SISTEMAS DE INFORMACIÓN DE GESTIÓN Y BUSINESS INTELLIGENCE
ENRIQUE LÓPEZ GONZÁLEZ

Cuaderno de campo

—

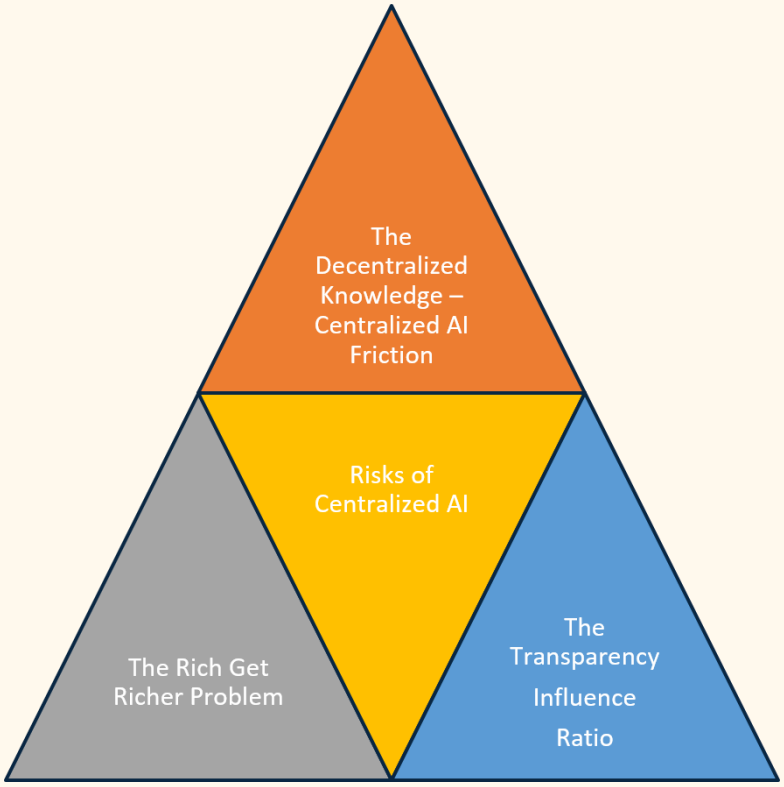
Adolfo Jiménez Prieto

Decentralized AI

La descentralización se ha convertido últimamente en un tema muy importante, ya que es un sistema autónomo que no es controlado ni depende de ningún ente. Pues bien, si sumamos las oportunidades que nos brinda la tecnología Blockchain y el potencial que tiene la inteligencia artificial obtenemos lo que a día de hoy es una de las tendencias tecnológicas que más se espere que prospere a lo largo de los años, la inteligencia artificial descentralizada.

Vamos a poner en contexto algunas dudas que se tienen acerca de este tema.

A. ¿Cuáles son los riesgos de las soluciones de IA centralizadas?
B. ¿Cuáles son los obstáculos para descentralizar la IA?
C. ¿Cuáles son los movimientos tecnológicos que permitirán la descentralización de la IA?
D. ¿Cuáles son algunas de las principales compañías pioneras en soluciones descentralizadas de inteligencia artificial hoy en día?



Riesgos IA centralizada.

Las soluciones de IA están completamente centralizadas. Desde el entrenamiento hasta la implementación y la optimización, los sistemas de IA dependen de autoridades centralizadas que controlan los datos y recursos necesarios para implementar una solución de inteligencia artificial **específica**.

Los ricos se vuelven más ricos: La IA centralizada es principalmente un privilegio de las grandes compañías que poseen un conjunto de datos ricos. Estas compañías pueden contratar equipos de ciencia de datos que desarrollan modelos que producen más datos que enriquecen los conjuntos de datos de la compañía.

Transparencia e influencia: Los sistemas de inteligencia artificial centralizados influyen en una relación del nivel de influencia que las grandes organizaciones tienen sobre sus clientes / usuarios y sus niveles de transparencia. Estas grandes compañías poseen muchos datos acerca de las personas sin ninguna obligación de ser transparentes acerca de su conocimiento. Véase el nivel de influencia que las campañas políticas lanzadas por diversas compañías pueden tener en el resultado de la elección.

Desafíos

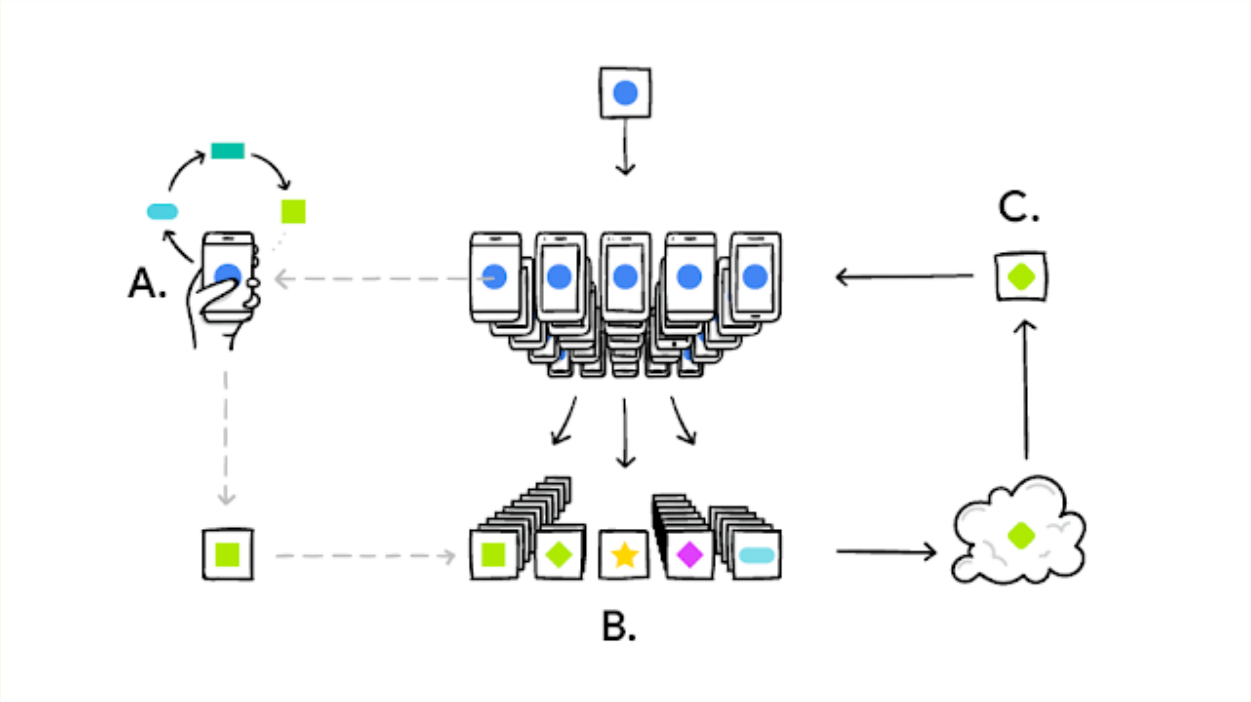
Más allá de las barreras tecnológicas, los expertos en el tema creen que existen cuatro desafíos clave que deben resolverse para hacer la IA descentralizada una realidad.

- **El problema de la privacidad:** ¿Pueden las entidades entrenar un modelo sin tener que revelar sus datos?
- **El problema de la autonomía:** ¿Pueden los modelos ser distribuidos y ejecutados autónomamente a través de cientos de miles de nodos?
- **El problema de la transparencia:** ¿Pueden la actividad y el comportamiento de un modelo IA estar disponible transparentemente para todas las partes sin la necesidad de confiar en una autoridad central?
- **El problema económico:** ¿Pueden las terceras partes estar correctamente incentivadas a contribuir al conocimiento y calidad de un modelo IA?

Tecnologías para la descentralización de la IA

- **Ledgers distribuidos y contratos inteligentes:** se están convirtiendo en el modelo preferido de tiempo de ejecución y programación, respectivamente, para las soluciones descentralizadas de inteligencia artificial.
- **Aprendizaje federado:** el aprendizaje federado proporciona un método eficaz para distribuir el proceso de creación de conocimiento colectivo a través de una red de nodos. Los programas tradicionales de aprendizaje automático se basaban en un modelo centralizado de capacitación en el que un grupo de servidores ejecutaba un modelo específico contra los conjuntos de datos de capacitación y validación. Ese enfoque de capacitación centralizada puede funcionar de manera muy eficiente en muchos escenarios, pero también ha demostrado ser un desafío en los casos de uso que involucran un gran número de puntos finales que usan y mejoran el modelo. El aprendizaje federado fue inicialmente propuesto por investigadores de Google en un documento publicado el año pasado.

    - Google describe el enfoque del aprendizaje federado en cuatro simples pasos:
        1. Se selecciona un subconjunto de clientes existentes, cada uno de los cuales descarga el modelo actual.
        2. Cada cliente en el subconjunto calcula un modelo actualizado basado en sus datos locales.
        3. Las actualizaciones del modelo se envían desde los clientes seleccionados al servidor.
        4. El servidor agrega estos modelos (generalmente promediando) para construir un modelo global mejorado.
- El claro beneficio del aprendizaje federado es distribuir la calidad del conocimiento en una gran cantidad de dispositivos sin necesariamente centralizar los datos utilizados para optimizar y capacitar al modelo. Ese enfoque también permite mejorar la calidad de los modelos centralizados de aprendizaje automático al tiempo que se mantiene la privacidad de los conjuntos de datos de capacitación.



- **Cifrado homomórfico:** permite la ejecución de operaciones matemáticas (como modelos de aprendizaje automático) en conjuntos de datos encriptados. El cifrado homomórfico permitirá que los nodos en la arquitectura descentralizada de IA ejecuten modelos sobre conjuntos de datos encriptados sin tener que descifrar los datos. Matemáticamente, el homomorfismo se define como "un mapeo de un conjunto matemático (como un grupo, anillo o espacio vectorial) en o en otro conjunto o en sí mismo de tal manera que el resultado obtenido al aplicar las operaciones a los elementos del primer conjunto se mapea en el resultado obtenido aplicando las operaciones correspondientes a sus respectivas imágenes en el segundo conjunto".
    - **Cifrado homomórfico parcial (PHE)**
    - **Cifrado completamente homomórfico (FHE)**
- **Criptografía Neural Adversarial:** es una técnica inteligente para permitir comunicaciones seguras entre diferentes partes de una manera que puede ser resistente a casi cualquier conexión. La criptografía GAN permitirá a los nodos en una red descentralizada intercambiar información de forma segura sin tener que confiar en esquemas de cifrado predefinidos.La criptografía GAN fue iniciada por Google en un documento de investigación de 2016 bajo el título "Aprender a proteger las

comunicaciones con la criptografía neuronal adversa". El documento propone un método en el que las redes neuronales pueden descubrir dinámicamente nuevas formas de cifrado y descifrado para proteger los canales de comunicación de los adversarios que intentan romper los esquemas de seguridad.

- **Computación multipartita segura:** proporciona una alternativa más económica al cifrado homomórfico que permite a las diferentes partes expresar afirmaciones sobre un conjunto de datos que se puede verificar matemáticamente sin tener acceso al conjunto de datos subyacente.

Plataformas que hacen uso de la IA descentralizada

- SingularityNet: es un protocolo de código abierto y una colección de contratos inteligentes para un mercado descentralizado de servicios coordinados de inteligencia artificial. Conceptualmente, SingularityNET actúa como un mercado descentralizado y de uso general que proporciona una cartera de agentes AI que se pueden usar a cambio de criptomonedas.
- Cerebrum: es una plataforma descentralizada para el aprendizaje automático de crowdsourcing. Cerebrum permite a cualquier persona encriptar sus datos y competir en el aprendizaje de máquina de host para utilizar modelos de aprendizaje automático de fuentes múltiples.
- OpenMined: es una comunidad centrada en la construcción de tecnología de código abierto para la propiedad descentralizada de datos e inteligencia.
- Ocean Protocol: es un protocolo de intercambio de datos descentralizado que permite a las personas compartir y monetizar datos al tiempo que garantiza el control, auditabilidad, transparencia y cumplimiento a todos los actores involucrados. Su red maneja el almacenamiento de los metadatos (es decir, a quién pertenece qué), enlaces a los datos en sí, y más.

Convergencia de AI y Blockchain

El uso conjunto de las AI y Blockchain puede ser capaz de rediseñar todo el paradigma tecnológico (y humano) desde cero. Estas dos tecnologías se apoyan mutuamente de forma bidireccional, es decir, tanto Blockchain puede cambiar gracias a AI como AI puede cambiar gracias a Blockchain.

Cómo AI puede cambiar Blockchain

Un blockchain también tiene sus propias limitaciones. Algunas de ellas están relacionadas con la tecnología, mientras que otros provienen de la antigua cultura heredada del sector de servicios financieros, pero todos ellos pueden verse afectados por la IA de una manera u otra.

- **Consumo de energía:** la minería es una tarea increíblemente difícil que requiere una tonelada de energía para completarse. La IA ya ha demostrado ser muy eficiente en la optimización del consumo de energía , por lo que también se pueden lograr resultados similares para la cadena de bloques.
- **Escalabilidad:** la cadena de bloques está creciendo a un ritmo constante de 1 MB cada 10 minutos y ya suma 85 GB. AI puede introducir nuevos sistemas de aprendizaje descentralizado, como el **aprendizaje federado**. por ejemplo, o nuevas técnicas de fragmentación de datos para hacer que el sistema sea más eficiente.
- **Seguridad:** incluso si la cadena de bloques es casi imposible de hackear, sus capas y aplicaciones adicionales no son tan seguras (por ejemplo, DAO, Mt Gox, Bitfinex, etc.). El increíble progreso realizado por el aprendizaje automático en los últimos dos años hace de AI un aliado fantástico para que blockchain garantice un despliegue seguro de las aplicaciones, especialmente dada la estructura fija del sistema.
- **Privacidad:** el problema de privacidad de la propiedad de datos personales plantea preocupaciones normativas y estratégicas para obtener ventajas competitivas. El cifrado homomórfico (realizar operaciones directamente en datos encriptados), podría ser una de las soluciones.
- **Eficiencia:** Un sistema inteligente podría eventualmente ser capaz de calcular sobre la marcha la posibilidad de que nodos específicos sean los primeros en realizar una determinada tarea, dando la posibilidad a otros mineros de cerrar sus esfuerzos para esa transacción específica y reducir los costos totales. Además, incluso si existen algunas restricciones estructurales, una mejor eficiencia y un menor consumo de energía pueden reducir la latencia de la red permitiendo transacciones más rápidas.
- **Hardware:** los mineros vertieron una cantidad increíble de dinero en componentes de hardware especializados. Dado que el consumo de energía siempre ha sido un tema clave, se han propuesto muchas soluciones y se introducirán muchas más en el futuro. Tan pronto como el sistema se vuelva más eficiente, un poco de hardware podría convertirse (a veces parcialmente) para el uso de redes neuronales
- **Puertas de datos:** en un futuro donde todos nuestros datos estarán disponibles en una cadena de bloques y las compañías podrán comprarlos directamente a nosotros, necesitaremos ayuda para otorgar acceso, rastrear el uso de datos y, en general, dar

sentido a lo que le sucede a nuestro personal. Información a una velocidad informática. Este es un trabajo para máquinas (inteligentes).

Cómo Blockchain puede cambiar la IA

¿Qué impacto tendría la cadena de bloques en el desarrollo de los sistemas de aprendizaje automático? Más en detalles, blockchain podría:

- **Ayuda a AI a explicarse:** la caja negra de AI sufre un problema de explicabilidad. Tener una pista de auditoría clara no solo puede mejorar la confiabilidad de los datos así como de los modelos, sino que también proporciona una ruta clara para rastrear el proceso de decisión de la máquina.
- **Aumento de la efectividad de la inteligencia artificial:** un intercambio seguro de datos significa más datos (y más datos de capacitación), y luego mejores modelos, mejores acciones, mejores resultados ... y mejores datos nuevos. El efecto de red es todo lo que importa al final del día.
- **Bajar las barreras de entrada al mercado:** Las tecnologías de blockchain pueden asegurar sus datos. En primer lugar, blockchain fomentará la creación de datos personales más limpios y organizados . En segundo lugar, permitirá el surgimiento de nuevos mercados : un mercado de datos (fruta de bajo rendimiento); un mercado de modelos (mucho más interesante); y, finalmente, incluso un mercado de inteligencia artificial(SingularityNET). Por lo tanto, el intercambio sencillo de datos y los nuevos mercados, junto con la verificación de datos de blockchain, proporcionarán una integración más fluida que reduce la barrera de entrada para los jugadores más pequeños y reduce la ventaja competitiva de los gigantes de la tecnología. En realidad estamos resolviendo dos problemas, es decir, brindando un acceso más amplio a los datos y un mecanismo de monetización de datos más eficiente.
- **Aumente la confianza artificial:** tan pronto como una parte de nuestras tareas sea gestionada por agentes virtuales autónomos, tener una pista de auditoría clara ayudará a los robots a confiar entre sí (y nosotros también a confiar en ellos). También aumentará eventualmente cada interacción máquina-a-máquina y la transacción, proporcionando una forma segura de compartir datos y decisiones coordinadas, así como un mecanismo robusto para alcanzar un quórum (extremadamente relevante para robótica de enjambres y agentes múltiples). escenarios).

- **<u>Reducir el escenario de riesgos catastróficos:</u>** una IA codificada en un DAO(Organización Autónoma Descentralizada) con contratos inteligentes específicos sólo podrá realizar esas acciones, y nada más (tendrá entonces un espacio de acción limitado).

Blockchain y AI son las dos partes extremas del espectro tecnológico: una que fomenta la inteligencia centralizada en plataformas de datos cercanas y la otra que promueve aplicaciones descentralizadas en un entorno de datos abiertos. Sin embargo, si encontramos una forma inteligente de hacer que trabajen juntos, las externalidades positivas totales podrían amplificarse en un abrir y cerrar de ojos.

Ocean Protocol: Technical Whitepaper

Este paper presenta el protocolo Ocean. Ocean es una red y protocolo descentralizado de inteligencia artificial de datos y servicios. Incentiva una gran cantidad de datos/servicios relevantes de AI. La red ayuda a impulsar los mercados de datos / servicios de inteligencia artificial, así como los datos de los bienes públicos.

Introducción.

La sociedad moderna funciona con datos. La inteligencia artificial extrae valores de esos datos. Más datos significa unos modelos AI más precisos, que a su vez significa más beneficios para a sociedad y los negocios. Los mayores beneficiarios son las empresas que tienen tanto datos y experiencia interna en inteligencia artificial como Google y Facebook. En contraste, AI startups tienen increíbles algoritmos pero les faltan datos. Y por último las típicas empresas se ahogan en datos pero tienen menos pericia en IA. El poder de los datos y la inteligencia artificial y por lo tanto la sociedad, está en manos de pocos.

El objetivo de Ocean es igualar la oportunidad de acceder a los datos para que una gama mucho más amplia de profesionales puedan crear valor a partir de esos datos, y a su vez, difundir el poder de los datos. También es importante respetar las necesidades de privacidad, lo que implica que se debe incluir un proceso de preservación de la privacidad.

Para reducir esto a un objetivo práctico, nuestro objetivo es desarrollar un protocolo y una red - un ecosistema tokenizado - que incentiva la puesta a disposición de datos y servicios IA. Esta red puede ser utilizada para impulsar un nuevo ecosistema de mercados de datos, y más ampliamente, compartir datos por el bien público.

El objetivo principal es **cómo incentivar un gran suministro de datos y servicios de IA** relevantes. Esto no es fácil, ya que hay varios retos:

- ¿Como sabemos(o la red) qué es relevante? ¿Podemos incluso juzgar esto de manera determinista o necesitamos algún otro medio?
- Queremos incentivar no solo los datos de precios relevantes, sino también los bienes comunes relevantes. Lo último es más difícil porque es libre por su naturaleza.

- ¿Cómo incluimos/incentivamos no solo los datos, sino también los servicios informáticos de AI? ¿Cómo podemos asegurarnos de que puedan tener en cuenta la privacidad? ¿Cómo incluimos proveedores de servicio de cómputo descentralizado? ¿Cómo garantizamos que el servicio fue realmente proporcionado?
- ¿Cómo podríamos incentivar para que los actores incorporen nuevos actores al sistema y compartan información sobre los activos de datos relevantes?
- ¿Cuales son los vectores de ataque y cómo los abordamos? Por ejemplo, el spamming de datos de baja calidad para obtener muchas recompensas ó "escape de datos" donde un actor publica los datos que posee un titular de derechos diferente.

La red Ocean está compuesta por activos y por servicios de datos. Los activos están en forma de datos y algoritmos. Los servicios son el procesamiento y la persistencia que aprovechan los activos. Los activos y servicios son los productos básicos disponibles para el consumo a través de la red, y son similares a los que se encuentran en cualquier ecosistema de datos maduro.

Ocean tiene fuertes incentivos para enviar, referir y poner a disposición(de manera comprobable) datos y servicios de AI de calidad, a través de una nueva técnica que llaman Proofed Curation Market(CPM). Un CPM tiene dos partes: la popularidad predicha de un conjunto de datos/servicios , y su popularidad real:

1. **Prueba criptográfica:** La popularidad real es el conteo de la cantidad de veces que el conjunto de datos / servicio se entrega o se pone a disposición. Para evitar ser juzgado, debe hacerse disponible de forma demostrable utilizando una prueba criptográfica.
2. **Curation Market:** Esto es para la popularidad predicha. La gente sabe mucho mejor que los diseñadores de Ocean si un conjunto de datos/servicio dado es relevante; así que aprovechamos la multitud a través de un entorno de mercado de curación. Se puede pensar en este mercado en dar reputación a los datos / servicios donde el los actores participan para comprar en ese conjunto de datos/servicio. Cuanto antes se apueste o apueste un actor en un conjunto de datos / servicio determinado, más acciones obtendrán por la cantidad apostada y, a su vez, mayor será la recompensa.

Solo las partes interesadas que puedan proporcionar datos / servicios de alta calidad podrán obtener recompensas. Las recompensas en bloque para un conjunto de datos / servicio dado se distribuyen según la cantidad de participación en ese conjunto de datos / servicio y su popularidad. En otras palabras, los CPM instancian los objetivos de verificación y viralidad.

Por lo que sabemos, Ocean es el primer sistema que incentiva explícitamente a las personas a compartir sus datos / servicios, independientemente de si son gratuitos o tienen un precio.

Quien apuesta a los datos / servicios más populares (y los pone a disposición) gana la mayor cantidad de recompensas.

Los tokens de Ocean son los tokens principales de la red, la unidad para servicios de compra / venta y para recompensas en bloque. Denotamos Ocean Tokens como "Ọ". También necesitamos Ocean Tokens para medir la participación en cada conjunto de datos / servicio dado.

Para ello, utilizamos “Drops”. Los “Drops” son tokens derivativos de Ocean Tokens indicados en "Ḍ". Por ejemplo, 100 drops de participación en el conjunto de datos X es “100 Ḍ X”. Los drops se relacionan con Ocean Tokens a través de las curvas de unión de los Curation Market(CPM).

Casos de Uso

1. Datos propietarios: Vehículos autónomos.

La corporación RAND calculó que se necesitan de 500 mil millones a 1 billón de millas para obtener modelos AI con la precisión suficiente para el despliegue de producción de automóviles automáticos. Los colaboradores de Ocean en el Toyota Research Institute (TRI) vieron que sería prohibitivamente costoso para cada fabricante de automóviles generar esa cantidad de datos por su cuenta. ¿Por qué no agrupar los datos a través de un mercado de datos? Con ellos, construimos tal prototipo [BigchainDB2017].

Entonces, el desafío es que un solo mercado de datos puede estar centralizado: llegamos a otro silo de datos. Necesitamos un sustrato que permita que surjan muchos mercados de datos. Este es un objetivo clave del Ocean Protocol. Surgen nuevos beneficios críticos: mayor liquidez para cada mercado, y se incentiva directamente a las organizaciones a agrupar datos en lugar de agruparlos. Los datos de entrenamiento de automóviles que conducen por sí mismos ilustran cómo no todos los datos son fungibles: una milla conducida en una ventisca vale más que una milla conducida en una carretera vacía y soleada del desierto. Pero una milla en la ventisca es fungible con otras millas en ventiscas. El sistema debe tener en cuenta los datos fungibles y no fungibles.

2. Datos regulados: Investigación médica

Este es un caso de uso líder para datos que deben cumplir con las regulaciones de protección de datos en apoyo de la privacidad; y, por lo tanto, necesitará servicios informáticos de IA que preserven la privacidad.

DEX PTE. Ltd. ("DEX") está trabajando con ConnectedLife [ConnectedLife2018], Investigadores Médicos del Instituto Nacional de Neurociencia de Singapur, Especialistas Profesionales y Grupos de Hospitales en Singapur, Alemania, y en otros lugares, para una medición objetiva de los síntomas de Enfermedad de Parkinson. El objetivo es crear modelos específicos y específicos para cada sujeto basados en datos de sensores free-living y biomédicos para pacientes.

Sin embargo, las leyes éticas y nacionales de protección de datos personales evitan que los datos de pacientes se copien y compartan sin una transformación considerable del lugar de toma de datos y, por lo tanto, eliminan gran parte del valor y el impacto potencial en términos de las aplicaciones basadas en datos de pacientes. Un mercado de datos facilita la conexión de los proveedores de datos; y debe ser descentralizado para evitar el problema del silo. Esto nos proporciona un excelente caso de uso para el cálculo de preservación de la privacidad.

3. Global Data Commons

Nuestra visión es hacer crecer un conjunto masivo de activos de datos, todo gratis. Por ejemplo, ImageNet es un conjunto de datos abierto con más de 10 millones de imágenes etiquetadas, mucho más grande que los conjuntos de datos de imagen abiertos anteriores. Ha permitido a los investigadores de AI entrenar clasificadores de imágenes con menos errores radicales que antes, para docenas de aplicaciones de visión artificial. Hay otros proyectos de datos abiertos; desafortunadamente, cada uno está aislado con poco incentivo para crear datos / información más actuales y valiosos y compartirlos entre ellos. El hecho de incentivar directamente el intercambio de datos puede solucionar esto.

Stakeholders

La comprensión de las partes interesadas de la red es un precursor del diseño del sistema. En la siguiente tabla se resumen los accionistas que participan en la red. Hay partes interesadas más allá, desde desarrolladores hasta auditores, pero eso está fuera del alcance de este documento.

