constantemente disponible (Disponibilidad + Tolerancia de Partición + Consistencia temporal), porque necesitamos recibir rápidamente una respuesta del sistema a petición. Esto limita nuestra selección de bases de datos cerca de noSQL, porque ACID [19] SQL DBMSs principalmente proporcionan consistencia.

Hay muchas implementaciones de bases de datos distribuidas noSQL como MongoDB [20], Cassandra [21], RethinkDB [22] que son fáciles de usar y configurar en un clúster con replicación y sharding. Las réplicas son incompletas, es decir, implican sharding, que es un tipo de partición de base de datos que separa bases de datos muy grandes en partes de datos más pequeñas, más rápidas y más fáciles de manejar.

El cliente trabaja con una de las réplicas, y los datos se sincronizan automáticamente con los demás. Para el balanceo de carga, se puede usar sharding cuando parte de los datos se almacena sólo en parte de las réplicas. La adición de una nueva réplica al cluster aumenta la escala del clúster y algunas implementaciones (por ejemplo, Cassandra) permiten que la réplica controle automáticamente parte del trabajo del clúster.

Las bases de datos de noSQL proporcionan “consistencia temporal”, es decir, el sistema es

consistente. Si no se realizan actualizaciones a un elemento de datos dado durante un período de tiempo “suficiente”, entonces, eventualmente, todas las lecturas de ese elemento devolverán el mismo valor consistente.

Las bases de datos NoSQL pueden almacenar un valor-clave simple y mantener la estructura interna del valor, así como índices adicionales. Los más avanzados también tienen soporte para transacciones básicas y un lenguaje de consulta similar al SQL (por ejemplo, Cassandra).

En todo lo anterior, esta clase de base de datos puede parecer ideal para su uso en una cadena de bloques. Pero si se agrega una réplica malintencionada a dicho clúster, que empieza a decir a otras réplicas del clúster que todos los datos deben eliminarse, el resultado será la eliminación dócil de los datos con las réplicas restantes y la corrupción de la base de datos. Por lo tanto, el trabajo coordinado de réplicas es ahora posible sólo en un entorno de confianza (un grupo de bases de datos no es estable al problema de los generales bizantinos). Si una réplica de trabajo malicioso se coloca en un clúster, puede causar la destrucción de todos los datos del clúster.

Ventajas:

1. Alta velocidad
2. Velocidad lineal y tamaño del almacenaje escalado
3. Resistencia a la indisponibilidad de ciertas réplicas

Desventajas:

1. Factor de confianza - vulnerabilidad al Problema de los Generales Bizantinos**.**

Por lo tanto, las bases de datos distribuidas tienen la única desventaja pero siguen siendo la esencial. Por lo tanto no pueden ser utilizados en el sistema descentralizado sin modificación.

Tenga en cuenta que TiesDB trae Tolerancia de Prueba Bizantina a la base de datos noSQL (ver 4.4.2 y adelante). Debido a la organización de datos especiales y el mecanismo de incentivos Ties.Network no necesita un procedimiento de consenso, donde los nodos de la red comparten información sobre las transacciones candidato, porque la firma cifrada del usuario protege la información. Es decir, los nodos dañinos no pueden borrar y cambiar datos en otros nodos sin mostrar un impacto notable.

4.9.6 BigChainDB

La implementación de la cadena de bloques, llamada BigChainDB [23], o IPDB (Base de datos interplanetaria) reclama una potente velocidad de transacción (1 millón por segundo) y una enorme capacidad de almacenamiento (debido al almacenamiento distribuido con replicación parcial). BigChainDB obtiene estos beneficios a través de comenzar con una gran base de datos de datos distribuidos y luego agregar las características cadena de bloques - control descentralizado, inmutabilidad y la transferencia de activos digitales.

