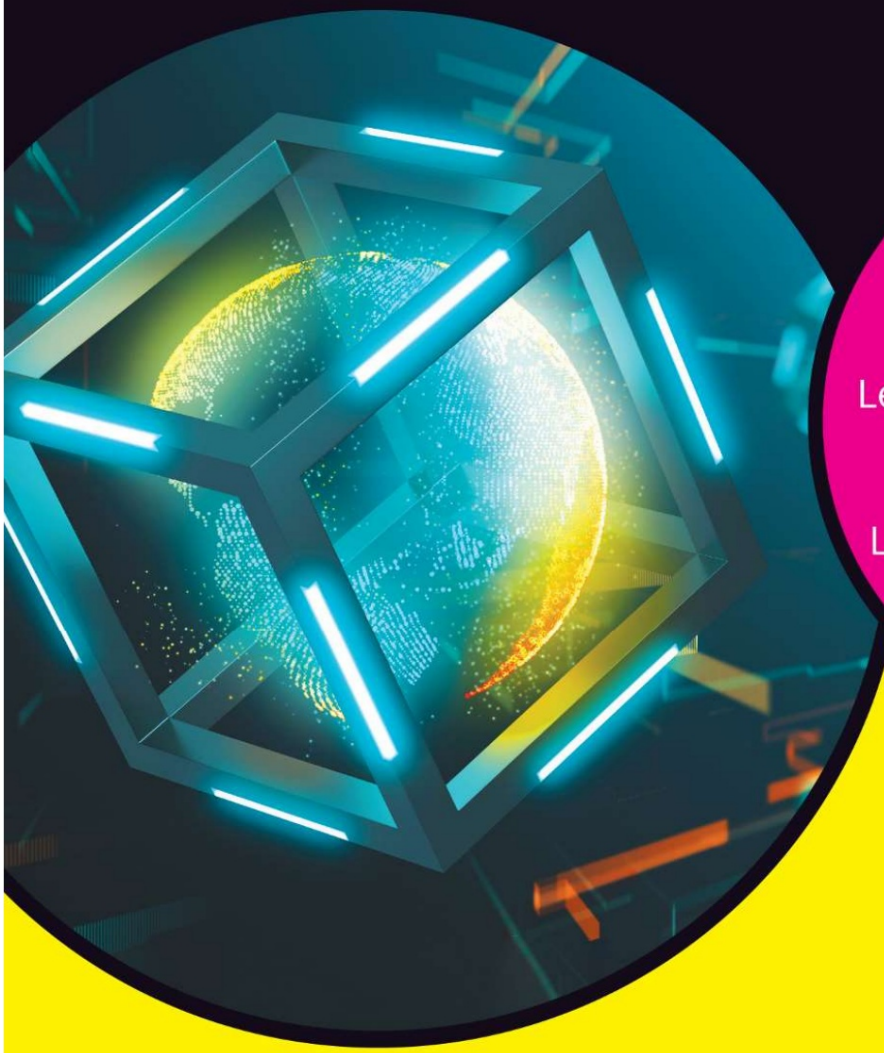
LEARNING MADE EASY

3rd Edition

Blockchain

for dummies®

A Wiley Brand



Peek under the hood of tech changing finance

Learn how Blockchain powers cryptocurrency

Launch your own blockchain apps on stable platforms

Tiana Laurence

Blockchain pioneer and investor

Blockchain

for dummies®

A Wiley Brand

Blockchain

3ra edición

por Tiana Laurence

for dummies®
A Wiley Brand

Blockchain para Dummies®, 3.ª edición

Publicado por: John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774, www.wiley.com

Para obtener información general sobre nuestros otros productos y servicios, comuníquese con nuestro Departamento de atención al cliente dentro de los EE. UU. al 877-762-2974, fuera de los EE. UU. al 317-572-3993 o al fax 317-572-4002. Para obtener asistencia técnica, visite https:// hub.wiley.com/community/support/dummies.

Wiley publica en una variedad de formatos impresos y electrónicos y por impresión bajo demanda. Es posible que parte del material incluido con las versiones impresas estándar de este libro no se incluya en los libros electrónicos o en la impresión bajo demanda. Si este libro hace referencia a medios como un CD o DVD que no está incluido en la versión que compró, puede descargar este material en http://booksupport.wiley.com. Para obtener más información sobre los productos Wiley, visite www.wiley.com.

Número de control de la Biblioteca del Congreso: 2023931209

ISBN 978-1-394-15966-6 (pbk); ISBN 978-1-394-15967-3 (ebk); ISBN 978-1-394-15968-0 (ebk)

Contenido de un vistazo

Tabla de contenido

Introducción

¡Bienvenido a Blockchain para Dummies! Si quieres saber qué bloque son las cadenas y los conceptos básicos de cómo usarlas, este es el libro para usted.

Mucha gente piensa que las cadenas de bloques son difíciles de entender. También pueden pensar que las cadenas de bloques son solo criptomonedas como Bitcoin, pero son mucho más. Cualquiera puede dominar los conceptos básicos de blockchains.

En este libro, encontrará consejos útiles para navegar por el mundo de las cadenas de bloques y las criptomonedas que las ejecutan. También encontrará tutoriales prácticos paso a paso que le ayudarán a comprender cómo funcionan las cadenas de bloques y dónde agregan valor.
No necesita tener experiencia en programación, economía o mundo para entender este libro, pero toco todos estos temas porque la tecnología blockchain los cruza a todos.

Sobre este libro

Este libro explica los conceptos básicos de las cadenas de bloques, los contratos inteligentes y las criptomonedas. Probablemente eligió este libro porque ha oído hablar de las cadenas de bloques y sabe que son importantes, pero no tiene idea de qué son, cómo funcionan o por qué debería importarle. Este libro responde a todas estas preguntas en términos fáciles de entender.

Este libro es un poco diferente de casi cualquier otro libro de blockchain en el mercado. Proporciona una encuesta de todas las cadenas de bloques clave en el mercado público, cómo funcionan, qué hacen y algo útil que puede probar con ellas hoy.

Este libro también cubre el panorama de la tecnología blockchain y señala algunas de las cosas clave que debe tener en cuenta para sus propios proyectos blockchain. Aquí, descubra cómo instalar una billetera Ethereum, crear y ejecutar un contrato inteligente, realizar entradas en Bitcoin y ganar criptomonedas.

No tienes que leer el libro de principio a fin. Justip al tema que le interesa.

Finalmente, dentro de este libro, puede notar que algunas direcciones web se dividen en dos líneas de texto. Si estás leyendo este libro impreso y quieres visitar una de estas web

páginas, simplemente ingrese la dirección web exactamente como se indica en el texto, fingiendo que el salto de línea no existe. Si está leyendo esto como un libro electrónico, lo tiene fácil: simplemente haga clic en la dirección web para ir directamente a la página web.

suposiciones tontas

No hago muchas suposiciones sobre usted y su experiencia con las criptomonedas, la programación y los asuntos legales, pero sí asumo lo siguiente:

» Tienes una computadora, un teléfono inteligente y acceso a Internet.

» Conoces los conceptos básicos de cómo usar tu computadora e Internet.

» Sabe navegar por los menús dentro de los programas.

» Eres nuevo en blockchain y no eres un programador experto. Por supuesto, si usted es un programador experto, aún puede sacar mucho provecho de este libro; es posible que pueda pasar rápidamente por alto algunas de las pautas paso a paso.

Iconos utilizados en este libro

A lo largo de este libro, utilizo íconos en el margen para llamar su atención sobre ciertos tipos de información. Esto es lo que significan los íconos:

El ícono de Sugerencia marca sugerencias y accesos directos que puede usar para hacer que las cadenas de bloques sean más fáciles de usar.

El ícono de Recordar marca la información que es especialmente importante saber: las cosas que querrás memorizar. Para desviar la información más importante de cada capítulo, simplemente hojee estos íconos.

El ícono Technical Stu marca información de naturaleza altamente técnica que puede omitir sin perder el punto principal del tema en cuestión.

¡El icono de Advertencia le indica que tenga cuidado! Marca información importante que puede ahorrarle dolores de cabeza, o fichas.

Más allá del libro

Además del material en el libro impreso o electrónico que está leyendo en este momento, este producto también incluye algunas ventajas de acceso desde cualquier lugar en la web. Consulte la hoja de trucos gratuita para obtener más información sobre las cadenas de bloques. Para obtener esta hoja de trucos, simplemente vaya a www.dummies.com y escriba Blockchain For Dummies Cheat Sheet en el cuadro de búsqueda.

A dónde ir desde aquí

Puede aplicar la tecnología blockchain a prácticamente todos los dominios comerciales. En este momento hay un crecimiento explosivo en las industrias financiera, de salud, gubernamental y de seguros, y esto es solo el comienzo. El mundo entero está cambiando y las posibilidades son infinitas.

1

Primeros pasos con la cadena de bloques

EN ESTA PARTE . . .

Descubra de qué se tratan las cadenas de bloques y cómo pueden beneficiar a su organización.

Identificar el tipo correcto de tecnología y los pasos para desarrollar y ejecutar una cadena de bloques efectiva proyecto.

Haga sus propios contratos inteligentes en Bitcoin y determine dónde no puede encajar esta tecnología dentro de su organización.

EN ESTE CAPÍTULO

» Descubriendo el nuevo mundo de las cadenas de bloques

» Comprender por qué son importantes

» Identificando los tres tipos de blockchains

» Profundizando su conocimiento de cómo las cadenas de bloques funcionan

Capítulo 1

Introducción a la cadena de bloques

Originalmente, blockchain era solo el término informático para referirse a cómo estructurar, almacenar y compartir datos. Hoy en día, las cadenas de bloques se proclaman como la "quinta evolución" de informática. O más comúnmente ahora la columna vertebral del movimiento Web3.

Las cadenas de bloques son un enfoque novedoso para la base de datos distribuida. la innovación proviene de la incorporación de tecnología antigua en formas nuevas. Puede pensar en las cadenas de bloques como bases de datos distribuidas que un grupo de individuos controla y que almacenan y compartir información.

Hay muchos tipos diferentes de cadenas de bloques y aplicaciones de cadenas de bloques. La cadena de bloques es una tecnología integral que se está integrando en plataformas y hardware en todo el mundo.

Empezando por el principio: Qué son las cadenas de bloques

Una cadena de bloques es una estructura de datos que hace posible crear un registro digital de datos y compartirlo entre una red de partes independientes. Hay muchos tipos diferentes de cadenas de bloques.

» Cadenas de bloques públicas: las cadenas de bloques públicas, como Bitcoin, son grandes redes distribuidas que se ejecutan a través de una criptomoneda nativa. Una criptomoneda es un dato único que se puede intercambiar entre dos partes. Las cadenas de bloques públicas están abiertas para que cualquier persona participe en cualquier nivel y, por lo general, tienen un código fuente abierto que mantiene su comunidad.

» Cadenas de bloques autorizadas: cadenas de bloques autorizadas, como Ripple, roles de control que los individuos pueden jugar dentro de la red. Todavía son sistemas grandes y distribuidos que usan un token nativo. Su código central puede o no ser de código abierto.

» Cadenas de bloques privadas: las cadenas de bloques privadas, también conocidas como tecnología de contabilidad distribuida (DLT), tienden a ser más pequeñas y no utilizan tokens ni criptomonedas. Su membresía está estrechamente controlada. Estos tipos de cadenas de bloques son favorecidos por consorcios que tienen miembros de confianza y comercio con dencial. información.

Los tres tipos de cadenas de bloques usan criptografía para permitir que cada participante en cualquier red administre el libro mayor de manera segura sin la necesidad de una central autoridad para hacer cumplir las normas. La eliminación de la autoridad central de la base de datos. La estructura es uno de los aspectos más importantes y poderosos de las cadenas de bloques.

Todos los tipos de cadenas de bloques están contribuyendo a lo que se conoce como Web3, también conocida como Web 3.0. Es tanto un movimiento social como una nueva evolución del mundo. Banda ancha. La idea general detrás de esta tendencia es que las personas se apropian de sus propios datos mediante el uso de herramientas que les brindan la descentralización, las tecnologías de cadena de bloques y la economía basada en tokens. A diferencia de la Web 2.0, donde los datos y el contenido está controlado por un pequeño grupo de megaempresas como Apple, Google y Facebook.


REMEMBER

Las cadenas de bloques crean registros permanentes e historiales de transacciones, pero nada es realmente permanente. La permanencia del registro se basa en la confiabilidad y el estado de la red. En el contexto de las cadenas de bloques, esto significa que si una gran parte de la comunidad de cadenas de bloques quisiera cambiar la información escrita en su cadena de bloques, podría hacerlo. La criptomoneda se usa como recompensa para incentivar lotes de usuarios para facilitar el sano funcionamiento de la red a través de la competencia. Si los registros se modifican de manera inapropiada, esto se conoce como un ataque del 51 por ciento.

Las redes pequeñas con pocos menores independientes son vulnerables porque no
tomar mucho esfuerzo para cambiar su información, y los mineros poderosos podrían hacerlo
y gana criptomonedas extra. Ethereum experimentó este tipo de ataque.

Cuando los datos se registran en una cadena de bloques, es extremadamente difícil cambiarlos o eliminarlos.
él. Cuando alguien quiere agregar un registro a una cadena de bloques, también llamada transacción
o una entrada, los usuarios de la red que tienen control de validación verifican la propuesta
transacción. Aquí es donde las cosas se complican porque cada cadena de bloques tiene un
diferentes giros sobre cómo funciona esto y quién puede validar las transacciones.

Qué hacen las cadenas de bloques

Una cadena de bloques es un sistema de igual a igual sin una autoridad central que gestione el flujo de
datos. Una de las formas clave de eliminar el control central mientras se mantienen los datos
integridad es tener una gran red distribuida de usuarios independientes. Esto significa
que los equipos que componen la red se encuentran en más de una ubicación. Estas computadoras a
menudo se denominan nodos completos.

La Figura 1-1 muestra una visualización de la estructura de la red blockchain de Bitcoin. Puede verlo en
acción en http://dailyblockchain.github.io.

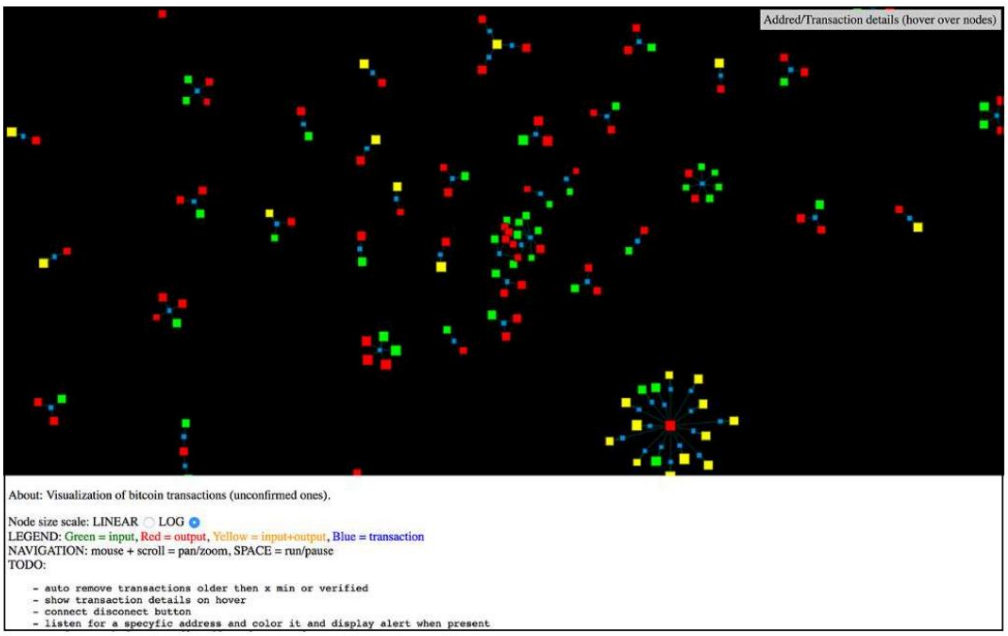


FIGURA 1-1: La estructura del Bitcoin cadena de bloques red.

Para evitar que la red se corrompa, no solo se descentralizan las cadenas de bloques, sino que a menudo
también utilizan una criptomoneda. Las redes Blockchain producen criptomonedas como incentivo para
mantener la integridad de la red. Muchos
Las criptomonedas se negocian en bolsas como las acciones.

Las criptomonedas funcionan un poco diferente en cada cadena de bloques. Básicamente, el software le paga al hardware para que opere. El software es el protocolo blockchain. Los protocolos de cadena de bloques bien conocidos incluyen Bitcoin, Ethereum, Ripple, Cardano, Solana y Polkadot. El hardware consta de los nodos completos que protegen los datos en la red.

Por qué importan las cadenas de bloques

Las cadenas de bloques se reconocen como la "quinta evolución" de la informática porque son una nueva capa de confianza para Internet. El espacio blockchain ha madurado significativamente desde su inicio alrededor de 2009. Ahora los usuarios individuales tienen acceso a niveles más altos de seguridad y autonomía.

Antes de las cadenas de bloques, las autoridades centrales establecían la confianza que emitía certificados. Un certificado con el que puede estar familiarizado es Secure Sockets Layer (SSL). Un certificado SSL es el “candado” que ves junto a una dirección en tu web navegador. Te permite saber que estás en un sitio web seguro. Los certificados SSL han demostrado para no ser infalible, sin embargo. Se han robado certificados de los dominios de la Agencia Central de Inteligencia (CIA), el Servicio Secreto de Inteligencia del Reino Unido (comúnmente conocido como MI6), Microsoft, Yahoo!, Skype, Facebook y Twitter. confiando en un tercero permite un único punto de falla, y los piratas informáticos tienen con frecuencia aprovechado esta vulnerabilidad.

Las cadenas de bloques, por otro lado, establecen la confianza de formas novedosas. Prueba de trabajo Las cadenas de bloques (POW) requieren que los mineros tengan un historial completo y preciso de sus transacciones para participar en la red. Las cadenas de bloques de prueba de participación (PoS, por sus siglas en inglés) crean confianza al requerir que los nodos que procesan transacciones "apuestan" algunas criptomoneda que se puede perder si se les descubre defraudando a la red.
Las cadenas de bloques privadas generan confianza mediante la distribución de datos a través de una red de participantes conectados pero independientes que se conocen entre sí y pueden rendir cuentas. Cada tipo de blockchain utiliza un sistema de incentivos diferente para establecer confiar en que cada participante de la red cooperará en mantener un historial completo e inalterado de cada transacción o entrada que se realice dentro de la base de datos que comparten.

Entonces, en resumen, las cadenas de bloques no tienen un solo punto de ataque; ellos distribuyen el misma fecha replicada a través de su red de nodos. Cada nodo se suma a la dificultad de manipular los datos de esa red, al menos en teoría.

Es muy importante tener en cuenta que las cadenas de bloques no son todas iguales en su distribución. de control y seguridad de datos. La evolución del robo de Internet se ha vuelto progresivamente más convencional. Más específicamente, juegos habilitados para blockchain y los tokens no fungibles (NFT) han generado miles de millones de dólares en ventas. ellos tambien empoderó a una nueva generación de creadores y creativos a nivel mundial.

La industria de la cadena de bloques también se ha rebautizado como Web 3.0. Este apodo se refiere a cómo las personas interactúan en línea y quién controla los activos y datos digitales. Como referencia, Web 1.0 era una experiencia de Internet más estática, donde las personas buscaban contenido y creó sitios web estáticos. Web 2.0 es la Internet interactiva a la que se accede a través de portales comerciales como Google, Facebook y Twitter. En la Web 2.0 Internet, los datos están controlados por entidades comerciales y la privacidad es rara para el individuo promedio usuarios

Web 3.0 es un movimiento social global que lucha contra las flagrantes violaciones de la privacidad y el fraude que se han vuelto omnipresentes en línea. También apela a el espíritu emprendedor y creativo de artistas y creadores. software web 3.0 permite a los usuarios interactuar entre sí a través de una identidad digital soberana que cada uno controles de usuario. Las credenciales digitales del usuario se autentican a través de su monedero digital (como MetaMask), una extensión del navegador, las claves privadas del usuario (ver Capítulo 3).

Una identidad controlada por el usuario permite a los usuarios individuales promedio controlar sus datos y privacidad Los usuarios también pueden poseer activos digitales, crear nuevos activos digitales y vender ellos directamente. Internet ha permitido el comercio digital durante mucho tiempo. Lo que hace que la Web 3.0 sea especial es la elegancia con la que permite a cualquier persona en cualquier parte del mundo que tenga acceso a un dispositivo inteligente e Internet crear y realizar transacciones. directamente con cualquier otra persona.

Los gobiernos globales han respondido fuertemente a la Web 3.0 y han actuado rápidamente para controlar la entrada y salida de una moneda en el espacio de la cadena de bloques, por ejemplo, requiriendo Anti-Lavado de Dinero (AML) y Conozca a su Cliente Verificación (KYC) sobre individuos que mueven más de $1,000 de valor de una billetera a otra.

Cuando los datos son permanentes y confiables en un formato digital, puede realizar transacciones comerciales en línea de formas que, en el pasado, solo eran posibles en línea. todo lo que tiene permanecido analógico, incluidos los derechos de propiedad y la identidad, ahora se puede crear y mantener en línea. Los procesos comerciales y bancarios lentos, como transferencias de dinero y liquidaciones de fondos, ahora se pueden realizar casi instantáneamente. Las implicaciones para los registros digitales seguros son enormes para la economía global.

Las cadenas de bloques son importantes porque permiten una nueva eficiencia y confiabilidad en el intercambio de información valiosa y privada que alguna vez requirió un tercero facilitar, como el movimiento de dinero y la autenticidad de la identidad. Este es un gran problema porque gran parte de nuestra sociedad y economía se ha estructurado en torno al establecimiento de la confianza, la aplicación de la confianza cuando se rompe y los terceros que facilitan la confianza. Puede imaginar cómo este software simple se puede utilizar en áreas tóxicas que han demostrado no ser infalibles, como la votación, la gestión de la cadena de suministro, el movimiento de dinero y el intercambio de bienes.

La estructura de las cadenas de bloques

Cada cadena de bloques está estructurada de forma ligeramente diferente. Sin embargo, Bitcoin es un gran blockchain para estudiar porque se usó como plantilla para la mayoría de las cadenas de bloques posteriores. Los datos de Bitcoin están estructurados de modo que cada nodo completo (las computadoras ejecutando la red) contiene todos los datos en la red. Este modelo es convincente desde el punto de vista de la persistencia de datos. Garantiza que los datos permanecerán intactos. incluso si algunos de los nodos se ven comprometidos. Sin embargo, debido a que cada nodo tiene una copia completa del historial de transacciones, desde el principio, y cada transacción en el futuro, requiere que las entradas sean lo más pequeñas posible de desde el punto de vista de la capacidad de almacenamiento.

Comparativamente, otras redes distribuidas de las que puede haber oído hablar como Napster y Pirate Bay son un índice de datos en línea. Individualles se comparten de specic nodos en la red. Esto permite compartir grandes cantidades. Sin embargo, debido a que los datos que le puede interesar no está disponible en todos los participantes de la red, obtener los datos que le interesan es problemático. También es difícil saber si los datos que está extrayendo están intactos y no se han dañado ni contienen información que no desea, como un virus.

La forma en que Bitcoin coordina la organización y el ingreso de nuevos datos comprende tres elementos centrales:

» Bloque: una lista de transacciones registradas en un libro mayor durante un período determinado. El tamaño, el período y el evento de activación de los bloques es diferente para cada cadena de bloques.

No todas las cadenas de bloques registran y aseguran un registro del movimiento de su criptomoneda como su objetivo principal. Pero todas las cadenas de bloques registran el movimiento de su criptomoneda o token. Piense en la transacción como simplemente el registro de datos. Asignarle un valor (como sucede en una transacción financiera) se usa para interpretar lo que significan esos datos.

» Cadena: un hash que vincula un bloque con otro, "encadenándolos" matemáticamente. Este es uno de los conceptos más difíciles de comprender en blockchain. También es la magia que une las cadenas de bloques y les permite crear confianza matemática.

El hash en blockchain se crea a partir de los datos que estaban en el bloque anterior. El hash es una huella digital de estos datos y bloquea los bloques en orden y tiempo.

Aunque las cadenas de bloques son una innovación relativamente nueva, el hashing no lo es. Hashing se inventó hace más de 70 años. Esta antigua innovación se utiliza porque crea una función unidireccional que no se puede descifrar. Una función hash crea un algoritmo matemático que asigna datos de cualquier tamaño a una cadena de bits de un tamaño fijo. Una cadena de bits suele tener 32 caracteres, lo que representa

los datos que fueron hash. El algoritmo hash seguro (SHA) es una de las funciones hash criptográficas que se utilizan en las cadenas de bloques. SHA-256 es un común algoritmo que genera un hash casi único de tamaño fijo de 256 bits (32 bytes). A efectos prácticos, piense en un hash como una huella digital de datos que se utilizado para bloquearlo en su lugar dentro de la cadena de bloques.

» Red: La red está compuesta por "nodos completos". Piense en ellos como la computadora que ejecuta un algoritmo que protege la red. Cada nodo contiene un registro completo de todas las transacciones que alguna vez se registraron en esa cadena de bloques.

Los nodos están ubicados en todo el mundo y pueden ser operados por cualquier persona. Es difícil, costoso y lleva mucho tiempo operar un nodo completo, por lo que la gente no lo hagas gratis. Están incentivados para operar un nodo porque quieren ganar criptomonedas. El algoritmo blockchain subyacente los recompensa por su servicio. La recompensa suele ser un token o una criptomoneda, como Bitcoin.


TIP

Los términos Bitcoin y blockchain a menudo se usan indistintamente, pero no lo son. lo mismo. Bitcoin tiene una cadena de bloques. La cadena de bloques de Bitcoin es el protocolo subyacente que permite la transferencia segura de Bitcoin. El término Bitcoin es el nombre de la criptomoneda que alimenta la red Bitcoin. La cadena de bloques es una clase de software y Bitcoin es una criptomoneda específica.

Aplicaciones de cadena de bloques

Las aplicaciones de cadena de bloques se basan en la idea de que su red de cadena de bloques y las reglas establecidas en las que se creó serán el árbitro de todas las transacciones y el guardián de toda la información. Este tipo de sistema es implacable y ciego. ambiente. El código de computadora se convierte en ley y las reglas se ejecutan como antes. escrito e interpretado por la red. Las computadoras no tienen las mismas redes sociales prejuicios y comportamientos como lo hacen los humanos.

La red no puede interpretar la intención (al menos no todavía). Los contratos de seguros arbitrados en una cadena de bloques se han investigado intensamente como un caso de uso construido en torno a esta idea.

Otra cosa interesante que permiten las cadenas de bloques es el mantenimiento de registros impecable. Se pueden utilizar para crear una línea de tiempo clara de quién hizo qué y cuándo. Muchos las industrias y los organismos reguladores pasan incontables horas tratando de evaluar este problema. El mantenimiento de registros habilitado por Blockchain aliviará algunas de las cargas que son creado cuando tratamos de interpretar el pasado.

El ciclo de vida de la cadena de bloques

Las cadenas de bloques se originaron con la creación de Bitcoin. Demostró que un grupo de personas que nunca se habían conocido podía operar en línea dentro de un sistema que era insensibilizado para engañar a otros que estaban cooperando en la red.

La red Bitcoin original fue construida para asegurar la criptomoneda Bitcoin. Al momento de escribir, tiene alrededor de 13,000 nodos completos que se distribuyen globalmente. Es principalmente para intercambiar Bitcoin y valor de intercambio, pero la comunidad vio el potencial de hacer mucho más con la red. Debido a su tamaño y seguridad comprobada, también se usa para asegurar otras cadenas de bloques y cadenas de bloques más pequeñas. aplicaciones

La red Ethereum es una segunda evolución del concepto blockchain. Se necesita la estructura tradicional de blockchain y agrega varios lenguajes de programación nuevos que se construyen en su interior. Al igual que Bitcoin, tiene más de 10 000 nodos completos y es globalmente repartido. Ethereum se utiliza principalmente para intercambiar Ether y crear contratos inteligentes. El contrato inteligente de Ethereum más popular es el ERC 20. Permite la generación de tokens intercambiables. Estos tokens se pueden utilizar para fines de recaudación de fondos. Puede descubrir más sobre los contratos inteligentes en el Capítulo 5.

Hay una tercera evolución en la tecnología de cadenas de bloques que se encuentra en desarrollo activo para abordar las limitaciones de velocidad y tamaño de los datos. La solución de estos problemas permitirá que la tecnología blockchain se utilice de manera más realista con las aplicaciones principales. Pasarán varios años antes de que quede claro qué estructura ganará.

Los nuevos desarrollos populares incluyen fragmentación, un tipo de partición de base de datos que separa grandes bases de datos en partes más pequeñas llamadas fragmentos de datos. Un esfuerzo de desarrollo de Ethereum llamado regla de elección de bifurcación divide la cadena de bloques de Ethereum en varios redes paralelas. Puede permitir que Ethereum escale de manera más eficiente y reduzca el congestión en la red, aumentando las velocidades de transacción y reduciendo los costos de transacción.

Otra teoría de escala popular se llama PoS. Cubro este tema con más detalle en Capítulo 8. En términos generales, PoS es el concepto de colocar tokens o criptomonedas como un fianza para el procesamiento de transacciones. Si el nodo está dañado y no procesa las transacciones con precisión, el nodo puede perder sus tokens o criptomonedas.

Un tercer esfuerzo para escalar la tecnología blockchain utiliza nodos confiables. Por ejemplo, Accumulate, la bifurcación dura de la red Factom, opera con nodos federados y un número ilimitado de nodos de auditoría. Se confía en estos nodos para garantizar el sistema. La red elegida de Accumulate es pequeña, poco más de 60 nodos. A cobertura de riesgos de seguridad, Accumule se ancla en otros

redes para aprovechar la seguridad de sistemas más extensos. Acumular también
divide su red en partes más pequeñas, más rápidas y más fáciles de administrar llamadas cadenas.
Accumulate tiene velocidades de transacción más rápidas y costos de transacción más bajos que las
cadenas de bloques POW, y no tiene los costos irrecuperables de las cadenas de bloques PoS.

Consenso: La fuerza impulsora de cadenas de bloques

Las cadenas de bloques son herramientas poderosas porque crean sistemas honestos que se corrigen a sí mismos sin la necesidad de que un tercero haga cumplir las reglas. Logran la aplicación de las reglas a través de su algoritmo de consenso.

En el mundo blockchain, el consenso es el proceso de desarrollar un acuerdo
entre un grupo de accionistas comúnmente desconfiados. Estos son los nodos completos en la red. Los
nodos completos están validando las transacciones que se ingresan
la red que se registrará como parte del libro mayor.

La figura 1-2 muestra el concepto de cómo se ponen de acuerdo las cadenas de bloques.

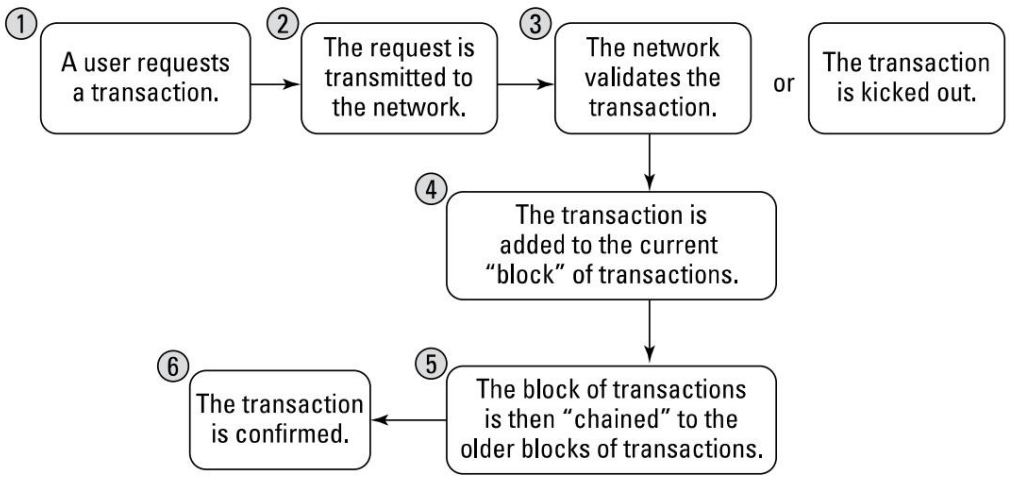


FIGURA 1-2:
Cómo funcionan las cadenas de bloques.

Cada cadena de bloques tiene sus propios algoritmos para crear un acuerdo dentro de su red sobre las entradas que se agregan. Hay muchos modelos diferentes para crear consenso porque cada cadena de bloques crea diferentes tipos de entradas. Algunas cadenas de bloques intercambian valor, otras almacenan datos y otras protegen los sistemas.
y contratos.

Bitcoin, por ejemplo, está negociando el valor de su token entre miembros en su
red. Los tokens tienen un valor de mercado, por lo que los requisitos relacionados con el rendimiento, la escalabilidad, la consistencia, el modelo de amenaza y el modelo de falla serán más altos.
Bitcoin opera bajo el supuesto de que un atacante malicioso puede querer corromper el historial de transacciones para robar tokens. Bitcoin evita que esto suceda
sucediendo mediante el uso de un modelo de consenso llamado "prueba de trabajo" que resuelve el El problema del general bizantino: “¿Cómo sabes que la información que estás
mirando no ha sido cambiado interna o externamente? Porque cambiar o
la manipulación de datos casi siempre es posible, la fiabilidad de los datos es un gran problema para la informática.

La mayoría de las cadenas de bloques operan bajo la premisa de que serán atacadas por agentes externos. fuerzas o por los usuarios del sistema. La amenaza esperada y el grado de confianza que la red tiene en los nodos que operan la cadena de bloques determinarán el tipo de algoritmo de consenso que utilizan para liquidar su libro mayor. Por ejemplo, Bitcoin tiene un alto grado de amenaza y utiliza un fuerte algoritmo de consenso llamado prueba de trabajo. No hay confianza en la red.

En el otro extremo del espectro, las cadenas de bloques que se utilizan para registrar
las transacciones entre partes conocidas pueden utilizar un consenso más ligero y rápido. Su necesidad de transacciones de alta velocidad es más importante. La prueba de trabajo es demasiado lenta y costosa para que operen debido a los relativamente pocos participantes dentro
la red y la necesidad de inmediatez de cada transacción. ellos tampoco
necesita un token o criptomoneda para incentivar el procesamiento de transacciones. Entonces ellos elimine estas cosas de su sistema y funcione más rápido y más barato que los sistemas POW.

Cadenas de bloques en uso

Actualmente hay miles de cadenas de bloques y aplicaciones basadas en cadenas de bloques en uso en todo el mundo. Estos sistemas permiten la creación de tokens no fungibles (NFT), el uso de criptomonedas en los juegos, un movimiento de dinero más rápido.
a través de redes distribuidas, y el desarrollo de redes seguras y confiables
aplicaciones y hardware. El interés mundial por estas tecnologías continúa creciendo a medida que las personas descubren los numerosos beneficios y posibilidades que ofrecen.

Puede ver muchas de estas cadenas de bloques públicas yendo a un intercambio de criptomonedas.

La Figura 1-3 muestra el intercambio de altcoin para Poloniex (https://poloniex.com), un
plataforma de comercio de criptomonedas.

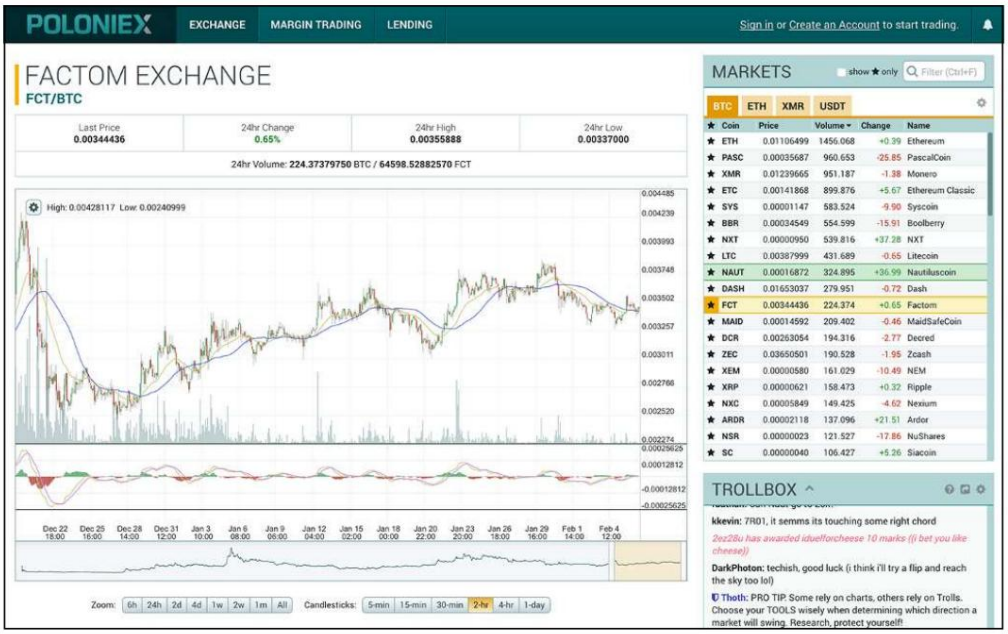


FIGURA 1-3: El intercambio de altcoins plataforma.

Las cadenas de bloques se están moviendo más allá del mercado de valor comercial y se están incorporando a todo tipo de industrias. Las cadenas de bloques agregan una nueva capa de confianza que ahora hace que el trabajo en línea sea seguro de una manera que antes no era posible.

Usos actuales de blockchain

Las aplicaciones Therst blockchain giran en torno a mover dinero u otras formas de valor de forma rápida y barata. Esto incluye negociar acciones de empresas públicas, pagar empleados en otros países, y cambiar una moneda por otra. Las cadenas de bloques ahora también se utilizan como parte de una pila de seguridad de software. El Departamento de Seguridad Nacional de EE. UU. ha estado investigando un software de cadena de bloques que protege los dispositivos de Internet de las cosas (IoT) y la integridad de la cadena de suministro. El mundo IoT tiene algo de lo que más se puede beneficiar de esta innovación, porque es especialmente vulnerable a los ataques de cucharita y otras formas de piratería. Los dispositivos IoT también se han vuelto más omnipresente, y la seguridad se ha vuelto más dependiente de ellos. Los sistemas hospitalarios, los automóviles autónomos y los sistemas de seguridad son buenos ejemplos.

Las ofertas iniciales de monedas (ICO, por sus siglas en inglés) son otra innovación emocionante de blockchain. son un tipo de contrato inteligente que permite al emisor ofrecer un token a cambio de fondos de inversión. Usado a menudo como una opción de recaudación de fondos no dilutiva, los empresarios a nivel mundial han recaudado miles de millones de dólares. Los gobiernos y los reguladores han sido rápido para tomar medidas enérgicas contra las ICO. Los tokens pueden ser valores sin licencia, y el la oferta puede estar defraudando a los inversores. La tecnología es impresionante incluso si todavía se están abordando los problemas de cumplimiento.

Una de las fantásticas innovaciones inherentes a los tokens de ICO es que son un instrumento de compensación y liquidación automática. En nuestro sistema actual de negociación de valores, existen dos tipos de agencias de compensación: sociedades de compensación y depositarios. Las sociedades de compensación auditan las transacciones y actúan como intermediarios en la realización de liquidaciones. Los depositarios tienen certificados de valores y mantienen registros de propiedad de los valores. Las cadenas de bloques realizan ambas funciones para tokens sin necesidad de que terceros auditen y retengan la posesión de los activos.

Puede obtener más información sobre los tokens de ICO en el Capítulo 15.

Los NFT y los juegos criptográficos de jugar para ganar también han inyectado miles de millones de dólares en el industria y empoderó a los usuarios promedio con la capacidad de crear y vender sus propios recursos digitales. Las redes sociales, la navegación web y la comunicación segura habilitada por blockchain también se están volviendo más populares cada año. Asimismo, los gobiernos (incluyendo la República Centroafricana y El Salvador) están adoptando Bitcoin como su moneda de curso legal.

Futuras aplicaciones de blockchain

La revolución de la cadena de bloques se ha extendido por Internet y está transformando rápidamente las experiencias digitales de la antigua Web 2.0 en otras más controladas por El usuario final. La humanidad está experimentando la última etapa de la globalización. este es un mundo donde la mano de obra basada en lo digital se está convirtiendo en mercancía y se iguala en precio. Un contador en Nueva York algún día costará lo mismo que un contador equivalente que vive en New Kingston o Nueva Delhi.

Las aplicaciones de Blockchain se volverán perfectas en la vida de miles de millones de personas porque funcionará como identidad y dinero y habilitará datos confiables en todas las aplicaciones.

Las posibilidades de un futuro infundido con blockchain han excitado la imaginación de empresarios, gobiernos, grupos políticos y humanitarios en todo el mundo. Países como el Reino Unido, Singapur y los Emiratos Árabes Unidos lo ven como una forma de reducir costos, crear nuevos instrumentos financieros y mantener registros limpios. Ellos tener inversiones e iniciativas activas que exploren blockchain.

Las cadenas de bloques han sentado las bases de las que se ha eliminado la necesidad de confianza la ecuacion. Donde antes pedir "confianza" era un gran problema, con blockchains es pequeño. Además, la infraestructura que hace cumplir la regla si se rompe esa confianza puede ser más ligera. Gran parte de la sociedad se basa en la confianza y el cumplimiento de las normas. lo social y Las implicaciones económicas de las aplicaciones de la cadena de bloques pueden ser emocional y políticamente polarizantes porque la cadena de bloques cambiará la forma en que estructuramos la información basada en valores y transacciones de base social.

EN ESTE CAPÍTULO

» Descubrir la cadena de bloques adecuada para sus necesidades

» Hacer un plan para su proyecto

» Descubriendo obstáculos para su proyecto

» Construyendo una hoja de ruta del proyecto

Capitulo 2

Elegir una cadena de bloques

La industria de la cadena de bloques es complejo y está creciendo en tamaño y capacidades cada día. Cuando comprenda los tres tipos básicos de cadenas de bloques y sus limitaciones, sabrá lo que es posible con esta nueva tecnología.

Este capítulo trata sobre la evaluación de la tecnología blockchain y el desarrollo de un plan de proyecto. Pone en contexto los siguientes capítulos sobre plataformas y aplicaciones blockchain individuales.

Aquí, verá cómo evaluar los tres tipos diferentes de plataformas de cadena de bloques, qué se está construyendo en cada tipo, y por qué. Te doy algunas herramientas que te ayudan a delinear tu proyecto, predecir obstáculos y superar desafíos.

Donde Blockchains agrega sustancia

Hay mucho revuelo en torno a las cadenas de bloques y las criptomonedas que las ejecutan. Parte de este rumor se debe a la fluctuación en el valor de las criptomonedas y al temor de que la tecnología blockchain interrumpa muchas funciones de la industria y el gobierno. Se ha invertido mucho dinero en investigación y desarrollo porque las partes interesadas no quieren quedarse obsoletas y los empresarios quieren explorar nuevos modelos de negocio.

Cuando se trata de encontrar una oportunidad para que la tecnología blockchain agregue valor a una organización, a menudo surge la pregunta: "¿Dónde agregan valor las cadenas de bloques y en qué se diferencian de las tecnologías existentes?"

Las cadenas de bloques son un tipo especial de base de datos. Una base de datos es una colección de datos que se organizan de una manera específica y se almacenan electrónicamente. Las bases de datos están diseñadas para almacene, recupere y administre grandes cantidades de datos de manera rápida y eficiente. Ellos son comúnmente utilizado para almacenar datos estructurados (datos que siguen un formato específico y son organizados de una manera específica) y son ampliamente utilizados en una variedad de aplicaciones, incluidos los sistemas financieros, los sistemas de gestión de las relaciones con los clientes y sitios web de compras en línea.

Una cadena de bloques es como una base de datos en el sentido de que es un sistema de mantenimiento de registros digitales que almacena datos de manera estructurada. Una diferencia clave es que una cadena de bloques es una base de datos distribuida: no se almacena en una sola ubicación, sino que se distribuye en una red de computadoras o nodos. La mayoría de las cadenas de bloques requieren nodos completos en la red y tienen una copia de la cadena de bloques completa, y cuando se agrega una nueva pieza de datos a la cadena de bloques, se agrega a todas las copias de la cadena de bloques en la red.
Esta estructura descentralizada dificulta que una sola entidad altere la datos en la cadena de bloques, porque cualquier cambio tendría que hacerse simultáneamente en todas las copias de la cadena de bloques.

Una vez que se han agregado datos a la cadena de bloques, en términos generales, no se pueden modificar ni eliminar. Esto convierte a la cadena de bloques en un sistema de mantenimiento de registros seguro y confiable, ya que garantiza la integridad y autenticidad de los datos almacenados en ella.
Algunas cadenas de bloques han implementado sistemas para eliminar datos a menos que pague para mantenerlos informados, pero esta no es la norma.

Por el contrario, las bases de datos tradicionales a menudo están centralizadas y pueden ser modificadas o manipuladas más fácilmente por una sola entidad con acceso a la base de datos. También son menos seguros, porque pueden ser vulnerables a la piratería y las filtraciones de datos. Al considerar los usos de las cadenas de bloques, es importante tener en cuenta que puede utilizar una cadena de bloques en cualquier lugar donde usaría una base de datos normal, pero es posible que no lo haga.
tiene sentido pasar por el problema y el gasto de usar una cadena de bloques cuando una base de datos normal puede hacer el trabajo. Una cadena de bloques es una base de datos intencionalmente ineficiente que se distribuye a través de la web.

Realmente ve valor en el uso de alguna forma de cadena de bloques cuando desea compartir información con partes en las que no confía completamente, sus datos deben auditarse o sus datos corren el riesgo de verse comprometidos interna o externamente. La mayoría de las cadenas de bloques publican un registro público de sí mismas. Incluso si los datos se han cifrado, es posible que no sean privados en el futuro cuando la computación cuántica se vuelva

más barato y más fácilmente disponible. Ninguna de estas preguntas es simple, y las soluciones correctas pueden ser difíciles de determinar.

Esta sección ayuda a reducir sus opciones.

Determinando sus necesidades

Las cadenas de bloques vienen en muchos favores. Encontrará uno que se adapte a sus necesidades: el truco es encontrarlo! Asignar sus necesidades a la mejor cadena de bloques puede ser abrumador. Siempre que tengo muchas opciones y, a menudo, necesidades contradictorias, me gusta utilizar una matriz de decisión ponderada.

Una matriz de decisión ponderada es una excelente herramienta para evaluar las necesidades de un proyecto y luego mapear esas necesidades en posibles soluciones. La ventaja clave de la matriz es ayudarlo a cuantificar y priorizar las necesidades individuales de su proyecto y simplificar la toma de decisiones. Las matrices de decisión ponderadas también evitan que se sienta abrumado por los criterios individuales. Si se hace correctamente, esta herramienta le permite converger en una sola idea que es compatible con todos sus objetivos.

Para crear una matriz de decisión ponderada, siga estos pasos:

1. Haga una lluvia de ideas sobre los criterios u objetivos clave que su equipo debe cumplir.


TIP

Si no está seguro de los criterios que debe considerar al evaluar su proyecto de cadena de bloques, aquí hay algunas cosas que debe tener en cuenta:

- Escala y volumen
- Velocidad y latencia
- Seguridad e inmutabilidad
- Capacidad de almacenamiento y necesidades estructurales

Su equipo tendrá su propia lista de objetos y prioridades. Estos son solo algunos a considerar al evaluar la plataforma correcta para satisfacer sus necesidades.

2. Reducir la lista de criterios a no más de diez elementos.


TIP

Si tiene dificultades para refinar su lista de necesidades, considere usar un herramienta de matriz de comparación.

3. Cree una tabla en Microsoft Excel o un programa similar.
4. Introduzca los criterios de diseño en la primera columna.

5. Asigne un peso relativo a cada criterio en función de la importancia que
objetivo es el éxito del proyecto.

Limite el número de puntos a 10 y distribúyalos entre todos sus criterios, por ejemplo, 1
= prioridad baja, 2 = media y 3 = prioridad alta.


TIP

Si está trabajando en un equipo, haga que cada miembro pondere los criterios por separado.

6. Sume los números para cada objetivo y divida por el número de equipo
miembros para un peso de equipo compuesto.

7. Realice cualquier ajuste necesario a los pesos para asegurarse de que cada criterio sea
ponderado correctamente.

¡Felicidades! Ahora tiene una lista clasificada de criterios que debe cumplir para tener éxito con su proyecto de cadena de bloques.

De nir tu meta

Puede perderse fácilmente construyendo un proyecto de cadena de bloques que no tiene un objetivo o propósito claro. Tómese el tiempo para entender a dónde les gustaría ir usted y su equipo y cuál es el objetivo final. Por ejemplo, un objetivo podría ser negociar un activo con un empresa colaboradora sin intermediario. Este es un gran objetivo con muchas partes interesadas.

Vuelva a construir un proyecto pequeño que sea un caso de uso viable mínimo para la tecnología que articule claramente el valor agregado o los ahorros para su empresa. En la misma línea que el ejemplo anterior, un objetivo más pequeño sería construir una red privada que pueda intercambiar valor entre partes confiables.

Luego construya sobre ese valor. La próxima victoria podría ser construir un instrumento que sea negociable en su nueva plataforma. Cada paso debe demostrar una pequeña ganancia y valor creado.

Elegir una solución

Hay tres tipos básicos de cadenas de bloques: redes públicas como Bitcoin, redes autorizadas como Ripple y privadas como R3.

Las cadenas de bloques hacen algunas cosas sencillas:

» Mueven valor y comercializan valor rápidamente ya un costo muy bajo.

» Crean historiales de datos casi permanentes.

La tecnología Blockchain también permite algunas soluciones menos sencillas, como la capacidad de demostrar que tiene una "cosa" sin revelarla al otro.
fiesta. También es posible “probar lo negativo”, o probar lo que falta dentro
un conjunto de datos o sistema. Esta característica es particularmente útil para auditar y probar el cumplimiento.

La Tabla 2-1 enumera los casos de usos comunes que son adecuados para cada tipo de cadena de bloques.

TABLA 2-1 Usos públicos versus privados de Blockchain

Propósito primario	Tipo de cadena de bloques
Mover valor entre partes no confiables	Público
Mover valor entre partes de confianza	Privado
Valor comercial entre cosas diferentes	autorizado
Valor comercial de la misma cosa	Público
Crear una organización descentralizada	Público o autorizado
Crear contrato descentralizado	Público o autorizado
Comercio de activos titulizados	Público o autorizado
Construir identidad para personas o cosas.	Público
Publicar para mantenimiento de registros públicos	Público
Publicar para mantenimiento de registros privados	Público o autorizado
Auditoría de preformas de registros o sistemas	Público o autorizado
Publicar datos de títulos de propiedad	Público
Comercia con dinero o activos digitales	Público o autorizado
Crear sistemas para la seguridad de Internet de las cosas (IoT)	Público
Seguridad de los sistemas de construcción	Público

Puede haber excepciones según su proyecto, y es posible utilizar un tipo diferente de cadena de bloques para alcanzar su objetivo. Pero, en general, aquí se explica cómo desglosar diferentes tipos de redes y comprender sus fortalezas y
debilidades:

» Las redes públicas son grandes y descentralizadas, cualquiera puede participar en ellas en cualquier nivel; esto incluye cosas como ejecutar un nodo completo, minería criptomoneda, fichas comerciales o entradas de publicación. Suelen ser más

seguras e inmutables que las redes privadas o autorizadas. Suelen ser más lentos y más caros de usar. Están protegidos con una criptomoneda y tienen una capacidad de almacenamiento limitada.

» Las redes autorizadas son visibles para el público, pero la participación es revisado. Muchos de ellos utilizan una criptomoneda, pero pueden tener un costo menor para las aplicaciones que se construyen sobre ellos. Esta característica facilita la escala del proyecto y aumenta el volumen de transacciones. Las redes autorizadas pueden ser muy rápidas con baja latencia y tener mayor capacidad de almacenamiento que las redes públicas.

» Las redes privadas se comparten entre partes de confianza y es posible que no se visible al público. Son muy rápidos y pueden no tener latencia. También tienen un bajo costo de funcionamiento y se pueden construir en un fin de semana laborioso. La mayoría de las redes privadas no utilizan una criptomoneda y no tienen la misma inmutabilidad y seguridad de las redes descentralizadas. La capacidad de almacenamiento puede ser ilimitada.

También existen híbridos entre estos tres tipos principales de cadenas de bloques que buscan encontrar el equilibrio adecuado entre seguridad, auditabilidad, escalabilidad y almacenamiento de datos para aplicaciones construidas sobre ellos.

Dibujar un árbol de decisión de blockchain

Algunas de las decisiones a las que se enfrenta mientras trabaja en un proyecto de cadena de bloques dentro de su organización pueden ser difíciles y desafiantes. Vale la pena tomarse el tiempo para tomar decisiones que involucren

» Incertidumbre: muchos de los hechos en torno a la tecnología blockchain pueden ser desconocido y no probado.

» Complejidad: Las cadenas de bloques tienen muchos factores interrelacionados a considerar.

» Consecuencias de alto riesgo: El impacto de la decisión puede ser signi cativo para tu organización.

» Alternativas: puede haber tecnologías y tipos de cadenas de bloques alternativos, cada uno con su propio conjunto de incertidumbres y consecuencias.

» Problemas interpersonales: debe comprender cómo la tecnología blockchain podría afectar a diferentes personas dentro de su organización.

Un árbol de decisiones es una herramienta de apoyo útil que lo ayudará a descubrir las consecuencias, los resultados de los eventos, los costos de los recursos y la utilidad de desarrollar un proyecto de cadena de bloques.

Puede dibujar árboles de decisión en papel o utilizar una aplicación informática. Estos son los pasos para crear uno para descubrir otros desafíos en torno a su proyecto:


TIP

1. Obtenga una hoja grande de papel.

   Cuantas más opciones haya y más complicada sea la decisión, más grande será la hoja de papel que necesitará.

2. Dibuja un cuadrado en el lado izquierdo del papel.
3. Escriba una descripción de la meta central y los criterios para su proyecto en ese cuadrado.
4. Dibuja líneas a la derecha del cuadrado para cada problema.
5. Escriba una descripción de cada problema a lo largo de cada línea.


TIP

   Asigne un valor de probabilidad para encontrar cada problema.

6. Piense en soluciones para cada problema.
7. Escribe una descripción de cada solución a lo largo de cada línea.
8. Continúe con este proceso hasta que haya explorado cada tema y descubierto un posible solución para cada uno.

Haga que sus compañeros de equipo desafíen y revisen todos sus problemas y soluciones antes de analizarlos.

haciendo un plan

En este punto, debe tener una comprensión clara de sus objetivos, obstáculos y qué opciones de blockchain tiene disponibles.

Aquí hay una hoja de ruta simple para construir su proyecto:

1. Explique el proyecto a las partes interesadas clave y discuta sus componentes clave y resultados previstos.
2. Escriba un plan de proyecto.

   Este es un conjunto vivo de documentos que cambiará a lo largo de la vida de su proyecto.

3. Desarrollar las medidas de desempeño, declaración de alcance, cronograma, y líneas de base de costos.
4. Considere la posibilidad de crear un plan de gestión de riesgos y un plan stang.
5. Consiga aceptación y defina funciones y responsabilidades.

6. Organiza una reunión de kickom para comenzar el proyecto.

La reunión debe cubrir lo siguiente:

- Visión para el proyecto
- Estrategia del proyecto
- Cronograma del proyecto
- Funciones y responsabilidades
- Actividades de trabajo en equipo
- Compromisos del equipo
- Cómo tomará decisiones su equipo
- Métricas clave con las que se medirá el proyecto


REMEMBER

Después de completar su proyecto, ¡no habrá terminado! Regrese y analice sus éxitos y fracasos. Aquí hay algunas preguntas que debe hacerse:

» ¿ Están contentos mis principales interesados?

» ¿ Se mantuvo el proyecto dentro del cronograma?

» Si no, ¿qué causó que se retrasara?

» ¿ Qué aprendí de este proyecto?

» ¿ Qué desearía haber hecho diferente?

» ¿ Realmente creé valor nuevo para mi empresa o ahorré dinero?


TIP

Es posible que desee volver a este capítulo cuando tenga un conocimiento más profundo de la tecnología blockchain y esté desarrollando un plan para construir un proyecto.

EN ESTE CAPÍTULO

Capítulo 3

Poner tus manos en Blockchain

Las blockchains son herramientas muy poderosas y están cambiando la forma en que se mueve el mundo dinero, protege los sistemas y crea identidades digitales. Si no es un desarrollador principal, es probable que no realice ningún desarrollo de cadena de bloques en profundidad. ment en un futuro próximo. Dicho esto, aún debe comprender cómo funcionan las cadenas de bloques y cuáles son sus limitaciones principales, ya que se integrarán en muchas interacciones diarias en línea en un futuro cercano, desde cómo las empresas pagan a las personas a cómo los gobiernos saben que sus sistemas y datos están intactos y seguros.

En este capítulo, se sumerge directamente en la tecnología blockchain. tu compras el primero criptomoneda y aprende a cambiarla por otras monedas. Configura aplicaciones especiales que le darán acceso a todo un ecosistema de aplicaciones descentralizadas (conocidas como dApps). También configura un entorno seguro para usar su criptomoneda. En este capítulo, también creará y arrendará activos digitales de cadena de bloques a través de un juego de cadena de bloques.

Después de trabajar en este capítulo, comprenderá muchas de las funcionalidades básicas que ofrece la tecnología blockchain. También tendrá una comprensión básica de algunas de las medidas de seguridad adicionales que debe tener mientras trabaja con criptomonedas. Este capítulo también lo ayuda a establecer las cuentas criptográficas básicas que necesitará en capítulos posteriores.

Sumergirse en la tecnología Blockchain

La cadena de bloques Ethereum es una de las cadenas de bloques más grandes y poderosas del mundo. Fue diseñado para construir dApps, que son aplicaciones que se construyen dentro de una red descentralizada sin confianza. Dentro de la red Ethereum, los desarrolladores utilizan contratos inteligentes para construir estas aplicaciones. Ethereum también utiliza una criptomoneda llamada Ether para recompensar a los usuarios por proporcionar potencia informática y crear el sistema sin confianza que estos contratos inteligentes necesitan ejecutar.

Los contratos inteligentes no son realmente como un contrato que puede haber visto para una empresa. En cambio, los contratos inteligentes son códigos desplegados a través de una red descentralizada. Como un contrato comercial, tienen términos predeterminados. Una diferencia clave es que los contratos inteligentes son aplicados por su red blockchain. Son una innovación informática importante porque permiten que las personas que no se conocen o no confían entre sí colaboren sin temor a que la otra parte no se desempeñe según lo estipulado en los términos acordados por las dos partes.


TIP

Las cadenas de bloques que utilizan una criptomoneda a veces se pueden llamar sistemas "sin confianza" porque la red hace cumplir el código (a diferencia de un contrato comercial, que es ejecutado por un sistema judicial).

En las siguientes secciones, configurará cuentas para comprar su primer Bitcoin. Tú también intercambie algunos de los Bitcoin que compra por Ether para que pueda utilizar Ethereum dApps en las siguientes secciones.

Crear un entorno seguro

Lo primero que debe hacer es crear un entorno seguro para trabajar en línea. Allá hay un número creciente de razones para pensar en usar un navegador seguro y una red privada virtual (VPN). Evitan que sus datos se recopilen sin su consentimiento y ayudan a evitar los piratas informáticos. Los piratas informáticos pueden atacar al usuario promedio cuando usa criptomonedas y una conexión a Internet no segura.

En esta sección, descarga el navegador web Brave, ProtonVPN y una extensión de navegador MetaMask. Puede utilizar estos tres servicios sin pagar. Sin embargo, también ofrecen un servicio mejorado por una tarifa.


TIP

Prepara una hoja de papel y un bolígrafo para anotar la información importante. Nunca tome una captura de pantalla o foto de cosas como contraseñas o frases iniciales.

Descarga e instalación del navegador Brave

Brave es un nuevo navegador web seguro basado en Google Chromium que es rápido, de código abierto y centrado en la privacidad. Bloquea anuncios, rastreadores y tiene una función que le permite recompensar a los editores que le gustan con tokens. El pionero de Internet Brendan Eich creó Brave; inventó JavaScript y también cofundó Mozilla.

Para descargar el navegador web Brave, sigue estos pasos:

1. Vaya a https://brave.com.
2. Haga clic en Descargar Brave.
3. Ve a tu carpeta de descargas.
4. Haga doble clic en el navegador Brave.
5. Arrastre y suelte el nuevo ícono del navegador Brave en su carpeta de aplicaciones.

Ahora que tiene un navegador web más seguro, puede agregarle la extensión blockchain que le permite explorar aplicaciones descentralizadas.

El navegador Brave es un gran navegador por sí solo, pero si desea mejorar su seguridad, puede usar el navegador Brave Tor. Tor (abreviatura de The Onion Router) es un software gratuito y de código abierto para la comunicación anónima y la navegación web. Dirige el tráfico de Internet a través de una red superpuesta de voluntarios en todo el mundo que le ayuda a ocultar su ubicación y uso de cualquier persona que realice vigilancia de red o análisis de tráfico. Esto puede parecer una exageración, pero crypto
los usuarios son el blanco de naciones deshonestas y grupos terroristas que quieren robar sus activos.

Con la conectividad Tor, obtiene dos beneficios adicionales: su dirección IP está oculta de los sitios que visita, y los sitios que visita están ocultos para los observadores pasivos de la red. Tenga en cuenta que Tor puede ralentizar la navegación o dañar algunos sitios web.


TIP

Para usar el navegador Brave Tor, seleccione Archivo Nueva ventana privada con Tor desde su navegador Brave.

Una ventana privada con Tor lo hace más difícil, pero no imposible, para su proveedor de servicios de Internet (ISP) para ver qué sitios visita. Sin embargo, una ventana privada con Tor no lo defenderá por completo contra el seguimiento, y puede considerar revisar Cybersecurity For Dummies, 2nd Edition, de Joseph Steinberg (Wiley) para obtener más información sobre cómo mantenerse seguro en línea.

Descarga e instalación de ProtonVPN

ProtonVPN es una VPN administrada por una empresa suiza. Cuando usa ProtonVPN para navegar por la web, su conexión a Internet está encriptada para que los posibles atacantes no puedan espiar su actividad. También le permite acceder a sitios web que pueden estar bloqueados.

Para descargar ProtonVPN, siga estos pasos:

1. Vaya a https://protonvpn.com.
2. Haga clic en Obtener ProtonVPN ahora.
3. Haga clic en Obtener gratis.
4. Introduzca su dirección de correo electrónico cuando se le solicite.

Para instalar ProtonVPN, siga estos pasos:

1. Vaya a su carpeta de descargas en Mac o PC.
2. Haga doble clic en ProtonVPNIe.
3. Arrastre y suelte el nuevo icono de ProtonVPN en su carpeta de aplicaciones.

Una VPN es una buena segunda capa de seguridad para ayudar a garantizar que su conexión sea segura. Para obtener más información sobre cómo puede protegerse a sí mismo y a sus dispositivos, consulte Cybersecurity For Dummies de Joseph Steinberg (Wiley).