Stakeholder	***¿Qué valor pueden proporcionar?***	***¿Que pueden obtener a cambio?***
Proveedor de datos / servicios	Datos / servicios	Ocean Tokens para hacer disponible / proporcionar un servicio.
Referentes de datos / servicios, curadores. Incluye intercambios y otros proveedores de capa de aplicación.	Datos / servicio (a través de un proveedor, etc.), curación.	Ocean Tokens para CURACION.
Verificador de datos / servicios. Incluye resolución de pruebas enlazadas en otras cadenas.	Datos / servicio (a través de un proveedor, etc.), verificación.	Ocean Tokens para verificación.
Consumidor de datos / servicios	Ocean Tokens.	Datos / servicios (demanda del mercado)
Keepers	Ejecutar correctamente los nodos en la red.	Ocean Tokens para el mantenimiento de la cadena

Ocean como ecosistema de datos

1. Data Hub descentralizado

Podemos aprovechar la experiencia y la tecnología de los ecosistemas de datos centralizados existentes, que potencian las aplicaciones empresariales modernas, el aprendizaje automático a gran escala, el análisis de datos y mucho más. Estos ecosistemas combinan muchas tecnologías, tales como: sistemas mainframe, almacenes de datos operacionales, buses de datos y servicios empresariales, almacenes de datos y lagos de datos, ETLs (Extract, Transform, Load) y ELT, computación distribuida y en memoria, API y servicios web.

Los data hub empresariales tradicionales (EDH) tienen las siguientes capacidades:

1. **Fuente:** la exposición de los activos de datos iniciales disponibles.

2. **Ingestión:** ayuda a integrar los activos de datos en el ecosistema.
3. **Procesamiento:** transforma, normaliza y consolida activos, incluida la limpieza, la normalización y la consolidación.
4. **Persistencia:** Almacenar los activos para su uso.
5. **Consumo:** Utilizar los activos.
6. **Descubrimiento:** Encontrar los activos.
7. **Gobernanza:** implementar las reglas de gobierno del ecosistema, incluidas las condiciones criptográficas.

Cada servicio incorpora una o más de estas capacidades. Por ejemplo, un servicio ETL incorpora la prueba y el procesamiento, mientras que la distribución Spark incorpora el procesamiento y la persistencia en memoria algo definida.

Ocean apoya estas capacidades, de manera descentralizada. Por lo tanto, es un DataHub descentralizado (DDH). La figura 1 ilustra. Además de esto, habrá innumerables mercados de datos / servicios, tanto centralizados como descentralizados.

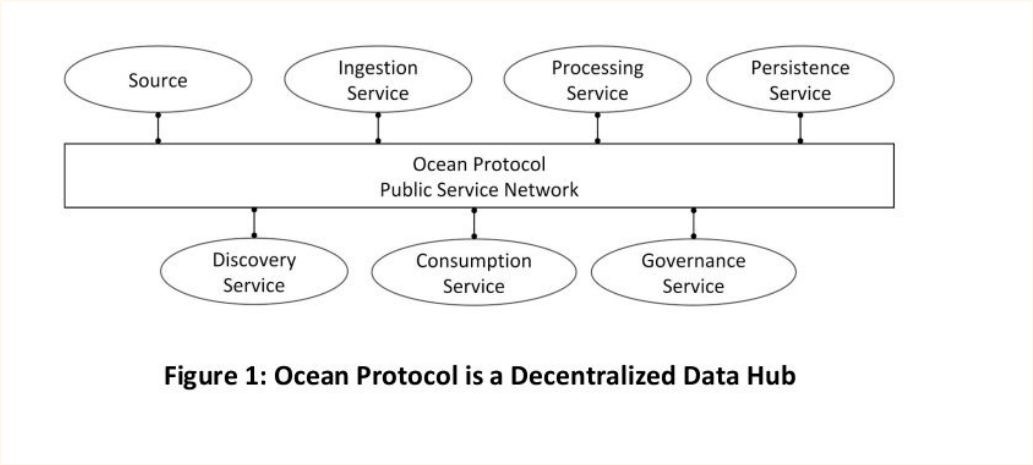


Figure 1: Ocean Protocol is a Decentralized Data Hub

2. Data Pipeline descentralizado

La organización de servicios en un EDH es manejada por data pipelines. Un data pipeline consta de control y flujos de datos que administran las interacciones del sistema entre los servicios.

Ocean facilitará dicha funcionalidad entre servicios descentralizados. La siguiente figura muestra un ejemplo de cómo Ocean cumple algunas de estas capacidades en un flujo de datos descentralizado que va de izquierda a derecha.

La **fuente** es una secuencia de registro o archivos de registro. Estos se **ingieren** en una cola de mensajes. Luego está el **procesamiento**, que podría ser centralizado (p. Ej., EC2 [Amazon2018c] o Lambda), descentralizado (p. Ej., Golem [Golem2016], iExec [iExec2017]) y posiblemente con capacidades especiales como AI (p. Ej., SingularityNET [SingularityNET2017]) o privacidad (p. Ej., Enigma [Zyskind2015]).

El siguiente paso es la **persistencia**, que podría ser blob stores o bases de datos, y centralizada o descentralizada. Por ejemplo, AWS S3 [Amazon2018b] es un blob store centralizado, IPFS / Filecoin [IPFS2018] [Filecoin2017] y Ethereum Swarm [Trón2018] son blob stores descentralizados, AWSAurora [Amazon2018] y Atlas MongoDB Amazon Aurora [Amazon2018] y MongoDB Atlas [MongoDB2018] son servicios de base de datos centralizados, y BigchainDB [BigchainDB2018] y OrbitDB [OrbitDB2018] son bases de datos descentralizadas.

Por último, el activo de datos lo **consume** un humano mirando un dashboards, o por software en la forma de Webhooks [Webhook2018], IFTTT u otra tecnología de callbacks.

La convergencia de Blockchain, AI y Big Data Analytics

Las regulaciones de la industria son necesarias para mantener a los consumidores seguros y las empresas responsables, pero los costos de cumplimiento son a menudo muy altos.

Para combatir esto, las tecnologías regulatorias centradas en el cumplimiento están en aumento. Deloitte incluso ha compilado una lista de las nuevas compañías "RegTech" que están dispuestas a interrumpir el panorama regulatorio.

La convergencia de blockchain, AI y el análisis de big data están abriendo las puertas a soluciones más poderosas e innovadoras que administran los costos de cumplimiento y reducen los riesgos operativos.

Los consumidores exigen más transparencia y las empresas no quieren gastar tiempo y dinero cumpliendo con las regulaciones de manera casual cuando hay una solución mejor y más rápida disponible.

Caso de uso: Alimentos y bebidas

Los dispositivos Blockchain y IoT pueden brindar a las grandes empresas una forma única de realizar un seguimiento de los productos, desde el campo hasta el supermercado.

Por ejemplo, cuando ocurre un brote de listeria o E.coli es importante rastrear de una manera rápida de dónde vienen esas bacterias para evitar que más personas ingieran alimentos contaminados.

Una cabeza de lechuga que se cosecha y se coloca en un recipiente se puede rastrear si el recipiente utiliza un dispositivo IoT para registrarlo en la cadena de bloques. Desde allí, el producto se traslada a una instalación donde se procesa y empaqueta, eventos que también se pueden registrar y rastrear.

Si surge un problema, los datos de seguimiento están disponibles para intervenir más rápido.

Caso de uso: Productos farmacéuticos

En los Estados Unidos, hay una regulación llamada DSCSA. En la UE, existe la Directiva de medicamentos falsificados. Ambas regulaciones requieren que todos los medicamentos estén identificados de manera única con un número de serie para evitar la falsificación y promover una mayor transparencia en la cadena de suministro.

Para cumplir con estas regulaciones se propuso una solución llamada **MediLedger**. Permite a las compañías farmacéuticas registrar fácilmente números de serie únicos en blockchain y rastrear los medicamentos a medida que avanzan a través de la cadena de suministro.

Caso de uso: Metales preciosos y minerales de conflicto

Muchos minerales y metales se extraen en zonas de conflicto y luego se venden para alimentar más conflictos y sufrimientos.

La SEC exige que las empresas informen si están usando minerales de conflicto. Pero el gobierno no está parando su negocio por hacerlo.

Por otro lado, muchas empresas que no usan minerales o metales en conflicto estarían felices de probar su autenticidad al rastrear y rastrear su producción. Este proceso es fácil de implementar con sistemas de cadena de suministro basados en blockchain.

EOS: Whitepaper

Background.

La tecnología Blockchain se introdujo en 2008 con el lanzamiento de la moneda de Bitcoin, y desde entonces los emprendedores y desarrolladores han intentado generalizar la tecnología para admitir una gama más amplia de aplicaciones en una única plataforma de blockchain.

Mientras que varias plataformas de blockchain han luchado para admitir aplicaciones descentralizadas funcionales, las blockchains específicas de la aplicación como el intercambio descentralizado de BitShares (2014) y la plataforma de redes sociales Steem (2016) se han convertido en blockchains muy utilizadas con decenas de miles de usuarios activos diarios. Lo han logrado al aumentar el rendimiento a miles de transacciones por segundo, reduciendo la latencia a 1.5 segundos, eliminando las tarifas por transacción y brindando una experiencia de usuario similar a la que proporcionan actualmente los servicios centralizados.

Las plataformas de blockchain existentes están sobrecargadas por grandes tarifas y capacidad de cálculo limitada que previenen la adopción generalizada de blockchain.

Requisitos para aplicaciones de blockchain.

Para obtener un uso generalizado, las aplicaciones en la cadena de bloques requieren una plataforma que sea lo suficientemente flexible para cumplir con los siguientes requisitos:

- ### Apoya a millones de usuarios

Para competir con empresas como eBay, Uber, AirBnB y Facebook, se requiere una tecnología de cadena de bloques capaz de manejar decenas de millones de usuarios activos diarios. En ciertos casos, una aplicación puede no funcionar a menos que se alcance una masa crítica de usuarios y, por lo tanto, una plataforma que pueda manejar un gran número de usuarios es primordial.

- ### Uso gratuito

Los desarrolladores de aplicaciones necesitan la flexibilidad para ofrecer a los usuarios servicios gratuitos; Los usuarios no deberían tener que pagar para utilizar la plataforma o beneficiarse de sus servicios. Una plataforma blockchain que es de uso gratuito para los usuarios

probablemente obtendrá una adopción más generalizada. Los desarrolladores y las empresas pueden crear estrategias de monetización efectivas.

- **Actualizaciones fáciles y recuperación de errores**

Las empresas que crean aplicaciones basadas en blockchain necesitan la flexibilidad para mejorar sus aplicaciones con nuevas características. La plataforma debe ser compatible con software y actualizaciones de contratos inteligentes.

Todo software no trivial está sujeto a errores, incluso con la verificación formal más rigurosa. La plataforma debe ser lo suficientemente robusta como para corregir errores cuando ocurren inevitablemente.

- **Baja latencia**

Una buena experiencia de usuario requiere una retroalimentación confiable con un retraso de no más de unos pocos segundos. Los retrasos más prolongados frustran a los usuarios y hacen que las aplicaciones creadas en una cadena de bloques sean menos competitivas con las alternativas existentes que no son cadenas de bloques. La plataforma debe soportar baja latencia de las transacciones.

- **Rendimiento secuencial**

Hay algunas aplicaciones que simplemente no se pueden implementar con algoritmos paralelos debido a pasos secuencialmente dependientes. Las aplicaciones como los intercambios necesitan un rendimiento secuencial suficiente para manejar grandes volúmenes. Por lo tanto, la plataforma debe soportar un rendimiento secuencial rápido.

- **Rendimiento paralelo**

Las aplicaciones a gran escala necesitan dividir la carga de trabajo entre varias CPU y computadoras.

Algoritmo de consenso (BFT-DPOS).

El software EOS.IO utiliza el único algoritmo de consenso descentralizado conocido que ha demostrado ser capaz de cumplir con los requisitos de rendimiento de las aplicaciones en la cadena de bloques, Prueba de estaca delegada (DPOS) . Bajo este algoritmo, aquellos que tienen tokens en una cadena de bloques que adopta el software EOS.IO pueden seleccionar productores de bloques a través de un sistema de votación de aprobación continua. Cualquiera

puede optar por participar en la producción de bloques y se le dará la oportunidad de producir bloques, siempre que puedan persuadir a los poseedores de fichas para que voten por ellos.

El software EOS.IO permite que los bloques se produzcan exactamente cada 0,5 segundos y un productor está autorizado para producir un bloque en cualquier momento dado. Si el bloque no se produce a la hora programada, entonces se omite el bloque para ese intervalo de tiempo. Cuando se omiten uno o más bloques, hay un espacio de 0.5 segundos o más en la cadena de bloques.

Usando el software EOS.IO, los bloques se producen en rondas de 126 (6 bloques cada uno, 21 productores). Al comienzo de cada ronda, se seleccionan 21 productores de bloques únicos por preferencia de votos emitidos por los poseedores de fichas. Los productores seleccionados están programados en un orden acordado por 15 o más productores.
Si un productor pierde un bloque y no ha producido ningún bloque en las últimas 24 horas, se le retirará de consideración hasta que notifique a blockchain su intención de comenzar a producir bloques nuevamente. Esto garantiza que la red funcione sin problemas al minimizar la cantidad de bloques que se pierden al no programar a los productores que no son confiables.

En condiciones normales, una cadena de bloques DPOS no experimenta ninguna bifurcación porque, en lugar de competir, los productores de bloques cooperan para producir bloques. En el caso de que haya una bifurcación, el consenso cambiará automáticamente a la cadena más larga. Este método funciona porque la velocidad a la que se agregan los bloques a una bifurcación de blockchain se correlaciona directamente con el porcentaje de productores de bloques que comparten el mismo consenso. En otras palabras, una horquilla(fork) blockchain con más productores crecerá en longitud más rápido que una horquilla con menos productores, porque la horquilla con más productores experimentará menos bloques perdidos.

Además, ningún productor de bloques debe producir bloques en dos horquillas al mismo tiempo. Un productor de bloque atrapado haciendo esto probablemente será eliminado. La evidencia criptográfica de tal doble producción también puede usarse para eliminar automáticamente a los abusadores.

La Tolerancia a fallos bizantina se agrega al DPOS tradicional al permitir que todos los productores firmen todos los bloques, siempre que ningún productor firme dos bloques con la misma marca de tiempo o la misma altura de bloque. Una vez que 15 productores han firmado un bloque, el bloque se considera irreversible. Cualquier productor bizantino tendría que generar evidencia criptográfica de su traición firmando dos bloques con la misma marca de

tiempo o altura de bloque. Bajo este modelo, se debe alcanzar un consenso irreversible en 1 segundo.

- ### Confirmación de la transacción

Las cadenas de bloques típicas de DPOS tienen una participación del 100% del productor de bloques. Una transacción puede considerarse confirmada con 99.9% de certeza luego de un promedio de 0.25 segundos desde el momento de la emisión.

Además de DPOS, EOS.IO agrega Tolerancia a fallos bizantinos asíncronos (aBFT) para un logro más rápido de la irreversibilidad. El algoritmo aBFT proporciona un 100% de confirmación de irreversibilidad en 1 segundo.

- ### Transacción como Prueba de Juego (TaPoS)

El software EOS.IO requiere que cada transacción incluya parte del hash de un encabezado de bloque reciente. Este hash sirve para dos propósitos:

1. evita la reproducción de una transacción en las horquillas(forks) que no incluyen el bloque al que se hace referencia; y
2. indica a la red que un usuario en particular y su participación están en una bifurcación específica.

Con el tiempo, todos los usuarios terminan confirmando directamente la cadena de bloques, lo que dificulta la falsificación de cadenas falsas, ya que la falsificación no podría migrar transacciones de la cadena legítima.

OpenMined

OpenMined es un proyecto de código abierto que busca devolver el poder a las personas.

OpenMined es una comunidad enfocada en la construcción de tecnología para la propiedad descentralizada de datos e IA. Los científicos de datos pueden pagar a los usuarios directamente por sus datos y entrenar a los modelos de AI de forma descentralizada. Cubriremos el aprendizaje profundo, el aprendizaje federado, el cifrado homomórfico y los contratos inteligentes de cadena de bloques.

El modelo de negocio de la Inteligencia Artificial

1. Adquirir datos sobre personas.
2. Entrenar un modelo que haga algo útil.
3. Vender el uso de ese modelo (la aplicación)

Problemas

- **Privacidad**: las personas pierden el control de sus datos.
    - Riesgos: Robo, Reventa y Persuasión.
- **Ingreso natural perdido**: Los datos son un recurso natural.
- **Problema del producto sensible**: Algunos servicios son espeluznantes.
- **Potencia agregada**: las empresas muy grandes tienen todos los datos, las pequeñas empresas no tanto.

Criterios de éxito

- **Privacidad**: Las personas mantienen el control de sus datos.
- **Ingresos**: Las personas obtienen ingresos pasivos de los datos.
- **Productos Sensibles Posibles**: Se pueden construir de manera segura.
- **Poder descentralizado**: Todos controlan los datos.
- **Productizable**: sigue facilitando la creación de todos los productos y servicios que la gente espera de AI.

Esquema

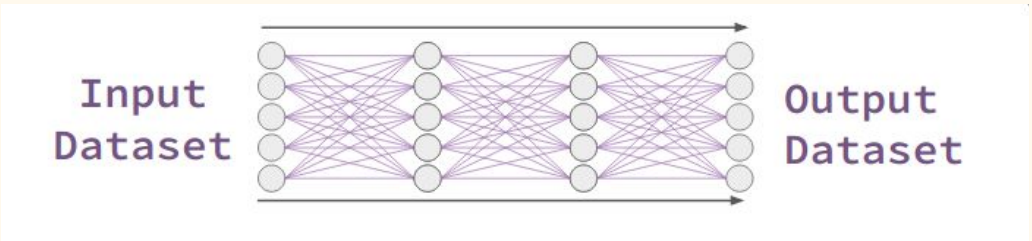
Parte 1: Ingredientes para una solución.

Deep Learning

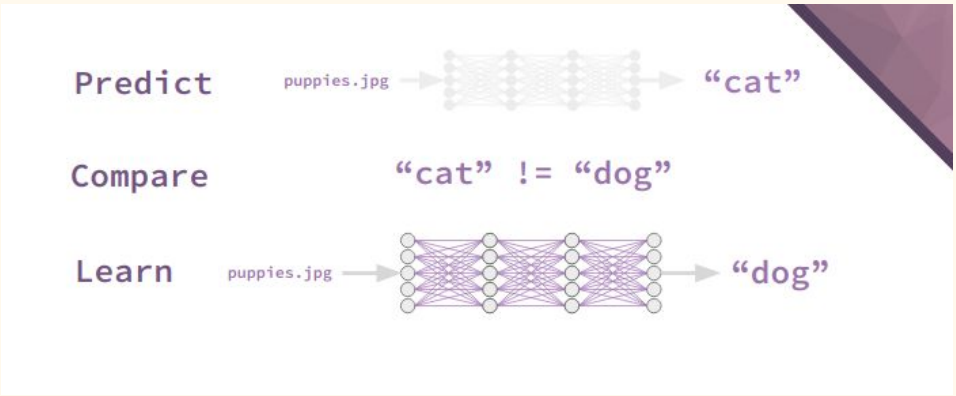
Deep Learning es un conjunto de herramientas para la automatización de la inteligencia, que aprovecha principalmente las redes neuronales. Como un campo de la informática, es en gran parte responsable del reciente auge de la tecnología A.I, ya que ha superado los registros de calidad anteriores para muchas tareas de inteligencia.

Una red neuronal hace predicciones basadas en la entrada. Aprende a hacer esto efectivamente por ensayo y error. Comienza haciendo una predicción (que es en gran parte aleatoria al principio), y luego recibe una "señal de error" que indica que predijo demasiado alto o demasiado bajo (generalmente probabilidades). Después de que este ciclo se repite muchos millones de veces, la red comienza a descubrir las cosas.

- Aprende a convertir Dataset A -> Dataset B
- Machine Learning jerárquico con redes neuronales.
- “Deep” viene de su naturaleza jerárquica.



- **Pasos:**
    - Step 0: Inicio. Se crea una función aleatoria.
    - Step1: Predicción. Output dado un input.
    - Step2: Comparación: ¿Predicción muy alta?¿Muy baja?
    - Step 3: Aprender: Ajustar la función para reducir el error.
    - Volver al paso 1.



Algunas de las **librerías** que se emplean para **Deep Learning**:

- Pytorch
- TensorFlow
- Keras
- Torch
- DL4J

Federated Learning

En lugar de llevar los datos a un solo lugar para el entrenamiento, el aprendizaje federado se realiza al llevar el modelo a los datos. Esto permite al propietario de los datos mantener la única copia de su información.

- **Steps:**
    - Step 1: Usuarios descargan un modelo.
    - Step 2: Usuarios entrenan el modelo con sus datos.
    - Step 3: Usuarios suben sus gradientes a un servidor.
    - Step 4: Los gradientes se suman para proteger la privacidad.
    - Step 5: El modelo se actualiza en la nube.
    - Repetir.

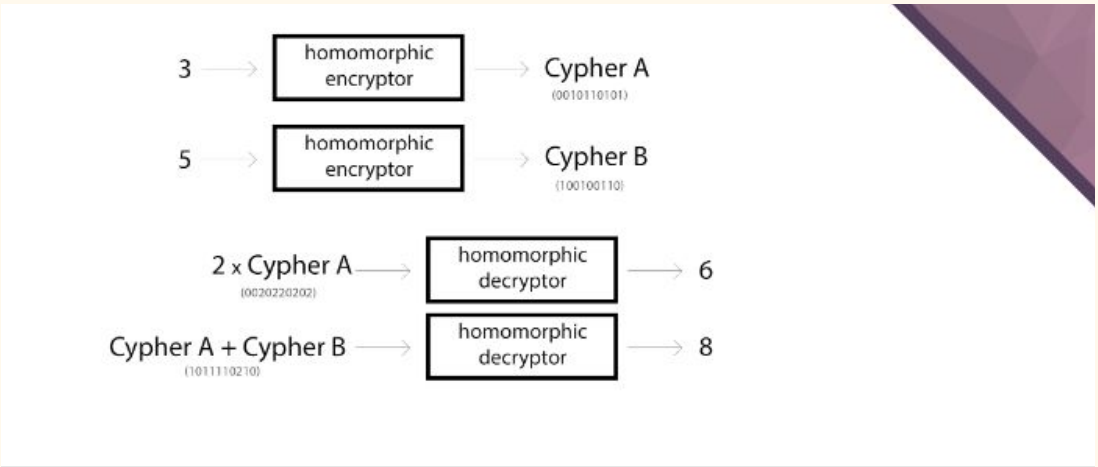
Plataformas de Lenguaje Federado

- Apple Inc. de forma interna.
- Google/Android de forma interna.

Encriptación Homomórfica.

Sin embargo, el cifrado homomórfico es un tipo especial de cifrado. Permite que alguien modifique la información cifrada de maneras específicas sin poder leer la información. Por ejemplo, el cifrado homomórfico se puede realizar en números, de modo que la multiplicación y la suma se pueden realizar en valores cifrados sin descifrarlos. Aquí hay algunos ejemplos de juguetes.

Ahora, hay un número creciente de esquemas de cifrado homomórficos, cada uno con diferentes propiedades. Es un campo relativamente joven y hay varios problemas importantes que aún no se han resuelto.



Blockchain

La cadena de bloques (Blockchain), es un registro único, consensuado y distribuido en varios nodos de una red. En el caso de las criptomonedas, podemos pensarlo como el libro contable donde se registra cada una de las transacciones.

La cadena de bloques se construye en base a propiedades criptográficas que buscan imposibilitar la modificación de la información que en ella se contiene.

- Nadie puede editar / borrar una entrada antigua.
- Nadie puede falsificar una nueva entrada.
- Aplicado por límites fundamentales de computación (Prueba de trabajo / **Proof Of Work**).

Smart Contracts

Los contratos inteligentes se encargan de leer y escribir datos en la cadena de bloques, así como de ejecutar la lógica empresarial. Los contratos inteligentes están escritos en un lenguaje de programación llamado Solidity. La función de los contratos inteligentes en la cadena de bloques es muy similar a un microservicio en la web

- Dato: Libros mayores, eventos, estadísticas.
- Estado: Libro de hoy, eventos de hoy.
- Código: reglas para cambiar de estado.

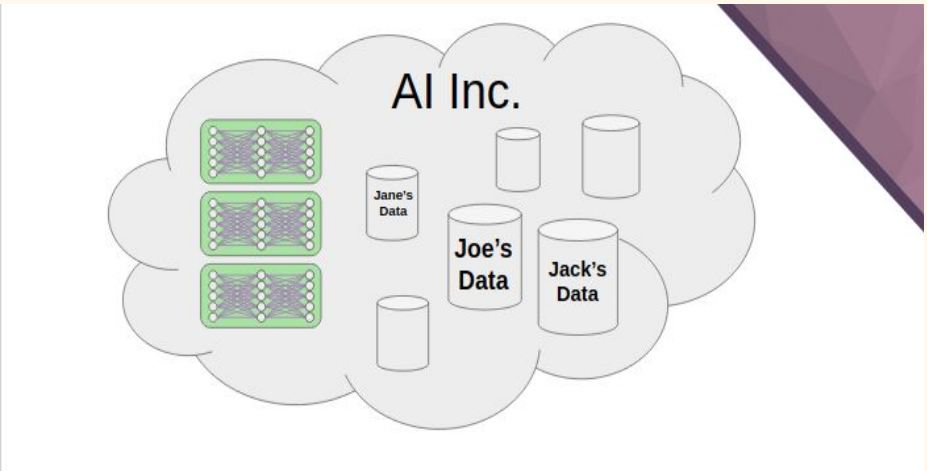
Parte 2: "Recetas" para aplicaciones:

La combinación de todas las tecnologías descritas en la sección anterior crean:

- Deep Learning + Federated Learning+Homomorphic Encryption + Blockchain Smart Contracts = ***OpenMined***.

Propuesta de arquitectura de OpenMined.

Deep Learning

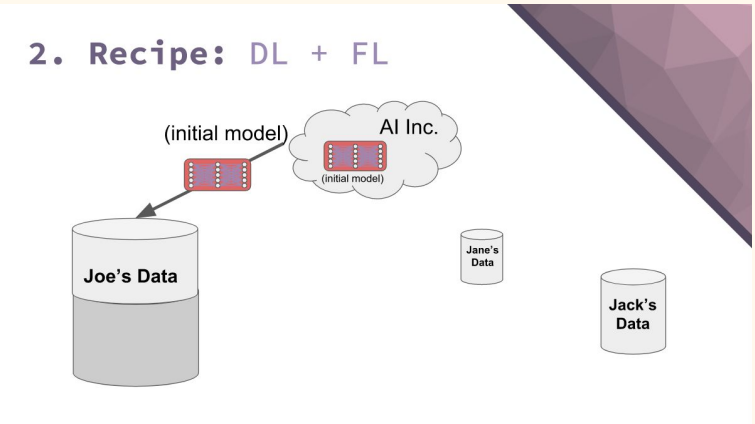


Modelo base en la nube. Toda el entrenamiento se realiza dentro de la nube para AI Inc. Todos los usuarios que tienen datos viven dentro de la nube, por lo que esta es la arquitectura que

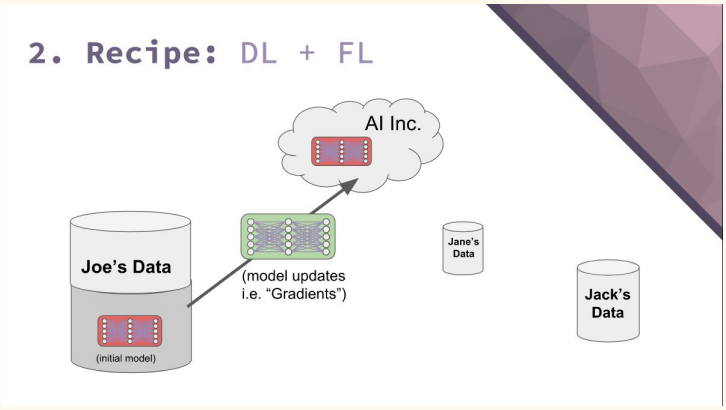
vamos a intentar separar.

