O'REILLY®

Compliments of IBM

Getting Started with Enterprise Blockchain

A Guide to Design and Development

Michael Bradley, David Gorman,
Matt Lucas & Matthew Golby-Kirk

Getting Started with Enterprise Blockchain

A Guide to Design and Development

Michael Bradley, David Gorman,
Matt Lucas, and Matthew Golby-Kirk

Beijing • Boston • Farnham • Sebastopol • Tokyo O'REILLY®

Introducción al Blockchain empresarial Una guía para el diseño y el desarrollo

Blockchain es un libro de contabilidad compartido y distribuido que registra transacciones a través de redes empresariales con el objetivo de ayudar a las empresas a eliminar ineficiencias del comercio. Lo hace mediante el uso de pruebas (proof) criptografícas, que ayudan a generar confianza al garantizar que los hechos sean informados consistentemente a todos aquellos que necesitan verlos. Ese es el discurso del acenso de blockchain. En el resto de este capítulo, analizaremos con más detalle qué es blockchain y por qué es así de importante. Para empezar, exploremos la necesidad de redes empresariales.

Redes Empresariales

La riqueza se genera en las economías de mercado por el flujo de bienes y servicios a través de redes empresariales. Las redes empresariales son necesarias debido a las enormes ventajas que aporta la especialización. El economista Adam Smith escribió por primera vez sobre estas ganancias de eficiencia refiriéndose al ejemplo de la producción de alfileres, en trabajos que actualmente está inmortalizado en el reverso de un billete inglés de £ 20. El economista Leonard Read, en su breve artículo "Yo, lápiz", utilizó posteriormente el ejemplo de un lápiz, y el hecho de que nadie en la tierra sabe cómo crear uno completamente desde cero, para demostrar la importancia de las redes empresariales a la industria manufacturera.

Las redes empresariales no sólo son necesarias para fabricar cadenas de suministro más eficientes; También se utilizan en cualquier tipo de interacción entre empresas. Las redes comerciales pueden abarcar fabricantes, empresas de logística, bancos, aseguradoras, consumidores: cualquier persona u organización que esté dispuesta a intercambiar un activo por otro, ya sea que ese activo sea tangible (por ejemplo, casas, automóviles, efectivo, terrenos) o intangible (por ejemplo, servicios, propiedad intelectual, patentes, licencias).

Usemos un ejemplo para ilustrar la importancia del tejido empresarial y cómo se genera la riqueza.

Ted el empresario

Ted es un hombre de negocios que aparece en un pequeño pueblo para hablar en una conferencia, al día siguiente. Fue fichado por la conferencia en el último minuto, así que cuando llega al pueblo todavía necesita un hotel para pasar la noche. Encuentra uno, se acerca al dueño y reserva una habitación. Colocando $100 en la recepción. “Volveré en breve”, dice al dueño del hotel. "Primero voy a comprobar el lugar de la conferencia". Ted se aleja.

Unos momentos más tarde, el propietario del hotel lleva los 100 dólares a un constructor local quien hizo algunos trabajos menores de reparación en el hotel la semana anterior. "Aquí está los 100 dólares que te debo”, le dice el dueño del hotel al constructor. El propietario regresa a su hotel. El constructor, con dinero en mano, se había interesado por un bonito jarrón que había estado en exhibición en la tienda de antigüedades local. Lleva los $100 a la tienda de antigüedades, compra el jarrón y felizmente se lo lleva a su casa.

Los dueños de la tienda de antigüedades eran una pareja de ancianos que de pasó están llegando a su 40 aniversario de bodas. Para celebrarlo toman los $100 que acaban de recibir del constructor y deciden gastarlos en noche en un hotel local, el mismo hotel en el que Ted había reservado una

habitación antes. La pareja llega a la recepción, paga $100 al propietario del hotel, se registra en su habitación y disfruta de un breve descanso encantador. Después de revisar el lugar de la conferencia, Ted regresa al hotel y le da malas noticias al dueño del hotel. "Lo siento", dice Ted. Resulta que mi conferencia ha sido cancelada. Por favor, ¿puedo tener mi Devolución de dinero? El dueño del hotel acepta y le devuelve los $100 a Ted, quien luego regresa a casa, decepcionado por no haber hablado en la conferencia, pero de lo contrario, no de su bolsillo.

¿Qué pasó en esa historia?

La historia comienza y termina exactamente con la misma cantidad de activos en la ciudad, pero fundamentalmente los diferentes participantes de este negocio cada red ha ganado utilidad debido al flujo de capital (los $100) dentro de él: el dueño del hotel ha alquilado una habitación, el constructor tiene un jarrón, y los dueños de las tiendas de antigüedades tienen sus vacaciones. Ted el empresario simplemente sirvió como estímulo para iniciar el flujo de transacciones, proporcionando el insumo de capital inicial y la producción de capital final.

Puede ver este flujo en la Figura 1-1.

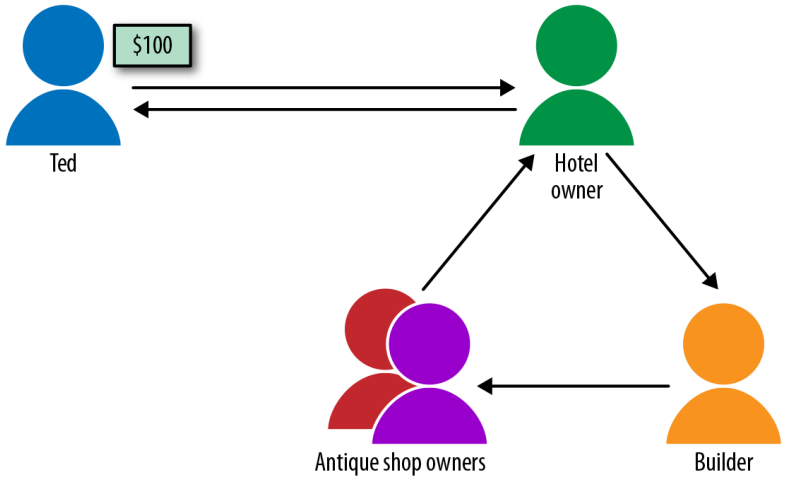

Figura 1-1. El flujo de transacciones en el tejido empresarial de la ciudad

Es un escenario simplista, pero la lección aquí es que lo más importante importante para la generación de utilidad (y, en última instancia, riqueza) es el flujo de activos (bienes, servicios y efectivo) alrededor de una red. Puede fabricar una gran cantidad de activos, pero si nadie está dispuesto a intercambiar otros bienes y servicios (o efectivo) para ellos, verdadero crecimiento económico no puede ocurrir. (Existen otras formas de generar riqueza artificialmente, como las ganancias obtenidas mediante la especulación en el mercado de valores. Está más allá del alcance de este libro, pero remitimos a cualquier persona interesada a cualquier buena guía.)

En realidad, las redes empresariales pueden ser enormemente complejas. puede tomar muchos cientos de proveedores y fabricantes para obtener y ensambla los componentes de tu auto. El valor de las transferencias de fondos entre instituciones financieras estadounidenses asciende a billones de dólares estadounidenses cada día, y esto requiere un sistema de red empresarial que sea altamente disponibles, eficientes y resilientes.

Entonces, ¿qué tiene esto que ver con blockchain? Bueno, una blockchain es un sistema para registrar el flujo de activos en una red empresarial; Permite los participantes asociados con las transacciones registrar que sucedieron con ellas. Por supuesto, ya tenemos un sistema para hacer esto: se llama el libro mayor. ¿En qué se diferencia blockchain?

El libro mayor

Dependiendo de cuándo empieces a contar, el concepto de libro mayor tiene existe desde hace más de 500 años. En 1494, un monje franciscano y matemático Luca Pacioli publicó Summa de arithmetica, geometría; proporcionali et proporcionalita (Resumen de aritmética, geometría, proporciones y proporcionalidad), que dio la primera descripción escrita del concepto de contabilidad por partida doble, dando lugar a los libros de contabilidad tal como los conocemos hoy.

Los libros mayores son esencialmente registros de transacciones: listas ordenadas de entradas y resultados de una empresa. Su extracto bancario es un ejemplo de libro mayor personal; muestra cada débito y crédito en su cuenta y detalles de la organización con la que realizó la transacción. Los libros de contabilidad son particularmente importantes para las empresas porque describen lo que poseen y cuánto valdría el negocio si iba a ser vendido. Una empresa podría tomar su saldo inicial y por cada transacción suma el valor de los créditos y resta el valor de los débitos, para derivar su patrimonio neto. El patrimonio neto derivado de los libros mayores de la empresa se conoce como posición de liquidez, que se pueden utilizar otras cosas para influir en las decisiones de inversión, para satisfacer auditores y gestionar el riesgo.

Los libros de contabilidad han evolucionado desde los libros encuadernados en cuero de Luca Día de Pacioli, y ahora suelen estar representados por una base de datos de alguna clase. Pero los conceptos (y las deficiencias) siguen siendo los mismos, pero de eso hablaremos más adelante.

Transacciones y Contratos

Si un libro mayor es un registro de transacciones, ¿qué es realmente una transacción? A generalmente se entiende por transacción el cambio de propiedad de una activo a cambio de otra cosa. Entonces, si Matt compra el auto de Helen, la transacción registrada es el intercambio de un automóvil a Matt por el precio acordado. Matt registraría esa transacción en su libro mayor y Helen registraría la misma transacción en el suyo (el débito pasa a ser crédito y el crédito pasa a ser débito, de curso).

Una transacción podría ser el intercambio de dos bienes, uno de los cuales puede ser efectivo. De manera más general, se podría considerar que una transacción significa cualquier cambio en el estado de un activo. Si se vuelve a pintar un automóvil de amarillo a verde aumenta su valor de reventa, esto podría tener un efecto en el patrimonio neto del propietario, por lo que podría ser útil iniciar sesión en un libro mayor.

Las transacciones están respaldadas por un conjunto de términos y condiciones, las cuáles son los requisitos previos para que esa transacción sea válida. Cuando al comprar el auto de Helen, es posible que venga con una garantía que diga que si el coche resulta defectuoso y Matt recupera su dinero. Para muchas transacciones, los términos de la transacción son acordados por los participantes y representado en un contrato. Las transacciones y los contratos están estrechamente vinculados; una transacción puede ser considera como la invocación de las reglas de un contrato, y

esto así es precisamente como las blockchains tienden a ejecutar sus implementaciones de contratos (también conocidos como contratos inteligentes). De nuevo, más sobre esto más tarde.

Los problemas con los libros mayores y los contratos

Tanto los libros de contabilidad tradicionales como los contratos tradicionales tienen problemas. El problema con los libros de contabilidad es que todos en la red empresarial tiene su propia versión. ¿Qué pasa si un participante ha registrado una transacción? en su libro mayor, pero el otro participante lo ha registrado de manera diferente, ¿O incluso no tiene constancia de ello? ¿Qué pasa si Matt registra el hecho? que compró el auto de Helen, pero Helen no: cuyo libro de contabilidad es correcto, ¿Y quién es el dueño del auto? Es importante para las empresas, mientras que las transacciones están en disputa, los activos no pueden reclamarse como parte de un patrimonio neto de la empresa. Es común que las empresas tengan un número de transacciones en disputa en un momento dado. Por ejemplo, IBM el brazo de Financiamiento Global tiene una gran cantidad de dinero invertido en disputas, hasta $100 millones en capital en disputa a la vez, lo cual es una cantidad significativa responsabilidad con un proceso de resolución de disputas que puede tomar muchas semanas para liquidar una transacción.

Es un problema similar para los contratos: son ambiguos por su naturaleza. Los contratos representan un acuerdo abstracto entre múltiples participantes; lo que está escrito en papel o implementado en los sistemas de TI puede no ser la esencia de lo que los participantes pensaban que estaban suscribiendo. Los contratos a menudo pueden tomar equipos de abogados y jueces para interpretar.

La falta de un significado mutuamente acordado tanto para los libros mayores como para los contratos conduce al largo y costoso proceso de reconciliación, que garantiza que los detalles de la transacción y la ejecución del contrato sean correctos sincronizado y acordado por todos los participantes relevantes. Las disputas conducen a procesos (a menudo manuales) de resolución de disputas, que a su vez puede llevar a procesos legales aún más largos y costosos. Esto podría ser genial para los abogados, pero no tanto para los participantes involucrados en esas disputas.

Ingrese a la cadena de bloques

Blockchain tiene como objetivo resolver los problemas de los libros de contabilidad y los contratos mediante la compartición de este de forma inequívoca entre los participantes de la red empresarial. Se puede hacer referencia a Blockchain como un sistema compartido y distribuido de libro mayor con contratos inteligentes.

Separemos esos términos. En primer lugar, blockchain es un libro de contabilidad: una transacción registro que se puede utilizar para describir las entradas y salidas de un negocio. En segundo lugar, se comparte entre los participantes de la red de modo que todos vean el mismo conjunto de hechos. Finalmente, evita cualquier punto único de falla asegurando que las copias se distribuyan a todos los que necesiten verlo.

Los contratos inteligentes se refieren a un código informático que se comparte entre los participantes de la red empresarial, y estos implementan las reglas del negocio asociadas con cada transacción. Como el código es compartido, puede ser ejecutado por todos los participantes relevantes y pueden acordar la producción.

A pesar del nombre, los contratos inteligentes no son contratos. Contratos inteligentes puede utilizarse para proporcionar la ejecución compartida de los términos del contrato, de la misma manera que los sistemas de TI de un solo participante pueden ejecutar el contrato términos hoy. No se esperaría que un juez dictaminara sobre el significado de un contrato inteligente, ya que no suelen ser ingenieros de software. Sin embargo, podrían regir sobre el contrato jurídico del que procede o deriva.

Un ejemplo de coche

Para ilustrar cómo funcionan los libros de contabilidad compartidos y los contratos inteligentes, imaginemos el escenario de una cadena de bloques que rastrea la propiedad de un automóvil. La cadena de bloques en sí sería una estructura de datos ordenada que contiene los detalles de cada cambio de propiedad acordado. Por ejemplo, una transacción podría indicar que “la propiedad del automóvil con número de identificación CXU7592875 ha cambiado de Helen a Mate." El contrato inteligente asociado con esta transacción describe la lógica informática que hace que se realice la transacción: por ejemplo, "verifique que el vendedor sea igual al propietario actual y, si lo es, establezca el propietario como comprador, disminuir el saldo de efectivo del comprador, e incrementar el saldo de caja del vendedor”.

Cada participante interesado (por ejemplo, Helen y Matt) ejecutaría ese código de contrato inteligente y acordará el resultado, y si todo es aceptable, luego actualiza el libro mayor en consecuencia. El libro mayor actualizado podría hacerse visible para Helen y Matt, pero también para otras partes interesadas, como el regulador de vehículos o las aseguradoras, dependiendo de las reglas acordadas de la red. Las cadenas de bloques son útiles porque ayudan a generar confianza en las redes de empresas, que es algo que los sistemas tradicionales de empresa a empresa no pueden proporcionar. Con una base de datos compartida, por ejemplo, no hay garantía de que un administrador no haya alterado la transacción. Blockchain ofrece a los participantes de una transacción el no repudio, lo cual es evidencia de que la transacción fue acordada.

Blockchain y confianza

La cadena de bloques puede generar confianza al proporcionar pruebas de que se acordaron las transacciones. Para ello, la cadena de bloques implementa varias cualidades de servicio relacionadas, incluido el **consenso**, la **procedencia**, **inmutabilidad** y **finalidad**.

• El consenso es el proceso mediante el cual se acuerdan las transacciones por los participantes en la red. Esto significa acordar cuáles transacciones ocurrieron, en qué orden y cuál fue el resultado de ejecutar cada transacción. Participantes que necesitan proporcionar ese acuerdo podrían ser solo aquellos afectados por él (en nuestro ejemplo, solo Matt y Helen), pero también podría incluir participantes interesados (como un proveedor de pagos), o en el Caso de blockchains públicas como Bitcoin, la mayoría de la red.