Descarga, instalación y protección de MetaMask

MetaMask es una extensión del navegador que le permite ejecutar dApps de Ethereum directamente en su navegador sin ejecutar un nodo completo de Ethereum. (Ethereum es una de las cadenas de bloques más grandes del mundo; consulte el Capítulo 5 para obtener más información). metamáscara incluye una bóveda de identidad segura. Le permite iniciar sesión en sitios web, administrar sus identidades en la web y firmar transacciones de blockchain. También puede guardar algo de criptomoneda Ether en su billetera MetaMask para realizar pagos en línea.

Para descargar e instalar MetaMask, sigue estos pasos:

1. Abra el navegador web Brave.

   Consulte "Descarga e instalación del navegador Brave", anteriormente en este capítulo, si aún no lo ha instalado.

2. Vaya a https://metamask.io.
3. Haga clic en Descargar para Brave.
4. Haga clic en Agregar a Brave.

5. Haga clic en Agregar extensión dentro de la nueva ventana.

   Ahora debería ver un pequeño ícono de zorro en la esquina superior derecha de su navegador Brave.

Debido a que MetaMask es una billetera, también deberá asegurar y hacer una copia de seguridad de su billetera con una contraseña segura y asegurar su semilla de respaldo. Una semilla de respaldo le permite recuperar su billetera si pierde su contraseña.

Tome un bolígrafo y un cuaderno o una hoja de papel que pueda mantener en privado. Luego sigue estos pasos:

1. En la parte superior de su hoja de papel, escriba "MetaMask", "navegador Brave", el la fecha y el dispositivo en el que lo has descargado.
2. Abra el navegador web Brave.
3. Haga clic en el icono del zorro en la esquina superior derecha.
4. Haga clic en Continuar.
5. Cree una contraseña fuerte y única.
6. Escriba su nombre de usuario y contraseña.
7. Haga clic en Crear.

Obtenga otro cuaderno o una hoja de papel separada para esta próxima serie de pasos.
No uses el mismo cuaderno o hoja de papel en el que acabas de escribir tu nombre de usuario y contraseña. Asegúrese de guardar estos documentos en un lugar donde no puedan ser destruidos o encontrados. Muchas personas abren bóvedas bancarias o usan una caja fuerte para guardar sus frases y contraseñas de respaldo porque el acceso a una u otra es acceso a su criptografía.

1. En la parte superior de su hoja de papel, escriba "MetaMask", "navegador Brave", el fecha, el dispositivo en el que descargó Brave y "Frase inicial".
2. Abra el navegador web Brave.
3. Haga clic en el icono del zorro en la esquina superior derecha.
4. Haga clic en Aceptar.
5. Haga clic en el icono de candado.
6. Escriba y numere la frase de 12 palabras.
7. Haga clic en Siguiente.
8. Reordena la frase semilla usando lo que escribiste.
9. Haga clic en Listo.


TIP

Considere plastificar los pedazos de papel con su nombre de usuario y contraseña y su semilla de respaldo. Y recuerda no guardar estas dos hojas de papel en el mismo lugar.

Compra tu primer Bitcoin

Hay varios lugares donde puede comprar su primer Bitcoin. si estas dentro
los Estados Unidos, experimentará cierta fricción al configurar una cuenta y vincularla a su tarjeta de crédito o cuenta bancaria. Puede tomar uno o dos días para que usted sea autenticado y se le permita comprar su primera criptomoneda. Todo virtual
Los proveedores de servicios de activos (VASP) deben realizar vericaciones contra el lavado de dinero (AML) y Conozca a su cliente (KYC) en los clientes que realizan transacciones de más de $1,000 debido a la nueva regla de viaje global (ver la barra lateral cercana).

Recomiendo usar uno de los siguientes sitios web si se encuentra dentro de los Estados Unidos Unidos y me gustaría comprar alguna criptomoneda por primera vez:

» Aplicación de efectivo: https://cash.app

» Coinbase: www.coinbase.com

» Géminis: https://gemini.com/

» Robinhood: https://robinhood.com

Vaya a uno de estos sitios u otro de su elección y configure una cuenta. Querrá comprar $ 10 a $ 20 en criptomonedas. Sugiero comprar monedas Bit. Es universalmente aceptado y comercializado por todas las demás criptomonedas. También puede tener la opción de comprar Ether, la criptomoneda Ethereum utilizada para ejecutar dApps. Si es así, continúe y compre un valor de $5 a $10 porque estará
usarlo en la siguiente sección. Si solo puede comprar Bitcoin, está bien. Podrá cambiarlo por Ether dentro de su billetera usando ShapeShift, un intercambio de criptomonedas de baja fricción.

Una nota importante para recordar es que la criptomoneda ha estado en la zona gris regulatoria. Al momento de escribir este libro, es posible comprar y retirar fondos de estas fuentes. Es posible que la compra y el retiro de criptomonedas no estén disponibles en el futuro o dentro de su país o región. Si ese es el caso, es posible que desee pasar al Capítulo 5. Allí, podrá minar en la red de prueba y
recibir prueba de éter.

LA NUEVA REGLA GLOBAL DE VIAJES

La regla de viaje global es un conjunto de pautas que requiere que los VASP, como Coinbase y Gemini, recopilen y transmitan cierta información al facilitar la transferencia de activos virtuales entre VASP o entre un VASP y un no VASP. El propósito de
La regla de viaje global es para ayudar a combatir el lavado de dinero y el terrorismo al proporcionar una forma para que las agencias de aplicación de la ley rastreen el movimiento de activos virtuales e identifiquen a las partes involucradas en las transacciones.

La regla de viaje global fue desarrollada por el Grupo de Acción Financiera Internacional (GAFI), una organización intergubernamental que establece estándares y mejores prácticas para combatir el lavado de dinero y el terrorismo. La regla de viaje global se aplica a una amplia gama de activos virtuales, incluidas las criptomonedas, y requiere que los VASP recopilen y transmitan la siguiente información al facilitar una transacción:

- El nombre y la dirección del originador
- El número de cuenta del originador o la dirección del activo virtual
- El nombre y la dirección del beneficiario
- El número de cuenta del beneficiario o la dirección del activo virtual
- El monto de la transacción
- La fecha y hora de la transacción

Los VASP están obligados a transmitir esta información al VASP receptor o no VASP, así como a retenerla durante un cierto período de tiempo para una posible investigación por parte de las agencias de aplicación de la ley.

Asegurar e intercambiar Tu Criptomoneda

Si pudo comprar Ether cuando configuró su cuenta, no dude en omitir esta sección. Aquí, configurará una billetera Jaxx para intercambiar el Bitcoin que compró por Ether utilizando el intercambio ShapeShift incorporado. La billetera Jaxx fue desarrollada por Anthony Di Iorio. Es uno de los primeros pioneros de blockchain y cofundador de Ethereum.

El dispositivo en el que descarga la billetera puede ser una computadora o un teléfono. Para este ejercicio, descargará la extensión de Chrome. Si elige descargar los otros tipos de billetera, no olvide que sus dispositivos pueden verse comprometidos.
La piratería común de criptomonedas se realiza a través de la ingeniería social, como una piratería de la tarjeta SIM. También puede perder sus activos porque tiene una conexión a Internet insegura. Jaxx se considera una billetera caliente porque está conectado a Internet, por lo que tiene algunas vulnerabilidades.


TIP

Hay algunas cosas que puede hacer para ayudar a mitigar sus riesgos:

» Usa tu VPN.

» Utilice el Autenticador de Google.

» Utilice un número de Google Voice.

» Mantenga un correo electrónico separado que use solo para cuentas de criptomonedas.

» Tenga un dispositivo que use solo en una conexión segura para su criptomoneda actividades.

» Nunca guarde ningún registro digital de sus contraseñas y semillas de recuperación.

Descargando Jaxx

En esta sección, descargará y configurará una billetera de criptomonedas. Hay muchos en el mercado que lo ayudan a proteger Bitcoin y otros activos que usa.
El Jaxx Liberty es una billetera fácil de usar que admite más de 80 diferentes CRIPTOMONEDAS. También funciona muy bien para iOS, Android, escritorio y también tiene una versión de Google Chrome. Siéntase libre de mirar otras opciones, también. Por ejemplo, Éxodo. io (www.exodus.io) también es otra billetera excelente y fácil de usar.

1. En su navegador Brave, vaya a https://jaxx.io.
2. Haga clic en Descargas.
3. Seleccione Agregar la extensión Jaxx Liberty de Google Chrome a su navegador.
4. Haga clic en Agregar a Chrome.
5. Haga clic en Agregar extensión en la ventana emergente.

Asegurando su billetera Jaxx

Ahora está listo para asegurar su billetera Jaxx. Necesitará al menos dos hojas de papel limpias para escribir su frase semilla y contraseña.


REMEMBER

No guarde su contraseña con su frase semilla.

Sigue estos pasos:

1. En la parte superior de una hoja de papel, escriba "Jaxx", "navegador valiente", la fecha, y el dispositivo en el que has descargado Jaxx.
2. Abra el navegador web Brave.
3. Haga clic en el icono del corazón en la esquina superior derecha.
4. Haga clic en Crear nueva cartera.
5. Haga clic en Acepto.
6. Haga clic en Continuar.
7. Haga clic en Hacer copia de seguridad ahora.
8. Seleccione Sí cuando vea la advertencia.
9. Haga clic en Iniciar copia de seguridad.
10. Escriba y numere su frase semilla.
11. Vuelva a escribir sus palabras en orden.
12. Haga clic en Confirmar.
13. Haga clic en Jaxx Liberty Home.


TIP

En la siguiente sección, asegurará una contraseña para su billetera Jaxx para su navegador Brave. No omita este paso: necesitará la contraseña más adelante para acceder a sus activos. Si tiene dificultades para abrir Jaxx, intente navegar a un sitio web de dApp como www.cryptokitties.co y vuelva a intentar los pasos anteriores.

Sigue estos pasos:

1. En la parte superior de la segunda hoja de papel, escriba "Jaxx", "Navegador valiente", el fecha y el dispositivo en el que ha descargado Jaxx.
2. Abra el navegador web Brave.
3. Haga clic en el icono del corazón en la esquina superior derecha.
4. Haga clic en el ícono de menú en su billetera Jaxx.
5. Haga clic en Contraseña de seguridad.
6. Seleccione Sí cuando vea la advertencia.
7. Haga clic en Establecer contraseña.
8. Escriba una contraseña única y segura en su hoja de papel.
9. Introduzca su contraseña dos veces y haga clic en Continuar.

REMEMBER

Guarde estos dos pedazos de papel en lugares separados. Es posible que desee laminarlos solo para estar seguro.

Transferencia de Bitcoin a Jaxx

En esta sección, agregará algunas criptomonedas de Bitcoin a su billetera Jaxx para su navegador Brave. Al momento de escribir este artículo, era posible comprar Bitcoin desde la billetera del navegador Jaxx Brave, por lo que puede considerar hacerlo en lugar de transferir activos de anillo desde un intercambio como Coinbase. Dicho esto, no se salte la compra de criptomonedas; las necesitará más adelante para comprar Ether para el ejercicio de CryptoKitties.

Sigue estos pasos:

1. Abra el navegador web Brave.
2. Haga clic en el icono del corazón en la esquina superior derecha.
3. Haga clic en Carteras.
4. Haga clic en Bitcoin.
5. Haga clic en Recibir.
6. Haga clic en Copiar dirección.

Cambiando Bitcoin por Ether

Ahora necesita abrir la cuenta en la que guarda su Bitcoin. Buscará un botón de transferencia o envío y pegará la dirección en el campo cuando se presente.
Una vez que haya recibido su Bitcoin en su billetera Jaxx, puede usar la función de intercambio. Sigue estos pasos:

1. Abra el navegador web Brave.
2. Haga clic en el icono del corazón en la esquina superior derecha.
3. Haga clic en Carteras.
4. Haga clic en Bitcoin.
5. Haga clic en Intercambiar.
6. Seleccione Ethereum ETH.
7. Ingrese la cantidad que le gustaría cambiar.

   Para la siguiente sección, necesitará de $5 a $10 de Ether.
8. Haga clic en Continuar.
9. Haga clic en Intercambiar.

Cargando su cuenta MetaMask

Una vez que se haya realizado su intercambio, puede seguir las mismas instrucciones dadas anteriormente para enviar su Ether a su cuenta MetaMask:

1. Ve a la cuenta donde tienes Ether.
2. Haga clic en Cuenta.
3. Haga clic en Enviar.
4. Haga clic en el icono del zorro en la esquina superior derecha de su navegador.
5. Haga clic en el icono de menú.
6. Haga clic en la dirección Ether.
7. Copie la dirección.
8. Pegue su dirección MetaMask Ether en la ventana Destinatario.
9. Ingrese la cantidad que desea enviar.
10. Haga clic en Continuar.
11. Haga clic en Confirmar.

Configurar una cuenta de CryptoKitties

En esta sección, te divertirás un poco usando la cadena de bloques de Ethereum. Aquí aprenderá cómo comprar un activo de cadena de bloques único, crear sus propios activos de cadena de bloques únicos y luego vender su activo en un mercado global.

Este ejercicio increíblemente complejo de crear y vender activos basados en blockchain está disfrazado de adorables imágenes de gatos. Llamado CryptoKitties, te permite coleccionar y crear un nuevo gato digital. Cada imagen tiene características únicas que ha heredado de sus imágenes principales. Cuando haya "criado" un nuevo CryptoKitty, puede arrendar a su gato para que lo críe para crear nuevos activos o venderlo por Ether.

Sigue estos pasos:

1. En su navegador web Brave, vaya a www.cryptokitties.co.
2. Haga clic en Inicio.
3. Haga clic en Conectar.
4. Haga clic en Iniciar sesión.
5. Haga clic en Cantar en la ventana emergente.

Compra de CryptoKitties

En esta sección, tienes dos gatitos para comprar. Esto le permitirá "criar" un nuevo gatito y arrendar sus gatos a otros para que se reproduzcan.

Sigue estos pasos:

1. En su navegador web Brave, vaya a www.cryptokitties.co.
2. Haga clic en Iniciar sesión.
3. Haga clic en Cantar en la ventana emergente.
4. En Great-Value Kitties, haga clic en Examinar todo.
5. Selecciona un lindo gato.


TIP

Tiene muchas opciones, pero debido a que este ejercicio es principalmente solo por diversión, sea barato. Además, busque un gatito que sea "rápido" y "de baja generación". Son más rápidos en la reproducción y tienen tiempos de recuperación más cortos entre reproducción.

6. Haga clic en Comprar ahora.
7. Haga clic en Aceptar, comprar este gatito.
8. Haga clic en Confirmar.
9. Seleccione su segundo gato y siga las instrucciones de compra.

Cría de tus CryptoKitties

En esta sección, tomará los dos gatos que compró en la sección anterior y los cruzará para crear un nuevo gatito. Esta es una actividad muy interesante en la que está creando un nuevo activo digital que es único, tiene una procedencia verificable y puede comercializarse en un mercado global abierto sin un intermediario para facilitar la autenticación o la transferencia.

Según la velocidad de la red Ethereum en el momento en que compró sus gatos, es posible que tarde unos minutos en verlos en Gatitos. Ten paciencia, aparecerán. Siempre puede consultar su registro de transacciones para ver el estado.

Sigue estos pasos:

1. En su navegador web Brave, vaya a www.cryptokitties.co.
2. Haga clic en Iniciar sesión.
3. Haga clic en Mi perfil.
4. Seleccione uno de sus gatos.

5. Haga clic en Crianza.

   La reproducción está representada por un icono de berenjena.

6. Haga clic en Engendrar con mis gatitos.
7. Haga clic en Aceptar, comencemos.
8. Haga clic en el cuadro que dice Seleccione su gatito.
9. Seleccione el otro gato.
10. Haga clic en Aceptar, bríndeles un poco de privacidad.
11. Haga clic en Confirmar en la ventana emergente.

Arrendamiento de sus CryptoKitties

En esta sección, sacaremos uno de sus gatos para reproducirse en el mercado. Al hacer esto, está arrendando su activo en un mercado abierto sin intermediarios. Si una de sus gatas todavía está embarazada, seleccione la otra gata para arrendarla.

Sigue estos pasos:

1. En su navegador web Brave, vaya a www.cryptokitties.co.
2. Haga clic en Iniciar sesión.
3. Haga clic en Mi perfil.
4. Seleccione uno de sus gatos.
5. Haga clic en Crianza.
6. Haga clic en Enviar al público.
7. Ajuste los precios y el tiempo como desee o deje la configuración predeterminada.
8. Haga clic en Listo.
9. Haga clic en Confirmar en la ventana emergente.

¡Felicidades! Has comprado tu primer Bitcoin y lo has cambiado por Ether. Luego compró activos de blockchain y creó los suyos propios. Finalmente, arrendó sus activos en un mercado global abierto para ganar más Ether. Excepto por su primera compra, todas estas acciones se habilitaron en una cadena de bloques pública abierta y no necesitaron un banco o intermediario para facilitar. Si disfrutó de CryptoKitties y le gustaría aprender a crear su propio juego basado en blockchain, puede seguir un sencillo tutorial en línea que le enseña cómo hacer todo. Puede encontrar este tutorial en https://cryptozombies.io.

2 Desarrollando su Conocimiento

EN ESTA PARTE . . .

Descubra el comienzo de la tecnología blockchain con Bitcoin blockchain.

Aclare su conocimiento de la red Ethereum y amplíe su comprensión de la red descentralizada organizaciones autónomas y contratos inteligentes.

Identificar el concepto central de Cardano y cómo es construyendo una nueva plataforma para crear blockchain aplicaciones que escalan.

Mire el nuevo ecosistema de Polkadot y cómo utiliza la prueba de participación y los sustratos.

Conoce la nueva super blockchain Solana y sus plataforma de alto rendimiento para descentralizados aplicaciones que escalan.

EN ESTE CAPÍTULO

» Comprender de dónde proviene la cadena de bloques de Bitcoin

» Buceando en Bitcoin Cash

» Despejando algunos mitos sobre Bitcoin

» Mantenerse seguro al usar Bitcoin

» Minería de Bitcoins

» Hacer una billetera de papel para guardar Bitcoins

Capítulo 4

Contemplando el Bitcoin cadena de bloques

¡Advertencia! Después de leer este capítulo, es posible que se enganche con esta genial tecnología emergente. Leer bajo tu propio riesgo.

Bitcoin demuestra los aspectos más puros de la tecnología blockchain. Es la línea base con la que se comparan todas las demás cadenas de bloques y el marco en el que se han basado casi todas. Conocer los conceptos básicos de cómo funciona la cadena de bloques de Bitcoin le permitirá comprender mejor todas las demás tecnologías que encuentre en este ecosistema.

En este capítulo, le explicaré los fundamentos de cómo funciona la cadena de bloques de Bitcoin. opera. Ofrezco consejos de seguridad que harán que su experiencia con Bitcoin sea más fluida y más exitoso. También te muestro cosas prácticas que puedes empezar a hacer ahora con Bitcoin. En estas páginas, descubra cómo minar el token de Bitcoin, brindándole una nueva forma de conseguir Bitcoins sin comprarlos. Finalmente, descubre cómo transferir sus tokens a billeteras de papel y otras formas prácticas de mantener sus tokens seguros en línea.

Obtención de una breve historia de la Cadena de bloques de Bitcoin

Bitcoin y el concepto de su cadena de bloques se introdujeron por primera vez en el otoño de 2008 como documento técnico y luego lanzado como software de código abierto en 2009. (Puede leer el documento técnico de Bitcoin en www.bitcoin.org/bitcoin.pdf).

El autor que presentó Bitcoin en ese documento técnico de 2008 es un anónimo programador o cohorte que trabaja bajo el nombre de Satoshi Nakamoto. Nakamoto colaboró con muchos otros desarrolladores de código abierto en Bitcoin hasta 2010. Esto Desde entonces, el individuo o el grupo ha dejado de participar en el proyecto y ha transferido el control a destacados desarrolladores centrales de Bitcoin. Ha habido muchas afirmaciones y teorías sobre la identidad de Nakamoto, pero ninguna de ellas ha sido confirmada hasta el momento de escribir este artículo.

De todos modos, lo que Nakamoto creó es un extraordinario pago entre pares. sistema que permite a los usuarios enviar Bitcoin, el token de transferencia de valor, directamente y sin un intermediario para responsabilizar a las dos partes. La propia red actúa como intermediario verificando las transacciones y asegurándose de que nadie intente engañar al sistema gastando Bitcoins dos veces.

El objetivo de Nakamoto era cerrar el gran agujero en la confianza digital, y el concepto de cadena de bloques fue su respuesta. Resuelve el problema del general bizantino, que es el principal problema humano, especialmente en línea: ¿Cómo confía en la información que recibe y en las personas que le brindan esa información, cuando el interés propio, terceros maliciosos y similares pueden engañar? ¿tú? Muchos entusiastas de Bitcoin sienten que la tecnología blockchain es la pieza faltante que permitirá a las sociedades operar completamente en línea porque reformula la confianza al registrar información relevante en un espacio público que no se puede eliminar y siempre se puede hacer referencia, lo que hace que el engaño sea más difícil.

Blockchains mezcla muchas tecnologías antiguas que la sociedad ha estado usando durante miles de años de nuevas maneras. Por ejemplo, la criptografía y el pago se fusionan para crear criptomonedas. La criptografía es el arte de la comunicación segura bajo la mirada de terceros. El pago a través de un token que representa valores también es algo que los humanos han estado haciendo durante mucho tiempo, pero cuando se fusiona, crea criptomonedas y se convierte en algo completamente nuevo. La criptomoneda le permite tomar el concepto de dinero y moverlo en línea con la capacidad de intercambiar valor de forma segura a través de un token.

Las cadenas de bloques también incorporan hashing (transformación de datos de cualquier tamaño en datos cortos, valores de longitud fija). Hashing también incorpora otra tecnología antigua llamada Árboles de Merkle, que toman muchos hashes y los reducen a un solo hash, al mismo tiempo que pueden probar cada pieza de datos que fue procesada individualmente (ver Figura 4-1).

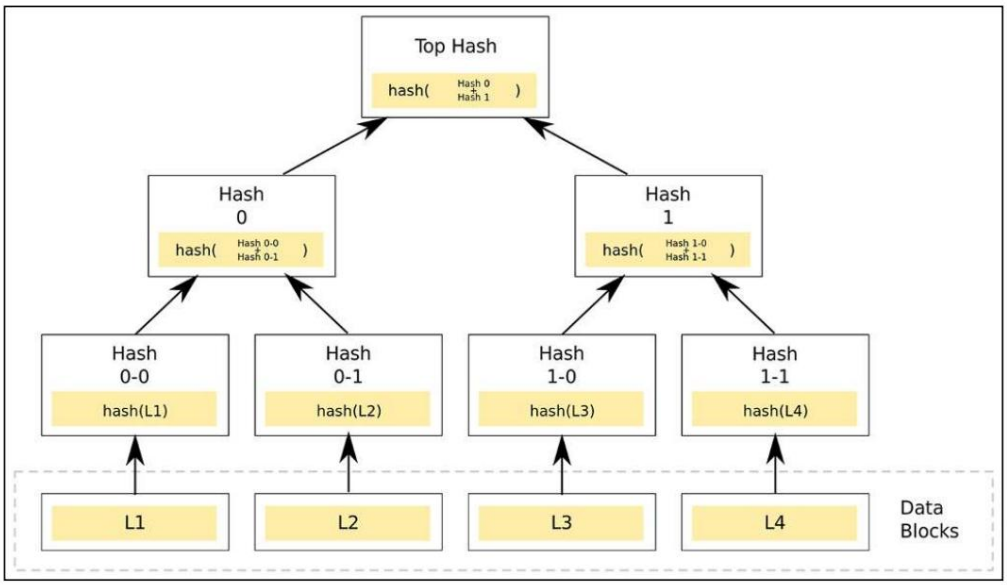


FIGURA 4-1:
Un árbol Merkle.

En última instancia, las cadenas de bloques son libros de contabilidad que la sociedad ha estado utilizando durante miles de años para llevar las cuentas financieras. Cuando todos estos modelos antiguos se fusionan y facilitan en línea en una base de datos distribuida, se vuelven revolucionarios.

Bitcoin fue diseñado principalmente para enviar la criptomoneda Bitcoin. Pero muy rápidamente, los creadores se dieron cuenta de que tenía un potencial mucho mayor. Con eso en mente, diseñaron la cadena de bloques de Bitcoin para poder registrar más que los datos relacionados con el movimiento del token. La cadena de bloques de Bitcoin es la cadena de bloques más antigua y una de las más grandes del mundo. Está compuesto por miles de nodos que ejecutan el protocolo Bitcoin. El protocolo está creando y asegurando la cadena de bloques.

REMEMBER

En términos muy simples, la cadena de bloques es un libro de contabilidad público de todas las transacciones en la red de Bitcoin, y los nodos son computadoras que registran entradas en ese libro de contabilidad. El protocolo Bitcoin son las reglas que rigen este sistema.

Los nodos protegen la red mediante la extracción de la criptomoneda Bitcoin. Los nuevos Bitcoins se crean como recompensa por procesar transacciones y registrarlas dentro de la cadena de bloques. Los nodos también ganan una pequeña tarifa por confirmar transacciones.

Cualquiera puede ejecutar el protocolo Bitcoin y extraer el token. Es un proyecto de código abierto que prospera a medida que más personas participan en la red. Cuanta menos gente participe, más centralizado se vuelve, y la centralización se debilita.
el sistema. Lo principal que hace de Bitcoin un sistema seguro es la gran cantidad de nodos independientes que se distribuyen globalmente.

Los mineros más exitosos tienen sistemas robustos que pueden superar a los mineros más lentos. Al principio de su historia, podía ejecutar el protocolo Bitcoin y ganar Bitcoins en una computadora de escritorio. Ahora, para tener alguna esperanza de recibir Bitcoins, debe comprar un equipo especializado costoso o utilizar un servicio en la nube.

Para crear un mensaje en la cadena de bloques de Bitcoin, debe enviar Bitcoin de una cuenta a otra. Cuando envía una transacción en Bitcoin, el
El mensaje se transmite a través de toda la red. Una vez que se envía el mensaje, es imposible modificarlo porque el mensaje se registra dentro de la cadena de bloques de Bitcoin. Esta característica hace que sea imperativo que siempre elijas tu mensaje sabiamente y nunca difundas información confidencial.

Transmitir el mismo mensaje a miles de nodos y luego guardarlo para siempre en el registro del token puede acumularse rápidamente. Entonces, Bitcoin requiere que mantengas tus comunicaciones muy breves. Hay algunas formas de escribir un mensaje en la cadena de bloques de monedas Bit, como OP_Returneld. Actualmente, puedes escribir hasta 83
caracteres.

El nuevo Bitcoin: efectivo de Bitcoin

Existe un conflicto significativo en torno al desarrollo central de Bitcoin. Apodado el
"Guerra civil de Bitcoin" o el "debate del límite de tamaño de bloque", el conflicto general es entre manteniendo el núcleo de Bitcoin tal como está y ampliando la funcionalidad del software. Este conicto parece simple, pero las repercusiones son enormes. permanente de bitcoin
La naturaleza y los miles de millones de dólares en activos que protege el software de Bitcoin significan que cada cambio de código se revisa y debate rigurosamente.

Bitcoin se bifurcó y se dividió en dos cadenas de bloques separadas en 2017. La comunidad de desarrolladores y mineros de Bitcoin no podía ponerse de acuerdo sobre cómo abordar el crecimiento. Bitcoin se había vuelto cada vez más poco confiable y costoso de usar. una vez había sido un sistema casi instantáneo y casi gratuito; ahora las transacciones costaban más de $50 y tardaban horas o días en liquidarse. El alto costo y la lentitud ahuyentaron
usuarios

Un problema principal fue que las velocidades de transacción de Bitcoin eran demasiado lentas, siete transacciones por segundo, para satisfacer la demanda en la red. Las tarifas de transacción aumentaron a medida que los usuarios competían para que sus transacciones se procesaran más rápido. Uno de los factores limitantes fue que el límite de tamaño de bloque de Bitcoin era de 1 MB en 2017.

Bitcoin Cash usó la misma base de código que Bitcoin pero ajustó el límite de tamaño de bloque. Aumentaron el tamaño del bloque a 32 MB. En el momento del tenedor, cualquiera que tenga Bitcoin también recibió la misma cantidad de Bitcoin Cash. El aumento fue controvertido porque privaba de sus derechos a los mineros más pequeños que tenían equipos más lentos.

Muchos mineros temían no poder ser competitivos en la minería de bloques más grandes. También existía la preocupación de que el tamaño de bloque más grande conduciría a la centralización de la red de cadena de bloques de monedas Bit.

Bitcoin es un sistema vivo y en constante cambio. La comunidad de desarrollo central de Bitcoin está buscando activamente formas de mejorar el sistema haciéndolo más fuerte y más rápido. Cualquiera puede contribuir al protocolo Bitcoin participando en su página de GitHub (www.github.com/bitcoin). Sin embargo, existe una pequeña comunidad de desarrolladores centrales dominantes de Bitcoin. Los colaboradores más prolijos son Wladimir Van

Der Laan, Pieter Wuille y Gavin Andresen.

LAS LIMITACIONES DE BITCOIN

Los bloques que componen la cadena de bloques de Bitcoin están limitados a 1 MB de tamaño. Esto limita la cantidad de transacciones que la cadena de bloques de Bitcoin puede manejar a siete transacciones por segundo. Los nuevos bloques ocurren en promedio cada diez minutos, pero no están garantizados.

Estas limitaciones están codificadas en el protocolo de Bitcoin y ayudan a garantizar que la red permanezca descentralizada. Y la descentralización es clave para la solidez de Bitcoin. Los bloques más grandes impondrían dificultades a los mineros y podrían provocar operaciones pequeñas.

Bitcoin tiene limitaciones incorporadas que le impiden manejar el volumen global de transacciones monetarias. También se está utilizando para proteger otros tipos de datos y sistemas. La demanda de usar el libro mayor seguro de Bitcoin es alta. Esta dificultad se conoce como Bitcoin bloat, y ha ralentizado la red y aumentado el costo de las transacciones.

En este punto, la mayoría de los desarrolladores de cadenas de bloques solo están experimentando con la expansión de la utilidad de la cadena de bloques de Bitcoin. La mayoría no está en un punto en el que necesite ampliar sus prototipos y conceptos para que la cadena de bloques de Bitcoin pueda manejar su solicitud. Otras nuevas tecnologías de cadena de bloques también han ayudado a reducir la presión sobre Bitcoin y han brindado a los desarrolladores opciones más económicas para proteger los datos.

A MEDIDA QUE EL MUNDO GIRA: EL DRAMA DE BITCOIN

Bitcoin está bajo un intenso escrutinio desde el exterior. La naturaleza descentralizada de Bitcoin que puede desplazar a las autoridades centrales lo convirtió en un objetivo para los reguladores. Bitcoin también es favorecido por personas que desean comprar artículos ilícitos de forma anónima o mover dinero de una economía controlada a una economía no controlada, sin pasar por los controles gubernamentales.

Todos estos factores le han dado a Bitcoin una mala reputación y han provocado el juicio de la sociedad. Los empresarios que querían capitalizar la tecnología de Bitcoin la cambiaron de nombre. El cambio de terminología se utilizó para diferenciar la estructura del software de Bitcoin y otras criptomonedas. El software que usaba la estructura de las criptomonedas comenzó a llamarse blockchain. El cambio para restar énfasis a los tokens controvertidos y resaltar la estructura de las criptomonedas cambió la visión tanto del gobierno como comercial de Bitcoin del miedo al entusiasmo.

Desacreditando algunos comunes Conceptos erróneos de Bitcoin

Las personas a menudo sospechan de cualquier cosa nueva, especialmente de las cosas nuevas que no son fáciles de entender. Entonces, es natural que Bitcoin, una moneda totalmente nueva diferente a todo lo que el mundo había visto antes, confundiría a la gente, y un pocos conceptos erróneos resultarían.

Estos son algunos de los conceptos erróneos que puede haber escuchado sobre Bitcoin:

» Bitcoin fue pirateado. Hubo un caso conocido en 2011 en el que alguien gastó el doble de su Bitcoin, pero se resolvió en una hora. Desde este problema, no se conocen ataques exitosos en la cadena de bloques de Bitcoin que hayan resultado en el robo de Bitcoins. Sin embargo, muchos sistemas centrales que usan Bitcoin han sido pirateados. Y las billeteras y los intercambios de Bitcoin a menudo son pirateados debido a una seguridad inadecuada. La comunidad de Bitcoin se ha defendido desarrollando soluciones elegantes para mantener sus monedas seguras, incluido el cifrado de billetera, firmas múltiples, billeteras en línea, billeteras de papel y billeteras de hardware, solo para nombrar unos pocos.

» Bitcoin se usa para extorsionar a la gente. Debido a la naturaleza semianónima de Bitcoin, se usa en ataques de ransomware. Los piratas informáticos violan las redes y las mantienen como rehenes hasta que se les realiza el pago. Hospitales y escuelas han sido víctimas de este tipo de ataques. Sin embargo, a diferencia del efectivo, que fue el favorito de los ladrones en el pasado, Bitcoin siempre deja un rastro en la cadena de bloques que los investigadores pueden seguir.

» Bitcoin es un esquema piramidal. Bitcoin es lo opuesto a un esquema piramidal desde el punto de vista de los mineros de Bitcoin. El protocolo Bitcoin está diseñado como una carrera armamentista caníbal. Cada minero adicional solicita el protocolo para aumentar la dificultad de la minería. Desde un punto de vista social, Bitcoin es un puro mercado. El precio de Bitcoin se basa en la oferta, la demanda y la demanda del mercado. valor percibido. Bitcoin no es un esquema piramidal, pero hay muchas estafas en torno a Bitcoin, así que tenga cuidado.

» Bitcoin colapsará después de que se extraigan 21 millones de monedas. Bitcoin tiene un límite en la cantidad de tokens que lanzará. Ese número está codificado en 21 millones. Se cree que la fecha estimada en que Bitcoin emitió su última moneda es el año 2140. Nadie puede predecir qué sucederá en ese momento, pero los mineros siempre obtendrán algún beneficio de las tarifas de transacción. Además, los usuarios de la cadena de bloques y los Bitcoins mismos serán incentivados para proteger la red, porque si la minería se detiene, los Bitcoins se vuelven vulnerables y también los datos que han sido bloqueados en la cadena de bloques.

» Suficiente poder de cómputo podría hacerse cargo de la red de Bitcoin. Esto es cierto, pero sería extremadamente difícil, con poca o ninguna recompensa. Cuanto más nodos que ingresan a la red Bitcoin, más difícil se vuelve este tipo de ataque. Para lograr esto, un atacante necesitaría el equivalente de todos los producción de energía de Irlanda. La recompensa de este tipo de ataque también es extremadamente limitado. Solo permitiría al atacante revertir su propia transacción. No podía tomar los Bitcoins o las transacciones o monedas falsas de nadie más.

» Bitcoin es una buena inversión. Bitcoin es una evolución nueva e interesante en cómo la gente intercambia valor. No está respaldado por ningún gobierno u organización, y solo vale algo porque la gente está dispuesta a cambiarlo por bienes y servicios. La voluntad y la capacidad de las personas para utilizar Bitcoinuctuates mucho. Es una inversión inestable que debe abordarse con cautela.

Bitcoin: el nuevo salvaje oeste

El mundo de Bitcoin es muy parecido a los primeros días del Salvaje Oeste. lo mejor es acercarse con cautela hasta que descubras quiénes son los buenos y los malos y cuáles salón sirve la cerveza más fría. Si es víctima de una estafa, tendrá poca o ninguna protección.

Los bitcoins y otras criptomonedas descentralizadas se consideran moneda en muchos países, pero existe poca o ninguna supervisión o protección para consumidores

En esta sección, enumero tres de las estafas comunes que prevalecen en el mundo de las criptomonedas. Todos giran en torno al robo de tus monedas y se parecen mucho a las estafas tradicionales con las que quizás ya estés familiarizado. Esta lista no es exhaustiva y los ladrones no son más que creativos, así que tenga mucho cuidado al usar Bitcoins. Tú Nunca se sabe lo que hay a la vuelta de la siguiente esquina.

Sitios falsos

Los sitios web que parecen bolsas de valores o monederos web, pero que son falsos, han afectado a algunos de los principales sitios web de Bitcoin. Este tipo de estafa es común en el mundo Bitcoin y en la web en general. Los estafadores esperan ganar dinero robando la información de inicio de sesión de los usuarios o engañándolos para que envíen Bitcoins.


TIP

Siempre verifique dos veces la URL y solo use sitios web seguros (aquellos que comienzan con https://) para evitar este problema. Si un sitio web o reclamo parece dudoso, verifique si aparece en https://db.aa419.org. Esta no es una lista exhaustiva, pero tiene muchos de los malos jugadores enumerados.

¡No, el tuyo!

"Envíeme sus Bitcoins y luego le enviaré los productos". Huele a timidez, ¿verdad? Estafas como esta son similares al fraude de transferencia de dinero. En este tipo de fraude, un individuo pretende venderle algo pero nunca lo entrega.

La naturaleza semi-anónima de Bitcoins, combinada con la incapacidad de hacer una Reembolso: haga que sea difícil recuperar su dinero. Además, los gobiernos no actualmente ofrecen protección para las transacciones de Bitcoin, por lo que está listo para ese proverbial arroyo sin remo.

Los estafadores intentarán ganarse su confianza enviando identificaciones falsas o incluso haciéndose pasar por Otras personas que tal vez conozcas. Siempre verifique dos veces la información que le envían.


TIP

La mejor manera de esquivar este tipo de estafa es escuchar su instinto y nunca arriesgar más Bitcoins de los que está dispuesto a perder. Si hay una manera de verificar la identidad de la persona oine, hágalo.

Esquemas para hacerse rico rápidamente

Los esquemas locos para hacerse rico rápidamente han proliferado en el mundo de las criptomonedas. La buena noticia es que es fácil reconocerlos si sabe qué buscar.

A menudo, se le prometen ganancias masivas y hay algún tipo de proceso de reclutamiento y adoctrinamiento. Este proceso podría incluir cosas como capacitación en ventas, pedirle que reclute a sus amigos y familiares y prometerle que esta es una inversión libre de riesgos y que nunca perderá su dinero. Esto incluye nunca dar acceso a nadie a sus claves privadas.

El resultado final: si un esquema parece demasiado bueno para ser verdad, probablemente lo sea. Pase lo que pase, analice detenidamente cómo la inversión está generando valor fuera de lo que recibirá de su inversión. Si no hay una razón clara y racional de que una cantidad significativa de valor sea la tasa de generación, es una estafa.


TIP

Ejecute todas las inversiones por un abogado y un CPA. Ellos pueden ayudarlo a entender su riesgos e implicaciones fiscales.

Minería de Bitcoins

Puede comenzar a ganar Bitcoins de varias maneras. La minería de Bitcoin es cómo para ganar Bitcoins participando en la red. Por lo general, lo maneja un hardware de minería especial que es costoso y especializado. El equipo también necesita Software de minería de Bitcoin para conectarse a la cadena de bloques y su grupo de minería (una colaboración de muchos mineros que trabajan juntos y luego dividen las recompensas de sus esfuerzos).

Aquí hay tres formas estándar de explorar la minería de Bitcoin:

- Bitcoin-QT: El cliente Bitcoin-QT es el software original escrito por Satoshi Nakamoto. Puede descargarlo en https://bitcoin.org/en/download.
- CGminer: CGminer es uno de los software de minería más populares. Es de código abierto y está disponible para Windows, Linux y OS en www.github.com/ckolivas/cgminer.
- Multiminerapp: Multiminerapp es un cliente Bitcoin fácil de ejecutar. Puede descárguelo en www.multiminerapp.com.


REMEMBER

Bitcoin es un entorno muy competitivo y, a menos que compre equipos de minería especializados, es posible que nunca gane Bitcoins. No apruebo ni recomiendo ningún equipo de minería en particular en este libro porque la industria cambia constantemente y queda obsoleta rápidamente. Espere pagar entre $500 y $5,000 por máquina en promedio. Amazon.com es un buen lugar para buscar. Tienen una gran oferta y muchas reseñas de clientes para guiarlo.

La minería en la nube te permite empezar a ganar Bitcoins en una tarde laboriosa, sin necesidad de descargar software ni comprar equipos. Siempre lea las reseñas sobre los proveedores de servicios de minería en la nube: la industria ha sido poco fiable en el pasado. Uno plataforma que usted puede querer considerar es ECOS. ECOS lo ayuda a comenzar la minería en la nube Bitcoin con bastante facilidad. También vende equipos con alto poder de hash, una billetera criptográfica, un intercambiador y carteras de criptomonedas. Solo sigue estos pasos:

1. Navegue a https://ecos.am.
2. Haga clic en Registrarse.
3. Introduzca su dirección de correo electrónico y haga clic en Siguiente.

   Se envía un código de verificación a su dirección de correo electrónico.

   Revisa tu carpeta de correo no deseado si no ves un código de verificación de inmediato.


TIP

4. Ingrese el código de verificación que recibió.
5. Cree una nueva contraseña.

   Use una contraseña segura y guárdela en un lugar en línea como un cuaderno. Esto es importante para mantener su cuenta segura.

6. Ingrese su número de teléfono celular.

   Se envía un código de verificación a su número de teléfono.

7. Ingrese el código de verificación que recibió.

   ¡Felicidades! Ha configurado su panel de control de minería en la nube. Desde aquí, tú puede navegar a Buy Hashrate, que le permitirá ganar tiempo en un dispositivo en la nube para comenzar a minar su Bitcoin.


WARNING

El retorno de la inversión para la minería en la nube puede ser negativo. Revise sus opciones cuidadosamente para asegurarse de que sea una inversión positiva.

Hacer tu primera billetera de papel

Una billetera de papel es una copia en papel de su clave pública y privada para sus Bitcoins. Debido a que son completamente únicas, las billeteras de papel son una de las formas más seguras para mantener Bitcoins cuando se hace correctamente. La ventaja es que su clave privada no se almacena digitalmente, por lo que no está sujeta a piratería. Dicho esto, las billeteras de papel tienen algunos riesgos inherentes que deben tenerse en cuenta:

» Debe almacenar las billeteras de papel de forma segura, ya que pueden ser robadas fácilmente si caen en las manos equivocadas.

» Los pedazos de papel regulares pueden dañarse fácilmente con agua, fuego u otros elementos, haciéndolos ilegibles. Para evitar esto, puede ser necesario almacenar las billeteras de papel en un recipiente a prueba de agua, resistente al agua o a prueba de daños, y para imprimirlos en papel de alta calidad con tinta de calidad. Algunas personas incluso laminan sus billeteras de papel para mayor protección.

» Los sitios web utilizados para generar billeteras de papel pueden ser pirateados, por lo que debe elegir un servicio de confianza.

Para aumentar aún más la seguridad de las billeteras de papel, existen herramientas disponibles como Cryptotag, que le permiten almacenar la semilla de su billetera en una placa de titanio casi indestructible. Algunos generadores de billeteras de papel populares incluyen BitAddress, WalletGenerator y Mycellium Entropy, que es un dispositivo de hardware específicamente diseñado para generar billeteras de papel de alta seguridad. Puede considerar un hardware dispositivo para asegurar grandes sumas.

Hacer una billetera de papel es bastante fácil en BitAddress. Solo sigue estos pasos:

1. Vaya a www.bitaddress.org.
2. Mueva el mouse por la pantalla hasta que la cantidad de aleatoriedad muestra el 100%.
3. Haga clic en el botón Monedero de papel.

   Esto le da la opción de crear una billetera de papel que puede imprimir.
4. En el campo Direcciones para generar, ingrese 1.

   Puede hacer varias billeteras a la vez, si es necesario, pero también puede Comience con uno para entenderlo.
5. Haga clic en el botón Generar.

   La Figura 4-2 muestra una billetera de papel que creé.
6. Haga clic en el botón Imprimir.


WARNING

No dejes que nadie te vea crear tu billetera de papel. Esto no es algo que quieras hacer en una computadora pública. Asegúrese de usar una impresora que sea privada y que no esté conectada a Internet para que no corra el riesgo de que sus claves privadas sean pirateadas.


TIP

Lamine su billetera de papel para que sea un poco más duradera.

FIGURA 4-2:
Una billetera de papel.

EN ESTE CAPÍTULO

Capítulo 5

Encuentro con el Cadena de bloques de Ethereum

El proyecto Ethereum es uno de los bloques más desarrollados y accesibles. cadenas de bloques en el ecosistema. También es uno de los más necesarios en términos de innovación y casos de uso. Comprender esta tecnología es esencial porque está a la vanguardia en contratos inteligentes, organizaciones descentralizadas y ofertas de tokens.

En este capítulo, cubro la composición de Ethereum y explico la nueva forma de crear organizaciones y empresas en la cadena de bloques de Ethereum. También profundizo en la seguridad y las aplicaciones comerciales prácticas de la cadena de bloques de Ethereum. ¿Estás enfermo? sobre cómo comenzó el proyecto y hacia dónde planea ir.

Este capítulo lo prepara para crear su propia organización descentralizada. Explico cómo minar la criptomoneda en la red de prueba para impulsar tus proyectos. Después de leer este capítulo, podrá configurar su propia billetera Ethereum e intercambiar el token. También podrá generar su propio token personalizado que se puede comercializar a nivel mundial.

Explorando la breve historia de Ethereum

Ethereum se describió por primera vez en 2013 en un documento técnico escrito por Vitalik Buterin, quien fue muy activo en la comunidad de Bitcoin como escritor y programador. Buterin vio que había mucho más potencial en Bitcoin que la capacidad mover valor sin una autoridad central. Había estado contribuyendo al esfuerzo de monedas de colores dentro de Bitcoin para expandir la utilidad de Bitcoin más allá del comercio de sus ficha nativa. Buterin creía que otros casos de uso empresarial y gubernamental que requerir una autoridad central para controlarlos también podría construirse con blockchain estructuras

En ese momento, hubo un debate acerbo sobre la "inflación" de la red Bitcoin. por muchas transacciones de bajo valor de aplicaciones que se protegen contra Bitcoin. Las principales preocupaciones eran que las aplicaciones adicionales, basadas en Bitcoin protocolo, tendría problemas para escalar en volumen. Además, en ese momento no había la capacidad de hacer secuencias de comandos para permitir cosas como contratos inteligentes. Bitcoin no fue construido para manejar la cantidad de transacciones que necesitan las aplicaciones. Vitalik y muchos otros vieron que para que las personas puedan crear aplicaciones descentralizadas en la cadena de bloques de Bitcoin, la cadena de bloques necesitaría una revisión masiva del código o necesitarían construir una nueva cadena de bloques por completo.

Bitcoin ya estaba bien establecido en ese momento. Estaba claro que los tipos de las actualizaciones del código central que se necesitaban estaban mucho más allá de lo que era realmente posible. La política de Bitcoin detendría cualquier cambio en la red. Vitalik y su equipo establecieron la fundación Ethereum a principios de 2014 para recaudar fondos para construir una red blockchain con un lenguaje de programación integrado dentro de ella. Vitalik esperaba crear una red que le permitiera construir aplicaciones protegidas por blockchain.

El desarrollo inicial fue financiado por una venta multitudinaria pública en línea durante julio y agosto de 2014. La fundación inicialmente recaudó un récord de $18 millones a través de la venta de su token de criptomoneda llamado ether. La gente ha debatido apasionadamente si este tipo de venta colectiva es ilegal porque puede constituir una oferta de valores sin licencia.

La zona gris regulatoria no ha obstaculizado el proyecto. En todo caso, la naturaleza vanguardista del proyecto ha atraído más atención y talento a la fundación. Desarrolladores y empresarios descontentos y privados de sus derechos de todo el mundo se han unido al proyecto. La descentralización se considera la solución perfecta para las autoridades centrales corruptas y opresivas.

Los $18 millones recaudados en la venta de tokens le dieron a la fundación los fondos que necesitaba para contratar un gran equipo de desarrollo para construir Ethereum. Ethereum Frontier, la primera lanzamiento de la red Ethereum, se lanzó al público en julio de 2015. Fue un

lanzamiento de software básico que solo los más expertos en tecnología podrían usar para construir sus aplicaciones.

Las propuestas de mejora de Ethereum (EIP) son sugerencias para mejorar la red de Ethereum. Pueden tratarse de cambiar la forma en que funciona la red o agregar nuevas funciones. En 2022, EIP-3675 actualizó Ethereum Mainnet para usar un nuevo
forma de llegar a un acuerdo (consenso) sobre el estado de la red llamada prueba de participación (PoS). Esto cambió a Ethereum del mecanismo de consenso original de prueba de trabajo (PoW) para cambios en la estructura de bloques, el procesamiento de bloques, la regla de elección de bifurcaciones y la interfaz de red.

PoS es diferente de PoW porque implica retener una cierta cantidad de
Criptomoneda Ethereum para ayudar a tomar decisiones sobre la red en lugar de usar la potencia de la computadora para resolver problemas matemáticos complejos. Este EIP explica cómo funcionaría la actualización a PoS y qué cambios deberían realizarse en la red. Fue escrito por Mikhail Kalinin, Danny Ryan y Vitalik Buterin y tiene
sido analizado

Ethereum: el código abierto Computadora mundial

Ethereum puede ser una de las cadenas de bloques más complejas jamás construidas. Tiene varios de sus propios lenguajes de programación completos de Turing (lenguajes de programación de funcionamiento completo que permiten a los desarrolladores crear cualquier aplicación). Estos nuevos lenguajes de programación se parecen mucho a los lenguajes de programación populares como JavaScript y Python. El protocolo Ethereum puede hacer casi cualquier cosa que puedan hacer sus lenguajes de programación habituales. La excepción es que el código está escrito en la cadena de bloques de Ethereum y tiene los beneficios y la seguridad adicionales que
viene con eso Si puede imaginar un proyecto de software, puede construirse en Ethereum.

El ecosistema Ethereum es actualmente el mejor lugar para construir aplicaciones descentralizadas. Tiene una documentación encantadora e interfaces fáciles de usar que lo ponen en funcionamiento rápidamente. Tiempo de desarrollo rápido, seguridad para aplicaciones pequeñas y
la capacidad de las aplicaciones para interactuar fácilmente entre sí son características clave de este sistema.

Los lenguajes de programación completos de Turing son la característica principal que hace que la cadena de bloques de Ethereum sea mucho más potente que la cadena de bloques de Bitcoin para construcción de nuevos programas. El lenguaje de secuencias de comandos de Ethereum hace que cosas como las aplicaciones de Twitter sean posibles en pocas líneas de código y extremadamente seguras.

Los contratos inteligentes, como el que crea en el Capítulo 3, también se pueden construir en Ethe
reum. El protocolo Ethereum ha abierto un nuevo género de aplicaciones.
Puede tomar casi cualquier proceso empresarial, gubernamental u organización y crear una
representación digital de él dentro de Ethereum. Actualmente, la plataforma de Ethereum se utiliza para
administrar activos digitales (una nueva clase de activo que vive en línea y puede representar un activo
digital completo, como un token de Bitcoin o un token digital).
representación de un activo del mundo real, como productos básicos de maíz), instrumentos financieros
(como valores respaldados por hipotecas), registro de la propiedad de activos como la tierra y
organizaciones autónomas descentralizadas (DAO). Ethereum también ha provocado un importante
esfuerzo de recaudación de fondos por parte de empresas emergentes de todo el mundo que utilizaron el token ERC.
estándar para recaudar capital para construir sus innovaciones. Ethereum ha abierto una nueva forma
de organizar negocios, sin fines de lucro y gubernamentales. Ha hecho posible
mantener, compartir y comercializar valor sin conocer a la otra parte o utilizar a un tercero para facilitar.
El código hace el trabajo.

Aplicaciones descentralizadas: Bienvenido al futuro

La manifestación más revolucionaria y controvertida de Ethereum es la aplicación autónoma y
descentralizada (dApp). Las dApps pueden administrar cosas como activos digitales y DAO.

Las dApps se crearon para reemplazar la gestión centralizada de activos y organizaciones. Esta
estructura tiene mucho atractivo porque mucha gente cree que el poder absoluto corrompe absolutamente.
Para aquellos que temen perder el control, este tipo de estructura tiene enormes implicaciones.

Aparecen nuevas dApps todos los días. Puede explorar y descubrir nuevos creados en Ethereum yendo
a https://dappradar.com. DappRadar actualiza una lista de todos
las últimas dApps de Ethereum y le brinda una vista previa de lo que hacen. Uno de los
La primera que se creó fue Etheria (ver Figura 5-1).

El poder de los organismos autónomos descentralizados

Los DAO son un tipo de aplicación de Ethereum que representa una entidad virtual dentro de Ethereum.
Cuando crea un DAO, puede invitar a otros a participar en el gobierno de la organización. Los
participantes pueden permanecer en el anonimato y nunca reunirse, lo que podría desencadenar reglas
de Conozca a su cliente (KYC) (el proceso que un
empresa debe pasar por la verificación de la identidad de sus clientes) y Anti-Money
Lavado (AML; las leyes y regulaciones diseñadas para detener la práctica de
generar ingresos a través de medios ilegales) problemas de cumplimiento.

FIGURA 5-1: el primero del mundo juego digital inmortal, Etheria.

Los DAO se han creado para recaudar fondos para invertir, pero también podrían diseñarse con fines cívicos o sin fines de lucro. Ethereum te da un marco básico para la gobernabilidad. Depende de los organizadores determinar qué se está gobernando. Ethereum ha creado plantillas para ayudarlo en la creación de DAO.

La Figura 5-2 muestra una descripción de la organización de una aplicación Ethereum.

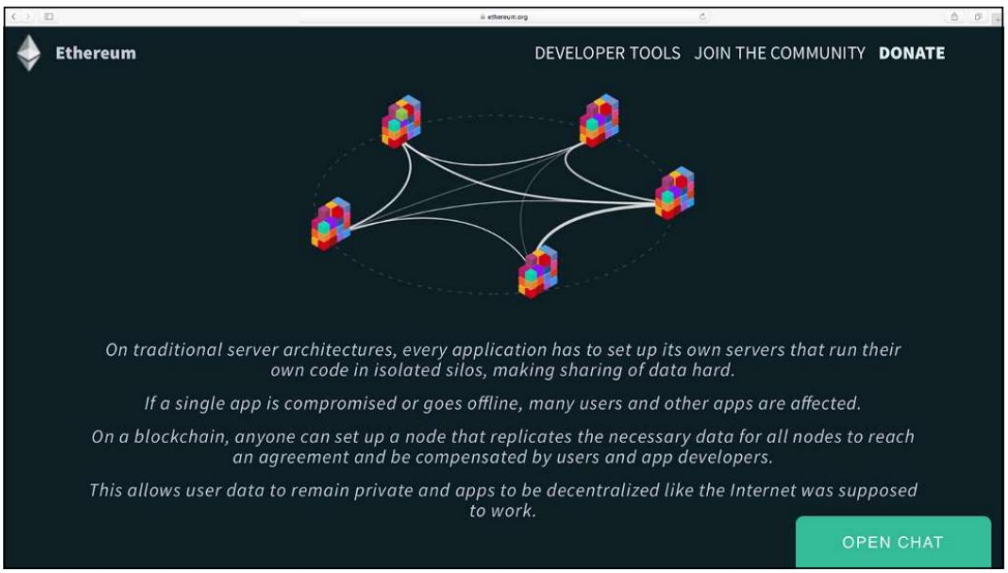


FIGURA 5-2: cadena de bloques Ethereum.org representación de la aplicación.

Así es como funcionan básicamente los DAO:

1. Un grupo de personas escribe un contrato inteligente para gobernar la organización.
2. Las personas agregan fondos a la DAO y reciben tokens que representan la propiedad.

   Esta estructura funciona como las acciones de una empresa, pero los miembros tienen el control de los fondos desde el primer día.
3. Una vez recaudados los fondos, la DAO comienza a funcionar al tener

   los miembros proponen cómo gastar el dinero. La votación puede verse afectada por cómo Cuánto Ether el miembro arriesga o apuesta en el DAO.
4. Los miembros votan sobre estas propuestas.
5. Transcurrido el tiempo predeterminado y acumulado el número predeterminado de votos, la propuesta pasa o no.
6. Las personas físicas actúan como contratistas para dar servicio a la DAO.

A diferencia de la mayoría de los vehículos de inversión tradicionales, donde una parte central toma las decisiones sobre las inversiones, los miembros de una DAO controlan el 100 por ciento de los activos.
Votan sobre nuevas inversiones y otras decisiones. Este tipo de estructura amenaza con desplazar a los administradores financieros tradicionales.

Los DAO están construidos con código que no se puede cambiar en ellos. El atractivo de esto es que los piratas informáticos maliciosos no pueden jugar con los fondos en un sentido tradicional. Los piratas informáticos aún pueden encontrar formas de ejecutar el código de formas inesperadas y retirar fondos. El la naturaleza inmutable del código de un DAO hace que sea casi imposible eliminar cualquier error una vez el DAO está en vivo en Ethereum.

CON GRAN PODER VIENE . . . GRAN PODER

El primer DAO de Ethereum jamás construido se llama, de manera bastante confusa, "The DAO". Es un ejemplo de algunos de los peligros que conllevan las entidades descentralizadas y autónomas.
Es el proyecto de financiación colectiva más grande del mundo: sus fundadores recaudaron aproximadamente $162 millones en 26 días con más de 11,000 miembros. Lo que la gente pensaba que era la mayor fortaleza de The DAO se convirtió en su mayor debilidad. El código inmutable dentro de The DAO aseguró cómo se gobernaría la organización y cómo se distribuirían los fondos. Esto permitió a los miembros sentirse seguros en su inversión.

mento Aunque el código fue bien revisado, no se habían solucionado todos los errores.

La primera amenaza importante para Ethereum provino del hackeo de The DAO. Un inesperado
La ruta de código en el contrato de la DAO permitía a cualquier usuario sofisticado retirar fondos. Un
usuario desconocido logró eliminar alrededor de $ 50 millones antes de que pudiera ser detenido.

La comunidad de Ethereum debatió amargamente si podía o debía reclamar el éter. El hacker de DAO
técnicamente no había hecho nada malo o incluso pirateado el sistema. Los fundamentalistas dentro
de la comunidad Ethereum sintieron que el código era la ley y, por lo tanto, no se debe hacer nada para
recuperar los fondos.

Lo mismo que hizo que Ethereum fuera fuerte también fue su mayor debilidad.
La descentralización, la inmutabilidad y la autonomía significaban que ninguna autoridad central podía
decidir qué hacer rápidamente. Tampoco había nadie a quien castigar por el mal uso del sistema.
Realmente no tenía ninguna medida de protección al consumidor. Era una nueva frontera, como
sugería el nombre del software.

Después de pasar varias semanas discutiendo el problema, la comunidad de Ethereum decidió
cerrar The DAO y crear un nuevo Ethereum. Este proceso se llama bifurcación dura. Cuando la comunidad
de Ethereum bifurcó la red, revirtió la transacción que había cometido el hacker. También creó dos
Ethereums: Ethereum y
Etéreo clásico.

No todos estaban de acuerdo con esta decisión. La comunidad continúa usando Ethereum Classic.
Los tokens de Ethereum Classic aún se comercializan, pero han perdido signi -
no puede valor de mercado. El nuevo token de Ethereum aún no ha recuperado su antiguo máximo
anterior al hackeo.

La decisión de bifurcar sacudió el mundo blockchain. Era la primera vez que un proyecto mayoritario de
cadena de bloques se bifurcaba para hacer completo a un inversor. Cuestionó muchos de los principios
que hacen que la tecnología blockchain sea tan atractiva en primer lugar.

Hackear una cadena de bloques

Ethereum nunca ha sido pirateado. La bifurcación dura en 2016 debido al hackeo de DAO mencionado en
"Con gran poder viene . . . gran poder" no era una barra lateral real
pirateo del sistema, pero de manera confusa a menudo se lo denomina pirateo. Ethereum funcionó
perfectamente. El problema era que era demasiado perfecto. Se hizo necesario reiniciar el sistema cuando una
gran cantidad de dinero y la mayoría de sus usuarios fueron amenazados.

La única forma de corregir una acción en una cadena de bloques como Ethereum es hacer una bifurcación
dura, que permite un cambio fundamental en el protocolo. Una bifurcación dura hace que los bloques y las
transacciones previamente válidos sean inválidos. Ethereum hizo esto para proteger el

fondos que un usuario estaba retirando de la primera DAO. El truco de DAO fue
conceptualmente, una de las recompensas de errores más grandes de la historia.

Dicho esto, muchas estafas e intentos de piratería ocurren en el espacio de las criptomonedas.
La mayoría de estos ataques se dirigen a intercambios y aplicaciones centralizados. Muchos hackers
quieren robar criptomonedas. Tiene un valor real y no está protegido de la misma manera que los gobiernos
protegen el dinero normal. La naturaleza anónima de la criptomoneda también la hace atractiva para los
delincuentes. Atrapar y enjuiciar a estos individuos es difícil. Sin embargo, la comunidad de criptomonedas
se está recuperando.
y crear nuevas medidas para protegerse.


REMEMBER

Hackear un lugar es significativamente más fácil y económico que tratar de superar un
red descentralizada. Cuando lee sobre la piratería en el mundo de la cadena de bloques, es probable que
solo se haya pirateado un sitio web o una billetera de criptomonedas, no toda la red.

Descubriendo los DAO de Ethereum

Ethereum fue construido para DAO. Ethereum es, en efecto, su propio DAO. Utiliza el consenso de sus
nodos distribuidos para gobernar su función. Ethereum desarrolló un código de contrato inteligente que no
se puede modificar después de su publicación; esto permite que la DAO
funcionar por las reglas que los participantes acordaron al inicio. Finalmente, los contratos inteligentes son
el tercero de confianza para cuando necesita enviar o recibir fondos.

En las siguientes secciones, cubro la importancia de configurar su DAO para el futuro. También me sumerjo
en el concepto de delegación en DAO, que permite a los poseedores de fichas delegar sus votos en
personas designadas que los representarán y administrarán el protocolo Ethereum. Muchos DAO utilizan
la delegación como una forma de gestión.
herramienta para las operaciones diarias.

Gobernanza DAO

Deberá tener en cuenta muchas cosas al crear o unirse a una DAO. Dado que
es casi imposible cambiar las reglas o revertir una transacción después de que se haya publicado un
contrato inteligente DAO, asegúrese de considerar cómo funcionan las votaciones y las propuestas.

DELEGACIÓN DAO

La delegación funciona de manera muy parecida a cómo las personas eligen a los funcionarios para que
los representen en el gobierno. La versión DAO de la democracia representativa requiere que los
poseedores de tokens deleguen sus votos a los usuarios que han sido nominados. Luego, las personas
nominadas se comprometen a administrar el protocolo Ethereum y se mantienen activamente involucrados.

Un ejemplo es ENS, el estándar de nomenclatura más ampliamente integrado para blockchain.
En el momento de escribir este libro, más de 500.000 usuarios se habían registrado más de 2,6
millones de nombres. Los poseedores de tokens de ENS pueden delegar sus votos a miembros de la comunidad
comprometidos para que los representen dentro de la DAO de ENS.