Deep Learning + Federated Learning

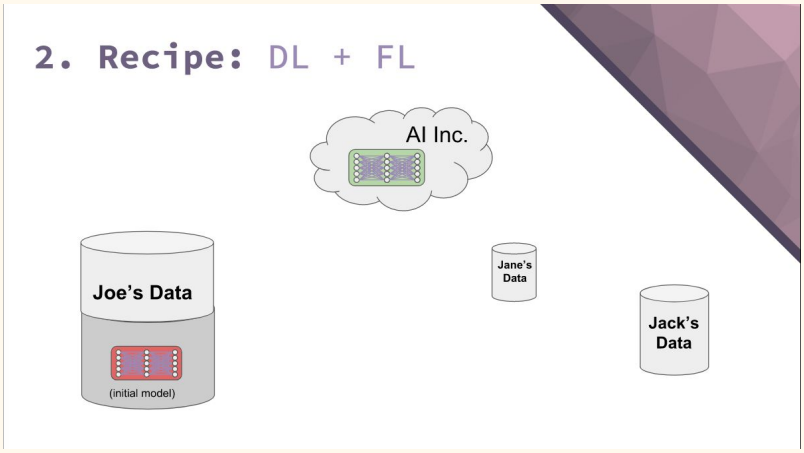
Dentro de la nube de AI Inc. se inicializará un modelo. El modelo inicializado se enviará a Joe, que recibirá esto y entrenará el modelo.



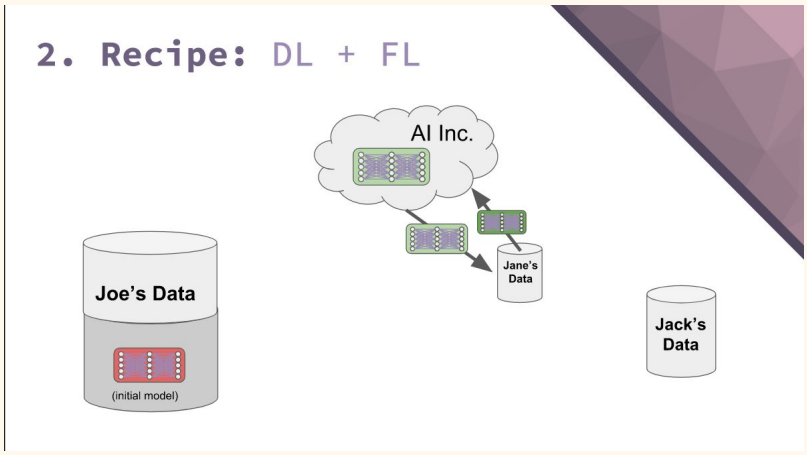
El modelo es subido a AI Inc con sus correspondientes gradientes.



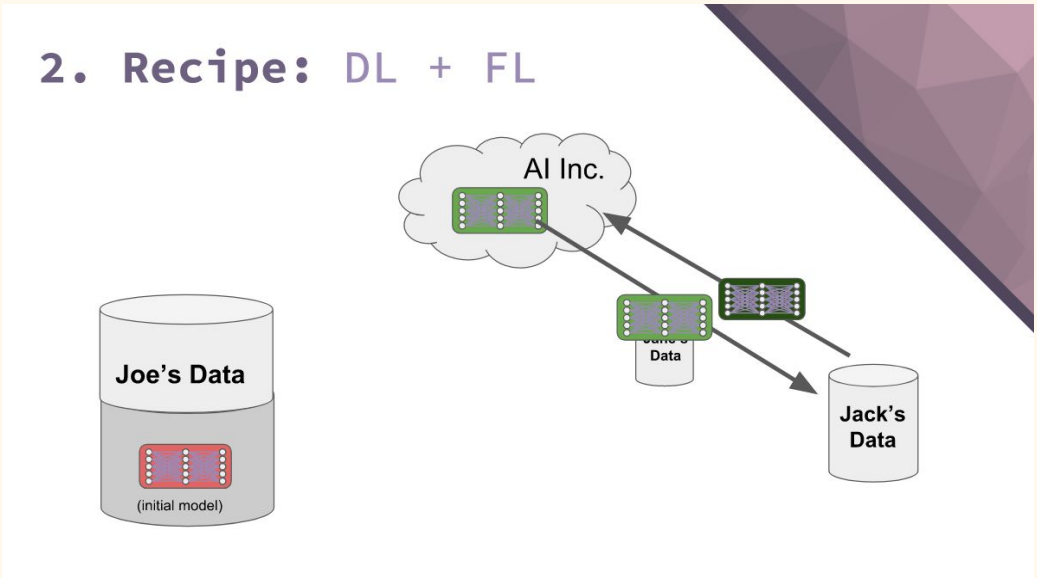
El modelo consigue ser más “inteligente”.

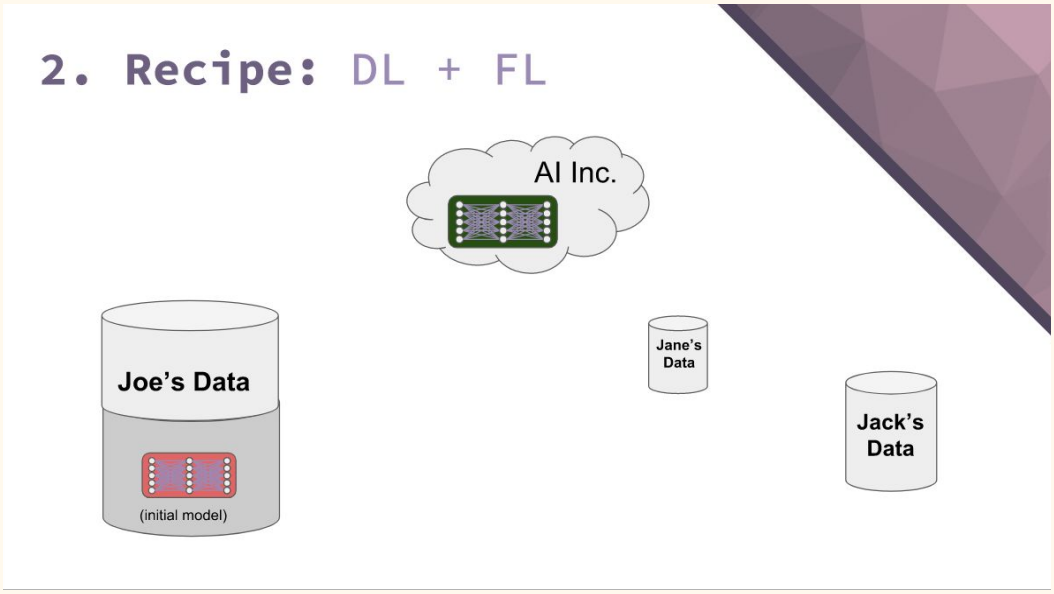


Repetimos el proceso con los datos de Jane, de esta forma el modelo continúa evolucionando y se convierte en más inteligente.



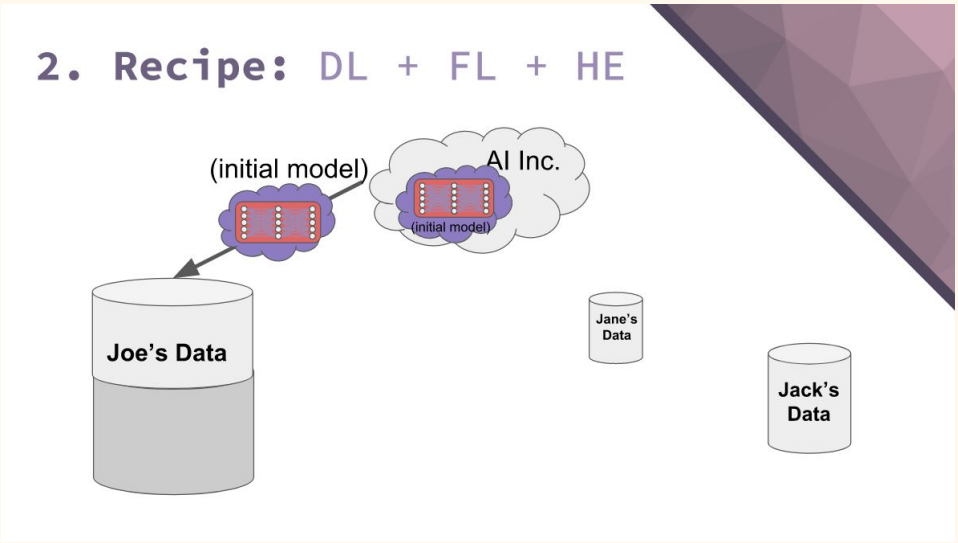
Lo mismo para los datos de Jack, así conseguimos un modelo aún más inteligente que está en posesión de AI Inc. y está basado en los datos donados.

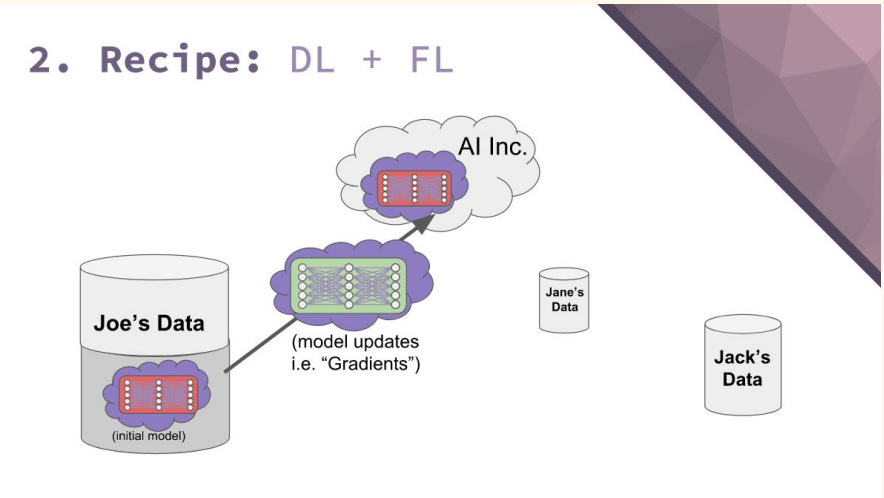

2. Recipe: DL + FL
AI Inc.
Joe's Data
(initial model)
Data
Jack's Data


2. Recipe: DL + FL
AI Inc.
Joe's Data
(initial model)
Jane's Data
Jack's Data

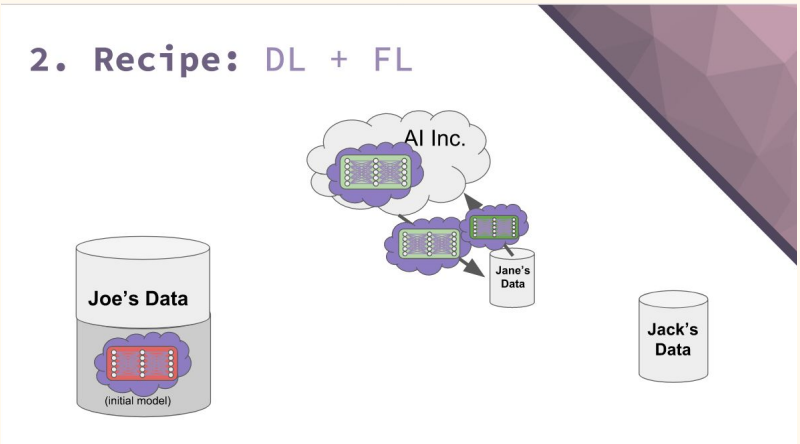
Deep Learning + Federated Learning + Homomorphic Encryption

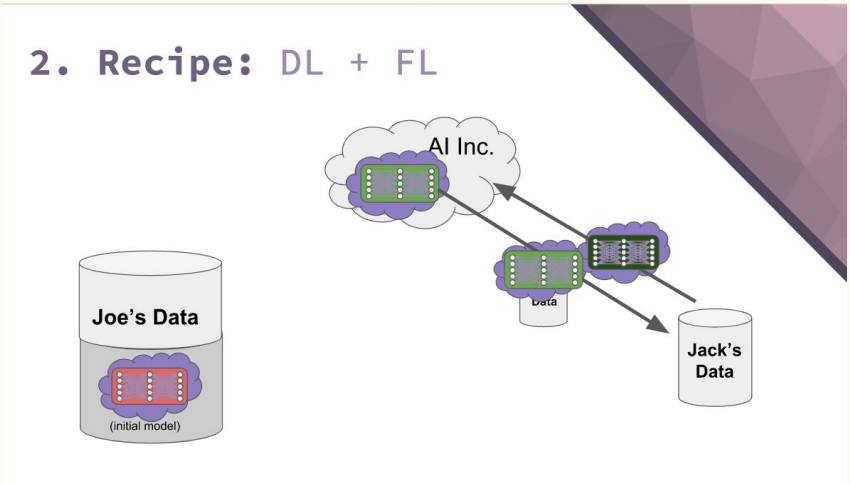
Con **Encriptación Homomórfica** pasaremos por el mismo flujo de trabajo. Esta vez, el modelo inicializado dentro de la nube se envolverá en cifrado homomórfico.Este modelo inicializado se enviará a Joe. Éste no puede ver lo que está haciendo el modelo porque está envuelto en HE(**Homomorphic Encrypytion**) .



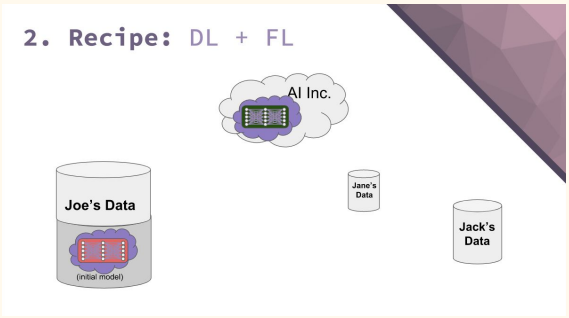


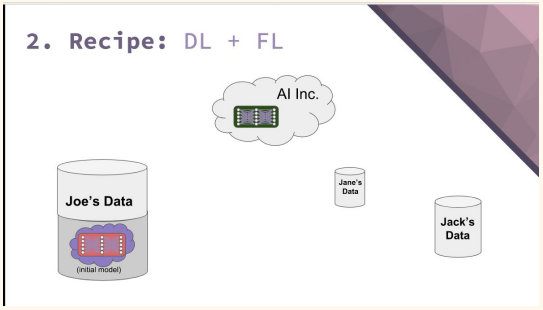
El entrenamiento del modelo funciona de la misma manera que antes, excepto que el modelo se devuelve de manera cifrada, por lo que repetiremos este ciclo y el modelo va evolucionando.





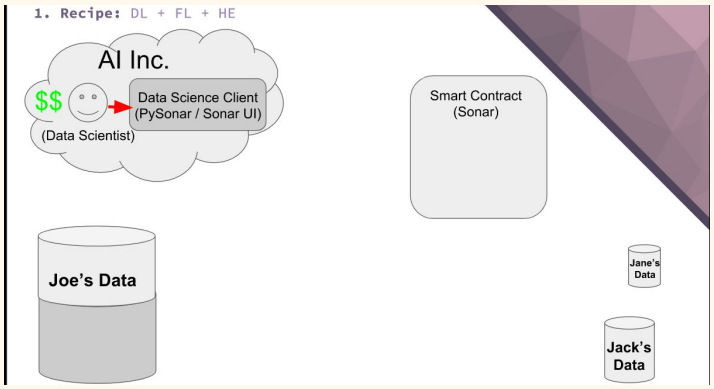
El modelo puede ser descifrado por AI Inc. y ser estudiado.



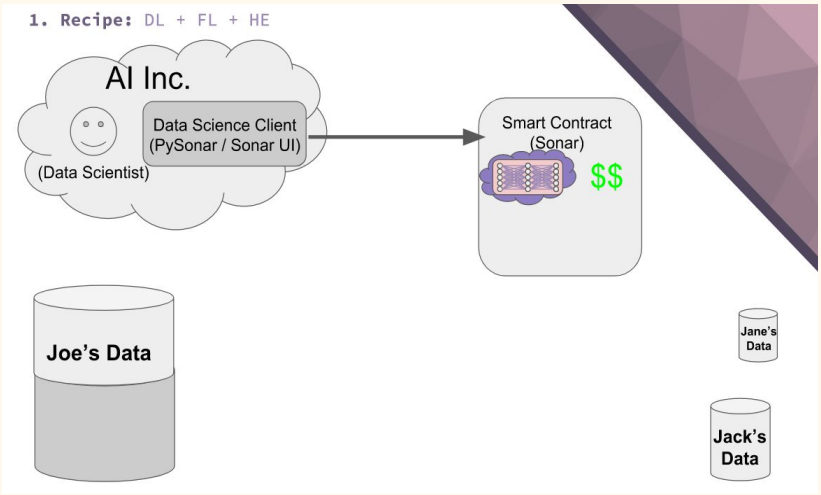


Deep Learning + Federated Learning + Homomorphic Encryption + Smart Contracts

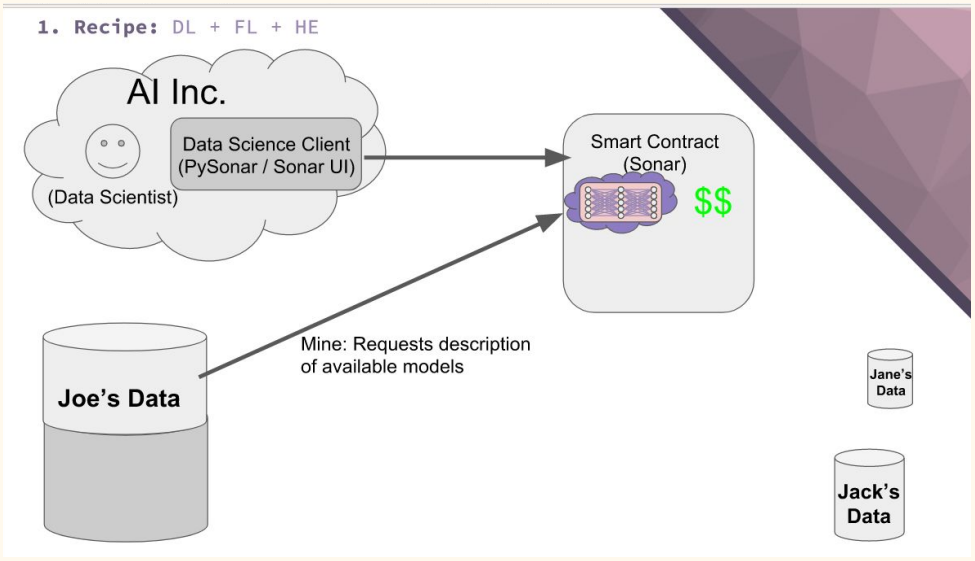
El modelo será inicializado en AI Inc.

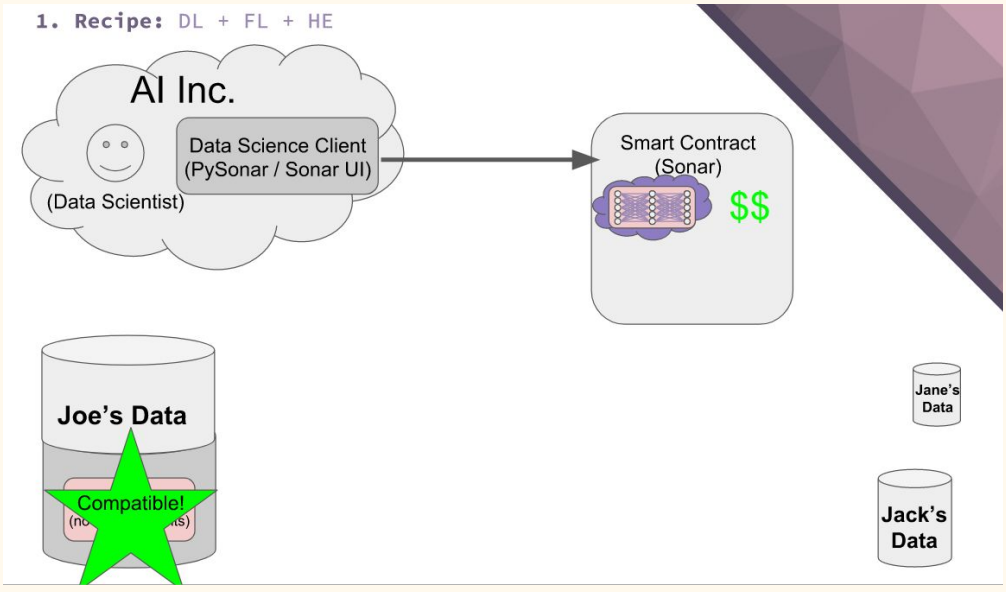


La especificación del modelo ahora se enviará a un contrato inteligente que vive en una cadena de bloques con criptomonedas.Como esta es solo la especificación del modelo, no hay pesos reales en este momento. El modelo se escribe en el contrato inteligente en la cadena de bloques. Se inicializan pesos aleatorios, el modelo ahora es HE(**Homomorphic Encryption**).

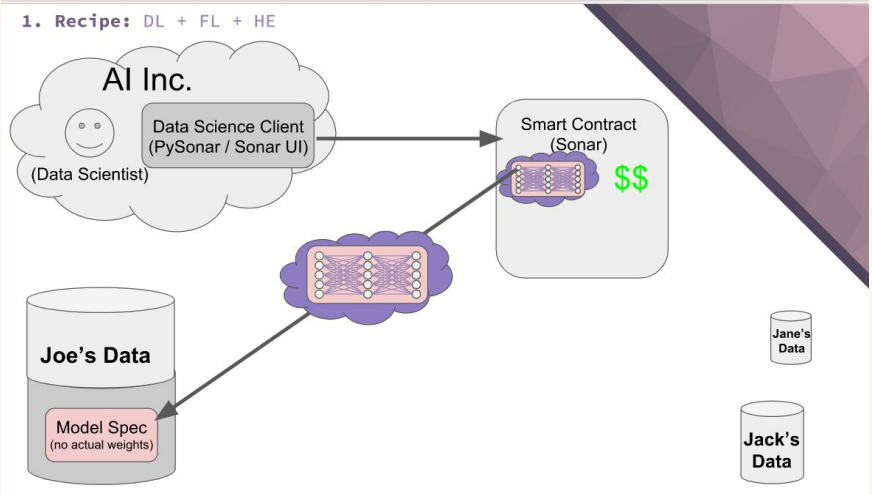


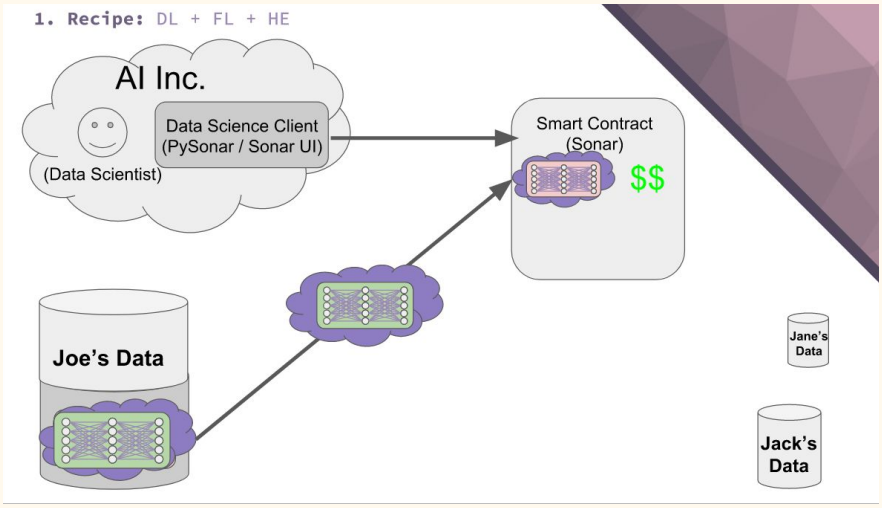
Joe solicita una descripción de los modelos disponibles. Las especificaciones del modelo establecen que se ha verificado que son compatibles para solicitar los parámetros del modelo.

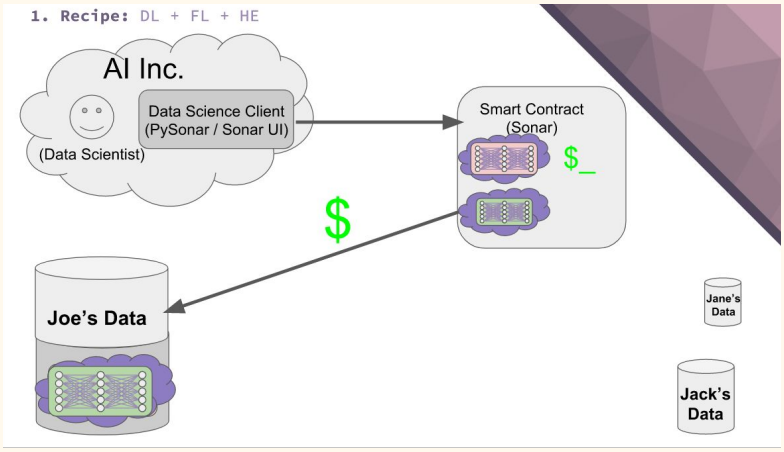




El modelo ahora se envía de nuevo HE, Joe recibe este modelo y entrena al modelo.El modelo entrenado se vuelve a subir al contrato inteligente en la cadena de bloques.







Se verifica que los gradientes sean buenos. Ahora Joe es recompensado con algunas criptomonedas por su trabajo.

PySyft: A generic framework for privacy preserving deep learning.

Introducción

La computación multipartita segura (SMPC) se está volviendo cada vez más popular como una forma de realizar operaciones en un entorno no confiable sin revelar datos. En el caso de los modelos de aprendizaje automático, SMPC protegería los pesos del modelo y permitiría que varios nodos de trabajadores participen en la fase de capacitación con sus propios conjuntos de datos, un proceso conocido como aprendizaje federado (FL). Sin embargo, se ha demostrado que los modelos entrenados de manera segura aún son vulnerables a los ataques de ingeniería inversa que pueden extraer información sensible sobre los conjuntos de datos directamente del modelo. Otro conjunto de métodos, etiquetados como Métodos Diferencialmente Privados (DP), aborda esto y puede proteger los datos de manera eficiente.