Procedencia significa que debería ser posible revisar antes transacciones para determinar el historial asociado a los activos. Por ejemplo, como propietario actual del coche, Matt debería poder ver su historial de fabricación, propiedad y servicio, a la derecha hasta el punto de venderlo. Estas reglas de visibilidad se deciden y son gobernado por la red (más sobre esto más adelante).

• La inmutabilidad es el hecho de que el historial de transacciones compartido no puede ser manipulado. Una vez que se ha acordado una transacción a través del consenso de la red y almacenado en la cadena de bloques, entonces no se puede editar, eliminar ni tener nuevas transacciones insertado antes de él. Esto hace que la cadena de bloques sea solo un anexo de estructura de datos, y es la razón por la cual la procedencia de la transacción es posible.

• La finalidad es la propiedad de que la transacción no puede modificarse una vez acordado. Las transacciones no deseadas sólo pueden ser revertido por la adición de una nueva transacción que revierte la transacción anterior, nuevamente con el acuerdo de la parte relevante.

Tenga en cuenta que la prueba no es lo mismo que la confianza. Blockchain proporciona prueba criptográfica del conjunto de transacciones, y corresponde a los participantes decidan si confiar o no en esa prueba, en la mayoría de los negocios en estos escenarios esto no es un problema. Pero imaginemos, por ejemplo, que un blockchain se utilizaron para rastrear la votación en una elección nacional. El sistema podría proporcionar una votación segura de una sola vez con un seguimiento de auditoría completo, pero sería crucial que contara con la confianza tanto de los perdedores de las elecciones como del electorado en general. Dada la desconfianza de muchas personas en las computadoras, éste no es un problema trivial de resolver; blockchain puede proporcionar el componente técnico de una solución a un problema que requiere algo más que tecnología.

Cadena de bloques y Bitcoin

Blockchain no es lo mismo que Bitcoin, aunque para muchas personas la primera experiencia de blockchain es a través de Bitcoin. Bitcoin es un sistema de pago que se describió por primera vez en un documento técnico de 2008 presentado bajo el nombre de Satoshi Nakamoto. Este documento técnico no hace en realidad mención de blockchain por su nombre, pero describe un mecanismo para enviar pagos de forma segura entre participantes anónimos.

Bitcoin utiliza lo que ahora llamamos blockchain para registrar el conjunto de transacciones confirmadas. Bitcoin introdujo una clase de activo llamada “criptomoneda”, que es como una moneda normal en el sentido de que es un recurso escaso que puede usarse (en teoría) para pagar bienes y servicios. Desde la introducción de Bitcoin, las criptomonedas han ganado popularidad. En el momento de escribir este artículo, la capitalización de mercado de las criptomonedas ha caído drásticamente, pero la cantidad de criptomonedas aún supera con creces la cantidad de monedas fiduciarias.

La criptomoneda bitcoin realmente no existe fuera de la red Bitcoin, de la misma manera que el saldo que tienes en un banco. La cuenta probablemente no existe fuera de un número en un registro en un base de datos bancaria, al menos hasta que vayas a un cajero automático. La moneda bitcoin se puede convertir en moneda fiduciaria mediante intercambios. Dado esta capacidad de retirar dinero y proporcionar capital en el mundo real, bitcoin ha sido tratado como una mercancía como el oro. Sin embargo, a diferencia de otros Bitcoin no está regulado en gran medida y es ampliamente incomprendido, lo que ha provocado, entre otras cosas, una enorme volatilidad en su precio de mercado.

La red Bitcoin New York

La red Bitcoin tiene un seudónimo y la cadena de bloques es totalmente público; puede ver el libro mayor de Bitcoin en su totalidad. Este seudónimo significa que, a menos que se puedan realizar análisis profundos de la red (por ejemplo, ChainAnalysis), como el seguimiento de transacciones en los intercambios, es casi imposible determinar la identidad de un usuario de Bitcoin. Esta es la razón por la que los piratas informáticos suelen solicitar el pago en bitcoins si su computadora ha sido comprometida. Los pagos de rescate no pueden rastrearse fácilmente hasta individuos, ya que los participantes asociados con transacciones individuales son secuencias sin sentido de números hexadecimales.

Dada esta falta de identidad en la red Bitcoin, Bitcoin tiene una técnica innovadora pero costosa para garantizar el consenso como, por ejemplo, imagina que tienes $100 e intentas transferir $50 a tres participantes al mismo tiempo. ¿Cómo está de acuerdo la red? ¿Cuáles dos transacciones tienen éxito y cuál falla? Esto es conocido como el problema del doble gasto, y es un ejemplo del tipo de procesamiento que realiza la red Bitcoin.

Es crucial que la red acuerde el orden en que se realizan las transacciones y los resultados de esas transacciones. De lo contrario, el sistema no podría funcionar de forma fiable. Para ello, utiliza un complejo proceso de consenso llamado “Prueba de trabajo” (“Proof of Work”), que se basa en una red de computadoras colaboradoras.

¿Qué es la prueba de trabajo?

La prueba de trabajo funciona agregando un costo artificial a la verificación de transacciones. Si quieres convencer a la red que su conjunto y orden de transacciones es correcto, tienes que demostrarle a la red que tienes incurrió en este costo. Lo hace forzando a los nodos de la red para resolver acertijos criptográficos que son difíciles resolver (es decir, requerir técnicas de fuerza bruta), pero son trivialmente fáciles de verificar para otros nodos una vez que se ha encontrado la respuesta. Para cada conjunto de transacciones (conocido como bloque), el primer nodo de la red que resuelva el rompecabezas criptográfico recibe una recompensa en Bitcoin. Esto se conoce como minería criptográfica y es una de las formas en que se mantiene segura la red Bitcoin. La prueba de trabajo es como darle a una sala llena de estudiantes un cubo de Rubik revuelto cada uno, y exigiéndoles que resuélvelo antes de que puedan hacer una pregunta. Lo sabemos, el cubo es difícil de resolver, pero fácil de verificar para el profesor si se ha solucionado. Esto tiene el efecto de eliminar el incentivo para hacer malas preguntas, porque saber que un estudiante debe tomarse en serio la pregunta si están dispuestos a hacer el esfuerzo de resolver un Rubik Cubo para preguntarlo.

El problema con la Prueba de Trabajo es que requiere un esfuerzo extraordinario y cantidad de electricidad para funcionar. Las estimaciones varían, pero se cree que la implementación de Prueba de Trabajo de Bitcoin utiliza el equivalente al consumo de energía de un país como Irlanda.

Blockchain no es Bitcoin. Además, los requisitos típicos de Blockchain para empresas es totalmente diferente de los requisitos de Bitcoin blockchain. En concreto, el uso de activos no regulados, El anonimato, la imposibilidad de rastrear y los requisitos excesivos de energía conducen a Muchas empresas tienen dificultades para adoptar Bitcoin para transacciones entre empresas. Esto ha llevado a la introducción de diferentes Implementaciones de blockchain que se ajustan mejor a las

necesidades de las empresas y, al mismo tiempo, pueden lograr pruebas criptográficas de un conjunto de transacciones.

Los requisitos de Blockchain para las empresas

Los requisitos de blockchain para las empresas en realidad difieren de Bitcoin de cinco maneras distintas: (1) los activos que se rastrean, (2) conocer a los participantes de cada transacción, (3) las reglas sobre privacidad y confidencialidad, (4) cómo se respaldan las transacciones y (5) cómo se gobierna la red. Discutiremos cada uno de estos en la siguiente sección.

Los activos que se rastrean

Blockchain se puede utilizar para una gama mucho más amplia de activos que solo las criptomonedas. Los activos tangibles, como automóviles, bienes raíces y productos alimenticios, así como los activos intangibles, como la propiedad intelectual, las licencias y los conjuntos de información compartida, son todo un juego limpio, siempre que puedan representarse digitalmente. Parte del arte de configurar una cadena de bloques en un entorno empresarial es decidir qué compartir.

Conocer a los participantes de cada transacción

Como hemos visto, Bitcoin prospera gracias al anonimato: cualquiera puede ver el libro mayor de Bitcoin y ver cada transacción que haya ocurrido, pero la información de los participantes no es rastreable. Por otra parte, las empresas tienen requisitos como KYC (conozca a su cliente) y AML (contra el blanqueo de capitales). Estos son ejemplos de cumplimiento de reglas que requieren que las empresas sepan exactamente con quién están tratando con.

Las reglas sobre privacidad y confidencialidad

La privacidad y la confidencialidad son requisitos clave de una cadena de bloques para negocio. En primer lugar, de la misma manera que los mercados pueden ser públicos o privados, debería ser posible que una cadena de bloques sea privada, es decir que la red pueda decidir exactamente quién se une. Una cadena de bloques pública aumenta el riesgo de que una empresa realice transacciones o inadvertidamente de información de relación de conocimiento público, ya sea accidental o a través de medios maliciosos (por ejemplo, explotando vulnerabilidades). Además, las transacciones individuales requieren confidencialidad para evitar dar a otros miembros una ventaja injusta. Probablemente no queramos que un proveedor en la red sepa el nivel de descuento que le estamos dando a otro proveedor, incluso si están en la misma cadena de bloques. Por supuesto, un regulador podría exigir una visibilidad total de todas las transacciones.

Características como estas dan lugar a la necesidad de obtener permisos de la red blockchain, donde diferentes participantes pueden hacer cosas diferentes. Es posible tener redes públicas y autorizadas como Stellar, así como redes privadas autorizadas como IBM Food Trust construidas con Hyperledger Fabric.

Las redes autorizadas son totalmente diferentes a Bitcoin, que es tanto públicos como no autorizados. Bitcoin revela a todos todas las transacciones que ocurrieron, pero no quién está involucrado en ellas. Las empresas necesitan todo lo contrario: saber con quién están tratando, pero no necesariamente consciente de los detalles de cada transacción. Estos requisitos de privacidad

también significan que probablemente no sea factible tener una única instancia de blockchain que cubra todo. Al igual que hoy en día existen muchos libros de contabilidad (y hay muchas redes de empresa a empresa), probablemente habrá muchas cadenas de bloques en un futuro previsible, aunque con la capacidad de transferir activos entre instancias: una red de redes, en otras palabras.

Cómo se respaldan las transacciones

No se suele conseguir consenso en una blockchain para empresas a través de Prueba de trabajo, pero a menudo a través de un proceso de aprobación selectiva. Esto significa poder controlar exactamente quién recibe y respalda las transacciones, de la misma manera que suceden los negocios hoy. Si transferimos dinero a un tercero, entonces nuestro banco, el banco del destinatario, y posiblemente un proveedor de pagos respaldaría la transacción. Estas transacciones luego son validadas por aquellos en la red tiene permiso para recibirlos. Esto es diferente de Bitcoin, donde los mineros compiten para respaldar transacciones a cambio para una recompensa de bitcoin y una red de usuarios que ejecutan nodos completos (aquellos que verifican completamente todas las reglas de Bitcoin) colaboran para verificar transacciones.

Cómo se gobierna la red

Las redes Blockchain se pueden gobernar de dos maneras: utilizando una política preacordada o mediante un conjunto de tokens. Basado en políticas los enfoques requieren un conjunto de reglas acordadas desde el principio por las partes interesadas clave, como un consorcio de miembros, un regulador o un creador de mercado. Las reglas pueden ser de amplio alcance y podrían, por ejemplo, describir cómo se logra el consenso, cómo se deciden los cambios futuros en la membresía o quién es responsable de los errores en los contratos inteligentes. Algunas cadenas de bloques utilizan tokens para controlar el comportamiento. La cadena de bloques pública Ethereum es un ejemplo en el que su riqueza (en términos de su saldo de la criptomoneda Ethereum conocida como Ether) se utiliza para determinar su capacidad de procesamiento de contratos inteligentes.

Se considera que la política basada en tokens está en la gobernanza de la cadena como en la capacidad de gobernar está encerrada en la cadena de bloques. Gobernanza basada en políticas Puede estar tanto dentro como fuera de la cadena dependiendo del acercamiento. Tanto los enfoques de gobernanza basados en políticas como los basados en tokens son reflexivos de sistemas establecidos en el mundo real. Por ejemplo, las leyes de un país son un sistema de gobierno basado en políticas, pero su riqueza puede determinar otras cosas que puedes hacer dentro de ese marco. Mientras que los primeros negocios las cadenas de bloques generalmente se han gobernado a través de políticas. Hay un número cada vez mayor de blockchains empresariales que se han ampliado con sistemas de fichas como medio para fomentar el comportamiento dentro la red.

Tecnología de cadena de bloques

Para que cualquier blockchain empresarial tenga éxito, los participantes deben acordar el enfoque para compartir transacciones y contratos inteligentes. De la misma manera que HTTP(S) es un enfoque acordado para compartir información a través de Internet, es necesario que exista un estándar común para blockchains (al menos dentro de cada red empresarial) para la red crecer y prosperar.

Hay muchas decisiones que deben tomarse al establecer una red, incluidos formatos de datos de activos y transacciones, topología de red, reglas de gobernanza y validación. Uno de las más importantes decisiones es la elección de la tecnología blockchain: el software que proporciona la implementación del libro mayor compartido y el contrato inteligente marco de ejecución. Los participantes de la red deben adoptar la misma tecnología para compartir información; no hay universalidad estándar de interoperabilidad para tecnologías blockchain todavía, aunque el trabajo de estandarización continúa.

La tecnología blockchain seleccionada debe complementar al proveedor, sesgos y diversos panoramas de TI que normalmente están presentes en las redes empresariales. Esto significa que la apertura de la tecnología blockchain es esencial, no sólo en términos de la fuente, sino también para que toda la comunidad tenga la oportunidad de influir en la dirección del proyecto (lo que se conoce como gobernanza abierta). Por lo general, no tiene sentido adoptar una tecnología blockchain patentada, ya que requeriría que todos los participantes presentes y futuros en la red empresarial adopten el mismo proveedor, lo que aumenta el riesgo de bloqueo, aumentos de costos y falta de margen para innovación.

El proyecto Hyperledger

En febrero de 2016, la Foundation®Linux anunció formalmente Hyperledger®, un esfuerzo de gobernanza abierta y de código abierto para avanzar el blockchain intersectorial. Sirve como invernadero para múltiples tecnologías blockchain, incluidos marcos que implementan libros de contabilidad compartidos y replicados y herramientas para desarrollar y operar instancias de ellos.

Al igual que otros proyectos de la Fundación Linux, Hyperledger se basa en este espíritu de apertura, y esto ha contribuido a su constante éxito. Al momento de escribir este artículo, más de 260 organizaciones se han unido a Hyperledger desde una amplia gama de industrias y disciplinas, y hay una fuerte comunidad de desarrolladores que ha estado contribuyendo a más de 10 proyectos individuales bajo el paraguas de Hyperledger.

Uno de los proyectos Hyperledger más avanzados se llama Hyperledger Fabric™. Esto proporciona una implementación del libro mayor compartido y el marco de ejecución de contratos inteligentes, y se basa en los principios de seguridad (para reflejar las necesidades de las empresas reguladas) y modularidad (para permitir la innovación). Lo desarrolla un equipo mundial que representa docenas de organizaciones únicas y hay numerosos ejemplares en producción. Este libro se centrará principalmente en Hyperledger Fabric.

IBM y Blockchain

IBM ha contribuido con código, propiedad intelectual y recursos de desarrollo a Hyperledger desde sus inicios. La plataforma IBM Blockchain fue la primera plataforma disponible comercialmente para aprovechar las tecnologías de Hyperledger. Plataformas como esta proporciona un conjunto de herramientas para ayudar con el desarrollo, la gobernanza y la operación de las redes Hyperledger Fabric, y se ha utilizado para respaldar muchas de las soluciones blockchain en producción hoy en día, incluidas IBM Food Trust y TradeLens. Estas redes, junto con las de otros proveedores, se pueden descubrir en un registro público de redes llamado Registro de redes ilimitadas.

Resumen

En esta sección hemos visto qué es blockchain para empresas: un Libro mayor compartido, distribuido y autorizado con contratos inteligentes. Blockchain es importante porque ayuda a generar confianza en las redes empresas proporcionando pruebas criptográficas sobre un conjunto de transacciones. Esto puede eliminar la fricción de las redes empresariales, por ejemplo, eliminando la necesidad de costosos procesos de resolución de disputas.

