¿Qué es Ethereum?

Ethereum es una plataforma de bloqueo abierto que permite a cualquier persona construir y usar aplicaciones descentralizadas que funcionan con tecnología de bloques. Como Bitcoin, nadie controla o es dueño de Ethereum - es un proyecto de código abierto construido por muchas personas alrededor del mundo. Pero a diferencia del protocolo Bitcoin, Ethereum fue diseñado para ser adaptable y flexible. Es fácil crear nuevas aplicaciones en la plataforma Ethereum, y con el lanzamiento de Homestead, ahora es seguro para cualquiera usar esas aplicaciones.

Un bloque de próxima generación

La tecnología Blockchain es la base tecnológica de Bitcoin, descrita por primera vez por su misterioso autor, Satoshi Nakamoto, en su documento "Bitcoin: un sistema de dinero electrónico punto a punto", publicado en 2008. Si bien el uso de bloqueos para usos más generales ya era Discutido en el documento original, no fue sino hasta unos pocos años más tarde que la tecnología blockchain surgió como un término genérico. Una cadena de bloques es una arquitectura de computación distribuida donde cada nodo de red ejecuta y registra las mismas transacciones, que se agrupan en bloques. Sólo se puede agregar un bloque a la vez, y cada bloque contiene una prueba matemática que verifica que se sigue en secuencia desde el bloque anterior. De esta manera, la "base de datos distribuida" de la cadena de bloques se mantiene consensuada en toda la red. Las interacciones individuales del usuario con el libro mayor (transacciones) están aseguradas por una fuerte criptografía. Los nodos que mantienen y verifican la red están incentivados por incentivos económicos aplicados matemáticamente codificados en el protocolo.

En el caso de Bitcoin, la base de datos distribuida se concibe como una tabla de saldos de cuenta, un libro mayor y las transacciones son transferencias del token bitcoin para facilitar la fEn el caso de Bitcoin, la base de datos distribuida se concibe como una tabla de saldos de cuenta, un libro mayor y las transacciones son transferencias del token bitcoin para facilitar la financiación sin confianza entre individuos. Pero a medida que bitcoin comenzó a atraer mayor atención por parte de desarrolladores y tecnólogos, nuevos proyectos comenzaron a usar la red bitcoin para propósitos diferentes a las transferencias de fichas de valor. Muchos de estos tomaron la forma de "monedas alt" - bloques separados con cryptocurrencies propios que mejoraron en el protocolo bitcoin original para agregar nuevas características o capacidades. A finales de 2013, el inventor de Ethereum Vitalik Buterin propuso que una sola cadena de bloques con la capacidad de reprogramarse para realizar cualquier computación arbitrariamente compleja podría subsumir estos muchos otros proyectos.inanciación sin confianza entre individuos. Pero a medida que bitcoin comenzó a atraer mayor atención por parte de desarrolladores y tecnólogos, nuevos proyectos comenzaron a usar la red bitcoin para propósitos diferentes a las transferencias de fichas de valor. Muchos de estos tomaron la forma de "monedas alt" - bloques separados con cryptocurrencies propios que mejoraron en el protocolo bitcoin original para agregar nuevas características o capacidades. A finales de 2013, el inventor de Ethereum Vitalik Buterin propuso que una sola cadena de bloques con la capacidad de reprogramarse para realizar cualquier computación arbitrariamente compleja podría subsumir estos muchos otros proyectos.

En 2014, los fundadores de Ethereum Vitalik Buterin, Gavin Wood y Jeffrey Wilcke comenzaron a trabajar en una cadena de bloques de nueva generación que tenía la ambición de implementar una plataforma de contrato inteligente general, totalmente confiable.

Máquina Virtual Ethereum

Ethereum es una cadena bloqueable programable. En lugar de dar a los usuarios un conjunto de operaciones predefinidas (por ejemplo, transacciones bitcoin), Ethereum permite a los usuarios crear sus propias operaciones de cualquier complejidad que deseen. De esta manera, sirve como una plataforma para muchos tipos diferentes de aplicaciones de bloques de bloques descentralizados, incluyendo, pero sin limitarse a, criptocurrencias.