Con PySyft se proporciona un framework transparente para la privacidad que preserva el aprendizaje profundo para cada usuario de PyTorch, permitiendo el uso de FL, MPC y DP desde una interfaz intuitiva.

Las principales aportaciones son las siguientes:

- Primero se construyó un protocolo estandarizado para la comunicación entre los trabajadores que hizo posible el aprendizaje federado.
- Luego, se desarrolló un modelo de abstracción en cadena sobre los tensores para anular de manera eficiente las operaciones (o codificar otras nuevas), como el envío / intercambio de un tensor entre los trabajadores.
- Por último, se proporcionó los elementos para implementar la privacidad diferencial propuesta recientemente y los protocolos de cómputo multipartita utilizando este nuevo framework. Al hacerlo, pretendemos ayudar a popularizar las técnicas de preservación de la privacidad en el aprendizaje automático, haciéndolas disponibles a través de las herramientas comunes con las que los investigadores y los científicos de datos trabajan diariamente. Nuestro framework de trabajo está diseñado de manera extensible, de manera que los contribuyentes externos que desean poner su trabajo a disposición de la comunidad más amplia de aprendizaje profundo pueden incorporar nuevos métodos de FL, MPC o DP.

Un framework estandarizado para operaciones abstractas en tensores.

Estructura de la cadena

Realizar transformaciones o enviar tensores a otros trabajadores puede representarse como una cadena de operaciones, y cada operación está representada por una clase especial. Para lograr esto, creamos una abstacción llamada **SyftTensor**. Los SyftTensors están destinados a representar un estado o transformación de los datos y se pueden encadenar juntos. La estructura de la cadena siempre tiene a la cabeza el tensor de PyTorch, y se accede a las transformaciones o estados incorporados por los **SyftTensors** utilizando el atributo ***child*** y hacia arriba utilizando el atributo ***parent***.

La imagen de abajo presenta la estructura general de una cadena de tensor, donde los **SyftTensors** se reemplazan con instancias de algunas subclases que tienen un rol específico, como la clase **LocalTensor** que se describirá a continuación. Todas las operaciones se aplican primero al tensor Torch, lo que hace posible tener la interfaz NativeTorch, y luego se transmiten a través de la cadena mediante el reenvío al atributo **child**.

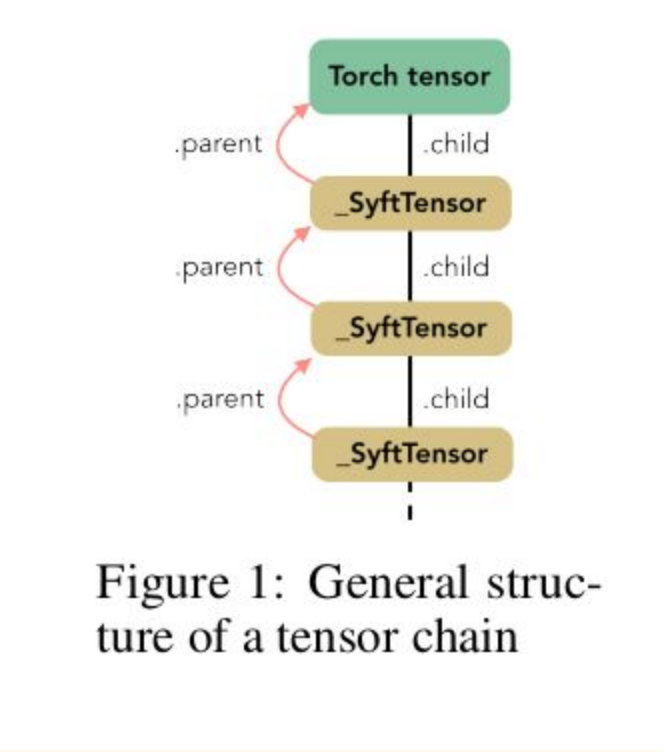


Figure 1: General structure of a tensor chain

Hay dos subclases importantes de **SyftTensor**.

- Primero, el ***LocalTensor*** que se crea automáticamente cuando se crea una instancia del Torch tensor. Su función es realizar en el Torch tensor la operación nativa correspondiente a la operación sobrecargada. Por ejemplo, si el comando es **agregar**, entonces el LocalTensor ejecutará el comando nativo **Toch** *native_add* en el tensor principal. La cadena tiene dos nodos y realiza un bucle, de modo que el elemento secundario Local Tensor se refiere al tensor del nodo principal que contiene los datos sin necesidad de volver a crear un objeto tensor secundario, lo que reduciría el rendimiento.
- Segundo, el ***PointerTensor*** que se crea cuando se envía un tensor a un trabajador remoto. Enviar y recuperar un tensor es tan simple como llamar a los métodos ***send(worker)*** y ***get()*** en el tensor. Cuando esto sucede, toda la cadena se envía al trabajador y se reemplaza por una cadena de dos nodos: el tensor, ahora vacío. y el **PointerTensor**, que especifica quién es el propietario de los datos y la ubicación remota de almacenamiento. Esta vez, el puntero no tiene hijo. La imgan de abajo ilustra cómo se modifican las cadenas cuando se envían a un trabajador remoto y cómo se utilizan **LocalTensor** y **PointerTensor** en esas cadenas.

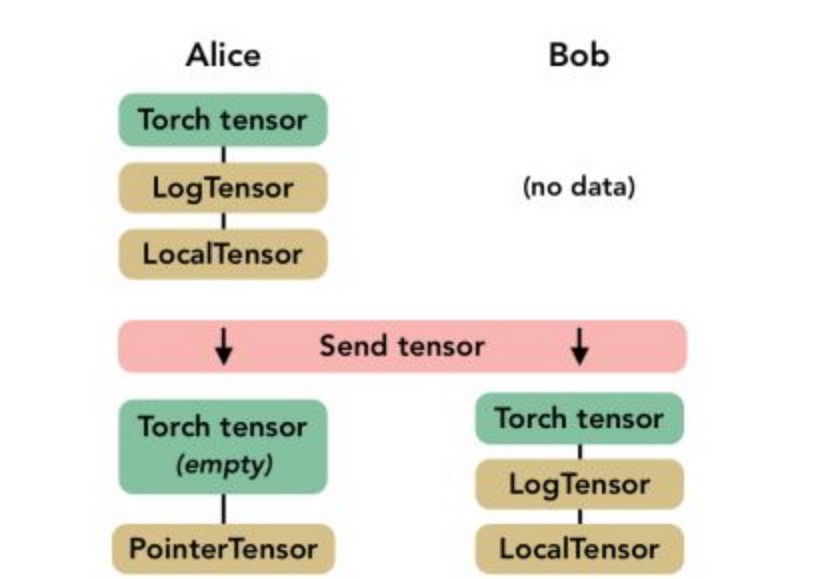


Figure 2: Impact of sending a tensor on the local and remote chains

De la ejecución virtual al contexto real del aprendizaje federado.

Para simplificar la depuración de complejas cadenas de operaciones, este framework desarrolla la noción de Trabajadores Virtuales. Todos los trabajadores virtuales viven en la misma máquina y no se comunican a través de la red. Simplemente replican la cadena de comandos y exponen la misma interfaz que los trabajadores reales para comunicarse entre sí.

Los **Network Workers** en el contexto de aprendizaje federado tienen dos implementaciones en los frameworks de ahora. Uno se basa en sockets de red simples, mientras que el otro admite **WebSockets**. Los trabajadores de WebSocket permiten crear múltiples instancias de trabajadores desde un navegador, cada uno dentro de su propia pestaña. Esto nos da otro nivel de granularidad al crear aplicaciones de aprendizaje federadas antes de dirigirse a los trabajadores remotos que no están en la misma máquina. Los trabajadores de **WebSocket** también se adaptan muy bien al ecosistema de la ciencia de datos que gira en torno a los *notebooks* basados en navegador.

Hacia un framework seguro de MPC

Construyendo un MPCTensor

Los elementos introducidos en la sección anterior forman los ladrillos de construcción necesarios para crear nuestro MPCTensor. La división y el envío de los recursos compartidos se pueden realizar utilizando una lista de PointerTensors. La MPC toolbox propuesta en nuestro framework implementa el protocolo SPDZ.

La MPC toolbox incluye operaciones básicas como la suma y la multiplicación, pero también herramientas de preprocesamiento para generar, por ejemplo, los triples utilizados para la multiplicación, y operaciones más específicas para redes neuronales, incluida la multiplicación de matrices. Debido a las especificidades de MPC, se realizan algunos ajustes a los elementos tradicionales de una red convolucional: utilizamos la agrupación promedio en lugar de la agrupación máxima y el ***sigmoide*** aproximado de mayor grado en lugar de ***relu*** como una función de activación.

Dado que el protocolo SPDZ asume que los datos se proporcionan como números enteros, agregamos a la cadena un nodo llamado FixedPrecisionTensor que convierte los números flotantes en números de precisión fijos. Este nodo codifica el valor en un entero y almacena la posición del punto radix. La estructura completa de un tensor que implementa SPDZ se resume en la figura 3.

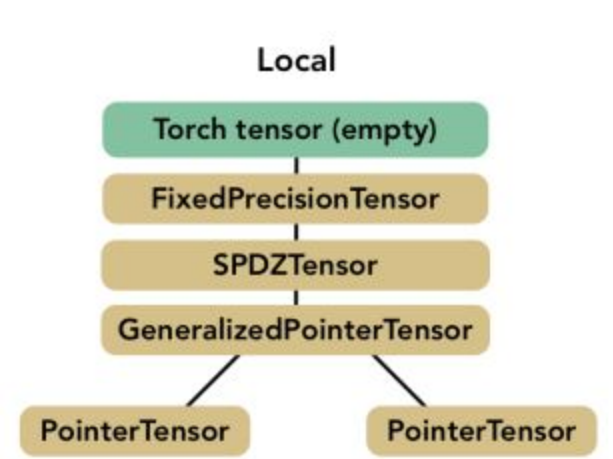


Figure 3: Chain structure of a SPDZ tensor

A diferencia del protocolo MPC , los trabajadores(**workers**) no son iguales en nuestro framework, ya que uno es el propietario del modelo (llamado trabajador local). Actúa como líder al controlar el procedimiento de entrenamiento en todos los demás trabajadores (los trabajadores remotos). Para mitigar este sesgo de centralización cuando se trata de datos, el trabajador local **puede** crear tensores compartidos remotos sobre datos que **no posee** y que no puede ver.

De hecho, esperamos que los trabajadores remotos tengan sus **propios datos en un entorno general**, por ejemplo, cuando los hospitales contribuyen con imágenes médicas para entrenar a un modelo. Luego, varios trabajadores están interesados en ver que la ejecución se realice correctamente, lo cual es particularmente crucial durante la fase de inferencia, donde muchos factores podrían llevar a predicciones corruptas.

Hasta ahora, la implementación actual de **PySyft** no viene con un mecanismo para garantizar que cada trabajador se comporte con honestidad. Una mejora interesante sería implementar la autenticación MAC del valor compartido secreto.

Aplicando Privacidad Diferencial

Se implementa la privacidad diferencial basada en el trabajo de [1], que proporciona un método de entrenamiento para redes neuronales profundas dentro de un presupuesto de privacidad

modesto ("un dígito"). Para lograr esto, el documento proporciona una nueva estimación de la pérdida de privacidad utilizada para ajustar cuidadosamente el ruido necesario, junto con un nuevo algoritmo que mejora la eficiencia del entrenamiento privado.

En particular, implementamos el Stochastic Gradient Descent (SGD): en lugar de iterar de la misma manera en el dataset y en las iteraciones, el entrenamiento se realiza en fases, cada una de ellas consiste en muestrear L elementos de los N elementos del conjunto de datos y usarlos para actualizar el modelo. Reutilizamos directamente el contador de privacidad proporcionado por [1], pero implementamos nuestro propio "***sanitizante***" que recorta los gradientes y agrega ruido gaussiano.

Nuestro framework también proporciona algunos refinamientos guiados por el contexto de aprendizaje federado. Primero, cuando muestreamos mucho, elegimos aleatoriamente un trabajador y muestreamos entre sus propios datos. En segundo lugar, los gradientes se "***sanean***" en el trabajador remoto para garantizar la privacidad de los datos de manera eficiente. De esta manera, el trabajador local obtendrá gradientes seguros para actualizar el modelo que no puede revelar información sobre el conjunto de datos.

El enfoque descrito en [5] propone otro enfoque para asegurar la privacidad diferencial mediante el entrenamiento del modelo final (llamado modelo del estudiante) utilizando los votos ruidosos y agregados de los modelos pre-entrenados y no publicados (los maestros). Actualmente se está implementando y se integrará como otro Tensor de DP en nuestro framework.

Resultados y discusión.

La Tabla 1 informa el tiempo de ejecución requerido para entrenar una red neuronal en el conjunto de datos canónico de Boston Housing, utilizando tres declinaciones de nuestro framework. Un análisis de rendimiento denota una sobrecarga razonablemente pequeña por el uso de los trabajadores de Web Socket en lugar de los trabajadores virtuales, validando así su propósito de herramienta de desarrollador de notebook. Esto se debe a la **baja latencia de la red** cuando se comunica entre diferentes pestañas locales. Sin embargo, **somos 46 veces más lentos que usar PyTorch regular.** Observamos la misma sobrecarga en el rendimiento en nuestro segundo experimento que entrena a un clasificador para detectar la diabetes usando el conjunto de datos Pima Indian Diabetes, un pequeño conjunto de datos que contiene 768 filas y 8 columnas [6].

Training mode	Training time (s)
PySyft (Virtual)	10.1
PySyft (Socket)	14.6
PySyft (Virtual) + DP*	15.3
Pure PyTorch	0.22

Table 1: Training time using different training settings on the Boston Housing dataset (10 epochs)
**Equivalent time for the same number of batches processed for DP*

La Tabla 2 muestra cómo el aumento de “e”mejora el modelo a expensas de la privacidad de los datos. El modelo DP alcanza un 25-30 MSE en comparación con 20-24 en el modelo inicial, pero la garantía de privacidad se mantiene firme a medida que alcanzamos la privacidad diferenciada (0.5, 10 - 5).

(ϵ, δ)-privacy	Boston MSE	Pima Acc.
$(0.5, 10^{-5})$	29.4	60.6%
$(1, 10^{-5})$	29.2	64.2%
$(2, 10^{-5})$	28.5	66.1%
$(4, 10^{-5})$	28.6	67.1%
no privacy	23.7	70.3%

Table 2: Accuracy of differentially private federated learning on the Boston Housing and Pima Diabetes datasets

Para el conjunto de datos de Boston Housing, el modelo inicial gasta aproximadamente 19.8ms por lote, mientras que el modelo diferencialmente privado gasta alrededor de 30.0ms, lo que es un costo general muy razonable (+ 50%) para una característica como la privacidad. Una última observación que podemos hacer es que la convergencia es mucho más lenta con DP habilitado. El MSE mantiene un valor en el rango de 500 en una primera fase de 50 muestreos. Luego, el MSE comienza a disminuir y alcanza constantemente un valor de 10-50 MSE. Dos razones pueden explicar este comportamiento: primero, el recorte de gradiente reduce la eficiencia de las actualizaciones de las últimas capas, y en segundo lugar, el ruido gaussiano interfiere con las actualizaciones sugeridas por los gradientes que son, por lo tanto, eficientes. Tenga en cuenta que aumentar el límite para el recorte de gradiente también aumenta la varianza del ruido gaussiano.

Conclusiones.

Hemos introducido un framework de aprendizaje federado preservado de la privacidad construido sobre PyTorch. El diseño se basa en cadenas de tensores que se intercambian entre trabajadores locales y remotos. Nuestras implementaciones de tensor soportan los comandos de la API de PyTorch y combinan las funcionalidades de MPC y DP con el mismo framework.

Todavía hay muchos problemas que abordar, a la vanguardia de los cuales está disminuyendo el tiempo de entrenamiento. La eficiencia aún no se ha abordado, pero la sobrecarga actual sugiere que hay espacio para mejorar en un marco de Python puro en oposición a las API de Python de alto nivel que se combinan con las bibliotecas de bajo nivel optimizadas. Otra preocupación tiene que ver con asegurar el MPC para asegurarse de detectar y anular los intentos malintencionados de corromper los datos o el modelo.

Libro: Blockchain – ICBC 2018 First International Conference, Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA, June 25–30, 2018, Proceedings

La Conferencia Internacional sobre Blockchain (ICBC) tiene como objetivo proporcionar un foro internacional para que tanto los investigadores como los profesionales de la industria intercambien los últimos avances fundamentales en las tecnologías de vanguardia y las mejores prácticas de blockchain, así como los estándares emergentes y los temas de investigación. Eso definiría el futuro de blockchain.

Los temas de interés incluyen, entre otros, nueva arquitectura de blockchain, construcciones de plataforma, desarrollo de blockchain y tecnologías de servicios de blockchain, así como estándares, y ciclo de vida de innovación de servicios de blockchain que incluyen modelado empresarial, consultoría de negocios, creación de soluciones, orquestación de servicios, optimización de servicios, gestión de servicios, marketing de servicios e integración y gestión de procesos de negocio.

Research Track: Blockchain Research

Using Ethereum Blockchain in Internet of Things: A Solution for Electric Vehicle Battery Refueling

Haoli Sun, Song Hua, Ence Zhou, Bingfeng Pi, Jun Sun and Kazuhiro Yamashita

La tecnología de Internet de las cosas (IoT) se ha vuelto más y más popular recientemente. Sin embargo, debido a los recursos limitados de los dispositivos de IoT y la arquitectura centralizada del sistema, algunos problemas graves siguen siendo difíciles de resolver, como la sobrecarga del servidor centralizado, el punto único de falla y la posibilidad de un uso malicioso de la información personal. Gracias al Blockchain muchos de los problemas que causa la arquitectura centralizada. Algunas de las características de Blockchain que sirven en este entorno son el mecanismo de consenso, la comunicación de igual a igual(peer-to-peer), la implementación de la confianza sin un tercero de confianza y la transacción basada en un contrato inteligente.

En este capítulo del libro se presenta una solución IoT empleando Ethereum Blockchain, en concreto se presenta un sistema de recarga de baterías para vehículos eléctricos en el que se adopta el enfoque de intercambio de baterías. También explica la racionalidad de la solución mediante experimentos y compara la solución con otras soluciones de IoT basadas en blockchain. La conclusión es que esta solución blockchain-IoT es adecuada para varios escenarios de IoT y evita los problemas causados por los recursos limitados de los dispositivos IoT.

Some blockchain based IoT solutions

IoT significa Internet a la que se conectan "cosas" (dispositivos, sensores, actuadores, etc.). Los datos del mundo físico son recopilados por sensores, entregados a través de Internet. Los usuarios (o la unidad de control) de los sistemas de IoT pueden analizar los datos recopilados para descubrir tendencias o patrones, o cambiar el estado de los actuadores en función de los datos.

Debido a la potencia informática, el almacenamiento y el ancho de banda de red limitados de los dispositivos IoT y la arquitectura centralizada del sistema, algunos problemas graves siguen siendo difíciles de resolver.

Los problemas de IoT que pueden resolverse mediante blockchain son principalmente los problemas causados por la arquitectura centralizada de los sistemas actuales de IoT. Algunos de los temas son:

- Fallas del servidor central: las fallas pueden ser causadas por fallas de software o ataques.
- Un solo punto de falla: un dispositivo comprometido puede causar fallas en todo el sistema.
- Falta de privacidad: la información personal guardada en el servidor central puede ser abusada.

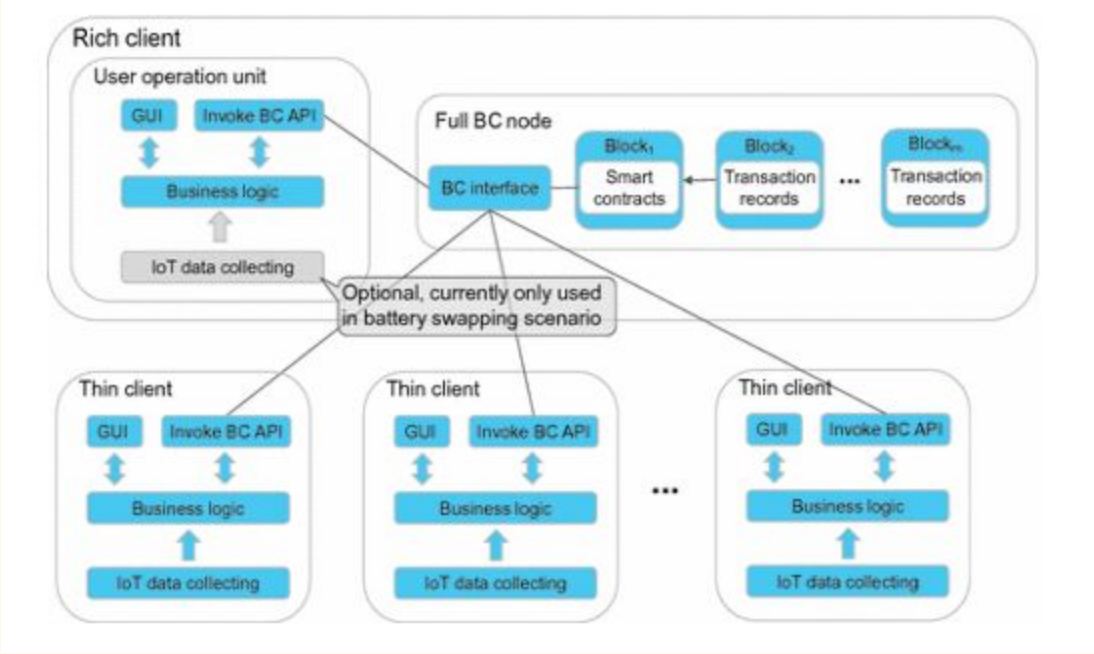
Blockchain puede resolver los problemas anteriores porque su arquitectura descentralizada puede evitar fallas en el servidor central o un punto único de falla, y su cifrado de clave pública-privada puede proporcionar seudonimia para proteger la información personal en cierta medida. Sin embargo, los problemas causados por los recursos limitados de los dispositivos IoT siguen siendo difíciles de resolver: por un lado, la mayoría de los dispositivos IoT no tienen recursos suficientes para soportar PoW, por otro lado, si un dispositivo no es un nodo de blockchain Red, su seguridad e identidad es difícil de garantizar.

Ethereum Blockchain Based Rich-Thin-Clients IoT Solution

Se diseñó una arquitectura de clientes “finos”(thin) para resolver el dilema mencionado entre los recursos limitados de los dispositivos de IoT y las preocupaciones por la arquitectura centralizada. Los thin clients, que son responsables de la interacción del usuario y la recopilación de datos de IoT, pueden considerarse como dispositivos de IoT con recursos limitados; Los clientes ricos(rich clients), que son clientes ligeros(thin clients) más nodos de cadena de bloques completos, pueden considerarse como dispositivos que tienen recursos mayores o iguales que las computadoras personales. Se utilizó una red privada de cadenas de bloques Ethereum, construida por los autores de este paper como su sistema de cadenas de bloques subyacentes.

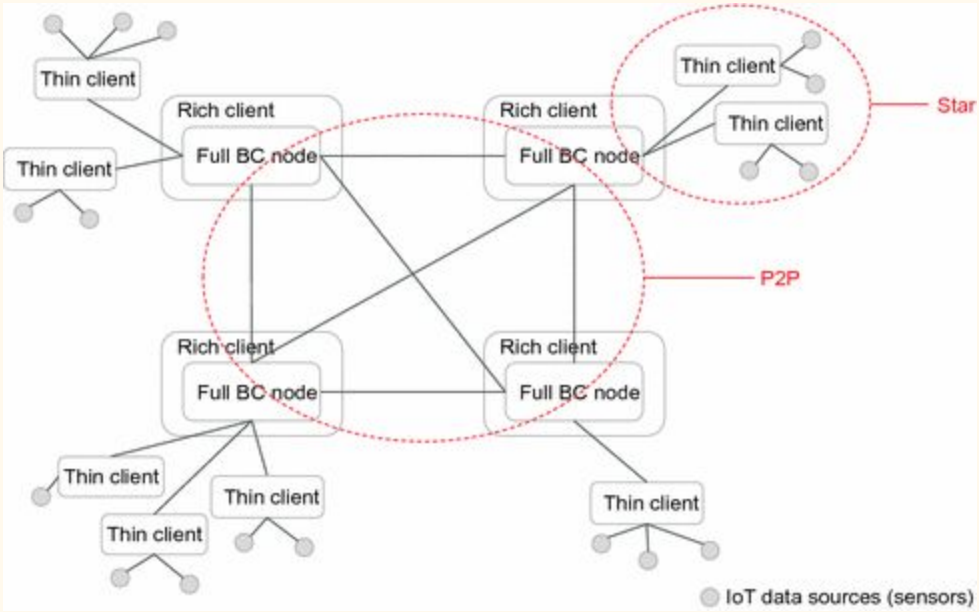
El cliente enriquecido y el cliente ligero pueden proporcionar una GUI para los usuarios, invocar las API de blockchain (BC) a través de la interfaz de BC que se implementa en un cliente rico, definir lógicas de negocios y recopilar datos de IoT (opcional para clientes ricos), pero solo un cliente rico contiene un nodo de BC completo que puede realizar la minería y contiene todos los registros de transacciones del sistema de BC.

Rich-Thin-Clients architecture



Cada cliente enriquecido contiene un nodo Ethereum BC completamente funcional que puede realizar la minería y ejecutar el algoritmo de consenso de PoW con otros nodos Ethereum BC. Los clientes ricos forman una red P2P, al igual que los nodos públicos de Ethereum BC. Los clientes ligeros conectados a un mismo cliente rico forman una topología en estrella con el cliente rico. Dado que solo los clientes ricos con recursos altos realizan un algoritmo de minería y consenso, nuestra red debe ser similar a la red pública de Ethereum BC, por lo que se puede resolver el dilema entre los recursos limitados de los dispositivos de IoT y las preocupaciones por la arquitectura centralizada.

Overall system architecture



Implementation of Ethereum Based Cyber-Physical Battery Refueling System

Repostaje de baterías para vehículos eléctricos.