Blockchain no es Bitcoin; los requisitos de blockchain para los negocios son completamente diferentes y se centran en características como confidencialidad y activos del mundo real. También hemos analizado Hyperledger, alojado por la Fundación Linux, y cómo pretende resolver estos requisitos de blockchain para negocio. Concluimos analizando la contribución de IBM a blockchain y cómo está ayudando a los clientes en el camino de este apasionante tecnología.

En el próximo capítulo veremos qué hace que el blockchain sea buena solución y evaluar algunos ejemplos de cómo blockchain ha sido utilizado con gran efecto.

CAPITULO 2

Identificando cuándo usar Blockchain

En este capítulo analizamos cuándo utilizar blockchain como solución. Nosotros vimos en el Capítulo 1 que blockchain es un sistema compartido, distribuido y autorizado, de libro mayor que registra transacciones a través de una red empresarial. Hay algunos requisitos específicos de un escenario que hacen particularmente adecuado para el uso de blockchain, y exploraremos esos en este capítulo.

Primero, identificaremos los tipos de problemas que enfrentan las redes empresariales antes de mirar los criterios que utilizamos para determinar si blockchain hace que esta buena tecnología sea adecuada para resolver esos problemas.

Identificación de problemas en la red empresarial Es importante tener una idea clara de los requisitos del escenario y saber qué problemas se intenta resolver. Esto puede parecer obvio, pero con cualquier tecnología nueva (y particularmente con una muy publicitada) a menudo existe la tentación de lanzarse a una implementación sin pensar mucho en los problemas que pretende resolver.

Las empresas actúan por varias razones. Lo más común es que vayan a buscar un nuevo mercado (por ejemplo, abrir oportunidades de financiación del comercio a pequeñas y medianas empresas), o tratar de eliminar costos o ineficiencias de un proceso empresarial (por ejemplo, eliminar intermediarios). Identificar los problemas y expresarlos en términos de ganancia esperada (o retorno de la inversión) es el primer paso para proyecto exitoso.

Volvamos a la solución blockchain de Global Financing presentada por IBM en el Capítulo 1. Identificaron que dentro de esta red empresarial de unos 4.000 participantes que había 100 millones de dólares de capital en disputa en cualquier momento. Esta era una responsabilidad importante y era un resultado directo del tiempo necesario para resolver unas 25.000 disputas al año de los 2,9 millones de facturas emitidas. Ejemplos de disputas incluir el número incorrecto de piezas de computadora que se entregan en un el pedido o las entregas van mal. También se observó que cada uno de las 25.000 disputas tardarían en promedio 44 días en resolverse, lo que requeriría alguien que vuelva sobre los pasos a través de seis o siete aplicaciones, incluyendo contactar con terceros como bancos.

Podemos resumir los problemas como:

1. Disputas que surgen debido a problemas de envío

2. No existe una única fuente de información confiable que ayude a resolver los problemas.

3. Transacciones en disputa que tardan mucho en resolverse

En “The Blockchain Fit” en la página 21, revisaremos estos problemas y veremos si blockchain puede ayudar a proporcionar una solución sensata para resolverlos. Antes de eso, veremos los beneficios de una solución blockchain.

¿Cuáles son los beneficios de una solución basada en blockchain?

Blockchain es una solución para redes empresariales. Tiene sentido implementar una solución basada en blockchain solo donde haya una red de participantes colaboradores que emiten transacciones en torno a un conjunto de activos comunes en la red.

Por lo tanto, nuestra primera observación de cuándo blockchain es la solución correcta es que debe haber una red empresarial de múltiples participantes. Nuestro segundo sería que requieren una visión compartida de los activos y sus transacciones asociadas.

Luego utilizamos las siguientes cuatro características clave de blockchain introducidas en el Capítulo 1 para definir mejor los beneficios de una solución basada en blockchain.

Recordemos estos beneficios:

Consenso

El proceso de acordar nuevas transacciones y distribuírselos a los participantes de la red.

Procedencia

Un historial completo de todas las transacciones relacionadas con los activos registrados en la cadena de bloques.

Inmutabilidad

Una vez que una transacción se ha almacenado en la cadena de bloques, no puede editarse, eliminarse o insertarse transacciones antes.

Finalidad

Una vez que una transacción se confirma en la cadena de bloques, se considera "final" y ya no se puede "revertir" ni deshacer.

Hay varios otros beneficios de blockchain que sustentan estos cuatro beneficios clave, y vale la pena tenerlos en cuenta al revisar cualquier escenario potencial:

Identidad

Todos los participantes en una red blockchain autorizada tienen una identidad en forma de certificado digital: la misma tecnología que sustenta la seguridad y confianza cuando utilizamos un web navegador para acceder a nuestro banco en línea.

Seguridad

Cada transacción en la red autorizada es criptográficamente firmada, lo que proporciona autenticidad de qué participante lo envió, no repudio (lo que significa que no pueden negar el envío), e integridad (lo que significa que no ha cambiado desde que se envió).

Contratos

Los contratos inteligentes contienen la lógica empresarial para las transacciones y son ejecutado a través de la red por los participantes que respaldan una transacción. Estos beneficios ayudan a

generar confianza entre los participantes en las redes de negocios, y podemos utilizarlas como prueba de fuego a la hora de comprobar si blockchain es una buena tecnología. Debemos notar que, si bien no es necesario que un escenario requiera todos los beneficios enumerados, cuanto más se requieren, más se fortalece el caso por usar blockchain.

Siempre debemos tener cuidado al pensar que blockchain es una panacea para todas las soluciones. Hay muchas razones por las que blockchain no encaja bien. Por ejemplo:

• Blockchain no es adecuado si solo hay un participante en la red empresarial.

• Aunque hablamos de transacciones y bases de datos de estados mundiales en blockchain, no debería considerarse como un reemplazo de servidores de transacciones o bases de datos tradicionales.

• Blockchain por diseño es una red distribuida de igual a igual, y se basa en gran medida en la criptografía. Con esto vienen una serie de consideraciones de requisitos no funcionales. Por ejemplo, el rendimiento y la latencia no coincidirá con una base de datos tradicional o servidor de transacciones, pero escalabilidad, redundancia y alta disponibilidad están incorporados.

Activos, participantes y transacciones

Al pensar en una posible solución blockchain y sus beneficios que trae a la red de participantes, es útil verlo en relación con los siguientes conceptos:

• Activos

• Participantes

• Transacciones

Ya hemos introducido algunos ejemplos de estos, son conceptos centrales en una red blockchain que se favorecen de los cuatro principales beneficios fiduciarios introducidos en la sección anterior.

Activos

Ya sea puramente digital o respaldado por un objeto físico, un activo representa algo que está registrado en la cadena de bloques. El activo puede compartirse en toda la red o mantenerse privado dependiendo de sobre los requisitos. Un contrato inteligente define el activo.

Participantes

Los participantes ocupan diferentes niveles en una red blockchain. Son aquellos participantes que dirigen partes de la red y respaldan transacciones. Otros miembros podrán consumir servicios de la red, pero puede depender y confiar en otros participantes para administrar la red y respaldar transacciones. Luego están los usuarios finales que interactúan con la red blockchain a través de una interfaz de usuario. Es posible que el usuario final ni siquiera sea consciente de que una cadena de bloques sustenta el sistema.

Actas

Las transacciones están codificadas dentro de los contratos inteligentes junto con los activos a los que pertenecen las transacciones. Piense en las transacciones como los puntos de interacción entre

los activos y los participantes; un participante puede crear, eliminar y actualizar un activo determinado, asumiendo que están autorizados para ello. Son estas transacciones las que se almacenan inmutablemente en la cadena de bloques, que también proporciona la procedencia de cualquier cambio en el activo a lo largo del tiempo.

El ajuste de blockchain

En una sección anterior, analizamos los problemas en IBM Global Ejemplo de finanzas que llevó a la implementación de una solución blockchain junto con los beneficios que un sistema basado en blockchain puede proporcionar. Ahora consideraremos por qué la tecnología blockchain fue la elección sensata.

Lo primero y más importante es comprobar que existe una red empresarial. El sistema IBM Global Finance cuenta con unos 4.000 proveedores y socios, así como IBM dentro de la red. Así que tenemos una buena red empresarial en la que considerar características del resto de la cadena de bloques.

Como algunas de las disputas están relacionadas con diferencias entre lo que se ordenado y posteriormente recibido, esto a menudo puede ser el resultado de diferentes participantes en una red empresarial (socios, proveedores y empresas de entrega) que rastrean mercancías en sistemas aislados separados.

Por lo tanto, un libro mayor compartido con consenso y finalidad proporcionado por blockchain en toda la red empresarial ayudará a reducir el riesgo general de número de disputas, ya que dará a todos los participantes la misma información sobre los activos que se están rastreando. Además, si los cambios en los datos que se rastrean ya sean intencionalmente o involuntariamente son parte de la causa fundamental de estas disputas, entonces las características de procedencia e inmutabilidad de blockchain podrían también ayudar.

Por último, consideramos la cantidad de tiempo necesario para resolver estos problemas. Como había múltiples sistemas (incluidos sistemas de terceros) que alguien necesitaba verificar para resolver cualquier transacción en disputa, tener un único libro de contabilidad compartido que se mantiene mediante consenso ayudará a reducir el tiempo necesario para resolverlos.

Algunas observaciones adicionales sobre cómo una solución basada en blockchain pueden beneficiar esta red empresarial:

• Cada participante de la red empresarial tiene una identidad y está autorizado en la red. Esto podría ayudar con sus procesos relacionado con Conozca a su Cliente (KYC) y Anti-Dinero, Lavado de Dinero (AML).

• Se podrían diseñar contratos inteligentes para resolver algunas de las disputas automáticamente manteniendo la coherencia en toda la empresa red y, por tanto, reduciendo aún más el número de disputas.

Elegir un primer escenario

Es posible que esté considerando múltiples escenarios en los que blockchain proporciona una buena solución. En este caso necesitarás comparar cada uno para determinar cuál es el mejor escenario para trabajar primero.

Recomendamos un enfoque simple para comparar cada escenario utilizando un gráfico de cuadrantes, donde cada uno se coloca en el gráfico según su relativo beneficio y simplicidad.

En la Figura 2-1, el eje x es la simplicidad del escenario (más simple de la derecha) y el eje y representa el beneficio (más beneficioso para la parte superior). Coloque cada escenario en el cuadro de cuadrantes, considerando su beneficio esperado y simplicidad como solución blockchain, esto es mejor realizarse como un ejercicio de grupo con las partes interesadas adecuadas que puedan proporcionar la información necesaria sobre dónde cae cada escenario en el gráfico basado en el nivel de simplicidad y los beneficios potenciales.

Una vez que se han trazado todos los escenarios en el gráfico, resulta obvio cuáles son los primeros escenarios en los que concentrarse: aquellos que proporcionan el mayor beneficio y son los más simples.

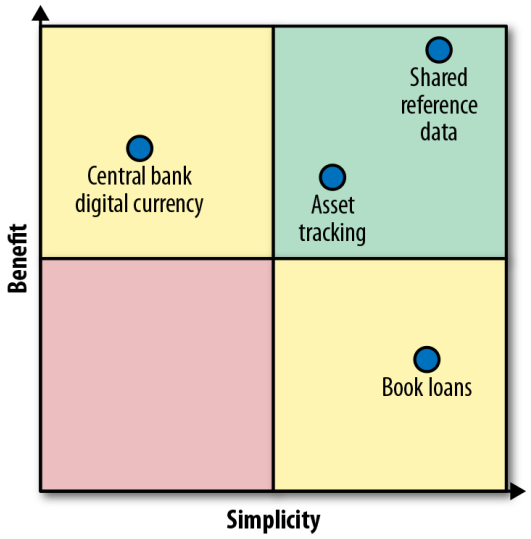

Figura 2-1. Comparación de escenarios en función de su beneficio y simplicidad.

Transformando la red empresarial

Una vez que se haya identificado su primer escenario blockchain, podrá querer pasar a la siguiente fase: construir el producto mínimo viable (MVP). Un MVP representa el producto mínimo que se puede ser construido para lograr un objetivo del escenario blockchain.

Iniciar un MVP con blockchain no debería ser diferente a cualquier otro tecnología y buenas prácticas de ingeniería de software, como el uso de los principios **ágiles** siempre serán aplicables. A continuación, se presentan algunas observaciones que le ayudarán a empezar a transformar su negocio con una nueva solución basada en blockchain:

Blockchain es un deporte de equipo. Habrá múltiples partes interesadas de diferentes organizaciones del tejido empresarial. Algunos de estas organizaciones es posible que no hayan trabajado tradicionalmente directamente una con la otra. Por lo tanto, una comprensión clara de los requisitos y problemas entre todos los participantes, y líneas claras de comunicación y acuerdo, son fundamentales para el éxito del proyecto.

• Utilizar técnicas design thinking que se centren en los objetivos del usuario, para acordar el alcance del MVP.

• Utilice las mejores prácticas ágiles de ingeniería de software, como la integración y retroalimentación de las partes interesadas, para iterar a lo largo del desarrollo del MVP. Mantener a las partes interesadas informadas y actuar según la retroalimentación.

• Comience con una red pequeña y crezca. Habrá algunos desafíos adelante, ya que esto puede ser un cambio de paradigma para el negocio red.

• Si reemplaza un sistema existente, considere ejecutar la solución basada en blockchain como cadena en la sombra para mitigar el riesgo. Es decir, durante la fase piloto, ejecutar la nueva plataforma junto con el sistema heredado. Lo ideal sería pasar la producción de datos real al nuevo sistema basado en blockchain para probar y validarlo, mientras continúa confiando en el sistema heredado para esta fase del proyecto. Sólo después de que se hayan completado pruebas exhaustivas y el nuevo sistema ha sido probado en caso de que cambie del sistema heredado al nuevo.

• Aunque es probable que blockchain sea una parte fundamental de la solución, probablemente no será su mayoría. La red de blockchain seguirá integrándose con otros sistemas externos, proporcionando funciones adicionales como almacenamiento de datos fuera de la cadena, identidad gestión de acceso, interfaz de programación de aplicaciones (API) capas de gestión y presentación, etc.

Hacer crecer la red empresarial

Con una solución basada en blockchain es recomendable comenzar con una pequeña red y luego crecer. ¿Qué significa hacer crecer la red? Eso puede significar agregar cualquiera de los siguientes:

• Participantes de la red, es decir, aquellos participantes en la red que son pares.

• Aplicaciones que interactúan con la red.

• Usuarios de la solución basada en blockchain

También puede significar aumentar lo siguiente:

• Contratos inteligentes

• Canales o libros auxiliares para la privacidad entre los participantes de la red.

• Rendimiento de transacciones

• Número de activos

Es necesario un modelo de gobernanza democrática fuerte para gestionar este tipo de cambios a medida que se realizan en la red blockchain. Recuerde, ninguna organización tiene el control por sí sola.

Esta es una de las áreas que distingue a una solución basada en blockchain de otras tecnologías. Por ejemplo, hay cambios dentro de la red que requiere múltiples participantes (organizaciones) dentro de la red que esté de acuerdo antes de que el cambio entre en vigor. A continuación, se presentan dos ejemplos de cambios que requieren este tipo de acuerdo.

1. Una red existente consta de tres participantes: Dave, Matt, y Luc. A John le gustaría unirse a la red. Para que John se una a la red autorizada, Dave, Matt y Luc deben cada uno criptográficamente firmar el cambio de configuración antes de que John sea permitido conectarse a la red. Por supuesto, esta es una opción de gestionar este escenario; alternativamente, si solo hay una red se necesita un miembro para aprobar dicho cambio, entonces la red se puede configurar en consecuencia.

2. Se instalará un nuevo contrato inteligente en la red y ambos las organizaciones de Dave y Matt deberán respaldar las transacciones para el nuevo contrato inteligente. En este escenario, tanto Dave y Matt deben instalar el contrato inteligente a sus pares y garantizar que se cree una instancia del contrato inteligente en un canal (o libro mayor auxiliar) antes de una aplicación al cliente.