RECLAMANDO SU NOMBRE EN ENS

En esta sección, se sumerge en el Servicio de nombres de Ethereum (ENS) para reclamar un nombre en ENS.
Para ello, vaya al sitio web de ENS, inicie sesión con su MetaMask
monedero, y buscando y registrando su nombre deseado. Este proceso es para comprar un nombre de dominio.
Solo sigue estos pasos:

1. Vaya a https://claim.ens.domains.
2. Haga clic en su billetera MetaMask en su navegador web.

   Esto lo iniciará en el sitio web de ENS. Si aún no ha configurado su billetera MetaMask, regrese al
   Capítulo 3 y siga las instrucciones.

3. Haga clic en Ir a la aplicación.
4. Introduzca el nombre que le gustaría reservar.

   Piense en este nombre como lo haría con el dominio de un sitio web.

5. Haga clic en Buscar.
6. Haga clic en Registrarse.

Si el nombre que desea está disponible, tendrá la opción de comprarlo como lo haría con un dominio. Repita este
proceso con un nuevo nombre si su nombre deseado no es
disponible.

¡Felicidades! ¡Ya ha asegurado su primer dominio Web 3.0!

GOBERNANZA AUTOMÁTICA DE TRANSACCIONES EN DAO

En muchas DAO, las transacciones se ejecutarán automáticamente si un quórum de miembros vota armativo.
Un quórum es el número de miembros que la especie de contrato inteligente requiere para aprobar una nueva
transacción. Un ejemplo destacado de esto
es Sustantivos DAO (https://nouns.wtf). La DAO de Sustantivos permite que una transacción se ejecute
automáticamente si se alcanza un quórum de votos para la transacción.

LA GOBERNANZA MULTISIG DE LAS DAO

Aunque las DAO pueden tener miles de miembros con derecho a voto, la gobernanza real de los fondos está
controlada por una billetera compartida por 5 a 20 miembros activos de la comunidad.
Estos miembros son de confianza, y sus identidades públicas suelen ser conocidas por el

comunidad. Normalmente, cuando se hace una propuesta a la DAO, los miembros votarán para su aprobación. Cada miembro votante hace esto a través de una transacción en Ethereum usando multisig.

Una dirección multisig (abreviatura de multifirma) es un tipo de dirección que requiere varias firmas para autorizar una transacción. Esto también se puede usar para agregar una capa adicional de seguridad a una billetera o cuenta de criptomonedas.

Por ejemplo, supongamos que tiene una dirección multisig que requiere dos firmas para autorizar una transacción. Puede configurarlo para que se requiera una firma de su dispositivo personal y otra de un dispositivo que pertenezca a un amigo de confianza. Esto significa que para enviar fondos desde la dirección multisig, tanto usted como su amigo de confianza deberán firmar la transacción con sus respectivos dispositivos. Al agregar esta función, agrega una capa adicional de seguridad a sus transacciones y requiere el consentimiento de varias partes.

Las direcciones multisig también pueden requerir más de dos firmas, según el implementación específica. Una DAO podría requerir potencialmente miles o más firmas. Imagínese si un gobierno utilizara una DAO como infraestructura para autorizar la aprobación de nuevas leyes o la votación para la elección de funcionarios públicos. El multigrado
La característica es útil para las organizaciones que desean organizarse en un mundo sin confianza.

En general, las direcciones multisig pueden ser una herramienta útil para agregar una capa adicional de seguridad a las transacciones de criptomonedas, DAO, ofertas de tokens y, especialmente, en casos donde múltiples partes necesitan estar involucradas en el proceso de autorización.

Membresía DAO

Puede convertirse en miembro de una DAO a través de algunos modelos diferentes. Su membresía generalmente gira en torno a los derechos de voto que se le otorgan a través del contrato inteligente. Hay varias estructuras DAO comunes:

LA LEGALIDAD DE LA DAO

En 2021, Wyoming se convirtió en el primer estado en establecer leyes que reconocen las DAO como un entidad de negocios. Al momento de escribir este libro, Wyoming, Vermont y las Islas Vírgenes tienen leyes DAO de alguna forma.

Un ejemplo notable de una DAO reconocida es CityDAO, que utilizó la ley DAO de Wyoming.
para comprar 40 acres de tierra cerca del Parque Nacional de Yellowstone para construir una ciudad criptográfica en cadena, gobernada por la comunidad.

» Membresía basada en tokens: la membresía basada en tokens significa que usted es un miembro por defecto simplemente manteniendo el token DAO. Estos tipos de DAO normalmente están abiertos a cualquier persona con las formas y los medios para unirse, a menudo llamados totalmente sin permiso. Sus tokens de gobernanza se pueden intercambiar sin permiso en un intercambio descentralizado e incluso pueden tener algún valor monetario. Es también posible tener un token intransferible; este tipo de fichas se denominan vinculados al alma. Otros tipos de DAO requieren que obtenga tokens mediante la realización de servicios, como proporcionar liquidez o realizar pruebas de trabajo para asegurar transacciones.

Un ejemplo interesante de este tipo de DAO es el MakerDAO. Su token, MKR, es se usa en intercambios descentralizados, y puede comprarlo y obtener poder de voto en el protocolo Maker. El protocolo Maker le permite crear una moneda de precio estable que usted controla llamada Dai. Dai impulsa un ecosistema en crecimiento de más de 400 aplicaciones, incluidas billeteras, plataformas financieras descentralizadas (DeFi), y juegos

» Membresía basada en acciones: los DAO basados en acciones tienen más permisos grupos que requieren que envíes una propuesta para unirte a la DAO. También a menudo requieren que pague la membresía a través de tokens o el trabajo que realiza para el grupo. Sus tokens representan su poder de voto y propiedad. Por lo general, puede dejar la DAO en cualquier momento con su parte proporcional de la tesorería de la DAO.

Estos tipos de DAO se crean para organizaciones centradas en el ser humano, como organizaciones benéficas, colectivos de trabajadores y clubes de inversión. El MolochDAO es un fantástico ejemplo de este tipo de DAO. Los miembros de MolochDAO aportan capital para financiar el desarrollo de Ethereum. Actúa como una organización sin fines de lucro enfocada en infraestructura como un bien público digital esencial. MolochDAO requiere una propuesta de membresía para que el grupo pueda evaluar si tiene la experiencia y el capital necesarios para hacer juicios informados sobre el potencial beneficiarios No se puede comprar el acceso a la DAO.

» Membresía basada en la reputación: Otra estructura DAO interesante es Membresía basada en la reputación, que es una estructura de prueba de participación que le otorga poder de voto dentro de la DAO. Los DAO basados en la reputación no transferir la propiedad a los contribuyentes: esta es una estructura ligada al alma. La reputación no se puede comprar, asignar o delegar a otra persona. Usted gana su reputación a través de su participación. Votar no requiere permiso cuando tienes tu token ligado al alma. Los miembros potenciales pueden enviar propuestas para unirse a la DAO. Las nuevas solicitudes reciben reputación y tokens como recompensa por sus contribuciones. Este tipo de DAO es excelente para el desarrollo descentralizado y la gobernanza de protocolos y dApps.

El DXdao utiliza este tipo de estructura. Los miembros de la DAO desarrollan, gobiernan y hacen crecer los productos DeFi. Creado en mayo de 2019, DXdao es un colectivo de unas 400 personas centradas en el ecosistema DeFi. Es un ejemplo fascinante de un colectivo soberano mundial. DXdao aprovecha la gobernanza basada en la reputación y el consenso holográfico para coordinar y administrar fondos. No puedes comprar tu entrada.

Entendiendo los contratos inteligentes

Los contratos inteligentes de Ethereum son como acuerdos contractuales, excepto que no hay una parte central para hacer cumplir el contrato. El protocolo Ethereum "hace cumplir" los contratos inteligentes al agregar presión económica. También pueden hacer cumplir la implementación de un requisito si vive dentro de Ethereum, porque Ethereum puede probar que ciertas condiciones se cumplieron o no. Si no vive dentro de Ethereum, es mucho más difícil de hacer cumplir.

Los contratos inteligentes de Ethereum aún no son legalmente exigibles y es posible que nunca lo sean porque la percepción es que no necesita autoridades externas para hacer cumplir los acuerdos. Los sistemas legales están controlados por los gobiernos. Tal como están ahora, los gobiernos son autoridades centrales, algunos con más o menos consentimiento y principios democráticos. Dentro de un contrato inteligente de Ethereum, cada participante tiene un voto inalienable.

Los contratos inteligentes de Ethereum no incluyen inteligencia artificial. Esta es una posibilidad interesante en un futuro próximo. Pero por ahora, Ethereum es solo un código de software que se ejecuta en una cadena de bloques.

Los contratos inteligentes de Ethereum no son seguros. El hackeo de DAO es un gran ejemplo del tipo de peligros que pueden ocurrir. Todavía es pronto, y poner mucho dinero en un sistema no probado no es inteligente. En su lugar, experimente con pequeñas cantidades hasta que todos los errores hayan sido resueltos en los nuevos contratos.

Descubriendo la criptomoneda Ether

Ether es el nombre de la criptomoneda para la cadena de bloques Ethereum. Recibió su nombre de la sustancia que se creía que impregnaba todo el espacio y hacía posible el universo. En ese sentido, Ether es la sustancia que hace posible a Ethereum. Ether incentiva a la red para que se asegure a sí misma a través de la minería de prueba de trabajo, como el token Bitcoin incentiva la red Bitcoin. Se necesita éter
para ejecutar cualquier código dentro de la red Ethereum. Cuando se utiliza para ejecutar un contrato en Ethereum, Ether se denomina gas.

Ejecutar el código dentro de un contrato inteligente también cuesta una cierta cantidad de éter. Esta característica le da al token una utilidad adicional. Mientras las personas quieran usar Ethereum para aplicaciones y contratos, Ethereum tendrá un valor más allá de la especulación.

El crecimiento salvaje en el valor del éter lo ha convertido en un token popular para especular. Se negocia ampliamente en bolsas de todo el mundo. Algunos fondos de cobertura nuevos lo ven como un vehículo de inversión. Sin embargo, la naturaleza volátil y la baja profundidad del mercado hacen que ether sea una inversión riesgosa.

Ponerse en marcha en Ethereum

En esta sección, lo explico cómo comenzar en el ecosistema blockchain de Ethereum. Antes de que pueda construir cualquier cosa en Ethereum, necesita un Ethereum billetera.


REMEMBER

Su billetera contendrá sus tokens Ethereum llamados ether. Ether es la criptomoneda que te permite crear contratos inteligentes dentro de Ethereum. Esto a veces se denomina gas.

La descarga de la billetera Ethereum puede llevar algún tiempo, pero la interfaz es muy intuitiva y las instrucciones proporcionadas a lo largo del proceso son fáciles de seguir.


TIP

Dentro de la billetera Ethereum, puede ganar éter de prueba para construir sus organizaciones y contratos de prueba. No es necesario extraer éter para aprender cómo funciona.

Minería de éter

Ethereum se mantiene en funcionamiento gracias a una red de computadoras en todo el mundo que procesan los contratos y aseguran la red. Estas computadoras a veces se denominan nodos y extraen cripto éter.

Para recompensar a las personas por el tiempo y el costo involucrados en la minería, hay un premio de cinco éteres aproximadamente cada 12 segundos. El premio se otorga al nodo que fue capaz de crear el último bloque en la cadena de bloques de Ethereum.

Todos los bloques nuevos tienen una lista de las últimas transacciones. El algoritmo de consenso de prueba de trabajo garantiza que los premios los ganen con mayor frecuencia los nodos con la mayor potencia computacional. Las computadoras que no son tan poderosas también pueden ganar, simplemente toma mas tiempo. Si desea probar suerte en la extracción de éter, puede hacerlo con la computadora de su hogar, pero tomará mucho tiempo extraer con éxito un bloque y ganar éter.

La minería de éter no es para los novatos técnicos. Debe estar familiarizado con la línea de comandos. Si no tiene idea de qué es la línea de comandos, probablemente desee omitir este proceso. Además, asegúrese de seguir las instrucciones más actualizadas en Ethereum GitHub (http://github.com/ethereum).

Configuración de su billetera Ethereum

Para configurar su billetera Ethereum, siga estos pasos:

1. Vaya a www.ethereum.org.
2. Haga clic en el botón Descargar.

Tienes que desplazarte un poco hacia abajo en la página para encontrar el botón.

Asegúrese de guardar la descarga de la billetera Ethereum en algún lugar donde pueda encontrarla más tarde.

3. Abra la billetera Ethereum.

Es posible que deba buscar actualizaciones del software en Ayuda.

4. Elija Desarrollar en el menú desplegable.
5. Seleccione una de las redes de prueba, como Robsten o Rinkeby.

Aquí te preparas para probar ether. Este proceso requiere mucho menos tiempo que la extracción de éter real, pero aún lleva algo de tiempo; actualmente, son unas dos horas.

6. Cree una contraseña segura.

No olvides guardar tu contraseña en un lugar seguro.

7. Haga clic en el menú de inicio.

El equipo de Ethereum tiene algunos tutoriales que son interesantes para revisar mientras espera que se descargue su red de prueba. La descarga puede tardar diez minutos más o menos.

8. Seleccione Desarrollar Iniciar minería.

No te saltes este paso. Necesitas el éter para proyectos posteriores.

Acaba de configurar su billetera y está ganando éter de prueba para sus futuros proyectos de contratos inteligentes.

Construyendo su primer descentralizado Organismo Autónomo

Los DAO cambiarán la forma en que el mundo hace negocios en el futuro. Permiten que cualquier persona en el mundo cree un nuevo tipo de empresa en línea que se rige por reglas acordadas previamente que luego se aplican a través de la red blockchain. Crear una DAO es más fácil de lo que piensas. En esta sección, construye su primer DAO de prueba. Divido este proyecto en tres secciones: construcción, congreso y gobierno.

REMEMBER

Para completar con éxito su DAO de prueba, debe haber configurado su billetera Ethereum y realizado algo de minería en la red de prueba de Ethereum (consulte la sección anterior).

Siga estos pasos para crear su primer DAO de prueba:

1. Vaya a www.ethereum.org/dao.
2. Desplácese hacia abajo en la página hasta el cuadro Código (que se muestra en la Figura 5-3) y copie el código.
3. Abra la billetera Ethereum que creó anteriormente.

   Desarrollarás tu DAO en tu billetera Ethereum.

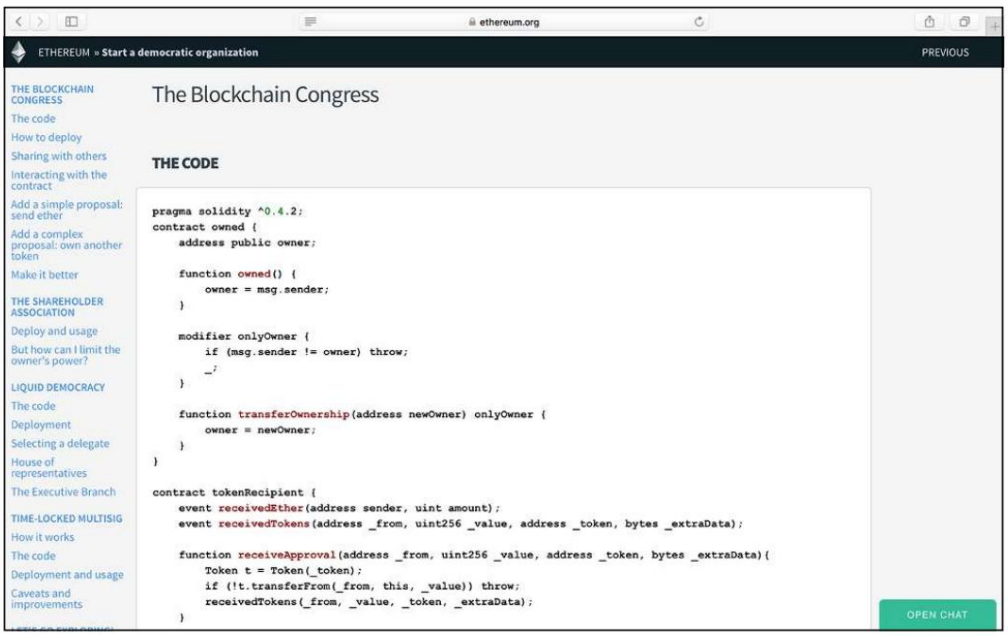


FIGURA 5-3:
El cuadro de código.

Test net y congreso

La siguiente fase de su proyecto DAO es configurar el marco para su DAO. Sigue estos pasos:

1. En su billetera Ethereum, seleccione Desarrollar Red Probar red.
2. Haga clic en la pestaña Contratos y luego haga clic en Nuevo contrato.

   El equipo de Ethereum ha configurado algunas plantillas de prueba para DAO.
3. Pegue el código que copió en la sección anterior en Solidity cuadro de código

   Asegúrese de seleccionar Código fuente del contrato de solidez en la pestaña y no Código de bytes del contrato.
4. En el Selector de contratos, seleccione Congreso.
5. Elija algunas variables cuando se le solicite hacerlo.

   Aquí están sus opciones:

   - El quórum mínimo para las propuestas es la menor cantidad de votos que debe tener una propuesta antes de que pueda ser ejecutada.
   - El acta de debate es la menor cantidad de tiempo, en minutos, que debe pasar antes de que pueda ejecutarse.
   - El margen de votos para la mayoría. Las propuestas pasan si hay más del 50 por ciento de los votos más el margen. Déjalo en 0 para una mayoría simple.

Gobernanza y votación

Ahora va a nombrar y configurar el gobierno de su DAO. Necesitas configurar establecer un quórum mínimo para las propuestas (cuántos votos debe tener una nueva propuesta antes de ser aprobada). También configura el margen de votos para una mayoría (cuántos votos necesita aprobar un plan) y el tiempo asignado para discutir nuevos planes.

1. Asigne un nombre a su nueva DAO.

   Esto es como nombrar una empresa.
2. Para Tiempos de debate, seleccione 5 minutos.

   Este es el tiempo que las nuevas propuestas están abiertas a la conversación.
3. Deje el Margen de votos para la mayoría establecido en 0.

   Esto establece cómo funciona la democracia de su contrato.

4. Conrma el precio de la DAO.

   Ha extraído algo de Ether en la red de prueba a través de su billetera cuando lo configuró por primera vez. Si te saltaste ese paso, regresa y hazlo ahora. Necesitas un poco de Ether de red de prueba para construir tu DAO.

5. Haga clic en Implementar y escriba su contraseña.

   El DAO puede tardar algún tiempo en implementarse. Cuando llegue a su nuevo tablero, desplácese hacia abajo y podrá ver cómo se produce su DAO.

6. Haga clic en el icono Nuevo.

   Se generará un nuevo ícono único que representa su DAO.

¡Felicidades! Ha creado su primer DAO.

Descubriendo el futuro de las DAO

Los contratos inteligentes y las organizaciones descentralizadas son muy prometedores. La naturaleza puramente democrática e hiperracional de ellos es muy atractiva. Sin embargo, en este punto, hay más posibilidades que conocidas, y cada contrato que se crea puede ser innovador o una operación masiva.

Si te acercas a Ethereum como la nueva frontera que es, tendrás más éxito.
La red Ethereum tiene más beneficios que inconvenientes si tiene cuidado. Pero esperar que todo funcione a la perfección y que todos los participantes actúen con integridad lo expondrá a mayores pérdidas. Ethereum tiene su parte de bandidos, sin mencionar a esos amistosos entusiastas a los que les gustaría que tuvieras éxito.

Los hackeos de contratos inteligentes de 2016 han resaltado la importancia de la seguridad y revisar adecuadamente los contratos. También ilustró que hay personas con integridad que tienen problemas de toxicidad.

Leer este libro es sólo el comienzo. Le dará una base sólida para construir su conocimiento de Ethereum, pero como con todas las nuevas tecnologías, Ethereum está evolucionando rápidamente. Siga revisando las mejores prácticas y medidas de seguridad.

En las siguientes secciones, menciono algunas cosas que debe tener en cuenta al crear sus primeros DAO, crear contratos inteligentes y depurar sus nuevos sistemas de cadena de bloques.

Poner dinero en una DAO

No confíe grandes sumas de dinero a contratos no probados y contratos que no han sido examinados completamente. Los piratas informáticos atacan con mayor frecuencia los contratos grandes. El truco DAO descrito anteriormente en este capítulo (consulte la barra lateral "Con gran poder llega . . . gran poder") mostró que incluso los contratos bien pensados tienen debilidades inesperadas.


REMEMBER

Aunque los contratos inteligentes y las cadenas de bloques le permiten hacer negocios con cualquier persona en todo el mundo, aún es el comienzo. Puede mitigar su riesgo trabajando solo con partes conocidas y confiables.


TIP

El panorama de la seguridad evolucionará constantemente con nuevos errores. Revisando todo nuevas mejores prácticas es imprescindible. Administra la cantidad de dinero que estás poniendo en riesgo y despliegue de contratos lentamente y en fases. Ethereum es una tecnología nueva y aún no se han creado soluciones maduras.

Construyendo contratos inteligentes más inteligentes

La programación de contratos inteligentes requiere una mentalidad diferente a la redacción de contratos estándar. No hay un tercero para arreglar las cosas si el contrato se ejecuta de una manera que usted no esperaba o pretendía. La naturaleza inmutable y distribuida de las cadenas de bloques dificulta cambiar un resultado no deseado.


REMEMBER

Su contrato se vence y puede fallar. Incorpore válvulas de seguridad en sus contratos para que pueda responder a los errores y vulnerabilidades a medida que surjan. Los contratos inteligentes también necesitan un interruptor de apagado que le permita desconectar y pausar su contrato cuando las cosas van mal


TIP

Si su contrato es lo suficientemente grande, ofrezca recompensas de búsqueda de errores que incentiven el comunidad tond vulnerabilidades andaws en su contrato.

Como ocurre con muchas cosas, la complejidad de su contrato también aumenta la probabilidad de errores y vectores de ataque. Mantenga la lógica de su contrato simple. Construya pequeños módulos que contengan cada sección del contrato. Crear un contrato de esta manera lo ayudará a compartimentar cualquier problema.

Encontrar errores en el sistema.

No reinvente la rueda creando sus propias herramientas, como generadores de números aleatorios. En su lugar, aproveche el trabajo que la comunidad ya ha realizado y que ha sido bien probado.

Solo puede controlar las cosas dentro de su propio contrato. Tenga cuidado con lo externo llamadas de contrato. Pueden ejecutar código malicioso y quitarle el control.

La comunidad de Ethereum tiene una excelente lista de errores conocidos e incluso más consejos útiles sobre cómo crear contratos inteligentes seguros en su página de GitHub en https://github.com/ethereum/wiki/wiki/seguridad.

Descubriendo DAOhaus en Ethereum

DAOhaus es una plataforma sin código para crear y administrar una DAO. El DAOhaus aplicación le permite:

» Crear una DAO.

» Añadir miembros a la DAO.

» Coordine propuestas con una interfaz fácil de usar.

La aplicación DAOhaus tiene tres componentes: el contrato inteligente, los subgráficos y el cliente.

» Contrato inteligente: DAOhaus utiliza los contratos inteligentes de Moloch DAO para facilitar Funcionalidades DAO en cadena. Por ejemplo, puede agregar miembros a través de propuestas y tesorería. Debido a que DAOhaus es una plataforma sin código, interactúa con los contratos de Moloch para todas las acciones y funciones en cadena, por lo que no es necesario. Actualmente, la aplicación DAOhaus es compatible con Moloch v2 DAO mediante los siguientes contratos:

- Moloch v2.1 y 2.5 son capacidades de múltiples invocadores, además de un registro Función para metadatos y patrón proxy EIP-1167 para reducir costos de gasolina.
- Minion le brinda la capacidad de interactuar con sus contratos inteligentes mientras mantiene los fondos seguros en una bóveda de terceros llamada Gnosis Safe.

La aplicación DAOhaus está programada para usar Moloch v3 (Baal) por el finales de 2023.

» Subgraphs: DAOhaus utiliza The Graph, un protocolo de indexación para consultar redes como Ethereum e IPFS. Puede crear y publicar una aplicación abierta interfaces de programación (API), llamadas subgrafos, que hacen que los datos sean fácilmente accesibles y monetizables. Los subgráficos aseguran que los datos en cadena estén indexados y disponible para consulta. Un protocolo de indexación incentiva y coordina la indexación de datos públicos de blockchain. Puede encontrar datos en todos los DAO compatibles instantáneamente usando The Graph. Puede encontrar más información sobre The Graph en https://thegraph.com.

» Cliente: El cliente es un software que le permite acceder e interactuar con el DAO. Está construido utilizando el marco React, que es una biblioteca de JavaScript popular para la construcción de interfaces de usuario. El cliente permite al usuario hacer referencia a datos en cadena de subgráficos, que son estructuras de datos que almacenan información sobre una cadena de bloques de una manera más organizada y fácilmente accesible. Los subgráficos se pueden usar para indexar y consultar datos en la cadena de bloques, lo que facilita el trabajo con ellos. y analizar El cliente también se puede utilizar para realizar funciones en cadena, que se refieren a acciones que tienen lugar en la propia cadena de bloques. Por ejemplo, el cliente se puede utilizar para interactuar con los contratos inteligentes de Moloch, que son contratos autoejecutables con los términos del acuerdo entre el comprador y el vendedor se escribe directamente en líneas de código. El cliente permite al usuario ejecutar estos contratos inteligentes e interactuar con ellos en la cadena de bloques.

Construyendo y configurando su propio club DAO en DAOhaus

En esta sección, construyes y configuras tu propia DAO en DAOhaus, una plataforma que proporciona herramientas y recursos para crear y administrar DAO.


REMEMBER

Una DAO es un tipo de organización que funciona con tecnología blockchain y se rige por un conjunto de reglas codificadas en un contrato inteligente. Las DAO permiten que individuos o grupos colaboren y tomen decisiones de manera descentralizada, sin necesidad de una autoridad central.

La plataforma DAOhaus ofrece una variedad de funciones y herramientas para administrar una DAO. Él permite a los miembros de una DAO administrar fondos en una tesorería compartida y monitorear las transferencias de fondos. La plataforma proporciona votación basada en acciones, lo que permite a los miembros crear y votar sobre una variedad de tipos de propuestas. También incluye un mercado de "impulsos" desarrollados por la comunidad que brindan funcionalidad personalizada para DAO. Debido a que los humanos no siempre se llevan bien, el DAOhaus permite períodos de gracia y Funcionalidad "ragequit" para proteger las inversiones de los miembros de DAO. DAOhaus es es propiedad y está operado por miembros de la comunidad y brinda oportunidades para que usted se involucre en el cultivo de la plataforma.

Puede configurar su DAO visitando el sitio web de DAOhaus e iniciando sesión con su billetera MetaMask. También deberá agregar las direcciones de los miembros que estará participando en el DAO contigo. Si está haciendo esto por su cuenta, simplemente puede crear una segunda dirección. Si tiene otras personas que desea agregar, primero deberá obtener sus direcciones de Ethereum. Cuando termines, tú y el otros miembros podrán empezar a tomar decisiones y participar en la organización.

Siga estos pasos para configurar su DAO:

1. Vaya a https://app.daohaus.club.
2. Haga clic en su billetera MetaMask para iniciar sesión.
3. Haga clic en Clubes.

   Si no ve esta opción, vaya a https://app.daohaus.club/summon.
4. Haga clic en Agregar varios invocadores.

   Asegúrese de que haya una dirección poblada. Puedes añadir más si quieres.
5. Haga clic en Convocar.
6. Dentro de su billetera MetaMask, haga clic en Confirmar.


TIP

Establezca su tarifa de gas al nivel más bajo para reducir el costo de configurar su DAO. Puede haz esto desde tu billetera MetaMask.

La configuración de una DAO implica establecer las reglas y la estructura de gobierno para la organización. Esto incluye determinar cómo se tomarán las decisiones, quién puede participar en la toma de decisiones y qué acciones puede tomar la DAO. Allá
Hay varias formas de configurar un DAO, y el enfoque específico dependerá de sus necesidades y metas en el futuro. Algunos elementos comunes incluyen:

» Reglas de votación: cómo se realizarán las votaciones y qué porcentaje de la votación se necesario para aprobar una decisión

» Reglas de membresía: quién considera que es elegible para unirse a la DAO y cómo alguien puede convertirse en miembro

» Distribución de tokens: cómo se distribuirá la propiedad en el DAO entre miembros

» Reglas de financiación: cómo financiará la DAO y cómo se asignarán los fondos a diferentes proyectos o iniciativas

» Proceso de toma de decisiones: el proceso que seguirá al tomar decisiones y quién tendrá la autoridad para tomar decisiones en nombre de la DAO

Una vez que se ha configurado un DAO, se puede utilizar para facilitar la descentralización toma de decisiones y permitir que sus miembros colaboren y trabajen hacia objetivos compartidos.

Para configurar tu club DAO, sigue estos pasos:

1. Haga clic en Configurar.

   Se abre una nueva ventana que le permite actualizar la información sobre su organización.

2. Introduzca los datos de su club en el formulario.

   Puede regresar y editar estos detalles; no son parte del contrato inteligente.

3. Haga clic en Guardar.

Ahora tienes un club DAO completamente funcional.

Creación de sus propios tokens ERC20

En esta sección, le muestro cómo crear su propio token usando Polymath. Poly math es un servicio de token de seguridad que se basa en la cadena de bloques de Ethereum. Le ha quitado el arduo trabajo de programar su propio token en Ethereum. Polymath ofrece una interfaz de apuntar y hacer clic que cualquiera puede usar.

Antes de leer esta sección, asegúrese de haber configurado MetaMask. Si
Si no lo ha hecho, consulte el Capítulo 3, donde encontrará instrucciones detalladas para configurar su computadora y descargar MetaMask.

También necesita tener en sus manos algo de Kovan Test Ether (KETH) para establecer
elabore los contratos inteligentes para su nuevo token. KETH es el Éter de prueba del Kovan
red de prueba, una red de prueba para desarrolladores que trabajan en aplicaciones Ethereum.
KETH no tiene valor de mercado. Puedes obtenerlo gratis si tienes una cuenta de GitHub.

En esta sección, lo guiaré a través de cómo configurar su cuenta de GitHub, cómo
solicita KETH, y cómo crear tus tokens.

Ver tu cuenta de GitHub

GitHub es una plataforma de desarrollo para almacenar el código que desarrollas. GitHub ofrece gratis cuentas para proyectos de código abierto. Entonces, si se siente cómodo compartiendo el código que ha desarrollado, GitHub es una fuente fantástica para administrar sus proyectos y
software de construcción. GitHub también ofrece una versión paga si desea conservar su código privado. A los efectos de esta sección, una cuenta gratuita funcionará muy bien.

Para abrir una cuenta de GitHub, siga estos pasos:

1. Abra el navegador web Brave.

   Si aún no tiene el navegador Brave, vaya al Capítulo 3.

2. Navegue a https://github.com.
3. Ingrese sus credenciales deseadas.
4. Haga clic en Registrarse en GitHub.

Estás listo.

Solicitud de KETH en el grifo Gitter

Para solicitar KETH, sigue estos pasos:

1. Abra el navegador web Brave.
2. Vaya a https://gitter.im/kovan-testnet/faucet.
3. Haga clic en Iniciar sesión para comenzar a hablar.
4. Seleccione Iniciar sesión con GitHub.

A continuación, obtendrá la dirección de su cuenta de MetaMask para poder pegarla en la ventana de chat social y permitir que uno de los miembros de la comunidad le envíe algo de KETH. Sigue estos pasos:

1. Abra su cuenta MetaMask.

   Para abrir su cuenta MetaMask, haga clic en el ícono del zorro en la esquina superior derecha de la ventana del navegador Brave.

2. Desde su cuenta de MetaMask, haga clic en la pestaña desplegable.
3. Seleccione Red de prueba de Kovan.
4. Copie su dirección de MetaMask haciendo clic en Cuenta 1.


REMEMBER

Ahora estás listo para solicitar un Ether de prueba llamado KETH de la comunidad Kovan. Tomará su dirección de Kovan Ethereum de su cuenta de MetaMask y la publicará en la ventana de chat. Asegúrate de publicar solo tu dirección. Sigue estos pasos:

1. Vuelva a navegar a https://gitter.im/kovan-testnet/faucet.
2. Pegue su dirección copiada en la ventana de chat.

Ahora deberá esperar porque uno de los miembros de la comunidad verificará su cuenta de GitHub y se asegurará de que no esté enviando spam a la red. Esto puede llevar algún tiempo porque el proceso de envío de KETH se realiza manualmente. Verá el KETH en su cuenta MetaMask después de que se complete la transacción. Este proceso me llevó tres días, pero trabajé en él durante un fin de semana festivo.

Para configurar su cuenta de Polymath, siga estos pasos:

1. Abra el navegador web Brave.
2. Vaya a https://tokenstudio.polymath.network.
3. Haga clic en Crear su token de seguridad.
4. Navegue hasta el ícono del zorro para su billetera MetaMask.
5. Haga clic en Firmar desde MetaMask.

Creando tus fichas

Ahora que tiene el requisito previo de KETH necesario para crear su propio token, ya puede comenzar. En esta sección, utilizará el contrato inteligente de Polymath para crear un token Ethereum ERC20 personalizado.

Reservando su símbolo de token

Polymath le permite reservar su símbolo de token durante 60 días. Este proceso de reserva es esencial para configurar su token. Puede verificar qué nombres ya se han tomado yendo a Etherscan (https://etherscan.io/token) y buscando el nombre que está pensando usar.


TIP

Reservar su nombre con Polymath solo lo protege dentro del sistema Polymath. No evitará que otra persona emita un token con el mismo nombre en Ethereum.

Ingrese a su billetera Jaxx y use el servicio Shapeshift para intercambiar parte de su BTC o Ether por POLY. Después de hacer esto, mueva sus nuevos tokens POLY de su billetera Jaxx a su cuenta MetaMask. (El Capítulo 3 brinda instrucciones sobre cómo mover fichas de una dirección a otra).

Para nombrar su token, siga estos pasos:

1. Ingrese el nombre de su token de cotización deseado.

   Debe tener cinco caracteres o menos.

2. Ingrese el nombre de su token.

3. Haga clic en Reservar símbolo de token.

   Estas son algunas letras que representarán su token en la red.

4. Haga clic en Confirmar.

5. Navegue hasta el ícono del zorro para su billetera MetaMask.

6. Haga clic en Aprobar en contrato.

7. Haga clic en Aprobar en tarifa.

Si su transacción no es aprobada, asegúrese de tener suficiente Ether en su billetera para pagar la tarifa de minería de Ethereum. Tomará algún tiempo para que su contrato sea aprobado. Esto se debe a la latencia inherente a las cadenas de bloques.

Creando tus fichas

Ahora que ha reservado el nombre que desea usar para su token, puede crear su nuevo token. Polymath le habrá enviado un correo electrónico con un enlace a su panel de creación de tokens.

Su tablero está integrado con varios proveedores de servicios que brindan servicios de asesoría, legales, KYC/AML, marketing y custodia que puede necesitar si planea poner su token a disposición del público. KYC (Conozca a su cliente) es un procedimiento contra el lavado de dinero que se utiliza para identificar a los clientes que desean mover dinero. Es parte de un esfuerzo global contra el lavado de dinero y el terrorismo llamado AML (Anti-Money Laundering) y Combate al Financiamiento del Terrorismo (CFT). Siempre haga su debida diligencia y busque su propio consejo legal. Si elige trabajar con estos proveedores integrados, la información que ingrese en cada formulario se enviará automáticamente a los términos que seleccionó. Therms se comunicará con usted para ayudarle a través de los siguientes pasos.

En los siguientes pasos, asumo que no va a ofrecer su token a el público.

1. Navegue hasta el correo electrónico de Polymath que recibió.

2. Haga clic en el enlace Haga clic aquí para continuar con la creación de su token.

3. Abra su billetera MetaMask.

4. Haga clic en Firmar.

5. Haga clic en I Have My Own para cada uno de los proveedores de servicios.

Ahora que ha conrmado que tiene sus propios proveedores de servicios, puede
comience a especificar su token. El lado izquierdo de la página tiene varios íconos que le permiten saber en qué parte del proceso se encuentra.

1. Haga clic en Ficha en el lado izquierdo de la página.
2. En Mi token de seguridad debe ser, haga clic en Divisible.
3. Haga clic en Crear mi token de seguridad.
4. Abra su billetera MetaMask y haga clic en Confirmar.
5. Haga clic en Confirmar.
6. Espere un minuto, abra su billetera MetaMask nuevamente y haga clic en Confirmar
   por la tarifa minera.

Si la página se atasca en la aprobación de su contrato durante más de cinco minutos, actualice la página y use MetaMask para iniciar sesión nuevamente. Además, desde el interior de tu MetaMask billetera, puede ver el estado de su contrato. Puede aumentar la tarifa de minería y hacer que se procese más rápido. Sin embargo, esto puede disparar el costo de la transacción, así que tenga cuidado si elige esta opción.

Polymath tiene una distribución incorporada de tokens para aquellos que los usan como un medio para recaudar capital. En su tablero de Polymath, esto se conoce como STO, abreviatura de Security Token Oering. En las instrucciones que proporcioné, asumí que el token que está creando no se usará para recaudar capital, por lo que puede hacer clic en Omitir acuñación y luego en Confirmar.

Polymath ha creado plantillas para la creación de tokens de seguridad. En estas instrucciones, utiliza el contrato inteligente que crea un límite estricto de la cantidad de tokens generados por el contrato inteligente. Usted establece una hora y una cantidad de tokens que le gustaría crear. Debido a que estos tokens irán a su propia dirección,
use números mínimos para no desperdiciar su Ether.

Ahora creará un token de seguridad personalizado limitado. El tope se refiere al hecho de que el número total de tokens creados es el número que eliges en ese momento.
de su creación. Siga estos pasos para comenzar:

1. Seleccione la hora actual.

   Tómese unas horas para ingresar la transacción en caso de que
   suceda algo que lo detenga.

2. En Raise In, seleccione ETH.

3. En Hard Cap, ingrese la cantidad de tokens que desea.
4. En Tarifa, ingrese 1000.


TIP

Piense en esto como la tarifa por generar sus nuevos tokens. Los estarás "comprando" del contrato inteligente. Si ingresa 1000 en Tasa, entonces el costo de producir sus nuevos tokens será de 1 ETH por 1000 tokens nuevos.

5. En Dirección ETH para recibir los fondos recaudados durante la STO, ingrese su dirección MetaMask.
6. Haga clic en Implementar y programar STO.
7. Haga clic en Confirmar.
8. Navegue a su billetera MetaMask.
9. Haga clic en Confirmar.

Obtención de sus tokens Recibirá un correo

electrónico de Polymath informándole que ha configurado correctamente su token. Cuando recibas este correo electrónico, sigue estos pasos:

1. Navegue a https://tokenstudio.polymath.network.
2. Inicie sesión a través de MetaMask.
3. Haga clic en Ficha en el lado derecho.
4. En Mint Your Token, descargue el CSVle de muestra.
5. Abra el archivo CSV.
6. Elimine los datos ficticios.
7. Ingrese su propia dirección de Kovan Test Network en su lugar.
8. Guarde su nuevo CSVle.

Ahora que ha ingresado su dirección para recibir su token, puede cargarlo en la misma página de la que descargó la muestra:

1. Vuelva a navegar a https://tokenstudio.polymath.network.
2. Inicie sesión a través de MetaMask.
3. Haga clic en Ficha en el lado derecho.
4. Haga clic en Cargar archivo.

5. Haga clic en Confirmar.
6. Abra MetaMask.
7. Haga clic en Confirmar.

¡Felicidades! Ha creado su propio token de seguridad de prueba. Ethereum es una herramienta poderosa, y con herramientas como Polymath, es más fácil y rápido crear las aplicaciones de cadena de bloques que desea.

EN ESTE CAPÍTULO

» Familiarizarse con la cadena de bloques de Cardano

» Viendo cómo funciona la cadena de bloques de Cardano obras de consenso

» Tener en tus manos ADA, el token nativo de Cardano

» Creación de un contrato inteligente sin código con Marlowe

Capítulo 6

Descubriendo el Cardano cadena de bloques

En este capítulo, les presento la cadena de bloques Cardano, una relativamente nueva blockchain con capacidades extraordinarias. El equipo de Cardano trabajó durante años investigando, construyendo y probando nuevas tecnologías para crear una cadena de bloques fácil de usar, amigable y confiable. Es emocionante para los desarrolladores construir porque tiene la funcionalidad de contrato inteligente y utiliza un algoritmo de consenso de próxima generación llamado prueba de participación (PoS), lo que le brinda algunas de las velocidades más altas para una cadena de bloques pública. Pero no necesitas saber codificar para obtener algo de Cardano.

Este capítulo es esencial si está interesado en crear contratos inteligentes o desea ganar más criptomonedas mediante la participación. Aquí, descubra cómo asegurar su billetera web, compre ADA (el token nativo de Cardano), gane criptomonedas alquilando sus activos y cree su propio contrato inteligente.

Conociendo a Cardano

Cardano es una plataforma de contrato inteligente descentralizada y de código abierto asegurada por un mecanismo de consenso PoS. Creado en 2015 por los miembros del equipo fundador de Ethereum, Charles Hoskinson y Jeremy Wood, Cardano se creó como una plataforma de cadena de bloques que le permite almacenar, transformar y administrar cosas que valora, incluida su identidad. Cardano se ha posicionado como una cadena de bloques de "investigación".


TIP

PoS es una forma en que algunas cadenas de bloques, como Ethereum y Cardano, llegan a un consenso y validan las transacciones. En un sistema PoS, las personas que tienen criptomonedas (también conocidas como participantes) pueden obtener recompensas por validar transacciones y agregar nuevos bloques a la cadena de bloques.

Fueron necesarios dos años de investigación antes de que el equipo escribiera el primer código. La razón Detrás de este comienzo reflexivo estaba que los fundadores querían que Cardano fuera el sistema operativo financiero para miles de millones de personas. El equipo hizo criptografía investigar y profundizar en la teoría de juegos, la gestión de identidades y el lenguaje de programación. Toda su investigación se documentó en más de 100 artículos académicos y revisados por pares.

Cardano es diferente de la mayoría de las cadenas de bloques. Por ejemplo, crea tokens en Cardano sin contratos inteligentes. Los tokens se rigen y contabilizan de la misma manera que ADA, el token nativo de Cardano. Cuando mueve sus tokens, todos usan la misma infraestructura central. Cardano ha eliminado una capa de complejidad adicional y error humano. Dicho esto, también puede usar un contrato inteligente en Cardano para casos de uso más complejos, como organizaciones autónomas descentralizadas (DAO).

Aquí hay seis cosas que puede hacer con Cardano:

» Enviar y recibir tokens.

» Delegue su ADA a un grupo y gane recompensas.

» Votar sobre propuestas impulsadas por la comunidad.

» Obtenga recompensas de la ADA votando.

» Contribuir a mejorar Cardano.

» Crear contratos inteligentes.

Hay varias razones por las que puede querer considerar a Cardano como el back-end para su aplicación descentralizada (dApp):

LA FUNDACIÓN CARDANO

La Fundación Cardano es una organización sin fines de lucro responsable de supervisar y promoviendo el desarrollo de este protocolo blockchain de Cardano. Trabaja con las partes interesadas de todas las industrias para garantizar que los estándares legales y comerciales estén alineados para aumentar la adopción global. Su responsabilidad más importante es impulsar la adopción de la plataforma.

La Fundación Cardano tiene un consejo de gobierno que incluye dos entidades — EMURGO (https://emurgo.io) y IOHK (https://iohk.io). EMURGO desarrolla, apoya, e incuba oportunidades comerciales e integra negocios. IOHK está contratado para diseñar, construir y mantener la plataforma Cardano.

» Ofrece una infraestructura revisada por pares. Esta puede ser una mejor experiencia que algunos proyectos puramente dirigidos por la comunidad. Tiene una infraestructura más rápida, más segura y más rentable con un equipo dedicado.

» Ofrece previsibilidad precisa de costos porque no subasta por tarifas de transacción. Esta característica es esencial cuando está construyendo una infraestructura empresarial. La mayoría del desarrollo de software necesita capital externo, y Cardano tiene un fondo de riesgo. Cada pocas semanas, se seleccionan nuevos proyectos de las aplicaciones propuestas. La comunidad de Cardano discute y vota propuestas. Si está considerando crear una aplicación en Cardano, consulte el fondo dirigido por la comunidad en https://cfund.vc.

» Fue construido con un método de desarrollo formal de alta seguridad. El mecanismo de consenso, llamado Ouroboros, fue revisado por pares y publicado en publicaciones de primer nivel en ciberseguridad y criptografía. Cubro Ouroboros con más detalle en la siguiente sección.

Entendiendo a Ouroboros: Cardano

Consenso de cadena de bloques

Ouroboros es un protocolo PoS que tiene como objetivo mejorar la seguridad de la cadena de bloques y reducir el consumo de energía. Utiliza técnicas criptográficas, matemáticas y teoría de juegos para garantizar que las transacciones en la cadena de bloques sean precisas y eficientes. El protocolo se considera seguro siempre que la mayoría (51 por ciento) de la ADA apostada esté en manos de participantes honestos. También recompensa a los usuarios que contribuyen a la red de forma positiva. En general, Ouroboros tiene como objetivo proporcionar garantías de seguridad similares a las de los protocolos de prueba de trabajo (PoW), pero con costos de energía más bajos.

El protocolo Ouroboros PoS tiene dos características interesantes:

» Distribuye el control de la red entre los grupos de participación de ADA. Eso significa que casi cualquier persona puede ser recompensada por apoyar el protocolo.

Los pools en participación son operados por nodos que controlan el voto de la ADA que se les ha otorgado. Cuanto más ADA controle el nodo, más probable será que sea recompensado y seleccionado para crear el siguiente bloque. Ouroboros ha puesto algunos límites a esto para ayudar a garantizar que todos tengan una oportunidad justa. Cuando se asigna un nodo como líder del espacio, será recompensado con ADA por agregar un bloque a la cadena. La recompensa también se distribuye a los propietarios de la piscina.

» La ventaja más signi cativa de Cardano sobre las cadenas de bloques PoW es que puede escalar de forma segura, sostenible y ética. Afirma tener cuatro millones de veces la eficiencia energética de Bitcoin.

Reunión ADA: El nativo Ficha de Cardano

ADA es la criptomoneda de Cardano. Lleva el nombre de Ada Lovelace, una matemática inglesa a la que se le atribuye la invención de la programación informática en el siglo XIX.

ADA se usa como una moneda digital y una recompensa en bloque para los nodos en la cadena de bloques de Cardano. Como la mayoría de las criptomonedas, permiten que cualquier persona intercambie valor sin necesidad de que un tercero, como un banco, facilite el intercambio. Cada transacción se registra de forma permanente, segura y transparente en la cadena de bloques de Cardano.

Cada titular de ADA tiene una participación en la red Cardano. También puede tomar el ADA que está almacenado en una billetera y delegarlo a un grupo de apuestas para ganar recompensas. Explico cómo hacerlo en la sección "Delegar su ADA en un stake pool", más adelante en este capítulo.

Compra y venta de ADA

Puede comprar o vender ADA por dinero u otras criptomonedas utilizando intercambios de criptomonedas o desde las dos billeteras Cardano admitidas: Daedalus (https://daedaluswallet.io) y Yoroi (https://yoroi-wallet.com). Puedes encontrar todo los otros lugares donde puede comprar ADA dirigiéndose a CoinMarketCap en https://coinmarketcap.com.

WARNING

Asegúrese de mantener sus claves privadas en privado para mantener sus fondos seguros. Para más información manteniendo su criptomoneda segura, vaya al Capítulo 3.

REMEMBER

Evite mantener su criptomoneda en un intercambio más tiempo del necesario. El escándalo FTX de 2022 es un recordatorio importante de los peligros de incluso un popular
y el intercambio seguro. En su lugar, use una billetera de criptomonedas para proteger su ADA.

Nadar en las piscinas de apuestas de la ADA

Los pools de participación pueden ser públicos o privados. Un grupo de participación público es un nodo de la red de Cardano con una dirección pública a la que otros usuarios pueden delegar su ADA (consulte "Delegación de su ADA en un grupo de participación", más adelante en este capítulo). Como su nombre indica, privado
Solo sus propietarios pueden acceder a los stake pools.

Un operador confiable que se mantiene en funcionamiento las 24 horas del día tiene más probabilidades de tener un grupo exitoso. Estos operadores suelen ser personas con el conocimiento y los recursos para ejecutar el nodo las 24 horas del día. Como titular de ADA, puede delegar en grupos públicos de participación si desea participar en el protocolo y recibir recompensas.
No tiene que operar un nodo de red de Cardano usted mismo.

Cuanta más ADA se delegue a un stake pool, mayor será la posibilidad de que el pool sea seleccionado. Cada vez que se selecciona el grupo, escribirá toda la transacción y producirá un bloque que se registrará en la cadena de bloques de Cardano. El pool es recompensado por hacer este trabajo, y el ADA que recibe se comparte entre el operador del stake pool y los delegadores del stake pool.

Comprometiendo su ADA

Los grupos de Cardano no tienen un monto mínimo de compromiso requerido, pero la mayoría de los intercambios tienen un monto mínimo de pedido que debe tener en cuenta. Al momento de escribir este artículo, Moonpay (un proveedor de pagos de terceros que se usa más adelante en este capítulo) costaba $30.

A menudo, los operadores de piscinas comprometerán parte o la totalidad de su ADA a su piscina para que sea más atractiva. Cuantas más promesas de ADA, más recompensas recibirá el grupo.

Elegir un grupo ADA

Puede medir la conveniencia de un grupo por su clasificación de grupo. El número se genera tomando la participación, los costos y el margen del propietario comprometido y combinándolos con el tamaño y el rendimiento del grupo. Este número se usa para clasificar los grupos en las carteras de Daedalus y Yoroi. Las billeteras indicarán y ordenarán las quinielas por cuán “deseables”
el grupo es para apostar su ADA.

SATURACIÓN DE LOS GRUPOS DE PARTICIPACIÓN DE LA ADA

Cuando un grupo de participación está saturado, tiene más participaciones de ADA delegadas de lo que es ideal para la salud de la red. Cuando un grupo alcanza el punto de saturación total, tendrá recompensas de bloque decrecientes. El mecanismo de saturación evita la centralización al activar ADA tenedores para delegar su ADA a diferentes grupos de participación. También aumenta la demanda de grupos de participación e incentiva a los operadores a establecer nuevos grupos para continuar ganando recompensas máximas.

Cardano creó una métrica de saturación para mantener el bienestar de los titulares de ADA y operadores de pools de participación. Lo hace desincentivando que un grupo se vuelva demasiado grande.

Delegar su ADA en un stake pool

La delegación es el proceso mediante el cual usted, como titular de ADA, puede enviar su dinero a un grupo con otros titulares de ADA. Esto se llama participación delegada. Le permite obtener los beneficios de apostar sin el trabajo de apostar usted mismo.

ADA en la red de Cardano representa una participación en la cadena de bloques. El tamaño de su apuesta es proporcional a la cantidad de ADA que tiene. Tener más de 500 ADA le permite votar sobre asuntos de Cardano.

También puede delegar o prometer su participación a otra parte. Esto es esencial para el funcionamiento de Cardano. Tiene dos formas de ganar recompensas al tener ADA:

» Puede delegar su participación en un grupo de participación administrado por un tercero.

» Puede administrar su propio pool de apuestas.

EL PARÁMETRO DE DESCENTRALIZACIÓN

Cardano opera mediante nodos federados, lo que garantiza que las transacciones en la red funcionen sin problemas y permanezcan activas. El número de nodos federados cambia según la descentralización de la red. La proporción de espacios creados por la federación de nodos es equilibrado en relación con el número de nodos del stake pool.

Esta característica puede cambiar en el futuro. Todas las recompensas en bloque se distribuyen a los grupos de participación operativos. En este momento, los nodos federados no reciben recompensa. Cuando Cardano se haya estabilizado, esta medida de descentralización puede desaparecer.

INCENTIVOS EN APUESTAS DE LA ADA

Se otorgan incentivos a los titulares de ADA para garantizar la longevidad y la salud de la red Cardano. En el momento de escribir este artículo, podría ganar alrededor del 4 por ciento anualizado por apostando su ADA. Los creadores de Cardano utilizan un mecanismo de incentivos que incorpora matemáticas, teoría económica y teoría de juegos.

Tienes tres opciones para apostar tu ADA:

- Puede delegar la participación en un grupo a través de la billetera Daedalus. Dédalo es un completo billetera de nodos desarrollada por IOHK.
- Puede delegar la participación a través de la billetera basada en el navegador Yoroi que EMURGO creado. Explico cómo hacer esto en la sección "Configuración de su sistema para hacer staking".
- Puede configurar su propio grupo de apuestas. Esta opción requiere más tiempo y técnico — más allá del alcance de este libro.

La cantidad de participación delegada a un grupo es la forma principal en que el protocolo elige quién podrá agregar el siguiente bloque a la cadena de bloques de Cardano. Los grupos compiten por la oportunidad de agregar bloques para poder recibir más ADA. El bloque
la recompensa se comparte entre todos los que delegaron su participación en ese grupo.

Configurando su sistema para hacer staking

En esta sección, configura una billetera para mantener ADA, asegura su billetera, compra un mínimo de $ 30 de ADA (el mínimo requerido en el momento de escribir este artículo) y apuesta su ADA dentro de un grupo.

Necesitará dos hojas de papel limpias, un bolígrafo que no manche, una conexión a Internet y el navegador web Brave (https://brave.com) o Chrome (www.google.com/chrome) instalado en su computadora. . Nota: La billetera web que usa en esta sección funciona con todos los navegadores populares, pero las instrucciones se escribieron para el navegador Brave.

REMEMBER

Este tutorial es para una billetera web. Las billeteras web no son tan seguras como el hardware o billeteras de papel, así que no deje una cantidad significativa de criptomonedas en su billetera. ¿Cuánto es “una cantidad significativa”? Ese número es diferente para todos.
Pienso en ello de la misma manera que lo haría con mi billetera física: nunca guardo más de lo que estoy dispuesto a perder en una noche de fiesta.


TIP

Yoroi es una billetera caliente que se conecta a su navegador favorito. Es simple, rápido y seguro. IOHK creó Yoroi como parte de su producto EMURGO y sigue las mejores prácticas de software en la industria. IOHK también ha realizado auditorías de seguridad integrales. Yoroi es un excelente lugar para comenzar con ADA. La billetera se puede usar como su billetera diaria para Cardano.

Paso 1: obtenga su billetera ADA

El primer paso es obtener una billetera para mantener su ADA. Sigue estos pasos:

1. Vaya al sitio web de Yoroi en https://yoroi-wallet.com.
2. Haga clic en Descargar y elija su navegador preferido.

   Serás dirigido a una nueva página.


TIP

   Si está utilizando el navegador Brave, seleccione la opción Chrome; funcionará para Brave.

3. Desde la nueva página, haga clic en el botón Agregar al navegador y haga clic para agregar la extensión.

Paso 2: Asegúrate de no perder tu billetera

Después de agregar Yoroi a su navegador, puede acceder a él desde el ícono de extensión de su navegador. En los siguientes pasos, realiza algunas configuraciones en su billetera.

1. Abra su navegador.
2. Haga clic en el icono de la extensión.
3. Seleccione el icono de Yoroi.

   Se abre una nueva página.

4. Haga clic en Continuar.
5. Lea y acepte los términos de uso.
6. Haga clic en Continuar.
7. Haga clic en Permitir URL de pago de Cardano.
8. Haga clic en Permitir nuevamente.
9. Haga clic en Finalizar.

¡Gran trabajo! Ahora está listo para configurar su billetera.

Paso 3: Configuración de su billetera Yoroi

Si acaba de terminar la sección anterior, debe tener su navegador abierto en una página de Yoroi para crear y restaurar billeteras. Si no está en esa página, haga clic en la extensión Yoroi en su navegador. Luego siga estos pasos para configurar y asegurar su billetera Yoroi:

1. Haga clic en Crear billetera.
2. Haga clic en Cardano.
3. Haga clic en Crear billetera.
4. Asigne un nombre a su billetera y cree una contraseña única.


REMEMBER

Escriba su contraseña en una hoja de papel y guárdela en algún lugar que no pueda olvidar. ¡Si pierdes tu contraseña, pierdes tu dinero!

5. Haga clic en Crear billetera personal y haga clic en la página de advertencia.
6. Escriba su frase inicial en orden en una nueva hoja de papel limpia.
7. Haga clic en Sí, lo he escrito.
8. Vuelva a ingresar su frase inicial en orden.
9. Haga clic en la página de advertencia y haga clic en Con rmar.

¡Felicidades! Su billetera ha sido configurada y asegurada. Considere plastificar los papeles en los que escribió su contraseña y frase inicial. Trate la contraseña y la frase semilla con tanto cuidado como lo haría con el dinero que asegura su billetera.

Paso 4: Conseguir algo de ADA

Ahora que tiene una billetera segura, puede comprar algo de ADA. Esta sección comienza con la página que dejó en la sección anterior. Si cerró su navegador, ábralo nuevamente y haga clic en la extensión del navegador Yoroi. Luego sigue estos pasos:

1. Navegue a su billetera Yoroi.
2. Haga clic en la flecha desplegable en la esquina superior derecha de su billetera Yoroi.
3. Seleccione Comprar ADA.
4. Seleccione la dirección de su billetera ADA.
5. Ingrese la cantidad de ADA que desea comprar.
6. Haga clic en Acepto los Términos de uso y haga clic en Intercambiar.
7. Haga clic en Continuar.

8. Haga clic aquí para redirigir

   Se le dirige a un proveedor de pago externo llamado Moonpay.

9. Introduzca su dirección de correo electrónico.

10. Obtenga el código de verificación de su correo electrónico e ingréselo en el Página de Moonpay.

11. Acepte los términos de uso y haga clic en Continuar.

12. Introduzca sus datos y haga clic en Continuar.

13. Haga clic en el resto de las páginas para completar la transacción.


TIP

Si se encuentra en una región que Moonpay no admite, puede comprar ADA a través de Coinbase (www.coinbase.com) u otro intercambio.

Paso 5: Apostar su ADA

Ahora que tiene un saldo de ADA en su billetera, puede apostar su ADA. Apostar su Ada le permite recibir ADA adicional y ayuda a mantener saludable la red de Cardano. Sigue estos pasos:

1. Navegue a su billetera Yoroi.

2. Haga clic en la pestaña Lista de delegación.

3. Seleccione un grupo de apilamiento.

   Al seleccionar un grupo de apilamiento, preste atención al costo fijo y al retorno de los activos (ROA). El ROA es el rendimiento porcentual de ADA. El ROA de cada grupo es diferente.

4. Ingrese la cantidad que le gustaría apostar.

5. Ingrese la contraseña de su billetera.

6. Haga clic en Delegar.

Puede verificar su ADA apostado haciendo clic en la pestaña Transacciones en su billetera Yoroi.

¡Felicidades! Ha asegurado con éxito su billetera, comprado ADA y configurado para ganar ADA a través de un grupo de participación delegado.

Creación de contratos inteligentes con Marlowe

Los contratos inteligentes son programas que se pueden construir en cadenas de bloques; a menudo se utilizan para automatizar varios procesos. Sin embargo, la creación e implementación de contratos inteligentes generalmente requiere un desarrollador experto y puede ser complejo y costoso, ya que a menudo están escritos en lenguajes de programación especializados.

Marlowe es un conjunto de productos que facilita la creación de contratos inteligentes en la cadena de bloques de Cardano, incluso para personas que no son programadores experimentados. Marlowe incluye un conjunto de plantillas preprogramadas que se pueden usar con soluciones de código bajo o sin código, así como un lenguaje de programación llamado Plutus que se puede usar para escribir contratos en JavaScript. Marlowe también tiene una herramienta llamada Blockly que permite a los usuarios crear contratos simplemente arrastrando y soltando bloques prediseñados.

En este tutorial, utilizará las herramientas sin código de Marlowe para crear contratos inteligentes en la cadena de bloques de Cardano. Sigue estos pasos:

1. Vaya a https://marlowe-finance.io.
2. Haga clic en Ejecutar Marlowe.
3. Haga clic en Probar demostración.
4. Haga clic en Generar billetera de demostración.
5. Ponle nombre a tu billetera.
6. Haga clic en Conectar billetera.


TIP

Ahora está configurado para hacer una demostración sin código en Marlowe Run.

En el tablero de Marlowe Run, tiene tres opciones para contratos inteligentes. En los siguientes pasos, usará la plantilla Préstamo, pero los otros dos también son fáciles de usar y debería probarlos más adelante.

7. Haga clic en el botón Elegir una plantilla.
8. Seleccione Préstamo.
9. Haga clic en Configuración.
10. Nombre su contrato PRUEBA.
11. Nombre las partes de su contrato.
12. Introduzca 5 en el campo Interés.
13. Introduzca 100 en el campo Importe del préstamo.

14. Haga clic en Revisar.

Ahora ha establecido los términos de su préstamo y puede ejecutar el contrato.

15. Haga clic en el botón Pagar y comenzar.

16. Haga clic en Depósito para el prestamista.

17. Haga clic en Depositar nuevamente.

Ahora que los fondos han sido transferidos, tienen unos minutos para depositar el monto más los intereses nuevamente en su cuenta.

18. Haga clic en Depósito para el prestatario.

19. Haga clic en Depositar nuevamente.

Ahora puede explorar algunas de las otras herramientas que ha creado el equipo de Marlowe. Sugiero la herramienta de creación de contratos inteligentes llamada Playground como su próximo paso.

EN ESTE CAPÍTULO

Capítulo 7

Encontrando el lunar cadena de bloques

La cadena de bloques de Polkadot ahora se denomina protocolo de capa-0. Una capa-0 El protocolo es responsable de mantener la integridad y seguridad de la estructura de datos subyacente y de hacer cumplir las reglas y el mecanismo de consenso. anismos que gobiernan el sistema.

La cadena de bloques de Polkadot proporciona la infraestructura subyacente para crear aplicaciones descentralizadas (dApps) y otros sistemas distribuidos encima de ellas. En el caso de Polkadot, es un blockchain de mini blockchains especializados. Polkadot también es una cadena de bloques verde que utiliza un nuevo tipo de consenso llamado prueba de participación nominada.

Polkadot y sus ecosistemas en constante crecimiento están evolucionando rápidamente. Pero a pesar de este rápido crecimiento, la plataforma tiene algunas herramientas increíblemente accesibles y fáciles de usar. La fácil accesibilidad de Polkadot ha ayudado a impulsar su popularidad y uso.

En este capítulo, explico cómo obtener DOT, la criptomoneda nativa de Polkadot, y cómo convertir su DOT en más DOT. Para ello, participe en un grupo, vote sobre proyectos comunitarios y nomine validadores para la red.

Después de leer este capítulo, no solo tendrá un profundo conocimiento práctico de la cadena de bloques de Polkadot, sino que probablemente tendrá más DOT que al principio.
Con esta información, comprenderá mejor las implicaciones de desarrollar Polkadot e invertir en DOT. Esto le ahorrará tiempo y dinero mientras explora
otras cadenas de bloques.

Comprender el ecosistema Polkadot de cadenas especializadas

Polkadot fue fundado por Gavin Wood, cofundador y exdirector de tecnología (CTO) de Ethereum e inventor del lenguaje de contrato inteligente Solidity.
Gavin comenzó a trabajar en Polkadot en 2016 como una versión fragmentada de Ethereum. (Dividir, por cierto, dentro de este contexto significa distribuir datos).