Debido al desarrollo de las tecnologías de baterías y la conciencia ambiental, las tecnologías EV se han desarrollado rápidamente en las últimas décadas. Con la utilización a gran escala de tecnologías EV, la emisión de gases de efecto invernadero puede reducirse y la utilización de la energía puede ser más eficiente. Sin embargo, el repostaje de la batería sigue siendo un problema que no se ha resuelto bien. Hay tres métodos principales de repostar de la batería EV: carga de corriente alterna (AC), carga de corriente directa (DC) e intercambio de batería. La carga de CA se puede adoptar en el garaje de un propietario de vehículos eléctricos. Es conveniente pero requiere mucho tiempo. Costará más de ocho horas cargar completamente

una batería EV agotada mediante la carga de CA. La carga de CC puede ser proporcionada por la estación de carga. Costará 1–2 h cargar completamente una batería EV agotada por la carga de CC. Sin embargo, la carga de CC puede dañar la batería EV debido a la gran potencia. El cambio de batería es el que consume menos tiempo entre los tres métodos de repostaje de la batería del EV. Solo le costará unos minutos cambiar una batería agotada por una completamente cargada por una estación de intercambio de baterías [12].

En el trabajo anterior de los autores de este paper, se propuso un sistema de intercambio de baterías con EV basado en blockchain (en forma de una aplicación web) para evaluar las baterías que se intercambiarán de manera justa con los contratos inteligentes y para administrar la información de las baterías, como su fabricante, marca. , capacidad de potencia, precio e historial de repostaje.

En realidad, es un escenario de IoT utilizar nuestro sistema de intercambio de baterías EV basado en blockchain anterior en una situación real, ya que las estaciones de intercambio de baterías y los EV deben estar conectados a Internet, y la interacción ciber física de la información de la batería debe estar involucrada.

Arquitectura del sistema de intercambio de baterías.

Se implementa el sistema de intercambio de baterías basado en la propuesta de arquitectura de clientes ligeros - ricos(rich-thin-clients). La imagen muestra cómo se compone el sistema.

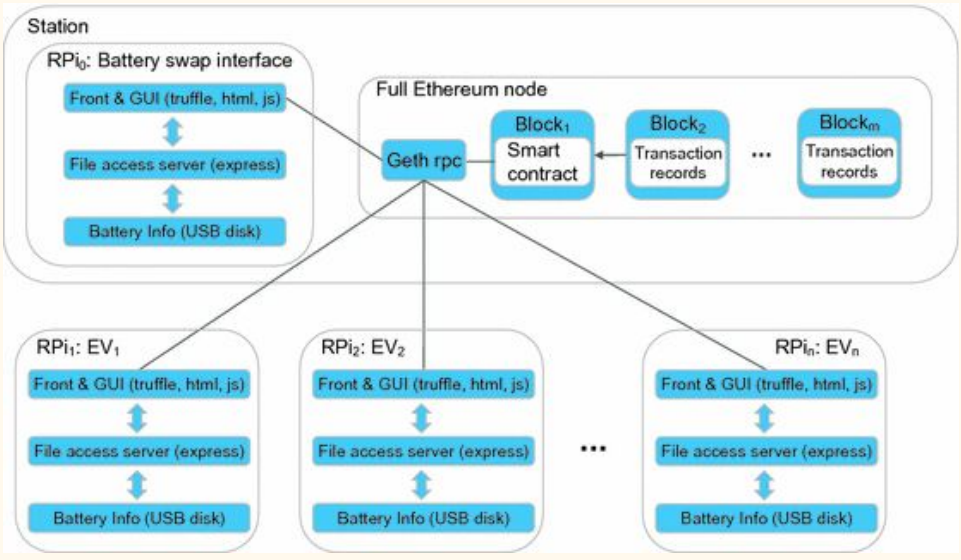


Imagen. Sistema de intercambio de baterías

Raspberry Pi (RPi) [24] es usada como el hardware de un thin client, cada thin client representa un EV. En cada EV, se utiliza "truffle" [25] para invocar el servicio de Remote Procedure Call(RPC) de blockchain, y se usa un servidor local "express" [26] para controlar la interacción ciber-física. Utilizamos discos USB que se pueden conectar a RPi para representar baterías reales, la información de cada batería se almacena en un archivo en cada disco USB correspondiente. La imagen de abajo muestra la información estática y la información dinámica de un archivo de información de batería típico.

```
{
    "batteryID": 1,
    "ownerAddress": "",
    "filePath": "/media/usb0/battery_information.json",
    "staticInfo": {
        "brand": "Samsung",
        "maxChargingCount": 200,
        "maxDischargingCount": 200,
        "maxYearLimited": 20,
        "maxChargingTotalTime": 2000,
        "maxDischargingTotalTime": 2000,
        "manufactureYear": 2017,
        "manufactureMonth": 11,
        "manufacturePrice": 200
    },
    "dynamicInfo": {
        "price": 164,
        "energy": "20",
        "SOC": "100",
        "chargingCount": "1",
        "dischargingCount": "1",
        "chargingTotalTime": "2",
        "dischargingTotalTime": "2"
    }
}
```


Imagen. Ejemplo de archivo de información de batería.

Una estación consta de una interfaz de intercambio de batería (un RPi funciona como un EV) y un nodo Ethereum completo. Usamos "Geth" [27] como la interfaz de línea de comandos para ejecutar nodos Ethereum completos y proporcionar el servicio RPC para invocadores.

Smart Contracts.

Tres contratos inteligentes para administrar la máquina de estados del sistema de intercambio de baterías:

- El contrato inteligente "**BatteryProcess**" se utiliza para operar y almacenar información de la batería. Almacena la información estática de las baterías y la información dinámica. La información estática se determina desde que se produjo una batería y no se puede modificar, como la marca, el tiempo de producción, el precio de fabricación, etc. La información dinámica se utiliza para mostrar el estado de una batería, como los tiempos de carga, el estado de carga (SOC), el precio, la cuenta del propietario, etc.
- El contrato inteligente "**BalanceProcess**" se utiliza para gestionar la transferencia de valor entre cuentas. Dado que no es racional exigir que todos los usuarios de EV tengan Ehter [4], definimos un token llamado ***E-coin*** como la moneda en nuestro sistema.
- El contrato inteligente "**BatteryInterface**" proporciona interfaces API para tres tipos de usuarios de terminales: operador de estación, propietario de EV y super cuenta. Los propietarios de EV pueden descargar la batería en su propio EV y pueden enviar una solicitud de cambio de batería a una estación de batería y esperar la confirmación. Los operadores de la estación son los empleados de la estación de la batería. Pueden cargar, descargar y reciclar las baterías que pertenecen a la estación de baterías, y pueden aprobar o rechazar una solicitud de intercambio de baterías enviada por los propietarios de EV. Super cuenta es el administrador del sistema de este sistema de intercambio de baterías, puede crear otros tipos de cuentas, otorgar monedas electrónicas, definir el GAS requerido para invocar contratos inteligentes, etc.

Diagrama de flujo del sistema.

La imagen de abajo muestra cómo funciona el sistema. Al principio, el EV tiene una batería agotada que pertenece a la marca TOY, y la estación tiene dos baterías completamente cargadas que pertenecen a la marca SUM y BYD, respectivamente. Luego, el propietario del EV accede a la GUI del sistema de intercambio de baterías y envía una solicitud de intercambio para cambiar su batería TOY por la batería BYD de la estación. Una vez que el operador de la estación confirma la solicitud de intercambio, se cambia la información de propiedad almacenada en blockchain. Sin embargo, en este momento, las baterías "reales" (discos USB) correspondientes aún no se han intercambiado, por lo que se advierte la inconsistencia entre la información

cibernética y la información física. Finalmente, después de cambiar las baterías correspondientes, ya no hay alerta y se puede verificar el estado actual de la batería.

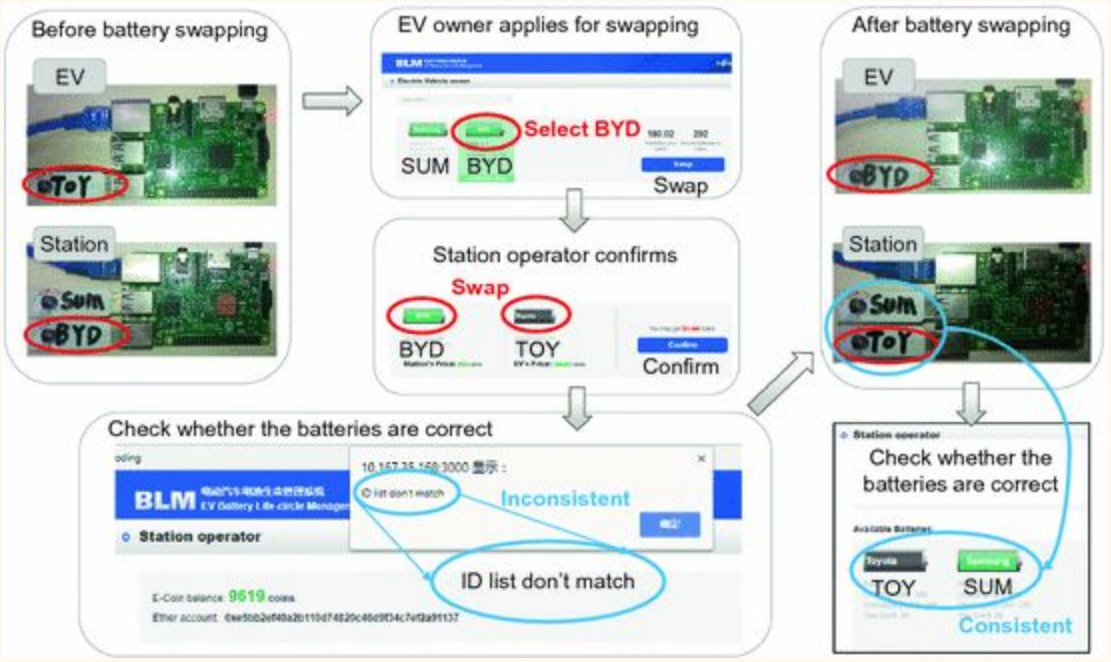


Imagen. Diagrama de flujo del sistema.

Conclusión.

Este capítulo propone una solución de IoT basada en la cadena de bloques Ethereum, presenta un sistema de intercambio de baterías implementado basado en la solución y experimentos para probar los índices de rendimiento del sistema, y compara esta solución con otras soluciones de IoT basadas en la cadena de bloques. Se utiliza Ethereum (un sistema de blockchain que soporta contratos inteligentes) para resolver los problemas causados por la arquitectura tradicional de IoT centralizada. Y al adoptar una arquitectura rich-thin-clients, se puede resolver el dilema entre los recursos limitados de los dispositivos de IoT y las preocupaciones por la arquitectura centralizada. Además, el uso de esta solución no se limita a la aplicación de intercambio de batería, otras aplicaciones de IoT como los sistemas de intercambio de datos de sensores u otras propiedades digitalizadas también pueden beneficiarse de esta arquitectura propuesta.

A Simulation Approach for Studying Behavior and Quality of Blockchain Networks

Bozhi Wang , Shiping Chen, , Lina Yao, Bin Liu, Xiwei Xu, and Liming Zhu

Blockchain ofrece algunas capacidades / características únicas, como descentralización, confiabilidad e inmutabilidad, que permitieron a las personas establecer confianza y realizar transacciones sin depender de un tercero confiable. Hasta ahora, Blockchain está comenzando a mostrar sus potenciales en muchos dominios interesantes, como el pago transnacional, el almacenamiento distribuido, la procedencia de los alimentos, etc.

Antes de que Blockchain pueda ser adoptado ampliamente en otras áreas, todavía tiene varios problemas por resolver. Primero, el mecanismo actual de minería (PoW-Proof of Work) de Blockchain está desperdiciando una gran cantidad de poder de cómputo en el cálculo, que es necesario para PoW pero no tiene sentido y es costoso. Segundo, cada nodo en la red tiene un libro completo. A medida que pasa el tiempo, el libro mayor será cada vez más grande. Y cuando un minero verifica una transacción, debe rastrear todas las transacciones históricas registradas en la cadena de bloques. El problema de rendimiento es cada vez peor. Entonces, aunque Blockchain es un sistema anónimo, todas las transacciones están disponibles públicamente, lo que puede causar problemas de privacidad. Por último, en la red actual de Bitcoin, una estrategia de seguridad común es esperar seis bloques para confirmar las transacciones en el último bloque, que dura alrededor de una hora, lo que limita significativamente la adopción y las aplicaciones de las tecnologías actuales de Blockchain.

En este capítulo, se propone un enfoque de simulación para estudiar las redes Blockchain a gran escala. Primero, identificamos los requisitos clave para el software de simulación para implementar los protocolos de PoW. En segundo lugar, recopilamos y definimos una serie de métricas de rendimiento para cuantificar la calidad de Blockchain (QoB). Luego, demostramos la idea propuesta utilizando una herramienta de simulación simple para duplicar un protocolo simplificado de Bitcoin PoW usando diferentes configuraciones. El caso de estudio que se plantea muestra que es posible y práctico estudiar una red Blockchain a gran escala utilizando un software de simulación.

Parameters and QoS Metrics for a Blockchain Network.

Podemos definir y simular una red Blockchain usando estas métricas. Ignoramos los bloques huérfanos y el retardo de red en el simulador. Se fijará en la investigación futura.

- **TBN (Número de Bloque Total)**. La cantidad de bloques que se han extraído en un período de tiempo específico
- **ABS (Tamaño promedio del bloque)**. El tamaño de bloque promedio en MB.
- **BCT (Block Commit time**). El tiempo promedio necesario para enviar un bloque a la cadena principal desde su creación.
- **TPB (Transacciones por Bloque)**. El promedio de transacciones por bloque.
- **ATS (Tamaño de transacción promedio)**. El tamaño de transacción promedio en bytes.
- **TCT (Tiempo de Confirmación de Transacción)**. El tiempo promedio para que una transacción sea aceptada en un bloque extraído.
- **TPD (Transacciones por día)**. El número de transacciones diarias confirmadas.
- **MS (Tamaño Mempool)**. El número total de transacciones en espera de ser confirmado.

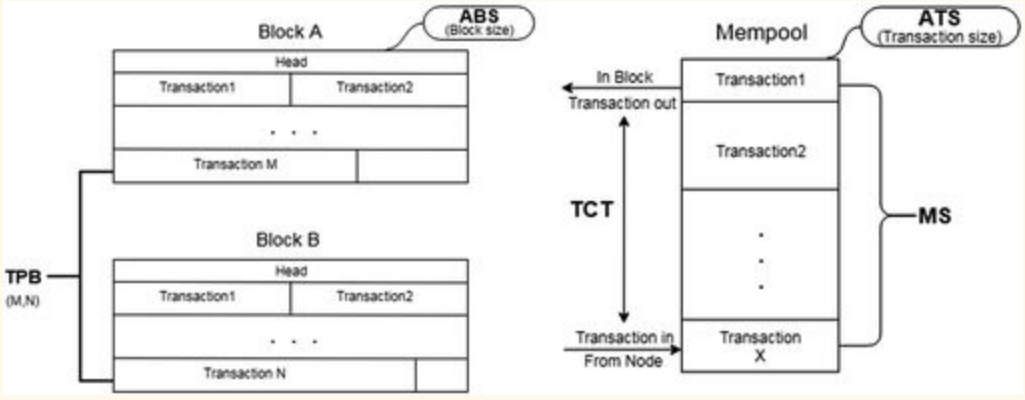


Imagen. Métricas QoS para una red Blockchain.

Requirements for Blockchain Simulation

Hay varios requisitos que debemos considerar, como se muestra a continuación:

- **Simulación de tiempo:** la escala de la Blockchain aumenta con el tiempo. El tiempo de minería, el tiempo de transacción y el retraso de la red afectan mucho el rendimiento del sistema.
- **Difusión:** En realidad, usamos multidifusión para realizar la comunicación IP. En la simulación, resulta ser una situación ideal. Así que tenemos que transmitir todas las transacciones.
- **Impulsado por eventos:** un minero puede cambiar su estado una vez que ocurre algún evento durante la extracción. El simulador debe ser controlado por eventos para ajustarse a este patrón.
- **Procesamiento de mensajes:** una vez que un minero encuentra un nuevo bloque, el minero emite su bloque, al mismo tiempo que otros nodos reciben el nuevo bloque (que se empaqueta como un mensaje) y hacen su propia respuesta. Así que el software debería soportar el procesamiento de mensajes.
- **Concurrencia:** la red Blockchain se compone de muchos que hacen cosas diferentes pero similares (extracción, verificación, recepción o envío de mensajes) al mismo tiempo. También se requiere concurrencia.

Results of Simulate Blockchain Using SimPy

Después de realizar alguna simulación con diferentes configuraciones, los resultados son:

En la Fig. 10, como el número de transacciones por día y el tamaño del bloque se mantienen, solo cuando el tamaño de la transacción es de 100B a 2000B, las transacciones completan el bloque. Cuando la transacción es pequeña, se pueden registrar más transacciones en un bloque. Una vez que no haya suficientes transacciones, el bloque no se llenará. En el sistema real, la extracción de un bloque cuesta mucho, por lo que queremos que contenga la mayor cantidad de información posible.

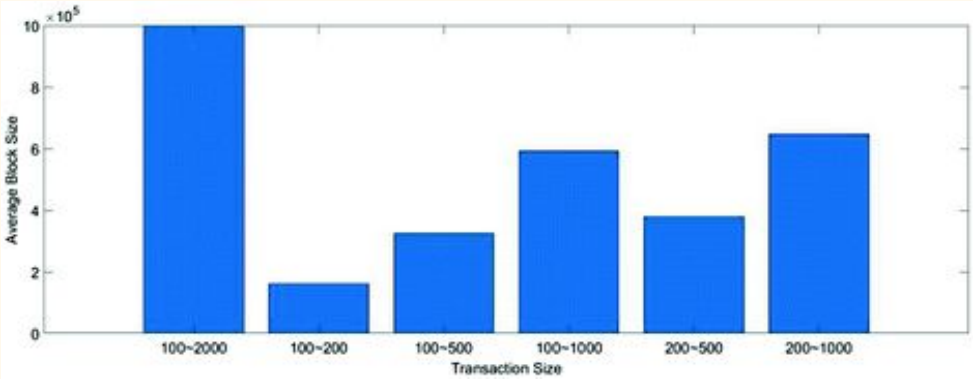
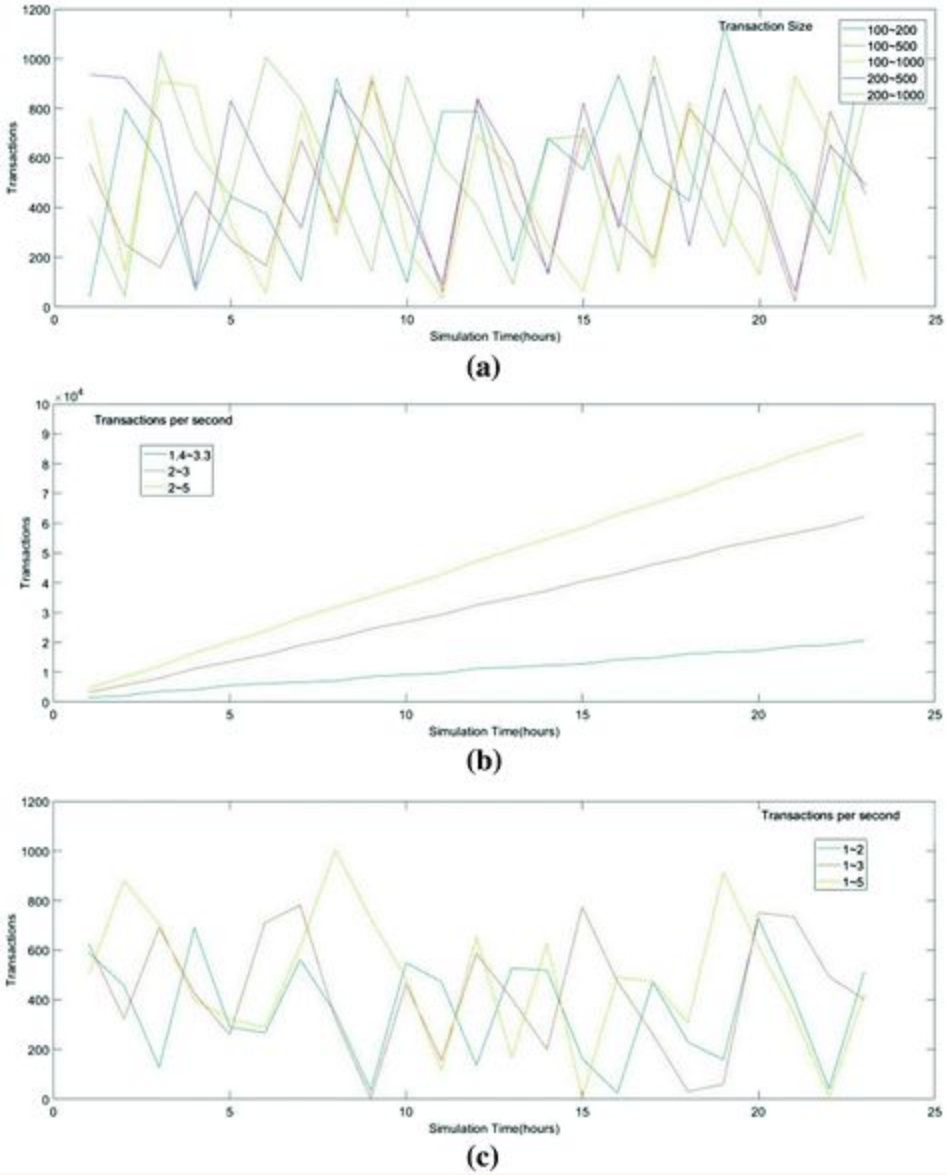


Imagen. ABS(cambio del tamaño de la transición)

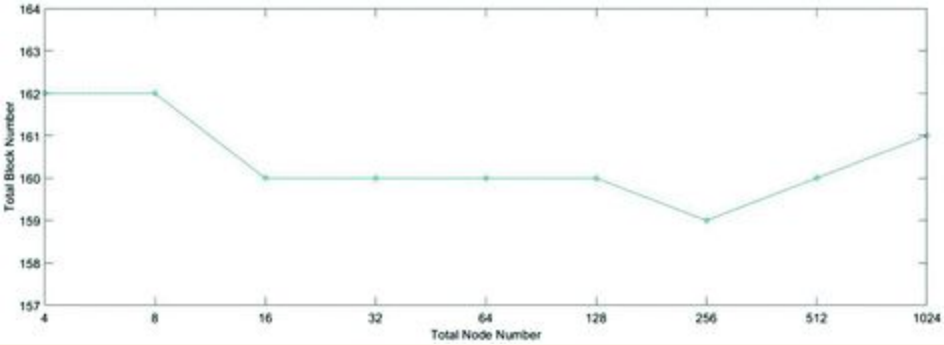
En la Fig. 11 (a), muestra detalles durante un día que el tamaño de mempool se mantiene en un nivel bajo. Las transacciones no necesitan esperar mucho tiempo para establecerse en un bloque. También en la Fig. 11 (b) y (c), cuando la transacción por segundo cambia, el tamaño del mempool puede mantenerse en un nivel bajo o ir directamente al alza. Una vez que el tamaño de mempool sea alto, el sistema será cada vez más redundante. Al igual que en la Fig. 13, el tiempo de confirmación de transacción aumenta con el tiempo. En la red real, el número de transacción depende de diferentes eventos, que tienen horas pico y no pico. Así como el tamaño de la transacción. En investigaciones adicionales, probaremos la red con grandes transacciones en un tiempo limitado y la capacidad que la red podría resolver con el Mempool apilado.



(a): tamaño de Mempool (cambia tamaño de transacciones) (b): tamaño de Mempool (cambia transacción por segundo) (c): tamaño de Mempool (cambia transacciones por segundo)

En la Fig. 12, el número de nodos tiene poco impacto en el rendimiento de Blockchain. Durante nuestra simulación, el nodo podría ser de hasta 20000. En realidad, el aumento del número de nodo le dará al sistema más poder de cómputo, lo que puede causar un tiempo de extracción más corto. Una vez que el tiempo de extracción está fuera del rango, el sistema mejorará la dificultad de cálculo, lo que finalmente mantiene limitado el tiempo de extracción. En nuestra

simulación, el tiempo de minería al azar está dentro de un rango. Así que el aumento del número de nodo solo causa algo de presión en la memoria.



Conclusión.

En este capítulo, recopilamos y definimos una serie de métricas de rendimiento clave para cuantificar la Calidad de Blockchain (QoB). También utilizamos una herramienta de simulación simple para simular un protocolo simplificado de prueba de trabajo de cadena de bloques (PoW) dentro de diferentes argumentos y nuestras observaciones. Los resultados muestran su relación entre la configuración básica y la Calidad de Blockchian. Muestra que es posible y práctico utilizar un enfoque de simulación para estudiar redes Blockchain con diferentes tamaños y protocolos de red.

A Design of Digital Rights Management Mechanism Based on Blockchain Technology

Zehao Zhang and Li Zhao

La gestión de derechos digitales (DRM) se ha utilizado ampliamente en la protección de contenido digital en la actualidad y ha hecho una gran contribución a la protección de contenido digital. Sin embargo, la tecnología DRM tradicional tiene varios inconvenientes, como la centralización, la falta de transparencia de la información de copyright y la información de transacción. Los servidores centralizados son vulnerables a ser atacados y la información opaca no es fácil de usar. La tecnología blockchain que ha surgido en los últimos años tiene las ventajas de la descentralización, el mantenimiento colectivo, la seguridad y la confiabilidad. Puede ser una gran solución a los problemas anteriores. En este artículo, proponemos un diseño de mecanismo DRM basado en tecnología blockchain. Registramos la información de la transacción de derechos de autor y la información de la licencia en el blockchain para que la información sea transparente y segura. Utilizamos el contacto inteligente para garantizar la confiabilidad de las transacciones de derechos de autor y emitir licencias automáticamente, lo que elimina la necesidad de servidores centralizados para verificar identidades y emitir licencias. Nuestro mecanismo permite a los propietarios de derechos de autor establecer precios para las diferentes reglas de uso de contenido que deseen. Los clientes eligen las reglas de uso que les gustaría comprar de manera flexible. También diseñamos una estructura de licencia basada en blockchain, que está cerca de los estándares DRM actuales y es fácil de promover.

Arquitectura DRM

La gestión de derechos digitales (DRM) es un tipo de sistema de gestión desarrollado para permitir una distribución segura y, lo que es más importante, para deshabilitar la distribución ilegal de contenido de pago. Las tecnologías DRM se están desarrollando como un medio de protección contra la piratería en línea de material comercializado comercialmente. La arquitectura de alto nivel y los componentes principales de un sistema DRM típico se muestran en la Fig. 2.