Diez preguntas para explorar el escenario con más detalle

Hasta ahora, hemos analizado a un nivel bastante alto si blockchain hace una elección sensata para el escenario. Por supuesto que podemos explorar el escenario con mucho más detalle para ayudar a identificar la idoneidad de blockchain, y comenzar a mapear el tipo de red que podría estar involucrado.

Las siguientes preguntas ayudarán a comprender el escenario desde una perspectiva de blockchain:

1. ¿Cuál es el problema o desafío empresarial específico que plantea el escenario abordar?

2. ¿Cuál es la forma actual de solucionar este problema empresarial?

3. Suponiendo que el problema empresarial es grande, ¿qué aspectos específicos se abordarán en este problema empresarial?

4. ¿Quiénes son los participantes de la red empresarial (organizaciones) involucrados? y ¿cuáles son sus roles?

5. ¿Quiénes son las personas específicas dentro de la organización? y ¿cuáles son sus funciones laborales?

6. ¿Qué activos están involucrados? y ¿cuál es la información clave asociada con los activos?

7. ¿Cuáles son las transacciones involucradas, entre quién y qué? ¿Los activos están asociados con las transacciones?

8. ¿Cuáles son los pasos principales del flujo de trabajo actual? y ¿cómo estos son ejecutados por los participantes de la red empresarial?

9. ¿Cuál es el beneficio esperado de aplicar la tecnología blockchain? ¿Cuál es el problema empresarial de cada uno de los participantes de la red?

10. ¿Qué sistemas heredados están involucrados? ¿Qué grado de integración con los sistemas heredados es necesario?

Nuevamente, trabajar en estas preguntas con las partes interesadas apropiadas (negocios, técnicos y usuarios) y capturar los resultados ayudará enormemente antes de pasar el proyecto a la siguiente fase, como un MVP.

Papel comercial: un escenario de ejemplo

La comunidad Hyperledger Fabric de la Fundación Linux ha producido un excelente conjunto de materiales en torno al escenario del Pagarés de empresa. Para obtener más información sobre el escenario, puede ir aquí. Volveremos al escenario del Pagarés de empresa en capítulos posteriores pero introducimos los conceptos de un negocio de Pagarés de empresa conéctese aquí y vea por qué blockchain es una buena tecnología. El Pagaré de empresa es un instrumento de deuda emitido por una empresa que necesita superar sus necesidades de financiación a corto plazo. El Pagarés de empresa se vende a otra empresa que puede canjearlo a un precio fecha posterior por un valor superior al que pagaron por él. Esto proporciona y proporciona un retorno de la inversión para la empresa que compra el Pagarés de empresa. Pagarés de empresa puede revenderse a otras empresas durante su ciclo de vida.

Anteriormente en este capítulo, introdujimos los conceptos de activos, participantes y transacciones. Miremos el Pagarés de empresa a través de esta lente.

Activos de pagare de empresa

El principal activo del tejido empresarial es el pagera de empresa.

Este activo tendrá varios atributos, tales como:

• La empresa emisora

• ¿Qué empresa es la propietaria actual?

• La fecha de emisión

• La fecha de vencimiento

• El valor nominal

• El estado actual

Participantes de pagare de empresa o papel comercial

El principal participante del tejido empresarial es una empresa. Allá Por supuesto, habrá varias empresas en la red, y estas empresas desempeñarán diferentes papeles en relación con un pagare de empresa activo, como emisores y compradores.

Está claro que dentro de esta red empresarial hay múltiples participantes. Recuerde, esto es fundamental para que un escenario sea una buena cadena de bloques.

Transacciones de pagare de empresa

Principales transacciones asociadas al activo de pagarés son:

Asunto

Una empresa emite pagare de empresa.

Comprar

Una empresa compra pagare empresarial y, por tanto, es el actual dueño

Canjear

Una empresa (el propietario actual) rescata el pagare comercial contra el emisor original

Por último, veamos los cuatro beneficios de una solución blockchain y cómo podrían beneficiar al tejido empresarial del pagare comercial.

Consenso

Se negociarán múltiples activos de papel comercial a través de la red. Un único activo de papel comercial puede moverse entre varias empresas, y cada empresa negociará con muchas otras compañías. Por lo tanto, es fácil ver cómo el consenso sobre el estado del activo y cualquier transacción almacenada en el libro mayor compartido hace sentido.

Se podrían obtener más beneficios utilizando una solución basada en blockchain en esta red empresarial, como la visibilidad en toda la red.

Por ejemplo, si una empresa emite papel comercial por USD $100,000, se considera bien, pero ¿y si emiten 20 de estos? ¿Papeles a diferentes empresas al mismo tiempo? Un basado en blockchain La solución puede proporcionar información adicional, como cuántas se han emitido efectos comerciales en toda la red empresarial, y su valor total. Esta información confiable se puede utilizar para evaluar el riesgo de comprar papel comercial.

Procedencia

Una empresa que compre papel comercial existente querrá estar segura qué empresa lo emitió. También querrán estar seguros que están comprando el papel comercial al propietario actual. Por razones de privacidad y confidencialidad, la identidad de otros anteriores los propietarios de papel comercial bien puede quedar ocultos a los nuevos compradores. Sin embargo, un número total de propietarios anteriores del papel podría proporcionarse fácilmente.

Inmutabilidad

Es fácil ver la importancia de esta característica de blockchain. Una compañía que está comprando papel comercial existente de otra empresa quiere asegurarse de que no haya sido modificado de ninguna manera desde que fue emitido. Una empresa que canjea efectos comerciales quiere estar segura no hay duda sobre la validez del artículo.

Finalidad

Por último, la finalidad en toda la red de papel comercial es importante. Imagine que hay un mercado o intercambio dentro de la red empresarial. Una empresa ofrece papel comercial al mercado. Otra empresa ofrece comprar el papel comercial emitido. Todas las empresas involucradas querrán estar seguras de que el nuevo sistema de papel comercial se emite una sola vez en toda la red empresarial. no seria bueno si fuera posible que dos empresas compraran el mismo papel comercial al mismo tiempo.

Resumen

En este capítulo hemos visto la importancia de identificar los requisitos de un escenario de blockchain y cualquier problema relacionado con el escenario que se está considerando. siendo considerado. Luego aprendimos cómo los cuatro beneficios clave de blockchain (consenso, procedencia, inmutabilidad y finalidad) ayudan a determinar si blockchain es una buena tecnología, al tiempo que garantiza que siempre haya una red comercial de múltiples participantes. El uso de los conceptos de blockchain (activos, participantes y transacciones) ayudará a guiar la decisión y ayudará a los usuarios a comprender cómo se podría aplicar blockchain a la red empresarial.

CAPÍTULO 3

Diseñando una red Blockchain

En el Capítulo 2, se identificó que blockchain es una buena tecnología adecuada para su escenario. En este capítulo exploraremos algunos de los aspectos del diseño de una solución basada en blockchain.

Modelo de gobernanza

En términos generales, existen dos modelos utilizados para iniciar una nueva red Blockchain:

Dirigida por el fundador

Una sola organización inicia la red. No lo harán de forma aislada. Se espera que tengan profundas conocimiento de la industria y trabajará con las partes interesadas dentro de la industria respectiva. El fundador definirá el modelo de gobernanza y políticas de la red, e invitará a otras organizaciones a unirse.

Dirigida por un consorcio

Un grupo de empresas pone en marcha la red. Por ejemplo, un grupo de bancos trabajan juntos para crear una nueva plataforma basada en blockchain que cada uno de ellos se beneficia de utilizar. Es posible que esta red permanezca privada para los miembros del consorcio inicial, pero es mucho más probable que, una vez construida, permitan a otras organizaciones unirse a la red. También es posible que la propiedad y la gobernanza se trasladen más tarde a una nueva empresa. Por ejemplo, la plataforma de financiación del comercio we.trade fue creada por un consorcio de bancos y más tarde pasó a ser propiedad de una empresa conjunta. Independientemente de cómo se cree la red, requerirá políticas de gobernanza flexibles. La blockchain debe poder adaptarse con el tiempo, permitir la introducción de nuevos tipos de modelos de gobernanza a medida que crezca la red. A medida que nuevas organizaciones se unan a las redes deberán aceptar los modelos de gobernanza ya existentes.

Miembros y consumidores de la red

Hasta ahora nos hemos referido a participantes o miembros de la red en un sentido muy amplio. Sin embargo, existen diferentes roles y responsabilidades para los participantes en una solución basada en blockchain. Cuando al diseñar la red, es importante identificar el papel de un participante. Para comprender los diferentes tipos de roles, debemos observar dos conceptos de una red blockchain:

Servicios de red

Estos son los servicios fundamentales de la red blockchain: la red blockchain peer-to-peer, contenedores de ejecución de contratos inteligentes, y servicios de seguridad.

Servicios de negocios

Esta es la aplicación blockchain construida en la red subyacente. Incluyen la lógica del contrato inteligente, el lado del cliente, lógica de aplicación que se conecta a la cadena de bloques, y cualquier lógica de integración con sistemas externos.

Con estos conceptos en mente, ahora podemos ver los diferentes roles en la red:

Proveedor de servicios de red

Gobierna la red y define las políticas de red.

Consumidor de servicios de red

Un participante en la red ejecutando sus pares y certificado autoridades.

Proveedor de servicios empresariales

El participante que escribe la lógica empresarial de la plataforma, incluidos contratos inteligentes, aplicaciones de cliente e integración lógica.

Consumidor de servicios empresariales

El participante que aloja las aplicaciones del lado cliente que se conectan a la red blockchain y la lógica de integración.

Usuario final

Se conecta a la plataforma a través de la interfaz de usuario. Lo hacen a través del móvil, la tableta o el navegador web, y puede que desconozca la red blockchain que la sustenta.

Es importante tener en cuenta que un participante individual puede tener varios roles. Por ejemplo, una organización puede ser a la vez un servicio de proveedor de red y consumidor, ya que ambos definen la gobernanza y las políticas de la red y también usarla activamente ejecutando su propio par. Otro ejemplo es el de un único socio tecnológico que puede escribir el contrato inteligente y la lógica de la aplicación del cliente, así como proporcionar la infraestructura de TI en la que se ejecutan las aplicaciones del cliente.

Una característica importante de una buena tecnología blockchain es que es flexible en su instalación y configuración de red, y que puede configurarse de tal manera que coincida con los requisitos de los fundadores de la red.

Consideraciones de arquitectura y diseño

Este es un tema muy amplio y demasiado para cubrirlo en detalle en este capítulo. Sin embargo, introduciremos una serie de aspectos arquitectónicos clave y consideraciones de diseño al analizar una red blockchain.

Tipos de participantes

Estos identifican los tipos de participantes en la red. Por ejemplo, en el escenario del pagares comerciales, identificamos organizaciones como tanto emisores como compradores.

Roles de red

Estos se asignan a los participantes dentro de la red como se discutió en el apartado anterior. Usando este conocimiento, puedes comenzar a mapear una topología de red blockchain.

Activos
Estos se registran en la cadena de bloques. Por ejemplo, en el escenario del pagare comercial identificamos el pagare comercial como el principal activo. Esto ayudará a identificar los contratos inteligentes que se necesitarán. Los activos tienen tres atributos importantes relacionados con los participantes en una red blockchain: quién emite o crea el activo, quién es el propietario del activo y quién lo destruye. Con esta información puede agregar los activos conocidos a la topología de la red, mostrando los participantes que los emiten, poseen y destruyen.

Actas
Se refieren a los activos registrados en el libro mayor que envían los participantes de la red. Puede agregar transacciones a la topología de la red, aumentando los activos agregados en el paso anterior.

Avales
Estos son realizados por una o más organizaciones en la red por cada transacción enviada. Siempre recomendamos una póliza de al menos dos patrocinadores para mantener la confianza y evitar cualquier actividad maliciosa. Las políticas de respaldo se pueden definir tanto a nivel en el contrato inteligente y para estados individuales escritos en el libro mayor de blockchain. Por ejemplo, en el escenario del pagaré comercial, los pagarés comerciales individuales los activos en papel pueden definir su propia política de respaldo (basada en el estado de respaldo), o todas las transacciones y actualizaciones de estado pueden definir una política de respaldo que se aplica a todos los efectos comerciales (endoso del smart contrato). Revisar los activos y transacciones agregadas a la topología de la red y considerar para cada qué organización debería respaldarlo. Te sorprenderá lo que esto revela sobre las interacciones y supuestos de confianza en la red.

Implementación
Hay muchas maneras en que se puede implementar una red blockchain en un ambiente heterogéneo. Por ejemplo, se podría aprovisionar una red dentro de un único entorno de nube, local o en un híbrido de los dos. En particular, estamos viendo más redes unidas en múltiples entornos de nube. Al revisar el despliegue, la ubicación geográfica y cualquier requisito de jurisdicción de datos debe también ser considerado.

Acceso a la red
¿Los entornos para cada uno de los componentes de la red permitirán acceso a la URL y a los puertos de los demás componentes de la red dentro de la red para que puedan comunicarse?

Reglamentos
Normativas como la General de Protección de Datos de la Unión Europea, el reglamento (GDPR) puede influir en su diseño y arquitectura. Por ejemplo, el “derecho al olvido” significa que es necesario evitar almacenar cualquier dato personal en una cadena de bloques si más adelante va a ser capaz de cumplir con una solicitud para eliminarlo. Existen buenos patrones de diseño para manejar datos personales en una cadena de bloques; estos incluyen, por ejemplo, el uso de hashes para datos almacenados fuera de la cadena de bloques.

Requerimientos no funcionales
Aspectos como latencia de transacciones, transacciones por segundo y el volumen de datos debe confirmarse lo antes posible. Estos requisitos deben revisarse de manera realista para garantizar que blockchain es la solución tecnológica correcta.

Consideraciones de Seguridad
Aunque una red blockchain autorizada como Hyperledger, la red está construida con seguridad desde cero, te recomendamos comenzar su planificación de seguridad con anticipación. Esto puede convertirse fácilmente en el mayor tema en esta lista.
Al revisar la seguridad, estas son algunas de las cosas que deberá tener en cuenta a considerar:
Claves privadas
Dónde y cómo se almacenarán las claves privadas de cada uno de los componentes en la red. ¿Son los módulos de seguridad de hardware un ¿requisito?

Autoridades de certificación
¿Existen autoridades de certificación específicas que deban emitir certificados para organizaciones de la red?

Cifrado
¿Qué nivel de seguridad de la capa de transporte requieren los participantes al interactuar con la red blockchain?

Privacidad y confidencialidad
¿Existe algún requisito de privacidad y confidencialidad de los datos de identidad y transacciones almacenadas en la cadena de bloques?

Gobernanza, administración y operación
Consideraciones
Anteriormente en este capítulo, presentamos los diferentes roles que desempeñan los participantes dentro de una red blockchain. Cada rol define qué puede hacer el participante con respecto a las actividades de administración y operación. Por ejemplo, un consumidor de servicios de red que está ejecutando sus propios pares y autoridades de certificación dentro de un Hyperledger.

La red Fabric blockchain instalará nuevos contratos inteligentes en sus pares. Un consumidor de servicios empresariales que gestiona un cliente. La aplicación necesitará gestionar sus identidades blockchain y la aplicación que se está conectando a la red. También hay tareas administrativas y operativas que deben realizarse coordinadas. Por ejemplo, un contrato inteligente implementado por dos participantes a sus pares debe ser diseñado, codificado y revisado. Una vez completadas las revisiones, cada participante instala el contrato inteligente. El diseño y el código los realiza la empresa proveedor de servicios, y la revisión y el acuerdo son manejados por cada de los consumidores de servicios de red.

Para gestionar este tipo de cambios en la red por diferentes participantes, es necesario definir un conjunto de políticas de gobernanza. Esas políticas podrían exigir, por ejemplo, que todos los participantes digitalmente firmen el contrato inteligente antes de que pueda instalarse. Afortunadamente, en blockchain Redes como Hyperledger Fabric han sido diseñadas para permitir esto. Plataformas construidas sobre Hyperledger Fabric, como la plataforma IBM Blockchain, puede entonces proporcionar interfaces de usuario para hacer la gestión simplificada de estas políticas de gobernanza.
El consejo aquí es planificar esto con anticipación. Las políticas de gobernanza se deciden en función de los requisitos del negocio y posiblemente de las regulaciones. Comprender estos requisitos desde el principio ayuda a la hora de diseñar el tipo de red blockchain que sustentará el nuevo sistema.