En 2017, Gavin fundó Web3 Foundation (W3F), una entidad sin fines de lucro creada para apoyar la investigación y el desarrollo de Polkadot y recaudar capital para construirlo.
W3F recaudó $145 millones en dos semanas a través de una venta de fichas y eligió a la empresa de desarrollo de Gavin, Parity Technologies, para crear Polkadot. Esto tenía mucho sentido, dado que Gavin había diseñado el sistema blockchain y estaba en la mejor posición para ejecutar su desarrollo.

Diez días después de este aumento sustancial de capital, un error de billetera multi-sig congeló $ 90 millones de ETH de la venta de tokens de Polkadot. A pesar de la pérdida masiva, Polkadot y W3F avanzaron y alcanzaron los hitos de desarrollo. W3F recaudó $ 60 millones adicionales en una venta de tokens en 2019. Estos fondos se han destinado a perfeccionar la implementación de la red y respaldar el crecimiento del ecosistema.

El primer lanzamiento significativo de Polkadot fue en 2019 con el lanzamiento de Kusama, una red de prueba de alto funcionamiento que fue diseñada para ampliar y forzar la gobernanza, el replanteo y la fragmentación en el uso real.

De lo que el equipo de Polkadot aprendió de Kusama, creó la primera red principal cadena candidata, Fase 1, que se lanzó en 2020. Operaba como una red de prueba de autoridad (PoA) administrada por seis validadores controlados por W3F. (Las cadenas de bloques para bebés son vulnerables y necesitan muchas actualizaciones a medida que se levantan).
La red principal hizo la transición a la prueba de participación nominada (PoS) más tarde ese año como planificado. Polkadot también desbloqueó la funcionalidad de gobierno y el control del protocolo se entregó a la comunidad. Ahora W3F financia iniciativas de ecosistemas y respalda proyectos basados en Polkadot.

Profundizando más en Polkadot:
La cadena de bloques de las cadenas de bloques

Polkadot es un bloque de construcción fundamental para las aplicaciones Web 3.0 que permite a los desarrolladores crear aplicaciones privadas y seguras que no dependen de terceros. Se considera un protocolo de capa 0 y una red multicadena. Las redes multicadena no son nuevas en el espacio de la cadena de bloques.

La red de cadena de bloques de Polkadot se diseñó para admitir subcadenas interconectadas y específicas de la aplicación. La idea detrás de esto es que cada cadena podría especializarse y equiparse en relación con la aplicación para la que se estaba utilizando y también poder comunicarse con otras aplicaciones que necesitaban backends de blockchain.
El objetivo de Polkadot era habilitar la escalabilidad al permitir que cadenas de bloques especializadas se comunicaran con otras en un entorno seguro y libre de confianza.

Utiliza un modelo fragmentado donde las transacciones se procesan en paralelo en lugar de secuencialmente. Polkadot es la cadena principal del sistema. Para hacerlo un poco confuso, la cadena principal de Polkadot se conoce como cadena de relevo. Entonces, si estás leyendo
sobre Polkadot en otro lugar, y ves cadena de retransmisión, cadena principal o Polkadot, lo más probable es que se refieran a lo mismo.

En lugar de que todas las aplicaciones se conecten y compartan el mismo libro mayor (la forma en que funciona Bitcoin, por ejemplo), Polkadot utiliza una estructura llamada parachains (abreviatura de cadenas paralelas). Las paracadenas definen su lógica e interfaz, y la cadena de retransmisión
los validadores lo ejecutan. Polkadot es la primera cadena de bloques completamente fragmentada que divide el datos en particiones más pequeñas, conocidas como fragmentos. Los fragmentos comprenden sus propios datos distintivos e independientes.

En Polkadot, cada fragmento aloja la lógica central, los fragmentos se ejecutan en paralelo y Polkadot puede enviar mensajes asincrónicos entre fragmentos. Sin embargo, cada Polkadot
shard (o, en la terminología de Polkadot, parachain) tiene una función de transición de estado única (STF). Las aplicaciones pueden existir dentro de un solo fragmento o entre fragmentos usando
la misma lógica. El STF de un fragmento puede ser abstracto si los validadores en Polkadot pueden
ejecútelo dentro de un entorno WebAssembly (Wasm). Mientras cada una de las paracaídas de Pol kadot siga la misma lógica y reglas, funcionarán y hablarán con otras paracaídas.

Polkadot también se centra en el desarrollador en su uso del sustrato de Parity Technologies.
marco modular. Lo que significa es que los desarrolladores pueden seleccionar componentes específicos que se adapten a las necesidades de la cadena específica de su aplicación cuando están construyendo su
aplicaciones descentralizadas (dApps). Cadenas de bloques personalizadas construidas sobre Polkadot concéntrese en realizar bien una tarea (como juegos, finanzas o seguros). Esto es un
un poco diferente en el mundo de las cadenas de bloques, donde muchas cadenas de bloques intentan resolver cada problema con las mismas herramientas y almacenar todos los datos en un solo lugar.

Polkadot no admite la funcionalidad de la aplicación; en cambio, proporciona seguridad a las paracadenas, el consenso, la nalidad y la lógica de votación de la red. Esto permite a los desarrolladores contribuir al crecimiento del ecosistema diseñando y contribuyendo a las paracadenas en las que están trabajando.

En las siguientes secciones, me sumerjo en el sustrato, un marco para construir cadenas de bloques. También cubro las paracadenas que gobiernan la red y explico algunas de las reglas que mantienen unida a la red.

Sustrato: El marco de la cadena de bloques de Polkadot

El marco de construcción de blockchain de Polkadot se llama Substrate. Todo basado en sustrato Las cadenas son perfectamente compatibles con Polkadot, lo que significa que todas son interoperables dentro del ecosistema de paracadenas, aplicaciones y otros recursos.

El token nativo de la red Polkadot, llamado DOT, alimenta sus sustratos y cumple varias funciones dentro de la red. Estas funciones incluyen cubrir las tarifas de transacción, apostar, participar en la gobernanza y comprar tragamonedas de parachain. DOT es un componente esencial de la red Polkadot y juega un papel crucial en sus operaciones.

El saldo mínimo requerido para tener una cuenta activa en Polkadot Network es 1 DOT. Si el saldo de su cuenta es inferior a 1 DOT, su cuenta se reducirá.
Cortar es donde la red lleva su DOT. No he encontrado otras cadenas de bloques que limpien las cuentas de polvo (cuentas que tienen saldos muy bajos), por lo que es algo a tener en cuenta con respecto a su propia cuenta.

También es posible que desee tener en cuenta algunos otros requisitos inusuales del DOT:

- La contribución mínima requerida para hacer préstamos colectivos es de 5 DOT; apostando requiere 10 DOT.
- Cuando tenga 20 DOT, puede registrar una identidad en cadena y votar.

Estos mínimos arbitrarios pueden cambiar. Desafortunadamente, la comunidad aún necesita mantenerse al día con la documentación que le permite conocer los requisitos para diferentes actividades.

En las siguientes secciones, cubro las diversas formas en que se utiliza el token nativo de Polkadot, llamado DOT, para potenciar su plataforma descentralizada. Estos incluyen la construcción de cadenas de paracaídas, el staking, la participación en la gobernanza y más. Al comprender el papel del DOT en estos procesos, puede obtener una comprensión más profunda de cómo funciona el ecosistema descentralizado de Polkadot.

Descubriendo paracadenas

Las paracadenas construyen y proponen bloques a los validadores en Polkadot. cada bloque se somete a controles de disponibilidad y validez antes de agregarse. Los nodos son responsables de agregar los nuevos datos y verificar que la información se ajuste a las reglas y sea correcta. Los nodos completos para parachains se denominan intercaladores.

Las intercaladoras juegan un papel crucial en el mantenimiento de las cadenas de paracaídas de Polkadot. Son responsables de recopilar y agregar transacciones de los usuarios y crear candidatos de bloque que luego se utilizan para producir pruebas de transición de estado para los validadores de la cadena de retransmisión. Para cumplir con estos deberes, los cotejadores deben mantener plena nodos tanto para la cadena de retransmisión como para sus respectivas paracadenas, así como para realizar un seguimiento de toda la información necesaria para la autoría del bloque y la ejecución de la transacción. Esencialmente, los recopiladores realizan muchas de las mismas tareas que los nodos PoW para mantener la integridad y funcionalidad de las cadenas de paracaídas.

Polkadot une parachains y ofrece compatibilidad bidireccional para que las transacciones puedan ujo entre diferentes paracadenas. El formato de mensajería de consenso cruzado (XCM) permite que las paracadenas envíen mensajes de cualquier tipo a otras paracadenas. Este Así es como Polkadot ha creado un modelo multicadena con una infraestructura robusta para que diferentes dApps puedan comunicarse sin problemas mensajes y valor entre sí.

He aquí una forma simplificada de ver esto: Polkadot es la principal fuente de información, verdad y lógica. También genera subcadenas con herramientas especializadas y lógica adaptada a sus aplicaciones. Pegando todo el aire hay capas de nodos de validación que aseguran que todo funcione sin problemas.

Ver qué prueba de participación nominada tiene que ofrecer

La prueba de participación (PoS) se presentó por primera vez en un artículo de Sunny King y Scott Nadal en 2012. Se propuso como una forma de abordar las ineficiencias del mecanismo de consenso de prueba de trabajo (PoW) y reducir los recursos computacionales necesarios para ejecutar una red de cadena de bloques. PoS se basa en la existencia de una participación real en el ecosistema y se ha convertido en uno de los mecanismos de consenso más populares para las redes blockchain, dado el impulso de una infraestructura más verde.

La distinción entre PoW y PoS es que, mientras que PoW requiere que los mineros gastar energía para resolver problemas matemáticos complejos para validar transacciones en la red blockchain, PoS no requiere "trabajo". En cambio, con PoS, los usuarios necesitan demostrar que poseen una cierta cantidad de criptomonedas. La propiedad implica que tienen un interés creado en garantizar que todas las transacciones sean válidas.

El beneficio de usar PoS sobre PoW es que no requiere ningún gasto de energía o recursos computacionales significativos. Esto significa usar PoS en lugar de PoW puede reducir significativamente los costos asociados con el funcionamiento de una red blockchain. Además, debido a que los usuarios no necesitan plataformas mineras costosas o grandes cantidades de electricidad para participar en actividades de participación, es más accesible que la minería para usuarios ocasionales que no pueden pagar las plataformas mineras. Finalmente, porque tantos los usuarios están apostando monedas en lugar de que solo unos pocos mineros realicen el trabajo, se crea más diversidad dentro del sistema, lo que conduce a una mayor seguridad y estabilidad en general, al menos en teoría.

La prueba de participación es un mecanismo de consenso cada vez más popular para blockchains debido a su conveniencia y ahorro de costos en comparación con otras opciones como la prueba de trabajo. Al exigir a los usuarios que demuestren que poseen una cantidad particular de tokens de criptomoneda nativos de su red, se reducen los costos asociados con el funcionamiento de una red de cadena de bloques y, al mismo tiempo, se crea una mayor diversidad dentro de su ecosistema, lo que conduce a una mejor seguridad y estabilidad en general. Por estas razones, muchas otras redes de cadenas de bloques están comenzando a utilizar este mecanismo de consenso en lugar de métodos tradicionales como PoW. Ethereum es un notable nuevo usuario de PoS. para sitio web propietarios y entusiastas de las criptomonedas que buscan una forma eficiente de participar en redes distribuidas sin desperdiciar recursos significativos de energía o dinero en plataformas mineras y facturas eléctricas, PoS ofrece una solución atractiva.

Polkadot tiene un PoS único llamado prueba de participación nominada (NPoS). El NPoS incentiva a los titulares de DOT para que participen en la operación diaria de la red eligiendo los nodos de validación, votando en el negocio de la red y apostando activos.

Los titulares de DOT tienen derecho a seleccionar nodos que validen las transacciones de la red. Los titulares de DOT que seleccionan nodos se conocen como nominadores; un nominador debe tener un mínimo de 10 DOT para nominar. Los nodos se denominan validadores. Un valor dator indica su intención de ser un candidato a validador. Todas las candidaturas están hechas público, y los nominadores luego envían una lista de hasta 16 candidatos que apoyan. Polkadot distribuye la participación entre los validadores seleccionados para maximizar la seguridad económica de la red. En Polkadot, en el momento de escribir este artículo, hay un máximo de 1000 validadores.

Para incentivar a los nominadores y validadores a actuar en el mejor interés de la red, el mecanismo de prueba de participación nominada (NPoS) de Polkadot permite que La participación de ambas partes se reducirá drásticamente si se involucran en un comportamiento que dañaría la red. (La reducción es cuando la red les quita una parte de su DOT). Al crear consecuencias económicas reales por el mal comportamiento, NPoS alienta a los nominadores y validadores a trabajar hacia la estabilidad y seguridad general de la red.

Ponerse en marcha en Polkadot

Debe comprar al menos 11 DOT para configurar una cuenta y participar en apostar y al mismo tiempo asegurarse de que Polkadot no elimine su cuenta por tener menos de 1 DOT. La forma más fácil de obtener DOT es comprando algunos en su intercambio favorito, como Coinbase (www.coinbase.com). En el momento de escribir este artículo, 11 DOT cuestan aproximadamente $60 (pero este número varía).


REMEMBER

Si necesita ayuda para comprar DOT, vaya al Capítulo 3. Allí encontrará instrucciones detalladas sobre cómo configurar su cuenta y conectarse a Coinbase u otro intercambio.

Una vez que haya obtenido algo de DOT, estará listo para configurar una extensión de navegador que actuará como firmante e inyección de cuenta básica. La extensión del navegador lo protegerá contra todos los sitios de phishing informados por la comunidad y facilitará un poco el uso de su DOT. Antes de continuar con las siguientes secciones, tome dos piezas limpias de papel y un bolígrafo que no se corra, y asegúrese de tener al menos 11 DOT listos para transferir.

Paso 1: Descargue la extensión del navegador DOT

La extensión recomendada para DOT es la extensión Polkadot{.js}. Esta extensión inyecta los datos de la cuenta y permite la firma de mensajes y transacciones sin poner los secretos de la cuenta a disposición de las aplicaciones que llaman.
Siga estos pasos para configurar la extensión Polkadot{.js}:

1. Usando el navegador web Brave (disponible en https://brave.com), vaya a https://polkadot.js.org/extension.
2. Haga clic en Descargar para Chrome.
3. Haga clic en Agregar a Brave.
4. Haga clic en Agregar extensión.

Ahora que ha instalado la extensión del navegador Brave, la configurará para usarla en Polkadot en la siguiente sección.

Paso 2: Con guración de la extensión del navegador DOT

Siga estos pasos para configurar la extensión y agregar DOT a su nueva dirección:

1. En el navegador web Brave, haga clic en el icono Extensiones.
2. Haga clic en Lunares{.js}.
3. Lea la advertencia y haga clic en Entendido.
4. Haga clic en el signo más (+) para agregar una cuenta.
5. Escriba su semilla mnemotécnica de 12 palabras.
6. Asigne un nombre a su cuenta y cree una contraseña única.
7. Escriba su contraseña en otra hoja de papel para guardarla.
8. Haga clic en el icono de engranaje.
9. En Mostrar formato de dirección, seleccione su cuenta.
10. Haga clic en la Cadena de retransmisión de Polkadot.

Ahora que su extensión Polkadot{.js} está configurada, es hora de transferir en algún DOT. Para hacer esto, debe recuperar su nueva dirección de su extensión Polkadot{.js} e iniciar una transferencia desde el intercambio donde compró su DOT. Si necesita orientación sobre cómo hacer esto, consulte el Capítulo 3. Una vez que se complete la transferencia y su DOT se haya transferido a su nueva dirección, estará listo para apostar su DOT en la red de Polkadot en el siguiente paso.

Paso 3: unirse a un grupo de nominaciones

En este paso, apuestas tu DOT para ganar más DOT. Como mencioné anteriormente, Polkadot tiene un consenso NPoS en el que los nominadores seleccionan una red descentralizada de validadores para proteger todo el ecosistema multicadena de Polkadot. Para ayudar a proteger la red, se le recompensará con una fracción de la recompensa del bloque. El grupo de nominación le permite arriesgar menos DOT. Tampoco tiene que administrar sus nominaciones.

Puedes unirte a un grupo de nominaciones con 10 DOT. Los miembros del grupo dividen las recompensas y las penalizaciones proporcionalmente.

La documentación antigua que puede ver en línea dice que el mínimo es 1 DOT. Esto ya no es cierto y puede cambiar en el futuro.

Siga estos pasos para unirse a un grupo de nominaciones:

1. Vaya a https://polkadot.js.org/apps/#/staking.
2. Seleccione Piscina en la barra de navegación.

   Tendrá muchas opciones, así que tómese un momento para revisar algunas de ellas. Mirar hacia vea si el grupo está "abierto" y asegúrese de que haya seleccionado 16 validadores como mínimo.

3. Seleccione un grupo para unirse.
4. Ingrese la cantidad de DOT que asignará al grupo y haga clic en Unirse.

   Preste atención a las tarifas de transacción antes de firmar.

5. Haga clic en Firmar y enviar.
6. Introduzca su contraseña en la nueva ventana que aparece.

Los fondos nominados a un grupo no serán visibles en el saldo de su cuenta en la interfaz de usuario de Pol kadot JS Apps. Esto se debe a que sus fondos se transfieren a la cuenta del fondo común. Nadie puede acceder a esta cuenta del grupo, incluido el operador del grupo, solo la lógica interna del grupo puede acceder a la cuenta.

Después de apostar su DOT en un grupo, puede reclamar su parte de las recompensas obtenidas en las eras desde que se unió. Cada era tiene 24 horas de duración. En las siguientes secciones, usted reclama su DOT recompensado del grupo que usó en la sección anterior.

Paso 4: reclamar sus recompensas

En esta sección, retira sus fondos del grupo y reclama su parte de las recompensas. Puede salir de la piscina en cualquier momento, pero si sale de una piscina, estará sujeto a un período de desvinculación de 28 días en Polkadot.

El período de desvinculación es la cantidad de tiempo que debe pasar antes de que una persona pueda retirar su participación de una red o grupo de blockchain. En este caso, el período de desvinculación es de 28 días, lo que significa que una persona debe esperar 28 días antes de poder retirar su participación. Esto a menudo se implementa como una medida de seguridad para garantizar que las personas no muevan rápidamente su participación dentro y fuera de la red, lo que podría dañar la estabilidad y la seguridad de la red.
El período de desvinculación puede variar de una red blockchain a otra y, a menudo, lo establecen los mecanismos de gobierno de la red.

1. Vaya a https://polkadot.js.org/apps/#/staking/actions.
2. Haga clic en Cuentas.

3. Haga clic en Agrupados.

Esto muestra el grupo y los DOT que apostaste.

4. Debajo de los grupos enumerados en la página, haga clic en el icono de tres puntos a la derecha.

5. Seleccione Retirar sin garantía.

6. Seleccione Retiro reclamable (si tiene alguna recompensa para reclamar).

7. Haga clic en las ventanas emergentes hasta que termine.

En las siguientes secciones, descubrirá cómo se usa DOT para gobernar la red Polkadot.

Descubriendo la Gobernanza en Polkadot

Polkadot tiene un mecanismo de gobernanza que le permite evolucionar en la dirección de sus partes interesadas. También tiene una democracia económica que permite a cada uno una voz ponderada por la cantidad de DOT que controlan. En este momento, necesitas más y más DOT incluso para tener una voz en Polkadot, pero con suerte thisaw lo hará.
ser rectificado para que la red sea accesible a todos los que deseen participar. El
Sin embargo, el objetivo de los fundadores parece ser benévolo: quieren asegurarse de que el
las partes interesadas siempre pueden controlar la red.

Una de las formas en que Polkadot ha trabajado para garantizar el control de las partes interesadas es cómo la red utiliza varios mecanismos de votación en cadena, como referéndums con umbrales adaptativos de mayoría calificada y votación de aprobación por lotes. Ponderado por participación los referéndums se utilizan para hacer todos los cambios al protocolo. Esto significa que todos los cambios en el funcionamiento de la red se someten a votación de las partes interesadas. Los fundadores de Polkadot incorporaron muchas lecciones de las guerras anteriores de blockchain que sufrieron Bitcoin y Ethereum. Las peleas por la estructura y la utilidad de las redes llevaron a la fractura de esas redes, a menudo entre titulares de tokens, operadores de nodos, desarrolladores de dApp y desarrollo central. (Puede obtener más información sobre el
la historia y los desafíos de esas redes a lo largo de este libro).

Polkadot tiene una forma relativamente civilizada y organizada de equilibrar las necesidades de todas las partes interesadas. Por ejemplo, todos los poseedores de tokens activos y el consejo de Polkadot colaboran para administrar cualquier decisión de actualización de la red. Los tenedores de fichas públicas o el consejo pueden hacer una propuesta, pero tiene que pasar por un referéndum para dar tiempo a que todas las partes interesadas decidan. Cada voto es ponderado por la cantidad de DOT que el individuo controla.

Hay cuatro tipos de referendos:

» Propuestas presentadas públicamente

» Propuestas presentadas por el consejo

» Promulgación de un referéndum previo

» Propuestas de emergencia del comité técnico

En las siguientes secciones, se sumerge en la mecánica de los referéndums y su papel en el gobierno de Polkadot.

Proponer un referéndum

Cualquiera, incluido usted, puede proponer un referéndum. Depositas el minimo cantidad de tokens por un período determinado y si alguien respalda la propuesta, puede depositar la misma cantidad de tokens para apoyarlo. Las propuestas con el mayor número de simpatizantes vinculados se seleccionan para el siguiente ciclo de votación. Su los tokens vinculados se liberarán después de que la propuesta se someta a votación.

Cada 28 días se votan nuevos referendos. Hay dos colas, una para propuestas aprobadas por el consejo y otra para propuestas presentadas públicamente. El referéndum sobre el que se votará alterna entre la propuesta superior de las dos colas. La propuesta superior es la que tiene la mayor participación en bonos detrás de ella. Emergencia los referéndums tienen prioridad y se votan de inmediato.

Si vota, debe guardar sus tokens hasta después de que se haya promulgado el referéndum. Esta política está destinada a disuadir la venta de votos.

En las siguientes secciones, utilizará su DOT para participar en la gobernanza de la red Polkadot y opinar sobre su dirección futura. También descubres cómo emita sus votos en varias propuestas y desempeñe un papel en la configuración del futuro de la plataforma descentralizada.

Democracia blockchain en acción

En esta sección, averigüe cómo votar en los referéndums esenciales que se están poniendo adelante en la cadena de bloques de Polkadot. Para seguir estos pasos, debe tener al menos 2 DOT en su cuenta. Además, prepárese para perder el acceso a los DOT que usará para apostar su voto hasta después de que se promulgue el referéndum. Si aún necesita configurar

la extensión de su navegador Polkadot, vuelva a la sección "Puesta en funcionamiento en Polkadot" para configurarlo.

1. Vaya a https://polkadot.js.org/apps/#/democracy.
2. Revisar los referendos actuales que están sujetos a votación.

   Al hacer clic en cada uno, puede revisar el número de días que le quedan y cuántas personas han votado.
3. En el lado derecho de la pantalla, haga clic en el botón Votar.
4. Seleccione Vote No o Vote Aye como desee.
5. Haga clic en Firmar y enviar.

¡Felicidades! Acabas de votar y, al hacerlo, apoyaste el sistema ecológico de Polkadot. Su voto ayudó a dar forma al futuro de la red y le ha permitido
seguir evolucionando a través de un nuevo tipo de democracia en línea.

Nombrar a sus validadores

Uno de los roles más críticos dentro de la red Polkadot es el de validador.

Los validadores son los encargados de mantener los nodos de la red en consenso (es decir, todos los nodos están de acuerdo con la misma realidad). Lo hacen verificando las transiciones de estado. Al momento de escribir este libro, el número de validadores está limitado a 1000, pero Polkadot puede actualizar este número en el futuro. Además, aunque su objetivo es 1000 validadores, es posible que no consigan tantos. ¿Por qué? Aquí hay algunas razones:

» Los validadores son responsables de estar en línea y ejecutar fielmente sus tareas las 24 horas del día, los 7 días de la semana, sin tiempo de inactividad. Eso es un gran compromiso.

» Ser validador significa recibir un pago de la red. Dividir demasiado este pago podría desincentivar la participación o incluso introducir una nueva teoría del juego que centralice la red.

» Los validadores tienen que arriesgar su propio capital. La apuesta mínima para ser elegido como validador activo es dinámica y cambia con el tiempo, pero mientras escribía esto, había alrededor de 600 validadores, y el DOT apostado valía más de $2000 en la mayoría de ellos. El equipo de Polkadot planea cambiar esto a medida que crece la red.

» Los validadores deben proteger sus claves de firma de terceros. Por aquí, los atacantes no pueden tomar el control y cometer un comportamiento recortable que les provoque perder su depósito.

Cortar es donde la red toma todo o una parte del DOT por mal comportamiento.

REMEMBER

Si desea echar un vistazo a los validadores en Polkadot, puede verlos todos y la cantidad que cada uno ha arriesgado personalmente en https://ipfs.io/ipns/polkadot.dotapps.io/#/replanteo/objetivos.

En las siguientes secciones, descubra cómo ganar DOT como recompensa por la red. participación como nominador. Como nominador, usted es responsable de seleccionar validadores confiables. Al momento de escribir esto, necesita 176 DOT para completar este tutorial y ganar una recompensa. Todavía puede nominar a un validador si tiene al menos menos 10 DOT para unir.

WARNING

Antes de comenzar, tenga en cuenta que puede perder una parte de su DOT apostado si un validador elegido se porta mal.

Si aún necesita configurar su extensión web para Polkadot y obtener algo de DOT, diríjase a la sección "Primeros pasos en Polkadot", anteriormente en este capítulo.

En las siguientes secciones, descubrirá el panel de control de participación de Polkadot y lo utilizará para administrar su DOT.

Paso 1: Conectarse al panel de staking

Para acceder al tablero para hacer staking y usar su Polkadot{.js} para iniciar sesión, siga estos pasos:

1. Vaya a https://staking.polkadot.network/#/overview.
2. Haga clic en Conectar.
3. Seleccione su cuenta de Polkadot{.js}.
4. Haga clic y acepte el aviso que aparece con un descargo de responsabilidad.
5. Haga clic en Conectar nuevamente y seleccione su dirección.

Paso 2: Nombrar un validador de Polkadot

Para seleccionar un nodo de validación en la red Polkadot, siga estos pasos:

1. Para comenzar, navegue a su tablero desde el paso anterior. En la barra de navegación izquierda, asegúrese de que la red seleccionada sea Polkadot en la opción Red.

   Si no es así, haga clic en la red actual y cámbiela a Polkadot.
2. Haga clic en Nominar en la navegación de la izquierda.
3. Haga clic en Comenzar a nominar.
4. Seleccione su cuenta de controlador.
5. En Destino de la recompensa, seleccione Al controlador.

   Esto volverá a ejecutar los fondos en su cuenta.
6. En Nominar, seleccione Selección óptima y haga clic en Continuar.
7. En Bono, ingrese la cantidad que desea depositar y haga clic en Continuar.
8. Revise el resumen y haga clic en Comenzar a nominar.
9. Verifique su transacción en su cuenta de Polkadot{.js}.

Deberá esperar una era de Polkadot, que es de aproximadamente 24 horas, antes de revisando sus nominaciones.

Puede usar el panel de control para administrar sus otras actividades en Polkadot, como el grupo de participación al que te uniste anteriormente en el capítulo. El tablero tiene una interfaz más fácil de usar que el explorador que usó anteriormente (https://ipfs.io/ipns/polkadot.dotapps.io/#/explorer), pero como también habrá notado, no tiene todos la misma funcionalidad.

EN ESTE CAPÍTULO

» Conociendo a Solana

» Creando una aplicación descentralizada en Solana

» Construyendo una organización autónoma descentralizada en Solana

Capítulo 8

Examinando la Solana cadena de bloques

Los desarrolladores de Solana esperan crear una cadena de bloques escalable, infinitesimales de bajo costo y verde. Solana (SOL) es una de las criptomonedas más populares que se negocian en la actualidad. La empresa de desarrollo detrás de Solana ha recaudado un total de 315,8 millones de dólares en financiación. Dada esta importante financiación, sería prudente vigilar el proyecto Solana; lo más probable es que crezca más que cualquier otro proyecto en el espacio de la cadena de bloques.

La diferencia definitoria entre Solana y Ethereum, y por qué es posible que desee obtener más información sobre el sistema Solana, es el algoritmo de consenso de Solana, un nuevo sistema llamado prueba de la historia.

Este capítulo se sumerge en las aplicaciones prácticas y el futuro de la cadena de bloques Solana y explica los usos de su tecnología. Descubra cómo crear su propia aplicación descentralizada (dApp) y organización autónoma descentralizada (DAO).

Descubriendo Solana

Solana es una plataforma blockchain descentralizada y de código abierto diseñada para ser escalable, rápida y segura. Fue creado en 2017 por Solana Labs, una empresa de desarrollo de software con sede en San Francisco, California.

Una de las principales características de Solana es su alto rendimiento y escalabilidad. Puede procesa una cantidad significativamente mayor de transacciones que otras plataformas populares de cadena de bloques como Ethereum y Bitcoin.

Solana utiliza una combinación de dos mecanismos de consenso para proteger su red: prueba de historial (PoH) y prueba de participación (PoS). Incluso con dos mecanismos de consenso, Solana es energéticamente eficiente y respetuosa con el medio ambiente.

Solana tiene un lenguaje de programación nativo llamado Move, que se usa para escribir contratos inteligentes y aplicaciones descentralizadas (dApps). es de tipo estático lenguaje que está diseñado para ser fácil de aprender y usar mientras que también es altamente seguro.

En general, Solana es una plataforma de cadena de bloques poderosa e innovadora que se adapta bien a muchos casos de uso, incluida la descentralización (DeFi), juegos y gestión de la cadena de suministro.

La prueba de la historia de Solana

Solana es un proyecto de cadena de bloques de código abierto y alto rendimiento que se basa en un algoritmo de consenso único llamado PoH. PoH permite a Solana mantener la hora exacta a través de su red descentralizada, incluso cuando las computadoras que componen la red no confían entre sí. Esto le permite a Solana procesar transacciones rápidamente y de forma segura sin sacrificar la descentralización o la seguridad.

Solana usa PoH para marcar el tiempo de los hashes de bloques anteriores usando un hash criptográfico función. Luego, estas marcas de tiempo se organizan en árboles de Merkle, con cada nodo en el árbol que contiene el hash de sus nodos secundarios. Al compartir estas marcas de tiempo con otras computadoras en la red, cada computadora puede construir un "historial" de lo que ha sucedido en la red a lo largo del tiempo.

Esta estructura de datos tiene dos ventajas sobre las arquitecturas tradicionales de blockchain:

- Reduce los requerimientos de almacenamiento. Cada nodo necesita realizar un seguimiento de solo una pequeña cantidad de datos (los hashes de bloques anteriores).
- Acelera la sincronización. Cada nodo necesita descargar solo una pequeña cantidad de datos (las marcas de tiempo) de otros nodos en lugar de descargar todo el historial de la cadena de bloques.

Solana afirma procesar 710 000 transacciones por segundo en una red antagónica, lo que la convierte en una de las plataformas de cadena de bloques más rápidas del mundo. Es único El algoritmo de consenso y las capacidades de alto rendimiento lo hacen adecuado para casos de uso como la gestión de la cadena de suministro y la verificación de identidad.

El PoH de Solana es un mecanismo de consenso único que permite que la cadena de bloques de Solana para lograr un alto rendimiento de transacciones y tarifas de transacción bajas. Funciona usando una función de retardo verificable (VDF) para asegurar la red, en lugar de depender de PoW como lo hacen muchas otras plataformas de blockchain.

En un sistema PoW, los mineros compiten entre sí para resolver acertijos matemáticos complejos con el fin de validar las transacciones y agregarlas a la cadena de bloques. Este El proceso consume mucha energía y puede ser lento, lo que lo hace difícil de escalar. En Por el contrario, el sistema PoH de Solana utiliza un VDF para seleccionar aleatoriamente los validadores (llamados nodos de validación) que agregarán el siguiente bloque de transacciones a la cadena de bloques.

El VDF es una función criptográfica que lleva mucho tiempo calcular, pero es fácil para verificar después de haber sido calculado. Esto significa que los nodos validadores pueden usar el VDF para generar números aleatorios de una manera segura y verificable por el resto de la red. Los nodos de validación utilizan estos números aleatorios para determinar qué nodo agregará el siguiente bloque de transacciones a la cadena de bloques.

Este proceso es mucho más eficiente que PoW, porque no requiere mineros competir entre sí y consumir grandes cantidades de energía. También permite un rendimiento de transacción mucho mayor y tarifas de transacción más bajas, lo que lo hace ideal para aplicaciones descentralizadas a gran escala. Además, porque el VDF es fácil de verificar, la red Solana puede llegar a un consenso rápido y de forma segura

EL HOMBRE DETRÁS DE LA PRUEBA DE LA HISTORIA

En noviembre de 2017, Anatoly Yakovenko publicó un documento técnico sobre PoH, una técnica para mantener el tiempo entre computadoras que no confían entre sí. Esta técnica estaba destinada a hacer posible que los sistemas de cadena de bloques escalaran hasta el nivel de los sistemas de pago centralizados como Visa.

Yakovenko implementó la técnica en un código base privado utilizando el lenguaje de programación C. Greg Fitzgerald, un desarrollador central de Solana, alentó a Yakovenko a cambiar al lenguaje Rust, y Yakovenko lo hizo en solo dos semanas. Luego, Fitzgerald comenzó a crear prototipos de la implementación de código abierto del documento técnico de Yakovenko y lo publicó en GitHub con el nombre Silk.

En 2018, el equipo detrás del proyecto creó una empresa llamada Loom. Sin embargo, para evitar confusiones con otro proyecto llamado Loom Network, cambiaron su nombre a Solana y publicaron una red de prueba de 50 nodos que soportaba de manera constante ráfagas de 250 000 transacciones por segundo.

En general, el mecanismo de consenso PoH de Solana es una característica clave que la diferencia de otras plataformas de cadena de bloques y le permite alcanzar altos niveles de escalabilidad y rendimiento.

Ficha nativa de Solana

SOL es el token nativo de la plataforma Solana. Se puede usar para pagar nodos en un clúster de Solana para ejecutar programas en cadena o validar su salida. El sistema también utiliza micropagos llamados lamports, que son fracciones de un SOL. Estos lamports llevan el nombre de la mayor influencia técnica de Solana, Leslie Lamport, una famosa científica informática estadounidense. Cada puerto tiene un valor de 0.000000001 SOL.

El valor de SOL está determinado por las fuerzas del mercado, como cualquier otra criptomoneda. SOL se puede negociar en intercambios de criptomonedas y se puede usar para realizar pagos de bienes y servicios en los comerciantes que lo aceptan.

Cuentas en Solana

Las cuentas de Solana son una parte fundamental de la cadena de bloques de Solana, sirviendo como la unidad básica de almacenamiento de datos y código. En muchos sentidos, son herramientas similares en sistemas operativos como Linux, porque pueden almacenar datos persistentes y arbitrarios y se pueden usar en una amplia variedad de formas.

Uno de los usos clave de las cuentas de Solana es almacenar el token nativo de la plataforma, SOL. Al igual que con otras criptomonedas, SOL se puede usar para transferir valor en la red de Solana y se puede comprar y vender en intercambios. Sin embargo, las cuentas de Solana no se limitan solo a tener SOL; también se pueden usar para almacenar estructuras de datos personalizadas y código ejecutable.

Estas estructuras de datos y código se utilizan para crear dApps en la plataforma Solana. Cuando una cuenta contiene código, se puede ejecutar como un programa en la red de Solana, lo que le permite interactuar con otras cuentas y datos en la cadena de bloques. Esto hace que Solana
Accounts es una poderosa herramienta para construir una amplia gama de dApps y sistemas descentralizados.

En general, las cuentas de Solana son una parte esencial del ecosistema de Solana y están involucradas en casi todo lo que los usuarios hacen con la plataforma. Ya sea que esté utilizando SOL para transferir valor, creando una dApp o almacenando datos personalizados, las cuentas de Solana están en el centro de todo.

Alquiler en Solana

Una cosa importante a tener en cuenta sobre Solana es que almacenar datos en cuentas cuesta SOL para mantener. Esto se llama alquiler. La buena noticia es que si mantiene un

saldo mínimo equivalente a dos años de pagos de renta en su cuenta, estará exento del pago de renta. También puede recuperar su alquiler cerrando la cuenta y devolviendo los lamports a su billetera.

Debe pagar el alquiler una vez por época (cada dos días). El costo del alquiler en la cadena de bloques de Solana depende de varios factores, incluido el tamaño de los datos que se almacenan, el tiempo que se almacenarán y la demanda actual de almacenamiento en la red.

En general, el costo del alquiler en la cadena de bloques de Solana se calcula en función de la cantidad de espacio de almacenamiento y la duración que necesita. Puede optar por alquilar el almacenamiento por un período de tiempo específico o puede optar por pagar de forma recurrente.

El costo del alquiler también está influenciado por la oferta y la demanda. Si hay una gran demanda de almacenamiento en la red, el costo del alquiler puede ser mayor. Por el contrario, si hay una menor demanda de almacenamiento, el costo del alquiler puede ser menor.

Es importante tener en cuenta que el costo del alquiler en la cadena de bloques de Solana no está fijado y puede cambiar con el tiempo. Los usuarios deben considerar cuidadosamente sus necesidades de almacenamiento y presupuestar en consecuencia.

Se destruye un porcentaje de la renta recaudada por Solana. El resto de la renta se distribuye en cuentas de votación al final de cada turno. Si su cuenta no tiene suficiente SOL para pagar el alquiler, su cuenta se desasignará y se eliminarán los datos.

Claves públicas y Solana

Las claves públicas, también conocidas como direcciones, son una parte crucial de la cadena de bloques de Solana. Son los identificadores únicos que apuntan a cuentas en la red y son necesarios para interactuar con esas cuentas. Si desea ejecutar un programa o transferir SOL en la red Solana, deberá proporcionar las claves públicas adecuadas para hacerlo.

Las claves públicas en Solana son valores de 256 bits, que normalmente se representan como cadenas codificadas en base 58. Esto significa que están compuestos por una combinación de letras y números, y se ven así:

7C4jsPZpht42Tw6MjXWF56Q5RQUocjBBmciEjDa8HRtp

Estas cadenas son largas y complejas, pero son necesarias para garantizar la singularidad y seguridad de cada clave pública en la red.

Además de utilizarse para identificar cuentas en la red de Solana, las claves públicas se utilizan para verificar la autenticidad de las transacciones. Cuando una transacción se firma con una clave privada, la clave pública correspondiente se utiliza para verificar que el

la transacción es válida y proviene de la cuenta correcta. Esto garantiza la seguridad e integridad de la red Solana.

En general, las claves públicas juegan un papel crucial en el ecosistema de Solana, proporcionando una forma única y segura de identificar cuentas y verificar transacciones. Ya sea que esté ejecutando un programa, transfiriendo SOL o interactuando con una dApp, necesitará usar claves públicas para hacerlo.

Racimos de Solana

Un clúster de Solana es un grupo de computadoras de propiedad independiente que trabajan juntas para verificar la salida de los programas enviados por los usuarios. El clúster se puede utilizar para conservar un registro de eventos y sus interpretaciones programáticas, así como para rastrear la posesión de activos y las computadoras que realizan un trabajo significativo para mantener el clúster.

El clúster de Solana produce un libro de contabilidad, que es un registro de todos los eventos que se conserva durante la vida útil del clúster. Siempre que se mantenga una copia del libro mayor, el resultado de los programas del clúster puede reproducirse y seguirá siendo independiente de la organización que lo puso en marcha.

Ponerse en marcha en Solana

Solana Playground es un entorno de desarrollo integrado (IDE) basado en navegador para Solana. Le permite desarrollar e implementar programas Solana sin tener que instalar ningún software en su computadora. Simplemente abra Solana Playground en su navegador web y estará listo para comenzar a escribir e implementar programas de Solana.

En esta sección, usará Solana Playground para desarrollar e implementar un programa básico de Solana. Esto lo ayudará a comenzar con Solana Playground y le dará una idea de cómo es desarrollar en la plataforma Solana.

Después de esta sección, tendrá una comprensión básica de cómo usar Solana Playground y cómo desarrollar en la plataforma Solana. Esto lo preparará para el éxito a medida que continúe aprendiendo y explorando el mundo del desarrollo de blockchain.

Creando una billetera Playground

Al desarrollar en la plataforma Solana con Solana Playground, no necesita crear una billetera del sistema de archivos con la interfaz de línea de comandos (CLI) de Solana.
En cambio, puede crear una billetera basada en navegador con solo unos pocos clics.

Para configurar su billetera Playground, siga estos pasos:

1. Vaya a https://beta.solpg.io/6314a69688a7fca897ad7d1d.
2. Haga clic en el indicador de estado rojo en la parte inferior izquierda (donde dice No Conectado).

   Aparece una ventana emergente (consulte la Figura 8-1), que le brinda la opción de guardar un copia del par de llaves de su billetera.

WARNING

Su billetera Playground se guarda en el almacenamiento local de su navegador. Si borra la memoria caché de su navegador, se eliminará su billetera guardada. Por lo tanto, es importante asegurarse de guardar una copia local del par de claves de su billetera como respaldo. Esta voluntad asegúrese de que puede acceder a su billetera incluso si necesita borrar su caché.

3. Haga clic en Guardar par de claves.
4. Haga clic en Continuar para crear su billetera.

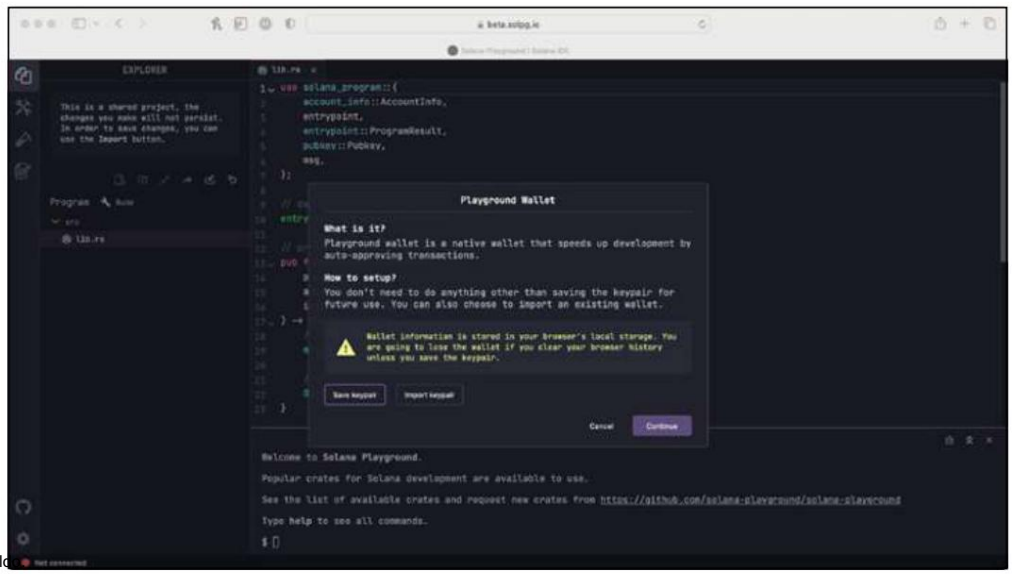


FIGURA 8-1: Decide si deseas guardar una copia local del archivo de par de claves de tu billetera como respaldo.

Después de crear su Playground Wallet, verá la dirección de su billetera, su SOL equilibrio y el grupo Solana al que está conectado en la parte inferior de la pantalla. Por predeterminado, estará conectado al clúster de Devnet, pero también puede conectarse a un validador de prueba localhost si lo prefiere. Considere usar testnest cuando experimente porque es gratis

Creación de un programa Solana

Solana usa Rust, un lenguaje de programación de sistemas que está diseñado para ser rápido, seguro y concurrente. Fue creado en 2010 por Graydon Hoare y está patrocinado por Rust Project, un esfuerzo colaborativo de voluntarios.

El código para su programa Solana basado en Rust se encuentra en src/lib.rsle dentro de Solana Playground. Thisle es donde importará sus cajas de Rust y definirá la lógica de su programa. En Rust, una caja es una biblioteca o binario compilado que se puede usar como una dependencia en otros proyectos de Rust. Las cajas se publican en un registro central de paquetes llamado crates.io, que permite a los desarrolladores descubrir y reutilizar fácilmente el código existente.

La caja del programa solana proporciona las herramientas y la funcionalidad necesarias para desarrollar programas Solana en Rust. El equipo de Solana ha agregado útilmente el código con comentarios en la página cuando lo carga, por lo que es fácil para usted volver a mirarlo para verificar su trabajo.

Importando la caja del programa solana

Siga estas instrucciones para guiarlo a través del proceso de creación de un nuevo programa Rust que use la caja del programa solana .

1. Vaya a https://beta.solpg.io/6314a69688a7fca897ad7d1d.
2. Haga clic en el icono de la esquina superior izquierda para crear una nueva.
3. Asigne el nombre test.rs.
4. Agregue el siguiente código en la parte superior de su archivo test.rs :

```
use solana_program::
        { account_info::AccountInfo,
        punto de
        entrada, punto de
        entrada::ProgramResult, pubkey::Pubkey,
        mensaje,
};
```

El código que acaba de agregar importa la caja del programa solana y trae los elementos necesarios al espacio de nombres local, lo que le permite usarlos en su programa. Con este código en su lugar, está listo para comenzar a escribir la lógica de su programa Solana.

Escribiendo la lógica de tu programa

Cada programa de Solana debe definir un punto de entrada, que le dice al tiempo de ejecución de Solana dónde comenzar a ejecutar su código en cadena. El punto de entrada es una función pública.

denominado process_instruction que toma tres argumentos: program_id, account e instrucción_datos.

Utilizará la función process_instruction para registrar el mensaje "¡Hola, mundo!" a la cadena de bloques y luego salga con gracia con el resultado Ok(()) . Esto le dice al tiempo de ejecución de Solana que el programa se ejecutó con éxito sin ninguna errores

Una vez que haya escrito el código para su programa Solana, puede compilarlo usando la pestaña Build & Deploy en la barra lateral izquierda de Solana Playground.

1. Vaya a https://beta.solpg.io/6314a69688a7fca897ad7d1d.
2. Ingrese este código en el archivo test.rs de la sección anterior:

```
// declara y exporta el punto de entrada del programa entrypoint!
(process_instruction);

// implementación del punto de entrada del programa
pub fn process_instruction( program_id:
        &Pubkey, accounts:
        &[AccountInfo], instrucción_datos:
        &[u8]
) -> ProgramResult { //
        registrar un mensaje en la cadena de bloques
        msg! ("¡Hola, mundo!");

        // salimos con gracia del programa
        De acuerdo(())
}
```

3. Haga clic en el botón Construir.

    Tu programa comienza a compilarse.

Si la compilación es exitosa, verá un mensaje de éxito en la terminal de Playground. Puede recibir algunas advertencias sobre variables no utilizadas, pero estas no afectarán la compilación de su programa; puede ignorarlas con seguridad.

Desplegando su programa

Una vez que haya creado con éxito su programa Solana (consulte la sección anterior), puede implementarlo en la cadena de bloques de Solana usando el botón Implementar (parece una llave inglesa y un martillo) en la pestaña Build & Deploy de Solana Playground. Su programa se implementa en el clúster de Solana seleccionado, como Devnet o Testnet.

Cuando implemente su programa, verá que cambia el saldo de su billetera Playground.
De forma predeterminada, Solana Playground solicitará automáticamente lanzamientos aéreos SOL en su nombre para asegurarse de que su billetera tenga suficiente SOL para cubrir el costo de implementación. Si necesita más SOL, puede lanzar más desde el aire escribiendo solana airdrop en la terminal Play Ground, seguido de la cantidad de SOL que desea lanzar desde el aire, así:

```
Lanzamiento aéreo de solana 2
```

Este comando lanza 2 SOL a su billetera, lo que le permite implementar su programa e interactuar con él en la cadena de bloques de Solana.

Inicializando tu cliente

Usará Solana Playground para crear un cliente para su programa Solana usando el ejecute el comando en el terminal Playground para crear una carpeta de cliente y un archivo client.tsle predeterminado. Aquí es donde trabajará para el resto del programa "¡Hola, mundo!" programa.

Desde donde lo dejó al final de la sección "Escribir la lógica de su programa", ahora está listo para ejecutar su programa.

Paso 1: ejecutar su programa

Para ejecutar su "¡Hola, mundo!" programa, sigue estos pasos:

1. Abra Solana Playground en su navegador web yendo a https://beta.solpg.io.
2. En la terminal Playground, que es la caja negra en la parte inferior de la pantalla, ingrese ejecutar.

En Solana Playground, hay muchas utilidades que están disponibles globalmente para ti para usar sin tener que instalar o configurar nada. Los más importantes para el "¡Hola, mundo!" son web3 para @solana/web3.js y pg para las utilidades Solana Playground. Puede acceder a estas utilidades presionando Ctrl+Espacio (Windows) o +Espacio (macOS) dentro del editor.

ENCONTRAR SU ID DE PROGRAMA

Cuando esté ejecutando un programa Solana utilizando web3.js o desde otro programa Solana, deberá proporcionar el ID del programa, que también se conoce como la dirección pública de su programa. Puede encontrar su ID de programa en la barra lateral Build & Deploy en Solana Playground, en el menú desplegable Credenciales del programa.

Paso 2: Creando tu transacción

Para ejecutar su programa en cadena, debe enviarle una transacción. Cada transacción enviada a la cadena de bloques de Solana contiene una lista de instrucciones y los programas con los que interactuarán estas instrucciones. Para crear una nueva transacción y agregarle una sola instrucción, use el siguiente código:

```
// crea una transacción vacía const
transaction = new web3.Transaction();

// agrega una instrucción de programa hello world a la transacción transacción.add(

    new web3.TransactionInstruction({keys: [],
        programId:
        new web3.PublicKey(pg.PROGRAM_ID), }) );
```

Cada instrucción debe incluir todas las claves involucradas en la operación y el ID del programa que desea ejecutar. En este ejemplo, las teclas están vacías porque su programa solo registra "¡Hola, mundo!" y no necesita ninguna cuenta.

Paso 3: Firma de tu transacción

Una vez que haya creado su transacción, puede enviarla al clúster de Solana usando el siguiente código:

```
// envía la transacción al clúster de Solana console.log("Enviando
transacción..."); const txHash = await
web3.sendAndConfirmTransaction(pg.conexión, transacción,
    [pg.wallet.keypair] );
```

Vale la pena señalar que el primer firmante en la matriz de firmantes es el pagador de la tarifa de transacción de forma predeterminada. En este caso, está firmando con su pg.wallet.keypair.

Ejecutando tu aplicación

Puede usar el comando ejecutar en Solana Playground para ejecutar la aplicación cliente que ha escrito. Una vez que se complete su aplicación, verá un resultado similar al siguiente:

```
Ejecutando cliente...
    cliente.ts:
```

```
Mi dirección: GkxZRRNPfaUfL9XdYVfKF3rWjMcj5md6b6mpRoWpURwP Mi saldo:
5.7254472 SOL Enviando transacción...

Transacción enviada con hash: 2Ra7D9JoqeNsax9HmNq6MB4qWtKPGc
LwoqQ27mPYsPFh3h8wignvKB2mWZVvdzCyTnp7CEZhfg2cEpbavib9mCcq
```

Puede usar solana-cli directamente en Solana Playground para obtener información sobre una transacción. Ejecute el siguiente comando, reemplazando TRANSACTION_HASH con el hash que recibió al llamar a "¡Hola, mundo!" programa:

```
solana confirmar -v TRANSACTION_HASH
```

Deberías ver "¡Hola, mundo!" en la sección Mensajes de registro de la salida.

¡Ahora eres un desarrollador de Solana! Puede intentar actualizar el mensaje de su programa y reconstruir, volver a implementar y volver a ejecutar su programa para ver cómo funciona.

Construyendo un DAO en Solana

Realms es una plataforma en la cadena de bloques de Solana que permite a los usuarios crear y administrar fácilmente DAO. Con Realms, puede crear DAO personalizados, administrar sus miembros, votar propuestas y asignar su tesorería (fondos que ha puesto dentro de un contrato inteligente). La plataforma está diseñada para ser flexible y se puede usar para crear una variedad de diferentes tipos de DAO, incluida la comunidad multisig, token no fungible (NFT) y DAO de token comunitario. Una comunidad NFT podría ser utilizada, por ejemplo, por un artista para ayudarlo a distribuir su musicrst a sus súper fanáticos.

Una DAO usa tokens para otorgar a sus miembros derechos de voto en su gobierno. Por ejemplo, una DAO podría usarse para administrar una organización benéfica.

Realms también sirve como front-end para SPL Governance, un estándar para crear y mantener DAO en Solana que es independiente tanto del tipo de DAO como del tipo de activo.
Esto facilita que los constructores creen DAO que se adapten a las necesidades específicas de sus comunidades.

En esencia, una DAO es una comunidad con una cuenta bancaria compartida que se ejecuta y se rige por contratos inteligentes en una cadena de bloques. Los miembros de un DAO pueden usarlo para tomar decisiones de manera transparente y descentralizada, con contratos inteligentes que ejecutan esas decisiones. Por ejemplo, un miembro puede crear una propuesta que sugiera una inversión de la tesorería de la DAO o una actualización del programa. Luego, los otros miembros de la DAO pueden votar sobre la propuesta, y si un quórum predeterminado vota a favor, la propuesta se acepta y ejecuta mediante un contrato inteligente.

Esta estructura proporciona una estructura organizativa en la que cada miembro de la DAO tiene la misma voz en la dirección de la organización. Esto permite una toma de decisiones más democrática y descentralizada, lo que puede ser beneficioso para una variedad de diferentes tipos de comunidades.

Para configurar su Solana DAO, necesitará dos hojas de papel limpias para escribir su contraseña y frase inicial. También deberá comprar algunos SOL. La compra mínima para mamá con la billetera Phantom es de $50.

Crear una billetera Solana

Para crear una billetera Solana, siga estos pasos:

1. Vaya a https://phantom.app.
2. Haga clic en Descargar.
3. Haga clic en Valiente.
4. Haga clic en Agregar a Brave.
5. Haga clic en Agregar extensión.
6. Haga clic en Crear una nueva billetera.
7. Escriba su contraseña en un papel limpio.
8. Escriba su semilla en la otra hoja de papel.
9. Haga clic en Tonish.

Ahora tiene un lugar seguro para guardar su SOL e interactuar con la cadena de bloques de Solana. No olvide mantener su contraseña y frase inicial seguras. Incluso puedes considerar plastificar el papel para que sea más difícil de dañar.

Poner tus manos en SOL

Ahora necesita cargar su billetera con SOL para tener la cantidad requerida para construir su contrato. Sigue estos pasos:

1. Abra el navegador web Brave y navegue hasta las extensiones de su navegador.
2. Abra su billetera Phantom.
3. Haga clic en Comprar.
4. Haga clic en Solana.
5. Ingrese un mínimo de $50.

6. Haga clic en Siguiente.
7. Haga clic en Coinbase.
8. Haga clic en Autorizar.
9. Haga clic en Vista previa de compra.
10. Haga clic en Confirmar.

Ahora tiene su billetera cargada con SOL y puede pasar a construir su DAO.

Creando un DAO en Realms

Crear una DAO en Realms es un proceso simple y directo que implica algunos pasos clave. Siguiendo estos pasos, puedes crear tu propio DAO personalizado y comenzar a usarlo para tomar decisiones de forma descentralizada y transparente:

1. Vaya a https://app.realms.today.
2. Haga clic en el botón Crear DAO.

   Aparece su billetera Phantom.
3. Haga clic en el botón Conectar.
4. Seleccione el token comunitario DAO.
5. Introduzca el nombre de su comunidad.
6. En ¿Tiene un token existente para la comunidad de su DAO, seleccione
   el botón de opción No, creemos uno.
7. ¿Cuál es el número mínimo de tokens comunitarios necesarios para
   Administre este DAO, ingrese 10.
8. Establezca los quórumes de aprobación de su comunidad en un 60 %.
9. En ¿Tiene un token existente para el consejo de su DAO?, seleccione No.
10. Haga clic en la flecha siguiente.
11. Haga clic en Crear token comunitario DAO.
12. Cuando aparezca su billetera Phantom, haga clic en Aprobar.

3

Poderoso cadena de bloques Plataformas

EN ESTA PARTE . . .

Determinar el mayor consorcio de blockchain empresarial, Hyperledger, y qué beneficios e impacto tendrá para su industria y organización.

Comprender los esfuerzos de blockchain y las herramientas principales de Microsoft disponible para usted a través de sus ofertas de red.

Evaluar el proyecto IBM Bluemix y las implicaciones de tecnología blockchain combinada con arti cial inteligencia.

EN ESTE CAPÍTULO

Capítulo 9

Tener en tus manos Hyperledger

Hyperledger es una fundación que apoya a una comunidad de desarrolladores de software. Operadores y entusiastas de la tecnología que están construyendo estándares de la industria para marcos y plataformas de blockchain. El trabajo de Hyperledger es crucial porque están creando tecnología blockchain que satisface las necesidades de las empresas. Las criptomonedas en cadenas de bloques públicas tienen implicaciones regulatorias y responsabilidades que impiden que muchas empresas utilicen estas redes. Hyperledger tiene muchos de los mismos beneficios de la tecnología blockchain pública, pero opera sin un criptomoneda Con grandes partidarios como Intel e IBM, Hyperledger es la plataforma de implementación "confiable" para los equipos empresariales.

Hyperledger y su proyecto único crecen cada día. Al momento de escribir este artículo, tiene más de 100 empresas miembros y varias aplicaciones de blockchain en incubación. Los primeros proyectos de Hyperledger incluyen Fabric, Iroha y Sawtooth. Estos son marcos que los desarrolladores pueden usar para crear cadenas de bloques privadas, crear contratos inteligentes y crear una identidad distribuida para personas y cosas.

En este capítulo, explico cómo crear un seguimiento de activos y una aplicación de subasta inteligente utilizando la herramienta Composer de Hyperledger. También te presento a la Tela, Proyectos Iroha y Sawtooth. Obtienes una comprensión profunda de cuál será el futuro de blockchain comercializado se mantendrá para su empresa e industria. Este conocimiento lo ayudará a explorar qué tecnologías utilizar y cuáles evitar, ahorrándole tiempo y recursos de desarrollo.

Conociendo a Hyperledger

A fines de 2015, la Fundación Linux formó el proyecto Hyperledger para desarrollar un marco de libro mayor distribuido de código abierto y de nivel empresarial. Ellos esperaba enfocar a la comunidad blockchain en la construcción robusta, específica de la industria aplicaciones, plataformas y sistemas de hardware para apoyar a las empresas.

La Fundación Linux vio que había muchos grupos diferentes construyendo tecnología de cadena de bloques sin una dirección cohesiva. La industria estaba duplicando esfuerzo, y el tribalismo estaba liderando equipos para resolver el mismo problema dos veces. El Los miembros de la fundación vieron similitudes entre el nacimiento de Internet y el surgimiento de la tecnología blockchain: si la cadena de bloques iba a alcanzar su máximo potencial, se necesitaba desesperadamente una estrategia de desarrollo colaborativo y de fuente abierta.

El proyecto Hyperledger está dirigido por el Director Ejecutivo Brian Behlendorf, quien ha décadas de experiencia que se remontan a la Fundación Linux original y Apache Foundation, además de ser director de tecnología (CTO) del Foro Económico Mundial. Por lo tanto, no sorprende que Hyperledger haya sido bien recibido.
Muchos de los principales líderes empresariales y de la industria se han unido al proyecto, incluidos Accenture, Cisco, Fujitsu Limited, IBM, Intel, JP Morgan y Wells Fargo. Tiene también atrajo a muchas de las principales organizaciones de blockchain.

Los comités de dirección técnica de Hyperledger garantizan la solidez y la interoperabilidad entre estas diferentes tecnologías. La esperanza es que la industria cruzada,
La colaboración de código abierto hará avanzar la tecnología de cadena de bloques y generará miles de millones de dólares en valor económico al compartir los costos de investigación y desarrollo entre muchas organizaciones.

Hyperledger está identificando y abordando las características y requisitos críticos que faltan en el ecosistema de tecnología blockchain. También está fomentando un estándar abierto entre industrias para registros distribuidos y manteniendo un espacio abierto para que los desarrolladores contribuyan a construir mejores sistemas de cadena de bloques.

Hyperledger tiene un ciclo de vida de proyecto similar al de Linux Foundation. Se presenta una propuesta y luego las propuestas aceptadas se ponen en incubación.
Cuando un proyecto ha alcanzado un estado estable, se gradúa y pasa a un estado activo. Hasta el momento, todos los proyectos de Hyperledger se encuentran en la etapa de propuesta o incubación. Cada uno de los proyectos está liderado por una gran corporación o startup. Por ejemplo, la tela es liderado por IBM, Sawtooth por Intel e Iroha por la startup Soramitsu.


TIP

Hyperledger, como muchos proyectos de código abierto, usa GitHub (www.github.com/hyperledger) y Slack (https://slack.hyperledger.org) para conectarse con equipos trabajando en cada uno de los proyectos. Estos son excelentes lugares para obtener las últimas actualizaciones y para comprobar el progreso que estos proyectos están teniendo en desarrollo.

Identificación de proyectos clave de Hyperledger

Hyperledger tiene varios proyectos revolucionarios en incubación. En esta sección, le hablaremos de los tres proyectos más destacados y mejor desarrollados. Estas tecnologías de cadena de bloques incluyen marcos de contabilidad distribuidos, motores de contratos inteligentes, bibliotecas de clientes, interfaces gráficas, bibliotecas de utilidades y aplicaciones de muestra.

Centrándose en la tela

Fabric fue la primera implementación de blockchain en Hyperledger. se ha convertido en el base para desarrollar la mayoría de las aplicaciones de blockchain. La tela es única dentro el ecosistema blockchain porque permite a los desarrolladores usar piezas de Fabric sin comprometerse con toda la funcionalidad: un plug-and-play verdaderamente personalizado experiencia. Fabric también puede crear contratos inteligentes llamados chaincode.

Fabric es una cadena de bloques autorizada y no utiliza una criptomoneda. Este significa que todos los participantes son conocidos (a diferencia de una cadena de bloques pública típica donde todos los participantes son anónimos de forma predeterminada). La tela funciona como la mayoría de las cadenas de bloques en el sentido de que mantiene un registro de eventos digitales. estos eventos son estructurados como transacciones y compartidos entre los diferentes participantes. El las transacciones se ejecutan sin una criptomoneda (en contraste, una cadena de bloques pública usa su criptomoneda nativa para pagar a la red para operar y permitir que todos los participantes permanezcan en el anonimato). Para profundizar en el tema de Fabric, vaya a https://trustindigitallife.eu/wp-content/uploads/2016/07/marko_vukolic.pdf.