Por desgracia, la arquitectura de BigChainDB es fundamentalmente defectuosa, en que cada nodo tiene todos los derechos para escribir en el almacenamiento de datos común, lo que significa que su sistema es vulnerable al problema de los Generales Bizantinos. En otras palabras, todos los nodos BigchainDB se conectan a un único clúster RethinkDB. Si algo malo le sucede a ese clúster de RethinkDB, todos los demás nodos de esa cadena de bloque caen porque carecen de un almacenamiento independiente. Los autores de este proyecto lo conocen, prometiendo reflexionar sobre esto más adelante [24]. Sin embargo, la fijación de los defectos fundamentales en la arquitectura subyacente después de la liberación del producto es muy laboriosa y a menudo imposible, ya que esto puede conducir a un producto significativamente diferente con una arquitectura diferente. Una aproximación tan fácil al problema

fundamental provoca críticas de la comunidad del proyecto [25], ya que las características de alta velocidad y masa de BigChainDB, demostradas en ausencia de BFT (tolerancia a fallas bizantinas), son en realidad las demostradas por el RethinkDB y MongoDB Bases de datos utilizadas para el almacenamiento de datos. Pero ya que todavía necesita confianza completa entre los nodos, ¿por qué no utilizar las bases de datos especificadas directamente?

Nuestro resumen del BigChainDB es el siguiente:

Ventajas:

1. La velocidad y el almacenamiento son comparables a las bases de datos distribuidas noSql.

Desventajas:

1. BigChainDB es una base de datos ordinaria noSql que además tiene todos los inconvenientes de cadena de bloques.
2. Permanencia (los datos no pueden ser eliminados legalmente, pero pueden ser eliminados maliciosamente).
3. Susceptible al problema de los Generales Bizantinos, por lo tanto no se puede utilizar en una red pública.

Por estas y otras razones, hemos concluido que BigChainDB no es adecuado para almacenamiento de datos para Ties.Network.

4.9.7 Conclusión

Tras realizar un análisis exhaustivo de las soluciones de almacenamiento existentes, concluimos que ninguna solución actual satisface las altas exigencias de las aplicaciones descentralizadas emergentes. Lo que necesitan es una base de datos pública descentralizada. Es por eso que enfocamos nuestros esfuerzos en el desarrollo de TiesDB, que puede ser de utilidad no sólo para Ties.Network, sino también para impulsar el desarrollo de otras aplicaciones descentralizadas ricas en características en cadena de bloques Ethereum.

5. Autoorganización y motivación

5.1 Fuentes de ingresos de la plataforma

Los beneficios provienen de las siguientes fuentes:

- Publicidad
- Impuesto de depósito
- Cambio de moneda

Los ingresos de los nodos provienen de las siguientes fuentes:

- Colocación de contenido en el servidor de nodo
- Recuperación de contenido desde el servidor de nodo

Los usuarios deben pagar por almacenar sus datos en los servidores de base de datos. Eso permite que la red se sostenga haciendo rentable su apoyo. También evita que se inunde la red con basura o datos maliciosos. Pero este modelo de redes no es muy popular en este momento.

Por ejemplo, Jim (persona hipotética) se inscribe en Ties.Network. Antes de que pueda hacer algo, tiene que depositar un depósito en una 'chequera'. Ese es su registro pagado. Para las redes sociales ordinarias, donde los usuarios simplemente se divierten, tal paso significaría el fin de nuestra red - ¿por qué pagar algo que puedes conseguir gratis en otro sitio? *Dado que Ties.Network es diferente en que te gana dinero, nos sentimos justificados en pedir un pago inicial y comisiones por la línea para ayudarnos a continuar ofreciendo este servicio.*

A diferencia de los competidores centralizados que obtienen sus ingresos de la publicidad o de usar modelos freemium, Ties.Network pertenece a la comunidad, por lo que sus ingresos deben ser gastados en su desarrollo y mantenimiento. Una de las formas en que se utilizarán los ingresos será para pagar a los moderadores y para el mantenimiento de la plataforma. Así, el beneficio del proyecto se distribuirá para pagar a las personas clave que apoyan el proyecto. Estos son:

- Moderador de contenido (que tiene autoridad para eliminar contenido y prohibir usuarios).
- “Super moderador” (que investiga la colusión entre nodos y participantes, administra el presupuesto y rechaza o despide a los participantes).
- Moderadores (que arbitran disputas).
- Posiciones técnicas que incluyen Desarrolladores (que desarrollan software para Ties.Network).
- Usuarios comunes (que cubren los gastos justos de los usuarios).

La plataforma cubrirá los gastos de los usuarios de su uso justo de la plataforma haciéndolo finalmente libre de usar. La equidad del uso de la plataforma será observada por el presupuesto Super-moderadores.