Consideraciones de datos
En esta sección, analizamos cómo se procesan los datos en una red blockchain, la ubicación de donde es almacenada y cómo esta puede ser hecha privada.

Jurisdicción
Una blockchain es una red peer-to-peer. Datos en forma de transacciones y la estructura real de la cadena de bloques se comparte y replica a través de la red a diferentes pares. Porque la red puede abarcar múltiples jurisdicciones, es importante considerar qué datos se almacenan y donde.

Las diferentes tecnologías blockchain le permiten diseñar diferentes topologias de red. Por ejemplo, la red bitcoin tiene grandes números de pares que, en última instancia, almacenan cada uno la misma estructura cadena de bloques (hay bifurcaciones en la red que significan que a veces podrían ser versiones alternativas; el algoritmo de consenso finalmente resuelve esto). Otras tecnologías blockchain como Hyperledger Fabric le permite diseñar redes que puedan administrar múltiples estructuras blockchain (conocidas como canales) y también especifican pares que pueden almacenar qué canal (lo que significa que no todos los pares tienen que guardar todo).
Usando Hyperledger Fabric como ejemplo de tecnología blockchain, veamos ahora la importancia de la jurisdicción de datos y los tipos de opciones que podrían estar disponibles.
Hyperledger Fabric tiene dos tipos de pares según su función dentro la red:

Nodos ordenados
Estos reciben propuestas de transacciones, empaquetan estas transacciones en bloques y entregárselos a sus compañeros. Un grupo de nodos ordenados dentro de la red se denomina servicio de pedidos. Hay un único servicio de pedidos por red que ordena transacciones para todos los canales de la red.

Colegas
Estos mantienen una copia local de un libro mayor por canal. En hiperledger Fabric, el libro mayor comprende tanto la estructura blockchain, que es una lista de bloques que contienen transacciones, y también una Base de datos del estado mundial, que se escribe y se lee en el contrato inteligente. Un par puede unirse (si tiene permiso) a muchos canales y por lo tanto podría estar administrando múltiples libros de contabilidad. Recordar que no todos los pares necesitan unirse a todos los canales. Una opción avanzada es que un par se una a canales en diferentes servicios de pedidos, creando una red de redes.

No debemos olvidar la aplicación del cliente que envía transacciones a la red blockchain, ya que claramente tendrá acceso a los datos como bueno, ya sea como entrada a una transacción o consultando el contenido almacenado en la cadena de bloques.
La infraestructura física que sustenta la recolección de pedidos, los nodos y pares pueden ser multisitio y abarcar diferentes áreas geográficas. Las organizaciones que ejecutan nodos de orden y pares pueden elegir proveedores de nube, cada uno de los cuales ofrecerá una variedad de ubicaciones para el despliegue. Las organizaciones también pueden optar por implementar en sus instalaciones dentro de su propio centro de datos. A medida que se crean las redes blockchain formado por varias organizaciones, cada organización puede elegir la infraestructura sobre la que ejecutar los servidores de los que son responsables. A estas las llamamos redes blockchain híbridas multinube.

Por lo tanto, al considerar la ubicación jurisdiccional de los datos, debemos entender:

• Los requisitos comerciales de qué datos se deben enviar y ser almacenados por la red.
• La topología de la red, que consta de nodos ordenados, pares y canales.
• La ubicación física del orden de los nodos y de los pares que están accediendo los datos

Privacidad de datos
Veamos ahora cómo hacer que los datos sean privados y confidenciales en una red blockchain. Recuerde que todos los participantes en un grupo autorizado en la red blockchain como Hyperledger Fabric tiene una identidad criptográfica en forma de certificado digital. Esto incluye cualquier nodo ordenado y pares. Recuerde también que las transacciones son enviadas a la red y los datos finalmente se almacenan en los canales que contiene tanto la estructura blockchain como el estado mundial de la base de datos.

Al considerar la privacidad de los datos, primero debemos entender qué datos se hacen privados y para qué organizaciones y participantes debería ser privado.
Los tipos de datos que se pueden compartir a través de la red y, por lo tanto, los aspectos que se deben considerar al analizar la privacidad son:
• El certificado digital (identidad) del remitente de la transacción.
• El certificado digital (identidad) de los pares que avalan las transacciones
• La transacción llamada por la aplicación remitente y cualquier parámetro pasado a la transacción
• Cualquier dato leído y escrito por el contrato inteligente en el mundo estado.
• La respuesta a la aplicación del cliente a la llamada del sistema al contrato inteligente.

Además de lo anterior, hay un par de otras piezas pequeñas de metadatos asociados con una invocación de transacción: por ejemplo, los nombres clave de los datos almacenados en el estado mundial, y los nombres de cualquier recopilación de datos privados de los que haya leído el contrato inteligente o al que ha escrito.
Hyperledger Fabric proporciona varias funciones para administrar datos y hacerlo privado para ciertos participantes en la red. Resumiremos cada uno de estos a continuación:

Canales
Los canales son una forma de hacer un libro de contabilidad (blockchain y estado mundial) privado solo para aquellas organizaciones a las que se les permite unirse al canal. Además del servicio de pedidos, solo pares y aplicaciones cliente dentro de las organizaciones autorizadas pueden unirse y tener acceso a el canal. Cualquier persona que no tenga permiso para unirse a un canal nunca recibirá bloques del servicio de pedidos y por lo tanto nunca tendrá una copia del libro mayor del canal. Los canales proporcionan una experiencia realmente buena forma de crear subredes en la red blockchain.
Una cosa a tener en cuenta es que el servicio de pedidos seguirá viendo transacciones para todos los canales y cualquier organización autorizada para unirse al canal tendrá acceso a todos los datos contenidos en el canal. Este puede ser ideal para algunos escenarios, pero no tanto para otros.

Colecciones de datos privados
Las colecciones de datos privados aparecieron por primera vez en la versión Hyperledger Fabric 1.2. Estos funcionan dentro de un canal y permiten que las políticas definan que solo un subgrupo de organizaciones dentro del canal puede acceder a ciertos datos. A diferencia de las transacciones normales, donde toda la información se envía al servicio de pedidos, para Recopilaciones de Datos

Privados los datos son almacenados solo por los pares especificados en la política (y compartido a través de protocolo de chismes), y se envían hashes en lugar de datos reales en la transacción al servicio de pedidos. Esto significa que los datos pueden conservarse privado para un subconjunto de organizaciones dentro del canal y nunca compartido con el servicio de pedidos.

Cifrado

El cifrado es el proceso de convertir texto fuente legible en texto cifrado ilegible. Comúnmente esto se hace con un par de claves asimétricas, donde un poseedor de una clave pública puede cifrar una parte de datos sabiendo que sólo el poseedor de la clave privada puede descifrarlos. Es un error común pensar que los datos se cifran automáticamente en Hyperledger Fabric y algunas otras tecnologías blockchain. Sin embargo, Hyperledger Fabric proporciona un conjunto de cifrado y servicios de descifrado al contrato inteligente, lo que le permite descifrar datos recibidos de la aplicación cliente que llama o consulta el estado mundial, y también para cifrar cualquier dato que escriba en el mundo estado o vuelve a la aplicación cliente que llama. El cifrado puede usarse junto con canales y colecciones de datos privados como solo descrito. Por supuesto, es posible que el cliente que envía la solicitud para cifrar los datos antes de enviarlos al contrato inteligente. Uno lo que debes tener en cuenta es que necesitarás administrar las claves (ambas públicos y privados) al utilizar esta función.

Identidad

Si bien es imperativo que todos en una red autorizada tengan una identidad (a efectos de autenticación, integridad y no repudio), no significa que haya ocasiones en las que la participación de un participante no debe ocultarse a un público más amplio. Por ejemplo, digamos que hay un canal de 10 organizaciones que son competidoras el uno al otro. Cada organización envía transacciones a la red blockchain para este canal, pero no quiere revelar su identidad en la transacción almacenada en la cadena de bloques. Usando la función Identity Mixer agregada en Hyperledger Fabric versión 1.3, es posible para mantener la identidad del cliente que envía la solicitud anónima, pero sin perder la capacidad de autentificarlos. En el futuro se agregarán roles adicionales cuya identidad también puede hacerse anónimo.

Inducción

Cuando se trata de incorporar nuevas organizaciones en una cadena red de bloques como Hyperledger Fabric, deberá considerar mucho de lo que se ha discutido en este capítulo:

• Conocer y comprender el modelo de gobernanza de la red.
¿Son las políticas definidas por el fundador o el consorcio existente?
• Comprender el tipo de rol que tendrá la nueva organización en la red. ¿El puesto cumple con sus requisitos y existen supuestos de confianza que deben ser revisados y aprobados?
• Saber si la nueva organización gestionará sus propios pares, y si respaldarán las transacciones enviadas a la red. ¿Existe la opción de ejecutar en la nube o en las instalaciones?
• ¿Qué políticas existen con respecto a los cambios en la red? ¿Y nuevos contratos inteligentes?
• ¿Qué dicen las políticas para las organizaciones adicionales que se están incorporados, y las organizaciones recién incorporadas tendrán voz y voto? ¿En alguna organización futura que se incorpore?
• ¿Existe algún requisito de seguridad que deba cumplirse, como almacenar claves privadas en módulos de seguridad de hardware?
• ¿Existe algún requisito regulatorio como GDPR o protección de datos y requisitos de privacidad?

Resumen

En este capítulo hemos revisado muchas de las consideraciones de diseño al construir una nueva red blockchain. Observamos los tipos de roles que las organizaciones pueden asumir en una red y la necesidad de gobernanza. Analizamos áreas como la seguridad y la regulación, así como revisamos los requisitos de privacidad y jurisdicción de datos.

CAPÍTULO 4
Desarrollando una red Blockchain

Los capítulos anteriores introdujeron conceptos de blockchain y ayudaron para identificar cuándo un escenario sería idealmente resuelto por una solución blockchain. También revisamos aspectos del diseño de una red blockchain.
En este capítulo, analizamos los diferentes aspectos del desarrollo de la Aplicación blockchain que utiliza Hyperledger Fabric.

Contratos inteligentes
Lo primero que veremos son los contratos inteligentes, que son la parte nuclear del desarrollo de una aplicación blockchain.
Hyperledger Fabric ha adoptado un enfoque genérico para los lenguajes. Se utiliza para escribir contratos inteligentes. El primer idioma admitido fue Go, que también es el lenguaje en el que está escrito Fabric. Node.js y Java se ha agregado en versiones posteriores. Hyperledger Burrow™ también agregó a Hyperledger Fabric, que agrega lenguajes como como la solidity de Ethereum.
Aunque la industria utiliza y entiende el término genérico contrato inteligente, Hyperledger Fabric en realidad se refiere a la unidad instalable como código de cadena. Podemos pensar en los contratos inteligentes como equivalentes a código de cadena.

En Hyperledger Fabric v1.4 se realizan una serie de cambios significativos en la API. Estas mejoras simplifican la escritura de contratos inteligente, permitiendo que múltiples contratos asociados se escriban en un código de cadena único. Esto proporciona una relación de uno a muchos entre un código de cadena y los contratos inteligentes que contiene, y le da al desarrollador más flexibilidad para colocar contratos inteligentes que estén relacionados. Se realizaron otros cambios de API en Fabric Software Development Kit (SDK), lo que simplifica la escritura de la aplicación cliente que se conecta a la red blockchain. Para el resto de este capítulo Solo usaremos el término contrato inteligente y no nos referiremos al código de cadena.
Cada contrato inteligente escrito en Hyperledger Fabric define qué el estado se escribe en la base de datos del estado mundial (veremos más sobre esto en “Estado Mundial” en la página 46), las transacciones asociadas con el contrato inteligente y la lógica de negocios definida dentro de cada transacción.

En la parte superior de cada contrato inteligente, una interfaz importante llamada fabric-contrat-api se debe incluir, que define el conjunto de estructuras que debe cumplir un contrato inteligente. Una vez que se ha escrito, revisado y probado un contrato inteligente, es luego empaquetado en un archivo de especificaciones de implementación de código de cadena que incluye:

• El contrato inteligente (que podría constar de varios archivos)
• Una política de instanciación que describe qué organización administra la instanciación del contrato inteligente.
• Un conjunto de firmas digitales de las organizaciones propietarias del contrato inteligente.

Cada organización que necesita ejecutar el contrato inteligente para respaldar las transacciones luego lo instalará en cada uno de sus pares. Después de esto, el contrato inteligente es instanciado en un canal específico por una de las organizaciones identificadas en la política de creación de instancias. Una vez que el contrato inteligente ha sido instanciado en el canal, cada par que se unió

al canal y previamente instaló el contrato inteligente podrá respaldar transacciones para el contrato inteligente.
En la siguiente sección, después de presentar el libro mayor de canales, veremos exactamente cómo se ve el código de contrato inteligente.

Libro mayor de canales
Como mencionamos en capítulos anteriores, cada canal en Hyperledger Fabric tiene un libro mayor. El libro mayor consta de una estructura blockchain y el estado mundial.

Repasemos lo que está registrado en ambas estructuras y cómo esto podría afectar lo que escribe un desarrollador.

Estructura de la cadena de bloques
La estructura de blockchain son los bloques vinculados criptográficamente, con cada bloque que contiene una o más transacciones. Los hashes se utilizan para unir los bloques. Una vez que se ha agregado un bloque al blockchain, no se puede modificar ni eliminar.
Cada vez que se envía una transacción a un pedido de servicio Hyperledger Fabric, se escribirá en la estructura blockchain para el canal en el que fue enviado. Como vimos en el capítulo anterior cuando se analiza la privacidad de los datos, la transacción incluye varios datos, que volvemos a incluir aquí a título informativo:

• El certificado digital (identidad) del remitente de la transacción.
• El certificado digital (identidad) de los pares que avalan las transacciones
• La transacción llamada por la aplicación remitente y cualesquiera parámetros pasados a la transacción
• Cualquier dato leído y escrito por el contrato inteligente en el mundo estado
• La respuesta a la aplicación cliente al llamar al contrato inteligente

La validación de la transacción en realidad ocurre en la última fase del consenso dentro de Hyperledger Fabric. Se agregan todas las transacciones enviadas a la cadena de bloques, pero solo aquellas transacciones que se consideran válidas también modificarán el estado mundial. Si se considera una transacción para ser inválida (por ejemplo, no tiene respaldos suficientes, o hay un desajuste del estado mundial entre el respaldo y validación (también conocido como conflicto MVCC), todavía está escrito a la blockchain pero está marcado como no válido. Esto es muy importante, porque significa que Hyperledger Fabric no solo está grabando transacciones que afectan el estado mundial y los activos allí registrados, pero también registra transacciones no válidas para su auditoría.

Estado mundial
El estado mundial es una base de datos en la que los pares mantienen el estado escrito por los contratos inteligentes instanciados. Actualmente, el estado mundial puede ser cualquiera de los siguientes:

NivelDB
La opción por defecto, en la que una instancia de LevelDB se incrusta dentro del proceso peer. Esta base de datos permite al contrato inteligente escribir pares clave-valor simples. Se pueden realizar consultas sobre las claves, pero no hay soporte para consultas complejas sobre el valor.

CouchDB
Una opción alternativa, en cuyo caso cada par se conectará a su propio servidor CouchDB externo. Los datos todavía se registran como valor clave pares, pero CouchDB permite soporte de consulta adicional del valor cuando se modela como JSON.
Los contratos inteligentes deciden qué datos leer y escribir del mundo estado utilizando las funciones getState() y putState() proporcionadas por el API de contrato inteligente de Fabric.