Todas las transacciones son seguras, privadas y confidenciales. Fabric preserva su integridad al permitir solo actualizaciones por consenso de los participantes. Cuando se han ingresado los registros, nunca se pueden modificar.

Fabric es una solución empresarial interesada en la escalabilidad y el cumplimiento de las normativas. Todos los participantes deben registrar una prueba de identidad en los servicios de membresía para obtener acceso al sistema. Fabric emite transacciones con certificados derivados que no se pueden vincular con el participante propietario, por lo que ofrecen anonimato en la red. Además, el contenido de cada transacción está encriptado para garantizar que solo los participantes previstos puedan ver el contenido.

Fabric tiene una arquitectura modular. Puede agregar o quitar componentes implementando su especificación de protocolo. Su tecnología de contenedores puede manejar la mayoría de los principales lenguajes para el desarrollo de contratos inteligentes.

Mirando a la Interamericana trabajo del banco de desarrollo en Tela

El Banco Interamericano de Desarrollo (BID) ha estado trabajando con Fabric para respaldar sus innovaciones transversales. Los esfuerzos del BID incluyen formar una innovación laboratorio llamado IDB Lab.

El BID Lab se formó para dar solución a los problemas de cumplimiento regulatorio, soporte y gobernabilidad. Mientras investigaba el problema, BID Lab formó LACChain, una infraestructura blockchain pública autorizada. LACChain es una red escalable y sostenible para la región de América Latina y el Caribe (LAC), implementar una gobernanza neutral, responsable y sólida.

Comprobación doble de la identidad

LACChain abordó un problema importante al desarrollar un sistema que garantiza el cumplimiento de las reglamentaciones que exigen la responsabilidad de las transacciones. Conseguir esto, LACChain implementó dos niveles de firma:

- El tercer nivel está autorizado, lo que significa que solo se concede acceso a individuos u organizaciones que han sido examinados e identificados.
- El segundo nivel permite un mayor anonimato, porque separa los identidad del firmante de la transacción, evitando que el público en general saber quién lo firmó.

La capa autorizada de este sistema se basa en Hyperledger Besu, mientras que la La capa pública se basa en Ethereum.

Cualquiera puede unirse a las redes LACChain implementando un nodo. Cada nodo puede ser un validador, arranque, escritor y observador. Usted elige su entorno de implementación, que puede ser en la nube o en las instalaciones.

Las entidades deben cumplir con los términos y condiciones para las redes de prueba LACChain y el Acuerdo de Adscripción para LACChain Mainnet. El acuerdo de términos y condiciones requiere que cada operador de nodo sea responsable de las transacciones que envía a la red y su contenido. La Mainnet LACChain requiere que cada nodo que transmite transacciones para firmarlas y la firma anónima del usuario final.

LACChain implementó protocolos para la identidad auto-soberana. Este es un tipo de identidad que el individuo crea para sí mismo versus una emitida por un tercero como un gobierno o una corporación.

LACChain de punta cuántica

Una de las amenazas existenciales que enfrentan las cadenas de bloques son las computadoras cuánticas que son más rápido que las computadoras clásicas. Las computadoras cuánticas usan las reglas de la mecánica cuántica para hacer cálculos y resolver problemas. Funcionan de manera diferente a las computadoras regulares porque usan qubits en lugar de bits regulares para almacenar y procesar información.

Las computadoras clásicas almacenan y procesan información usando bits que solo pueden estar en uno de dos estados (0 o 1), mientras que los qubits pueden existir en múltiples estados simultáneamente. Esta propiedad, conocida como superposición, permite que las computadoras cuánticas realicen ciertos tipos de cálculos, como romper el cifrado, mucho más rápido que las computadoras clásicas. Cuantos más qubits tenga una computadora, más rápido podrá resolver problemas. Las computadoras cuánticas aún se están desarrollando y tienen algunos desafíos que superar antes de que tengan suficiente precisión y qubits para descifrar la clave pública utilizada en la tecnología blockchain.

Gran parte de la infraestructura de Internet utiliza el cifrado de clave pública, por lo que será un problema mucho mayor que alguien que tiene la capacidad de robar sus Bitcoins.

Se sumaron BID Lab, Cambridge Quantum Computing y el Tecnológico de Monterrey obliga a abordar un problema específico utilizando nuevos algoritmos de criptografía post-cuántica para el cifrado de clave pública y el establecimiento de claves. Con la ayuda del Instituto Nacional de Estándares y Tecnología (NIST), una agencia del gobierno de EE. UU. que promueve la innovación y la competitividad industrial, BID Lab puede probar dos nuevos algoritmos candidatos llamados CRYSTALS-Dilithium y FALCON para agregar un capa adicional de protección para la cadena de bloques LACChain que es resistente a ataques de computadoras cuánticas en el futuro.

Sostenibilidad económica

Una de las ventajas de usar una cadena de bloques pública es que cada transacción tiene un costo duro Probablemente recuerde que se pagan tarifas de transacción a los nodos en redes públicas. Cada cadena de bloques tiene una tarifa diferente que cambiará con el tiempo y congestión de la red. La razón de esta estructura es evitar que los individuos de enviar spam a la red. Cuando demasiadas transacciones llegan a la red simultáneamente, se crea una denegación de servicio (DoS) para los usuarios legítimos.

LACChain encontró una solución alternativa que le permitió resolver este problema sin dejar de ofrecer transacciones gratuitas a los usuarios. Desarrolló un nuevo Protocolo de Distribución de gas utilizando contratos inteligentes. Asigna gas por bloque a cuentas de nodos de escritor autorizados. La distribución de gas es dinámica al estrés de la red. Hay más gas disponible si se realizan menos entradas; hay menos gas disponible si la red está saturada.

El Protocolo de distribución de gas es una solución basada en contratos inteligentes. Los contratos inteligentes evalúan todas las transacciones enviadas a la red y analizan cuánto gas se usa por bloque. También comprueba que los nodos firmen las transacciones y tengan suficiente gas.

Gobernanza futura de LACChain

LACChain creó LACNet como una organización internacional sin fines de lucro con el respaldo de Red Clara, otra organización sin fines de lucro que apoya a la comunidad académica en América Latina. LACNet también cuenta con el apoyo del Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC). Juntas, estas organizaciones apoyarán el futuro de LACChain.

Cuando se escribió este libro, 60 proyectos estaban usando las redes LACChain. Con las innovaciones en la prueba cuántica y el apoyo a las transacciones gratuitas no sujetas a los ataques DoS, LACChain puede convertirse en una innovación esencial en el futuro de cadenas de bloques autorizadas.

Investigando el proyecto Iroha

El proyecto Iroha de Hyperledger se basa en el trabajo realizado en el proyecto Fabric. Está destinado a complementar Fabric, Sawtooth Lake y los otros proyectos bajo Hiperlibro. Hyperledger agregó el proyecto Iroha a la incubación porque los otros proyectos no tenían ningún proyecto de infraestructura escrito en C++. No tener un C++ proyecto limitó severamente la cantidad de personas que podrían beneficiarse del trabajo en Hyperledger y la cantidad de desarrolladores que podrían contribuir al proyecto.

Además, la mayor parte del desarrollo de blockchain en este punto se ha realizado en el nivel de infraestructura más bajo, y ha habido poco o ningún trabajo de desarrollo sobre la interacción del usuario o las aplicaciones móviles. Hyperledger cree que Iroha es necesaria para la popularización de la tecnología blockchain. Este proyecto llena la brecha en el mercado. al traer más desarrolladores y proporcionar bibliotecas para el desarrollo de la interfaz de usuario móvil.

Al momento de escribir este artículo, Iroha es un proyecto muy nuevo y no se ha integrado con Fabric o Sawtooth Lake. Hyperledger tiene planes de expandir la funcionalidad para trabajar con los otros proyectos de blockchain pronto. Sus bibliotecas de iOS, Android y JavaScript proporcionará funciones de apoyo como la firma digital de transacciones. Será útil para el desarrollo de aplicaciones comerciales y agregará nuevas capas de seguridad y modelos comerciales que solo son posibles con la tecnología blockchain.

Presentamos Sumeragi: El nuevo algoritmo de consenso

Las cadenas de bloques tienen sistemas que les permiten acordar una sola versión del verdad y luego registrar esa verdad acordada en su libro mayor. Un sistema de acuerdo se llama consenso. Un consenso es complicado. Comprender los matices de cómo y por qué los consensos actúan de la forma en que lo hacen está mucho más allá del alcance de este libro. También es mucho más de lo que necesitará como profesional de negocios. Lo que importa para usted son las consecuencias de los diferentes mecanismos de consenso y cómo afecta lo que estás haciendo en esa cadena de bloques en particular. Destaco el de Iroha consenso, Sumeragi, porque es muy diferente de las cadenas de bloques tradicionales.

Aquí hay algunas cosas clave que hacen que Sumeragi sea diferente:

- Sumeragi no tiene criptomoneda.
- Los nodos que inician el consenso son agregados al sistema por Fabric servicios a los miembros. Los nodos construyen una reputación con el tiempo en función de cómo han interactuado con el libro mayor. Esta es una cadena de bloques de permisos administrada por conocidos entidades.
- Las nuevas entradas se agregan al libro mayor de una manera única. El tercer nodo que inicia el consenso, llamado líder, transmite la entrada a un grupo de otros nodos; esos nodos luego validan. Si no validan, el primer nodo lo hará retransmitido después de un tiempo predeterminado.

Dependiendo de su caso de uso para blockchain, Iroha puede ser positivo o negativo. Si te preocupa la censura, puede que Iroha no sea adecuado para ti. En este caso, será mejor que busque una cadena de bloques que sea resistente a la censura. Si eres preocupado por otros jugadores en la red que cometen arbitraje, es posible que Iroha tampoco tenga razón: se necesita más investigación. Si quieres conocer a todos los jugadores en su cadena de bloques, Iroha puede ser exactamente lo que está buscando.

Desarrollo de aplicaciones móviles


TIP

Omita esta sección si no forma parte del espacio de desarrollo de aplicaciones.

Iroha está diseñado para los desarrolladores de aplicaciones web y móviles para que puedan acceder a las fortalezas de los sistemas Hyperledger. El equipo de Iroha vio que tener un libro mayor distribuido no era útil si no había aplicaciones que lo utilizaran.

Iroha tiene una ruta de desarrollo para los siguientes componentes C++ encapsulados:

- Biblioteca de consenso de Sumeragi
- Biblioteca de firmas digitales Ed25519

» Biblioteca hash SHA-3

» Biblioteca de serialización de transacciones de Iroha

» Biblioteca de difusión P2P

» Biblioteca del servidor API

» Biblioteca de iOS

» Biblioteca de Android

» biblioteca JavaScript

» Suite de visualización de datos/explorador de cadena de bloques

Uno de los principales obstáculos de la industria de la cadena de bloques ha sido crear sistemas fácil de usar. Iroha ha creado bibliotecas de software de código abierto para iOS, Android, y JavaScript e hizo que las funciones comunes de la interfaz de programación de aplicaciones (API) fueran convenientes para llamar. Todavía está en una etapa temprana de desarrollo, pero Iroha es un buen recurso para explorar casos de uso empresarial.

Buceo en el lago Sawtooth

Sawtooth Lake de Intel es otro proyecto de libro mayor distribuido en Hyperledger. Es enfocado en ser una plataforma altamente modular para construir nuevos libros distribuidos para empresas.

WARNING

Al momento de escribir este artículo, la versión de lanzamiento tiene un software que solo simula el consenso. No proporciona seguridad para su proyecto y solo debe utilizarse para probar nuevas ideas.

Sawtooth Lake no opera con una criptomoneda. Mantiene la seguridad de la plataforma al permitir que las empresas creen cadenas de bloques privadas. Estas empresas que ejecutan cadenas de bloques privadas luego comparten la carga de los requisitos computacionales de la red. En su documentación, Sawtooth Lake afirma que este El tipo de configuración garantizará un acuerdo universal sobre el estado del libro mayor compartido.

Sawtooth Lake ha tomado el modelo básico de blockchains y lo ha puesto patas arriba. La mayoría de las cadenas de bloques tienen tres elementos:

» Un registro compartido del estado actual de la cadena de bloques

» Una forma de ingresar nuevos datos

» Una forma de acordar esos datos

Sawtooth Lake fusiona los dos primeros en un proceso de señal que llama familia de transacciones. Este modelo es mejor en casos de uso donde todas las partes participantes tienen un mutuo beneficio de tener un registro correcto.

Intel ha permitido que su software sea lo suficientemente flexible para acomodar familias de transacciones personalizadas que reflejen los requisitos únicos de cada negocio. también construyó tres plantillas para crear activos digitales:

» EndPointRegistry: un lugar para registrar elementos en una cadena de bloques

» IntegerKey: un libro mayor compartido que se utiliza para la gestión de la cadena de suministro

» MarketPlace: una plataforma de comercio de cadena de bloques para comprar, vender y negociar recursos digitales

El algoritmo de consenso para Sawtooth Lake se llama Prueba de tiempo transcurrido (Poeta). Fue construido para ejecutarse en un área segura del procesador principal de su computadora, denominado entorno de ejecución de confianza (TEE). PoET aprovecha la seguridad del TEE para demostrar que el tiempo ha pasado mediante el sellado de tiempo de las transacciones.

Otros algoritmos de consenso también tienen algún tipo de elemento de marca de tiempo. La forma en que se aseguran de que los registros no han sido modificados es a través de información pública. publicando sus cadenas de bloques como prueba de que no han sido alteradas. El libro mayor publicado actúa como un testigo público que cualquiera puede retroceder y verificar. Es algo así como publicar un anuncio en un periódico para demostrar que algo sucedió.

PoET también tiene un sistema de lotería que funciona un poco diferente a otras cadenas de bloques. utilizando la prueba de trabajo. Selecciona aleatoriamente un nodo del grupo de nodos de validación. La probabilidad de que un nodo sea seleccionado aumenta proporcionalmente a cuánto recursos de procesamiento que ese nodo contribuyó al libro mayor compartido. Se pueden implementar medidas para evitar que los nodos jueguen con el sistema y corrompan el libro mayor.

Trabajando con Hyperledger Besu

Hyperledger Besu es un cliente de Ethereum que admite contratos inteligentes y dApp casos de uso de desarrollo, implementación y operaciones, utilizando herramientas como True, Remix y web3j. Fue desarrollado bajo la licencia de código abierto Apache 2.0 y escrito en Java. Puede ejecutar Besu en la red pública de Ethereum o en la suya propia red privada autorizada. También funciona en las redes de prueba de Ethereum. Rinkeby, Ropsten y Gorli.

Las funciones principales de Besu incluyen una máquina virtual Ethereum (EVM). El EVM es el Entorno de Turing que le permite implementar y ejecutar contratos inteligentes en el Cadena de bloques de Ethereum.

Una de las principales razones por las que puede considerar Besu es porque ha implementado varios algoritmos de consenso. El consenso es cómo la red acuerda el estado de su cadena de bloques y la validez de la transacción. El algoritmo de consenso dictará el costo, la velocidad y la escalabilidad de su software.

Aquí hay dos opciones populares que ofrece Besu:

- Prueba de autoridad (PoA): los protocolos de consenso de PoA se utilizan cuando los participantes se conocen entre sí. Las transacciones y bloques en un POA red son validados por validadores aprobados. Los validadores se turnan para crear el siguiente bloque y no compita por las recompensas del bloque.
- Prueba de trabajo (PoW): los protocolos de consenso POW se utilizan cuando los participantes no se conocen. La transacción y los bloques en las redes POW son validados por los nodos que ganan cada bloque.

Besu utiliza una base de datos RocksDB para almacenar datos de cadenas localmente. Este tipo de base de datos es excelente para almacenamiento rápido y de baja latencia. Le permite extraer rápidamente las transacciones ordenadas de la cadena de bloques y los metadatos de cada transacción.

Besu le permite monitorear el rendimiento de los nodos y la red mediante una herramienta llamada Prometheus o mediante la API JSON-RPC debug_metrics. También puedes estar pendiente rendimiento con otra herramienta llamada Alethio.

Besu también le permite mantener sus transacciones privadas. Esto significa que los terceros no pueden acceder al contenido de la transacción, la parte que envía o la lista de partes participantes.

En general, Besu le permite crear e implementar contratos inteligentes en los más populares plataforma de contrato inteligente, Ethereum, al mismo tiempo que le brinda algunos de los beneficios de software de cadena de bloques de empresa privada.

Configuración de su sistema para Besu

Puede usar Hyperledger Besu en todos los sistemas con una imagen de Docker para ejecutar un nodo en un contenedor. Si es un desarrollador moderadamente competente, es fácil de seguir la documentación en el sitio web de Docker y el sitio web de Hyperledger para Besu.

En las siguientes secciones, descubra cómo configurar Besu para su sistema iOS y cómo implementar su propia red. Necesitarás lo siguiente:

» Una Mac con macOS 10.13 (High Sierra) o una versión más reciente de macOS

» Un navegador web

» Una conexión a Internet

» Experiencia accediendo a la aplicación Terminal de su computadora

» Java 17, que será el requisito mínimo en la próxima versión de Besu serie

También descargará Teku, un cliente de consenso de Ethereum de código abierto. Teku le permite ejecutar una implementación de nodo de baliza completa y un cliente de validación para participar en el consenso de prueba de participación.


TIP

También puede instalar Java usando brew install OpenJDK.

Paso 1: Preparando su sistema para instalar Besu

El primer paso es instalar Homebrew:

1. Vaya al sitio web de Homebrew en https://brew.sh.
2. En Instalar Homebrew, copie el código de la línea de comando.
3. Abra la aplicación Terminal en su Mac.

   Terminal está en la carpeta Aplicaciones/Utilidades .
4. Pegue el código en la Terminal.
5. Si su sistema solicita su contraseña, ingrésela.
6. Presione Entrar.
7. Presiona Entrar nuevamente cuando Terminal te lo indique.

Paso 2: Instalación de Java

Para instalar Java, siga estos pasos:

1. Vaya al sitio web de Oracle en www.oracle.com/java/technologies/ descargas/.
2. Seleccione el sistema operativo de su computadora.
3. Haga clic en la opción Instalador.
4. Haga clic para completar el proceso de descarga.

Ponerse en marcha en Besu

En esta sección, se conecta a la red de desarrollo de Ethereum y comienza a probar ETH.

Paso 1: Instalación de Besu

Para instalar Besu, siga estos pasos:

1. Abra la aplicación Terminal.
2. Escriba el siguiente código de línea de comando en la Terminal:

```
brew tap hyperledger/besu brew
install hyperledger/besu/besu
```

3. Verifique su versión de Besu ingresando este comando en la Terminal:

```
besu --versión
```

Paso 2: Instalación de Teku

Para instalar Teku, sigue estos pasos:

1. Abra la aplicación Terminal.
2. Escriba el siguiente código de línea de comando en la Terminal:

```
preparar la instalación de ConsenSys/teku/teku
```

3. Verifique su versión de Teku ingresando este comando en la Terminal:

```
Teku --versión
```

Paso 3: Iniciar Besu

Para iniciar Besu y unirse a la red de prueba de desarrollo, siga estos pasos:

1. Abra la aplicación Terminal.
2. Escriba el siguiente código de línea de comando en la Terminal.

```
besu --network=dev --miner-enabled --miner-coinbase=0xfe3b5
    57e8fb62b89f4916b721be55ceb828dbd73 --rpc-http-cors origins="all"
    --host-allowlist="*" --rpc-ws-enabled --rpc-http-enabled --data-path=/tmp/
    tmpDatdir
```

¡Felicidades! Ahora está funcionando en la red de prueba de desarrollo de Ethereum utilizando Besu de Hyperledger. Si disfrutó de este tutorial y desea obtener más información sobre cómo construir una red privada o crear contratos inteligentes, diríjase a https://besu.hyperledger.org/en/stable/private-networks/tutorials.

EN ESTE CAPÍTULO

Capítulo 10

Aplicando Microsoft Azure

En este capítulo, obtendrá una vista previa de las emocionantes innovaciones que están teniendo lugar dentro de la plataforma Azure de Microsoft y cómo estos cambios pueden mejorar la eficiencia de su negocio y crear nuevas oportunidades para productos y servicios.

Este capítulo lo ayuda a competir, colaborar y atender a los clientes en una economía global. La tecnología Blockchain está abriendo nuevos mercados y cambiando los modelos de negocio. Microsoft está trabajando arduamente para que sea una tecnología accesible para los negocios tradicionales.

Este capítulo también explica los puentes innovadores de blockchain que se están construyendo para permitirle conectar y escalar sus sistemas existentes. Descubra cómo implementar su propia cadena de bloques dentro de Azure y los elementos clave para realizar una transición segura y sin complicaciones a los sistemas de cadena de bloques para su empresa.

Bletchley: el tejido modular de la cadena de bloques

Project Bletchley se concentra en ofrecer bloques de construcción arquitectónicos para clientes empresariales dentro de un ecosistema de cadena de bloques de consorcio (una red autorizada solo para miembros para que los miembros ejecuten contratos). La cadena de bloques de Bletchley

Fabric está impulsada por Azure, la plataforma informática en la nube de Microsoft.
El Proyecto Bletchley aborda lo siguiente:

» Identidad digital

» Gestión de claves privadas

» Privacidad del cliente

» Seguridad de datos

» Administración de operaciones

» Interoperabilidad del sistema

En Project Bletchley, Azure proporciona la capa de nube para blockchain, que sirve como plataforma donde se pueden crear y entregar aplicaciones. Estará disponible en 24 regiones a nivel mundial. Azure está combinando sus productos tradicionales, como capacidades de nube híbrida, una amplia cartera de certificación de cumplimiento y nivel empresarial
seguridad a varias cadenas de bloques. Microsoft quiere facilitar que los clientes existentes adopten rápidamente la tecnología blockchain, especialmente en industrias controladas como la atención médica, los servicios financieros y el gobierno.

La Figura 10-1 muestra el proyecto Bletchley's Blockstack Core v14, un nuevo sistema descentralizado web de aplicaciones sin servidor donde los usuarios pueden controlar sus datos.

Azure funcionará con varios protocolos de blockchain. Forman parte del proyecto Hyperledger y los protocolos basados en la salida de transacciones no gastadas (UTXO). Esto significa que la plataforma Azure no utiliza una criptomoneda y puede resultar más atractiva para los clientes empresariales. También tendrán integraciones con protocolos más sofisticados, incluido Ethereum, que utilizan una criptomoneda para proteger la red.

Cryptlets para cifrar y autenticar

El Proyecto Bletchley se basa en dos ideas:

» Middleware de cadena de bloques: almacenamiento en la nube, gestión de identidades, análisis y aprendizaje automático

» Cryptlets: Ejecución segura para la interoperación y comunicación entre
Microsoft Azure, el ecosistema de Bletchley y tu propia tecnología

Los Cryptlets se construyen como componentes de código de cadena, se escriben en cualquier idioma, se ejecutan dentro de un contenedor confiable y se comunican a través de un canal seguro. Los permisos de cripta se pueden usar en contratos inteligentes y sistemas UTXO, cuando se necesita funcionalidad o información adicional.

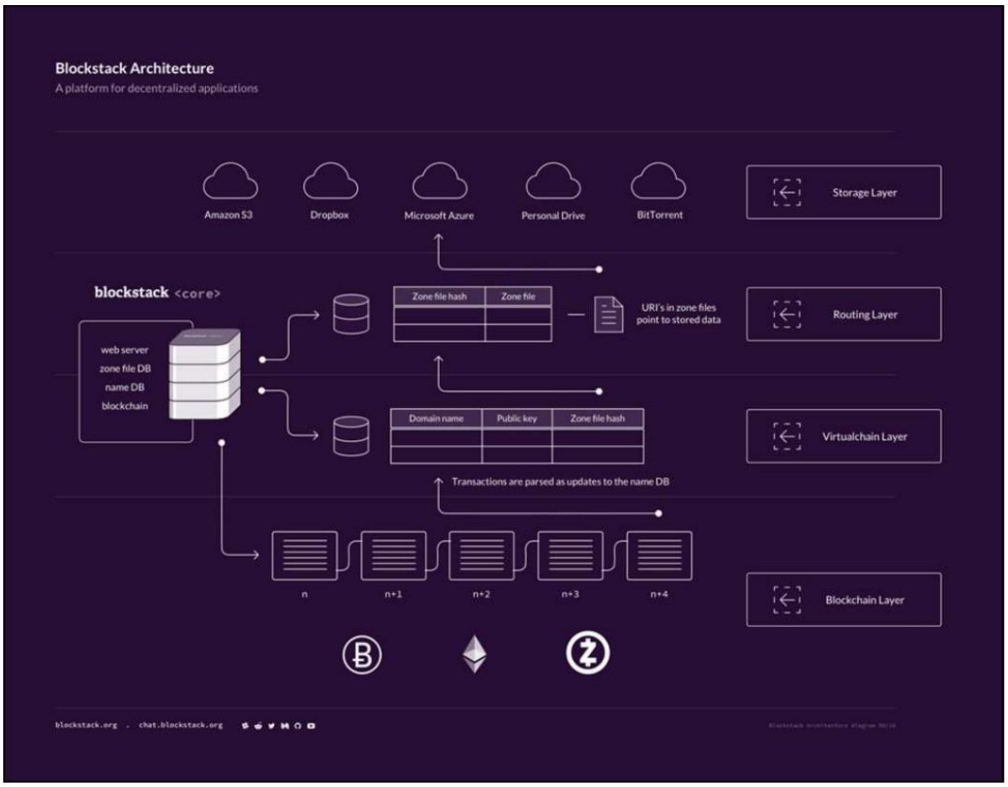


FIGURA 10-1: pila de bloques Núcleo v14.

Los Cryptlets cierran la brecha en la seguridad entre la ejecución de programas dentro y fuera de la cadena, operando cuando se necesita información segura adicional. Son lo que le permite a su gestión de relaciones con los clientes (CRM) o plataforma comercial conectarse con su almacenamiento en la nube y luego estar protegido con Ethereum, por ejemplo.

El middleware de Bletchley funciona junto con Cryptlets y los servicios existentes de Azure, como Active Directory y Key Vault, y otras tecnologías del ecosistema de cadena de bloques, para ofrecer una solución completa y garantizar el funcionamiento confiable de su integración de cadena de bloques.

La tabla 10-1 muestra la diferencia entre un oráculo y un Cryptlet de Devcon 2 presentación sobre Bletchley.

Los desarrolladores crean Cryptlets y los venden en el mercado de Bletchley. se dirigen muchos conjuntos de funcionalidades diferentes que son esenciales para crear aplicaciones basadas en registros distribuidos. El mercado está creciendo para satisfacer las demandas de los clientes que necesitan la funcionalidad necesaria, como ejecución segura, integración, privacidad, administración, interoperabilidad y un conjunto completo de servicios de datos.

TABLA 10-1 Criptas contra oráculos

	criptas	Oráculos
Veri cación requisitos	Requiere confianza con veri cación con un host de confianza (HTTPS), una clave de Cryptlet de confianza y una firma de enclave de confianza.	Requiere confianza pero no veri cación formal.
Infraestructura	Infraestructura estándar. Obtiene aislamiento y atestación basados en hardware a través de enclaves disponibles globalmente en Azure. Los marcos del kit de desarrollo de software (SDK) de Bletchley Cryptlet (utilidad y contrato) están disponibles para ayudarlo a comenzar rápidamente a crear y consumir Cryptlets.	Infraestructura personalizada. Puede escribir y hospedar por separado. Establecer confianza es difícil. Oráculos han sido especí cos de la plataforma, y la documentación es actualmente muy escasa.
Uso del desarrollador	Hay muchas opciones de idioma disponibles y son independientes de blockchain.	Atado a su propia cadena de bloques y pocas opciones de idioma.
Disponibilidad del mercado	Un mercado está disponible para la publicación y el descubrimiento.	No hay un mercado común disponible para la publicación y el descubrimiento.

Cryptlets y CryptoDelegates de servicios públicos y contratos

Hay dos tipos de criptas:

- Utilidad: los Cryptlets de utilidad brindan encriptación, marca de tiempo, datos externos acceso y autenticación. Crean transacciones más sólidas y confiables.
- Contrato: los Cryptlets de contrato son motores de delegación completos. Pueden funcionar como agentes autónomos o bots. Proporcionan toda la lógica de ejecución que normalmente hace un contrato inteligente, pero fuera de una cadena de bloques.

Los Cryptlets de contrato están vinculados a contratos inteligentes y se crean cuando su se publica el contrato. Se ejecutan en paralelo con su máquina virtual y tienen un mayor rendimiento que los contratos inteligentes tradicionales construidos dentro de cadenas de bloques porque no requieren una tarifa de minería para ejecutar su contrato. Son más atractivos para los usuarios de cadenas de bloques que no son criptomonedas, donde el código de cadena y los contratos inteligentes están firmados por partes conocidas.

La Figura 10-2 muestra una representación de un contenedor Cryptlet y la ruta de comunicación segura a su contrato inteligente.

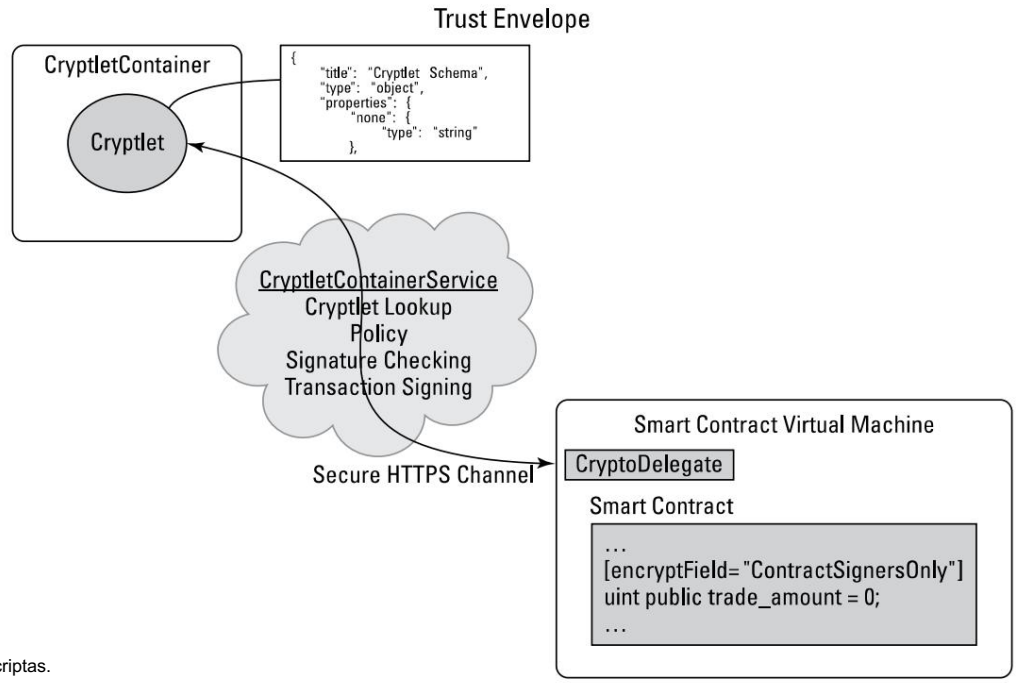


FIGURA 10-2:
Un
contenedor de criptas.

CryptoDelegates permite que funcionen las criptas de servicios y contratos. actúan como adaptadores mediante la creación de ganchos funcionales en sus máquinas virtuales de contrato inteligente. Llaman al Cryptlet desde el código de su contrato inteligente, que a su vez crea un sobre seguro y auténtico para transacciones.

Construyendo en el Ecosistema Azure

Azure es un ecosistema digital y una plataforma de computación en la nube. Conecta empresas directamente con sus socios en la nube y SaaS. Esto, a su vez, permite a las empresas transferir sus datos de forma interconectada, confiable y segura.

La plataforma en la nube de Azure es la segunda plataforma de infraestructura como servicio (IaaS) más grande del mundo. Es un refugio confiable y seguro para su computación en la nube y almacenamiento de datos. En Azure, existe un servicio conocido como ExpressRoute, que proporciona los consumidores una forma de conectarse directamente a Azure. Esto, a su vez, evita los problemas de rendimiento y seguridad que se ven ampliamente en la Internet pública.

En 2015, Microsoft decidió expandir su ecosistema Azure utilizando Ethereum y Sistemas de cadena de bloques Hyperledger. La última oferta de Azure Blockchain como servicio está impulsada por Ethereum. Ethereum es un marco de trabajo de cadena de bloques completo de Turing para aplicaciones de construcción, y puede leer sobre él en profundidad en el Capítulo 5 o en Ethereum para tontos, por Michael G. Solomon (Wiley). Microsoft tiene como objetivo construir más ofertas basadas en la tecnología blockchain e Hyperledger. Es también hacer crecer el mercado de Azure, mientras hace la transición a un portal para clientes en Azure.

El programa Azure Stack de Microsoft incorpora plantillas de inicio rápido de Azure, que implementan los diversos recursos de Azure con la ayuda de Azure Resource Manager. para ayudarle a hacer más trabajo. Azure Resource Manager permite clientes a trabajar con sus recursos comerciales como un grupo. Les permite implementar, eliminar o actualizar todos los recursos de su solución en una sola operación coordinada.

Las plantillas de inicio rápido de Azure pueden funcionar en varios entornos, como producción, ensayo y pruebas. A través de Azure Resource Manager, los clientes obtienen varios funciones de etiquetado, auditoría y seguridad. Estas funciones ayudan a los consumidores a administrar sus recursos después de la implementación.

El Proyecto Bletchley de Microsoft es su arquitectura de cadena de bloques que se fusiona con tecnologías empresariales establecidas que ya estaban ofreciendo. Le da a Azure un backend y mercado de blockchain.

El ecosistema de Bletchley es un enfoque adoptado por Microsoft para llevar cadenas de bloques o redes de registros distribuidos a un público más amplio de una manera segura y eficaz. Quieren ayudar a crear soluciones auténticas y abordar problemas comerciales reales.

ELEGIR SU PLANTILLA

La plantilla de inicio rápido es una herramienta diseñada para facilitar a los usuarios del Proyecto Bletchley la puesta en marcha de un grupo privado de blockchain. Actualmente, hay alrededor de una docena de plantillas de cadena de bloques que le permiten activar aplicaciones de cadena de bloques en Azure. En el futuro, habrá más plantillas disponibles.

La versión privada de Ethereum es una de las mejores para automatizar el proceso. step-it es un proceso paso a paso en el que puede seleccionar a los miembros de su consorcio, determinar la cantidad de nodos que cada usuario tendrá en la red y luego distribuir geográficamente esos nodos usando la nube de Azure para aumentar la resiliencia.

Implementación de herramientas de cadena de bloques en Azure

Azure tiene otras implementaciones útiles de tecnología y herramientas de cadena de bloques que podrían resultarle útiles. Cubro cuatro de las principales herramientas de blockchain de Azure y proyectos en esta sección, incluida su implementación Ethereum; Cortana, una herramienta analítica de aprendizaje automático; la herramienta de visualización de datos de Azure, Power BI; y su herramienta Active Directory (AD). Las tres últimas no son específicamente herramientas de blockchain, pero se pueden usar con su proyecto de blockchain de Azure.

Esta sección le da una idea de lo que puede construir con Azure y algunas de las herramientas disponibles para que su proyecto sea un éxito.

Explorando Ethereum en Azure

Ethereum Blockchain ya está disponible como servicio en la plataforma Azure de Microsoft. Esta iniciativa es ofrecida por ConsenSys y Microsoft en sociedad. La solidez es un nuevo proyecto que crearon que le permite comenzar a construir su aplicación descentralizada en Ethereum. Obtenga más información en https://marketplace.visualstudio.com/items?itemName=ConsenSys.Solidity.

Ethereum Blockchain as a Service (EBaaS) permite a los desarrolladores y clientes empresariales desarrollar un entorno de cadena de bloques en la nube y se puede activar con un solo clic.

Cuando implementa Ethereum blockchain en Azure, Azure ofrece dos herramientas inicialmente:

- BlockApps: un entorno de cadena de bloques de Ethereum semiprivado y privado
- Ether.Camp: un entorno de desarrollo integrado

BlockApps también se puede implementar en el entorno público de Ethereum. Estas herramientas permiten el desarrollo rápido de aplicaciones basadas en un contrato inteligente.

Ethereum es un sistema flexible y abierto, que se puede personalizar para satisfacer las diversas necesidades de los clientes. Lea más sobre Ethereum en el Capítulo 5.

Cortana: su herramienta de aprendizaje automático de análisis

Cortana es una poderosa herramienta de aprendizaje automático de análisis basada en sistemas en la nube. Es un servicio en la nube completamente administrado que permite a los usuarios construir fácil y rápidamente,

organizar y compartir soluciones de análisis predictivo. Proporciona muchos beneficios a consumidores

Al revisar los análisis proporcionados por Cortana Intelligence, puede tomar medidas antes que sus competidores al predecir el próximo gran acontecimiento. esteexible y El software rápido le permite crear soluciones rápidas para su industria, que se adaptan a sus necesidades particulares.

Además, la herramienta de aprendizaje de Cortana es segura y escalable. Cortana ofrece datos valor, independientemente de la complejidad y el tamaño de los datos. Y, sobre todo, Cortana. te permite interactuar con agentes inteligentes, para que puedas acercarte a tus consumidores de forma más natural, práctica y útil. Cortana Intelligence Suite es útil en varios sectores, incluidos la fabricación, los servicios financieros, el comercio minorista y el cuidado de la salud.

Visualización de sus datos con Power BI

Power BI, ofrecido por Microsoft, es un potente servicio basado en la nube sistema. Cubre los últimos servicios y herramientas de inteligencia empresarial de Microsoft. Este servicio ayuda a los científicos de datos a imaginar y compartir información de los datos de sus organizaciones.

El curso de visualización de datos de Power BI, proporcionado en línea por edX, es parte del Certificado del programa profesional de Microsoft en ciencia de datos. Este basado en la nube El servicio está ganando rápidamente popularidad entre los profesionales de la ciencia de datos.

Power BI lo ayuda a visualizar y conectar sus datos. En este curso, los estudiantes aprenden a conectar, importar, transformar y dar forma a sus datos para la inteligencia empresarial. Además, el curso de Power BI le enseña cómo crear tableros y compartirlos con usuarios comerciales en dispositivos móviles y la web.

Administrar su acceso en Directorio activo de Azure

Azure Active Directory (AD) es una solución de administración de identidades y acceso amplio. Proporciona un amplio conjunto de funciones que le permiten supervisar el acceso a la nube y los recursos y aplicaciones locales. Esto incluye varios servicios en línea de Microsoft, como Oce 365, además de numerosas aplicaciones SaaS que no son de Microsoft.

Una de las características principales de Azure AD es que puede manejar el acceso a sus recursos. Estos recursos pueden ser externos al directorio, como aplicaciones de software como servicio (SaaS), recursos locales o sitios de SharePoint y servicios de Azure, o pueden ser internos al directorio, como permisos para administrar objetos a través de roles de directorio.

Introducción a Chain en Azure

Chain, que proporciona soluciones de tecnología blockchain, lanzó su Chain Core
Edición para desarrolladores en Azure. Chain Core Developer Edition es un programa de código abierto y versión gratuita de la plataforma de contabilidad distribuida de la empresa. Le permite emitir y transferir activos en redes blockchain autorizadas.

A través de su red de prueba, sus desarrolladores pueden unirse o iniciar una red de cadena de bloques, acceder a tutoriales y documentación técnicos detallados y crear aplicaciones financieras.
También pueden ejecutar sus propios prototipos en la red de prueba de la Cadena o crear los suyos propios. red personal en Azure.

Uso de servicios financieros en Azure's Chain

Chain lanzó su plataforma de desarrollo gratuita y de código abierto. Incluye una prueba
red, que es operada por Microsoft, Chain y la Iniciativa para Criptomonedas y Contratos (3CI). 3CI es la plataforma lanzada por Chain, que brinda
soluciones de tecnología de cadena de bloques.

Esta plataforma le permite emitir y transferir activos en redes blockchain autenticadas. Es un esfuerzo entre las principales empresas financieras y de Cadena.
Se pueden desarrollar varias aplicaciones financieras a través de Chain Core.

Se planea lanzar muchos productos nuevos e innovadores en esta plataforma. La gama cubre pagos, banca, seguros y mercados de capital. Además, Visa se ha asociado con Chain para desarrollar una forma segura, rápida y sencilla
para procesar pagos de empresa a empresa (B2B) en todo el mundo.

El enfoque triple de Chain para el libro mayor distribuido

Chain crea herramientas para crear aplicaciones en Internet utilizando la tecnología blockchain.
Tienen tres productos: Sequence, Chain Token y Chain Cloud.

Sequence es un libro de contabilidad digital que ayuda a realizar un seguimiento del dinero y otras cosas en línea. Es bueno para almacenar mucha información y es fácil de usar, incluso para grandes empresas.

Chain Token y Chain Cloud son herramientas para crear y ejecutar aplicaciones en el
Internet. Chain Token se usa para ejecutar Chain Protocol, y Chain Cloud es una forma
para desarrollar y ejecutar aplicaciones descentralizadas en la nube.

En general, Chain es una herramienta útil para las personas que desean crear aplicaciones basadas en blockchain. Es fácil de usar, escalable y seguro, por lo que vale la pena explorarlo al considerar las plataformas blockchain para su aplicación.

Construyendo tu propio libro mayor con Sequence

Ponerse en marcha en Sequence es muy fácil. Y después de configurar su libro mayor, tienen una interfaz de usuario (IU) fácil de usar para ayudarlo a crear sus primeras transacciones. Cada libro mayor que crea con Sequence es un sistema de registro discreto, solo anexado y vinculado criptográficamente.

Siga estos pasos para configurar su libro mayor:

1. Navegue a https://sequence.chain.com/start.
2. Haga clic en Crear equipo.
3. Introduzca su dirección de correo electrónico.
4. Ingrese el código de verificación que se envió a su correo electrónico.
5. Nombra a tu equipo.
6. Introduzca una contraseña.
7. Asigne un nombre a su libro mayor.
8. Haga clic en Crear libro mayor.

¡Felicidades! ¡Has creado tu propio libro mayor en Chain!

Criptomoneda nativa de Chain Protocol

Chain Token, o XCN, es la criptomoneda nativa del Chain Protocol. XCN es un token basado en utilidades que se usa para descuentos, acceso premium y para pagar tarifas comerciales en Sequence. XCN también se usa para la gobernanza en cadena para varios programas impulsados por la comunidad a través de Chain DAO. En marzo de 2022, XCN se actualizó y se volvió a denominar para permitir funciones de gobernanza nativas inherentes al contrato inteligente de token.

XCN tiene algunos usos diferentes. En Sequence, un libro mayor como servicio diseñado para empresas, XCN se usa para pagar tarifas comerciales. XCN también se puede utilizar en otros productos Chain. Además, los participantes de XCN pueden participar en Chain DAO para votar las Propuestas de mejora de la cadena (CIP), obtener recompensas por asegurar el protocolo y votar por los beneficiarios de las subvenciones.

XCN se actualizó en marzo de 2022 para que pudiera usarse para funciones de gobernanza nativas inherentes al contrato inteligente de token. Esta actualización permite a los participantes de XCN participar en las decisiones sobre el futuro del Protocolo de la Cadena a través de la cadena votación.

Chain Token juega un papel importante en el ecosistema de Chain Protocol al proporcionar una forma de pagar tarifas, acceder a funciones premium y participar en la gobernanza en cadena. Si está buscando una criptomoneda con utilidad, XCN puede ser una buena elección para ti.

Nube de cadenas para Web 3.0

Chain Cloud Services es una ventanilla única para los desarrolladores de Web 3.0. Proporciona gratis, Puntos finales de llamada a procedimiento remoto público (RPC) para desarrolladores, junto con Premium y Planes empresariales repletos de herramientas avanzadas para desarrolladores. La Cadena de Nubes es impulsado por una red de nodos descentralizados y distribuidos globalmente, lo que lo convierte en una opción razonable para los desarrolladores y proyectos de blockchain que necesitan acceso a datos en cadena. La interfaz de programación de aplicaciones (API) estándar está disponible para todos y es de uso gratuito en el momento de escribir este artículo. Los desarrolladores pueden usar sus puntos finales de RPC para acceder a Bitcoin, Ethereum, BSC y Solana sin necesidad de ingresar ningún información de usuario o credenciales de inicio de sesión.

Como proveedor líder de servicios de infraestructura de cadena de bloques, Chain es excepcionalmente colocado para ayudarlo con todas sus necesidades cuando se trata de desarrollar aplicaciones Web 3.0, incluidas las siguientes:

- Chain ofrece puntos finales RPC públicos gratuitos para que los desarrolladores puedan acceder a Bitcoin, Ethereum, BSC y Solana sin necesidad de ingresar ninguna información de usuario o credenciales de inicio de sesión. Todo lo que necesita es una clave API.
- Los planes Premium y Enterprise tienen herramientas avanzadas para desarrolladores, lo que los hace útiles para aquellos que necesitan un poco de ayuda adicional al crear sus aplicaciones.
- Su red de nodos descentralizada y distribuida globalmente garantiza que siempre tenga acceso a los datos que necesita cuando los necesita.

Si está buscando un proveedor de servicios de infraestructura de blockchain, explore Chain Cloud Services. Tienen todo lo que necesita para crear aplicaciones Web 3.0. Puede hacerlo navegando a https://docs.chain.com.

EN ESTE CAPÍTULO

Capítulo 11

Ponerse a trabajar con IBM

En este capítulo, le presento las iniciativas blockchain de IBM, que IBM está fusionando con sus otras tecnologías innovadoras, como Bluemix, un completo Platform as a Service (PaaS) para la creación de aplicaciones, y Watson, su súper computadora.

La tecnología Blockchain crea un intercambio de valor casi sin fricciones. La inteligencia artificial acelera el análisis de cantidades masivas de datos. La fusión de las dos capacidades será un cambio de paradigma que afectará la forma en que hacemos negocios y asegurar nuestros dispositivos electrónicos conectados.

Si está involucrado en las industrias de Internet de las cosas (IoT), atención médica, almacenamiento, transporte o logística, se beneficiará de la información en este capítulo. Además, si es un emprendedor y le gustaría conocer las nuevas capacidades que vienen con la integración de inteligencia artificial (IA) y cadena de bloques en una plataforma de aplicación escalable, este capítulo es para usted.

Plataforma de cadena de bloques de IBM

IBM Blockchain Platform es una plataforma basada en la nube para crear, ejecutar y gestionar redes de cadena de bloques. Está diseñado para facilitar a las organizaciones la adopción y el uso de la tecnología blockchain en sus operaciones.

IBM Blockchain Platform proporciona una variedad de herramientas y servicios para desarrollar e implementar aplicaciones descentralizadas (dApps) sobre una red de cadena de bloques.
Admite una variedad de tecnologías de cadena de bloques populares, incluidas Hyperledger Fabric, Ethereum y Corda, y se puede usar para construir redes con diferentes
niveles de complejidad y escalabilidad.

La plataforma también incluye características como la generación automática de contratos inteligentes, análisis en tiempo real y herramientas de administración de redes, que pueden ayudar a las organizaciones a diseñar, implementar y mantener más fácilmente sus aplicaciones de cadena de bloques. Además, IBM Blockchain Platform ofrece una gama de seguridad y cumplimiento
características para ayudar a proteger contra amenazas como la piratería, el fraude y las filtraciones de datos.

En general, IBM Blockchain Platform tiene como objetivo proporcionar a las organizaciones una plataforma completa y fácil de usar para construir y ejecutar redes de cadenas de bloques, con el objetivo de ayudarlas a aprovechar de manera más efectiva los beneficios de
tecnología blockchain en sus operaciones.

Cadena de suministro

IBM tiene una solución Blockchain para la transparencia de la cadena de suministro. Entienden que mover mercancías es un proceso complejo que involucra a diferentes partes con diferentes
prioridades Las cadenas de suministro modernas son monitoreadas a través de una red de dispositivos IoT que escanean los productos a medida que pasan de la producción al envío y finalmente lo hacen
en manos del usuario final. La cadena de bloques habilitada para IoT puede almacenar las temperaturas, la posición, los tiempos de llegada y el estado de los contenedores de envío a medida que se mueven.
Las transacciones de blockchain inmutables ayudan a garantizar que todas las partes puedan confiar en los datos y tomar medidas para mover los productos de manera rápida y eficiente. Puede habilitar la transparencia de la cadena de suministro aprovechando una plataforma blockchain empresarial para realizar transacciones con sus socios de la cadena de suministro de una manera más confiable y eficiente.

La cadena de bloques de IBM puede ayudarlo a compartir datos con otras partes. Compartir datos a través de una cadena de bloques puede ser bueno para los negocios porque permite que las partes colaboren y compartan de manera transparente, con un registro claro de qué sucedió y cuándo. Pero si lo hace públicamente en una cadena de bloques, puede ser problemático porque sus competidores pueden usar los datos para obtener una ventaja sobre su empresa. Compartir datos en una plataforma blockchain empresarial es mejor porque usted decide quién puede ver sus datos. Con una solución de transparencia de la cadena de suministro, puede crear un libro mayor inmutable, distribuido y compartido para realizar transacciones con sus socios de la cadena de suministro de una manera más confiable y eficiente.
forma. En un mundo donde la velocidad, la precisión y el cumplimiento son primordiales, blockchain brinda una solución que puede ayudarlo a alcanzar sus objetivos.

Las plataformas empresariales de blockchain como IBM Blockchain ofrecen beneficios únicos para gestión de la cadena de suministro, incluyendo:

» La capacidad de rastrear bienes a lo largo de la cadena de suministro desde el proveedor al cliente

» Una visión compartida de la cadena de suministro en la que todos los miembros pueden confiar

» Visibilidad mejorada de la ubicación y el estado de las mercancías en tránsito

» Acceso prioritario a las temperaturas, posiciones y tiempos de llegada de los contenedores de envío

» Mejora del cumplimiento de las normas de seguridad alimentaria

» La capacidad de resolver disputas rápidamente con una mayor transparencia en todos aspectos del envio

Comercio mundial

IBM también ha desarrollado una solución de cadena de bloques para el comercio. El mundo se encuentra actualmente en un estado final de globalización en el que casi todos los países y culturas están completamente interconectados y son interdependientes. Experimentas esto como si tuvieras un fuerza de trabajo distribuida, donde puede trabajar con equipos en China, India y Europa como parte regular de su día. Su empresa puede depender completamente de el trabajo realizado en otro país. Por ejemplo, el 90 por ciento de los semiconductores avanzados del mundo se fabrican en Taiwán. Sin el trabajo de la gente de Taiwán, el mundo ya no podría producir productos electrónicos baratos. La pandemia de COVID-19 reveló una de las otras características de la globalización total: la libre circulación de personas a través de las fronteras.

IBM se está inclinando hacia cómo el mundo depende cada vez más del comercio transfronterizo. Tener una solución que fomente una mayor confianza y transparencia es más importante que nunca. Ahí es donde la experiencia de IBM Blockchain en estrategia, desarrollo rápido de productos, gobierno y regulación ayuda a las redes de blockchain a expandir la membresía, una parte esencial para construir una red exitosa. Cadena de bloques de IBM también ofrece una nueva clase de comercio transparente, con riesgo mitigado y estandarizado Soluciones de seguro de crédito financiero y comercial que pueden ayudarlo a encontrar nuevas oportunidades y mercados al mismo tiempo que reduce el riesgo y los costos operativos.

Con IBM Blockchain, las empresas pueden disfrutar de una mayor confianza y transparencia en el comercio transfronterizo. Esto se debe a que blockchain crea un registro compartido e inmutable de todas las transacciones dentro de una red. Esto significa que cada miembro de la red puede ver cada transacción que ha tenido lugar, lo que ayuda a fomentar transparencia y confianza. Además, blockchain permite a las empresas verificar la autenticidad de los documentos de forma rápida y sencilla, como conocimientos de embarque, contratos, y facturas, que pueden ayudar a reducir el fraude y ahorrar tiempo y dinero.

Otra forma en que IBM Blockchain está ayudando a establecer el liderazgo en la nueva era del comercio es ayudando a crear nuevos centros comerciales en todo el mundo. Al convocar nuevas redes comerciales y reunir a compradores y vendedores de diferentes geografías, IBM Blockchain está ayudando a crear nuevas oportunidades para el comercio transfronterizo. Además, al reducir las barreras de entrada para las pequeñas empresas, IBM Blockchain está abriendo nuevos mercados y creando cadenas de suministro globales más inclusivas.

Por último, con sus soluciones transparentes, estandarizadas y con riesgo mitigado para el seguro de crédito y comercio, IBM Blockchain está ayudando a las empresas a encontrar nuevos oportunidades al mismo tiempo que reduce el riesgo y los costos operativos. Por ejemplo, las empresas pueden ahorrar tiempo y dinero al automatizar todo el proceso de solicitud de crédito en la cadena de bloques y al mismo tiempo reducir el riesgo de fraude. Además, mediante el uso de blockchain para realizar un seguimiento de las transacciones desde el principio hasta el final, las empresas pueden obtener información sobre el cliente. posiciones financieras e historiales de transacciones, que pueden ayudar a reducir el riesgo o términos de optimización.

En el mundo interconectado de hoy, el comercio transfronterizo es más importante que nunca. Pero con esta mayor dependencia del comercio transfronterizo viene una mayor presión sobre las empresas para fomentar una mayor confianza y transparencia. Por lo tanto, mientras está considerando una solución para satisfacer sus necesidades en el comercio, debe ver lo que IBM puede hacer para ti.

Cuidado de la salud

La tecnología blockchain de IBM se ha utilizado en las industrias de la salud y las ciencias de la vida para abordar varios desafíos, incluida la falta de interoperabilidad entre diferentes sistemas, preocupaciones sobre la privacidad de los datos y la necesidad de una mejor trazabilidad en las cadenas de suministro. Estos problemas se han vuelto aún más apremiantes con la pandemia de COVID-19, ya que las organizaciones de atención médica han tenido que adaptar sus cadenas de suministro para satisfacer la demanda de equipos de protección y han trabajado para desarrollar tratamientos, pruebas y vacunas. La tecnología blockchain de IBM se ha utilizado para ayudar a abordar estos desafíos al proporcionar una plataforma segura y descentralizada para almacenar y compartir datos. También se ha utilizado para facilitar la comunicación entre diferentes sistemas de registros médicos electrónicos y para ayudar a combatir las drogas. falsificación

Se espera que el creciente mercado de atención médica que utiliza la tecnología blockchain tenga un valor de $ 126 mil millones para 2030. Hay muchas maneras en que se puede usar en el cuidado de la salud, como ayudar a prevenir la falsificación de medicamentos, facilitar el intercambio y la gestión de información médica y el seguimiento. envíos de material médico. También se ha utilizado durante la pandemia de COVID-19 para ayudar con cosas como contacto

rastrear y compartir datos de investigación. IBM tiene cuatro formas principales en las que respalda la tecnología de atención médica utilizando blockchain:

» IBM está ayudando a asegurar las cadenas de suministro de equipos de protección personal (PPE) mediante el seguimiento de la procedencia y la autenticidad de los productos de PPE.

» IBM está trabajando en un proyecto para permitir que los pacientes controlen el acceso a su salud datos.

» IBM está colaborando con compañías farmacéuticas y distribuidores para abordar los medicamentos falsificados.

» IBM está ayudando a agilizar el proceso de ensayo clínico al validar a los participantes identidad y garantizar el cumplimiento normativo.

Blockchain es particularmente adecuado para abordar los desafíos de las ciencias de la vida y la atención de la salud porque es seguro, a prueba de manipulaciones, descentralizado y transparente. Puede ayudar a garantizar la autenticidad de los productos de EPP, rastrear la procedencia de los medicamentos, proteger la privacidad del paciente y optimizar los ensayos clínicos.

La pandemia puso de relieve los muchos desafíos que enfrentan las industrias de la salud y las ciencias de la vida. Pero también mostró el potencial de la tecnología blockchain para ayudar a abordar algunos de esos desafíos. IBM Blockchain es solo un ejemplo de cómo se puede utilizar esta tecnología para asegurar las cadenas de suministro, proteger la privacidad de los pacientes, optimizar los ensayos clínicos y más. A medida que continuamos lidiando con la pandemia, es importante que exploremos todas las formas en que blockchain puede ayudarnos a superar estos desafíos.

IBM Blockchain tiene el potencial de transformar las industrias de la salud y las ciencias de la vida al resolver algunos de sus desafíos más apremiantes. La tecnología Blockchain puede crear una base de datos descentralizada de información de salud del paciente, una cadena de suministro de medicamentos rastreable y credenciales digitales para profesionales de la salud. Esto mejoraría la interoperabilidad, la privacidad y la trazabilidad de la cadena de suministro y, al mismo tiempo, garantizaría que los pacientes reciban medicamentos seguros y eficaces.

Blockchain empresarial en Bluemix

IBM ahora ofrece tecnología blockchain que se integra con su tradicional ofertas, como IBM Bluemix. Bluemix es un PaaS basado en la nube y de estándares abiertos para construir y administrar aplicaciones. IBM ha integrado una pila de cadena de bloques de Hyperledger, que forma parte de la fundación Lynx y está estableciendo las mejores prácticas en la tecnología de cadena de bloques.

Querrá prepararse para cambios rápidos y fundamentales dentro de las iniciativas de cadena de bloques de IBM. La tecnología es muy nueva y todavía está en incubación, tanto en IBM como en Hyperledger.

Hyperledger tiene varios subproyectos diferentes en desarrollo. A partir de este escrito, IBM está usando Fabric, pero puede abrir Bluemix a otros proyectos. Fabric es de código abierto y se encuentra en desarrollo activo dentro de Hyperledger. Puedes empezar a probar Fabric en Bluemix usando Hyperledger Fabric v0.6. Sin embargo, IBM advierte contra la ejecución de transacciones valiosas directamente en Fabric v0.6 o cualquier versión anterior.

Bluemix es la oferta de nube más nueva de IBM. Es una implementación de IBM arquitectura de nube abierta basada en Cloud Foundry, un PaaS de código abierto.

Bluemix le permite crear aplicaciones, implementarlas y administrarlas rápida y fácilmente. Bluemix ofrece servicios de nivel empresarial que pueden integrar con aplicaciones sin necesidad de saber instalarlas o configurarlas.

La Figura 11-1 muestra cómo IBM relaciona diferentes aspectos de blockchain y los sistemas de IBM. Puedes encontrar más en https://goo.gl/12Q6no.

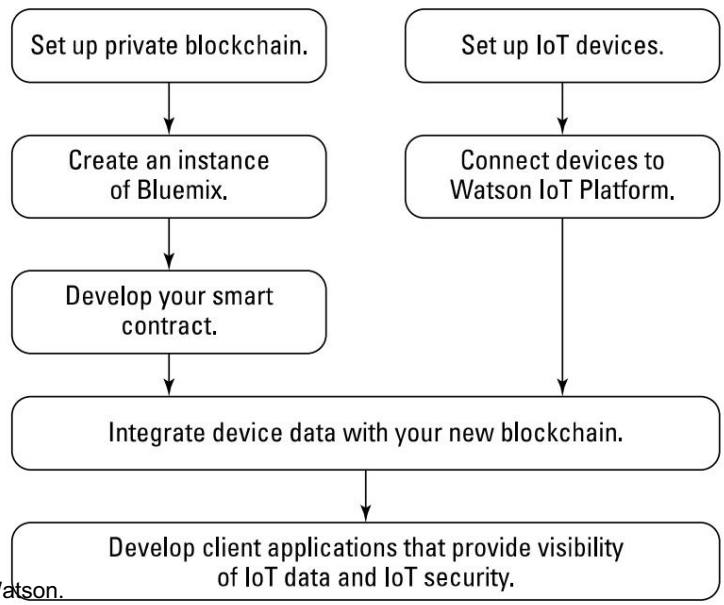


FIGURA 11-1: Cómo se fusionan IBM Bluemix e IoT con IBM Watson.

IBM Bluemix proporciona cuatro cosas principales:

» Infraestructura informática basada en las necesidades arquitectónicas de sus aplicaciones

» La capacidad de implementar aplicaciones en una nube pública o dedicada de Bluemix

» Herramientas de desarrollo, como editores de código y administradores

» Acceso a herramientas de código abierto de terceros en su sección de servicio

Bluemix le brinda todo lo que necesita para crear su aplicación. Ahora también ofrece infraestructura de cadena de bloques para probar.

Disponen de un servicio para integrar tus aplicaciones con la blockchain de Bluemix.
A partir de este escrito, hay dos modelos de precios. Una cuenta gratuita le proporciona lo que necesita para probar su idea. Obtiene cuatro pares y una autoridad de certificación para firmar transacciones, así como un tablero con registros, controles y API.

El plan empresarial tiene un precio de $10,000 al mes y ofrece mayor seguridad y velocidad que el modelo libre.

Dos notables pioneros empresariales están usando Bluemix y Hyperledger Integración de tela:

» Wanxiang: La empresa de componentes automotrices más grande de China, Wanxiang está trabajando con IBM para implementar una cadena de bloques privada. Están incrustando derechos de propiedad en cosas como los autos eléctricos. El objetivo es reducir los costos para los consumidores por el arrendamiento de equipos. Wanxiang utilizará su tecnología blockchain para rastrear la vida útil de los componentes y restaurar las baterías usadas. Bluemix se encargará de todo lo demás.

» KYCK!: La startup de tecnología financiera (ntech) KYCK! está utilizando IBM la integración de blockchain como una forma novedosa de abordar Know Your Customer (KYC) necesidades de corretaje. Este gasto es limitante y costoso para los bancos y otros servicios financieros. KYC se hace para prevenir el lavado de dinero y el comercio ilícito, y para combatir el terrorismo. KYCK! está construyendo una videoconferencia y cifrada plataforma de envío de documentos. Permitirá a los corredores trabajar y autenticar a los clientes que la empresa no ha conocido en persona.

IBM también ha creado tres aplicaciones simples de Chaincode que le permiten jugar con la red IBM Blockchain:

» Canicas: Canicas es una aplicación que demuestra la transferencia de canicas entre dos usuarios. Le permite ver cómo puede mover activos en una cadena de bloques.

» Commercial Paper: Commercial Paper es una red comercial de blockchain implementado en IBM Blockchain. Puede crear nuevos papeles comerciales para negociar, comprar y vender operaciones existentes y auditar la red.

» Car Lease: Car Lease se parece mucho a la demostración de Marbles. Está diseñado para permitirle interactuar con los activos. Puede crear, actualizar y transferir. También permite una tercero para ver el historial.

La cadena de bloques inteligente de Watson

La supercomputadora de IBM, Watson, también está disponible en la plataforma Bluemix. Watson es un sistema informático artificialmente inteligente de computación cognitiva. Puede analizar datos estructurados y, lo que es más impresionante, datos no estructurados a una velocidad increíble.

WARNING

Esta tecnología todavía está en desarrollo y los clientes se han quejado de su verdadera capacidad para comprender el lenguaje escrito no estructurado.

Watson puede responder a las preguntas que se le plantean a través del lenguaje natural y aprender a medida que absorbe más información. La implicación de esta tecnología, cuando se combina con la tecnología blockchain, es asombrosa. Una de las primeras implementaciones está dentro el espacio IoT. Existe una gran necesidad de proteger los datos que se emiten desde estos dispositivos y luego hacerlos procesables e inteligentes.