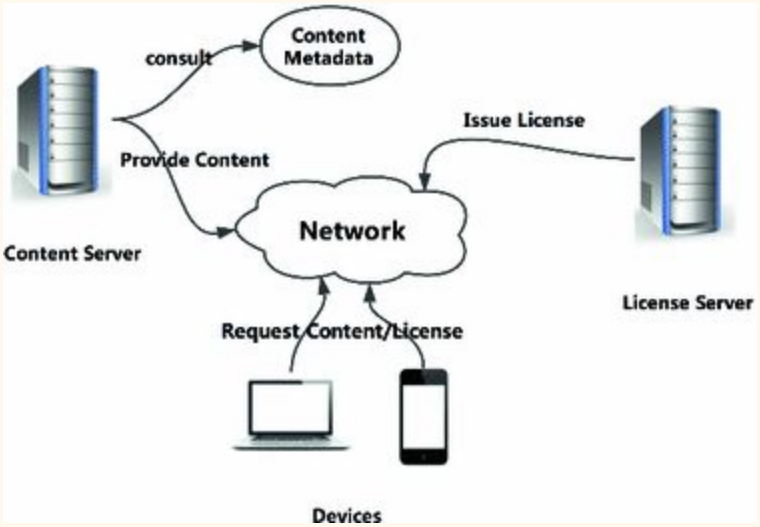


Imagen. Arquitectura de alto nivel de un sistema DRM típico.

DRM ha hecho grandes progresos en el mundo. Sin embargo, la tecnología DRM tradicional tiene varias desventajas debido a su centralización. Los servidores centralizados son vulnerables a ser atacados y la información opaca no es fácil de usar. Se cree que la tecnología blockchain es una buena solución para estas desventajas. Desde la aparición de una gran tecnología como blockchain, no ha habido un conjunto de mecanismos DRM adecuados combinados con la tecnología blockchain.

DRM basado en tecnología blockchain

Con esta nueva arquitectura se registra tanto la información de transacción de derechos de autor como la información de licencia en la cadena de bloques pública. Por un lado, se utilizan los contratos inteligentes para garantizar la confiabilidad de las compras de derechos de autor y registrar las transacciones en la cadena de bloques. No se necesita ninguna institución central. Por otro lado, se hace uso de contratos inteligentes que emiten licencias automáticamente y registramos las licencias en la cadena de bloques. De esta manera, tanto los proveedores de contenido como los consumidores pueden consultar y verificar la información de copyright en cualquier momento y, además, nadie puede falsificar la información de copyright.

La imagen de abajo muestra el prototipo del mecanismo DRM basado en blockchain. Los proveedores de contenido, los consumidores y los anunciantes utilizan clientes de blockchain para interactuar con los nodos. Los nodos son responsables de funciones básicas como la interacción con contratos inteligentes y la producción de bloques. El contenido digital solo

puede ser utilizado por el cliente. Las reglas y claves utilizadas se obtienen de la licencia. Esto evita el uso fraudulento de contenidos digitales.

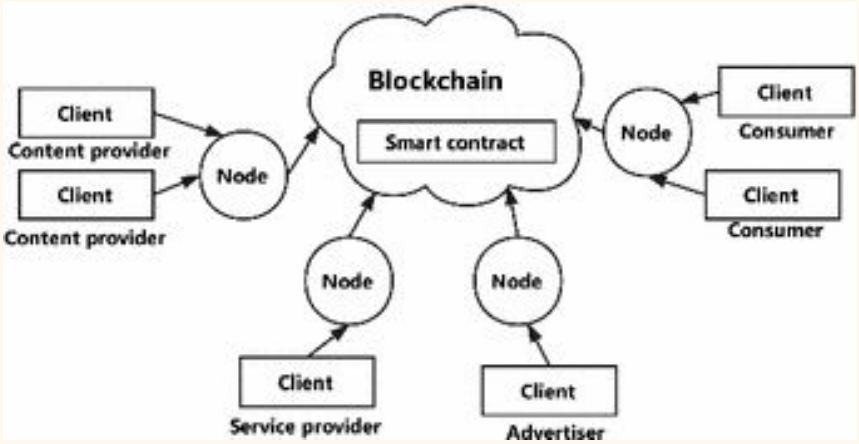


Imagen. Mecanismo DRM basado en Blockchain

Conclusión.

En este capítulo, se diseña un nuevo mecanismo DRM basado en la tecnología blockchain. Utilizan las características descentralizadas, seguras y creíbles de la tecnología blockchain para compensar la deficiencia de la tecnología DRM tradicional centralizada. Registran las transacciones de derechos de autor y la información de la licencia en el blockchain, lo que los hace seguros, confiables y transparentes. Al mismo tiempo, utilizan contratos inteligentes para garantizar la confiabilidad de la transacción y la emisión de licencias. No hay necesidad de información interactiva entre el propietario de los derechos de autor y el consumidor, y tampoco necesitamos un servidor de licencias centralizado para emitir licencias. De esta manera, simplifican el proceso y ahorramos los costos. La estructura de licencia basada en la tecnología de blockchain que propusimos está cerca de los estándares actuales de DRM, que es adecuado para la promoción.

Un defecto del trabajo puede ser que los pares(peers) de nuestra plataforma de cadena de bloques tengan que ser altamente potentes para lidiar con una alta adquisición de claves concurrentes.

InfiniteChain: A Multi-chain Architecture with Distributed Auditing of Sidechains for Public Blockchains

Gwan-Hwan Hwang , Po-Han Chen, Chun-Hao Lu, Chun Chiu, Hsuan-Cheng Lin and An-Jie Jheng

InfiniteChain propone un tipo totalmente nuevo de auditoría distribuida, así como un método para la operación de cadenas múltiples que supera los cuellos de botella encontrados hasta el momento por las tecnologías de cadena de bloques más avanzadas y su implementación en aplicaciones comerciales. Las transacciones se procesan primero fuera de la cadena principal y los árboles de Merkle de índice, y luego se emplean auditorías distribuidas para realizar pruebas de fraude para estas transacciones en la cadena lateral. Sus ventajas incluyen un gran ancho de banda de las transacciones, la protección de la privacidad de las transacciones y la fusión con los escenarios comerciales centralizados existentes. La implementación y los resultados experimentales demuestran la viabilidad del sistema propuesto.

Arquitectura Multi-chain

La arquitectura de la cadena de bloques de cadena múltiple propuesta se muestra en la imagen de abajo. Una cadena múltiple es un modelo operativo conjunto que consta de la cadena de bloques principal y varias cadenas laterales. En general, las transacciones que no necesitan ser procesadas rápidamente, como las transacciones en criptomonedas o los registros de contratos individuales, primero se envían directamente a la red P2P y luego se vinculan a la cadena principal mediante nodos que se han convertido en productores de bloques.

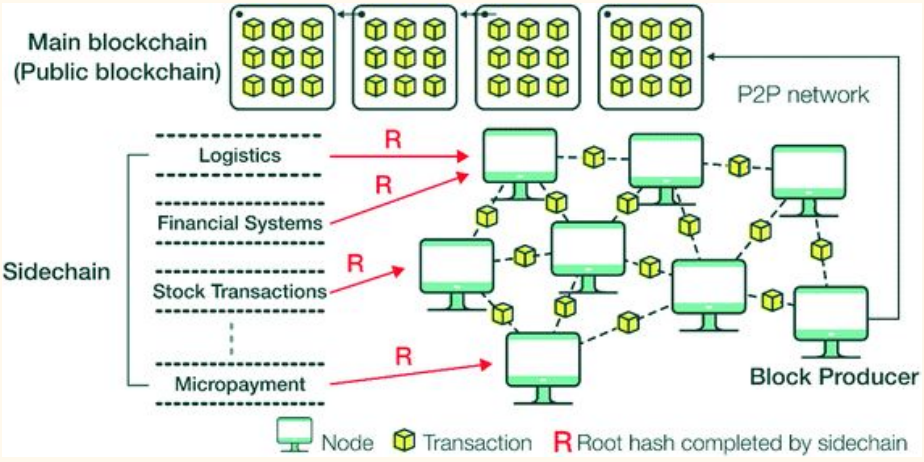


Imagen. Arquitectura Multi-chain.

Sin embargo, las transacciones de alto volumen, o aquellas que requieren emparejamiento centralizado, primero se procesan en una cadena lateral. Luego se genera un valor hash para las transacciones y se envía a un nodo en la red P2P y se vincula a la cadena principal. La cadena lateral se ejecuta a una alta velocidad y acumula una gran cantidad de transacciones después de un cierto tiempo. El nodo de auditoría responsable de la operación descentralizada de la cadena lateral genera un valor hash y el código de identificación correspondiente, que luego se envía a la cadena principal.

El mantenimiento y el funcionamiento de la cadena principal es el mismo que el funcionamiento y la gestión de las cadenas de bloques públicas ordinarias. Las operaciones de la cadena lateral se inician mediante aplicaciones de la industria (por ejemplo, plataformas de agentes de transacciones, corredores profesionales, bancos de inversión, compañías de valores, auditores, tasadores, abogados, desarrolladores de herramientas). Para el mercado y el desarrollo de negocios, las distintas cadenas laterales se administran y operan para tipos de negocios individuales. Las cadenas laterales deben sincronizar regularmente su información con la cadena principal para evitar la falsificación o manipulación de datos.

Conclusión.

Los sistemas de aplicación descentralizados basados en tecnologías de blockchain recién están comenzando a entrar en nuestra vida cotidiana. Sin embargo, los expertos han señalado algunos cuellos de botella en la tecnología básica. Si alguno de estos problemas sigue sin resolverse, entonces el sueño de que las cadenas de bloques se conviertan en máquinas de confianza será solo eso, un sueño. La cadena de bloques se limitará a una plataforma para la criptomoneda minera y comercial, o solo se utilizará en un número limitado de escenarios de aplicaciones. Se propone una arquitectura de cadena múltiple que emplee auditorías distribuidas para realizar pruebas de fraude en la cadena lateral. Una prueba de fraude eficiente y eficaz resuelve problemas. La prueba criptográfica generada a partir de un árbol Merkle índice es lo suficientemente pequeña como para ser validada en un contrato de blockchains públicas.

Research Track: Smart Contracts

A Method to Predict the Performance and Storage of Executing Contract for Ethereum Consortium-Blockchain

Huijuan Zhang, Chengxin Jin and Hejie Cui

Ethereum, como sucesor de Bitcoin, establece un contrato inteligente de Turing-complete en blockchain para realizar aplicaciones distribuidas DApps. Mientras tanto, el diseño basado en la cuenta de Ethereum proporciona comodidad para el acoplamiento de modelos de negocios existentes (en comparación con el modelo UXTO). Así, muchas empresas eligen Ethereum para construir su sistema de cadena de bloque o desarrollarlo en él (por ejemplo, EEA) basándose en dos puntos. Como resultado, en comparación con la cadena de bloques pública de Ethereum, la cadena de bloques de Ethereum utiliza principalmente la transacción para ejecutar el contrato en lugar de realizar una transferencia de criptomoneda ETH. Por lo tanto, este capítulo del libro se enfoca en el desempeño y almacenamiento de la ejecución del contrato de Ethereum.

Sin embargo, los resultados de las pruebas muestran que cuando el volumen de transacciones alcanza una escala determinada, el rendimiento de ejecución de Ethereum se reducirá significativamente y se ocupará un gran espacio de almacenamiento. (por ejemplo, cuando el límite de la tasa de generación de bloques se modificó a un bloque por segundo, el TPS de un contrato, que es de aproximadamente 200 al inicio, se reduciría a 100 a medida que el volumen de transacciones alcance un millón). Para las empresas, predecir el rendimiento y el almacenamiento prospectivos son indicadores importantes para tomar decisiones técnicas y también permite a las empresas prepararse para el hardware, el monitoreo y los planes con anticipación. Por lo tanto, es necesario predecir el rendimiento prospectivo y el almacenamiento del sistema en Ethereum blockchain en función de la escala comercial.

En la cadena de bloques de Ethereum pública, es imposible predecir la distribución y complejidad del contrato inteligente, ya que cualquiera puede implementar un contrato fácilmente. Como resultado, es difícil estimar con precisión el rendimiento y el almacenamiento en perspectiva. Sin embargo, es posible predecir el rendimiento y el almacenamiento en Ethereum blockchain como resultado de que los participantes son los nodos autorizados; que el contrato inteligente relativamente fijo con complejidad evaluable está determinado por el

modelo de negocio; y que el volumen de transacciones está determinado por la escala del negocio.

El método de predicción propuesto en este capítulo especula el rendimiento y el almacenamiento al analizar la relación entre el volumen de transacciones y el "World State". **"World State" es la parte central de Ethereum**. El sistema de cuentas asigna los datos de estado como forma clave / valor y los almacena en LevelDB a través de esta estructura especial [13]. "World State" se implementa utilizando "el árbol Merkle Patricia modificado (trie)" [4] (en lo sucesivo, MPT). PATRICIA trie (árbol de Patricia) es una **versión optimizada para el espacio de la estructura de datos trie tradicional**, en la que cada nodo con un solo hijo se fusiona con su hijo. Esta estructura de datos fue propuesta por primera vez por Morrison [16] en 1968, y luego fue bien analizada en "El arte de la programación de computadoras" por Knuth [17] en 1973. La parte "Merkle" de la radix trie surge en el hecho de que un factor determinista El puntero criptográfico de un nodo se usa como puntero al nodo, lo que lleva al hecho de que el Ethereum podría rastrear el estado histórico a través de la raíz de "World State" en cualquier encabezado de bloque. El contrato en Ethereum se llama transacción. Dependiendo de la implementación de Ethereum [2], el tiempo consumido por una llamada de transacción para un contrato está determinado principalmente por el tiempo de ejecución de la Máquina Virtual de Ethereum (EVM) y por la modificación del "World State". Mientras tanto, el incremento de datos generado por esta transacción depende de la escala de la transacción y del monto de incremento del "World State". Con el aumento del volumen de transacciones, el "World State" se hace más grande, lo que resulta en un aumento del consumo de tiempo y espacio de datos. En consecuencia, la estimación del rendimiento y el almacenamiento se puede obtener bajo la premisa de averiguar la relación entre el volumen de transacciones y el "World State".

Este capítulo se centra en la relación entre el rendimiento y el incremento de almacenamiento de "World State" una vez que el volumen de transacciones alcanza una escala determinada, y se propone una fórmula de predicción para esta relación. Usando esta fórmula, las compañías podrían predecir el posible consumo de tiempo de ejecución de una transacción y la ocupación del almacenamiento en función del volumen de transacciones. Al final del documento, se presenta una sugerencia para el diseño del contrato en Ethereum consortium-blockchain.

Conclusión.

Cuando las empresas utilizan la cadena de bloques del Ethereum, deben realizar predicciones sobre el rendimiento y el almacenamiento potenciales del sistema si la transacción alcanza una escala determinada. Este documento analiza los problemas principales que afectan el

rendimiento y el almacenamiento de Ethereum es el "World State". De acuerdo con el resultado del análisis de que "World State" está implementado por MPT, la relación entre el rendimiento de MPT o el incremento de almacenamiento y el volumen de transacción n se obtiene para ser log (n). Por otro lado, el "World State" está formado por la capa superior de State Trie y la capa subyacente de Storage Trie. La distribución de los datos sería diferente en función de la organización de los contratos. Las fórmulas se ofrecen para un modelo de negocio para predecir la relación entre el volumen de transacciones y el rendimiento / almacenamiento basado en State Trie. Otros modelos de negocio pueden ser derivados por el mismo método. De esta manera, las compañías pueden deducir el rendimiento y almacenamiento prospectivo de blockchain de acuerdo con sus propios contratos bajo la premisa de que su escala de negocios puede predecirse (volumen de transacciones).

Al mismo tiempo, cuando se puede estimar la escala de la transacción, podemos diseñar adecuadamente los contratos para minimizar el consumo de rendimiento y almacenamiento, de modo que la distribución de datos entre el Estado Trie y Almacenamiento Trie podría alcanzar un punto de inflexión, lo que minimiza la Costes de rendimiento y almacenamiento. Por lo tanto, se sugiere que el desarrollador del contrato pueda estimar el volumen de transacciones futuras con anticipación y asignar adecuadamente los datos en el árbol de estado y el árbol de almacenamiento para lograr la eficiencia y el almacenamiento óptimos al escribir el contrato.

Smart Contract Programming Languages on Blockchains: An Empirical Evaluation of Usability and Security

Reza M. Parizi, Amritraj and Ali Dehghantanha

Blockchain es una nueva tendencia que crece rápidamente desde la comunidad y el mundo empresarial. Una cadena de bloques es teóricamente una lista incremental de registros llamados bloques que se enlazan entre sí y se aseguran mediante criptografía, formando una cadena en el proceso. Las copias de esta cadena se almacenan en varios pares en una red que pueden ver la cadena y sus contenidos. Para agregar un nuevo bloque, un compañero debe encontrar una clave para un patrón aleatorio generado mediante criptografía y verificar el propio bloque. Tan pronto como un igual agrega un nuevo bloque, también transmite esta adición a todos los demás iguales en la red, para que puedan actualizar sus copias de la cadena de bloques.

Blockchain ya ha entrado en una amplia gama de industrias, incluyendo Finanzas, Computación en la nube, Privacidad, Seguridad, etc. Además, en los últimos años, ha surgido una nueva aplicación interesante de blockchain, es decir, contrato inteligente [2]. Los **contratos inteligentes** son contratos de ejecución automática en los que los **términos del acuerdo entre varias partes se escriben directamente en líneas de código.** El código y los acuerdos contenidos en él existen a través de una red de blockchain. Los contratos inteligentes permiten que se realicen transacciones y acuerdos confiables entre partes dispares y anónimas sin la necesidad de una autoridad central, un sistema legal o un mecanismo de cumplimiento externo. Hacen transacciones trazables, transparentes e irreversibles. El reconocimiento de los desafíos únicos de la programación por contrato inteligente ha inspirado a los desarrolladores a crear lenguajes específicos de dominio, como Solidity para **facilitar el desarrollo**.

Aunque es un dominio prometedor, los contratos inteligentes, en su primera década han estado plagados de incidentes desafortunados. En junio de 2016, se explotaron las vulnerabilidades en el código DAO para vaciar más de 2 millones (40 millones de dólares) de éter. El ataque se aprovechó del problema de reentrada en la función "splitDAO" del código. Dado que, el programa no se diseñó con cuidado, una llamada a la función que se comportó como una llamada regular se modificó en una llamada recursiva y se usó para hacer retiros múltiples cuando sólo se autorizaba una.

Además, en noviembre de 2017, un desarrollador mientras corría un error que permitía a los atacantes robar 32 millones de dólares de unas pocas billeteras con múltiples firmas,

accidentalmente dejó un segundo error en el sistema que permitía a un usuario convertirse en el único propietario de cada uno. -cartera de firma. Al darse cuenta del error, los desarrolladores intentaron arreglar los daños eliminando el programa en lugar de devolver los fondos a sus propietarios originales. Este acto de eliminación del programa simplemente bloqueó permanentemente todos los fondos en esas billeteras de múltiples firmas. Sin embargo, a diferencia de la mayoría de los hacks de criptomonedas, el dinero no se tomó deliberadamente, sino que se cerró permanentemente por accidente y no entendió el programa.

Los incidentes anteriores muestran que incluso los desarrolladores más experimentados pueden dejar atrás las vulnerabilidades de seguridad y los errores que son explotables y propensos a fallas. Por lo tanto, todavía hay una curva de aprendizaje empinada para los desarrolladores cuando se trata de la programación por contrato. Esta curva de aprendizaje empinada hace que sea aún más difícil para los nuevos desarrolladores escribir contratos correctos y seguros. A la fecha actual, el estado de los estudios empíricos en el dominio del desarrollo de contratos inteligentes todavía está en la infancia. Por lo tanto, el objetivo de este capítulo es tomar esta iniciativa al proporcionar una evaluación empírica de los lenguajes de programación de contrato inteligente, con el fin de arrojar luz sobre las direcciones futuras de su investigación de desarrollo, educación y prácticas. Con este fin, evaluamos los aspectos de vulnerabilidad de usabilidad y seguridad de tres lenguajes específicos de dominio, a saber, **Solidity, Pact y Liquidity**.

Conclusión.

La investigación sobre la evaluación de la programación de contratos inteligentes es bastante joven y todavía hay un largo camino por recorrer para alcanzar su madurez. Este documento realiza una evaluación de los idiomas actuales como un paso fundamental para alcanzar esta madurez y obtener avances útiles. La evaluación dada incluyó un experimento que se realizó para comparar la vulnerabilidad de la usabilidad y la seguridad de los tres lenguajes específicos del dominio, a saber, Solidity, Pact and Liquidity. Los resultados del experimento demostraron que, si bien Solidity es el lenguaje más útil para un nuevo desarrollador para programar contratos inteligentes, es el lenguaje menos seguro para las vulnerabilidades. Por otro lado, Liquidity y Pact muestran una menor facilidad de uso pero parecen seguros por ahora. En consecuencia, nuestros resultados contribuyen al cuerpo de evidencia experimental sobre la usabilidad y seguridad de los lenguajes de programación de contrato inteligente, que actualmente es escaso.

Applying Design Patterns in Smart Contracts

Yue Liu, Qinghua Lu, Xiwei Xu, Liming Zhu, and Haonan Yao

Blockchain, la tecnología detrás de Bitcoin [5], es un almacén de datos descentralizado, donde todos los participantes en la red pueden llegar a acuerdos sobre los estados de datos transaccionales, sin depender de un sistema centralizado. La transparencia de los datos y la inmutabilidad son las características clave de la tecnología blockchain, que pueden ayudar a prevenir el ***tempering*** o la revisión de las transacciones enviadas en blockchain.

Además del libro de contabilidad distribuido como almacenamiento de datos, blockchain proporciona una infraestructura programable de propósito general. Los contratos inteligentes son programas implementados y que se ejecutan en blockchain, que pueden expresar activadores, condiciones y lógica de negocios para permitir transacciones programables más complejas. Muchas empresas nuevas, empresas y gobiernos están actualmente explorando aplicaciones de blockchain en áreas tan diversas como la cadena de suministro, registros electrónicos de salud, votaciones, suministro de energía, administración de propiedad, administración de identidad y protección de infraestructura civil crítica. Sin embargo, dado que la tecnología de blockchain aún se encuentra en una **etapa temprana**, hay pocos trabajos en la aplicación de métodos de arquitectura de software para el diseño de aplicaciones basadas en blockchain, particularmente el diseño de contratos inteligentes.

En la comunidad de arquitectura de software, se ha propuesto una taxonomía de blockchain para comparar diferentes plataformas de blockchain y ayudar en el diseño y evaluación de arquitecturas de software utilizando la tecnología de blockchain. Además de la taxonomía, los **patrones de diseño arquitectónico** también son un mecanismo para clasificar y organizar las soluciones existentes.

Un patrón de diseño es una solución reutilizable a un problema que comúnmente ocurre dentro de un contexto dado durante el diseño del software [3]. En este capítulo se investiga algunos patrones existentes para sistemas de sistemas distribuidos, sistemas punto a punto y diseños de software en general, y se evalúa la aplicabilidad de los patrones existentes al diseño de contratos inteligentes. El estudio da como resultado la experiencia de que hay algunas soluciones reutilizables que se pueden aplicar al diseño de contrato inteligente en un sistema basado en blockchain.

En este capítulo, primero se resumen y clasifican ocho patrones de diseño de contratos inteligentes. Los patrones se dividen en **cuatro categorías**: patrones creacionales, patrones

estructurales, patrones inter-conductuales y patrones intra-conductuales. Al usar los patrones, blockchain no solo se puede usar para almacenar o intercambiar datos, sino también para manejar programas más complicados con lógica compleja, lo que puede beneficiar a los desarrolladores en la creación de aplicaciones basadas en blockchain. Además, se utiliza un sistema de trazabilidad basado en blockchain del mundo real, **originChain**, como un estudio de caso para mostrar cómo aplicar patrones de diseño a contratos inteligentes. Este capítulo se enfoca más en el diseño estructural de contratos inteligentes, brinda más detalles de varios patrones de diseño y también compartimos algunas experiencias en la aplicación de patrones para mejorar los atributos de calidad de originChain, como la adaptabilidad y la interoperabilidad.

- **Patrón creacional**
    - **Contract Factory**. Como el código compilado de un contrato inteligente implementado en blockchain no es legible, es tedioso implementar y administrar contratos inteligentes que tienen las mismas propiedades pero que apuntan a diversos clientes. Con la ayuda de este patrón, los desarrolladores no necesitan implementar los contratos inteligentes uno tras otro, sino implementar una ***contract factory*** una vez, a través de la cual se pueden crear instancias de las múltiples instancias requeridas.
        - **Contract Composer**. En una aplicación basada en blockchain, la combinación de servicios u objetos es inevitable. En consecuencia, cómo controlar de manera efectiva una combinación de este tipo se convierte en un desafío para los desarrolladores, especialmente bajo la condición de que cada servicio u objeto se represente en forma de contrato inteligente. En comparación con Contract Factory, Contract Composer se centra en la estructura compleja de una instancia de contrato, ya que puede construir un objetivo complicado a través de múltiples piezas pequeñas.
- **Patrón estructural**
    - **Contract Decorator**. Una vez que se implementa un contrato inteligente en blockchain, no se le permite modificar o actualizar el código fuente de ese contrato. El patrón de Contract Decorator puede evitar volver a escribir todo el contrato cuando hay nuevos requisitos, los desarrolladores solo necesitan encapsular los contratos anteriores y agregar las características requeridas a una

nueva versión del contrato a través de este patrón, para lograr la capacidad de actualización y modificabilidad.

        - **Contract Facade**. La gestión de contratos inteligentes puede ser un trabajo engorroso, ya que existen contratos masivos que tienen características similares en un sistema basado en blockchain. El patrón Contract Facade puede aliviar dicha presión al proporcionar una interfaz simple al hacer frente a las direcciones de contrato. Dicha interfaz también tiene la forma de un contrato inteligente, para que los desarrolladores llamen a las funciones de contratos similares.

- **Patrones inter-conductuales**

    - **Contract Mediator**. En un proceso de negocios, los contratos inteligentes deben interactuar entre sí para finalizar una determinada actividad, lo que puede resultar en un acoplamiento estrecho de los contratos. El patrón de mediador de contrato tiene como objetivo reducir la complejidad de la comunicación de los contratos inteligentes, una instancia de este patrón es la forma de contrato inteligente, que recopila y resume las interacciones e invocaciones de un contrato a otro, para desacoplar los contratos inteligentes.

    - **Contract Observer**. Cuando un contrato inteligente se modifica debido a los requisitos cambiantes en la industria, todos los contratos relacionados deben ser informados y actualizados automáticamente. El patrón Contract Observer puede resolver este problema para lograr la interoperabilidad y la actualización entre los contratos a través de una instancia de observador. Una instancia de Contract Observer debe definir los objetos y la información involucrados, una vez que haya algún cambio, debe notificar a todos los objetos para actualizar la información.

- **Patrones intra-conductuales**

Los patrones de comportamiento interno no contribuyen a la arquitectura del contrato tanto como las tres categorías mencionadas anteriormente, pero cada una tiene la capacidad de trabajar de forma independiente y en colaboración. En este estudio, se proponen Hash Secret y Multi-Signature, tienen al menos una propiedad específica para avanzar los requisitos no funcionales de una aplicación basada en blockchain respectivamente.