Es posible que un contrato inteligente no utilice el estado mundial en absoluto, aunque esto es muy improbable. También vale la pena señalar que el estado mundial se deriva enteramente de las transacciones registradas en la cadena de bloques en el libro mayor. Recuerde que cada transacción contiene el conjunto de lectura y escritura para el estado mundial. Esto significa que, si el estado mundial alguna vez se corrompe o se pierde, entonces se puede recrear por completo ejecutando las transacciones en la cadena de bloques. De hecho, esto es exactamente lo que sucede cuando un nuevo par se une a un canal por primera vez. Recibirá todos los bloques en la cadena de bloques del servicio pedido (y posiblemente otros pares) y construir su estado mundial basado en esto.
Aquí hay un contrato inteligente HelloWorld muy simple que ilustra la Interfaz de contrato inteligente de Hyperledger Fabric y operaciones del estado mundial.

```
'use strict';
const { Contract } = require('fabric-contract-api');
class HelloWorld extends Contract {
   async instantiate(ctx) {
   console.info('Writing to world state');
   await ctx.stub.putState('hw', 'Hello World');
}
async query(ctx) {
   console.info('Reading from world state');
   const value = await ctx.stub.getState('hw');
   console.info(value.toString());
}
}
module.exports = HelloWorld;
```

El contrato inteligente se llama HelloWorld. Implementa dos transacciones:

instantiate(ctx)

Esta transacción se llama una vez cuando el contrato inteligente es instanciado en el canal.

consulta(ctx)

Esta transacción se puede llamar después de crear una instancia.

La instanciación de la transacción escribe un simple par clave-valor (hw, HolaMundo) al estado del mundo usando putState().
La transacción de consulta recupera el valor de la clave hw del estado mundial usando getState() y escribe el valor en la consola.
En el próximo capítulo, exploraremos contratos inteligentes más complejos que implementan pagares comerciales.

Aplicación cliente
Para cada contrato inteligente habrá una o muchas aplicaciones cliente que llamen a las transacciones implementadas por el contrato inteligente. La aplicación cliente se comunica con la red de blockchain de Fabric utilizando el SDK de Fabric. Tanto Node.js como Java están soportados, y se están desarrollando lenguajes adicionales.

El SDK de Fabric permite a la aplicación conectarse a pares y ordenantes. Una vez conectada, la aplicación puede consultar la blockchain y también puede llamar a transacciones implementadas por contratos inteligentes.
Si se utiliza el SDK de Node.js, la aplicación cliente debe usar el módulo módulo fabric-network de Hyperledger Fabric para acceder a la API para enviar y consultar transacciones.
La aplicación cliente necesita dos datos clave para conectarse a un par utilizando la API:

Perfil de conexión

Proporciona los detalles básicos de conexión del par y el pedido servicio, como números de host y de puerto.

Cartas credenciales

Una billetera representa al usuario que envía la transacción. Este incluye la clave privada del usuario y el certificado digital. Veámoslos con más detalle.

Perfil de conexión

Un perfil de conexión no necesita incluir toda la red, sólo los detalles de conexión básicos requeridos para la solicitud del cliente específico. El SDK puede utilizar la función de descubrimiento de servicios de Fabric (si habilitado) para descubrir más información sobre la red, canales, y contratos inteligentes una vez que se realiza una conexión básica. Este es un extracto de un perfil de conexión que muestra la conexión. Detalles del solicitante, par y autoridad de certificación en nuestra red:

```
"orderers": {
"orderer.example.com": {
"url": "grpc://localhost:17050"
}
},
"peers": {
"peer0.org1.example.com": {
"url": "grpc://localhost:17051",
"eventUrl": "grpc://localhost:17053"
}
},
"certificateAuthorities": {
"ca.org1.example.com": {
"url": "http://localhost:17054",
"caName": "ca.org1.example.com"
}
}
```

Para cada componente se proporciona el nombre de host, así como la URL principal. Los pares tienen dos puertos, uno para recibir propuestas de transacciones y otro al que la aplicación cliente puede conectarse para registrarse y recibir mensajes de eventos. Cada autoridad certificadora tiene una propiedad caName.

Credenciales

Cada componente de la red, administrador y usuario tienen una identidad que es su credencial. La identidad digital comprende una clave privada (utilizada para firmar transacciones digitalmente) y un certificado digital (identidad pública).

Una red blockchain para empresas está formada por múltiples organizaciones, y cada organización gestionará sus identidades digitales para cualquier componente de red que tiene (pares y ordenantes) y cualquier administrador o usuarios. Estas identidades digitales se emiten a partir de

un Certificado Autoridad asociada a la organización. Fabric Hyperledger incluye un componente llamado Proveedor de servicios de membresía (MSP) que proporciona una capa de abstracción para que la organización emita, valide, autenticar y revocar identidades digitales.

Hyperledger Fabric tiene un proceso de dos pasos para la emisión de nuevas identidades: registro e inscripción, que se resumen a continuación:

Registro
Un administrador registra un nuevo usuario con un certificado de autorización dentro de la organización. El resultado del registro de un nuevo usuario es un ID de registro y un secreto (contraseña). Durante el registro no se emite ninguna identidad digital. El administrador envía los detalles de conexión de la autoridad certificadora junto con el ID de inscripción y el secreto al usuario.

Inscripción
El usuario se inscribe en la autoridad certificadora usando los detalles de la conexión, ID de inscripción y secreto proporcionados por el administrador. La inscripción crea claves públicas/privadas localmente antes llamar a la autoridad certificadora para emitir un certificado digital basado en las claves generadas. Este proceso utiliza lo que se conoce como solicitud de firma de certificado al llamar a la autoridad certificadora. El resultado es un certificado de clave pública X.509. Estos certificados luego se pueden validar en cualquier punto, revisándolos contra el certificado público de la autoridad certificadora, que también es conocido por toda la red.

Este proceso de dos pasos (registro e inscripción) es esencial para asegurar que la clave privada sólo sea conocida por el usuario.
Una vez creada la identidad digital (clave privada y certificado digital), estos luego se pueden almacenar en una billetera (wallet) (estructura de directorio definida por MSP) que es conocido por el SDK de Fabric.
Existe una clase de Fabric SDK separada llamada FabricCAClient para administrar identidades digitales y conectarse a la autoridad de certificación. A continuación, se muestra un ejemplo de una aplicación que utiliza esta clase para inscribir la identidad digital de un nuevo administrador.

```
// Create a new CA client for interacting with the CA.
const caURL = ccp.certificateAuthorities[caName].url;
const ca = new FabricCAServices(caURL);
// Create a new file system based wallet for managing identities.
const walletPath = path.join(process.cwd(), 'wallet');
const wallet = new FileSystemWallet(walletPath);
console.log(`Wallet path: ${walletPath}`);
// Check to see if we've already enrolled the admin.
const adminExists = await wallet.exists(appAdmin);
if (adminExists) {
return;
}
// Enroll the admin, and import new identity into wallet.
const enrollment = await ca.enroll({ enrollmentID: appAdmin,
enrollmentSecret: appAdminSecret });
const identity = X509WalletMixin.createIdentity(orgMSPID,
enrollment.certificate,
enrollment.key.toBytes());
wallet.import(appAdmin, identity);
```

En el código anterior, podemos ver cómo se definen los detalles de la autoridad certificadora y la ubicación de la billetera, antes de inscribir al nuevo administrador llamando a ca.enroll().
Los detalles completos de esta aplicación se pueden encontrar aquí. Hyperledger Fabric también incluye un comando para gestionar identidades digitales llamado fabric-ca-client.

SDK
El SDK proporciona las siguientes tres clases importantes que utiliza la aplicación cliente para comunicarse con la red blockchain:
puerta de enlace
Proporciona el punto de conexión para que una aplicación acceda a la red Fabric.
Red
Representa un canal al que se puede acceder a través de la puerta de enlace.

contrato
Representa un contrato inteligente instanciado en la red. A continuación, se muestra un código de muestra que muestra estas tres clases en uso por la aplicación cliente. Este código se conecta a nuestra red local y llama a la transacción de consulta en mi contrato inteligente HelloWorld visto anteriormente:

```
// Create a new gateway for connecting to our peer node.
const gateway = new Gateway();
await gateway.connect(ccp, { wallet,
identity: 'Admin@org1.example.com',
discovery: { enabled: false } });
// Get the network (channel) our contract is deployed to.
const network = await gateway.getNetwork('mychannel');
// Get the contract from the network.
const contract = network.getContract('HelloWorld');
// Evaluate the specified transaction.
const result = await contract.evaluateTransaction('query');
```

En el código anterior, es la declaración gateway.connect la que hace todo el trabajo para establecer la conexión a la red Fabric utilizando la identidad digital del usuario. Una vez conectada, la aplicación decide a qué canal y contrato inteligente debe hacer referencia para enviar una transacción.

Código, depuración
Como hemos visto, Hyperledger Fabric te permite desarrollar tanto sus contratos inteligentes y aplicaciones de clientes utilizando uno de varios lenguajes populares. Es probable que su IDE (Ambiente Desarrollo Integrado) de elección apoyará uno de estos. Ambos átomo y Visual Studio Code son IDE de código abierto populares que admiten complementos para estos idiomas.

También existen complementos que ayudan específicamente a simplificar el desarrollo y pruebas de contratos inteligentes para diferentes redes blockchain. Por ejemplo, existen complementos para desarrollar contratos inteligentes de Solidity en la red Ethereum y para desarrollar contratos inteligentes Fabric implementado en IBM Blockchain Platform. Este último complemento permite el desarrollador para construir, probar y depurar su contrato inteligente de Fabric dentro del entorno de Visual Studio Code antes de esa fecha conectándose a una red remota para continuar con las pruebas.

El complemento crea una red de prueba de Fabric localmente, lo que hace que sea muy rápido instalar y probar cambios en contratos inteligentes.

Funciones de contrato inteligente

Hyperledger Fabric continúa evolucionando y madurando a un ritmo rápido. Se han agregado muchas funciones adicionales para permitir al desarrollador escribir contratos inteligentes cada vez más elaborados. En esta sección, nosotros cubriremos algunas de estas características en un nivel alto:

• Los datos privados, que ya hemos descrito, permiten que los datos sean compartidos solo con aquellas organizaciones definidas dentro de la colección. El desarrollador de contratos inteligentes utilizará diferentes API para acceder el estado mundial de cualquier dato privado (getPrivateData() y putPrivateData()).

• Respaldo estatal, lo que significa que los contratos inteligentes pueden cambiar la política de patrocinio para entradas específicas en el estado mundial, anulando la política de respaldo de contrato inteligente de nivel superior. El desarrollador utilizará las siguientes API para verificar y establecer respaldo basado en el estado: GetStateValidationParameter() y SetStateValidationParameter().

• Hay una biblioteca de cifrado disponible para el desarrollador de contratos inteligentes que les permite cifrar y descifrar cualquier dato.

• Los datos se almacenan en el estado mundial dentro de un espacio de nombres asociado con el contrato inteligente. Esto significa que un contrato inteligente no puede acceder directamente al estado mundial de otro (a menos que sean escrito en el mismo código de cadena). Por lo tanto, Fabric incluye un API que permite que el primer contrato inteligente invoque otro.

• Es posible que un contrato inteligente emita eventos personalizados utilizando setEvent(), que luego es consumido por la aplicación cliente si la transacción está validada.

• Se puede consultar el certificado digital de los clientes por roles y organización y afiliaciones para que las reglas dentro del contrato inteligente puedan ser aplicadas.

Esta lista resume algunas de las muchas opciones disponibles para el contrato inteligente.

Tutoriales y patrones

Hay una serie de excelentes tutoriales y patrones disponibles tanto para Hyperledger Fabric como IBM Blockchain Platform. Dos muy buenos recursos son la documentación de Hyperledger Fabric, y los patrones de código de IBM Developer para blockchain.

Los tutoriales muestran cómo desarrollar contratos inteligentes y del lado del cliente aplicaciones, con los patrones mostrando escenarios más complejos y cómo blockchain puede funcionar con otros sistemas dentro de una arquitectura de sistema.

Resumen

En este capítulo, presentamos tanto el contrato inteligente como la aplicación cliente, que en conjunto forman la base de una aplicación blockchain. También analizamos la estructura del libro mayor dentro de Hyperledger fabric y la importancia de saber qué está grabado en qué parte del libro mayor, la cadena de bloques o el estado mundial. Finalmente, revisamos IDE como Visual Studio Code, que ayudan al desarrollador para construir y probar sus aplicaciones y contratos inteligentes.

CAPÍTULO 5
Un ejemplo de cadena de bloques:
Pagares comerciales

En el Capítulo 2, hicimos referencia al escenario de pagare comercial proporcionado como parte del repositorio de muestras de Hyperledger Fabric. En este capítulo, examinaremos este escenario en profundidad como un tutorial para comprender mejor lo que está haciendo. Luego ampliaremos el tutorial para crear una nueva transacción en el contrato inteligente y desarrollar una nueva aplicación de línea de comando para invocarla.

¿Qué es el papel comercial?
El tutorial de Papel Comercial simula una red comercial llamada PaperNet. El papel comercial es un tipo de préstamo sin garantía llamado pagaré. Normalmente lo emiten grandes empresas para obtener fondos con los que hacer frente a obligaciones financieras a corto plazo a un tipo de interés fijo. Una vez emitido a un precio fijo y por un plazo determinado, otra empresa o banco lo compra a un coste inferior a su valor nominal a un coste inferior a su valor nominal y, una vez vencido el plazo, se reembolsa por su valor nominal. Por ejemplo, si el papel se emite por un valor nominal de 10 millones de dólares a un plazo de seis meses y a un interés del 2%, el papel se canjeará por su valor nominal para un plazo de seis meses al 2% de interés, podría comprarse por 9,8 millones de dólares (10 millones - 2%) por otra empresa o banco dispuesto a riesgo de que el emisor no incumpla. Una vez finalizado el plazo, entonces el papel podría ser rescatado o vendido de nuevo al emisor por su valor nominal de 10 millones de dólares.

Entre la compra y el reembolso, el papel se puede comprar o vender varias veces entre diferentes partes en un mercado de papel comercial.

Comprender el tutorial sobre papel comercial
Anteriormente, analizamos cómo podemos utilizar la idea de activos, participantes, y transacciones para analizar casos de uso de blockchain.
De esta descripción, podemos ver que el principal activo aquí es el papel comercial en sí, que tendrá múltiples atributos tales como la empresa emisora, el valor nominal del papel, la fecha de reembolso y el estado actual (como emitido, comercializado y canjeado) del papel.

También podemos ver que hay múltiples participantes en este escenario: un emisor que será responsable de crear o emitir papel comercial, y uno o más compradores de papel comercial que serán propietarios del papel hasta que sea canjeado o vendido a otra parte. Finalmente tenemos las transacciones: son emisión, compra y redención, para emitir nuevos papeles comerciales, negociarlos y canjear el valor nominal del papel con el emisor, respectivamente.

En el tutorial hay dos participantes clave: MagnetoCorp y Digibank. El tutorial muestra a MagnetoCorp actuando inicialmente como un emisor, con DigiBank asumiendo el papel de comprador y redentor del papel comercial en la red PaperNet.

La Figura 5-1 muestra una descripción general de la red, con Isabella trabajando para MagnetoCorp, el emisor, Balaji trabaja para un comerciante de ejemplo (DigiBank), y las dos organizaciones que se comunican a través de la blockchain PaperNet:

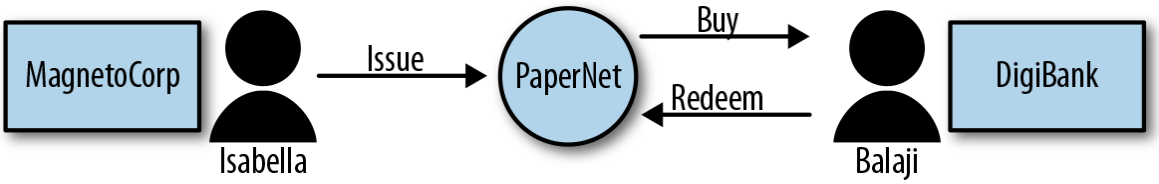

Figura 5-1. Red de muestra para el tutorial sobre papel comercial

Ejecución del tutorial sobre papel comercial
Hyperledger Fabric contiene un tutorial para papel comercial. En esta sección, presentamos el propósito de este tutorial y las tareas principales involucradas.