5.2 Funciones de la plataforma

Funciones sociales:

- Moderador de contenido (a los individuos se les da autoridad especial para hacer cumplir las reglas

de la plataforma y para regular, eliminar o prohibir contenido)
- Super moderador de defensa del presupuesto (este moderador investiga la colusión entre nodos y usuarios, prohibiendo nodos y usuarios si es necesario) Jueces (Solución de disputas entre usuarios)
- Los jueces (solucionan las disputas entre usuarios)
- Usuarios ordinarios

Función técnica:

- Desarrollador (desarrolla software para Ties.Network)

5.3 Sistema de referencia

Proponemos un sistema de referencia para motivar a los individuos a unirse a Ties.Network y afiliarse a la inversión inicial. Un miembro ya registrado de la red invita a otro participante a través de un canal alternativo, dándoles un código de invitación especial. Un nuevo participante entra con este código, mientras que una parte del dinero del invitador se transfiere inmediatamente al depósito, es decir, un nuevo usuario puede comenzar a usar el sistema inmediatamente, sin ninguna inversión inicial. Al final del período de presentación de informes, el costo de las invitaciones y el pago del almacenamiento de datos puede compensarse con el beneficio del proyecto. Para que este sistema funcione, el presupuesto es gestionado por los super-moderadores de la defensa presupuestaria que sólo deben utilizar las monedas reservadas para este fin.

6. Fichas TIE

Las fichas TIE son la moneda digital utilizada por los miembros en la plataforma Ties.Network.

6.1 Operaciones con las fichas TIE

1. La compra y venta de fichas se realiza a través del intercambio interno de plataforma o mediante un intercambio exterior que enumera las fichas TIE.
2. En el registro, el usuario envía una tarifa de participación al sistema, que luego se devuelve del presupuesto de la plataforma.
3. Todas las transacciones realizadas a través de la plataforma se pagan con fichas TIE (que pueden convertirse en otras criptomonedas (por ejemplo, BTC, ETH o Ripple) y en moneda fiduciaria).

7. Conclusión

En este documento se revisó la propuesta de Ties.Network, una plataforma para las transacciones de negocios y redes sociales. La plataforma es un sistema distribuido públicamente de servidores auto-motivados que sirven a un propósito común. El documento también describe la arquitectura y las interfaces clave de TiesDB. Estos incluyen: que es una base de datos noSql distribuida públicamente con una velocidad de procesamiento poderosa, que soporta un índice secundario y capacidad de búsqueda de texto completo, y que puede ser utilizado en conjunto con cualquier bloque de cadenas que soporte contratos inteligentes.

8. Referencias

1. Leslie Lamport, Robert Shostak, and Marshall Pease. El Problema de los Generales Bizantinos. Transacciones ACM en Lenguajes y Sistemas de Programación (TOPLAS), 4(3):382–401, Julio 1982. http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf.
2. https://ethereum.org/
3. https://www.rchain.coop
4. https://www.torproject.org/
5. https://geti2p.net/
6. https://hyperboria.net/
7. https://github.com/cjdelisle/cjdns
8. https://ipfs.io/
9. https://en.wikipedia.org/wiki/Distributed_hash_table
10. https://en.wikipedia.org/wiki/BitTorrent
11. https://akasha.world/
12. https://openbazaar.org/
13. https://www.dropbox.com/
14. http://sia.tech/
15. https://storj.io/
16. https://github.com/ethersphere/swarm
17. https://maidsafe.net/
18. https://en.wikipedia.org/wiki/CAP_theorem
19. https://en.wikipedia.org/wiki/ACID
20. https://www.mongodb.com/
21. http://cassandra.apache.org/
22. https://www.rethinkdb.com/
23. https://www.bigchaindb.com/
24. https://docs.bigchaindb.com/en/latest/bft.html y https://github.com/bigchaindb/bigchaindb/issues/293
25. https://reddit.com/r/Bitcoin/comments/4j7wjf/bigchaindb_a_prime_example_of_blockchain_bullshit/
26. viktor trón et al. “Swap, swear and swindle incentive system for swarm”, http://swarm-gateways.net/bzz:/theswarm.eth/ethersphere/orange-papers/1/sw%5E3.pdf
27. http://www.elassandra.io/
28. https://www.elastic.co/products/elasticsearch