- **Hash Secret**. Este patrón puede ayudar a un usuario a lograr la autorización de una actividad particular a autoridades desconocidas, generando una clave secreta digital conocida como el secreto hash. Cuando se decida la autoridad, recibirá el secreto hash y, por lo tanto, tendrá la capacidad de terminar una tarea adicional.
- **Multi-Signature**. Como existen múltiples autoridades en una red de blockchain, este patrón puede proporcionar una manera flexible de lograr una mejor cooperación. Una transacción es válida solo cuando hay suficientes firmas de las autoridades. Además, este patrón también se puede considerar como un mecanismo de protección individual, ya que la tecnología actual de la cadena de bloques no proporciona una manera de recuperar la clave privada perdida.

Conclusión.

En este capítulo, se propone una taxonomía de los patrones de diseño para contratos inteligentes, y comparte las experiencias de la aplicación de varios patrones de contrato inteligente basado en Solidity a un sistema de trazabilidad basado en blockchain del mundo real llamado originChain. Las propiedades únicas de Blockchain proporcionan nuevas ideas a la arquitectura de la aplicación, en la que la tecnología de blockchain actúa como un componente especial. Los patrones de diseño afectan algunos aspectos específicos de la aplicación basada en blockchain, como la capacidad de actualización, la adaptabilidad y la interoperabilidad.

Se dividen los patrones de diseño en cuatro categorías: Patrón de creación, Patrón estructural, Patrón inter-conductual y Patrón intra-conductual, de acuerdo con su contribución al diseño de la arquitectura de los contratos inteligentes. Específicamente, aplicamos **Contract Composer, Contract Facade, Contract Observer, Hash Secret y Multi-Signature** a una aplicación basada en la cadena de bloques del mundo real para mejorar los requisitos no funcionales.

Los contratos inteligentes solían ser independientes y dirigidos a una función específica, pero ahora en una aplicación basada en blockchain, los contratos inteligentes pueden hacer frente a algún proceso de negocio complejo en lugar de almacenar los datos apenas. La aplicación de algunos patrones de diseño de software a los contratos inteligentes ayuda a los desarrolladores a tener un mejor diseño en la arquitectura de los contratos inteligentes.

AODV–Based Routing for Payment Channel Networks

Philipp Hoenisch and Ingo Weber

Desde la primera aparición de Bitcoin en 2008, han surgido una multitud de derivados de blockchain y otras implementaciones. El propósito general es descentralizar la administración de un activo en particular, como una criptomoneda, eliminando la necesidad de una entidad central confiable y crear una red de nodos no confiables. Sin embargo, los problemas comunes de blockchain incluyen la confirmación lenta y los tiempos de confirmación y las altas tarifas de transacción. Para Bitcoin, una transacción a menudo se considera comprometida (irreversible) después de 6 bloques de confirmación, con un promedio de 60 min. Debido a esta demora de compromiso y las altas tarifas de transacción (recientemente entre USD 0,50 y 50 en Bitcoin), los pagos pequeños y particularmente los micropagos (es decir, pagos de unos pocos centavos o incluso una fracción de un centavo) no son muy económicos. Además, muchas cadenas de bloques tienen un rendimiento (7 a 20 transacciones por segundo, tps) que son muchas órdenes de magnitud por debajo de las redes de pago como VISA (hasta 47,000 tps).

Para abordar este problema, los investigadores propusieron no liquidar todas las transacciones en la cadena, sino más bien mover algunas transacciones fuera de la cadena, permitiendo que dos partes interactúen entre sí directamente. Al rastrear sus pagos entre sí por su cuenta, las dos partes pueden evitar interacciones costosas y prolongadas con la cadena de bloques. En caso de que exista una disputa sobre el saldo o si una parte deja de responder, el balance más reciente proporcionado por cualquiera de las dos partes se puede liquidar en la cadena de bloques (en cadena). La red Lightning (LN) es la más destacada de estas soluciones fuera de cadena. Se propone crear una red superpuesta de canales de pago fuera de la cadena, es decir, la Red de canales de pago (PCN), donde la transacción entre dos partes no se registra en la cadena de bloques de Bitcoin. Para eso, dos partes crean primero un par de transacciones: una transacción de financiación y una transacción de gasto. El primero especifica el monto total retenido en el canal, es decir, uno o ambos participantes pagan un monto arbitrario en este canal. La otra transacción específica la salida, es decir, define qué parte recibe cuánto de la cantidad total. Solo la transacción de financiamiento se liquida directamente en la cadena de bloques, mientras que la transacción de salida se puede retrasar en un momento dado en el futuro. Si una de las partes desea pagar a la otra parte, actualiza la transacción de salida que refleja el estado real. Decker et al. En [4] presentó una alternativa. Si bien la LN se diseñó específicamente para Bitcoin, las PCN también se pueden realizar en otras cadenas de bloques si brindan un lenguaje de secuencias de comandos mínimo que permita realizar el llamado

Contrato de Bloqueo de Hash-time (HTLC). Las alternativas incluyen la Red Raiden (Ethereum), Sprites (Bitcoin) o COMIT (cadena cruzada).

Abrir un canal solo tiene sentido para pagos recurrentes a (oa través de) la otra parte respectiva. Para realizar transacciones con partes donde no existe un canal directo, se pueden encadenar múltiples canales de pago. El pago se enruta a través de la red con uno o más intermediarios. Sin embargo, esto plantea un gran desafío: cómo encontrar una ruta óptima (o aceptable) a través de la red, es decir, desde el remitente de un pago al destinatario. La ruta debe ser aceptable (e idealmente optimizada) en términos de criterios específicos tales como tarifas de enrutamiento, tasas de cambio y confiabilidad. El enrutamiento dentro de la LN aplica un protocolo de enrutamiento proactivo: cada nodo transmite la información sobre sus vecinos (por ejemplo, los nodos a los que se conecta a través de un canal) a través de la red. Por lo tanto, la desventaja de esto es que se debe enviar una gran cantidad de información antes de poder establecer una ruta. En consecuencia, cada nodo tiene un conocimiento completo sobre la topología de la red. Hasta ahora, solo se incluye información sobre el financiamiento del canal, pero no la distribución del financiamiento, es decir, cuánto del financiamiento está actualmente en qué lado y la solución está limitada a la cadena de bloques de Bitcoin. Obviamente, la difusión de información de topología global es costosa e introduce sus propios límites de escalabilidad, que son particularmente graves cuando se considera una red de cadenas cruzadas.

Se argumenta que, sin una solución totalmente automatizada para el enrutamiento de pago, con el enrutamiento localizado y la capacidad de adaptarse al entorno siempre cambiante de dicha red, los PCN no pueden realizar su verdadero potencial o lograr una cobertura significativa a escala global. Por eso, se hacen las siguientes aportaciones:

- Se presenta una adaptación de un algoritmo de enrutamiento basado en vectores de distancia a pedido (AODV) ad-hoc para una red de canales de pago fuera de la cadena.
- El enfoque puede atender diferentes monedas, por lo tanto, permite enrutar pagos a través de múltiples cadenas de bloques.
- Se evalúan experimentalmente la aplicabilidad de nuestro protocolo de enrutamiento y discutimos las ventajas y desventajas.

Conclusión.

En este capítulo se presenta una adaptación de AODV para el enrutamiento de pagos en redes de canales de pago como Lightning, Raiden o COMIT. Se mejoran los mensajes con información sobre tarifas y tasas de cambio para encontrar una ruta económica a través de la red. AODV es un protocolo de enrutamiento reactivo que sólo establece una ruta cuando es necesario, evitando así la sobrecarga de mensajes superfluos enviados en un protocolo de enrutamiento

proactivo. Sin embargo, AODV conlleva el riesgo de inundar la red si la cantidad máxima de saltos no se establece correctamente. Los experimentos revelan que el AODV adaptado se puede usar fácilmente en una red de hasta unos pocos miles de nodos. Por lo tanto, el enrutamiento basado en AODV se puede integrar en PCN.

Application Track: Blockchain Solutions

Faster Dual-Key Stealth Address for Blockchain-Based Internet of Things Systems

Xinxin Fan

El Internet de las cosas (IoT) ha estado conectando una gran cantidad de dispositivos inteligentes a Internet y ha impulsado la transformación digital de la industria. Desafortunadamente, los sistemas existentes de IoT centrados en la nube tienen una serie de desventajas importantes, como los altos costos de mantenimiento del sistema, el lento tiempo de respuesta, la seguridad y la privacidad, etc. Se ha percibido Blockchain,como una forma de tecnología de contabilidad distribuida, inmutable y con marca de tiempo. como una solución prometedora para abordar los problemas mencionados y para desbloquear de forma segura los valores operativos y de negocio de IoT. La combinación de blockchain e IoT facilita el intercambio de servicios y recursos, crea pistas de auditoría y permite la automatización de flujos de trabajo que requieren mucho tiempo en diversas aplicaciones. Si bien la combinación de estas dos tecnologías está creando nuevos niveles de confianza, la red descentralizada y la verificabilidad pública de las transacciones de blockchain a menudo no proporcionan las propiedades de seguridad y privacidad necesarias para los usuarios.

Durante los últimos años, se han empleado bastantes técnicas criptográficas como “ring signature”, “stealth address”, and “zero-knowledge proof” para garantizar la privacidad de la transacción para los remitentes, los receptores y el monto de la transacción en cadenas de bloques. **Este trabajo se centra en “stealth address”**, una técnica de protección de la privacidad para los receptores de criptomonedas. Stealth address requiere que el remitente cree direcciones aleatorias de una sola vez para cada transacción en nombre del destinatario para que los diferentes pagos realizados al mismo beneficiario no se puedan vincular. El esquema de stealth address más básico fue esbozado por primera vez por un miembro del Foro de Bitcoin llamado 'ByteCoin' en 2011, que luego se mejoró al introducir el par de claves efímeras al azar. Más adelante, en 2014 se implementó una mejora de doble clave a los esquemas de stealth address anteriores, que utilizaba dos pares de claves criptográficas para terceros designados (por ejemplo, auditores, servidores proxy, carteras de solo lectura, etc.) eliminando la capacidad de desvinculación de las stealth address sin permitir simultáneamente que se gasten los pagos.

El protocolo de stealth address de doble clave (DKSAP) proporciona un fuerte anonimato para los receptores de transacciones y les permite recibir pagos no vinculables en la práctica. Sin

embargo, este enfoque requiere que los nodos de blockchain calculen constantemente las direcciones de destino supuestas y encuentren las coincidencias correspondientes en el blockchain. Si bien este proceso funciona bien para las computadoras de pleno derecho, plantea nuevos desafíos para los dispositivos de IoT con recursos limitados. Teniendo en cuenta el limitado presupuesto de energía de los dispositivos inteligentes, se propone una variante ligera de DKSAP, a saber, DKSAP-IoT, que se basa en la idea similar a la reanudación de la sesión TLS y requiere que tanto el remitente como el receptor realicen un seguimiento de las claves de pares continuamente actualizadas para cada sesión de pago. DKSAP-IoT puede mejorar el rendimiento de DKSAP en al menos un 50% y reducir el tamaño de la transacción de manera simultánea, proporcionando así una solución eficiente para proteger la privacidad de los destinatarios en sistemas IoT basados en blockchain.

Conclusión.

En este capítulo, se propone un eficiente protocolo de stealth address de doble clave DKSAP-IoT para sistemas IoT basados en blockchain. Motivado por las técnicas de reanudación de sesiones TLS, se aplica una función criptográfica hash para actualizar continuamente un secreto compartido entre dos pares de comunicación y extender la vida útil de este secreto compartido para N transacciones adicionales. Tanto el remitente como el destinatario deben mantener la información de estado localmente para poder realizar un seguimiento de las claves de sesión en pares. El análisis de seguridad muestra que DKSAP-IoT proporciona el anonimato del receptor y la privacidad hacia adelante. Al implementar DKSAP-IoT en una Raspberry Pi 3 Modelo B, se demustra que DKSAP-IoT puede lograr al menos un 50% de mejora en el rendimiento en comparación con el DKSAP original, además de una reducción significativa del tamaño de la transacción en el bloque. Nuestro trabajo es otro paso lógico hacia la protección sólida de la privacidad de los sistemas de IoT basados en blockchain.

Blockchain-Based Solution for Proof of Delivery of Physical Assets

Haya R. Hasan and Khaled Salah

Con la difusión de la tecnología y el Internet, las compras en línea o el comercio se han convertido en parte de la actividad diaria de las personas. A menudo, en la comodidad de sus hogares, las personas comienzan a buscar un artículo deseable y se preguntan si hay un proveedor en línea que pueda proporcionar el artículo en perfectas condiciones a sus puertas. Satisfaciendo las necesidades del mundo actual, muchas tiendas en línea han lanzado y prestado servicios de entrega e incluso envíos a todo el mundo. Por lo tanto, existe una inmensa necesidad de tener una solución que proporcione una prueba de entrega de cualquier artículo físico, como una prenda de vestir, un libro, artículos esenciales para el hogar, etc. entregados entre dos partes.

La Prueba de entrega (POD) o la "última milla" de entrega es crucial ya que muestra que un artículo ha alcanzado su destino final y requerido. En el mundo real, las empresas de servicios de mensajería y de entrega utilizan rastreadores y sistemas de prueba de entrega para garantizar que las necesidades de sus clientes se cumplan a tiempo y sin demoras. No solo la puntualidad es importante, sino que también la entrega del artículo tal como viene de la fuente inicial es extremadamente vital.

Los sistemas de prueba de entrega de hoy se basan generalmente en documentos firmados y documentos que se llevan con el transportista al destinatario. Otros servicios de mensajería pueden depender de un dispositivo de mano electrónico utilizado para obtener la firma del destinatario con una identificación válida. Esto es engorroso y no proporciona confianza total para la entrega, por lo que no hay una verificación verdadera y genuina por parte del mensajero de la firma y la identificación del destinatario, que puede ser falsa. Además, los minoristas en línea dependen de un tercero para el envío. Por ejemplo, Amazon depende de varias empresas de mensajería regionales para sus servicios de entrega, como UPS, FedEx, DHL, Pilot y muchos otros. Además, el servicio de entrega de hoy es completamente centralizado, costoso y extremadamente difícil de administrar. En general, los sistemas centralizados sufren una invasión de la privacidad, un solo punto de falla y una desconfianza que puede llevar a la corrupción y los ataques.

Problema: Hasta la fecha, el comercio en línea de confianza entre dos partes desconocidas aún no se ha establecido sin un tercero de confianza centralizado. Existe una inmensa necesidad de una prueba de entrega y seguimiento de los artículos enviados con una trazabilidad y audición altamente confiable, segura y descentralizada.

Una prueba ideal del sistema de entrega debe satisfacer las siguientes características deseables:

- **Responsabilidad**: debería ser posible rastrear las acciones realizadas en el sistema hasta la entidad iniciadora real.
- **Autorización**: Cada parte en el sistema tiene permitido realizar solo ciertos roles.
- **Auditabilidad**: debería ser posible realizar un seguimiento de todas las actividades realizadas por las entidades que actúan y, por lo tanto, rastrear el estado y la ruta del elemento.
- **Integridad**: nadie debe poder modificar las auditorías y los términos y condiciones acordados.
- **Puntualidad**: el sistema debe poder cronometrar cada acción y entregar el artículo a tiempo al cliente.
- **Honestidad**: Cada una de las entidades participantes (vendedor, transportista y comprador) debe ser incentivada a actuar honestamente y hacer su parte legítimamente.

Proponemos una solución de blockchain para la prueba de entrega de artículos físicos que resuelve el problema de la confianza, el seguimiento, el rastreo y la prueba de que el artículo llegó a su destino final y legítimo. La solución se puede ampliar para incluir destinos intermedios antes de la final y se puede integrar fácilmente con una protección **Know Your Customer**(KYC) para agregar una capa adicional de seguridad.

Conclusión

Este capítulo ha presentado una solución de blockchain que facilita el comercio y el seguimiento de los artículos vendidos entre dos partes de manera descentralizada. La solución proporciona una prueba de entrega de elementos físicos aprovechando la seguridad y la inmutabilidad que proporciona blockchain. La solución propuesta es suficientemente genérica y se puede aplicar a casi todos los elementos físicos y bienes enviados. En este documento, nos enfocamos en proporcionar, implementar y probar el código de contrato inteligente y el algoritmo de la solución de PoD(**Proof of Delivery**) que muestra a los casos la capacidad de probar la entrega de un artículo utilizando una garantía depositada por igual por el vendedor, el transportista y el comprador. En el capítulo, se muestra y se discute cómo la solución puede proporcionar características y requisitos clave de PoD que incluyen integridad, responsabilidad, autorización, puntualidad y honestidad.

Towards Legally Enforceable Smart Contracts

Dhiren Patel, Keivan Shah, Sanket Shanbhag and Vasu Mistry

Un contrato inteligente es un programa que se almacena y ejecuta en un sistema descentralizado, por ejemplo, una blockchain. Un contrato inteligente puede realizar cálculos, almacenar información y enviar fondos automáticamente a otras cuentas. Por lo tanto, los contratos inteligentes pueden considerarse como la automatización del sistema de mercado y que permiten que diferentes partes trabajen sin confianza mutua entre sí.

Los contratos inteligentes son una nueva forma de autoayuda preventiva que las legislaturas o los tribunales no deben desalentar . Un contrato inteligente puede dar lugar a obligaciones legalmente exigibles. Estas cuestiones se tratan de manera diferente de un país a otro. Mientras tanto, en este momento, diferentes jurisdicciones están lidiando, respaldando o revocando diferentes disposiciones legislativas para regular el uso de los sistemas DLT (**Distributed Ledger Technology**) en diferentes contextos. Por ejemplo, los contratos inteligentes que respaldan las transacciones en ICO (Ofertas iniciales de monedas, por ejemplo, KodakCoin) pueden ser completamente ilegales en algunas jurisdicciones, mientras que un contrato inteligente que maneja transacciones bancarias intrainstitucionales y otras transacciones financieras pueden ser bastante legales, en la misma jurisdicción o en otra parte.

Hay quienes promueven el enfoque de "código es contrato" (es decir, que la totalidad de un contrato de lenguaje natural puede codificarse). Por otro lado, hay quienes ven los contratos inteligentes como cajas negras que consisten en la digitalización del rendimiento de la lógica empresarial (por ejemplo, el pago), que puede o no estar asociado con un contrato de lenguaje natural. Entre estos dos extremos, es probable que surjan varias permutaciones, incluido un modelo de contrato inteligente "dividido" en el que los términos del contrato en lenguaje natural se conectan al código de la computadora a través de parámetros que se incorporan a los sistemas informáticos para su ejecución. Además, el efecto contractual legalmente vinculante depende de una serie de variables. Es tentador concluir que, solo porque el apodo "contrato inteligente" incluye la palabra contrato, es un contrato legalmente vinculante como cuestión de derecho. Esto no es necesariamente correcto.

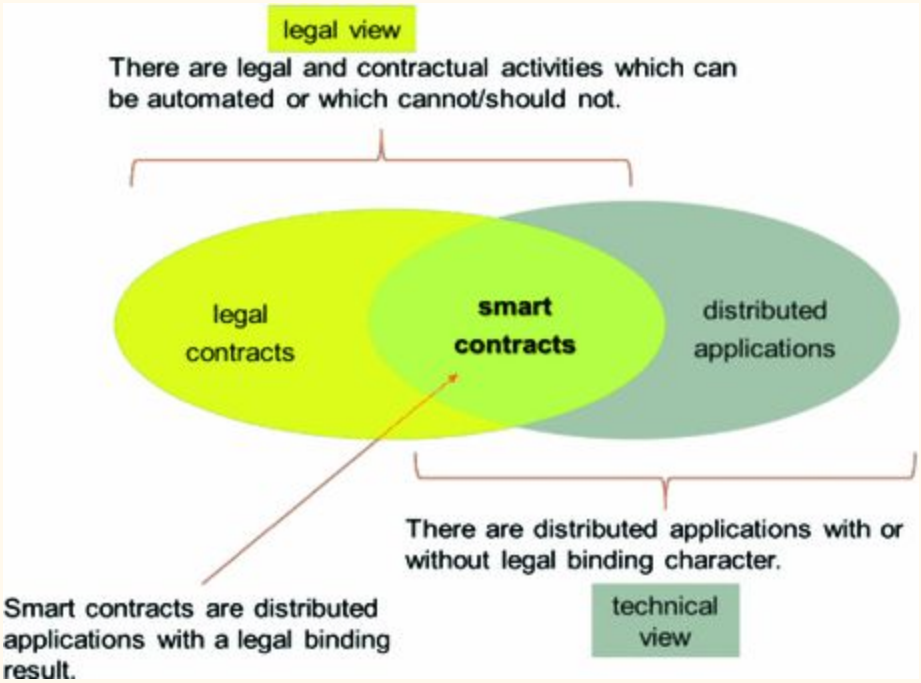


Imagen. Relación entre el punto de vista legal y técnico.

Conclusión

En el mercado descentralizado que utiliza la tecnología Blockchain y el libro mayor distribuido, la facilitación de transacciones y la comparación se mejoran sustancialmente debido al acceso no modificado a la información. Esto ha permitido que los sistemas basados en contratos inteligentes permitan a las partes sin confianza realizar transacciones que se adhieran directamente a los términos divulgados, sin manipulación por plataformas intermediarias. Los contratos inteligentes se están convirtiendo en parte integral de muchos sistemas críticos que permiten el intercambio de pagos y servicios con reglas preestablecidas. En este capítulo, se muestra cómo se puede implementar la aplicación freelancer en el mercado electrónico descentralizado utilizando Ethereum Blockchain y **cómo los contratos inteligentes se pueden hacer legalmente exigibles con la ayuda de la firma digital**; haciéndolos aceptables entre las partes involucradas, así como el marco legal de la jurisdicción.

Border Control and Immigration on Blockchain

Dhiren Patel, Balakarthikeyan and Vasu Mistry

Las fronteras entre países se aplican estrictamente para evitar el movimiento ilegal de personas o mercancías hacia el país. Un gran número de personas cruzan las fronteras internacionales diariamente. Esto significa que se debe llevar un registro efectivo, seguro y escalable de entradas y salidas. Para la seguridad nacional, es crucial que estos registros sean inmutables a cualquier ataque / alteración. Es importante garantizar que el movimiento de personas a través de las fronteras sea fácil y sin problemas. También es imperativo que las naciones compartan sus registros para proporcionar un mecanismo de control estricto y eficiente. Al mismo tiempo, estos registros deben almacenarse de manera segura, de conformidad con las leyes y regulaciones de privacidad de ese país. Esto ha hecho que sea aún más imperativo implementar sistemas para aliviar todas las preocupaciones anteriores.

El objetivo de este trabajo es implementar un sistema de control de fronteras seguro, descentralizado e inmutable que permita a los gobiernos registrar de manera fácil y efectiva a las personas que salen y entran a sus países. Este sistema también sincroniza todos los demás puertos de entrada en un sistema descentralizado unificado. También tiene como objetivo crear rutas de datos separadas para la transmisión internacional de registros de salida. El sistema también incluirá métodos para almacenar de forma segura la información biométrica para validar / verificar a los pasajeros automáticamente.

Conclusión.

En este capítulo se ha abordado los problemas de seguridad y confiabilidad de los sistemas actuales. Al utilizar blockchain en **Hyperledger**, este sistema sincroniza todos los demás puertos de entrada en un sistema descentralizado unificado. Se ha mostrado la creación de rutas de datos separadas para la transmisión internacional de registros de salida. Se contempla una infraestructura autorizada donde las agencias de seguridad del gobierno actúan como guardianes de puerta que permiten automáticamente la entrada / salida. Se ha previsto el almacenamiento de datos biométricos en un libro de contabilidad local que permita a los ciudadanos ingresar fácilmente a su propio país y al mismo tiempo mantener a raya las cuestiones de privacidad. Actualmente el sistema está en desarrollo activo.

Application Track: Business Models and Analyses

RPchain: A Blockchain-Based Academic Social Networking Service for Credible Reputation Building

Dong Qin, Chenxu Wang, and Yiming Jiang

Con el desarrollo de la tecnología Web 2.0, la investigación académica ha entrado en una era de colaboración y de intercambio. La propuesta de "Open Science" que aboga por el intercambio de datos, la evaluación abierta entre pares, la ciencia ciudadana, etc., se ha convertido gradualmente en la corriente principal de investigación en la era digital actual . Sin embargo, esto también trae consigo los problemas de construcción de reputación académica y protección de derechos de autor digitales.

Existen varios servicios de redes sociales académicas (ASNS) como Research Gate y Mendeley para superar estos problemas. Sin embargo, todavía hay algunos inconvenientes. En primer lugar, estos servicios se centran en servir a investigaciones/documentos académicos, lo que responde a la propuesta de investigación científica universal. En segundo lugar, estos servicios carecen de un mecanismo de incentivo adecuado para atraer participantes ordinarios. Algunos estudiosos son reacios a usar ASNS debido a la falta de confianza en ellos. En tercer lugar, los mecanismos públicos de revisión por pares utilizados por estos servicios pueden **dañar** las relaciones sociales entre los usuarios. En la práctica, la mayoría de los investigadores prefieren revisar en privado. Además, las ASNS centralizadas, como Research Gate, no pueden evitar los riesgos de seguridad asociados con los servicios de red **centralizados** tradicionales. Los ataques contra estos servicios pueden provocar la pérdida o falsificación de datos, lo que es fatal para la construcción de una reputación justa. Por lo tanto, se desea para un ASNS que tenga un alto grado de apertura e incentivos apropiados para la participación.

El surgimiento de la tecnología blockchain nos brinda una forma viable de construir dicho servicio. La tecnología blockchain tiene varias propiedades importantes, como la descentralización, la trazabilidad, la privacidad, la transferencia segura de valor, etc. El uso de blockchain para almacenar registros revisados por pares garantiza el máximo nivel de seguridad, ya que es casi imposible para los atacantes destruir o manipular los registros.

Sin embargo, no es trivial emplear la tecnología blockchain para construir un ASNS adecuado. En primer lugar, debemos diseñar un modelo de blockchain adecuado para proporcionar una plataforma que debería construir la reputación de un usuario basándose en las revisiones de

otros pares. En segundo lugar, tenemos que desarrollar un algoritmo de consenso creíble para seleccionar un peer elegible para el mantenimiento de bloques. En tercer lugar, debemos diseñar políticas de incentivos para atraer a los participantes ordinarios. Finalmente, debemos considerar los problemas de seguridad en la implementación del sistema.