Una descripción más detallada del tutorial sobre papel comercial está disponible en línea; si eres un desarrollador que busca experiencia práctica de Hyperledger Fabric, le recomendamos que siga este. Al momento de escribir este artículo, el tutorial está disponible aquí.

Inicialmente, el tutorial le guiará a través de la instalación de algunos requisitos previos de software y descargar las muestras. Una vez hecho esto tomas el papel de Isabella de MagnetoCorp, quien creará la red que DigiBank se unirá. Después de instalar y crear una instancia del contrato inteligente, ejecutará una aplicación de línea de comandos que invocará la transacción de emisión del contrato inteligente.
A continuación, cambia al rol de Balaji de DigiBank, quien utilizará diferentes aplicaciones de línea de comandos para comprar el papel que Isabella emitido y luego canjearlo con otra solicitud.
El tutorial utiliza una aplicación de línea de comandos para cada transacción del contrato inteligente. Aunque esto hace que sea muy fácil ver qué es desde el punto de vista del tutorial, en un escenario más realista, se podría esperar que una aplicación llame a varias transacciones de contratos inteligentes.
Al final del tutorial, un activo de papel comercial ha sido emitidos, comprados y canjeados en la red.

Ampliación del tutorial sobre papel comercial
Aunque el tutorial muestra muchos aspectos del desarrollo de contratos inteligentes y la invocación de transacciones, actualmente no proporciona una forma de consultar un documento en particular. Por lo tanto, en esta sección veremos cómo extender el contrato inteligente de papel comercial para agregar una nueva transacción getPaper que devolverá una representación de cadena del papel solicitado a la persona que llama. Luego crearemos una nueva aplicación de línea de comandos basada en una de las existentes para poder invocarla.
Esto nos proporcionará una manera de ver los diferentes estados que atravesará el papel comercial durante su ciclo de vida, entonces lo haremos emitir papel nuevo y seguirlo a lo largo de su ciclo de vida, consultándolo en cada paso del camino.

Escribir la nueva transacción getPaper
La nueva transacción getPaper sigue el mismo modelo que la compra y canjear transacciones, pero es mucho más simple ya que no necesitamos actualizar ninguna propiedad del papel en el estado mundial:

```
/**
* Get commercial paper
* @param {Context} ctx the transaction context
* @param {String} issuer commercial paper issuer
* @param {Integer} num paper number for this issuer
```

```
*/
async getPaper(ctx, issuer, num) {
try {
console.log("getPaper for: " + issuer + " " + num);
let paperKey = CommercialPaper.makeKey([issuer, num]);
let paper = await ctx.paperList.getPaper(paperKey);
return paper.toBuffer();
} catch (e) {
throw new Error('Paper does not exist' + issuer + num);
}
}
```

Agregue este código al documento comercial/organización/magnetocorp/ contract/lib/papercontract.js y guárdelo. Debe ubicarse como una transacción de nivel superior como las otras transacciones, así que colóquela después de canjear la transacción casi al final del archivo.
Ahora repasaremos los cambios que hicimos.

Después de los comentarios, está la definición de la transacción getPaper, que toma tres parámetros. El primero (ctx) es de tipo Context y es el primer parámetro que se pasa a todas las transacciones. Esto permite que el marco pase información adicional a la función de transacción cuando se llama. Por ejemplo, puede pasar información sobre la identidad de la persona que llama al contrato, así como métodos para consultar el estado mundial cuando se llama a la transacción. El segundo y tercer parámetro (emisor y número) se pasan desde la aplicación que realiza la llamada y contienen el emisor y el número del documento que deseamos recuperar.

Después de registrar los parámetros pasados en el registro de la consola, la transacción llama al método estático CommercialPaper.makeKey. Este método se define en el archivo ledger-api/state.js y es método ayuda para crear una clave de estado mundial para el documento. Recuerda que, en el último capítulo, los datos del estado mundial se almacenan como clave/valores pares, y para el tutorial de papel comercial la clave se define utilizando este método. En este ejemplo, la clave es simplemente una concatenación del emisor y el número del papel, separados por dos puntos; por ejemplo, MagnetoCorp:00001.
A continuación, la transacción utiliza el valor de retorno de paperKey para solicitar un documento específico llamando a ctx.paperList.getPaper y pasando la clave (paperKey). Como puede ver, esto está usando el parámetro ctx para acceder a paperList y llamar a su método getPaper. La descripción de este método se proporciona en el archivo lib/paperlist.js.

A su vez, paperList.getPaper simplemente llama al método getState definido en ledger-api/stateList.js. Es este método el que en realidad accede al estado mundial para recuperar el papel comercial solicitado activo.
Una vez que tenemos el papel solicitado, simplemente se lo devolvemos a nuestra persona que llama como un objeto de búfer. Si el papel comercial solicitado no existe en el estado mundial, se lanzará una excepción, informando a nuestra persona que llama que el pedido de papel no existe.

Escribiendo la nueva aplicación getPaper.js
La aplicación getPaper.js se basa en la aplicación buy.js existente que viene con el tutorial sobre papel comercial. No le muestro todo el código aquí, ya que hay más de 100 líneas de código. Sin embargo, la mayoría de estas líneas siguen siendo las mismas: solo vamos a cambiar unas 12 de ellos.
Para comenzar, haga una copia del documento comercial/organización/

digibank/application/buy.js y llame a la copia getPaper.js. Asegúrese de que la copia esté en la misma carpeta que buy.js. Abra el archivo en un editor de código como VSCode y revise el archivo para las líneas console.log que contienen la cadena "Comprar programa"; Por ejemplo:

```
console.log('Buy program complete.');
...
console.log('Buy program exception.');
```

Para evitar confusiones, cambie Buy a GetPaper en todo momento, de modo que cuando revisamos posteriormente estos registros de la consola, vemos la correcta salida de la aplicación.

A continuación, elimine las secciones de compra de papel comercial y respuesta al proceso en el método principal, ya que estos no son relevantes a la aplicación getPaper:

```
// buy commercial paper
console.log('Submit commercial paper buy transaction.');
const buyResponse = await contract.submitTransaction('buy',
'MagnetoCorp', '00001', 'MagnetoCorp', 'DigiBank',
'4900000', '2020-05-31');
// process response
console.log('Process buy transaction response.');
let paper = CommercialPaper.fromBuffer(buyResponse);
console.log(`${paper.issuer} commercial paper :
${paper.paperNumber} successfully purchased by
${paper.owner}`);
```

En lugar de este bloque eliminado, justo antes del mensaje de registro de transacción completa, agregue el siguiente código. (Tenga en cuenta que agregará en algunas líneas más de las que eliminaste, pero está bien, estamos haciendo un poco más trabajo para formatear bien el objeto de papel devuelto. Asegúrese de guardar el archivo cuando haya terminado).

```
// get commercial paper
console.log('Evaluate getPaper transaction.');
const getPaperResponse = await contract.evaluateTransaction(
'getPaper', 'MagnetoCorp', '00001');
console.log('Process getPaper transaction response.');
let paper = CommercialPaper.fromBuffer(getPaperResponse);
let paperState = "Unknown";
if (paper.isIssued()) {
paperState = "ISSUED";
} else if (paper.isTrading()) {
paperState = "TRADING";
} else if (paper.isRedeemed()) {
paperState = "REDEEMED";
}
console.log(` +--------- Paper Retrieved ---------+ `);
console.log(` | Paper number: "${paper.paperNumber}"`);
console.log(` | Paper is owned by: "${paper.owner}"`);
console.log(` | Paper is currently: "${paperState}"`);
console.log(` | Paper face value: "${paper.faceValue}"`);
console.log(` | Paper is issued by: "${paper.issuer}"`);
console.log(` | Paper issue on: "${paper.issueDateTime}"`);
console.log(` | Paper matures: "${paper.maturityDateTime}"`);
console.log(` +----------------------------------+ `);
```

Mirando este nuevo código que insertamos, podemos ver que comienza por registrar la llamada que está a punto de realizar en el contrato en la consola. Luego llama al método evaluaTransaction del contrato para enviar la llamada al par para ejecutar la transacción getPaper.

Tenga en cuenta que en getPaper estamos usando evaluaTransaction en lugar de que el método submitTransaction que las otras transacciones usar; la diferencia es que evaluaTransaction no registra la transacción en el libro mayor, y como no cambiamos ningún estado cuando devolver el periódico, está bien.

Los parámetros pasados para evaluarTransaction indican que quiero obtener el documento 00001 de MagnetoCorp, que fue el que se emitió cuando ejecutaste el tutorial. Una vez devuelto el papel, averiguar en qué estado se encuentra el documento (EMITIDO, COMERCIALIZADO o CANJEADO) (ISSUED, TRADING, or REDEEMED) y luego imprima esto junto con el resto de la información contenida dentro del papel, como su número de papel, emisor, propietario y cara valor.

Actualización del contrato inteligente

Ahora que hemos editado el contrato inteligente para agregar la nueva transacción y creado la nueva aplicación de línea de comando getPaper, es hora de probar ambos. Para hacer esto, primero tenemos que instalar el contrato inteligente modificado en el par. Desde la ventana de la consola de magnetocorp, que debería haber abierto al ejecutar el tutorial, ejecute este comando para instalar la nueva versión 2 del contrato:

```
(magnetocorp admin)$ docker exec cliMagnetoCorp peer chaincode
install -n papercontract -v 2 -p /opt/gopath/src/github.com/co
ntract -l node
```

Cuando se complete, debería ver un resultado como este:

```
2019-02-21 13:32:23.824 UTC [chaincodeCmd] checkChaincodeCmdPa
rams -> INFO 001 Using default escc
2019-02-21 13:32:23.824 UTC [chaincodeCmd] checkChaincodeCmdPa
rams -> INFO 002 Using default vscc
2019-02-21 13:32:23.832 UTC [chaincodeCmd] install -> INFO 003
Installed remotely response:<status:200 payload:"OK" >
```

A continuación, tenemos que actualizar el contrato inteligente versión 2 en los pares para activarlo:

```
(magnetocorp admin)$ docker exec cliMagnetoCorp peer chaincode
upgrade -n papercontract -v 2 -l node -c '{"Args":["org.papern
et.commercialpaper:instantiate"]}' -C mychannel -P "AND ('Org1
MSP.member')"
```

Cuando se complete (lo que puede tardar unos minutos), debería ver una salida como esta:

```
2019-02-21 13:32:35.508 UTC [chaincodeCmd] InitCmdFactory ->
INFO 001 Retrieved channel (mychannel) orderer endpoint:
orderer.example.com:7050
2019-02-21 13:32:35.511 UTC [chaincodeCmd] checkChaincodeCmdPar
ams -> INFO 002 Using default escc
2019-02-21 13:32:35.511 UTC [chaincodeCmd] checkChaincodeCmdPar
ams -> INFO 003 Using default vscc
```

Invocando la nueva aplicación getPaper.js

Ahora estamos listos para invocar la aplicación getPaper.js y probar si se lleva a cabo la nueva transacción de contrato inteligente. Primero, verifique que la consola ventana para Balaji de DigiBank, que deberías tener abierta de ejecutar el tutorial, se encuentra actualmente en el documento comercial/organización/ directorio digibank/aplicación. Si no es así, simplemente use cd para cambiar a este directorio. Aquí es donde surge la nueva aplicación getPaper.js. Emita este comando para ejecutar la aplicación:

```
(balaji)$ node getPaper.js
```

Debería esperar ver un resultado como este:

```
Connect to Fabric gateway.
Use network channel: mychannel.
Use org.papernet.commercialpaper smart contract.
Submit commercial paper getPaper transaction.
Process getPaper transaction response.

+--------- Paper Retrieved ---------+
| Paper number: "00001"
| Paper is owned by: "MagnetoCorp"
| Paper is currently: "REDEEMED"
| Paper face value: "5000000"
| Paper is issued by: "MagnetoCorp"
| Paper issue on: "2020-05-31"
| Paper matures on: "2020-11-20"
+----------------------------------+
Transaction complete.
Disconnect from Fabric gateway.
GetPaper program complete.
```

Suponiendo que haya completado el tutorial con éxito anteriormente, ahora deberías ver el estado REDIMIDO (REDEEMED)final del papel comercial número 00001 que MagnetoCorp emitió después de que DigiBank lo comprara y luego lo canjeara.

Prueba con papel comercial nuevo

Ahora repasemos esto una vez más: emisión, compra y canjeando un segundo papel (número 00002). Pero esta vez lo haremos mirando el resultado de getPaper en cada paso del camino.

Para hacer esto necesitaremos editar los cuatro programas para usar el nuevo papel comercial. Comenzaremos con uno de los más sencillos: getPaper.js. abrir obtener Paper.js en su editor y busque esta línea de código:

```
const getPaperResponse = await contract.evaluateTransaction(
'getPaper', 'MargetoCorp', '00001');
```

Cambie el número de papel de 00001 a 00002 y guarde el cambio en el archivo. Aunque podrías ejecutar getPaper.js en este punto, devolvería un error ya que actualmente no hay ningún papel con el número 00002. Entonces, creemos uno. Abra issues.js desde el directorio organización/magnetocorp/application y busque esta línea:

```
const issueResponse = await contract.submitTransaction(
'issue', 'MagnetoCorp','00001','2020-05-31',
'2020-11-20','5000000');
```

Cambia el número de papel de 00001 a 00002, y así podremos ver más diferencias, cambia la cantidad de 5000000 a 6000000. Puedes cambiar las fechas, así como si lo deseas. Su línea modificada debería verse así:

```
const issueResponse = await contract.submitTransaction('issue',
'MagnetoCorp','00002','2019-06-30','2019-12-30','6000000');
```

Desde la ventana de la consola de MagnetoCorp, emita este comando para el documento temático 00002:

```
(magnetocorp admin)$ node issue.js
```

Debería ver un resultado que indique que el documento se emitió correctamente, con el resultado del formulario:

```
MagnetoCorp commercial paper : 00002 successfully issued for
value 6000000
```

A continuación, desde la ventana de la consola de Balaji ejecute la aplicación getPaper:

```
(balaji)$ node getPaper.js
```

La salida debe contener:

```
+--------- Paper Retrieved ---------+
| Paper number: "00002"
| Paper is owned by: "MagnetoCorp"
| Paper is currently: "ISSUED"
| Paper face value: "6000000"
| Paper is issued by: "MagnetoCorp"
| Paper issue on: "2019-06-30"
| Paper matures on: "2019-12-30"
+----------------------------------+
```

Ahora podemos ver que el documento ya ha sido emitido por MagnetoCorp, pero aún es de su propiedad ya que aún no se ha vendido. Ahora compremos este nuevo papel comercial como DigiBank. Abra buy.js desde organización/digibank/carpeta de la aplicación y busque esta línea:

```
const buyResponse = await contract.submitTransaction(
'buy', 'MagnetoCorp', '00001', 'MagnetoCorp', 'DigiBank',
'4900000', '2020-05-31');
```

Si observamos la transacción de compra en el contrato inteligente de papercontract.js, podemos ver los parámetros que representan la transacción a llamar (comprar), el emisor, el número de papel, el propietario actual, el nuevo propietario, el precio y la fecha y hora de compra. Edite la línea para actualizar los parámetros del nuevo documento para que se vea así:

```
const buyResponse = await contract.submitTransaction(
'buy', 'MagnetoCorp', '00002', 'MagnetoCorp', 'DigiBank',
'5880000', '2019-10-30');
```

Cuando haya terminado, guarde el archivo y desde la ventana de la consola de Balaji ejecuta el comando de compra:

```
(balaji)$ nodo buy.js
```

Debería ver un resultado que indique que la transacción se realizó correctamente:

```
Papel comercial MagnetoCorp: 00002 comprado con éxito por DigiBank
```

A continuación, ejecutemos getPaper nuevamente:

```
(balaji)$ nodo getPaper.js
```

El resultado debe incluir esto:

```
+--------- Paper Retrieved ---------+
| Paper number: "00002"
| Paper is owned by: "DigiBank"
| Paper is currently: "TRADING"
| Paper face value: "6000000"
| Paper is issued by: "MagnetoCorp"
| Paper issue on: "2019-06-31"
| Paper matures on: "2019-12-30"
+-----------------------------------+
```

Como podemos ver, el papel comercial ahora es propiedad de DigiBank y ahora está en el estado COMERCIAL (TRADING).