La computación cognitiva de Watson simula procesos de pensamiento humano y utiliza el protocolo MQTT. Como una mente humana, crece con el tiempo. Sus sistemas de autoaprendizaje utilizan minería de datos, reconocimiento de patrones y procesamiento de lenguaje natural para imitar la forma en que funciona su cerebro. Watson procesa a una velocidad de 80 teraops por segundo (un teraop es un billón de operaciones de punto flotante). Para poner esto en contexto, eso replica, y en algunos casos supera, un alto funcionamiento la capacidad del ser humano para responder preguntas. Watson puede hacer esto accediendo a 90 servidores con un almacén de datos combinado de más de 200 millones de páginas de información, que procesa contra seis millones de reglas lógicas. Watson tiene aproximadamente el tamaño de diez refrigeradores, pero se ha vuelto más pequeño y más rápido.

La Figura 11-2 muestra cómo IBM Watson relaciona diferentes aspectos de blockchain y sistemas IBM. Sumérgete más en IBM https://goo.gl/12Q6no.

IBM está aplicando estas increíbles capacidades a las fuentes de datos de IoT que utilizan la implementación de Chaincode. Chaincode es un sistema de contrato inteligente de Hyperledger. Así es como funcionará la cadena de bloques habilitada para Watson para dispositivos IoT:

- Los dispositivos IoT envían datos a sus libros de contabilidad privados de blockchain para incluirlos en transacciones compartidas como un registro resistente a la manipulación marcado en el tiempo.
- Los socios y los proveedores de servicios de terceros también pueden acceder y suministrar datos de IoT, sin necesidad de un control y una gestión centrales.
- Todas las partes pueden firmar y verificar los datos, lo que limita las disputas y garantiza que cada socio sea responsable de su desempeño individual.

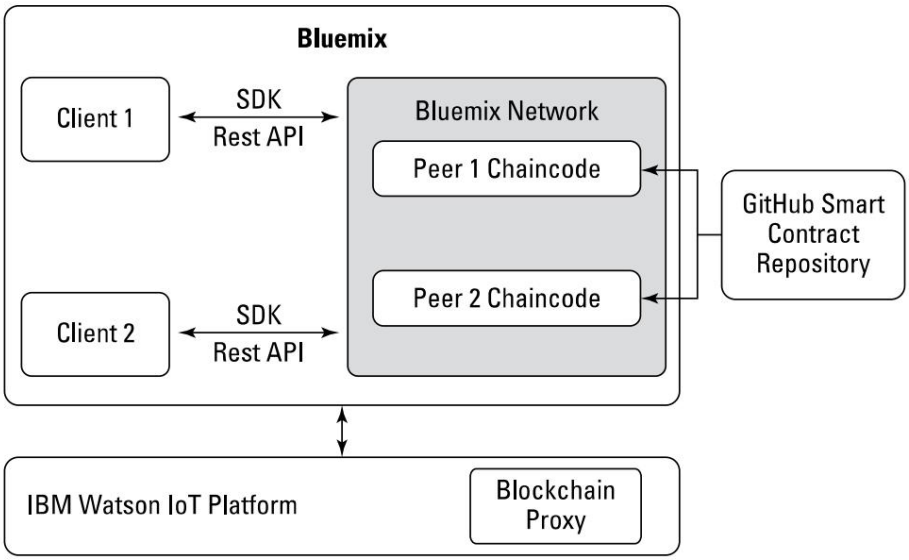


FIGURA 11-2: Cómo Bluemix integra clientes, pares e IBM Watson.

Esta es una implementación simple que no aprovecha todas las funciones y capacidades de Watson. La capacidad de Watson para aprender y hacer sugerencias, y actualizar información desactualizada, realmente la convertirá en una poderosa aplicación habilitada para blockchain en el futuro.

Puede integrar la plataforma IoT de Watson con Fabric de Hyperledger. Esta integración le permite ejecutar contratos de Chaincode a través de oráculos de computación cognitiva. La plataforma de IoT de Watson tiene una capacidad integrada que le permite agregar datos de IoT seleccionados a su propia cadena de bloques privada para crear un oráculo. Esto le ayuda a proteger los datos para que no sean vistos por terceros no autorizados.

Cuando haya establecido un espacio de trabajo de Bluemix, puede agregar servicios selectivos, incluida la plataforma IoT que integra varias tecnologías. Fabric es la tecnología de cadena de bloques que proporciona la infraestructura de cadena de bloques privada para pares distribuidos que replica los datos del dispositivo y valida la transacción a través de contratos seguros.

Watson IoT Platform traduce los datos de dispositivos existentes, de uno o más tipos de dispositivos, al formato que necesitan las API de contratos inteligentes. La plataforma IoT de Watson filtra los datos irrelevantes del dispositivo y solo envía los datos requeridos al contrato. La Figura 11-3 muestra cómo IBM Watson se integra con dispositivos IoT y API. watson actúa como el oráculo de Chaincode y le permite controlar qué información conocen las partes involucradas en el contrato. Esta funcionalidad es importante para la privacidad.

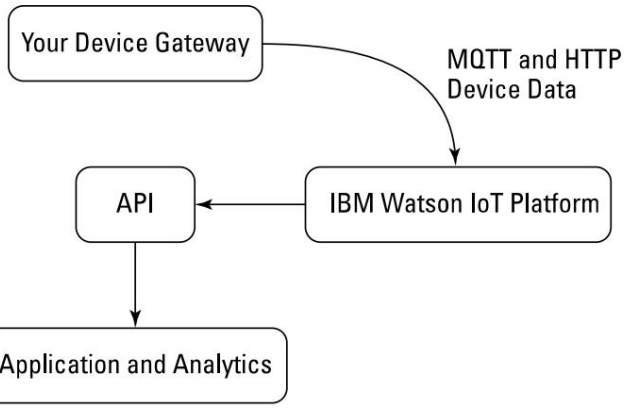


FIGURA 11-3:
El Watson/API/
dispositivo

Construyendo su red de inicio en Big Blue

La tecnología blockchain de IBM y la plataforma IoT ofrecen nuevas herramientas prometedoras y pueden aprovecharse para abordar muchos problemas que enfrentan las empresas que intentan escalar:

» Seguridad: el enorme volumen de datos que se recopila de millones de dispositivos
plantea problemas de privacidad de la información. Además, organizaciones nefastas han utilizado
dispositivos IoT pirateados para paralizar sitios web con negación distribuida de
ataques de servicio.

» Costo: El alto volumen de mensajes, datos generados por los dispositivos y
Los procesos analíticos aumentan a medida que más dispositivos se conectan y utilizan
esos datos

» Arquitectura: Las plataformas en la nube centralizadas siguen siendo un cuello de botella en la
Soluciones IoT y un punto central de ataque.

Las redes de IoT distribuidas basadas en estándares abiertos de IBM pueden resolver muchos de los problemas asociados con las soluciones de IoT centralizadas y basadas en la nube actuales. Los dispositivos conectados se comunican directamente con los registros distribuidos. Luego, los datos de esos dispositivos son utilizados por terceros para ejecutar contratos inteligentes, lo que reduce la necesidad de monitoreo humano.

La plataforma IBM Watson IoT con una integración Fabric replica los datos a través de una red blockchain privada y elimina la necesidad de recopilar y almacenar todos los datos de IoT de forma centralizada. Las redes blockchain descentralizadas también mejoran la seguridad de los dispositivos IoT. Se crean identidades digitales únicas para cada dispositivo a lo largo del tiempo. Esta nueva forma de crear y asegurar la identidad es excepcionalmente difícil de falsificar.

Estas nuevas identidades de blockchain permiten que los dispositivos IoT firmen transacciones que permiten la ejecución de contratos inteligentes. Una aplicación práctica de esto sería un producto de seguro que se alimentara con datos de un automóvil inteligente sobre el comportamiento de conducción de diferentes individuos El auto enviaría datos para ser publicados en Fabric; el producto de seguro creado con Chaincode reconocería los nuevos datos y la identidad de su automóvil y actualizaría su póliza.

Las posibilidades son casi infinitas e IoT ha presentado enormes oportunidades para empresas y consumidores, especialmente en las áreas de atención médica, almacenamiento, transporte y logística.

Hay tres niveles principales de soluciones de IoT compatibles con la nube de IBM que satisfacen las necesidades de diferentes problemas comerciales de IoT:

» Device Gateway: Device Gateway es para dispositivos inteligentes o sensores que recopilan datos sobre el mundo físico. Esto podría ser cosas como sensores meteorológicos, monitoreo de temperatura para contenedores refrigerados o datos de estadísticas vitales para un paciente. Estos dispositivos IoT envían sus datos a través de Internet para su análisis y procesamiento.

» IBM Watson IoT Platform: IBM combina su superordenador con su IoT Plataforma para recopilar datos de dispositivos IoT y luego analizar los datos y tomar acciones posteriores para resolver problemas. Watson proporciona aprendizaje automático, razonamiento automático, procesamiento de lenguaje natural y análisis de imágenes que mejoran la capacidad de procesar los datos no estructurados recopilados de la sensores

» IBM Bluemix: Bluemix es una plataforma de nube basada en estándares abiertos para crear, ejecutar y administrar aplicaciones y servicios. Admite aplicaciones de IoT al facilitar la inclusión de capacidades analíticas y cognitivas en esas aplicaciones.

Puede obtener más información sobre la solución de IBM en https://developer.ibm.com/tecnologías/cadena de bloques.

4

Impactos de la industria

EN ESTA PARTE . . .

Comprenda el futuro de la industria de servicios financieros cuando utilice la tecnología blockchain para mover dinero alrededor del mundo de manera rápida y económica.

Aclare su conocimiento de bienes raíces globales en relación con la tecnología blockchain.

Identificar oportunidades en la industria de seguros para reducir el fraude y aumentar las ganancias a través de nuevos instrumentos de seguros.

Examinar las implicaciones para las grandes industrias de los sistemas permanentes dentro de las organizaciones gubernamentales y los marcos legales.

Aclare otras grandes tendencias globales en la tecnología de cadena de bloques y cómo darán forma al mundo en el que vive y a las herramientas que usa todos los días.

EN ESTE CAPÍTULO

Capítulo 12

Tecnología financiera

Los que adoptaron la tecnología blockchain fueron los bancos, los gobiernos y otros instituciones financieras, y con los usuarios de blockchain de rápido crecimiento, también. Las poderosas herramientas que se están construyendo para administrar y mover dinero remodelarán nuestro mundo de maneras nuevas e inesperadas, por lo que tiene sentido que la tecnología financiera (ntech) salte a bordo.

Este capítulo le brinda información privilegiada sobre lo que los gobiernos están haciendo actualmente con la tecnología blockchain y cómo le afectará. Fintech toca su vida todos los días, ya sea que lo sepa o no.

En este capítulo, le presento las futuras tendencias bancarias, las nuevas regulaciones y las nuevas herramientas que pueden ayudarlo a mover dinero de manera más rápida y económica. También explico nuevos tipos de vehículos de inversión y otras innovaciones de blockchain. Finalmente, le advierto sobre los riesgos potenciales de las inversiones que involucran moneda virtual y nuevos productos financieros habilitados con tecnología blockchain.

Acarreando su bola de cristal: Tendencias bancarias futuras

La banca fue la primera industria en reconocer la amenaza de Bitcoin y luego el potencial de blockchain para transformar la industria. El sector bancario está altamente regulado y las tarifas para organizar y operar como banco son costosas. estos pesados

Las regulaciones han sido un escudo aislante y protector para toda la industria, así como una carga. La aplicación de dinero digital rápido, eficiente, que no conlleva el costo del manejo de efectivo y que es rastreable a medida que se mueve a través del sistema financiero, era una propuesta embriagadora y amenazante. La idea de que el valor puede mantenerse fuera del control de las autoridades centrales también despertó el interés de las instituciones financieras y los gobiernos que respaldan las monedas.

Inicialmente, las instituciones financieras y los gobiernos intentaron silenciar blockchain con la regulación. Hoy, están adoptando blockchain a través de inversiones en todos los ámbitos.

En 2013 y 2014, la Comisión de Bolsa y Valores de EE. UU. (SEC) emitió una advertencia a los inversores sobre los riesgos potenciales de las inversiones que involucran moneda virtual. La advertencia fue que los inversionistas podrían verse atraídos por la promesa de altos rendimientos y no serían lo suficientemente escépticos sobre el nuevo espacio de inversión que era tan novedoso y vanguardista. Según la SEC, la moneda digital fue una de las diez principales amenazas para los inversores. Hoy, la SEC está lista para comprometerse con empresas e inversores a medida que las criptomonedas ganan terreno en todas las industrias.

Ni siquiera dos años después, países de todo el mundo, incluidos el Reino Unido, Canadá, Australia, Japón y China, comenzaron a investigar cómo podían crear sus propias monedas digitales, apoderarse de las criptomonedas y poner dinero en la cadena de bloques. En 2018, Venezuela lanzó una criptomoneda llamada Petro.
El lanzamiento de Petro es un punto de inflexión significativo para la criptomoneda porque Venezuela fue la primera nación soberana en emitir su propia criptomoneda. El Petro lamentablemente fue utilizado para defraudar a los ciudadanos venezolanos. Sin embargo, el futuro puede tener una moneda digital respaldada por petróleo para Venezuela.

La promesa de Blockchain de un libro mayor intransigente ha sido un sistema atractivo para los gobiernos que buscan reducir el fraude y mejorar la confianza.
Las innovaciones en la tecnología de cadenas de bloques prometían poder manejar los miles de millones de transacciones necesarias para respaldar las economías, lo que hace que una criptomoneda sea factible a escala.

Las cadenas de bloques son en sí mismas registros permanentes e inalterables de cada transacción que se ingresa en ellas. Poner el suministro de dinero de un país en una cadena de bloques controlada por un banco central sería completamente transformador porque habría un registro permanente de todas las transacciones financieras, existentes en algún nivel dentro de su registro de cadena de bloques, incluso si no fueran visibles para el público. La tecnología Blockchain y las monedas digitales reducirían el riesgo y el fraude y les darían el control final en la ejecución de la política monetaria y los impuestos. No sería anónimo como lo fue Bitcoin al principio. De hecho, todo lo contrario: les permitiría un seguimiento completo y auditable de cada transacción digital realizada por individuos y empresas. Incluso podría permitir que los bancos centrales reemplacen el papel de los bancos comerciales en la circulación de dinero.

La pregunta de cómo será el futuro de la banca puede ser aterradora y emocionante. Los consumidores ahora pueden pagarles a sus amigos a través de sus teléfonos casi instantáneamente en casi cualquier tipo de moneda o criptomoneda. Cada vez más tiendas minoristas han comenzado a utilizar criptomonedas como una forma de pagar bienes y aceptar pagos de los clientes. En Kenia, usar criptomonedas es más normal que no hacerlo. Pero esta todavía no es la opción principal para la mayor parte del mundo. Los mercados occidentales aún se encuentran en la fase de adopción temprana.

Dado que la mayoría de las personas tienen su riqueza bloqueada en moneda de curso legal emitida por los gobiernos o bloqueada en activos que se encuentran dentro de los sistemas gubernamentales existentes, las innovaciones tecnológicas deben fusionarse con estos sistemas existentes antes de que veamos la utilidad principal de la cadena de bloques o las monedas digitales. Si los reguladores encuentran formas de gravar y registrar cuentas, la adopción masiva de billeteras orientadas al cliente con tokens digitalizados está a dos o tres años de distancia.

El mercado de empresa a empresa comenzará a utilizar blockchain mucho más rápido. Se está probando un sistema reforzado para producción con las políticas y operaciones asociadas. Ripple y R3, entre otros, han trabajado arduamente para que esto sea posible.
Estos sistemas se enfocarán primero en la creación institucional de representaciones digitalizadas de depósitos. Estos son pagarés entre departamentos organizativos internos y entre socios de confianza, como proveedores. Los reguladores, los bancos centrales y las autoridades monetarias están invirtiendo fuertemente para que esto sea posible. Canadá y Singapur se han estado moviendo muy rápidamente.

Las regulaciones Conozca a su cliente (KYC) y Anti-Money-Laundering (AML) requieren que los bancos sepan con quién están haciendo negocios y se aseguren de que no están participando en el lavado de dinero o el terrorismo. Los bancos que emiten criptomonedas aún tienen importantes desafíos que superar. Para cumplir con las normas KYC y AML, necesitan conocer la identidad de todas las personas que utilizan su moneda. En muchos casos, las cuentas bancarias de las personas ya son un servicio de transacciones de débito y crédito, como libros de contabilidad distribuidos en cadenas de bloques, a excepción de las centralizadas. Los primeros candidatos en esta área serán regiones donde los reguladores, los bancos y los bancos centrales trabajen juntos. Singapur y Dubai son buenos candidatos que ya tienen iniciativas de blockchain.

Mover dinero más rápido: más allá de las fronteras y más

Evaluar el volumen de transacciones necesario para que una cadena de bloques maneje la moneda de una economía como la del Reino Unido o la de los EE. UU. es difícil. Solo en EE. UU. se procesan miles de millones de transacciones al día y más de 17 billones de dólares en valor al año. ¡Esa es mucha responsabilidad para una nueva tecnología! La nación quedaría paralizada si su suministro monetario se viera comprometido.

El Fondo Monetario Internacional, el Banco Mundial, el Bank for International
Los asentamientos y los banqueros centrales de todo el mundo se han reunido para discutir
tecnología de cadena de bloques. El primer paso hacia dinero más rápido y más barato sería
adopción de una cadena de bloques como protocolo para facilitar las transferencias bancarias e interbancarias
asentamiento. Monedas digitales oficiales que los ciudadanos comunes usan a diario
vendría mucho más tarde.

Los consumidores individuales no sentirían directamente la reducción de costos al utilizar un
blockchain para la liquidación interbancaria. Los ahorros se verían en el resultado final del banco como
reducciones de costos por las tarifas cobradas por los intermediarios.

Los consumidores seguirán queriendo locales minoristas y bancos comerciales por lo que se prevé.
futuro capaz. Pero los millennials ya han adoptado los pagos activados por aplicaciones a través de
PayPal, Venmo, efectivo y más. Una nueva forma de pagar a través de sus teléfonos no
desconcertarlos.

El gran desafío es que si todo el dinero es digital, comprometerlo podría ser catastrófico. Es posible que la
arquitectura de los sistemas blockchain sea fuerte
suficiente. El problema podría ser, en cambio, que el código dentro del sistema se ejecuta en
de una manera inesperada, como sucedió en el hackeo de la organización autónoma descentralizada (DAO)
en Ethereum (ver Capítulo 5). Si la criptomoneda estuviera operando en una cadena de bloques pública
tradicional, entonces el 51 por ciento de los nodos en la red
Tendría que estar de acuerdo con el tema. Poner en marcha un acuerdo puede llevar un
mucho tiempo, y no sería práctico para las empresas y las personas que necesitan estable
y dinero seguro en todo momento.

REMEMBER

Muchas cadenas de bloques funcionan como democracias. Se necesita la mayoría (51 por ciento) de la red
de nodos de una cadena de bloques para realizar un cambio.

Creando una historia permanente

La soberanía de los datos y la privacidad digital serán temas importantes en el futuro.
La prevención del fraude será más fácil porque si toda la economía utiliza una criptomoneda, siempre habrá
un rastro auditable dentro de la cadena de bloques que
lo asegura. Esto es tentador para las fuerzas del orden público, pero una pesadilla para los consumidores.
privacidad.

Desde la perspectiva del cliente, ya existe un registro de auditoría para todo lo que
compra con tarjeta de crédito o débito. Desde la perspectiva de una institución, es beneficioso tener pistas
de auditoría porque aumenta la transparencia de la documentación y
ciclos de vida de los movimientos de estos activos entre diferentes regiones. agrega
legitimidad para el comercio de activos y les permite incorporar el cumplimiento en sus
transacciones del día a día.

Las reglas del "derecho al olvido" en Europa, que permiten a los ciudadanos el derecho a que sus datos no se propaguen para siempre en Internet, son un desafío difícil para las cadenas de bloques, porque las cadenas de bloques nunca pueden olvidar. Los gobiernos y las corporaciones tendrían registros históricos permanentes de cada transacción, lo que podría ser devastador para la seguridad nacional si estuvieran expuestos al público. O, en el caso de una empresa, puede permitir que sus competidores tengan información privilegiada sobre cómo están invirtiendo sus competidores.

El mayor desafío de usar una cadena de bloques sin permiso como Ethereum o Bitcoin sería garantizar que no haya enviado dinero a un país de la OFAC para apoyar el terrorismo. La respuesta es que no puedes porque son algo anónimos y cualquiera puede abrir una billetera. Es posible crear algoritmos para rastrear el movimiento de transacciones (el gobierno de EE. UU. lo ha estado haciendo durante años), pero cualquiera puede mover valor en un mundo sin permisos.

La Oficina de Control de Activos Extranjeros mantiene sanciones a organizaciones o individuos específicos en lo que se consideran países de alta amenaza. El gobierno no puede rastrear el historial de transacciones cuando utiliza plataformas sin permiso de forma anónima.

La necesidad de KYC y AML justifica la cadena de bloques autorizada en el espacio del libro mayor compartido. La compañía de software R3 desarrolló Corda, una plataforma similar a una cadena de bloques privada y autorizada para enfrentar muchos de estos desafíos directamente. Específicamente, no transmiten globalmente los datos de sus participantes. Esto mantiene la privacidad de los datos dentro de la cadena de bloques de Corda y fue el principal requisito no funcional solicitado por los más de 75 bancos que trabajaron con R3 para adoptar la tecnología de cadena de bloques. Necesitan mantener su privacidad y cumplir con fuertes exigencias regulatorias.

Volviéndose internacional: global Productos financieros

Blockchains marcará el comienzo de muchos nuevos tipos de valores y productos de inversión. Se abrirán nuevos mercados con formas más eficientes de calcular el riesgo porque la garantía será mucho más transparente y fungible entre instituciones cuando se contabilice dentro de un sistema respaldado por blockchain.

La tecnología Blockchain también tiene aplicaciones para ayudar a reducir las estafas dentro del mercado global de almacenes para productos fraudulentos de doble venta. Las entradas de blockchain permiten a los fabricantes y reguladores documentar la procedencia de los productos y, a su vez, permite a los compradores verificar la autenticidad de lo que están comprando. Existen varias soluciones en el mercado, incluidas Everledger y Provenance.


TIP

Hernando de Soto, el famoso economista peruano, estima que proporcionar a los pobres del mundo títulos de propiedad de sus tierras, viviendas y negocios no registrados desbloquearía $9,3 billones en activos. Esto es lo que significa el término capital muerto.

Es imaginable que los países que pueden liberar su capital muerto, los bienes inmuebles no financiables que poseen, podrán agrupar y vender estos intereses en estos activos en un mercado global. Esto sería cosas como valores respaldados por hipotecas transparentes para nuevos desarrollos inmobiliarios en Colombia o Perú.

En el futuro, los países podrán liberar su capital muerto. Los propietarios de propiedades, terrenos sin desarrollar y propiedades no financiables ahora tendrán la oportunidad de vender los intereses en estos activos en un mercado global.

Estos activos serán atractivos porque los administradores de activos podrán analizar activamente los activos de bajo rendimiento dada la transparencia y la capacidad de sustituir uno por otro a través de la tecnología basada en blockchain. El uso de cadenas de bloques para administrar estos activos les dará a los gerentes el poder de poseer siempre valores de alto rendimiento, eliminando las manzanas podridas, reclasificándolos y vendiéndolos como valores nuevos.

Para los clientes no institucionales, las microinversiones serán una salida atractiva habilitada a nivel mundial y local a través de plataformas comerciales de blockchain. El uso de la tecnología de cadena de bloques también les dará los medios para invertir en empresas y sus actividades específicas sin tener mínimos ni pasar por intermediarios que se lleven un porcentaje de la inversión.

Las organizaciones autónomas descentralizadas (DAO, por sus siglas en inglés) ya existen y están creando grupos de inversión de DAO para unos pocos inversores tolerantes al riesgo y con más conocimientos técnicos. Puede pasar algún tiempo antes de que un inversor institucional utilice uno o un administrador de cartera recomiende poner dinero en un vehículo basado en DAO para sus clientes.

Los DAO eliminan gran parte del papeleo y la burocracia necesarios para invertir al crear un sistema de votación basado en blockchain y otorgar acciones a quienes invierten en su producto. Para cualquier blockchain, el concepto de "código como ley" lo hace implacable. Los riesgos son muchos, particularmente cuando hay un código mal escrito que se ejecuta de manera no deseada. Las consecuencias son que los ataques a este sistema pueden ser graves. La naturaleza transparente del sistema original, el código deficiente, brinda a los piratas informáticos un vector de ataque más amplio y les permite atacar varias veces a medida que obtienen más y más información cada vez.

En la siguiente sección, discuto los efectos y beneficios de la tecnología blockchain en la economía mundial.

Nómina sin fronteras

Nuestro mundo es global y las empresas no tienen fronteras. La nómina instantánea y casi gratuita es atractiva y ahorraría muchos dolores de cabeza a las organizaciones. Pero también hay inconvenientes.

Los mayores riesgos serán la pérdida de fondos a través de la piratería. Si recibe una compensación en criptomonedas y fue pirateado, sería imposible recuperar sus fondos. No hay un centro de resolución de disputas. No hay servicio al cliente para quejarse por la pérdida de estos fondos. Los ladrones de moneda digital tienen acceso global y son algo anónimos. El hacker podría estar en cualquier parte.

Con la estructura actual de las cadenas de bloques, el consumidor es responsable de su propia seguridad. Actualmente, los clientes no tienen la carga principal de protegerse y asegurarse contra una pérdida. Las empresas más grandes y los gobiernos ofrecen protección y seguros, y lo han hecho desde que cualquiera puede recordar. Las personas normales no han tenido que protegerse de esta manera desde que dejaron de tener su propio oro durante la época medieval (más o menos).

Estos desafíos no han impedido que las empresas procesen la nómina utilizando criptomonedas. Bitwage y BitPay compiten en el mercado del procesamiento de nóminas a través de Bitcoin. Bitwage permite a los empleados y contratistas independientes recibir parte de sus cheques de pago en criptomonedas, incluso si sus empleadores no ofrecen la opción. BitPay, por otro lado, tiene los proveedores de servicios de nómina Zuman e Incoin integrados en sus API de pago y nómina. Nuevamente, la adopción temprana está ocurriendo en áreas que antes tenían soluciones inexistentes o inadecuadas.

Comercio más rápido y mejor

Las cadenas de bloques facilitarán un comercio más rápido y posiblemente más inclusivo. La financiación del comercio mundial se ha visto restringida en los últimos años. Algunos bancos como Barclays incluso se han retirado de los crecientes mercados africanos. Dejan tras de sí un vacío de financiación del comercio. Las empresas aún necesitan capital para enviar sus productos.

Las DAO y las microinversiones podrían satisfacer esa necesidad y brindar a los inversores rendimientos más rentables que los disponibles actualmente en el mercado. La transparencia de todos los bienes que se venden, la identidad segura y el seguimiento global continuo que está todo conectado a una cadena de bloques abriría esta oportunidad para los pequeños inversores.

La interoperabilidad entre monedas, que facilitan empresas como Ripple, también permitirá un mayor comercio porque ofrecen formas más flexibles de calcular los tipos de cambio de divisas que a través de los mecanismos de transferencia. La introducción de monedas digitales más populares en los intercambios de moneda extranjera se sumará a la adaptabilidad e integración de los mercados desatendidos.

Aza Finance, formalmente llamada BitPesa, es una empresa que convierte los minutos telefónicos de M-pesa de Kenia en Bitcoin. Con esta tecnología, ofrece a las empresas una forma más rápida y económica de enviar o recibir pagos entre África y China. El comercio entre África y China es un mercado de más de $ 170 mil millones. Lleva días liquidar los pagos a través de las fronteras y las tarifas son altas. Cuando utiliza la plataforma digital de Aza Finance, los pagos son instantáneos y económicos.

Pagos garantizados

Los pagos garantizados que se permiten a través de transacciones respaldadas por blockchain aumentarán el comercio en lugares donde la confianza es baja. Los países más pobres pueden competir en el mismo campo de juego que las naciones más ricas dentro de este tipo de sistemas. A medida que esto suceda durante los próximos diez años, las economías globales cambiarán. El costo de los productos básicos y la mano de obra puede aumentar.

Las empresas globales pagan a sus empleados en función de precios competitivos, así como de los salarios anteriores de los empleados. Si las cadenas de bloques permiten la igualdad entre las divisiones económicas, no sucederá de la noche a la mañana. Los desarrolladores y otros trabajadores del conocimiento serían la excepción porque les resultará más fácil mantenerse a sí mismos basándose en el trabajo anónimo.

La inclusión financiera y el comercio global equitativo son temas muy importantes para los gobiernos. Es más probable que la adopción de monedas digitales se realice a nivel nacional en países pequeños y en desarrollo. La mayoría de los países grandes tienen estructuras de poder descentralizadas que impiden cambios rápidos en sistemas vitales como el dinero.

Las estructuras de poder central de los países pequeños les permitirán saltarse la infraestructura y la burocracia heredadas. Por ejemplo, la mayoría de los países africanos y sudamericanos no tienen teléfonos fijos ni direcciones, pero todos tienen teléfonos inteligentes y la capacidad de crear billeteras de criptomonedas. La pieza que falta es la liquidez comercial general y la capacidad de pagar las necesidades básicas, como los servicios públicos, el alquiler y los alimentos, a través de una criptomoneda.

Micropagos: La nueva naturaleza de las transacciones

Los micropagos son la nueva forma de transacciones. Las compañías de tarjetas de crédito pueden usar la tecnología blockchain para liquidar la transacción, reducir el fraude y reducir su costos propios.

Los consumidores de las sociedades capitalistas siempre necesitarán instituciones globales como Visa y MasterCard, que brindan el beneficio de la demora en el pago. Incluso si el backend cambia, aún tiene los mismos puntos de acceso para los clientes. Pero

las tarjetas físicas desaparecerán. De hecho, eso está sucediendo ahora, incluso sin la tecnología de cadena de bloques. Con la tecnología blockchain, las identidades de los clientes detrás de los pagos estarán más protegidas contra el robo.

La gente todavía necesita crédito para operar un negocio y salir adelante personalmente. Las compañías de tarjetas de crédito seguirán ganando dinero a través de las tarifas de transacción. Los créditos manejan el mundo, y los mercados de capital siempre existirán en nuestra estructura social actual. El costo de enviar dinero entre grupos disminuirá, pero eso es algo bueno para las instituciones financieras. Quieren centrarse en el servicio de proporcionar a sus clientes las mejores opciones en sus mercados bancarios o de inversión.

Exprimiendo el fraude

Bitcoin se creó como una respuesta a la crisis financiera, donde el fraude y otras acciones poco éticas provocaron el colapso de la economía mundial. Cambia de una visión del mundo de “confía o no confía” a un sistema sin confianza. Esta sutil diferencia se pierde para la mayoría. Un sistema sin confianza es aquel en el que confía y desconfía por igual de todas las personas dentro de la red. Más importante aún, la cadena de bloques proporciona un marco que permite que se realicen transacciones sin confianza.

Estos mismos tipos de marcos se pueden usar para algo más que simplemente intercambiar valor a través de la red. Permítanme compartir un ejemplo que ayudará a ilustrar el potencial.

Voy a un bar y el hombre de la puerta me detiene y me pide mi identificación. Busco en mi billetera y le entrego mi licencia de conducir. Mi licencia tiene mucha información que el portero no necesita, ni debería tener acceso (como mi dirección).
Todo lo que necesita de la identificación es que tengo más de 21 años. Ni siquiera necesita saber cuántos años tengo, solo que cumplo con los requisitos reglamentarios.

En el futuro, los sistemas de identificación de blockchain le permitirán elegir qué información exponer a qué persona y en qué nivel. Cuantos más datos anónimos tenga, más seguro será. Los sistemas de cadena de bloques ayudarán a frenar el robo de identidad y datos al no compartir información con quienes no la necesitan o no tienen permiso para verla.

Otro aspecto de la tecnología blockchain es que desplazará el fraude de donde ocurrió (tiempo pasado) a donde está ocurriendo actualmente en tiempo real. Dentro de nuestro sistema actual, las auditorías son autopsias fraccionadas de lo que ha sucedido. Viene un grupo de auditores externos, saca algunas muestras al azar y ve si todo está en su lugar. Hacer cualquier cosa más allá de esto es demasiado costoso y requiere mucho tiempo.

Los sistemas de registro que tienen tecnología de cadena de bloques integrada dentro de ellos podrán auditar cerveza a medida que se crea, agregando incompletos o inusuales a medida que están

creado. Esto les dará a los gerentes las herramientas que necesitan para corregir proactivamente antes de que se conviertan en un problema.

Otra característica de los sistemas de cadena de bloques será la capacidad de compartir los datos con terceros de forma transparente. En el futuro, compartir datos será tan fácil como enviar un ziple por correo electrónico, excepto que el receptor tendrá acceso a la copia original, no a una copia si se envía por correo electrónico. Cuando alguien envía cerveza, tiene una versión en su computadora y el receptor tiene una versión. Con la tecnología blockchain, las dos personas solo compartirán una versión.

Blockchains actúa como un tercero que es testigo de la edad y la creación de ofles. Pueden identificar a nivel granular a cada persona que interactuó con ale en todos los sistemas, interna y externamente. Pueden mostrar lo que falta en la cerveza, no solo los datos que contiene ahora. Blockchainles también se puede compartir de forma redactada que no comprometa la validez de los documentos.

Lo que esto significa es que podrá ver la edad de la cerveza, la historia completa de la cerveza y cómo se veía con el tiempo a medida que evolucionaba. Más interesante aún, también podrá ver si falta algo en la cerveza. Este concepto se llama prueba de lo negativo. Los sistemas Mostle en este punto solo pueden decirle lo que tienen dentro de ellos. Pero podrás saber qué cerveza no tiene.

La auditoría será menos costosa y más completa. La actualización de las reglas de auditoría podría hacerse de una manera más centralizada. Cuando los nodos reguladores dentro de una red blockchain tienen una visión compartida y transparente de las transacciones de activos, el informe de estas transacciones se puede realizar a través de la ubicación del regulador, sin obligar a 100 o más instituciones a adherirse al mismo conjunto de reglas.

Los sistemas basados en blockchain que están completamente integrados en una organización podrán saber dónde se gastó cada centavo. La última milla de cómo se gasta el dinero es la más difícil de contabilizar entre organizaciones y gobiernos. Debido a que es tan difícil de contabilizar, aquellos que deseen robar fondos tienen la apertura que necesitan.

La última milla podría convertirse en la mayor oportunidad de una empresa para ahorrar recursos desperdiciados e identificar a las personas corruptas. Las organizaciones sin fines de lucro que tienen pautas estrictas sobre la contabilidad de cómo gastan su dinero podrían beneficiarse más de este tipo de sistema. Podrían satisfacer sus necesidades de auditoría y rendición de cuentas a sus donantes sin obstaculizarlos en sus misiones más importantes para el bien.

Un sistema que se ha explorado se integraría directamente en el flujo de trabajo de los trabajadores humanitarios. Este sistema se diseñó originalmente para realizar un seguimiento de los registros médicos, pero también podría realizar un seguimiento de todos los suministros que se utilizan con cada paciente médico. Los beneficios de este sistema serían monumentales, dado que tanto fraude y robo ocurren dentro del mundo de las ONG.

EN ESTE CAPÍTULO

Capítulo 13

Bienes raíces

El sector inmobiliario será una de las industrias más impactadas por las innovaciones en tecnología de cadena de bloques. El impacto se sentirá en todos los países de forma ligeramente manera diferente. En el mundo occidental, podríamos ver el advenimiento de cosas como valores respaldados por hipotecas transparentes negociados en intercambios habilitados para blockchain. En China, la integración de blockchain ya está ocurriendo con cosas como la certificación notarial, un componente esencial de las transacciones inmobiliarias. En el mundo en desarrollo, Las cadenas de bloques son las más prometedoras porque pueden liberar capital y aumentar el comercio.

Este capítulo se sumerge en las innovaciones que ya están ocurriendo en todo el mundo en la industria de bienes raíces. También les informaré sobre los posibles cambios que se avecinan. en el futuro y las implicaciones significativas de la tecnología blockchain.

Los bienes raíces contienen gran parte de la riqueza y la estabilidad económica del mundo. La industria cambiará muy rápidamente durante los próximos años, y saber dónde se encuentran estos Se producirán cambios y la forma en que usted y su empresa pueden aprovecharlos será un beneficio.

Eliminación del seguro de título

El seguro de título es una compensación por pérdida financiera por defectos en su título por un compra de bienes raices. Es obligatorio si saca una hipoteca sobre su casa o si lo renuncias. El seguro de título protege la inversión del banco contra problemas de título que podrían no encontrarse en los registros públicos, se pasan por alto en la búsqueda de títulos, u ocurrir por fraude o falsificación.

El seguro de título es necesario en lugares que utilizan el derecho consuetudinario para regir sus sistemas de títulos. El comprador es responsable de asegurarse de que el título del vendedor sea bueno. Dentro de estos sistemas, se realiza una búsqueda de títulos y se compra un seguro. En áreas que use un sistema de títulos de Torrens, un comprador puede confiar en la información del registro de la propiedad y no necesita mirar más allá de esos registros.

La tecnología Blockchain se ha propuesto como un complemento para ayudar a los consumidores en los sistemas de títulos de derecho consuetudinario. La idea es simple: las cadenas de bloques son fantásticos sistemas de mantenimiento de registros públicos; tampoco pueden ser retroactivos o modificados sin un registro. En teoría, las cadenas de bloques podrían transformar los sistemas de derecho consuetudinario en sistemas distribuidos. Sistemas de títulos Torrens.

En 2022, Future House Studios, una empresa de creación de contenido de metaverso, se convirtió en therst acuñar la propiedad de su oficina corporativa como NFT. De la empresa El título de propiedad inmobiliaria se mantendrá y se realizarán transacciones de forma permanente en una cadena de bloques. Tru Mint, una empresa de bienes raíces de blockchain, guió a Future House Studios a través del proceso y espera que la tecnología blockchain y NFT se convierta en una parte natural de bienes raíces. TruMint fue creado por un grupo de abogados capacitados en Harvard y ingenieros de software de cadena de bloques. Hicieron posible vender bienes raíces legalmente, como tan fácil como transferir un NFT. Su equipo creó medidas de seguridad adicionales para satisfacer todos los requisitos de compra de bienes raíces en los 50 estados de EE. UU. TruMint funciona como un caja de seguridad legal que coloca los títulos del mundo real en almacenamiento en frío, lo que permite que una "escritura digital" de NFT realice transacciones indefinidamente en la cadena. En cualquier momento, el titular de NFT puede recupere el título del mundo real devolviendo la "llave" NFT a la caja de seguridad. Este reducirá sustancialmente el costo y la molestia de vender y comprar bienes raíces. Es tan sencillo como firmar electrónicamente documentos de transferencia y luego mover el NFT de una billetera a otra billetera.

industrias protegidas

Cada industria tiene sistemas de autoprotección para mantener fuera a la nueva competencia. Que podría ser una alta carga regulatoria, monopolios otorgados por el gobierno o alta puesta en marcha costos La industria que se ha desarrollado en torno a la compra y venta de bienes raíces no ha cambiado mucho en los últimos 40 años y está lista para la disrupción. Muchas partes diferentes contribuyen al proceso.

Aquí están las diferentes industrias que se construyen alrededor de la compra y venta de casas:

» Agentes inmobiliarios: Un agente inmobiliario te ayuda a comparar diferentes vecindad
barrios y encontrar un hogar. A menudo lo ayuda a negociar un precio y se comunica con el vendedor en su nombre. Este servicio es valioso y no es probable que sea desplazado por la tecnología blockchain. Ya puede comprar una casa sin un agente de bienes raíces: las personas eligen trabajar con ellos porque mejoran el proceso.

» Inspectores de viviendas: Los inspectores de viviendas descubren defectos en la casa antes de que usted la compre, defectos que podrían costarle dinero en el futuro. Los inspectores de viviendas por defectos se pueden utilizar para negociar con el vendedor un mejor precio. En el futuro, las casas seguirán teniendo desgaste, eso nunca cambiará. Pero la tecnología blockchain podría usarse para registrar las reparaciones de la propiedad y los defectos encontrados en la inspección.

» Representantes de cierre: en el cierre, el paso final es la liquidación. El representante de cierre supervisa y coordina los documentos de cierre, los registra y entrega el dinero a las partes correspondientes. Los representantes de cierre pueden ser desplazados por la tecnología blockchain: las funciones realizadas por los representantes de cierre podrían integrarse en contratos inteligentes o código de cadena.

» Prestamistas y administradores de hipotecas: Los prestamistas y administradores de hipotecas
fondos para una hipoteca y cobrar los pagos hipotecarios en curso. No serán desplazados con el software de cadena de bloques, pero pueden usar la tecnología de cadena de bloques para ayudarlos a reducir los costos con el mantenimiento de registros y la auditoría.

» Tasadores de bienes raíces: El trabajo del tasador de bienes raíces es mirar una propiedad y determinar cuánto vale. El proceso de tasación se realiza cada vez que se compra o se re nancia una propiedad. Compañías como Zillow se han tomado mucho trabajo para saber el valor de mercado, pero cada casa es única y necesita ser evaluada periódicamente. Incluso en el proceso de hipoteca de bienes raíces, se pueden requerir múltiples apelaciones para satisfacer las necesidades de todos. Puede ser útil registrar estos datos dentro de una cadena de bloques como testigo público.

» Oficiales de préstamo: los oficiales de préstamo usan su información crediticia, financiera y de empleo.
información para ver si califica para una hipoteca. Luego hacen coincidir lo que usted es elegible con los productos que venden. Al igual que un agente de bienes raíces, un oficial de préstamos lo ayuda a obtener la mejor opción en un espectro de opciones. El software de cadena de bloques se puede usar para ayudar a los oficiales de préstamos a realizar un seguimiento de los documentos que le entregan y auditar el proceso para el cumplimiento justo de la ley de préstamos.

» Procesadores de préstamos: un procesador de préstamos ayuda a los oficiales de préstamos a preparar la mort
la información del préstamo del instrumento y la solicitud de presentación al suscriptor.
Se está explorando el software que extrae la información de origen del comprador. No es tecnología de cadena de bloques, pero podría ser perjudicial para este puesto.

» Suscriptores hipotecarios: un suscriptor hipotecario determina si usted está elegible para un préstamo hipotecario. Ella aprueba o rechaza su préstamo hipotecario solicitud basada en su historial crediticio, empleo, bienes y deudas. Las organizaciones están explorando la automatización del proceso de suscripción utilizando inteligencia artificial. Sin embargo, no es tecnología blockchain.

Cada uno de estos agentes tiene un propósito central que ayuda a proteger al comprador, al vendedor y al proveedor de hipoteca En la mayoría de las industrias, el costo de hacer negocios se reduce tiempo: mejoras en la eficiencia provocadas por la competencia y la innovación contribuir a reducir los costos. La industria hipotecaria es atractiva como candidata para la innovación de blockchain, porque ha ocurrido lo contrario: el costo del negocio ha subido. La hipoteca típica de los EE. UU. tiene más de 500 páginas y cuesta $ 7,500 para originarse. Esto es tres veces lo que costaba hace diez años. La tecnología Blockchain puede satisfacer las necesidades de proteger al comprador, al vendedor y al proveedor de hipotecas mientras reduciendo el costo de hacerlo.

Los consumidores y Fannie Mae

La Asociación Hipotecaria Nacional Federal (conocida como Fannie Mae) es a la vez una empresa patrocinada por el gobierno y una empresa que cotiza en bolsa. es actualmente la principal fuente de financiamiento para los prestamistas hipotecarios y ha dominado el mercado después de la recesión a medida que se fue el dinero privado.

Desde la recesión, el 95 por ciento de todos los préstamos hipotecarios hechos en los Estados Unidos han ven a través de Fannie Mae. Esto es alrededor de $ 5 billones en activos hipotecarios. con pocos excepciones, los préstamos que no se hacen a través de Fannie Mae o su primo cercano, Fred die Mac, son préstamos jumbo (típicamente más de $417,000 cada uno). Estos préstamos todavía financiada con dinero privado.

Fannie Mae tiene un programa automatizado utilizado por los originadores de préstamos para calificar a un prestatario. Les ayuda a navegar las pautas para un préstamo convencional. Los prestamistas administran su solicitud de préstamo a través del sistema informático de Fannie Mae, y escupe un respuesta de aprobar o rechazar su préstamo. Las plataformas en línea están utilizando este nuevo software para llegar a los consumidores, lo que les permite pasar por alto las ubicaciones minoristas tradicionales. Fannie Mae y Freddie Mac están explorando la tecnología blockchain para incluso optimizar aún más este proceso y llegar a los clientes directamente.

Hipotecas en el Mundo Blockchain

Una hipoteca en un mundo blockchain no parecerá muy diferente a una hipoteca en el mundo tradicional. La parte que notará es que una hipoteca blockchain será menos costosa al cierre.

Dado que la mayoría de las personas solo compra unas pocas casas en su vida, la diferencia puede no parecer un gran problema. Pero el dinero suma. La tecnología Blockchain podría reducir el costo de originar una hipoteca a los niveles anteriores a 2007.

Reduciendo sus costos de originación

Los costos de originación de hipotecas han aumentado, y la razón es simple: los bancos temen nes en los que pueden incurrir si estropean cualquier parte del proceso de la hipoteca. Entonces el la industria ha tomado medidas para ayudar a garantizar que cumplan con todos los requisitos en el momento del origen y años más tarde cuando se auditan. Los grandes bancos han pagado miles de millones de dólares por el mal manejo de documentos. Ahora son requeridos no sólo para tener todos los documentos esenciales, sino también para demostrar que siguieron las proceso correcto y le envió todos los documentos necesarios.

Los productos basados en blockchain reducen la redundancia que los bancos comenzaron a incorporar en su proceso después de la recesión. Los gastos de mantenimiento de registros y auditoría se han disparado desde la introducción de la reforma Dodd-Frank Wall Street. y la Ley de Protección al Consumidor, y la tecnología blockchain podría reducir ese costo.

Las empresas que deseen satisfacer las necesidades de los bancos con una solución de cadena de bloques deben dejar que los bancos demuestren que siguieron las pautas establecidas en Dodd-Frank. También ayudaría a los bancos a documentar por qué tomaron ciertas decisiones sobre los préstamos, y ayudarlos a ubicar los documentos que se usaron en la originación, incluso si no están en posesión de ellos.

Las aplicaciones de cadena de bloques podrían devolver cerca de $ 4,000 a la mesa para el promedio compra de vivienda. La industria hipotecaria es muy parecida a la industria de préstamos para automóviles y la industria de tarjetas de crédito. Aplicaciones similares podrían reducir el costo de administración que estas industrias tienen debido a las leyes de protección al consumidor, mientras que al mismo tiempo tiempo dejando que las empresas cumplan con esos requisitos.

Conocer su último documento conocido

Uno de los factores de costo más importantes en el proceso de originación de una hipoteca a menudo se presenta años después de que se hizo el préstamo por primera vez. A veces, quienes facilitan el proceso de préstamo agregue documentos innecesarios a clientes, o archivos antiguos que no se utilizan para originar un préstamo se dejan en la carpeta. Además, pueden ocurrir registros duplicados. cuando llega el momento para auditarlos, hay demasiada información para filtrar. Los bancos pagan dinero a agentes externos para verificar sus registros y tratar de determinar qué documentos fueron utilizado en la disección final en su préstamo.

El software Blockchain puede resolver este problema de una manera elegante. Las cadenas de bloques son sistemas de mantenimiento de registros distribuidos que permiten que varias partes colaboren en los datos a lo largo del tiempo sin perder de vista cómo se veían esos datos en un punto dado del camino. Esto significa que la media docena de organizaciones individuales que
colaborar para ayudarte a comprar tu casa ahora pueden interactuar todos en la misma cadena.

Una cadena en este caso de uso comenzaría contigo. Luego, a su cadena se le agregarán subcadenas con el tiempo, como la compra de una casa. Entonces podrías
autorizar a otros, como bancos, empleadores, agencias de crédito, empresas de tasación y similares, a escribir en contra de la cadena. Cada uno añadiría sus datos a
su cadena, y las otras partes autorizadas podrían leer estos datos y agregar los suyos propios.

Blockchains cambiaría la necesidad de repositorios centrales para archivos. Sería
automatizar parte del procesamiento del papeleo, y siempre daría una clara
historial de su préstamo, reduciendo la necesidad de auditar y preparar documentos para ser
Verificado

Esta es una gran idea, pero no requiere que todo el ecosistema colabore. Cada
sucursal que lo haga fortalecería el sistema y agregaría valor, de manera muy similar a la forma en que cada persona adicional que poseía una máquina de fax hizo que el poder de tener una fuera mucho más útil.

Pronóstico de tendencias regionales

Blockchain ha estado librando una batalla cuesta arriba para convertirse en un software convencional solución. A menudo se encuentra con miedo porque muchas personas no entienden cómo
funciona o cuáles son las implicaciones reales para su implementación generalizada.
Además, muchos de los primeros defensores, como los primeros en adoptar cualquier nueva tecnología, estaban visto como un poco "allá afuera". Blockchain queda atrapado en las malas relaciones públicas de Bitcoin y cosas ilícitas e ilegales que se hacen con la tecnología.

Sin embargo, 2016 fue un punto de inflexión para la industria. Quedó claro que la cadena de bloques sería disruptiva y que aquellos que querían estar en el lado positivo de esa ecuación tenían que idear una estrategia de cadena de bloques.

Todos los bancos importantes comenzaron programas para investigar y experimentar con blockchain. o se unió a un consorcio. Muchos pasaron primero a la liquidación interbancaria y las transferencias transfronterizas, que son aplicaciones relativamente sencillas para las cadenas de bloques. Las próximas y más transformadoras evoluciones serán los sistemas y datos que están protegidos a través de la descentralización.

En las siguientes secciones, cubro las tendencias en la tecnología blockchain en los Estados Unidos. Unidos, Europa, China y África.

Estados Unidos y Europa: Congestión de infraestructura

Los Estados Unidos y los países europeos pueden tardar más en implementar la tecnología de cadena de bloques que otros países. Aunque las empresas de estos países gastan miles de millones de dólares en mantenimiento de infraestructura, es solo eso: mantenimiento. Ya existen soluciones a los problemas que las cadenas de bloques quieren resolver. No se trata solo de decir que las cadenas de bloques ofrecerían una mejor
solución: esa solución debe ser diez veces mejor que un sistema existente o ser
capaz de implementar a través de la integración.

Uno de los principales desafíos que enfrenta Estados Unidos es que está descentralizado en la distribución del poder y la toma de decisiones. Cada condado y cada estado propondrán sus propias reglas sobre cómo implementar o usar la tecnología blockchain.
Este proceso ya ha comenzado.

Blockchains puede desencadenar leyes y regulaciones de transmisores de dinero. en los unidos Unidos, es más claro a nivel federal qué tipos de negocios se consideran dinero transmisores Dado que todas las cadenas de bloques públicas esenciales actualmente usan un token criptográfico para impulsar la seguridad, el problema se nubla, lo que ha dado lugar a blockchains privadas y de permisos que operan sin tokens.

Los requisitos de licencia estatal son ambiguos para las empresas que usan blockchain tecnología para aplicaciones distintas de los pagos. Se promulgarán reglamentos y leyes para proteger a los consumidores. Europa ya tiene leyes sobre "ser olvidado".
El cumplimiento de estas reglas puede ser complicado cuando los datos ingresados en blockchains son alrededor para siempre y no puede ser eliminado por nadie, incluso si quisiera.

Participar en la transmisión de dinero en muchos estados de EE. UU. es un delito grave si no lo está debidamente autorizado. Las duras consecuencias de sobrepasar la ley a través de la innovación obligan a las empresas de blockchain a gastar mucho más dinero y tiempo en Cumplimiento: por una suma de $ 2 millones a $ 7 millones por año por empresa porque deben cumplir con los requisitos reglamentarios en los 50 estados. El Los honorarios legales son cargas pesadas para estas nuevas empresas de tecnología.

La legislación de cada estado aplicada a la industria de la cadena de bloques aún no está clara. Nueva York y Vermont han comenzado a integrar esta tecnología en la ley. Nueva York ha aumentado el costo de cumplir e impulsado la innovación para trasladarse a ubicaciones más amigables. Vermont, por otro lado, aprobó una ley que hace que los registros de cadenas de bloques sean admisibles en los tribunales.

Luxemburgo creó un marco legal para los establecimientos de pago electrónico en 2011 y fue temprano en la idea del "dinero electrónico". Luxemburgo y el Reino Unido se han convertido en el hogar de muchas empresas de cadenas de bloques porque la regulación

el medio ambiente es más fácil para ellos navegar y pagar. Por menos de $ 1 millón,
Las empresas de blockchain pueden obtener una licencia de instrumento de pago en la Unión Europea. Esta
licencia otorga a las empresas acceso a 28 países de la UE. Este enfoque tiene
permitió a la UE avanzar más allá de los Estados Unidos en innovación tecnológica.

China: estado incierto

Bitcoin y otras criptomonedas han tenido una posición bipolar en China durante años.
El país tomó su primera postura hostil contra la criptoindustria desde 2013 cuando
lanzó su primer conjunto de restricciones criptográficas. En 2017, el gobierno emitió una prohibición
en ofertas iniciales de monedas (ICO). Como resultado, muchos criptoempresarios han tenido
China por temor a ser arrestado. Las medidas enérgicas son parte de un patrón más amplio de endurecimiento
y luego perder la regulación en China. Este reflujo ha hecho que sea difícil para
empresas de blockchain para operar en el país, y muchas se han visto obligadas a
cerrar o cambiar de lugar. Dada esta historia, no sorprende que muchos de los
Las primeras empresas de blockchain en China han desaparecido.

Bitcoin y otras criptomonedas se han visto durante mucho tiempo como una amenaza para China.
economía y estabilidad financiera. En 2021, el gobierno chino tomó medidas para
tomar medidas enérgicas contra el comercio y la minería de criptomonedas en lo que se considera una de las
medidas más intensas del mundo. La medida tuvo un impacto significativo en el mundo
mercado de criptomonedas, ya que China ha sido un jugador importante en la minería de Bitcoin y
comercio. Sin embargo, el gobierno chino no se opone del todo a blockchain.
tecnología y, en cambio, busca otros usos para ella, como la gestión de la cadena de suministro y los tokens
no fungibles (NFT). La diferencia clave es que estas aplicaciones deben estar bajo el control del gobierno, lo
que va en contra de la cadena de bloques.
carácter descentralizado y sin restricciones.

Queda por ver cómo esta represión afectará el papel de China en el mercado mundial.
mercado de criptomonedas, pero está claro que el gobierno tiene la intención de mantener un control estricto
sobre el uso de la tecnología blockchain dentro de sus fronteras.

El mundo en desarrollo: Obstáculos a la cadena de bloques

El futuro está aquí, simplemente no se distribuye. Esto es especialmente cierto en el desarrollo
países, que a menudo tienen una mayor necesidad de tecnología, pero no tienen la misma
recursos o el entorno político adecuado para permitir que esas innovaciones arraiguen. Algunos países
pequeños intentan medidas proteccionistas que bloquean la importación
de bienes que pudieran fabricarse dentro de sus fronteras; otros países también desconfían de la calidad y
benevolencia de los productos y servicios que provienen de fuentes externas. En una nota más sombría,
algunos sistemas políticos se benefician demasiado de
las ineficiencias y ambigüedades que su sistema legal tiene para cambiar.

Hernando de Soto Polar es un economista y autor peruano que ha hablado ampliamente sobre la economía informal y la importancia de las empresas y los derechos de propiedad. Uno de los temas prominentes que mantiene subdesarrollado al mundo en desarrollo es el capital muerto. La propiedad que se posee informalmente y no se reconoce legalmente con no se puede confiar en los sistemas actuales. Para los dueños de estos terrenos, es difícil o imposible su enajenación y venta. La incertidumbre también disminuye el valor de los activos El mundo occidental ha sido capaz de pedir prestado contra activos y vender ellos con relativa libertad. Esto ha impulsado la innovación y la prosperidad económica.

La tecnología que habilitan las cadenas de bloques podría cambiar esa realidad para los países en desarrollo muy rápidamente. Registros claros de propiedad de la tierra significaría que sería vendible y nanceable. Esto haría que la propiedad frente al mar de Colombia irresistible. Los pagos irreversibles y la verdadera identidad conocida abrirían crédito y comercio de nuevas formas.

Muchas startups y hackers se han unido para tratar de hacer realidad esta visión de futuro. Incluso los actores globales más grandes como el Banco Mundial han tenido reuniones repetidas sobre blockchain y su impacto en el mundo en desarrollo. Bitcoin y blockchain están incursionando en África, donde las monedas locales y la infraestructura están profundamente desconfiado. AZA Finance, una plataforma de pago y comercio que presta servicios a muchos países de África, ha comenzado a expandirse al Reino Unido y Europa. también ha comenzado ampliando su oferta de servicios a cosas como la nómina.

Por muchos obstáculos que tengan los países en desarrollo hacia el desarrollo y la innovación, también tienen ventajas que los países occidentales nunca superarán. El la falta de infraestructura existente en los países en desarrollo les facilita superar a las naciones occidentales. Esto fue evidente en la proliferación de teléfonos celulares en países en desarrollo. Los países en desarrollo tampoco tienen los mismos organismos reguladores y protecciones al consumidor. Esto es particularmente atractivo para las nuevas empresas de blockchain que se encuentran en la zona gris en los países occidentales. Países en desarrollo a menudo tienen menos tomadores de decisiones, por lo que es más fácil conocer a personas que tienen la poder para cambiar.

EN ESTE CAPÍTULO

» Creación de nuevos negocios

» Seguros individuales a medida

» Creación de nuevos mercados de seguros

» Reducir costos de formas inesperadas

Capítulo 14

Seguro

La tecnología de seguros de cadena de bloques está situada para cambiar la forma en que las personas y las empresas compran y obtienen cobertura de seguro, y empresas que tal vez conozca, como Toyota, lo están probando. Necesitas entender la implicación ciones de estas nuevas tecnologías que recién ahora están en el horizonte.

En este capítulo, explico cómo funcionan estas nuevas tecnologías y sus principales limitaciones. Le muestro cómo los dispositivos de Internet de las cosas (IoT) colaborarán con los proveedores de seguros. También describo cómo los contratos de blockchain autoejecutables darán forma a las políticas y estructuras de la empresa.

Este capítulo lo prepara para los cambios fundamentales en la tecnología que pueden cambiar la carga de la prueba. Después de leer este capítulo, podrá tomar decisiones más informadas sobre la cobertura y los pagos de seguros basados en blockchain.
Comprenderá cómo le afectará el costo de la cobertura y los diferentes tipos de cobertura que estará disponible para usted en el futuro.

Cobertura de sastrería precisa

Los dispositivos IoT, los datos inmutables, las organizaciones autónomas descentralizadas (DAO) y los contratos inteligentes están cambiando el desarrollo de los seguros para los consumidores. La convergencia de todas estas tecnologías es posible gracias al desarrollo de blockchains.

Las cadenas de bloques hacen algunas cosas realmente bien que permitirán dos cambios importantes en la forma en que se comprarán y venderán seguros en el futuro: las personas podrán obtener una cobertura más personalizada y se abrirán nuevos mercados que antes no eran posibles debido a costos

asegurando al individuo

Los seguros construidos alrededor del individuo permitirán un cambio significativo de prioridades. La gestión de activos será menos crítica y las aseguradoras podrán concentrarse en el cálculo del riesgo y en hacer coincidir la oferta y la demanda.

Podría crear una plataforma de mercado que asegure a los clientes. Hay muchas formas de organizar este nuevo negocio. Una posibilidad sería un mercado bajo demanda donde los usuarios publiquen sus solicitudes, ya sea estandarizadas por contrato inteligente personalizado o por contrato de código de cadena. Si no ha leído acerca de este tipo de nuevos contratos digitales autoejecutables, consulte el Capítulo 5 sobre Ethereum y
Capítulo 9 sobre Hyperledger.

Con este tipo de modelo, usted, como asegurador, podría calcular la prima para la demanda específica, con base en datos históricos y otros factores de cálculo de riesgo en su
modelo de riesgo. Si el cliente está satisfecho con la oferta, puede ofertar o suscribirse, según el modelo de demanda que se utilice.

Este nuevo tipo de seguro podría ser adoptado por un seguro peer-to-peer (P2P) o de financiación colectiva o una compañía de seguros tradicional que adopte la tecnología.
De cualquier manera, ambos se crean en un libro mayor de criptomonedas descentralizado con el uso de contratos inteligentes/chaincode, que garantizan el pago del cliente al inversor y viceversa en caso de incidencia. Blockchain es clave aquí, porque permite algunas cosas que no eran factibles o seguras hace unos años.

Las cadenas de bloques crean una transferencia de valor casi sin fricciones, lo que significa que los micropagos son factibles porque las tarifas de transacción son muy bajas. Ahora puede abrir nuevos mercados que no tenían un sistema monetario o un sistema legal en funcionamiento o instancias donde el costo de las transacciones y disputas superó el beneficio de ofrecer
cobertura.

Puede usar DAO, con contratos inteligentes, para gobernar grandes grupos a una fracción del costo y el tiempo. Podría usar este modelo para incorporar y administrar su nueva empresa, y posiblemente plataformas de seguros de fondos colectivos.

La naturaleza autoejecutable de los contratos inteligentes también podría arrojar luz sobre muchos de los costos del ajuste de reclamaciones y de terceros que ayudan con el procesamiento y la recaudación de fondos.

La legalidad de todo esto sigue en duda. Determinar las preocupaciones sobre la privacidad y los derechos del consumidor es difícil. Cada país tiene sus propias regulaciones y divulgaciones para la industria de seguros Dicho esto, los derechos del consumidor y los requisitos de divulgación pueden ejecutarse mejor utilizando la tecnología blockchain. El seguro descentralizado (también conocido como “Seguro 2.0”) es un tipo de seguro basado en la tecnología blockchain y opera descentralizado, sin necesidad de una autoridad central o intermediario. Su objetivo es mejorar los modelos de seguros tradicionales proporcionando productos y servicios de seguros más transparentes, flexibles y seguros.

Uno de los principales beneficios de los seguros descentralizados es el uso de contratos inteligentes, que son contratos autoejecutables con los términos del acuerdo entre el comprador y el vendedor que se escriben directamente en líneas de código. Los contratos inteligentes se pueden utilizar para automatizar la compra y venta de seguros y facilitar el pago de siniestros. Esto puede hacer que la compra y el uso de seguros sean más eficientes y transparentes.
porque todas las partes involucradas pueden ver los términos del contrato y las condiciones bajo las cuales se pagarán las reclamaciones.

El seguro descentralizado también puede ser más flexible que el seguro tradicional,
porque permite a los usuarios personalizar su cobertura y elegir entre una variedad de productos de seguros. También puede ofrecer una cobertura más diversa, porque no está limitada por fronteras geográficas o marcos regulatorios.

En general, los seguros descentralizados tienen el potencial de proporcionar productos y servicios de seguros más accesibles, transparentes y seguros, y es un área emergente de interés en la industria de la cadena de bloques.