En este capítulo, se presenta RPchain, un modelo de servicio de red social académico basado en blockchain. Para abordar el primer problema, se proponen tres tipos de transacciones, transacciones de token, transacciones de contenido y transacciones de voto. Las transacciones de token se utilizan para la transferencia de valor y el intercambio. Las transacciones de contenido representan el contenido publicado por los usuarios. El contenido incluye temas / temas publicados por los usuarios, respuestas de compañeros y contratos inteligentes, etc. Las transacciones de voto representan los votos que los compañeros dan a un contenido específico (a favor de él). Para garantizar una votación justa y una seguridad sistemática, sólo los usuarios autorizados por contratos inteligentes o aprobados por consenso son elegibles para votar. Los votos de los contenidos que pertenecen al mismo usuario se acumulan para evaluar la reputación del usuario. Todas las transacciones y contratos se almacenan en la cadena de bloques, lo que brinda a los usuarios una protección creíble de los derechos de autor y la trazabilidad del desarrollo de la reputación. Además, se divide el ciclo de vida de RPchain en tres fases: la fase inicial, la fase de extensión y la fase estable. Se adoptan diferentes algoritmos de consenso en diferentes fases para facilitar el desarrollo y la estabilidad del modelo.

El algoritmo de consenso es el alma de un sistema blockchain. Sin embargo, los algoritmos de consenso orientados a la potencia de la computación existentes, como la Prueba de trabajo (PoW) utilizados en Bitcoin, no son consistentes con los objetivos de nuestro modelo orientado a servicios. Para abordar este problema, proponemos un nuevo algoritmo de consenso denominado prueba de reputación (PoRe). PoRe utiliza la reputación ganada por las transacciones de contenido publicado del participante para llegar a un consenso. Cuando el contenido recibe votos, la reputación del contenido se evalúa en función del peso de esos votos (cuanto más votos, más contribuciones). Luego, cuando las condiciones lo permiten, los usuarios participan en el consenso de PoRe utilizando la reputación obtenida por la transacción de contenido. Cuanto mayor sea el valor de reputación utilizado para el consenso, menor será la dificultad del consenso de PoRe y mayor será la probabilidad de que el usuario obtenga el siguiente bloque. Es decir, cuanto mayor sea la contribución de un usuario al sistema, mayor será la posibilidad de que obtenga la recompensa.

Para abordar el problema de los incentivos, presentamos tres tipos diferentes de recompensas, ***consensus rewards*** (recompensas en bloque), ***vote rewards***, ***uncle block rewards***. Consensus rewards y las vote rewards se utilizan para incentivar a los usuarios a participar en el

mantenimiento de la cadena de bloques y dar opiniones sobre el contenido. Las uncle block rewards se utilizan para compensar a los usuarios que fallan en la competencia por consenso pero que contribuyen significativamente al sistema.

IPFS-Blockchain-Based Authenticity of Online Publications

Nishara Nizamuddin, Haya R. Hasan and Khaled Salah

Internet y la era digital han desencadenado el acceso único a la información. Con la facilidad en el acceso y el intercambio de información, la autenticidad de los materiales digitales publicados y publicados gratuitamente siempre es cuestionable. La autenticidad del contenido digital es un desafío importante para la industria de publicación de libros en línea de hoy, y el contenido digital en general, como los contenidos multimedia, películas, música, etc. El contenido digital, disponible en Internet, durante su vida útil puede ser modificado, copiado, reproducido, traducido a diferentes idiomas, reeditado y reformateado. Existe una inmensa necesidad de una autenticidad adecuada con la capacidad de rastrear el historial de publicaciones del material publicado en línea al autor, escritor o artista original, con un alto grado de confianza, credibilidad e integridad.

En la práctica, un manuscrito en papel de un libro o artículo periodístico puede imprimirse, escanearse, digitalizarse y traducirse a diferentes idiomas, lo que da como resultado múltiples versiones de los manuscritos originales que fueron publicados por diferentes entidades editoras o individuos. Es decir, el contenido digital disponible a través de diversos recursos, como revistas en línea, libros electrónicos y sitios web, puede estar sujeto a una alteración ilegítima que en última instancia conduce al acceso a la información contaminada. Además, hay una falta de una auditoría estricta para garantizar que el libro digital sea verificable, completo y preciso. Si bien el libro electrónico se recopila e imprime de diversas fuentes, la autenticidad e integridad de los activos digitales está en juego.

Imagen. Producción de diferentes versiones de un libro en línea a través de varios editores.

Blockchain es una tecnología innovadora y nueva que puede ser clave para proporcionar una solución a la autenticidad de los materiales digitales. Blockchain es la tecnología subyacente del Bitcoin, pero ahora es visto como un libro de contabilidad distribuido al que cualquier persona puede acceder a nivel mundial para verificar los datos y el contenido almacenados, con alta integridad, flexibilidad, credibilidad y, sobre todo, trazabilidad. Todo esto se realiza de manera descentralizada y sin intermediarios. Más tarde, los contratos inteligentes de Ethereum brindaron la capacidad de cargar y ejecutar el código que lleva a cabo la lógica de negocios a la cadena de bloques. El código de contrato inteligente reside en una cadena de bloques y proporciona funciones múltiples con direcciones únicas a las que puede llamar cualquier usuario de la cadena de bloques.

Sin embargo, Blockchain es un medio costoso para el almacenamiento de datos, especialmente para datos grandes y contenido digital. Para un almacenamiento eficiente de datos y contenido de gran tamaño, se propone utilizar el sistema de archivos **IPFS**. IPFS significa **Sistema de archivos interplanetarios**, que es un sistema de archivos descentralizado y distribuido y una plataforma para almacenar datos y archivos con alta integridad y flexibilidad. Fundamentalmente, IPFS es un sistema de archivos distribuido globalmente, peer-to-peer, open source, que se puede utilizar para almacenar y compartir grandes volúmenes de archivos con un alto rendimiento. La **solución propuesta** utiliza tanto los contratos inteligentes de cadena de bloques como el IPFS, por lo que los contenidos digitales se almacenan en el IPFS y los hashes de IPFS se almacenan en los contratos inteligentes de la cadena de bloques para proporcionar trazabilidad y autenticidad. Específicamente, el hash generado al almacenar los documentos en IPFS se puede almacenar en los contratos inteligentes de manera efectiva y se puede acceder a los documentos utilizando el hash. Si hay algún cambio en el contenido del documento digital, el hash cambia para mostrar que el contenido original se modificó y modificó.

En este capítulo, se propone una solución combinada basada en la cadena de bloques de IPFS para resolver la autenticidad y originalidad del contenido digital publicado libremente en Internet. En el capítulo se muestra cómo se puede resolver este problema para los libros publicados en línea, pero la solución puede extenderse y adoptarse para otros contenidos digitales y multimedia. Se muestra cómo la solución tiene la capacidad de rastrear el contenido digital, con sus diferentes versiones publicadas, de vuelta a la copia auténtica certificada creada por el autor original.

Blockchain Framework for Textile Supply Chain Management

Magdi ElMessiry and Adel ElMessiry

Los sistemas modernos de la cadena de suministro textil son grandes y complicados, con fuentes y proveedores globales que se alimentan de líneas de producción que pueden abarcar continentes. Una cantidad sustancial de defectos no se puede rastrear directamente a los lotes defectuosos que ingresaron a la cadena de suministro, causando desperdicio y frustración en el proceso. La trazabilidad es **casi imposible** debido a la cantidad de etapas que atraviesa el producto y al tamaño de los datos involucrados. No se utiliza un solo sistema a nivel mundial para registrar y rastrear el producto a lo largo de la cadena de suministro. En el momento en que se descubre la causa inicial de un problema, no es posible recurrir, excepto descartar el producto final, lo que genera pérdidas que podrían alcanzar el 40% del valor del producto final. Si bien la trazabilidad es un problema obvio en la cadena de suministro de textiles, la transparencia es un problema más impactante que no está bien abordado. La cadena de suministro y la falta de transparencia exacerban los problemas que enfrenta cada participante y obliga a cada entidad a trabajar localmente utilizando la información local. Este enfoque es fundamentalmente erróneo, ya que trata un problema global desde un punto de vista local. No todas las industrias están maduras para aprovechar la tecnología blockchain.

Blockchain requiere una industria con una cadena de suministro complicada y ampliamente distribuida, que contenga un mayor número de etapas intermedias. Esto no puede aplicarse más que en una de las industrias más antiguas del mundo, el textil.

En este capítulo, se propone un framework completo basado en blockchain para la mejora de la calidad textil que permite el intercambio de información entre cadenas casi en tiempo real con autenticidad y precisión garantizadas, lo que permite identificar lotes defectuosos de calidad en todos los sistemas tan pronto como se detectan en unos pocos.

Research on the Pricing Strategy of the CryptoCurrency Miner's Market

Liping Deng, Jin Che, Huan Chen, and Liang-Jie Zhang

Si bien las actitudes de los gobiernos y el público en general respecto de las criptomonedas varían enormemente, los precios de las criptomonedas han crecido a una tasa extremadamente exagerada desde 2016, atrayendo cada vez más a los inversores y la atención de los medios. No solo eso, sino que han crecido para ser rentables, y muchas personas han comprado ***mineros*** para invertir en la industria minera. Este capítulo examina la estabilidad de las dos series temporales del precio de bitcoin y el hashrate de los mineros desde 2016 hasta el presente. La investigación muestra que el cambio de precios es la causa de Granger de los cambios en hashrate. Al establecer un modelo de retraso distribuido, se analiza la relación cuantitativa entre hashrate y precio. Combinado con la investigación de seguimiento del mercado minero, se descubrió la estrategia de precios del mercado minero, es decir, el precio actual del minero está determinado por el precio de la criptomoneda anterior, y se calcula el período de retraso.

Conclusión

El precio actual de la criptomoneda determina el precio futuro de los mineros, y el período de demora es de 14 días, que es una estrategia de precios común para el mercado minero de la criptomoneda.

Short Paper Track: Fundamental Research

FBaaS: Functional Blockchain as a Service

Huan Chen and Liang-Jie Zhang

La arquitectura sin servidor ha ido ganando popularidad en los últimos tres años. La función como servicio (FaaS) es una realización concreta de la arquitectura de Serverless y tiene varias ventajas y características. Este capítulo propone un nuevo modelo de servicio que se basa en el modelo FaaS, denominado FBaaS - Functional Blockchain as a Service. En comparación con la cadena de bloques convencional como un servicio (BaaS), FBaaS tiene una implementación más ligera de la lógica de negocios de nivel superior, lo que brinda una serie de ventajas directas. En primer lugar, podría **mejorar** la velocidad de operación de un blockchain. En segundo lugar, los avances en alta **robustez** y alta **disponibilidad** de la red FaaS subyacente se pueden adaptar naturalmente al FBaaS debido a su arquitectura jerárquica. En tercer lugar, FaaS implementa un mayor nivel de abstracción de las lógicas que es mucho más sucinta. Este capítulo propone un método de abstracción en la realización de la lógica empresarial de la cadena de bloques del consorcio que podría mejorar aún más el rendimiento general. También se despliegan los detalles de una red de ejemplo concreta, que es la red de cadena de bloques de conferencia para la Federación de Conferencia de Servicios (SCF) 2018.

LedgerGuard: Improving Blockchain Ledger Dependability

Qi Zhang, Petr Novotny, Salman Baset, Donna Dillenberger, Artem Barger and Yacov Manevich

Un libro mayor distribuido(ledger) es el componente central de cualquier plataforma de **blockchain**. Cada peer en la red Blockchain mantiene su propia réplica del libro mayor. El ledger es una estructura de datos de solo apéndice inmutable, que contiene una secuencia de transacciones históricas agrupadas en bloques. El ledger se forma encadenando los bloques junto con punteros de hash (es decir, un bloque posterior contiene el hash de su bloque anterior).

La integridad del libro mayor es esencial para el correcto funcionamiento del peer. Con el libro mayor dañado, el peer no puede generar transacciones válidas cuando el contrato inteligente necesita recuperar las transacciones históricas del libro mayor. Además, cuando las transacciones históricas registradas en el libro mayor son solicitadas por **herramientas externas** como las aplicaciones analíticas o de auditoría, el peer verifica primero la integridad y la validez de los bloques relevantes antes de extraer las transacciones. Cualquier daño en los bloques descubiertos por estas operaciones conduce a una degradación significativa de la funcionalidad de igual a igual. Por lo general, el peer dejará de funcionar hasta que esté disponible el libro mayor correcto. Además, las aplicaciones que acceden a los datos dañados también pueden verse afectadas significativamente.

El peer protege su libro mayor de la introducción de datos dañados. Cuando se recibe un nuevo bloque, el peer valida la integridad del bloque antes de agregar el bloque al libro mayor. Sin embargo, el peer no tiene la capacidad de detectar y recuperar los bloques dañados que existen en el libro mayor durante su tiempo de ejecución.

Una corrupción del libro mayor puede tener una de varias causas diferentes. Se han observado varios tipos de daños en el libro mayor en las plataformas públicas de Blockchain, como Bitcoin y Ethereum. Por ejemplo, en la plataforma Ethereum, los usuarios informaron archivos de datos dañados debido a falsos positivos de software antivirus. Los usuarios de Bitcoin también informaron sobre la corrupción del libro mayor debido a la falta de coincidencia de la suma de comprobación del bloque. En las cadenas de bloques privadas como Hyperledger Fabric o R3 Corda, es fundamental mantener los nodos que alojan a sus peers de forma altamente segura. Sin embargo, cuando un peer se hospeda en un entorno menos seguro, un atacante externo o un

usuario malintencionado puede piratear el nodo del peer y modificar el contenido de los archivos de contabilidad. Además, dado que los archivos de contabilidad normalmente se almacenan en un medio de almacenamiento como discos magnéticos o SSD, una falla de hardware también puede causar la corrupción de los archivos de contabilidad.

En este capítulo, se presenta LedgerGuard, un mecanismo que permite al peer mantener la integridad de su libro mayor. LedgerGuard hace cumplir la integridad del libro mayor con las siguientes dos técnicas. Primero, valida el contenido de cada bloque y los enlaces de hash entre bloques. Segundo, si se identifica un bloque dañado, LedgerGuard recupera el bloque y corrige la parte afectada del libro mayor sin la necesidad de reconstruir todo el libro mayor. LedgerGuard está diseñado de una manera altamente configurable. Puede usarse como una herramienta (por ejemplo, por un operador) para validar y corregir el libro mayor en línea o fuera de línea. También se puede utilizar como un servicio del nodo igual, para monitorear y corregir continuamente el libro mayor y, por lo tanto, aumentar la resistencia y disponibilidad del igual.

Blockchain-Based Research Data Sharing Framework for Incentivizing the Data Owners

Ajay Kumar Shrestha and Julita Vassileva

Durante la última década, ha habido una gran innovación tecnológica que ha llevado a muchos consorcios de investigación a utilizar enfoques basados en datos y a colaborar en la toma de decisiones inteligentes para mejorar sus actividades de investigación científica. Las prácticas de **intercambio de datos** son, sin duda, necesarias para maximizar la ganancia de conocimiento del esfuerzo de investigación. También pueden reducir los ensayos duplicados y acelerar el descubrimiento y la generación de nuevas ideas para la investigación. Sin embargo, cuándo y qué datos deben compartirse con quién y por qué medios, y cómo debe otorgarse crédito al propietario del conjunto de datos, sigue siendo un tema de intenso debate e investigación. Este espíritu de investigación se ha renovado aún más por el surgimiento de los problemas de privacidad asociados con los datos de los usuarios recopilados por diferentes partes cuyo principal motivo es tener un modelo mejorado al tiempo que permite el máximo conocimiento de la investigación y los beneficios científicos. Los métodos de análisis de datos pueden mejorar significativamente la calidad de los servicios, pero dependen de la recopilación, el intercambio y la extracción de datos de investigación. El usuario aporta gran parte de los datos voluntariamente; el sistema obtiene otros a partir de la observación de las actividades de los usuarios, o se deduce a través del análisis avanzado de datos voluntarios u observados.

En muchos dominios importantes, por ejemplo, la medicina y la atención médica, tanto la atención personalizada del paciente como la investigación médica pueden beneficiarse al compartir datos de investigación de ensayos clínicos para maximizar la ganancia de conocimiento del esfuerzo de investigación. No a menudo, todos los propósitos posibles para el uso de esos datos son conocidos de antemano, y el consentimiento del propietario de los datos debe solicitarse nuevamente, lo que puede ser molesto para un investigador / propietario de los datos que no ve lo que se puede ganar. Además, resulta difícil o incluso imposible para los propietarios de datos recordar qué consentimiento han otorgado a qué empresa y realizar un seguimiento de quién accede a sus datos y con qué propósito. Se requiere un mecanismo flexible para obtener y renovar el consentimiento para el uso e intercambio de datos de investigación que proporcione incentivos apropiados y significativos para capitalizar el intercambio de datos y garantiza la transparencia para que los investigadores estén al tanto de cuál de sus conjuntos de datos ha sido accedido, por quién, con qué propósito y bajo que condiciones.

Se ha observado que la creatividad y el avance de las tecnologías han dado origen a tantas redes troncales computacionales para garantizar la privacidad y el intercambio de datos a través de la

informática inteligente y la seguridad contra piratas informáticos. Sin embargo, estos servicios a menudo son criticados por los problemas de centralidad, ya que en la mayoría de los casos, no recopilan ni comparten los diversos fragmentos de datos de usuarios que provienen de las enormes entidades autónomas e independientes. El fideicomiso reside dentro de los proveedores de servicios centralizados para todo el almacenamiento y la gestión de datos. En los últimos años, los **libros de contabilidad** distribuidos y la **tecnología de cadena de bloques** han evolucionado como un medio prometedor para respaldar registros inmutables y confiables en diversos casos de uso, como asistencia sanitaria, trabajos de investigación agrícola, dominios de turismo, etc. Además, muchos sistemas de cadena de bloques proporcionan una tecnología llamada **Contrato Inteligente** "que permite la construcción automática de verificación de las condiciones de acceso o modificación de cada entidad de datos. Los contratos inteligentes se pueden implementar para codificar los fines permitidos del uso de datos de investigación, las aplicaciones de software permitidas que pueden acceder a los datos, las limitaciones de tiempo, el precio del acceso, etc.

Este capítulo propone un framework de intercambio de datos de investigación basado en blockchain que incentiva a los propietarios de conjuntos de datos con **tokens digitales**, **reconocimiento apropiado o ambos**, al tiempo que les brinda acceso a la información detallada de todos los datos en una base de datos inmutable e incorruptible.

Conclusión

Este capítulo presenta un framework descentralizado para incentivar a los investigadores a compartir sus datos de investigación que proporciona una manera de especificar / controlar los parámetros de compartir y brindar una responsabilidad total del acceso a dichos datos. La seguridad, la escalabilidad y la privacidad de esos sistemas se realizan con mediante la implementación del **contrato inteligente y las cadenas de bloque**, que pueden ofrecer la red de intercambio de datos de investigación segura y distribuida.

A Novel Blockchain as a Service Paradigm

Zhitao Wan, Minqiang Cai, Jinqing Yang and Xianghua Lin

Blockchain es un tipo de **libro mayor** distribuido en el que las transacciones de intercambio de valores se agrupan secuencialmente en **bloques**. Cada bloque está encadenado al bloque anterior y se registra de manera inmutable en una red de igual a igual, utilizando mecanismos criptográficos de confianza y garantía. Blockchain ofrece una forma segura de intercambiar cualquier tipo de activos digitalizados y crear asociaciones de confianza. Blockchain ha sacudido la industria financiera y más agencias ahora creen que la tecnología podría rejuvenecer al sector público. Los defensores argumentan que su inmutabilidad protegerá los registros de los estafadores, su transparencia mantendrá a los empleados responsables, y su capacidad para procesar automáticamente nuevas entradas puede hacer que las agencias sean más eficientes. Se espera que el mercado de blockchain crezca a una tasa compuesta anual del 61,5% para 2021, con la transparencia y la inmutabilidad como los factores que impulsan el crecimiento exponencial del mercado de blockchain.

Nordrum informó en el espectro de IEEE que Dubai desea una única plataforma de software en la que las agencias lanzarán diferentes proyectos de blockchain, mientras que Illinois diseñó un proceso más experimental que proyectos individuales que prueban diferentes tipos de plataformas y aplicaciones de blockchain para encontrar la mejor opción para sus necesidades particulares. El diseño del sistema blockchain es un proceso relativamente complejo y propenso a errores. La interconexión P2P, el almacenamiento de archivos, el mecanismo de consenso y la aplicación deben desarrollarse y probarse detalladamente. Para enfrentar el desafío de la complejidad, los gigantes tecnológicos se han subido al carro y están proporcionando **BaaSs(Blockchain as a Service)** a través de sus plataformas y colaboraciones integradas. Se espera que BaaS crezca aún más y se convierta en la última revolución en todo el mundo que hace que la adopción masiva de la tecnología blockchain se realice.

Este capítulo es un esfuerzo por mejorar los actuales BaaS emergentes. Se propone un paradigma de BaaS descentralizado y confiable para mantener las características principales de blockchain de la migración en la nube.

Conclusión

Las ventajas de las soluciones basadas en blockchain son ampliamente aceptadas. El BaaS se utiliza para acelerar el despliegue de blockchain. En comparación con la cadena de bloques convencional, proporciona un acceso universal y un enfoque fácil de aplicar. Sin embargo, los BaaS actuales erosionan las características centrales de la descentralización y la capacidad de

auditoría. La consecuencia es que la confianza disminuyó a un nivel inferior similar a las bases de datos o servicios heredados. Se propuso un nuevo paradigma para enfrentar el desafío. El paradigma propuesto introduce componentes desplegables como parte del servicio blockchain. Los componentes desplegables se pueden implementar fácilmente en la computación en la nube o en un entorno local. La implementación basada en Hyperledger muestra que el paradigma es aplicable al sistema de cadena de bloques de la corriente principal actual. El sistema de prueba de concepto demuestra una complejidad aceptable de implementación. Actualmente, la implementación requiere una ventana acoplable y necesita una instalación y configuración manual. Se intenta facilitar la implementación en entornos diferentes en el futuro con la instalación y configuración automáticas. Y, cómo migrar más blockchains a la nube como BaaSs y descubrir más paradigmas son temas interesantes

Short Paper Track: Application Researches

A Business-Oriented Schema for Blockchain Network Operation

Sheng He, Chunxiao Xing and Liang-Jie Zhang

La cadena de bloques propuesta más antigua es un modo operativo completamente abierto, es decir, la cadena de bloques pública, donde todos los nodos operativos pueden unirse o salir libremente de la red de la cadena de cadenas sin ninguna restricción. Debido a la ineficiencia y al cuidado privado de la cadena de bloques **pública**, la cadena de bloques propuesta por el **consorcio**(consortium blockchain) o la cadena de bloques **privada** propuesta más adelante restringe el comportamiento de unión de los nodos operativos de acuerdo con un acuerdo previo. Sin embargo, el **mecanismo de consenso**, la característica más importante de la cadena de bloques, está estrechamente relacionado con el modo de operación elegido. A diferencia de los incentivos endógenos de la cadena de bloques pública, los nodos operativos en la cadena de bloques del consorcio generalmente se basan en los valores extrínsecos de las necesidades comerciales, que en realidad han debilitado los incentivos del sistema de la cadena de bloques. Este capítulo está tratando de diseñar un esquema orientado a los negocios para la operación de la red de blockchain, donde los nodos tipo consorcio pueden formar una red de blockchain, pero ofrecen servicios de red de tipo blockchain con un estándar uniforme. La red fundamental de blockchain puede establecer incentivos suficientes para impulsar los nodos operativos, centrándose en cómo mejorar sus capacidades operativas y de servicio. Por lo tanto, el esquema orientado a los negocios permitirá a los proveedores finales de servicios empresariales (desarrolladores de aplicaciones) y a los consumidores de servicios empresariales (usuarios de aplicaciones) utilizar los servicios de red fundamentales de la cadena de bloques de manera fácil y conveniente como el servicio de Internet actual.

Your Device and Your Power, My Bitcoin

Song Li and Scott Wu

El aumento de la criptomoneda abre una nueva forma para que los atacantes cibernéticos se beneficien. Los atacantes primero crearon ransomware, un tipo de malware que encripta los datos de la víctima. Para descifrar sus datos, la víctima debe pagar criptomoneda para obtener la clave privada. En el último año, los atacantes crearon un nuevo malware que convierte directamente los dispositivos infectados en máquinas de minería de criptomonedas. Recientemente, los atacantes se están volcando hacia un nuevo tipo de dispositivos IoT, máquinas mineras de criptomonedas, computadoras que se construyen con el único propósito de minar criptomonedas.

La empresa que desarrolla este paper, NewSky Security, analiza tanto el malware de minería de criptomonedas como el firmware de las máquinas mineras populares, para averiguar cómo se puede infectar un dispositivo y minar los atacantes. El objetivo es descubrir formas de proteger los dispositivos para que no sean controlados por atacantes que persiguen las criptomonedas. También se propuso una manera de evaluar la pérdida de potencia causada por los malware de minería, utilizando la máquina de minería como referencia.

Conclusión

En este capítulo se describe el panorama siempre cambiante del malware de criptomoneda y cómo los atacantes utilizan todo tipo de dispositivos de IoT para cosechar la criptomoneda, así como para atacar directamente las instalaciones mineras y robar la criptomoneda. Se describe la diferencia significativa entre los atacantes de criptomonedas y los cibernéticos tradicionales, ya que los atacantes de criptomonedas necesitan que el sistema infectado se ejecute de forma coherente, a fin de drenar más CPU y ancho de banda de red para la minería. Al final del capítulo, se propone una nueva forma de evaluar el daño causado por la red de bots de minería de criptomonedas.

Blockchain in Global Trade

Jack Duan and Milan Patel

Este capítulo resume la adaptación real de la tecnología Blockchain (BC) en el espacio de comercio global. Cada producto con una identificación única es rastreado desde el fabricante de origen hasta el usuario final en todos los países. Los datos se recopilan de fabricantes, proveedores de logística y usuarios finales. Una empresa de terceros actúa como operador de red de BC, de modo que cada transacción se registra en una red privada de BC con un hash periódico guardado en una red pública de BC para garantizar la inmutabilidad de los datos. Este capítulo explora más a fondo el uso de BC para administrar el propietario y los usuarios de las fuentes de datos.

Existen dos aplicaciones comerciales para este sistema:

1. Rastrear y entregar utilizando el modelo directo al consumidor para más de 100 bodegas premium de California en más de 20 países del mundo.
2. Rastrear y entregar utilizando el modelo directo al hospital para productos farmacéuticos especializados (medicamentos contra el cáncer, etc.) desde los EE. UU. Hasta los hospitales designados en China.

Conclusión

La cadena de bloques como una red distribuida basada en pares con un almacenamiento de datos basado en el libro mayor inmutable es útil para los datos transaccionales para el comercio global. Esto se ha demostrado para los vinos estadounidenses premium y productos farmacéuticos especializados (ambos son productos altamente regulados) que se utilizan desde los Estados Unidos a otros países. El exclusivo modelo de negocio directo al usuario simplifica los modelos de negocio tradicionales de exportación e importación. Con todos los datos guardados en la red de BC, beneficia a todos los participantes con una responsabilidad de canal, autenticidad del producto y eficiencia logística muy confiables. A medida que las funciones de administración de identidades basadas en BC se vuelvan maduras, el intercambio de identidades en las transacciones globales estará más protegido y bajo el control de los propietarios de identidades.