Finalmente, cambiemos canje.js, que está junto a buy.js en la carpeta de aplicaciones de DigiBank. Abra el archivo en su editor y busque esta línea:

```
const redeemResponse = await contract.submitTransaction(
'redeem', 'MagnetoCorp', '00001', 'DigiBank', '2020-11-30');
```

Aquí necesitamos cambiar el número de papel comercial y la fecha de canje para que esté completo, edite la línea para que se vea así:

```
const redeemResponse = await contract.submitTransaction(
'redeem', 'MagnetoCorp', '00002', 'DigiBank', '2019-11-30');
```

Cuando haya terminado, guarde el archivo y desde la ventana de la consola de Balaji ejecuta el comando canjear:

```
(balaji)$ nodo canjear.js
```

Debería ver un resultado que indique que la transacción se realizó correctamente:

```
MagnetoCorp commercial paper : 00002 successfully redeemed with
MagnetoCorp
```

A continuación, ejecutemos getPaper por última vez:

```
(balaji)$ nodo getPaper.js
```

La salida debería verse así:

```
+--------- Paper Retrieved ---------+
| Paper number: "00002"
| Paper is owned by: "MagnetoCorp"
| Paper is currently: "REDEEMED"
| Paper face value: "6000000"
| Paper is issued by: "MagnetoCorp"
| Paper issue on: "2019-06-30"
| Paper matures on: "2019-12-30"
+-----------------------------------+
```

Aquí podemos ver que el papel ya está canjeado y el ciclo está completo. En este punto, siéntete libre de experimentar por tu cuenta, tal vez ampliar aún más el contrato inteligente para mejorar la verificación de errores o escribir una nueva aplicación de línea de comandos para encontrar todos los COMERCIOS o Papeles CANJEADOS. O puede intentar facilitar las aplicaciones para usar tomando argumentos de la línea de comando para los parámetros como paperNumber para evitar tener que editar los archivos manualmente para trabajar con un nuevo activo.

Resumen

Hemos realizado un recorrido relámpago por el tutorial sobre papel comercial, y ha actualizado su contrato inteligente para incluir una nueva transacción getPaper. Hemos instalado y actualizado la red PaperNet a la nueva versión del contrato, e incluso hemos escrito una nueva aplicación de línea de comandos para ejecutar la nueva transacción getPaper.

Finalmente, emitimos un nuevo activo de papel comercial y seguimos su ciclo de vida, observando los cambios de estado que se le realizaron en su viaje. Si es desarrollador de contratos inteligentes, existe una herramienta de uso gratuito disponible para facilitar mucho el desarrollo de su contrato inteligente.

La extensión IBM Blockchain Platform para VSCode ayuda a Hyperledger Desarrolladores de Fabric para desarrollar y probar contratos inteligentes y aplicaciones cliente en sus máquinas locales, así como empaquetar sus proyectos para su implementación en tiempos de ejecución de IBM Blockchain Platform. En el capítulo final, haremos una mirada en la forma de las cosas vienen y dónde está el futuro de la tecnología blockchain.

CAPÍTULO 6
¿Qué sigue en Blockchain?

En este libro, hemos analizado en detalle al Blockchain para empresas. Comenzó definiendo conceptos comerciales relevantes, como libros mayores y contratos y cómo el principio clave detrás de blockchain es compartir estos artefactos entre los participantes de una red empresarial, haciendo los datos sean irrefutables y contribuyan así a generar confianza.

Analizamos aplicaciones comunes para blockchain y cómo identificarlas como buenas ideas. Luego nos sumergimos en la tecnología y analizamos cómo diseñar y desarrollar para ello, utilizando el papel comercial como ejemplo.

En este último capítulo, veremos dónde nos encontramos actualmente en términos del desarrollo y usos de blockchain, y cuál será el futuro que podría ser válido para esta interesante innovación. Haremos esto mirando blockchain a través de la lente de la tecnología y las aplicaciones que lo use.

Tecnología blockchain
Cuando una tecnología alcanza un cierto punto de madurez, el conjunto básico de requisitos se ha implementado en gran medida y es importante comenzar el período de optimización. Ahora estamos viendo esto en todo el blockchain para la comunidad empresarial, ya que existen esfuerzos importantes hacia características que brinden mejoras en la calidad de vida, como estandarización, estabilidad y simplificación. Además, estamos viendo (por supuesto) la próxima generación de innovación. Ahora veremos estas diferentes áreas.

Estandarización
Toda tecnología exitosa pasa por tres fases distintas: innovación, estandarización y mercantilización. La innovación es la desencadenante que despierta el interés inicial en la tecnología. Estandarización es el proceso de las fuerzas del mercado que obliga a una industria a aceptar un vocabulario común, ya sea un protocolo técnico, especificación, o alguna otra capa. La mercantilización es el proceso mediante el cual la tecnología se vuelve más barata y más fácil de adoptar.
Para blockchain, el detonante de la innovación fue posiblemente la creación de Bitcoin en 2008, aunque se pueden señalar otras tecnologías como redes peer-to-peer, hashchains o incluso la documentación de Luca Pacioli de la contabilidad por partida doble como peldaños que han conducido a nosotros a blockchain. Sin embargo, desde 2008, después de varios años de blockchain educación y experimentación, ahora se están invirtiendo esfuerzos sobre estandarización. Esta fase es importante porque los estándares permiten que los activos fluyan más fácilmente a través de diversas redes comerciales, y que las redes crezcan independientemente de la tecnología contable. Como se analiza en el Capítulo 1, el futuro está en la red de redes.

La estandarización puede ocurrir en muchos niveles diferentes; los mejores estándares son descriptivos más que prescriptivos, ya que permiten profundizar la innovación y para que se formen nuevos modelos de negocio. Cuerpos tales como ISO, IEEE y W3C están analizando diferentes aspectos de blockchain estándares. Además, la Enterprise Ethereum Alliance ha documentó una especificación para clientes blockchain que está comenzando a ganar terreno, y el Protocolo Inter-Ledgering es un esfuerzo en la capa de protocolo para que blockchains se comunique, esto es actualmente muy específico de los pagos.
Con el tiempo, surgirán estándares y aspectos de la tecnología blockchain que se convertirán en un producto básico, lo cual es bueno ya que proporciona la motivación para seguir innovando. Los

vendedores buscarán más valor encima de la cadena de bloques, ya sea a través de plataformas, análisis, Internet de las cosas o alguna otra innovación desencadenante y el ciclo puede comenzar de nuevo.

Estabilidad

Si bien se están agregando nuevas características a las tecnologías blockchain como como Hyperledger Fabric, podemos esperar ver un período de estabilización a medida que las redes empresariales llevan sus pilotos a producción. Un buen examen que pretende ser una base conocida que las empresas puedan cómodamente pasar a producción y sobre qué correcciones se pueden aplicar.

Simplificación

Existe una fuerte demanda de simplificación, lo que vuelve a ser un signo de la creciente madurez de la tecnología a medida que blockchain avanza desde un esfuerzo de la comunidad de investigación en la corriente principal. El aumento de la cobertura del lenguaje de programación, contratos inteligentes simplificados, y las API de cliente en Hyperledger Fabric lo harán aún más fácil para desarrollar soluciones blockchain. En el futuro, podemos esperar ver una mayor reducción de las barreras para ingresar a blockchain, incluida la atención a distritos no técnicos como líderes empresariales y abogados, que tal vez no necesiten interfaces técnicas con el libro mayor, pero tienen intereses creados en la naturaleza de los contratos inteligentes activos.

La próxima generación de características de Blockchain

Se sigue aplicando una gran cantidad de innovación a blockchain, normalmente a través de la aplicación de investigaciones relacionadas. Juntos estos, ayudan a abordar las preocupaciones y desafíos de la adopción de blockchain dentro de las redes empresariales. Por ejemplo:

Criptoanclajes

Estos proporcionan una forma de codificar huellas digitales en los objetos del mundo real. Para blockchain esto proporcionará una interesante forma de identificar y verificar activos en una cadena de bloques que no puede codificarse fácilmente (aspirina o aceite, por ejemplo), lo que ayudará a resolver el problema de los productos falsificados.

Servicios de gestión de tokens

Estos permiten que las blockchain autorizadas creen tokens fungibles que mapeen a los activos, lo que permite que múltiples de ellos sean fácilmente negociado. Mientras que el modelo UTXO que describe un mecanismo eficiente para la emisión, almacenamiento y transferencia de tokens ha estado presente durante mucho tiempo en implementaciones de criptomonedas como Bitcoin, ahora lo vemos aparecer en blockchain basadas en políticas como Hyperledger Fabric. Los tokens ayudarán a reunir previamente modelos conceptuales separados de activos y, por lo tanto, permiten que estas blockchain funcionen con un conjunto mucho más amplio de tipos de activos.

Pruebas de conocimiento cero

Estos le permiten demostrarle a un tercero que conoce un hecho sin revelar el hecho en sí. Esto permitirá que las cadenas de bloques utilizarse como un almacén de pruebas en lugar de un almacén de datos, permitiendo empresas para evitar el riesgo de compartir información confidencial con personas no autorizadas. Esto es particularmente importante en escenarios de negociación de activos, en los que los detalles de los participantes de una operación pueden seguir siendo confidencial y, al mismo tiempo, proporcionar transparencia a los organismos reguladores

Inteligencia artificial
Esta es un área amplia que cubre el aprendizaje automático, el análisis y otras tecnologías. Más comúnmente en blockchain, la IA puede ser utilizada para proporcionar información sobre los datos almacenados en el sistema compartido de registro, brindando información sobre el ciclo de vida de los activos y proporcionando los datos necesarios para una mayor optimización del proceso.

Aplicaciones blockchain
Por supuesto, toda esta tecnología es inútil si lucha por encontrar una aplicación convincente que resuelva una necesidad del mundo real. Con cientos de empresas invirtiendo en blockchain, no hay escasez de comunicados de prensa y otros artículos que describan el potencial y usos reales de la tecnología. Si el precedente de otras innovadoras tecnologías a lo largo de los años, desde la imprenta y el motor de vapor a Internet—según lo que se tenga en cuenta, pasarán muchos años hasta que descubramos toda la gama de aplicaciones para las que blockchain sea adecuado.

Las aplicaciones Blockchain se pueden clasificar en dos tipos principales: aquellos que tienen un beneficio predominante para los negocios y aquellos que tener mayores beneficios para la sociedad en su conjunto. Ahora veremos varios ejemplos.

Blockchain para empresas
Los primeros en adoptar blockchain para empresas fueron predominantemente en la industria financiera. Hay varias razones posibles para esto, incluyendo una fuerte comunidad fintech, la asociación de blockchain (al menos inicialmente) con las criptomonedas, y el hecho de que la confianza reside en el corazón del negocio bancario (es decir, confiamos en los bancos para que se encarguen de nuestro dinero en lugar de guardarlo debajo de nuestros colchones).

Existen varias blockchain financieras bien avanzadas, para escenarios que incluyen pagos internacionales, financiación del comercio y cartas de crédito.

Una de las áreas más populares para las blockchains empresariales de hoy es el seguimiento de activos en las cadenas de suministro. Esto se debe a la falta de confianza y transparencia que exhiben muchas cadenas de suministro, el problema de falsificación que resulta de esto, y la capacidad de blockchains para rastrear de manera irrefutable la procedencia de los activos. Algunos ejemplos de suministros incluyen alimentos, transporte, diamantes, vino y medicamentos, pero el mismo modelo podría aplicarse a cualquier medicamento de alto valor activo. Ahora estamos viendo la aparición de plantillas para facilitar el desarrollo de blockchains de cadena de suministro (por ejemplo, Hyperledger Cuadrícula™).

De cara al futuro, lo que las empresas empezarán a descubrir es que las industrias en los que se implementan las blockchains ya no son relevantes. La naturaleza interrelacionada de las redes empresariales significa que como blockchains ampliaran su membresía y complejidad, definiendo una cadena de bloques como pertenecer a una sola industria o geografía ya no tiene sentido.
Las cadenas de suministro suelen ser globales y pueden abarcar la fabricación, la distribución, comercio minorista, finanzas y otros sectores también. ¿En qué momento una blockchain de medicamentos deja de ser una blockchain de medicamentos cuando se dispensa la transacción y se desencadena un proceso de negocio de reabastecimiento de existencias que luego desencadena una operación de financiamiento, fabricación y repuestos?
En una red de redes, el efecto cascada será significativo y las empresas estarán verdaderamente interconectadas. Estas ganancias de eficiencia reducirán costos, permitirá llegar a nuevos mercados

y generará una nueva era de aplicaciones transaccionales. Diferentes gobiernos han dado prioridades cuando se trata de proteccionismo versus libre mercado acceso, pero con el tiempo sabemos que los mercados competitivos eliminar las barreras al comercio y gravitar hacia el costo más bajo, las más soluciones eficientes. Blockchain puede ayudar a que eso suceda.

Blockchains por el bien de la sociedad

También existe un conjunto atractivo de aplicaciones blockchain que (o ya) existen predominantemente para el bien de la sociedad, pero también proporcionan beneficio complementario para las empresas. Éstos son algunos de los más interesantes:

• Un estudio de 2009 de la Oficina de las Naciones Unidas contra la Droga y el Delito mostró que los ciudadanos afganos pagaron 2.500 millones de dólares en sobornos (unos 23% del PIB de Afganistán). Los contratos inteligentes hacen cumplir los términos para cualquier transacción determinada y la propia cadena de bloques engendra transparencia. Estas características, cuando se aplican a organizaciones benéficas donaciones y ayuda, ayudarán a reducir los sobornos y los efectos de corrupción, particularmente en los países en desarrollo.

• El mundo está viendo un aumento en el clima extremo, y la capacidad de asegurar viviendas en las zonas afectadas es a menudo imposible porque un solo asegurador no puede cubrir adecuadamente el riesgo. En California, por ejemplo, sólo el 12% de los propietarios de viviendas están cubiertos por seguro contra terremotos. Agrupar el riesgo mediante bonos de catástrofe y blockchain para automatizar el proceso de reclamaciones en todo el mundo.
La red de aseguradoras ayudará a las familias a reconstruir más sus vidas rápidamente después de eventos climáticos extremos.

• Los mercados dinámicos basados en blockchain conducirán a mercados más eficientes, uso de los recursos naturales en un sector energético cada vez más complejo red que incluye diversos productores y consumidores, como coches eléctricos y paneles solares. Por ejemplo, TenneT y Vandebron tienen un proyecto piloto que ofrece a los propietarios de automóviles acceso al mercado eléctrico. Estos mercados también ayudarán a limpiar el plástico en nuestros océanos creando incentivos para su recolección y reciclaje de residuos plásticos (por ejemplo, PlasticBank).

• Sistemas de identidad descentralizados (como la red Sovrin y plataformas creadas con Hyperledger Indy) ponen a los usuarios en control de sus propios datos personales y también proporciona un mecanismo de verificación reclamaciones (hechos) contra esos usuarios. Esto permitirá a las organizaciones tales como instituciones educativas y empleadores para dar fe calificaciones e historial laboral, lo que ayudará a prevenir fraude. La misma idea también podría ayudar a los productores de contenidos atribuir los medios a sus fuentes, ayudando así a combatir el plagio y "noticias falsas".

Resumen

Realmente estamos apenas arañando la superficie cuando se trata de aplicaciones blockchain. La tecnología viene con un conjunto muy simple de objetivos: generar confianza y eliminar fricciones en las transacciones. Imagine poder intercambiar activos de manera confiable con cualquier persona, en cualquier lugar en el mundo sin fronteras, tan fácilmente como puedes usar el Internet para intercambiar datos hoy. Con blockchain, vivimos en una era de la innovación, y es emocionante ver adónde nos llevará.