Estos son algunos de los innovadores prometedores dentro del espacio:

» InsurAce (www.insurace.io): InsurAce es una multicadena descentralizada
Protocolo de seguros que proporciona servicios de seguros a usuarios de seguros descentralizados. Le permite asegurar activos de inversión como contratos inteligentes, riesgo de custodia y ofertas de tokens. InsurAce afirma reducir su prima en crear productos centrados en la cartera que adopten la diversificación del riesgo.

» Harpie (https://harpie.io) es un seguro descentralizado interesante
empresa que ofrece planes de criptoprotección para criptomonedas, tokens, tokens no fungibles (NFT) y otros activos digitales. Harpie se conecta directamente a su billetera Ethereum, lo que le da a Harpie una visión clara de sus tenencias de activos y permitir que Harpie controle cualquier cosa que pueda ocurrirle a sus activos. Harpie brinda cobertura por robo, piratería, desastres naturales y más. Es convenientemente compatible con la mayoría de las billeteras criptográficas, lo que le permite asegurar más de una billetera a la vez. Harpie también está lanzando un firewall en cadena las reclamaciones evitarán hackeos, estafas y otros tipos de robo.

» Tidal (https://tidal.finance) es interesante dentro de los contratos inteligentes espacio porque las nuevas tecnologías que se están construyendo en el seguro descentralizado son vulnerable a manipulaciones y piratería. Tidal busca generar confianza en los protocolos de cadena de bloques mediante la creación de un mercado de seguros descentralizado para seguros descentralizados que permita a los nuevos pioneros financieros aprovechar algunos de los riesgos inherentes de construir software en Internet. Conecta a compradores y vendedores a la cobertura de fuentes múltiples para hacks de contratos inteligentes. Marea también permite le permite crear grupos de seguros especí cos para uno o más protocolos. El propósito principal de la plataforma es maximizar la eficiencia del capital mientras se ofrece primas de seguro competitivas.

El nuevo mundo de los microseguros

El microseguro es un seguro para proteger a las personas de bajos ingresos contra riesgos, como accidentes, enfermedades y desastres naturales. Se ha vuelto más factible a través de la tecnología de cadena de bloques.

Cuando piense en microseguros, preste atención a dos categorías (que pueden ir de la mano):

» Seguros dirigidos a hogares de bajos ingresos, agricultores y otras entidades donde el seguro está diseñado en torno a necesidades especí cas, por lo general, un seguro de prima baja y basado en índices

» Seguros que se ocupan de productos o servicios de bajo valor

El mayor problema con este tipo de contratos dentro de los modelos de seguros tradicionales es que sus costos de manejo son desproporcionadamente altos y hacen que sea poco atractivo atender estos mercados.

El atributo de baja fricción de las cadenas de bloques les permite mover valor a un costo extremadamente bajo, casi instantáneamente en cualquier parte del mundo, sin devoluciones de cargo, lo que abre la oportunidad de servir a más personas y a costos más bajos.

La ventaja clave de la cadena de bloques es que la creación de contratos inteligentes permite transacciones seguras sin ningún intermediario, por lo que el seguro tiene un costo significativamente menor. costos

El principio de microseguro de blockchain es simple y consta de cuatro pasos:

1. Propuesta de contrato de préstamo/seguro

   Una persona puede ofrecerse a prestar su propiedad a través de su proveedor de seguros, si el la propiedad está registrada digitalmente. La oferta se puede enviar al usuario potencial,

ya sea a través de los canales de la compañía de seguros o a través de una plataforma pública como como Facebook.

2. Revisión del acuerdo

El prestatario puede entonces revisar la propuesta que recibió y aceptar o rechazarlo La oferta se mantiene en los registros públicos, y si el prestatario acepta la propuesta, puede comprar el seguro a través de pago estándar canales, y el proceso avanza al tercer paso.

3. Firma del contrato y notarización

Si ambas partes están en la misma página, el seguro está pagado y el el prestatario recibe la propiedad en cuestión, y el acuerdo es digitalizado firmado y notariado en una cadena de bloques. Esto lo hace virtualmente a prueba de manipulaciones. Toda la información de la transacción se almacena de forma segura con un seguimiento de auditoría claro si alguna vez necesario.

4. Fichas de con rmación

Ambas partes reciben tokens digitales especiales que sirven como prueba de identidad para el acuerdo en cuestión. Estos tokens se utilizan para con rmar criptológicamente que ambas partes han firmado el acuerdo.

Además de esta facilidad de uso, los contratos inteligentes permiten seguros basados en índices, lo cual es muy útil para seguros agrícolas y otros campos donde los valores dependen en gran medida en factores dinámicos que pueden ser documentados con precisión por terceros confiables. En este caso particular, los agricultores asegurados pueden recibir pagos automáticos cuando las bases de datos meteorológicas verificadas informan condiciones particulares, como la sequía, lo que reduce aún más el costo potencial del servicio.

Este sector de seguros descentralizados, los microseguros, ha tenido un crecimiento lento. Los sistemas basados en la tecnología blockchain tienen más gastos y riesgos adicionales que el software tradicional. La escasez de desarrolladores competentes y las preocupaciones por la privacidad han retrasado la comercialización de algunas ideas bastante buenas. sin embargo, el La promesa de aplicaciones financieras descentralizadas y de código abierto, como contratos de seguros autoejecutables, ha hecho que sigan llegando dólares de inversión. Estas aplicaciones, a menudo llamadas contratos inteligentes, se pueden usar para una variedad de propósitos, como préstamos, préstamos, comercio y más.

Una startup llamada Yas Microinsurance (https://yas.io) ha comenzado a hacer olas. Es un proveedor de seguros en blockchain con sede en Hong Kong que recaudó $ 4.5 millones en 2022 para proporcionar un seguro para cosas como eventos especiales o simplemente para salir a caminar. Yas Microinsurance afirma que su producto es un seguro autónomo y un microseguro en blockchain. Todavía está en los primeros días de comercialización.

Testificando para usted: Internet de las cosas

Las cadenas de bloques permiten la creación de un nuevo tipo de identidad tanto para las personas como para las cosas. Se basan en un modelo tradicional en el que una autoridad certificadora emite una certificado Para las personas, ese certificado sería un documento como un certificado de nacimiento o una licencia de conducir. Pero las “cosas” tienen certificados similares que ayudan a los consumidores a validar la calidad y la autenticidad.

Estos tipos de certificados han sido eliminados durante años. Se ha invertido en su creación una seguridad cada vez más sofisticada, pero esto aumenta el costo. Las cadenas de bloques permiten registrar estos certificados tradicionales de forma inalterable.
historia que cualquiera puede consultar y consultar. Una característica adicional es la capacidad de actualizar esos registros a medida que ocurren nuevos eventos.

Los dispositivos IoT ahora pueden publicar todo tipo de datos de forma autónoma en sus registros y actualizar el estado actual en el que se encuentran. Ahora que los dispositivos IoT pueden hablar por sí mismos y publicar sus historias e identidades y compartirlas con terceros, el seguro será solo uno de las muchas industrias afectadas.

Proyectos IoT en seguros

IoT probablemente tendrá un impacto significativo en tres áreas de su vida: la conexión
automóvil, el hogar conectado y el yo conectado.

El IoT es, en esencia, una tecnología disruptiva y, como tal, cambiará la forma de una amplia gama de industrias, como los fabricantes de equipos originales (OEM) automotrices, la seguridad del hogar y los proveedores de cable y telefonía móvil. En esa mezcla están
compañías de seguros, en particular, las que trabajan con pólizas de propiedad y accidentes (P&C).

Los datos recopilados por los sensores en los nuevos aparatos y dispositivos, junto con la automatización y las opciones de control adicionales, generarán nuevas posibilidades cuando se trata de nuevas empresas emergentes en la industria de seguros. Combinado con los libros de contabilidad descentralizados de blockchain y los contratos inteligentes, todo el proceso podría automatizarse a un nivel que antes hubiera sido imposible.

El nuevo estilo de vida, siempre en línea, que viene con un cambio tan radical en la tecnología elimina algunos de los riesgos existentes, pero introduce otros nuevos, el más importante de los cuales es la seguridad de la información. Todo ello hace que haya que recalcular los factores de riesgo. Por ejemplo, los coches autónomos tendrán un riesgo reducido
de accidente debido a la ausencia de error humano, pero la confiabilidad de la tecnología estará en duda hasta que tengamos suficientes datos de la aplicación del mundo real.

Implicaciones de los grandes datos accionables

Big data ha existido desde el año 2000, y hoy en día es una industria de $ 200 mil millones.
y de particular importancia para el sector financiero. Sin embargo, los grandes datos vienen con una serie de problemas que solo crecen con su presencia en el mundo cotidiano:

» Control: Si tiene una gran empresa multinacional o un consorcio, el
el tema del intercambio de datos se vuelve bastante significativo. El control de versiones es imperfecto,
y a veces puede ser muy difícil saber cuál es el último, el más
copia actualizada.

» Confiabilidad de los datos: ¿Cómo demuestras si eres el creador de dichos datos, o
alguien mas lo es? ¿Qué sucede con los datos dañados?

» Monetización y transferencia de datos: ¿Cómo puede transferir, comprar o vender derechos de
algún dato, y asegúrese de que es la única copia que hay?

» Cambio de datos: ¿Cómo se asegura de que los datos no se cambien cuando se
¿no se supone que?

Todos estos problemas se pueden resolver utilizando criptomonedas y blockchain. El gran desafío que enfrenta la industria ahora es escalar la tecnología blockchain para adaptarse a las demandas de almacenamiento de datos y costos de las empresas.

Contratación del tercero en el seguro

Una de las mayores ventajas que la tecnología blockchain introduce en el mundo financiero moderno son los contratos inteligentes que permiten transacciones comerciales sin
la participación de un tercero, como bancos o intermediarios. La eliminación de terceros permite cosas como los micropagos y la reducción de costos asociados con el trabajo humano repetitivo.

En pocas palabras, un contrato inteligente es un protocolo que permite que dos partes registren su transacción en una cadena de bloques. Estos contratos se pueden usar para prácticamente cualquier cosa, desde el intercambio de bienes físicos (que tienen firmas digitales) hasta el intercambio de información o dinero.

La característica clave de seguridad aquí es que, a diferencia de la base de datos ordinaria, el la información es distribuida y verificada por todas las computadoras en la red, haciéndolo descentralizado. Los datos son únicos y no se pueden copiar; la pista de auditoría es inmutable.

Los automóviles autónomos presentan un caso de uso convincente para la tecnología blockchain. Existe un dilema al evaluar la culpa sin un ser humano como testigo. Determinar quién tiene la culpa: ¿fue una falla en la navegación del automóvil, una pieza fabricada o el
otro conductor?

Un grupo interesante que trabaja en la automatización de seguros es Squirrel Finance (https://squirrel.finance), una plataforma de seguros descentralizada para la agricultura de rendimiento en BNB Smart Chain (BSC), anteriormente Binance Smart Chain. Squirrel lo compensa instantánea y automáticamente si le roban sus fondos. Funciona al verificar si ha recibido la cantidad depositada esperada cuando retira. Si el monto no coincide, Squirrel lo compensará automáticamente con el monto de la transacción de retiro de su contrato en forma de NUTS, el token de Squirrel. No hay participación humana después de la configuración. El token de gobernanza de Squirrel también se usa para administrar el protocolo y ganar tarifas de seguro agrícola.

Seguridad descentralizada

En el núcleo de los modelos comerciales actuales se encuentra algo que podría llamarse el paradigma de la confianza centralizada, en el que intermediarios como banqueros, corredores y abogados coordinan y aseguran la veracidad de las transacciones financieras y los intercambios de valores.
bienes.

La centralización conlleva ciertos riesgos de seguridad inherentes, como la corrupción y el robo de datos. Las cadenas de bloques combaten esto creando un sistema descentralizado que se basa en la desconfianza mutua de todos los participantes que se controlan entre sí.

Para crear un sistema de este tipo, crea un libro de contabilidad distribuido que utiliza criptomonedas (como Bitcoin, Ethereum o Cardano), donde cada participante es tanto el
usuario del sistema y responsable de su mantenimiento y conservación.

Cobertura de financiación colectiva

De manera similar a las iniciativas estándar de crowdfunding, la idea es reunir recursos de numerosas entidades o personas para cubrir una deficiencia inesperada en un plan de seguro. Por ejemplo, un plan de seguro de jubilación podría entrar en vigor solo en
la edad de 65 años, pero una persona podría verse obligada a jubilarse anticipadamente debido a imprevistos circunstancias, y el desafortunado individuo necesitaría fondos adicionales.

La disparidad económica ha crecido a lo largo de los años, y numerosas personas con seguro insuficiente o las personas sin seguro podrían beneficiarse de dicho sistema. El crowdfunding puede potencialmente proporcionar beneficios a las tres partes en cuestión:

» Las aseguradoras obtienen mayores ingresos porque más personas están interesadas en sus planes Obtienen acceso a una mayor parte de la población con seguro insuficiente. Además, la compañía aseguradora podría mejorar el reconocimiento de su marca: podría verse como una empresa que se preocupa.

» Los donantes podrían bene ciarse de posibles exenciones impositivas, si la estructura de la campaña lo permite, o podrían obtener otros bene cios, como descuentos o gratis servicios.

» Los buscadores (aquellos que buscan un seguro) obviamente son los que más ganan, ya que pueden obtener una mejor protección y una cobertura más asequible.

Cognizant propuso ideas interesantes para el seguro de crowdfunding en su libro blanco. Puedes encontrarlo en https://goo.gl/u3Kd3U.

Las implicaciones del seguro DAO

Las DAO son entidades corporativas que no tienen empleados a tiempo completo, pero pueden realizar todas las funciones que puede realizar una corporación estándar. La capacidad de crear una entidad de este tipo se deriva directamente de la mejora de los algoritmos de la cadena de bloques, que ha ocurrido en los últimos años y ha creado lo que comúnmente se conoce como cadena de bloques 2.0.

Un DAO es, en esencia, una forma de contrato inteligente avanzado. La DAO puede tratar a la DAO como una corporación en la que todos los usuarios de pólizas individuales son accionistas, mientras que la corporación en sí misma nunca tiene el control directo de ningún grupo o individuo en particular.

De la misma manera, un DAO nunca está bajo el control de los desarrolladores, y estos no emiten ni niegan políticas. Es estrictamente un modelo de seguro entre pares. Si bien aún existen vulnerabilidades con respecto a la verificación de identidad, este sistema será mejorado, y en realidad, los mismos problemas existen incluso en los actuales sistemas centralizados de seguros.

EN ESTE CAPÍTULO

» Leer documentos de blockchain

» Construyendo ciudades inteligentes

» Crear una identidad a prueba de hackers

Capítulo 15

Gobierno

En este capítulo, le presento las emocionantes innovaciones que están teniendo lugar dentro de los gobiernos. Aplicaciones Web 3.0 y otras innovaciones de blockchain, como Bitcoin, están afectando la vida de los ciudadanos comunes en todo el mundo, gracias en parte a la revolución tecnológica de la Web 3.0 y la etapa final de la globalización, conocida como globalización de estado final.

Este capítulo explica cómo los gobiernos enfrentarán los desafíos de fronteras porosas y ciudadanos sin límites que pueden moverse libremente y operar fuera de las instituciones financieras tradicionales. Este capítulo también explica cómo los gobiernos luchan contra los delitos cibernéticos y el robo de identidad gracias al creciente número de casos relacionados con las ofertas de tokens y las criptomonedas.

Después de leer este capítulo, comprenderá claramente los cambios normativos y las iniciativas de ciudades inteligentes que serán fundamentales para el crecimiento económico y la sostenibilidad. Muchos gobiernos están utilizando la tecnología blockchain para tender puentes tecnológicos brechas.

Acción regulatoria mundial

La industria de las criptomonedas ha pasado a una nueva etapa de desarrollo, llamada Web 3.0. Artistas de todo el mundo se han unido a las tecnologías de cadena de bloques para crear arte programable y transferible digitalmente. La mayoría de los artistas están usando

tokens no fungibles (NFT) para representar la propiedad de su arte o fungible
tokens de membresía que permiten a los fanáticos un acceso especial al artista. La adopción masiva de
blockchain ha creado una presión interna para que los gobiernos se unan
para regular el flujo de valor a través de Internet. Los países más pequeños se enfrentan a una
crisis existencial con respecto a las cadenas de bloques, dado que la mayoría de los ciudadanos ahora pueden acceder
tecnología de cadena de bloques y ambos mantienen y crean valor con nada más que un teléfono
inteligente y una conexión a Internet.

Gobiernos como El Salvador se han apoyado en la revolución blockchain. en un
globalrst, El Salvador adoptó Bitcoin como su moneda en 2021. El presidente de El
Salvador, Nayib Bukele, cree que Bitcoin es el camino a la libertad financiera.
Los expertos económicos y muchos salvadoreños temen que el cambio pueda amenazar la
la soberanía del país. Un efecto secundario interesante de la decisión de El Salvador es que
otros países pueden tener que reconocer Bitcoin como moneda de curso legal.

El noventa y cinco por ciento de la población mundial ahora tiene acceso a las criptomonedas.
La mayoría de las personas en el mundo pueden comprar y comercializar nuevos productos financieros. Casi todos
persona en el planeta podría comenzar a usar una identidad soberana que crean para
ellos mismos.

La identidad soberana se refiere a la capacidad de una persona para controlar y administrar su propia
identidad digital, en lugar de depender de terceros para que lo hagan en su nombre. En un sistema de
identidad soberana, las personas tienen la capacidad de crear y administrar sus propias identidades
digitales, que pueden incluir información personal, credenciales y otros
tipos de datos Estas identidades generalmente se almacenan en una plataforma descentralizada,
como una cadena de bloques, que permite a las personas controlar y acceder a su información de
identidad sin depender de una autoridad central.

El objetivo de la identidad soberana es dar a las personas más control sobre sus datos personales y
permitirles interactuar de forma segura y privada con varios sistemas y servicios en línea. También se
ve como una forma de protegerse contra el robo de identidad.
y otros tipos de fraude en línea, porque las personas tienen más control sobre sus
propia información de identidad y puede verificar su identidad usando criptografía
tecnicas

La identidad soberana junto con los mercados abiertos y las plataformas de arte permiten que cualquiera pueda
ganar dinero vendiendo sus creaciones digitales. También hace posible que las personas
evitar impuestos y lavar dinero. Toda esta nueva actividad económica global ha reunido a muchos países
para crear y hacer cumplir las regulaciones y los impuestos en
un grupo conocido como el Grupo de Acción Financiera Internacional (GAFI). Si alguna vez has abierto un
monedero o cuenta de cambio, el GAFI te afecta. El grupo se centra en combatir
blanqueo de capitales y financiación del terrorismo. Incluye 37 de los más influyentes.
y países poderosos del mundo y cuenta con la cooperación de muchos más. El
La lista incluye grandes economías como Estados Unidos, Rusia, China, la mayor parte de Europa,
y la india

El GAFI ha anunciado que las transacciones que involucran criptomonedas y NFT deben cumplir con la Regla de viaje, que requiere que cada país miembro haga cumplir la verificación contra el lavado de dinero (AML) y Conozca a su cliente (KYC) y que las instituciones financieras deben transmitir la información a la próxima institución financiera.

Eso puede no parecer gran cosa, porque todos los bancos han cumplido con esta regla durante años. Pero estas reglas ahora se aplican a las criptomonedas que viven completamente fuera de las instituciones financieras tradicionales. La aplicación es difícil porque las criptomonedas son anónimas y no requieren permiso. Todos los países que forman parte del GAFI deben seguir estas reglas y hacer que los proveedores de servicios de criptomonedas, como billeteras y casas de cambio, recopilen información sobre sus clientes y la envíen a los gobiernos. Deberá ser conocido para enviar y recibir criptomonedas.

Las ciudades inteligentes de Asia

Las ciudades inteligentes están aprovechando la tecnología moderna para mejorar el funcionamiento de la infraestructura y la seguridad, y mejorar aspectos como el tráfico y la calidad del aire. El negocio de convertirse en una ciudad inteligente está en auge y casi todos los municipios más grandes han adoptado el concepto de ciudad inteligente.

Blockchain es especialmente útil cuando se integra con el Internet de las cosas (IoT) utilizado por las ciudades inteligentes. Varios proyectos interesantes están siendo probados ahora para su implementación comercial. El Departamento de Seguridad Nacional de EE. UU. está explorando la seguridad de los dispositivos IoT utilizados por Aduanas y Protección Fronteriza (CBP). Empresas como Slock.it permiten que los objetos conectados utilicen la cadena de bloques para celebrar contratos inteligentes; su primer producto fue una cerradura inteligente habilitada para blockchain, que podían usar los clientes de Airbnb. La integración de estas tecnologías permite que los dispositivos utilicen sus sensores para establecer contratos inteligentes. Esta misma tecnología podría ser utilizada por los parquímetros de la ciudad.

La figura 15-1 muestra la página de inicio del proyecto Smart Nation de Singapur. Singapur ha estado cortejando a nuevas empresas de todo el mundo para desarrollar nuevas tecnologías en su "caja de arena regulatoria". Es una invitación de bienvenida a las empresas de tecnología blockchain que han estado operando en la zona gris (donde no se ha establecido un marco regulatorio claro); sin embargo, muchos países, como Singapur, están tomando medidas directas para definir el espacio e informar a las empresas qué está permitido y qué no.

La tecnología Blockchain también podría usarse para compartir información entre redes en una ciudad inteligente de forma segura. Muchas ciudades están explorando cómo usar blockchain para aliviar los atascos de tráfico. El proyecto Smart Nation de Singapur espera usar el móvil

teléfonos de sus ciudadanos para medir las condiciones de sus viajes en autobús y luego analizar los datos para ver cuándo es necesario mejorar las carreteras. Singapur ha sido líder en el desarrollo de ciudades inteligentes y ha comenzado a desarrollar ciudades inteligentes en otros países.

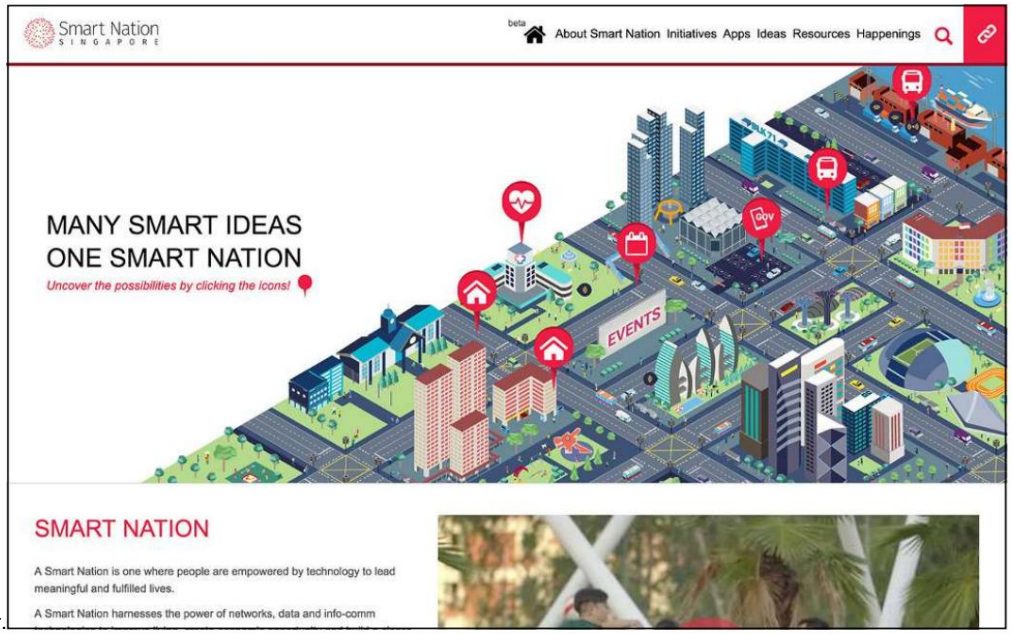


FIGURA 15-1: Proyecto Smart Nation de Singapur.

En esta sección, lo guío a través de algunos de los muchos esfuerzos de blockchain que se están llevando a cabo en Asia.

Ciudades satélite de Singapur en India

El gobierno indio lanzó su Misión Ciudades Inteligentes en 2015, con la intención de construir 100 nuevas ciudades inteligentes y más de 6000 proyectos. Muchos de estos desarrollos estarán en el Corredor Industrial Delhi Mumbai, que es un tramo de 620 millas (1000 km) entre Delhi y Mumbai. Ya se ha planificado infraestructura por un valor de $11 mil millones en 33 ciudades, y gran parte del desarrollo se financiará a través de un modelo público-privado. Se espera que el proyecto atraiga $ 90 mil millones en inversión extranjera, que se utilizará para crear parques empresariales, zonas de fabricación y ciudades inteligentes, todo lo cual se ubicará a lo largo de un corredor ferroviario de carga delegado.

Estas ciudades inteligentes se están desarrollando a medida que la economía de la India se industrializa y la población se vuelve más urbanizada. La intervención estatal en forma de ciudades centralmente planificadas es necesaria para evitar que las ciudades existentes se conviertan en

superpoblado e inhabitable. India es particularmente vulnerable al cambio climático debido a su inmensa y empobrecida población. Por eso, es importante que estas ciudades sean sostenibles e inteligentes. Necesitan materiales de vivienda de bajo consumo energético, redes inteligentes, transporte planificado, sistemas de TI integrados, gobierno electrónico y captación de agua innovadora.

Singapur es un excelente ejemplo de una ciudad inteligentemente planificada. A pesar de la alta densidad poblacional, cuenta con excelente infraestructura y alta calidad de vida. Muchos de las organizaciones privadas de Singapur tienen el conocimiento y los recursos que son necesario para desarrollar las ciudades inteligentes de la India. En colaboración con el gobierno indio, el sector privado podría proporcionar el capital, las habilidades y la tecnología que son necesarios para planes tan grandes.

Andhara Pradesh y la Autoridad Monetaria de Singapur han anunciado un asociación de innovación de tecnología financiera (ntech), con un enfoque principal en blockchain y pagos digitales. Singapur tiene como objetivo desarrollar un mercado para soluciones ntech en India.

El liderazgo de Singapur ha mostrado interés en asociarse con India para desarrollar un ciudad inteligente, así como una nueva capital para Andhra Pradesh, un estado en el sureste. Es establecer comités para analizar el potencial de colaboración en el plan de la India para construir 100 nuevas ciudades, así como desarrollar aún más la infraestructura en 500 pueblos y ciudades existentes.

El ministro de desarrollo urbano de India ha estado en conversaciones tanto con Singapur actual primer ministro y su ex primer ministro. el ha estado buscando La experiencia de Singapur en ciudades inteligentes, centrándose particularmente en sistemas de transporte inteligentes, gestión mejorada del agua y gobierno electrónico. el ministro de El desarrollo urbano también ha estado examinando los esquemas de vivienda pública de Singapur, así como sus reglamentos de vivienda privada. Estructuras de financiación para el transporte También se ha analizado la infraestructura.

Las autoridades indias también han contratado a un equipo de expertos de Singapur para ayudar a la desarrollo de una ciudad satélite en Himachal Pradesh. Los 49 acres (20 hectáreas) el proyecto tiene como objetivo ayudar a descongestionar Shimla, una ciudad que ha tenido una población masiva auge en las últimas décadas. Los singapurenses ayudarán en los aspectos educativos, residenciales y comerciales de la ciudad en desarrollo.

Tanto Singapur como Malasia han mostrado interés en invertir en otro satélite pueblo cerca de Jathia Devi. El gobierno de Singapur está realizando un estudio que evaluará varias opciones. El gobierno estatal de Himachal Pradesh está buscando en el desarrollo de cinco pueblos satélites cerca de las ciudades existentes, utilizando un sistema público-privado modelo de financiación.

Ascendas-Singbridge de Singapur inauguró su octavo parque de TI en India. Se espera que el International Tech Park Gurgaon de 59 acres (24 hectáreas) tenga su primer edificio terminado a mediados de año. El proyecto de $400 millones tiene como objetivo ofrecer 8 millones de pies cuadrados de espacio comercial para ayudar a acomodar el floreciente sector de TI de la India.

El gran problema de los datos en China

La tecnología Blockchain se está discutiendo ampliamente en China como una forma de mejorar la confiabilidad de los grandes datos. La gente lo ve como una forma de resolver el problema de confianza relacionado con el intercambio de datos entre dos o más partes que no tienen incentivos alineados. La tecnología Blockchain ofrece muchas soluciones nuevas para rastrear la propiedad, el origen y la autenticidad.

Peernova es una empresa estadounidense prometedora que está abordando problemas de big data. Anteriormente se centró en la minería de Bitcoin, pero giró hacia el espacio de la cadena de bloques y recaudó $ 4 millones de Zhejiang Zhongnan Holdings Groups, una empresa de construcción de China. Peernova planea utilizar la tecnología blockchain para consultar bases de datos tradicionales y realizar un seguimiento de los cambios.

Los casos de uso son para verificar cualquier cambio en subconjuntos de grandes almacenes de datos y utilizar auditorías criptográficas más eficientes y completas en lugar de un auditor tradicional para proporcionar un punto de referencia para una empresa. Espera ayudar a los fondos de cobertura a calcular la responsabilidad fiscal de sus inversiones mediante el uso de blockchain para rastrear el historial del dinero que se ha invertido a lo largo de los años.

Dalian Wanda, el desarrollador inmobiliario más grande de China, también se está metiendo en el juego de la cadena de bloques. Se ha asociado con la empresa de software de big data Cloudera para lanzar un proyecto de cadena de bloques llamado Hercules. Ve el potencial de usar la tecnología blockchain para hacer que las predicciones derivadas de los grandes datos sean procesables para los gerentes a medida que ocurren, moviendo a los gerentes de reactivos a proactivos en situaciones como modificaciones a sus protocolos, así como monitorear el comportamiento de los usuarios dentro de sus sistemas.

Dalian Wanda y Cloudera tienen como objetivo seguir desarrollando Hercules e integrar su tecnología en una variedad de industrias que dependen de TI y big data. Project Hercu les actuará como una suite de código abierto que respalda las necesidades de las empresas. Hace que sea más fácil para las organizaciones implementar y administrar aplicaciones de cadena de bloques en grandes clústeres de datos.

Puede que le resulte extraño ver a una empresa de minería digital asociarse con una tradicional empresa constructora para abordar problemas de auditoría para fondos de cobertura o bienes raíces empresas que trabajan con big data para resolver problemas para los administradores de sistemas, pero este es el salvaje oeste del mundo blockchain. La escasez de talento blockchain y la gran demanda de proyectos e inversiones de blockchain están alimentando esto ambiente.

La batalla por lo financiero capital del mundo

La tecnología Blockchain se ha hecho realidad desde que irrumpió en la conciencia pública con una gran cantidad de cobertura de noticias en 2015. Muchas nuevas empresas han sido trabajando en compilaciones beta y previas al lanzamiento desde entonces, con casi 2,000 nuevas empresas de cadena de bloques que se formaron de la noche a la mañana en 2016. Muchas de estas finalmente se lanzaron al mercado en 2017 y 2018 en Singapur, Dubái y Londres, donde los organismos reguladores dan la bienvenida a la innovación y compiten por ser la meca financiera del mundo. esto no es solo sobre tecnología y ciudades inteligentes para estos líderes. Es una carrera por la relevancia en un el cambio del mundo a ciudadanos globales sin fronteras y financieramente líquidos.

La previsión temprana de Londres

En 2016, el gobierno central del Reino Unido publicó un informe llamado "Tecnología de contabilidad distribuida: más allá de la cadena de bloques" (https://goo.gl/asIz6L), que afirmó que la tecnología de registros distribuidos (blockchains) podría usarse para reducir la corrupción, los errores y el fraude, y hacer que varios procesos sean más eficientes. También afirmaron que las cadenas de bloques podrían cambiar la relación de los ciudadanos con sus gobierno generando más transparencia y confiabilidad. Pero Londres ha sido muy amigable con la tecnología desde al menos 2014. Muchos de los primeros Las nuevas empresas de blockchain se incorporaron o trabajaron en Londres porque era el lugar excepcionalmente más seguro para construir un negocio. Esto fue un gran problema en ese momento porque muchos empresarios de criptomonedas fueron arrestados en 2014 y 2015.

Desde que salió este informe, las cadenas de bloques han sido aprobadas para su uso en todo aplicaciones gubernamentales en el Reino Unido, incluidos los departamentos de Whitehall (departamentos no ministeriales como el Registro de la Propiedad, la Comisión Forestal y la Comisión de Alimentos) Normas), autoridades locales y gobiernos delegados.

Aquí hay varios proyectos y experimentos interesantes que están ocurriendo en el Reino Unido:

» Distribución de bienestar basada en blockchain: El Departamento de Trabajo y Pensions se asoció con Barclays, RWE, GovCoin y la Universidad de Londres en un experimento que utilizará la tecnología blockchain para distribuir bienestar con una aplicación de teléfono. La prueba se diseñó para ver si los pagos podían enviarse y rastrearse utilizando la tecnología blockchain.

» DLT del gobierno: créditos, un proveedor de plataforma de cadena de bloques y el Reino Unido El gobierno está colaborando en un marco que permite a las agencias gubernamentales del Reino Unido experimentar con la tecnología blockchain. (DLT significa tecnología de libro mayor distribuido).

» Pagos internacionales basados en blockchain: Santander Bank ha lanzado una prueba de pagos internacionales basados en blockchain. El programa stapilot implica una aplicación que se conecta a Apple Pay. Los usuarios pueden usar Touch ID para transferir pagos de entre £10 y £10,000.

» Uso de la tecnología de cadena de bloques para comercializar oro: Royal Mint se ha asociado con CME Group, un operador de mercado, para utilizar la tecnología de cadena de bloques para construir un mercado de oro con la esperanza de hacer de Londres una ciudad más atractiva para las ventas de oro. Las dos entidades están adoptando la tecnología Blockchain porque la ven como un mecanismo digital eficiente para el comercio de oro.

Todos estos son experimentos para ver si la tecnología blockchain es la nueva plataforma para valor de cambio. El éxito o fracaso de este esquema definirá el rumbo futuro del Reino Unido y del resto del mundo.

El sandbox regulatorio de Singapur

Singapur, al igual que el Reino Unido, ha hecho todo lo posible para que trabajar allí sea lo más fácil, amigable, y financieramente atractivo como sea posible. En 2015, funcionarios del gobierno viajaron a San Francisco para anunciar y reclutar emprendedores para trabajar en lo que acuñaron una “caja de arena regulatoria”, un juego con el término caja de arena de desarrollo, que es un entorno seguro donde los desarrolladores pueden crear software. Singapur tenía la misma idea en mente para la creación de empresas de software.

En ese momento, las empresas de blockchain en los Estados Unidos y muchos otros lugares todavía estaban en la zona gris. La idea de un lugar seguro para operar e invertir dinero fue muy atractivo para muchos empresarios, incluido yo mismo. Si nunca has estado a Singapur, debes ir! Es hermoso, limpio y seguro.

Singapur está tomando medidas para explorar la tecnología y está dando sus frutos. Un banco poreano de Singa, OCBC, utilizó tecnología blockchain para transferencias transfronterizas. envió dinero a sus subsidiarias, OCBC Malaysia y el Banco de Singapur.

R3 también ha estado activo en Singapur. Abrió un laboratorio para investigar y desarrollar tecnologías de contabilidad digital junto con la Autoridad Monetaria de Singapur. R3 es trabajando en un intercambio para apoyar los pagos interbancarios. Los bancos depositarán efectivo y se emitirá una moneda digital.

El banco central de Singapur también lanzó un proyecto piloto, junto con ocho extranjeros y los bancos locales, así como la bolsa de valores. Este proyecto de prueba de concepto tiene como objetivo utilizar la tecnología blockchain para sus pagos interbancarios. El proyecto piloto también tiene como objetivo revisar las transacciones transfronterizas en moneda extranjera.

No son solo las empresas de blockchain las que van a experimentar en Singapur. Todo los jugadores más importantes se han involucrado: Bank of America, Merrill Lynch, IBM, Credit Suisse, Banco de Tokio-Mitsubishi UFJ Ltd, DBS Bank Ltd, JP Morgan, The Hong Kong and Shanghai Banking Corp Ltd, OCBC Bank, United Overseas Bank y la Bolsa de Singapur.

TIP

Todos los bancos del mundo deben saber con quién están haciendo negocios. toda la idea de Know Your Customer (KYC) ayuda a combatir el lavado de dinero y la financiación turística.

La siguiente fase será determinar las transacciones en moneda extranjera y construir sobre los esfuerzos KYC de Singapur. Esto podría llevar al país a forjar el camino en identidad basada en blockchain. Singapur ya cuenta con un sistema digital robusto y moderno sistema de identidad que podría conectarse fácilmente a una cadena de bloques.

La iniciativa Dubái 2020

El gobierno de Dubái tenía un plan ambicioso para trasladar todos los documentos y sistemas del gobierno a la cadena de bloques para 2020. El plan para dejar de usar papel era parte de su iniciativa para convertirse en un líder mundial en tecnología blockchain e impulsar eficiencia en todos los sectores.

El Ministro de Gabinete Aire y Futuro detalló cómo será el nuevo esquema permitir a los usuarios actualizar y verificar sus credenciales a través de la cadena de bloques. ellos solo tienen que iniciar sesión con sus credenciales una vez para tener acceso tanto a entidades gubernamentales como privadas, como aseguradoras y bancos. También anticipan compartir su tecnología con otros países para permitir cruces fronterizos más simples.
En lugar de pasaportes, los viajeros también podrían usar billeteras digitales previamente autenticadas como identificación preaprobada.

El gobierno de Dubai ha estimado que su iniciativa blockchain tiene el potencial de ahorrar 25,1 millones de horas en productividad. Este aumento de la eficiencia también ayudar a reducir las emisiones de carbono.

El Global Blockchain Council (GBC) de Dubái anunció siete nuevas colaboraciones público-privadas, combinando las habilidades y recursos de nuevas empresas, empresas locales y departamentos del Gobierno. Aplicarán la tecnología blockchain a lo siguiente:

» Atención médica: la empresa de software de Estonia, Guardtime, colaborará con uno de los operadores de telecomunicaciones más grandes de Dubái, Du, para brindar la experiencia tecnológica para digitalizar los registros de atención médica y trasladarlos a la cadena de bloques.

» El comercio de diamantes: un proyecto piloto utilizará la tecnología blockchain para la autenticación y transferencia de diamantes. El Dubai Multi Commodities Centre digitalizará los certificados de Kimberly (documentos creados por la ONU para restringir el comercio de diamantes en conflicto).

» Transferencias de títulos: las transferencias de títulos se digitalizarán y registrarán en una cadena de bloques. Una startup de blockchain de Singapur conocida como Dxmarkets ha desarrollado una prueba de concepto.

» Registro de empresas: GBC está probando el uso de la tecnología blockchain para el registro de empresas. Esto es diferente a la autonomía descentralizada. organización (DAO) de Ethereum, pero podría agilizar la verificación de identidad a través del programa Flexi Desk. Actualmente se encuentra en la etapa de demostración, con varias entidades trabajando en una prueba de concepto.

» Turismo: Dubai Points es un programa piloto que se lanzó en colaboración con Loyyal, utilizando la tecnología blockchain para ayudar a la industria del turismo. Su objetivo es incentivar los viajes otorgando puntos a los viajeros que visitan determinados lugares. Utilizará contratos inteligentes para facilitar las recompensas. Estos puntos pueden funcionar como un token criptográfico y ser negociables en intercambios.

» Envíos: IBM está trabajando con GBC para usar la tecnología blockchain para envío y logística mejorados. El programa tiene como objetivo ayudar a los actores regionales a colaborar en la forma en que intercambian bienes. Los contratos inteligentes se utilizarán como soluciones para problemas de cumplimiento y liquidación.

Dubái, al igual que Singapur, ha invertido su dinero y talento para asegurarse de que dominará rápidamente el espacio de la cadena de bloques. Este es un lujo del gobierno pequeño y Autoridad central.

Marco regulatorio de Bitlicense: Nueva York

Si planea operar una startup de blockchain en la ciudad de Nueva York, planifique tarifas adicionales En junio de 2015, el Departamento de Servicios Financieros del Estado de Nueva York

(NYDFS) publicó la versión final de Bitlicense, el marco regulatorio para la moneda digital destinado a brindar más claridad a la industria. En realidad, expulsó a muchas nuevas empresas de blockchain de la ciudad de Nueva York. La licencia en sí cuesta $5,000 y puede costar hasta
500 páginas. Requiere las huellas dactilares de los líderes de cada empresa y una extensa verificación de antecedentes de las empresas solicitantes. La principal queja es la aproximadamente $100,000 en gastos asociados con la solicitud. Esta estimación incluye el tiempo honorarios de asignación, legales y de cumplimiento. Bitlicense está en marcado contraste con los esfuerzos realizado por otros centros financieros como Londres, Singapur y Dubai.

Thenal Bitlicense fue el resultado de casi dos años de investigación y debate sobre cómo debe regularse la tecnología. Ocurrió después de que se consideró que las regulaciones existentes no eran adecuadas para las empresas de moneda digital.

En una nota positiva, las empresas de blockchain de NYC ya no necesitan la aprobación de NYDFS para nuevas actualizaciones de software o más rondas de financiación de capital de riesgo. El marco establece que las empresas de moneda digital solo necesitan aprobación para cambios que se “proponen a un producto, servicio o actividad existente que pueden hacer que dicho producto, servicio o actividad sea materialmente diferente de lo que figuraba anteriormente en la solicitud de licencia del superintendente”.

La primera empresa en recibir una Bitlicense fue Circle, los proveedores de monederos de Bitcoin. La licencia les permite operar en Nueva York bajo el marco regulatorio.
Circle es una de las pocas empresas que puede hacerlo legalmente. La mayoría de las nuevas empresas de blockchain están evitando trabajar en Nueva York porque el costo y el esfuerzo de la licencia superan el beneficio. Solo las startups mejor financiadas están haciendo un esfuerzo.

Ripple ha obtenido su segunda licencia. Esta iteración de su licencia ha le permitió vender y mantener XRP, que es el activo digital detrás de Ripple Libro mayor de consenso (RCL). Mejorará la capacidad de Ripple para hacer frente a los negocios. clientes que quieran utilizar su tecnología para transferencias internacionales de fondos.

Otras regiones de EE. UU. también han presentado proyectos de ley similares para regular la moneda digital y requieren licencia. El proyecto de ley AB 1326 de California habría hecho eso por la región, pero fracasó después de que la Electronic Frontier Foundation (EFF) pudiera oponerse. (El EFF es un grupo con sede en San Francisco que defiende los derechos del consumidor y los nuevos tecnología.)

Aunque la ciudad de Nueva York fue temprana en regular, ha sido un lugar difícil y peligroso para que operen las empresas basadas en blockchain. NYC ha prohibido algunos nuevos productos financieros que eran demasiado competitivos para las instituciones tradicionales, como cuentas criptográficas que devengan intereses que a menudo promediaban el 8 por ciento. También impuso una $ 100 millones contra BlockFi, un custodio líder de cuentas criptográficas, destruyendo una empresa tecnológica que alguna vez fue prometedora.

Estructura legal amigable de Malta

Malta, país miembro de la Unión Europea, ha tomado medidas drásticas y directas para adoptar la tecnología blockchain. Avanzando mucho más rápido que otras naciones, Malta vio el potencial de blockchain y tomó medidas para asegurarse como un centro para innovación. La mayoría de las nuevas empresas de blockchain se han enfrentado a un entorno hostil, por lo que muchos, incluido el megaexchange Binance, viajaron a Malta para establecer negocio.

Tras la salida del Reino Unido de la UE, Malta será uno de los pocos países que queden en la UE que tiene el inglés como lengua oficial. Malta también se rige por el derecho continental y el common law, lo que los hace más favorables para los negocios. Este ha posicionado bien a Malta para apoyar a las empresas internacionales relacionadas con blockchain y criptomonedas que desean incorporarse y tener una estructura legal.

Malta es una isla pequeña que ha visto muchos regímenes gobernantes diferentes. Cada uno estableció sus propias reglas y algunas de ellas se han mantenido. Malta tiene una legislación mixta marco actual que incluye el derecho romano, el derecho francés, el derecho británico y sus propios leyes promulgadas por el parlamento maltés después de la Independencia de 1964. Pero son conocido principalmente por el derecho civil o continental (que se ha codificado a lo largo de los años) y el common law (que se establece mediante sentencias judiciales).

Malta ha aprobado dos leyes innovadoras y un proyecto de ley que han cambiado la conversación en torno a la capacidad jurídica de las empresas de cadenas de bloques, ofreciendo protección legal y un marco que rige con mayor precisión la tecnología distribuida. blockchains y toda la innovación que ha surgido de ellas. aquí hay un resumen de estas tres leyes:

- Ley de Activos Financieros Virtuales: La Ley de Activos Financieros Virtuales regula las ofertas iniciales de monedas (ICO). La ley exige que cualquier empresa que obtenga capital a través de una ICO publicará un libro blanco con una descripción detallada de todo el proyecto. El ICO también debe hacer público el historial financiero de la empresa.
- Ley de la Autoridad de Innovación Digital de Malta: La Ley de la Autoridad de Innovación Digital de Malta crea procedimientos regulatorios para las empresas de criptomonedas y blockchain. También establece un organismo regulador llamado Autoridad de Innovación Digital de Malta (MDIA).
- Proyecto de Ley de Acuerdos y Servicios Tecnológicos: El Proyecto de Ley de Acuerdos y Servicios Tecnológicos permite que las empresas de blockchain y los intercambios de criptomonedas se registren y obtengan la certificación del gobierno de Malta.

Estos nuevos actos y proyectos de ley han abierto a Malta a las nuevas tecnologías y posiblemente serán utilizados como ejemplo por otros gobiernos que también esperan atraer la innovación. El mayor beneficio es brindar a las empresas un lugar seguro para crecer y experimentar dentro de parámetros conocidos.

Asegurando las fronteras del mundo

Muchos gobiernos están explorando Blockchain para asegurar las fronteras. el reino unido tiene un objetivo ambicioso de garantizar que los viajeros nunca tengan que perder el ritmo mientras viajan moverse por sus aeropuertos. Esto contrasta con las largas filas de seguridad que están presentes ahora en casi todos los aeropuertos. Los principales obstáculos que debe superar el Reino Unido para una experiencia de viaje sin fricción tienen que ver con la resolución del pasajero (la capacidad de conocer denitivamente la identidad de cualquier pasajero dado, incluso si el pasajero es de otro pais). La resolución de pasajeros ha sido un problema para los países que están lucha contra el terrorismo.

Estados Unidos ha abierto su tecnología para la resolución de pasajeros bajo el Sistema Global de Evaluación de Viajes (GTAS). Está disponible para la colaboración pública en GitHub (www.github.com/US-CBP/GTAS).

Computadoras, cámaras y sensores involucrados en la detección no invasiva y la autenticación de los pasajeros debe asegurarse para garantizar la seguridad nacional. Las cadenas de bloques, con sus propiedades inmutables subyacentes, son una tecnología prometedora para este caso de uso y se están probando ahora.

La otra cosa interesante que se puede crear a través de cadenas de bloques son las identidades biográficas, identidades que se construyen con el tiempo. Cualquier dato se puede vincular con un identidad biográfica, y la privacidad y legibilidad de los datos atribuidos pueden ser gestionado por los editores. Con el tiempo, la identidad se construye agregando atributos adicionales. Los atributos pueden ser casi cualquier cosa, desde datos o su dispositivo personal hasta instancias en las que sus documentos fueron revisados en un cruce fronterizo. Estos atributos son publicados en la cadena de identidad del individuo por las autoridades de certificación o los autorizados por las autoridades del certificado.

El Departamento de Seguridad Nacional y la identidad de las cosas

El Departamento de Seguridad Nacional de la Dirección de Ciencia y Tecnología exploró la seguridad de los dispositivos IoT para las fronteras de EE. UU. Ha trabajado con la ahora desaparecida Factom, Inc., una startup de blockchain con sede en Austin, Texas, para avanzar en la seguridad de identidad digital para dispositivos IoT.

Factom creó registros de identidad que capturan la identificación de un dispositivo, quién lo fabricó, listas de actualizaciones disponibles, problemas de seguridad conocidos y autorizaciones otorgadas mientras agregando la dimensión del tiempo para mayor seguridad. El objetivo es limitar los posibles habilidades de los piratas informáticos para corromper los registros anteriores de un dispositivo, lo que dificulta parodia.

Pasaportes del futuro

ShoCard (www.shocard.com) es una empresa de desarrollo de aplicaciones que trabaja con la empresa de cadena de bloques Blockcypher. Ha construido prototipos que le permiten establecer su identidad dentro de un entorno seguro de cadena de bloques. ID de la tarjeta ShoCard
vive en una aplicación en su teléfono y puede usarse para compartir todos los diferentes tipos de credenciales de forma segura.

El nuevo documento de alimentación

Puede que no hayas oído hablar de Smartrac, pero lo más probable es que toques un
pieza de su tecnología todos los días. Smartrac es el proveedor número uno de etiquetas de identificación por radiofrecuencia (RFID) y otros chips de identificación que viven dentro
de cosas como pasaportes y tarjetas de identificación.

Uno de los mayores desafíos que enfrentan los países en la lucha contra el fraude de identidad está en
la autenticación de los documentos subyacentes utilizados para construir identidades. Estos son
cosas como tarjetas de Seguro Social, certificados de nacimiento y diplomas, que actualmente son fáciles y baratos de eliminar.

Smartrac ha estado combatiendo este problema con tecnología cada vez más sofisticada. Su última innovación, dLoc, es una solución de autenticación de software que
permite que los documentos del alimentador se cotejen con un registro de cadena de bloques.

Los datos del documento están casados con una ID única de la etiqueta de comunicación de campo cercano (NFC) para crear un valor hash de 32 bits, que solo es reconocible por el emisor
agencia utilizando una clave privada. El valor hash se almacena en Smart Cosmos y se respalda
en una cadena de bloques pública. Después de que eso haya sucedido, el documento con el dLoc
La etiqueta se puede verificar usando un lector de escritorio o una aplicación móvil en un dispositivo habilitado para NFC. teléfono.

Lo que esto hace es crear dos cosas asombrosas que nunca han sido posibles con
documentos en papel:

» Un historial inalterable del documento, mostrando su verdadera antigüedad y propiedad.

» Permitir que las autoridades de certi cado firmen la autenticidad de un documento criptográficamente. Por lo tanto, incluso si se robara el papel subyacente utilizado para crear documentos, no se firmaría adecuadamente, o si se tomara un documento después de su emisión, podría marcarse como un documento robado.

EN ESTE CAPÍTULO

Capítulo 16

Otras industrias

Es fácil concentrarse en los proyectos y la industria de blockchain más destacados. impactos, pero la tecnología blockchain ya ha comenzado a tocar todos los aspectos de la sociedad.

En este capítulo, lo guío a través de algunas de las aplicaciones más interesantes e inusuales de la tecnología blockchain que quizás no haya sospechado. Algunas de las transformaciones más emocionantes ocurrirán dentro de los sistemas gubernamentales, nuevas capas de confianza para Internet y nuevas industrias creadas por blockchains. Aquí, descubre los cambios más impresionantes que están ocurriendo ahora y cómo estas transformaciones afectarán su vida y la industria en la que trabaja, así como la
gobiernos y agencias que te protegen.

Gobiernos esbeltos

Unas pocas naciones pequeñas se han dado cuenta de que si van a competir en una economía global, tienen que ofrecer más y hacerlo de una manera que no suponga una carga para sus clientes. los ciudadanos. Para poder competir, han cambiado muchas de las ideas tradicionales sobre lo que significa brindar ciudadanía. En un mundo que se mueve desde fronteras duras

a los muy porosos, donde las personas tienen el poder de elegir dónde vivir y qué país llamar hogar, estos pequeños países lo están haciendo bien.

La ciudadanía se está convirtiendo en un bien que se puede comprar, y cada nación ofrece diferentes ventajas. Los países se están alejando del modelo de ciudadanía pasiva, en el que naces ciudadano de un país, a uno en el que eliges la ciudadanía en función de las ventajas que ofrece ese país.

Bajo este nuevo modelo, la ciudadanía ya no está atada a una ubicación física. El gobierno puede existir sin fronteras o una ubicación física. Los viejos modelos ven a la ciudadanía como un lugar que puede ser invadido y anulado por otra nación o fuentes internas, como una revolución.

La tecnología Blockchain y otras innovaciones de primer nivel se están adoptando en estas áreas: primero, porque lo hacen posible y, segundo, porque ayudan
reducir el peso sobre el gobierno mediante la creación de sistemas más eficientes que los ciudadanos puede acceder rápidamente a cualquier parte del mundo, incluso si el territorio físico está invadido.

Singapur, Estonia, los Emiratos Árabes Unidos (EAU) y China han sido líderes del mercado en este tipo de iniciativas. El proyecto Smart Nation de Singapur y e-Residency de Estonia son sistemas únicos que se esfuerzan por reducir el papeleo y los tiempos de espera de los ciudadanos y aumentar la eficiencia de los recursos compartidos. El
La iniciativa 2020 que lanzó Dubai eliminará todos los documentos físicos y los reemplazará con documentos o sistemas respaldados por blockchain. Los esfuerzos de China para reducir
el fraude ha cambiado la dinámica del espacio blockchain.

Proyecto Smart Nation de Singapur

Smart Nation es el esfuerzo nacional de Singapur para crear un futuro de mejor vida para todos sus ciudadanos y habitantes. Las personas, las empresas y el gobierno están trabajando juntos. El proyecto abarca desde la identidad digital hasta los sensores IoT que optimizan los registros públicos.

Singapur cree que las personas empoderadas por la tecnología pueden llevar vidas más significativas y plenas. Está explotando nuevas tecnologías, redes y big data para
su búsqueda más completa y activa de innovación a través de sandboxes reguladores y el reclutamiento activo e incentivando la innovación por parte de las nuevas empresas.

Puede ver una representación de la iniciativa Smart Nation en https://goo.gl/EGmF4X.

Singapur ha podido probar e implementar rápidamente nueva tecnología porque tiene un gobierno de una sola capa. Coordina políticas y esfuerzos entre instituciones.
rápidamente. Smart Nation es un excelente ejemplo de esta filosofía de que la nueva tecnología triunfa sobre la política como de costumbre.

Residencia electrónica de Estonia

Estonia es un pequeño país de la Unión Europea con 1,3 millones de habitantes. Tiene recursos limitados para satisfacer las necesidades de sus ciudadanos, pero a través de la tecnología ha podido superar las capacidades de muchas naciones más grandes. Estonia lanzó tarjetas de identificación digitales para servicios en línea y fue el primer país en ofrecer e-Residency, una identidad digital, disponible para cualquier persona en el mundo interesada en operar un negocio en línea.

Registrarse para una residencia electrónica en Estonia toma unos minutos y la verificación de antecedentes cuesta alrededor de $ 100. Tener una tarjeta de residencia electrónica no te convierte en ciudadano de Estonia, pero te brinda muchos beneficios.

TIP

También puede convertirse en e-Resident de Estonia. Solicite en línea en www.e-resident.gov.ee/become-an-e-resident/.

Después de salir de la Unión Soviética, Estonia invirtió mucho en nueva tecnología. Se alejó completamente del gobierno tradicional a uno en el que utiliza un principio de ventanilla única (un punto de acceso para los ciudadanos). El principio de ventanilla única permite el acceso a todos los servicios fiscales y aduaneros para los ciudadanos con un único inicio de sesión seguro en cualquier parte del mundo. Las transacciones directas y sin papel son posibles a través de este sistema. Todo, excepto el matrimonio y las compras de bienes raíces, se puede hacer completamente en línea. Los ciudadanos estonios pueden realizar transferencias bancarias o pagar impuestos en unos minutos.

El pueblo estonio espera que su gobierno simplifique y utilice más soluciones de TI. El desarrollo activo de los servicios electrónicos ha reducido la cantidad de visitas a las oficinas de servicios de la Junta de Impuestos y Aduanas de Estonia en más del 60 por ciento entre 2009 y 2016, lo que reduce el costo total.

Estonia mejoró su entorno de declaraciones de impuestos sociales y sobre la renta en 2015 y recaudó 125 millones de euros más en impuesto al valor agregado (IVA) que el año anterior debido al desarrollo y uso extensivo de servicios electrónicos. El gobierno de Estonia agregó una calculadora de obligaciones tributarias que extrae datos de los sistemas bancarios incorporados de los ciudadanos. También facilitó el envío de facturas al sistema.

Los estonios han adoptado las tecnologías blockchain. El próximo gran desarrollo será una nube habilitada para blockchain. Estonia ha contratado a Ericsson, Apcera y Guardtime para desarrollar y operar conjuntamente una plataforma de nube híbrida que mejorará la escalabilidad, la resiliencia y la seguridad de los datos de la declaración de impuestos y el asesoramiento de atención médica en línea.

Nasdaq también está desarrollando servicios de cadena de bloques en Estonia. Está construyendo un mercado para empresas privadas que realiza un seguimiento de las acciones que emiten y les permite liquidar transacciones de inmediato. Se centra en mejorar el proceso de voto por poder para las empresas. Será una forma de registrar su negocio.

El proyecto Bitnation está colaborando con Estonia para ofrecer un notario público para e-Residents de Estonia, que permitirá a los e-Residents de Estonia, independientemente de dónde vivan o hagan negocios, certificar ante notario sus matrimonios, certificados de nacimiento y contratos comerciales en una cadena de bloques. Los documentos notariados de Blockchain no son legalmente vinculantes en la jurisdicción de Estonia, ni en ninguna otra nación o estado, pero permitirá a los ciudadanos probar la antigüedad de estos documentos.

Mejor notarización en China

China tiene una relación de amor y odio con las criptomonedas. Por un lado, los ciudadanos chinos han estado tratando de usar tokens como un medio para lavar dinero fuera del país u ocultar ganancias de los impuestos. Esto ha provocado que el gobierno chino endurecer la regulación en torno al uso de criptomonedas. Sin embargo, a medida que la utilidad de la tecnología blockchain subyacente se ha expandido más allá del movimiento del valor, China ha comenzado a adoptar la tecnología blockchain.

Un ejemplo interesante de su uso temprano fue el de Ancun Zhengxin Co., que está liderando el cambio a los servicios notariales de datos electrónicos en China a través de asociaciones con más de 100 oficinas notariales tradicionales en 28 provincias. También está ofreciendo almacenamiento electrónico de datos y solución de notarización blockchain a través de tradicional oces.

Ancun publica miles de registros en una cadena de bloques de búsqueda pública que permite a los usuarios regresar y verificar la autenticidad y la antigüedad de los certificados notariales. documentos.


TIP

Muchas nuevas empresas están trabajando en conceptos similares en los Estados Unidos. Por ejemplo, WordProof (https://wordproof.com) le permite usar hash y fecha y hora en su sitio web.

La capa de confianza para Internet

Durante los últimos 30 años, Internet se ha construido en capas: una capa sobre otra. el siguiente, haciéndolo más fácil y seguro para quienes lo usan. La cadena de bloques es el siguiente capa de Internet. Piense en ello como la capa de confianza. Es probable que se desvanezca silenciosamente de la conciencia del público y simplemente comience a hacer que sus interacciones en línea sean más placenteras. La implementación de la tecnología blockchain finalmente eliminará los irritantes problemas que comúnmente ocurren en línea porque no hay suficientes formas de confiar en la información.

Hay dos áreas clave en las que se ha comenzado a trabajar de las que tal vez no esté al tanto pero que le encantarán: correo electrónico con poco o ningún spam y un nuevo tipo de identidad en línea.

Correo electrónico web 3.0

Mailchain (https://mailchain.com) es una nueva plataforma de correo electrónico basada en blockchain que le permite enviar mensajes totalmente encriptados a otras cuentas de Mailchain y a los titulares de billeteras ETH y NEAR. Mailchain le brinda la propiedad total de sus datos y está trabajando para hacer que Internet sea un poco más privado. (El correo electrónico sin cifrar es una vulnerabilidad importante).

Todos los mensajes de Mailchain están cifrados de extremo a extremo de forma predeterminada. Sus claves privadas utilizadas para cifrar sus mensajes nunca se revelan al protocolo Mailchain. Su frase de recuperación secreta se utiliza para crear una serie de claves privadas, cada una de las cuales realiza acciones independientes que le permiten registrar direcciones y autenticar, almacenar y guardar mensajes de forma privada.

La aplicación Mailchain cifra sus datos desde su navegador web. Luego, los archivos cifrados se almacenan en Mailchain. Solo usted puede descifrar estos a través de sus claves privadas. Mailchain no puede descifrar su frase de recuperación secreta, mensajes o direcciones registradas.

Mailchain utiliza una clave de mensajería en lugar de la clave de su billetera para cifrar y descifrar mensajes para cada dirección. Las claves de mensajería son más seguras para el cifrado y significan que no expone la clave privada de su billetera.

Cuando registra una dirección de billetera con su cuenta de Mailchain, se crea una nueva clave de mensajería. Con su billetera, firma una confirmación para indicar que esta clave debe usarse para enviar mensajes. La firma de esta confirmación crea una prueba de que los usuarios puede verificar independientemente. Solo conoce la clave privada para la mensajería.

Las direcciones registradas se cifran antes de almacenarse y solo necesita verificar la propiedad de la dirección de su billetera una vez. Mailchain desconecta su billetera después de que su billetera haya creado la prueba. La clave privada de su billetera nunca está expuesta.

Cada vez que se envía un correo electrónico, se crea una nueva clave de cifrado para cifrar el mensaje y su ubicación. A continuación, la clave de cifrado se cifra de forma exclusiva para cada dirección que recibe el mensaje. Se crea una nueva clave para cada destinatario y para cada nuevo mensaje. Esto es importante para garantizar que solo el destinatario previsto lea el contenido del mensaje.

Cuando se envía un mensaje, el mensaje se cifra y se almacena en almacenamiento distribuido. Una "solicitud de entrega" encriptada contiene información para que el destinatario del mensaje pueda recopilar su mensaje encriptado. Sus mensajes se guardan en lo que se denomina una capa de transporte efímero, que es temporal y solo existe hasta que su mensaje se haya recuperado o su correo electrónico caduque.

Cuando recibe un mensaje nuevo, se guarda en su bandeja de entrada privada. Antes de almacenarse, su nuevo correo electrónico se vuelve a cifrar con una clave específica para su bandeja de entrada.

Su bandeja de entrada también está protegida a través de una clave privada. Todos los ID, ltros y metadatos son encriptado. Mailchain no puede identificar relaciones incluso si varias direcciones recibieron los mismos mensajes.

Si esto parece una opción interesante de correo electrónico seguro, vaya a https://mailchain.com para reclamar su cuenta de correo electrónico gratuita.


REMEMBER

Ninguna solución de seguridad de Internet es perfecta. Hay formas de ver sus datos (por ejemplo, mediante el uso del software espía Pegasus) incluso si envía mensajes totalmente encriptados. Desarrollado por la empresa israelí de armas cibernéticas NSO Group, Pegasus se instala de forma encubierta en todo tipo de dispositivos con iOS y Android. Utiliza un ataque de clic cero que explota las lagunas existentes en la verificación de datos. Pegaso es capaz
de leer mensajes de texto, rastrear llamadas, recopilar contraseñas, rastrear su ubicación, acceder al micrófono y la cámara de su dispositivo y recopilar información de otras aplicaciones.

Ser dueño de su identidad en web3

El World Wide Web Consortium (W3C) es una organización sin fines de lucro establecida en
2012 que ayuda a desarrollar protocolos y lineamientos que aseguran el crecimiento a largo plazo de la web. El W3C desarrolló el Paradigma moderno para estándares, cuyo objetivo es ayudar a mejorar radicalmente la forma en que las personas de todo el mundo desarrollan nuevas tecnologías e innovan para la humanidad.

Una iniciativa importante han sido los identificadores descentralizados (DID). DID, también
conocidas como identidad auto-soberana, son un nuevo tipo de identidad globalmente única.
Impulsados por las leyes de la identidad emitida centralmente, estas nuevas identificaciones autoemitidas permiten que controle su identidad mediante firmas digitales que utilizan pruebas criptográficas.

La mayoría de los identificadores únicos o modelos de identidad (como su número de Seguro Social) no están bajo su control. Las autoridades externas, como los gobiernos, emiten sus identificaciones y deciden lo que significan. Son válidos sólo en contextos específicos y
reconocida por ciertas organizaciones. Pueden desaparecer o dejar de tener vigencia en cualquier momento. Estas identificaciones a menudo revelan información personal sobre usted que no es necesaria. Los ID también son replicados de manera fraudulenta por terceros maliciosos, todo sin
tu consentimiento.

Debido a que usted controla la generación y afirmación de DID, puede tener tantos DID como sea necesario para mantener la separación de personas e interacciones en línea. Uno de los principios fundamentales de los que hablan los entusiastas de blockchain
about es la responsabilidad personal de poseer los datos que creas y que te identifican de manera única. Este concepto puede parecer sencillo, pero la mayoría de las personas
no poseen ni controlan los datos que representan sus identidades.

La mayor parte del control está en manos de bases de datos centralizadas que son vulnerables a la piratería. Estas bases de datos contienen la información y las autoridades certificadoras validan que el la información es correcta e inalterada. En la era de la información, sus datos son su identidad. Cuanto más distribuidos estén los datos, mayor será la probabilidad de que caigan en manos de quienes quieran hacer un mal uso de ellos.

La identidad basada en blockchain coloca el control de la identidad en manos de los individuos o corporaciones que representa la identidad. Bases de datos centrales y certificado las autoridades no son necesariamente reemplazadas. Los datos todavía necesitan un hogar seguro, y todavía tiene sentido que terceros validen la autenticidad de los documentos.

El valor de cambiar el orden de responsabilidad en torno a la identidad es que se vuelve más difícil robar, tomar como rehenes o manipular los documentos subyacentes que representan su identidad. La información se comparte según sea necesario sin exponer información innecesaria. Una identidad irrevocable y accesible a nivel mundial puede no ser siempre algo bueno. Quienes construyan plataformas de identidad deberán tener en cuenta la protección del consumidor, como la condonación de créditos, el derecho al olvido y el anonimato de los votantes.

Oráculo de la cadena de bloques

La tecnología Blockchain no resuelve el problema de que la información debe provenir de alguna parte. También es importante que se pueda confiar en la información. Es el elemento humano que aún no se puede eliminar de la ecuación cuando desea actuar sobre un contrato dentro de un sistema de cadena de bloques.

No existe una autoridad central para vigilar o hacer cumplir la honestidad en un sistema de cadena de bloques. Predecir la futura honestidad de los autores de la información es imposible. La conclusión lógica es que cada transacción debe costar menos que el costo de reconstruir la reputación. La reputación de los autores de confianza se construye con el tiempo, y cuanto más tiempo un autor es honesto y correcto, más valiosa se vuelve la reputación del autor.
Este concepto es similar al valor de una marca.

En esta sección, explico cómo los artistas y creativos utilizan la tecnología blockchain para monetizar su trabajo a través de la tecnología blockchain.

Autoría de confianza

Los contratos inteligentes y los códigos de cadena han creado una nueva oportunidad para que las personas y corporaciones con conocimientos moneticen su información. Estos tipos de sistemas necesitan fuentes confiables de información contra las cuales ejecutar. Estas fuentes confiables podrían ser agencias de calificación, medios meteorológicos o casi cualquier otra cosa.

También puede conectar dispositivos IoT a una infraestructura de cadena de bloques y hacer que creen sus propias voces e identidades en una red de cadena de bloques. Necesitan generar confianza con el tiempo y aún pueden corromperse en cualquier momento. La honestidad pasada no previene la deshonestidad futura o la corrupción de una fuente de información.

No todos los contratos inteligentes o códigos de cadena son autónomos o se ejecutan contra fuentes infalibles. El caso de uso comercial más práctico y aplicable requiere que la información se derive de fuentes fuera del universo conocido de cualquier red blockchain determinada. Varias startups están atacando este problema desde diferentes
anglos.

OpenSea es una startup que está construyendo un protocolo descentralizado para la propiedad, el descubrimiento y la monetización de contenido. Lo hace a través de un mercado NFT. Su sistema está diseñado para registrar y marcar metadatos e información de propiedad sobre activos creativos, como escritura y música.

Factom ha creado Acolyte, un servicio que permite a los usuarios construir una reputación en el tiempo por la información que brindan a la red. Los creadores de contratos inteligentes pueden suscribirse y compensar los oráculos que se crean. También pueden calificarlos por su confiabilidad.

Desde un ángulo radicalmente diferente, Augur, otra startup de blockchain, ha sido pionera en la idea de los mercados de predicción. Augur es una plataforma que recompensa a los usuarios por predecir eventos futuros del mundo real, como elecciones o compras corporativas. Las apuestas se realizan intercambiando acciones virtuales en el resultado de los eventos. Los usuarios ganan dinero comprando acciones en los resultados correctos. El costo de las acciones se eleva basado en cómo se siente la comunidad acerca de la probabilidad de que el evento suceda agudamente. Augur es similar a un sitio web de apuestas. Cualquiera puede hacer una predicción. Cualquiera puede crear un mercado de predicción para cualquier evento dado. Esto le permitiría, como propietario de un negocio, por ejemplo, realizar una encuesta sobre lo que la gente piensa que es más probable que ocurra. También puede descubrir información interna que a los autores les gustaría poder capitalizar.

Derechos de propiedad intelectual

Una de las industrias más afectadas que lucha con los derechos de propiedad intelectual es la industria de la música. Los artistas en la cima se ven exprimidos económicamente por los muchos intermediarios que dependen de su trabajo creativo. Los pequeños artistas no pueden hacer de la música una fuente principal de ingresos porque solo ven una pequeña fracción de los ingresos. Las megaestrellas lo logran gracias al gran volumen de fanáticos.

Internet ha facilitado que artistas de todos los tamaños compartan su trabajo. Al mismo tiempo, ha hecho que sea aún más difícil para las personas ganarse la vida cómodamente haciendo lo que aman. La cadena alimenticia de la industria de la música es larga, y cada intermediario toma una pequeña parte del pastel y se suma al tiempo que tardan los fondos en llegar al artista. A menudo, el artista esperará hasta 18 meses o más
para ver dinero y solo puede obtener $ 0.000035 por instancia de transmisión de su música. Esta situación es el mejor de los casos en nuestro mercado actual, sin que nadie defraude al artista.

Blockchain se ha introducido como una forma de ayudar a aligerar las enormes finanzas
carga sobre los creativos. La criptomoneda podría usarse para reducir las tarifas de transacción asociadas con las tarjetas de crédito y el fraude. También abriría nuevos mercados en países en desarrollo que no tienen acceso regular a tarjetas de crédito.

Una posibilidad aún más interesante pero menos sencilla sería migrar todo el ecosistema de la industria de la música a un sistema de cadena de bloques que utilizara contratos inteligentes o código de cadena para facilitar el pago inmediato por la utilización. También podría aclarar la propiedad de las licencias y facilitar a los consumidores la concesión de licencias de música para uso comercial.

Varios proyectos están trabajando en este tema y buscan promover un ecosistema saludable, sostenible y sin fricciones, uno que no desplace a los actores del mercado.
pero permite a los artistas ganar un poco más de su arduo trabajo.

UjoMusic está probando su plataforma beta que permite a los usuarios vender y licenciar música directamente. Utiliza la red Ethereum, contratos inteligentes para la ejecución y Ether (la criptomoneda Ethereum) para el pago. Puede descargar una canción completa o solo las partes vocales e instrumentales para uso comercial o no comercial. Luego, a los músicos se les paga inmediatamente con Ether.

Peertracks es una de las primeras empresas de blockchain que está trabajando para cambiar la industria de la música. Es un sitio web de transmisión de música que permite a los usuarios descargar y descubrir nuevos artistas. Lo hace a través de su red peer-to-peer llamada MUSE y la creación de tokens de artistas individuales. Estos tokens funcionan como otras criptomonedas y varían en valor según la popularidad del artista. Desde 2020
sin embargo, ha habido una proliferación de plataformas que le permiten descubrir artistas, incluidos OpenSea, SuperRare, Nifty Gateway y Mintable, solo por nombrar algunos.
Los propios artistas también se han metido en el juego, Snoop Dogg lanzando sus propios NFT en MakersPlace.

La tecnología Blockchain no elimina la necesidad de sellos discográficos y distribuidores.
Sin embargo, deberán actuar con rapidez si no quieren ser desplazados por nuevas empresas que adapten este modelo más eficiente, tal como Netix irrumpió
Éxito de taquilla.

5

La parte de las decenas

EN ESTA PARTE . . .

Descubra diez recursos gratuitos de blockchain que lo ayudarán a mantenerse actualizado sobre la tecnología y la industria.

Identifique diez reglas que nunca debe romper mientras trabaja en el mundo de las criptomonedas y la cadena de bloques.

Obtenga más información sobre los diez principales proyectos y organizaciones de cadenas de bloques del metaverso que están dando forma al futuro de la industria.

EN ESTE CAPÍTULO

» Descubrir recursos educativos gratuitos de blockchain

» Involucrarse en la comunidad blockchain

» Mantenerse actualizado sobre las últimas noticias de la cadena de bloques

» Profundizando su conocimiento de otros recursos de blockchain

Capítulo 17

Diez (más o menos) Gratis Recursos de cadena de bloques

En este capítulo, describo interesantes recursos gratuitos en el ecosistema blockchain. Aquí, puede encontrar herramientas gratuitas para crear oráculos (las fuentes de datos que permiten la ejecución de contratos inteligentes), videos que ampliarán su conocimiento y organizaciones que están dando forma al futuro de la industria.

Etéreo

Ethereum es un proyecto de financiación colectiva de código abierto que construyó las cadenas de bloques de Ethereum. Es uno de los proyectos más importantes en el espacio porque ha sido pionero en la construcción de un lenguaje de programación dentro de una cadena de bloques. Debido a su lenguaje de programación incorporado, la red Ethereum le permite crear contratos inteligentes, crear organizaciones descentralizadas e implementar aplicaciones descentralizadas.

Ethereum 101 (www.ethereum.org) es un sitio web iniciado por los miembros de la comunidad Ethereum. Es un repositorio curado de contenido educativo de alta calidad sobre la tecnología blockchain y la red Ethereum. Anthony D'Onofrio, Director de Comunidad de Ethereum, supervisa el proyecto.

acuñado

Si es nuevo en los tokens no fungibles (NFT) y está buscando una manera fácil y sin complicaciones de configurar su billetera y comenzar a recolectar activos digitales únicos, no busque más allá de Got Minted. Inve pasos simples, el sitio lo guía a través
crear su billetera, acuñar su primer NFT, conectar su billetera a OpenSea,
y explorar NFT en el mercado. Estará listo para experimentar el apasionante mundo de las NFT en unos diez minutos. Ya sea que quiera coleccionar, sea un jugador o simplemente tenga curiosidad acerca de esta tendencia digital emergente, Got Minted facilita comenzar con NFT al simplificar la configuración. Dirígete a https://gotminted.
com para empezar.

Universidad de la cadena de bloques

Blockchain University es un sitio web educativo que enseña a desarrolladores, gerentes y empresarios sobre el ecosistema blockchain. Ofrece servicios públicos y privados programas de capacitación, hackatones y eventos de demostración. Sus programas son pensamiento de diseño orientado a la solución y capacitación práctica experiencial. Puede encontrar Blockchain University en Mountain View, California, o en https://theblockchainu.
com y https://dlt.education.

Núcleo de Bitcoin

Bitcoin Core (https://bitcoin.org) fue utilizado originalmente por Satoshi Nakamoto para alojar su documento técnico sobre el protocolo Bitcoin. Es el hogar de material educativo sobre el protocolo central de Bitcoin y versiones descargables del software Bitcoin original.

El sitio está dedicado a mantener Bitcoin descentralizado y accesible para la persona promedio.


REMEMBER

Es un proyecto administrado por la comunidad, y no todo el contenido es administrado por el equipo central. Tenga esto en cuenta mientras examina el sitio.

Alianza de cadena de bloques

Blockchain Alliance fue fundada por la Cámara de Comercio Digital Blockchain y la organización de noticias Coincenter. Es una colaboración público-privada de la comunidad blockchain, las fuerzas del orden público y los reguladores. Comparten el objetivo común de hacer que el ecosistema de la cadena de bloques sea más seguro y promover un mayor desarrollo de la tecnología. Lo hacen combatiendo la actividad delictiva en la cadena de bloques al brindar educación, asistencia técnica y sesiones informativas periódicas sobre Bitcoin y otras monedas digitales y aquellas que utilizan la tecnología de la cadena de bloques.

Puede obtener más información sobre sus eventos o unirse a su organización en www.blockchainalliance.org.

Blog multicadena

Multichain es una empresa que ayuda a las organizaciones a crear rápidamente aplicaciones en cadenas de bloques. Ofrecen una plataforma que puede emitir millones de activos en una cuenta privada. blockchain y también puede rastrear y verificar la actividad en su red a través de sus herramientas. Más allá de su conjunto de herramientas y plataforma, han sido líderes de pensamiento en el espacio de blockchain.

Estas son mis publicaciones favoritas de su blog (www.multichain.com/blog):

- Cuatro casos de uso genuinos de blockchain (www.multichain.com/blog/2016/05/cuatro-genuinos-casos-de-uso-de-blockchain/)
- Cuidado con el contrato inteligente imposible (www.multichain.com/blog/2016/04/cuidado-contra-inteligente-imposible/)
- Contratos inteligentes y la implosión de DAO (www.multichain.com/blog/2016/06/smart-contrats-the-dao-implosion/)
- Comprender las cadenas de bloques de conocimiento cero (www.multichain.com/blog/2016/11/comprender-cero-conocimiento-blockchains/)

Mente de la colmena

Paul Sztorc fundó Truthcoin, un sistema oracle peer-to-peer y un mercado de predicción para Bitcoin. Utiliza una cadena lateral de prueba de trabajo que almacena datos sobre el estado de los mercados de predicción. Bitcoin puede soportar derivados financieros e inteligentes contratos a través de HiveMind, la plataforma desarrollada a partir del documento técnico de Truthcoin. Consulte sus recursos y materiales educativos en http://bitcoinhivemind.com.

herrero + corona

Smith + Crown es una organización de investigación de cadenas de bloques que se centra en las tendencias globales, la inteligencia de la industria y la estructura de los sistemas de cadenas de bloques. Han creado herramientas de investigación para expandir las empresas de blockchain. Smith + Crown busca impacto, aplicación y accesibilidad. Han puesto a disposición del público y de forma gratuita la mayor parte de su investigación. Puede aprovechar las herramientas de investigación, los innumerables informes y las bases de datos de todos los proyectos destacados en el espacio de la cadena de bloques. Smith + Crown son los investigadores y asesores de varios grupos destacados de defensa de las cadenas de bloques y las criptomonedas, como la Cámara de Comercio Digital, Token Alliance y Social Alpha. Échales un vistazo en https://www.smithandcrown.com.

Podcasts desencadenados y no confirmados

Los podcasts Unchained y Unconrmed son entrevistas sorprendentes y actualizadas con los mejores miembros de la industria en el espacio de la cadena de bloques y las criptomonedas. Unchained es un podcast semanal de una hora de duración de Laura Shin, ex editora sénior de Forbes y la primera reportera principal en cubrir los criptoactivos a tiempo completo. Shin hace impresionante e inmersiones profundas bien pensadas en las personas y empresas que construyen la Internet descentralizada. Ella puede ayudarlo a comprender mejor la regulación, problemas de seguridad y privacidad que son inherentes a la tecnología blockchain. Puedes escuchar su podcast en https://unchainedpodcast.com.

Aquí hay algunos buenos episodios para escuchar:

» Ledger sobre cómo los consumidores y las instituciones deberían proteger sus claves privadas: https://unchainedpodcast.com/ledger on-how-consumers-and-institutions-should-be-safeguarding their-private-keys-ep-101/

» Cómo la donación de criptomonedas puede ayudarlo a ahorrar en impuestos: https://unchainedpodcast.com/how-donating-crypto-can-help you-save-on-taxes-ep-94/

» Naval Ravikant sobre cómo Crypto está exprimiendo a los VC, obstaculizando a los reguladores y brindando opciones a los usuarios: https://unchainedpodcast.com/ naval-ravikant-on-how-crypto-is-squeezing-vcs-hindering regulators-and-bringing-users -elección/

» Cómo Binance se convirtió en el intercambio de criptomonedas más popular en 5 meses: https://unchainedpodcast.com/cómo-binance-se-convirtió-en-el-intercambio-criptográfico-más-popular-en-5-meses-ep-84/

EN ESTE CAPÍTULO

» Descubriendo sus vulnerabilidades legales

» Comprender las deficiencias técnicas de las cadenas de bloques

» Identificar los mejores puntos de ataque de los ladrones en sus sistemas

» Desarrollando sus mejores prácticas de seguridad

Capítulo 18

Diez reglas para nunca romper en la cadena de bloques

En este capítulo, profundizo en las cosas que debe tener en cuenta al trabajar con la tecnología blockchain y las criptomonedas que las ejecutan.

REMEMBER

Siempre consulte a su CPA y abogado antes de tomar decisiones financieras. Este la tecnología es nueva y las reglas que la gobiernan no están completamente desarrolladas.

No use criptomonedas o Blockchains para eludir la ley

La legalidad y la zonificación legal de las criptomonedas siguen fluctuando en muchos lugares del mundo. No estoy bromeando cuando le digo que hable con su CPA y su abogado. Será dinero bien gastado y lo mantendrá fuera de problemas.

Aquí hay tres preguntas muy tontas que me hacen aterradoramente a menudo:

» ¿ Puedo usar criptomonedas como una forma de ocultar dinero? Esta idea es peligrosa. Recuerde: las cadenas de bloques mantienen registros de todas las transacciones para siempre, por lo que incluso si cree que se le ocurrió una forma inteligente de ocultar algunos tokens, aquellos que buscan un mal comportamiento tienen tiempo para encontrarlo.

» ¿ Puedo usar blockchains como una forma de sacar dinero de contrabando de mi país? Muchos países tienen limitaciones sobre los fondos que los ciudadanos pueden sacar del país. No desea hacer esto por la misma razón que acabo de mencionar: las cadenas de bloques mantienen registros de todas las transacciones para siempre.

» ¿ Puedo usar criptomonedas para comprar productos ilícitos? La respuesta es: lo has adivinado. ¡que no! ¡Las cadenas de bloques mantienen un rastro de tus acciones para siempre! Incluso las fuerzas del orden que robaron Bitcoin del infame mercado de Silk Road fueron atrapadas.


REMEMBER

No haga nada con criptomonedas y cadenas de bloques que sería ilegal hacer con dinero real.

Mantenga sus contratos tan simples como sea posible

Organizaciones autónomas descentralizadas (DAO), contratos inteligentes y código de cadena están de moda en este momento. La promesa de recortar gastos administrativos y legales el costo es muy tentador para muchas corporaciones. Una característica que a veces se pasa por alto de esta tecnología es que es solo código. Eso significa que no hay ningún ser humano. interpretando las reglas que ha establecido para que todos las sigan. El código se convierte ley, y la ley solo se extiende a lo que está incorporado en el contrato de blockchain. La “grasa” que se cortó a veces puede ser muy importante.

No hay nadie para interpretar el código. Eso significa que si el código se ejecuta en un moda que no esperabas, tampoco hay nadie para hacer cumplir la intención de la contrato. El código es ley y no ocurrió nada ilegal. Es por eso que deberías mantenga sus contratos simples y de naturaleza modular para contener y predecir los resultados del cumplimiento del contrato. También es una buena idea hacer que su contrato sea probado y golpeado incluso por otros desarrolladores que están incentivados para romperlo.

El alcance de la cadena de bloques en la que está construyendo su proyecto también es importante. Puede Piense en ello como jurisdicciones. Claro, un contrato inteligente puede ejecutarse en datos externos, pero el contrato inteligente no puede exigir fondos de cuentas a las que no tienen acceso. Eso significa que todo el valor debe reservarse de alguna manera, lo que puede gravar el anacardo.

Otra cosa a tener en cuenta es la fuente de información que utiliza su contrato para ejecutarse. Si se trata de datos meteorológicos para un contrato de seguro, ¿confía y
de acuerdo con la fuente? ¿Es posible manipular los datos de origen? Se debe pensar mucho en la fuente de Oracle antes de la implementación. Al crear un contrato inteligente, tenga en cuenta que sus canales de datos pueden ser dinámicos. Por ejemplo, las API
se actualizan con frecuencia, y si su contrato llama a uno que ha cambiado, puede romper su contrato inteligente.

Publicar con gran precaución

El objetivo de las cadenas de bloques es que una vez que se ingresan los datos, es difícil sacarlos. Eso significa que lo que pongas estará presente durante mucho tiempo. si publicas
información confidencial encriptada, debe estar de acuerdo con el hecho de que los datos encriptados pueden romperse algún día y lo que publicó puede ser legible para
alguien.


TIP

Piensa en esto antes de publicar:

» ¿ Me sentiría cómodo con que esta información se descifre en algún momento?

» ¿ Me siento cómodo compartiendo esta información por toda la eternidad con cualquiera que quiere revisarlo?

» ¿ Son estos datos dañinos para un tercero y algo por lo que podría ser responsable si ¿publicado?

Se está trabajando en criptografía para hacer un cifrado de prueba cuántica, pero
Debido a que tanto la computación cuántica como el cifrado de prueba cuántica aún se encuentran en la fase de prueba, es difícil decir de qué será capaz la tecnología dentro de 20 años.
desde ahora.

Copia de seguridad, copia de seguridad, copia de seguridad

Tus claves privadas


REMEMBER

Las cadenas de bloques son criaturas muy implacables. No les importa si perdió sus claves privadas o contraseñas. Muchos nerds de las criptomonedas han quedado al descubierto y han entregado menos fichas a los grandes océanos de la cadena de bloques, un tesoro que nunca se recuperará.

Las claves privadas que controlan su criptomoneda a menudo viven dentro de sus billeteras, por lo que es importante protegerlos y asegurarlos. Tenga cuidado con los servicios en línea que almacenan su dinero por usted. Muchos intercambios de criptomonedas y billeteras en línea les han robado sus fondos. Además, tomar una captura de pantalla o una imagen y almacenarla en la nube es lo mismo que enviarse un correo electrónico. Hagas lo que hagas, no hacer esto. Comprometerá tus llaves. Debes hacer un plan para que tus seres queridos puede acceder a sus claves en caso de que algo le suceda. Un CEO sano de 30 años de un intercambio de criptomonedas murió y bloqueó $ 190 millones en activos porque no tenía un plan de sucesión. Además, no pase por alto la conectividad Bluetooth como una puerta oculta a su almacenamiento en frío. Asegúrese de que su dispositivo sea completamente inaccesible desde Internet.


TIP

Almacene solo pequeñas cantidades de tokens para uso diario en línea o en un dispositivo accesible por Internet. Piense en las billeteras de criptomonedas como su billetera en efectivo. No guarde más dinero del que está dispuesto a perder en un momento dado. Más de cien aplicaciones de malware conocidas buscan obtener sus claves privadas y robar sus tokens.

Mantenga el resto de su moneda en almacenamiento en frío: completamente en línea sin acceso a la Internet. Esto podría estar en una billetera de papel, en una computadora que no puede acceder al Internet, o en un dispositivo de hardware único construido para asegurar criptomonedas.

Si elige usar una billetera de papel para asegurar su criptomoneda, plastifíquela y haga copias. También tenga en cuenta que las impresoras a menudo tienen acceso a Internet y sus datos pueden ser recuperados por terceros. Los verdaderamente paranoicos solo usan impresoras que no tienen acceso a la web. Mantenga sus copias de billetera de papel en diferentes ubicaciones como la bóveda de un banco y un lugar seguro en su hogar.


REMEMBER

Haga una copia de seguridad de sus billeteras digitales y guárdelas en un lugar seguro. Una copia de seguridad es en caso de que su computadora falle, o si comete un error y elimina el error. La copia de seguridad se le permite recuperar su billetera en caso de que su dispositivo se dañe o sea robado. Además, no olvide cifrar su billetera. Cifrar su billetera le permite configurar un Contraseña para retirar tokens.


WARNING

El cifrado es una medida útil para protegerlo contra los ladrones, pero no puede proteger contra el software de registro de teclas. Utilice siempre una contraseña segura que contenga letras, números, signos de puntuación y que tenga al menos 16 caracteres. lo mas Las contraseñas seguras son aquellas generadas por programas diseñados específicamente para eso. objetivo. Las contraseñas seguras son más difíciles de recordar. Podría considerar escribir Anote su contraseña y plastificarla como sus claves privadas. hay limitado opciones de recuperación de contraseña dentro de la criptomoneda, y una contraseña olvidada podría significar tokens perdidos.

HERRAMIENTAS PARA MANTENER TUS TOKENS SEGUROS

Podría considerar usar la billetera BitGo para asegurar su Bitcoin. Aunque es una billetera en línea, BitGo requiere una firma en línea y en línea para mover sus tokens.
Debido a esta funcionalidad, es más seguro que su billetera en línea estándar.

Las billeteras BitGo usan tres claves. Ellos tienen uno, usted tiene uno y el otro lo tiene en su nombre un servicio de recuperación de claves (KRS) de terceros. Se requieren dos firmas en cada transacción. Por lo general, esto lo hacen BitGo y usted, a menos que pierda una de sus claves; en ese caso, el KRS ayudará. La billetera BitGo no es gratuita; requieren una pequeña tarifa por transacción.

Consulte la billetera BitGo en www.bitgo.com/wallet.

Verifique tres veces la dirección antes Moneda de envío

La criptomoneda ha atraído a una buena cantidad de sinvergüenzas, así que tenga cuidado cuando envíe dinero. Tan pronto como el dinero sale de su billetera, se va para siempre y no hay forma de recuperarlo. No hay contracargos y no puedes llamar
Atención al cliente. Tu dinero se ha ido.

Verifique tres veces la dirección de la billetera antes de enviar. Quieres asegurarte de que estás enviándolo a la dirección correcta. También verifique dos veces la dirección incluso si la copia y la pega. Existe un software malicioso que puede intercambiar sus direcciones por
Comandos Ctrl+C/Ctrl+V.

Tenga cuidado al usar intercambios

Los intercambios de criptomonedas son puntos centrales a los que los piratas informáticos les gusta apuntar para robar fichas Son vistos como ollas de oro maduras para ser cosechadas, y más de 150 de
ellos han sido comprometidos.

Tenga esto en cuenta al usar los intercambios y siga las mejores prácticas establecidas en este libro para mantener sus fichas seguras. Investigue un poco sobre el intercambio que está usando para ver qué medidas de seguridad tiene implementadas.

La autenticación de dos factores es fundamental. También puede considerar establecer un secreto frase con su proveedor de telecomunicaciones para ayudar a prevenir la ingeniería social. tu no quiere ser víctima de un cambio de tarjeta SIM. Su número de teléfono no tiene que ser tu copia de seguridad; Google y varias otras empresas también ofrecen una opción de autenticación de dos factores (consulte la aplicación Google Authenticator).

Finalmente, solo use los intercambios para mover sus fondos dentro y fuera. No uses el intercambio como un lugar para almacenar valor. En su lugar, mantenga cantidades significativas de criptomonedas en almacenamiento en frío o en una billetera de papel laminado con varias copias.

Cuidado con wifi

Si su enrutador no se configuró correctamente, es posible que alguien vea un registro de toda su actividad. Además, cuando está en un portal público o no seguro, también puede estar expuesto a malware. Debe asumir que el dueño de la red puede ver su actividad.

Solo use redes Wi-Fi confiables y asegúrese de haber cambiado la contraseña en su enrutador a algo tan seguro como una contraseña. La mayoría de las contraseñas de los enrutadores de Wi-Fi están configuradas con el valor predeterminado de fábrica de "admin" y un tercero puede tomarlas fácilmente. fiesta.

Identifique su desarrollador de Blockchain

La tecnología de cadena de bloques es nueva, y simplemente no hay muchas personas que tengan mucha experiencia en lo que respecta a la creación de aplicaciones de cadena de bloques.

Si está pensando en contratar a un desarrollador para que lo ayude con un proyecto, consulte su GitHub y vea qué trabajo ha hecho antes de comenzar. Es posible que no necesite tener experiencia con blockchain específicamente, pero si no la tiene, debería ser una desarrollador muy experimentado fuera del mundo blockchain.

Todavía no existen muchos recursos para ayudar a los desarrolladores cuando se atascan. Los desarrolladores sin experiencia pueden tener dificultades y, en este punto, la mayoría no tienen experiencia. y llevará más tiempo desarrollar su aplicación.

No te dejes engañar

La industria blockchain en su conjunto no cuenta con las mismas medidas de protección y seguridad que tienen los bancos y otras instituciones financieras, y no existen las mismas leyes para su protección y bienestar económico. no hay consumidor protección y sin seguro bancario FDIC de fondos del gobierno. Si te roban o te estafan, es posible que no puedas pedir ayuda a nadie.

Además, la industria ha tenido mucha publicidad en los últimos años sin mucha entrega de cosas de valor real. En el año 2016, más de mil nuevas empresas de blockchain surgieron de la noche a la mañana reclamando experiencia. Cuando buscas desarrollar un proyecto y tratando de decidir si vale la pena la inversión, siempre es una buena idea tomarse un minuto y asegurarse de que tenga sentido. Pregúntate a ti mismo las siguientes preguntas:

- ¿ Se genera valor real?
- ¿ Se crea valor de la manera que lo bene cia a usted?
- ¿ Por qué no se ha hecho ya?
- ¿ Existen otras tecnologías más probadas que podrían usarse para lograr lo mismo con la misma eficiencia o mejor?

La tecnología Blockchain es muy prometedora y poderosa y, como tal, debe abordarse con cuidado y consideración.

No intercambie tokens a menos que usted Sepa lo que está haciendo

Las criptomonedas son muy volátiles y su valor variará enormemente en un momento dado y, a veces, sin una razón aparente. Muchas de las criptomonedas tienen poca profundidad y el comercio de grandes cantidades puede colapsar el valor de mercado. Trabajar con cadenas de bloques públicas significa que probablemente necesitará tener cierta cantidad de la moneda para utilizarlas.

No se deje atrapar por el comercio de tokens a menos que se tome el tiempo para comprender bien el mercado. Una buena regla general es que si nunca antes ha negociado con activos tradicionales como acciones, asegúrese de tomarse un tiempo adicional para comprender las criptomonedas. Tú necesita sumergirse tan profundamente en él como lo haría para aprender sobre el mercado de valores antes de comenzar. Considere leer Cryptocurrency Investing For Dummies de Kiana Danial (Wiley). Si elige intercambiar tokens y criptomonedas,
no olvides reportar esta actividad a tu contador. Es posible que deba informar su ganancias o pérdidas en su declaración de impuestos.

EN ESTE CAPÍTULO

» Sumergirse en nuevos mundos de metaversos

» Descubriendo entornos educativos virtuales inmersivos

» Descubriendo nuevas compras virtuales centros comerciales

Capítulo 19

Los diez mejores metaversos Proyectos

Están surgiendo nuevos proyectos de metaverso que se basan en la tecnología blockchain. ing todos los días. Los empresarios han visto oportunidades para capitalizar las herramientas muy poderosas que ofrecen las cadenas de bloques para mover dinero más rápido y de manera segura. sistemas informáticos y construir identidades digitales. Han combinado estas tecnologías con entornos 3D inmersivos que te permiten explorar y crear mundos completamente nuevos.

En este capítulo, les presento algunos de mis proyectos de metaverso favoritos que incorpore economía de fichas divertidas, como ganar para jugar y votar. También descubre el mundo de la educación virtual y los centros comerciales.

Después de leer este capítulo, tendrá una idea de algunas de las cosas asombrosas sucediendo dentro del metaverso y sepa exactamente dónde comenzar su próximo proyecto. ¡Incluso puedes hacer nuevos amigos en línea en uno de estos mundos virtuales!

Decentraland

Decentraland es una plataforma descentralizada de realidad virtual (VR) que permite a los usuarios controlar completamente sus experiencias. Está alimentado por tokens no fungibles (NFT), que permitir a los usuarios acceder y comercializar activos digitales únicos que se pueden personalizar para satisfacer sus necesidades.

En Decentraland, los usuarios pueden crear, experimentar y monetizar su propio contenido. La plataforma se divide en parcelas denominadas LAND, que son digitales 3D no fungibles activos que se mantienen a través de un contrato inteligente de Ethereum. Estos paquetes son identificados por sus coordenadas (x, y) y son propiedad de miembros del ecosistema terrestre Decentra.

La propiedad de estas propiedades virtuales se asegura mediante el uso del token de criptomoneda MANA, que brinda a los usuarios control total sobre su LAND de la misma manera que un título sería para una propiedad física. Decentraland permite a los usuarios explorar una variedad de mundos virtuales y escenas creadas por artistas en diferentes parcelas de LAND. Si eres Si está interesado en explorar Decentraland, puede navegar a https://decentraland. org para comenzar su viaje.

el arenero

Sandbox es un mundo virtual que permite a los jugadores construir y monetizar sus experiencias de juego mediante el uso de NFT en la cadena de bloques de Ethereum. Es compuesto por tres productos integrados:

» VoxEdit, un software de creación de NFT y modelado 3D que permite a los usuarios crear y animar objetos 3D

» El Marketplace, donde los usuarios pueden cargar, publicar y vender su NFT creaciones

» Game Maker, que permite a los usuarios crear juegos en 3D sin necesidad de programar herramientas de secuencias de comandos visuales

Sandbox utiliza varios tipos de tokens para facilitar las transacciones y las interacciones dentro de la plataforma. SAND es el token ERC-20 utilizado como base para todos transacciones e interacciones dentro del Sandbox. LAND es un NFT único que representa una propiedad digital en el metaverso Sandbox que los jugadores pueden comprar para construir experiencias interactivas. Los ACTIVOS son NFT creados por jugadores que pueden ser comercializados en el mercado y utilizados como elementos de creación en Game Maker. Ellos utilizar el estándar ERC-1155.

Sandbox se basa en la cadena de bloques de Ethereum y utiliza contratos inteligentes para proporcionar propiedad de derechos de autor para el contenido generado por el usuario. Su objetivo es interrumpir a los creadores de juegos existentes como Minecraft y Roblox al proporcionar a los creadores la propiedad y el control total de sus creaciones y recompensarlos por su participación en el ecosistema. The Sandbox cuenta con una gran comunidad de creadores, habiendo generado 40 millones de descargas en iOS y Android con sus dos éxitos móviles, The Sand box (2011) y The Sandbox Evolution (2016). Puedes empezar a hacer el tuyo juegos navegando a www.sandbox.game.

Axie Infinito

Axie Innity es un mundo virtual nuevo y divertido lleno de fuerzas y mascotas adorables llamadas Axies. El modo de juego es similar al popular juego móvil Pokémon Go. En este emocionante nuevo panorama digital, puedes luchar contra tus Axies contra otros jugadores, aprovechando sus habilidades únicas. También ganas criptomonedas a través de tu juego.

Si está listo para una experiencia de juego verdaderamente inmersiva que combina blockchain tecnología con lindos avatares en un mundo virtual dinámico, salte en línea y descargue Axie Innity en https://axieinfinity.com.

metacalle

MetaStreet es un protocolo de tasa de interés descentralizado para el metaverso. Fue construido aumentar el producto interno bruto (PIB) de las economías virtuales emergentes dentro el metaverso. El protocolo MainStreet hace esto a través de una variedad de algoritmos bóvedas de capital que generan rendimiento diversificado a través de suscripción automática, agregación y la ejecución de notas respaldadas por NFT.

En la danza descentralizada (DeFi), puede pensar en las bóvedas como grupos de fondos con un estrategia asociada para maximizar la rentabilidad de sus inversores. la bóveda de capital permite la liquidez del mercado secundario para las notas respaldadas por NFT. La liquidez es importante en la creación de estabilidad del mercado. Las bóvedas se están volviendo atractivas para los inversores porque pueden obtener rendimiento invirtiendo capital en carteras diversificadas de activos respaldados por NFT. notas

MetaStreet también ofrece educación a los inversionistas para ayudarlos a aprender cómo invertir en estos nuevos tipos de nuevos activos. Puede descubrir más sobre MetaStreet navegando a https:// metastreet.xyz.

Moneda Enjin

Enjin ha tenido sus altibajos con la burbuja NFT de 2022. Construyó un multiverso de actividades digitales como los juegos impulsados por Enjin que le permiten ganar NFT. También permite a los usuarios intercambiar NFT y crear juegos basados en NFT.

Enjin es también la primera empresa NFT en ser aceptada en el Pacto Mundial de la ONU Afiliación. El Pacto Mundial obliga a las empresas a alinear sus negocios modelos con los diez principios derivados de las declaraciones de la ONU sobre derechos humanos, trabajo, medio ambiente y lucha contra la corrupción.

Enjin también ha creado JumpNet, un puente de cadena de bloques que le permite afirmar ser un sistema blockchain de carbono negativo. JumpNet también permite que Enjin elimine las tarifas de gas para sus usuarios y reduzca el costo de ejecutar sus contratos inteligentes NFT. no puedes salir más en https://enjin.io.

Metahéroe

Metahero es una plataforma que te permite crear avatares 3D realistas y objetos virtuales para juegos, plataformas de realidad virtual, redes sociales y moda. Combina tecnología 3D con un mercado y un ecosistema de fichas. Metahero también está convirtiendo arte del mundo real en NFT de ultra alta definición, preservando permanentemente el arte en formato digital. forma. Wolf Studio, líder mundial en escaneo 3D, apoya estos esfuerzos.

El token Metahero, HERO, se puede comprar con Binance Coin (BNB) en intercambios descentralizados. Metahero se ejecuta sobre la cadena inteligente Binance, un paralelo cadena inteligente que ejecuta contratos inteligentes en Binance Exchange.

Curiosamente, el token HERO es un activo deductivo. La oferta circulante total se reduce quemando hasta un 2 por ciento de cada transacción. La quema es cuando los tokens se envían a una billetera sin clave privada, destruyéndolos para siempre.

Puede comenzar a crear su metamundo navegando a https://metahero.io.

atlas estelar

Star Atlas es un juego de rol inmersivo con temática espacial. Utiliza tiempo real tecnología gráfica en Unreal Engine 5. Permite a Star Atlas tener imágenes de videojuegos de calidad cinematográfica.

Star Atlas también ha integrado la tecnología blockchain utilizando el protocolo Solana. Él afirma ejecutarse en una infraestructura en gran parte sin servidor. Utilizando el subidón de Solana el rendimiento de 50,000 transacciones por segundo permite interacciones de juego entre activos que se registrarán en tiempo real y evita la necesidad de un backend de servidor tradicional robusto para juegos multijugador en línea.

Start Atlas también incorpora NFT obtenidos e intercambiados dentro del juego. Su economía imita la tangibilidad de los activos y la propiedad del mundo real. Si te gustan los juegos de rol y quieres ganar para jugar, puedes comenzar navegando a https://staratlas.com.

Bloktopía

El Bloktopia Metaverse es un rascacielos virtual de 21 niveles que fue desarrollado en el Motor de unidad. Los 21 niveles simbolizan los 21 millones de Bitcoin que se acuñarán. Bloktopia tiene mucho material educativo y te permite ponerte al día rápidamente. velocidad en nueva información sobre criptomonedas y NFT.

Los expertos de la industria contribuyen con materiales educativos sobre modelos de ingresos, jugando juegos con amigos, construir redes y aprovechar otras formas de obtener comenzó en el metaverso.

Bloktopia permite que los proyectos criptográficos, los intercambios y los influenciadores muestren sus contenido. El rascacielos virtual incluye más de 200 tiendas virtuales, un auditorio para charlas y seminarios en vivo, un salón de juegos y espacios para eventos virtuales.

Puede desbloquear múltiples flujos de ingresos pasivos y activos, acceder a educación y herramientas de aprendizaje sobre criptografía, y participe en eventos y reuniones virtuales dentro de este lugar virtual. Para explorar este nuevo espacio, navegue a www. bloktopia.com.

Calle

El mundo de Highstreet es un metaverso de mundo abierto de jugar y ganar. incorpora compras, juegos y NFT. El juego ha sido capaz de atraer a los tradicionales y nuevas marcas criptográficas para ayudar a respaldar su juego de rol en línea multijugador masivo (MMORPG).

Puedes jugar para ganar completando misiones, asistiendo a eventos sociales, socializando con jugadores y comprando NFT de marcas del mundo real. Esto agrega un elemento divertido para que no se sienta solo como un centro comercial virtual para activos digitales.

Highstreet también incorpora el token HIGH, un token nativo de utilidad y gobernanza para el juego Highstreet. Se requieren fichas ALTAS para acceder a algunas áreas del juego y algunos eventos especiales. Los tokens HIGH también se pueden usar para comprar bienes raíces y productos virtuales en Highstreet Marketplace. Los poseedores de tokens HIGH también votan sobre las propuestas de gobernanza para determinar las características futuras de Highstreet, con el peso de la votación calculado en proporción a la cantidad de tokens que ha apostado.

Si está interesado en los juegos de rol, consulte Highstreet navegando a www.highstreet.market.

vóxeles

Voxels es una plataforma de metaverso basada en Ethereum. El mundo virtual de Voxels incluye infraestructura de la vida real, como carreteras, terrenos y edificios. Al igual que muchos otros juegos criptográficos del metaverso, puedes comprar terrenos virtuales, construir sobre ellos, personalizar tu avatar con NFT portátiles y explorar el mundo abierto.

Voxels es uno de los mundos virtuales más accesibles para comenzar y construir. Puede comenzar a construir arrastrando y soltando bloques en tiempo real. No necesita equipo o software especial, solo su navegador web favorito.

La ciudad central de Voxels se llama Origin City, y es donde comienzas a jugar. El mapa original de Origin City comprendía 3.026 parcelas de tierra adquiribles en una amplia gama de formas y tamaños. Ahora el juego incluye expansión e islas.

Si está listo para comenzar, puede ingresar a Origin City ahora mismo navegando a www.voxels.com/play.

Índice

C

F

j

k

L

METRO

O

Sobre el Autor

Tiana Laurence es autora, inversora, tecnóloga y docente. Le apasiona garantizar que las mujeres tengan voz en el futuro de la tecnología. Tiana cofundó la primera empresa de cadena de bloques empresarial que creó software de integridad de datos para el Departamento de Seguridad Nacional y software de identidad para la Fundación Gates. Ha disertado en el Instituto Nacional de Ciencia y Tecnología,
la Reserva Federal, el Foro Económico Mundial y numerosos bancos, compañías de seguros empresas y empresas Fortune 500 sobre el impacto de la tecnología blockchain, la moneda digital del Banco Central (CBDC), las innovaciones de marketing Web 3.0 y
activos tokenizados. También es autora de NFTs For Dummies (Wiley) e Introducción a la tecnología Blockchain (Van Haren Publishing), que se utiliza en Europa para
Certificación de blockchain. Tiana también enseña ntech en la Universidad de Santa Clara. Tiana también es colaboradora frecuente de Forbes. Puedes seguirla en Twitter en @laurencetiana.

Dedicación

Este es para mis hermanas. Gracias por todo el apoyo y los animos que
me dio mientras escribía este libro.

Agradecimientos del autor

Este libro es el producto de las ideas y el trabajo de muchas personas. no hubiera sido posible sin el mundo abierto y solidario de la cadena de bloques y las criptomonedas.
Me gustaría agradecer específicamente a Scott Robinson, John Pigott, Ryan Fugger, Charley Cooper, Alyse Killeen, Jeremy Kandah, Clemens Wan, Greg Wallace, Tom Bollich,
y Brian Behlendorf por la dirección y orientación en la cadena de bloques en evolución espacio y por tomarse el tiempo de sus ocupadas vidas para revisar y controlar mi cordura trabajar.

Este libro también requirió mucha edición. No estoy bromeando, realmente tomó mucho edición. Mi editora de proyectos, Elizabeth Kuball, hizo un gran trabajo manteniéndome concentrado en la tarea y a tiempo, y Steve Hayes, mi editor ejecutivo, hizo posible todo el libro.
También me gustaría agradecer a Danny Yang por su exhaustiva revisión técnica y su excelente sugerencias y todas las demás personas detrás de escena, que hicieron trabajos ingratos para traer este libro. Estoy para siempre en deuda con ellos.

Agradecimientos del editor

Editor ejecutivo: Steve Hayes
Editora de desarrollo: Elizabeth Kuball
Editora de estilo: Elizabeth Kuball
Editor técnico: Danny Yang
Editor de producción: Mohammed Zafar Ali
Imagen de portada: © phive/Shutterstock

Aprovechar el poder

Dummies es el líder mundial en la categoría de referencia y una de las marcas más confiables y respetadas del mundo. Ya no solo se enfocan en los libros, los clientes ahora tienen acceso al contenido ficticio que necesitan en el formato que desean. Juntos crearemos una solución que atraiga a sus clientes, se destaque de la competencia y lo ayude a cumplir sus objetivos.

Publicidad y patrocinios

Conéctese con una audiencia comprometida en un poderoso sitio multimedia y posicione su mensaje junto con contenido instructivo experto.

Dummies.com es una ventanilla única para obtener información y conocimientos gratuitos en línea seleccionados por un equipo de expertos. •

Anuncios dirigidos • Video • Marketing por correo electrónico • Micrositios • Patrocinio de sorteos

20 MILLÓN
VISTAS DE PÁGINA
CADA MES

15 MILLÓN ÚNICO
VISITANTES POR MES

43%
DE TODOS LOS VISITANTES
ACCEDER AL SITIO
A TRAVÉS DE SUS DISPOSITIVOS MÓVILES

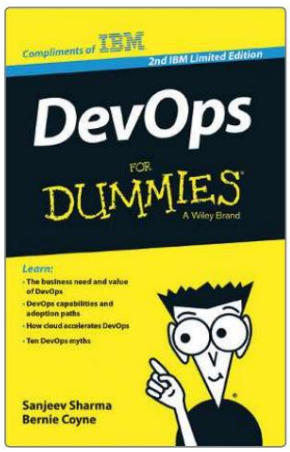
700,000 BOLETIN INFORMATIVO SUSCRIPCIONES
A LOS BUZONES DE
300.000 ÚNICOS PARTICULARES CADA SEMANA

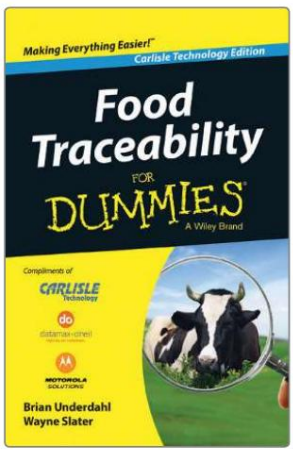
de tontos

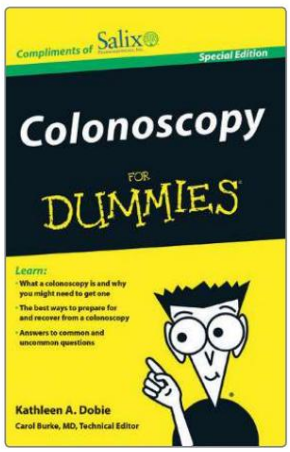
Publicación personalizada

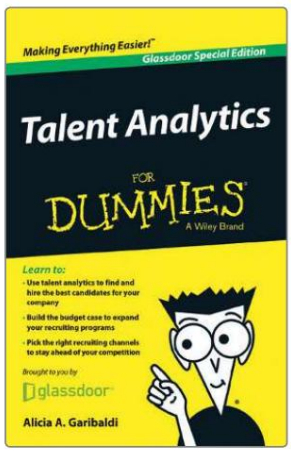
Reach a global audience in any language by creating a solution that will differentiate de la competencia, amplifique su mensaje y anime a los clientes a tomar una decisión de compra.

- Aplicaciones
- Libros
- libros electrónicos
- Vídeo
- Audio
- Seminarios web









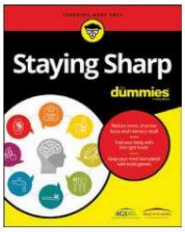
Licencias de marca y contenido

Aproveche la fortaleza de la marca de referencia más popular del mundo para llegar a nuevas audiencias y canales de distribución.

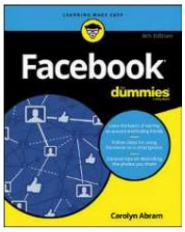
Para obtener más información, visite dummies.com/biz

dummies
A Wiley Brand

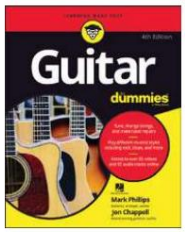
ENRIQUECIMIENTO PERSONAL



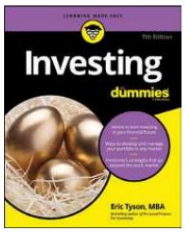
9781119187790 EE.
UU. $ 26,00
CAN $ 31,99
Reino Unido £ 19,99



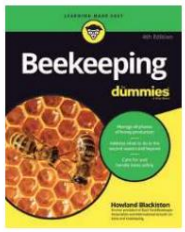
9781119179030 EE.
UU. $ 21,99
CAN $ 25,99
Reino Unido £ 16,99



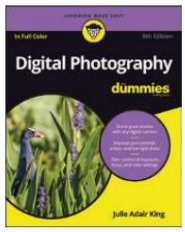
9781119293354 EE.
UU. $ 24,99
CAN $ 29,99
Reino Unido £ 17,99



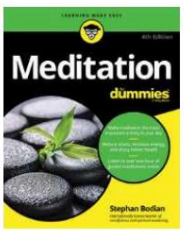
9781119293347 EE.
UU. $ 22,99
CAN $ 27,99
Reino Unido £ 16,99



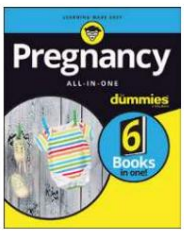
9781119310068 EE.
UU. $ 22,99
CAN $ 27,99
Reino Unido £ 16,99



9781119235606 EE.
UU. $ 24,99
CAN $ 29,99
Reino Unido £ 17,99

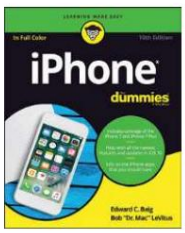


9781119251163 EE.
UU. $ 24,99
CAN $ 29,99
Reino Unido £ 17,99

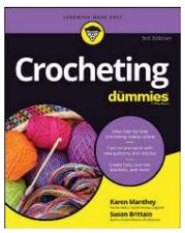


9781119235491 EE.
UU. $ 26,99
CAN $ 31,99
Reino Unido £ 19,99

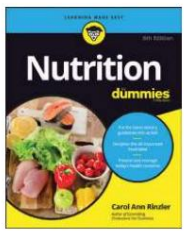
9781119279952 EE.
UU. $ 24,99
CAN $ 29,99
Reino Unido £ 17,99



9781119283133 EE.
UU. $ 24,99
CAN $ 29,99
Reino Unido £ 17,99

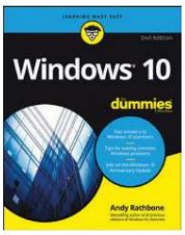


9781119287117 EE.
UU. $ 24,99
CAN $ 29,99
Reino Unido £ 16,99

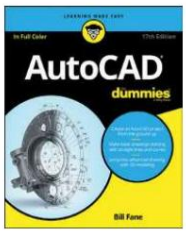


9781119130246 EE.
UU. $ 22,99
CAN $ 27,99
Reino Unido £ 16,99

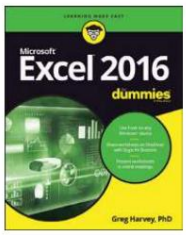
DESARROLLO PROFESIONAL



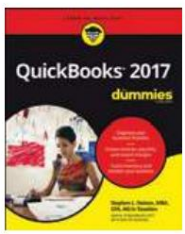
9781119311041 EE.
UU. $ 24,99
CAN $ 29,99
Reino Unido £ 17,99



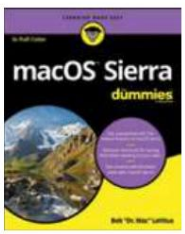
9781119255796 EE.
UU. $ 39,99
CAN $ 47,99
Reino Unido £ 27,99



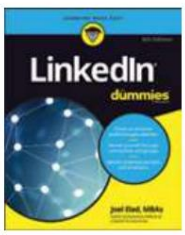
9781119293439 EE.
UU. $ 26,99
CAN $ 31,99
Reino Unido £ 19,99



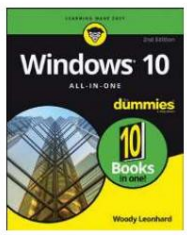
9781119281467 EE.
UU. $ 26,99
CAN $ 31,99
Reino Unido £ 19,99



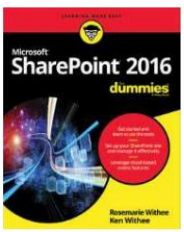
9781119280651 EE.
UU. $ 29,99
CAN $ 35,99
Reino Unido £ 21,99



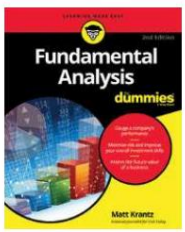
9781119251132 EE.
UU. $ 24,99
CAN $ 29,99
Reino Unido £ 17,99



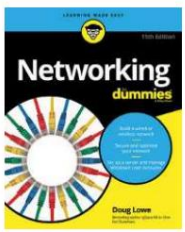
9781119310563 EE.
UU. $ 34,00
CAN $ 41,99
Reino Unido £ 24,99



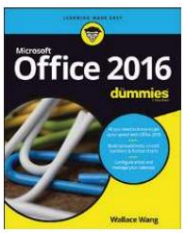
9781119181705 EE.
UU. $ 29,99
CAN $ 35,99
Reino Unido £ 21,99



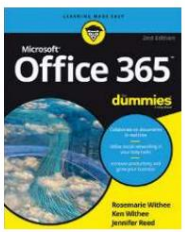
9781119263593 EE.
UU. $ 26,99
CAN $ 31,99
Reino Unido £ 19,99



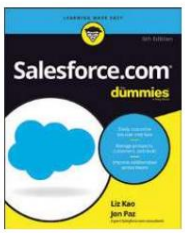
9781119257769 EE.
UU. $ 29,99
CAN $ 35,99
Reino Unido £ 21,99



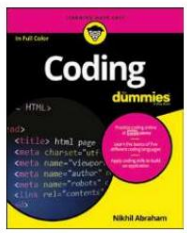
9781119293477 EE.
UU. $ 26,99
CAN $ 31,99
Reino Unido £ 19,99



9781119265313 EE.
UU. $ 24,99
CAN $ 29,99
Reino Unido £ 17,99



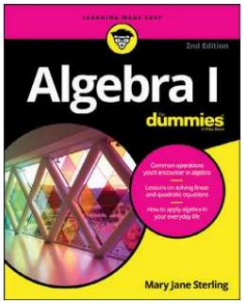
9781119239314 EE.
UU. $ 29,99
CAN $ 35,99
Reino Unido £ 21,99



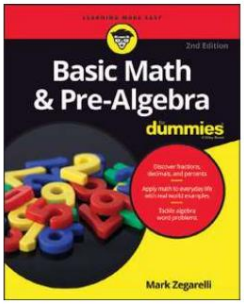
9781119293323 EE.
UU. $ 29,99
CAN $ 35,99
Reino Unido £ 21,99

Aprendizaje fácil

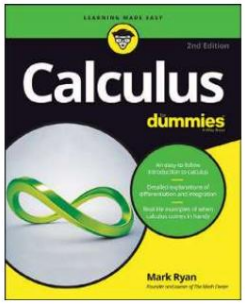
ACADÉMICO



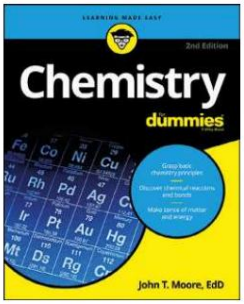
9781119293576 EE.
UU. $ 19,99
CAN $ 23,99
Reino Unido £ 15,99



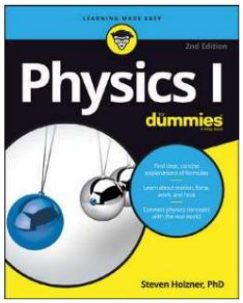
9781119293637 EE.
UU. $ 19,99
CAN $ 23,99
Reino Unido £ 15,99



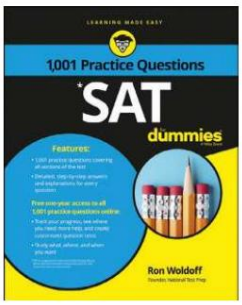
9781119293491 EE.
UU. $ 19,99
CAN $ 23,99
Reino Unido £ 15,99



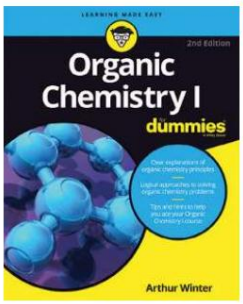
9781119293460 EE.
UU. $ 19,99
CAN $ 23,99
Reino Unido £ 15,99



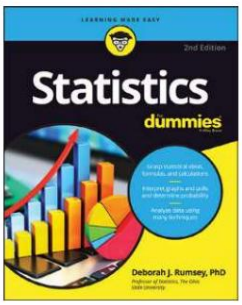
9781119293590 EE.
UU. $ 19,99
CAN $ 23,99
Reino Unido £ 15,99



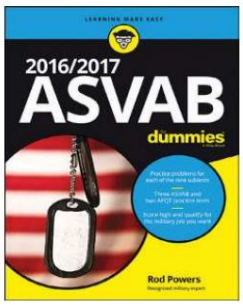
9781119215844 EE.
UU. $ 26,99
CAN $ 31,99
Reino Unido £ 19,99



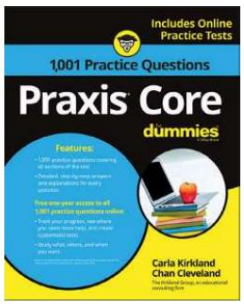
9781119293378 EE.
UU. $ 22,99
CAN $ 27,99
Reino Unido £ 16,99



9781119293521 EE.
UU. $ 19,99
CAN $ 23,99
Reino Unido £ 15,99



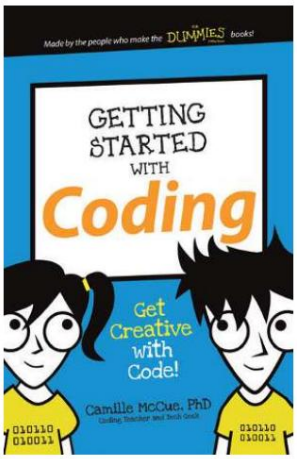
9781119239178 EE.
UU. $ 18,99
CAN $ 22,99
Reino Unido £ 14,99



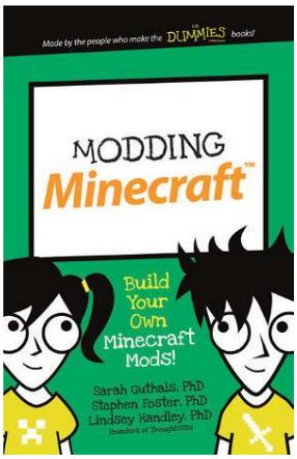
9781119263883 EE.
UU. $ 26,99
CAN $ 31,99
Reino Unido £ 19,99

Disponible en todos los lugares donde se venden libros

Pequeños libros para grandes imaginaciones.

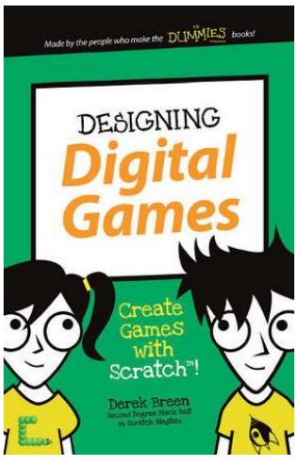


9781119177173 EE.
UU. $ 9,99
CAN $ 9,99
Reino Unido £ 8,99

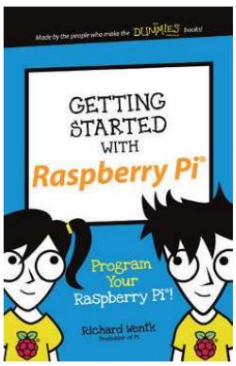


9781119177272 EE.
UU. $ 9,99
CAN $ 9,99
Reino Unido £ 8,99

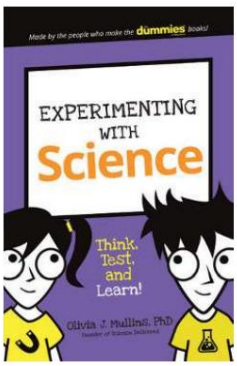
9781119177241 EE.
UU. $ 9,99
CAN $ 9,99
Reino Unido £ 8,99



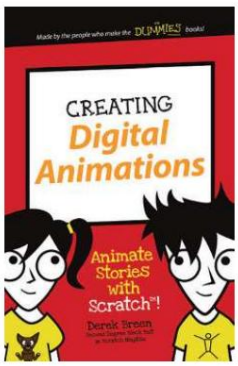
9781119177210 EE.
UU. $ 9,99
CAN $ 9,99
Reino Unido £ 8,99



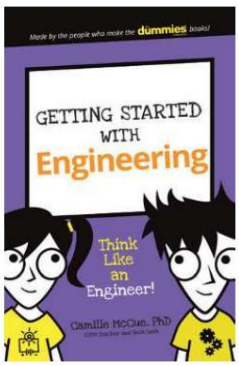
9781119262657 EE.
UU. $ 9,99
CAN $ 9,99
Reino Unido £ 6,99



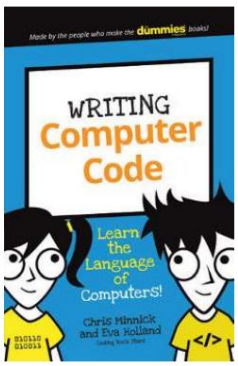
9781119291336 EE.
UU. $ 9,99
CAN $ 9,99
Reino Unido £ 6,99



9781119233527 EE.
UU. $ 9,99
CAN $ 9,99
Reino Unido £ 6,99



9781119291220 EE.
UU. $ 9,99
CAN $ 9,99
Reino Unido £ 6,99



9781119177302 EE.
UU. $ 9,99
CAN $ 9,99
Reino Unido £ 8,99

Dé rienda suelta a su creatividad

maniquíes.com

dummies
A Wiley Brand

ACUERDO DE LICENCIA DE USUARIO FINAL DE WILEY