Ethereum en sentido estricto se refiere a una serie de protocolos que definen una plataforma para aplicaciones descentralizadas. En el centro de ella está la Máquina Virtual Ethereum ("EVM"), que puede ejecutar código de complejidad algorítmica arbitraria. En términos de informática, Ethereum es "Turing completo". Los desarrolladores pueden crear aplicaciones que se ejecutan en el EVM utilizando lenguajes de programación amigables modelados en lenguajes existentes como JavaScript y Python.

Como cualquier cadena de bloques, Ethereum también incluye un protocolo de red peer-to-peer. La base de datos de bloques Ethereum es mantenida y actualizada por muchos nodos conectados a la red. Cada nodo de la red ejecuta el EVM y ejecuta las mismas instrucciones. Por esta razón, Ethereum se describe a veces evocador como una "computadora del mundo".

Esta paralelización masiva de la computación en toda la red de Ethereum no se hace para hacer la computación más eficiente. De hecho, este proceso hace que la computación sobre Ethereum sea mucho más lenta y costosa que en una "computadora" tradicional. Más bien, cada nodo Ethereum ejecuta el EVM con el fin de mantener el consenso a través de la cadena de bloques. El consenso descentralizado otorga a Ethereum niveles extremos de tolerancia a fallos, garantiza un tiempo de inactividad cero y hace que los datos almacenados en la cadena de bloques permanezcan inalterables y resistentes a la censura.

La propia plataforma de Ethereum no tiene rasgos ni valor. De forma similar a los lenguajes de programación, corresponde a los empresarios y desarrolladores decidir para qué se debe utilizar. Sin embargo, es claro que ciertos tipos de aplicaciones se benefician más que otros de las capacidades de Ethereum. Específicamente, ethereum es adecuado para aplicaciones que automatizan la interacción directa entre pares o facilitan la acción de grupo coordinada a través de una red. Por ejemplo, las aplicaciones para la coordinación de mercados peer-to-peer, o la automatización de contratos financieros complejos. Bitcoin permite que las personas intercambien dinero en efectivo sin involucrar a intermediarios como instituciones financieras, bancos o gobiernos. El impacto de Ethereum puede ser más profundo. En teoría, las interacciones financieras o los intercambios de cualquier complejidad podrían llevarse a cabo de forma automática y confiable utilizando el código que se ejecuta en Ethereum. Más allá de las aplicaciones financieras, cualquier entorno en el que la confianza, la seguridad y la permanencia sean importantes -por ejemplo, los registros de activos, las votaciones, la gobernanza y la Internet de las cosas- podría ser impactado masivamente por la plataforma Ethereum.

¿Cómo funciona Ethereum?

Ethereum incorpora muchas características y tecnologías que serán familiares para los usuarios de Bitcoin, al mismo tiempo que introducirá muchas modificaciones e innovaciones propias.

Mientras que la cadena de bloques Bitcoin era puramente una lista de transacciones, la unidad básica de Ethereum es la cuenta. La cadena de bloques Ethereum rastrea el estado de cada cuenta y todas las transiciones de estado en la cadena de bloques Ethereum son transferencias de valor e información entre cuentas. Hay dos tipos de cuentas:

* Cuentas de propiedad externa (EOA), que están controladas por claves privadas
* Cuentas de Contrato, que están controladas por su código de contrato y sólo pueden ser "activadas" por un EOA

Para la mayoría de los usuarios, la diferencia básica entre estos es que los usuarios humanos controlan los EOAs, ya que pueden controlar las claves privadas que dan control sobre un EOA. Las cuentas de contrato, por otra parte, se rigen por su código interno. Si son "controlados" por un usuario humano, es porque están programados para ser controlados por un EOA con una determinada dirección, que a su vez es controlada por quien posee las claves privadas que controlan ese EOA. El término popular "contratos inteligentes" se refiere al código en una cuenta de contrato - programas que se ejecutan cuando se envía una transacción a esa cuenta. Los usuarios pueden crear nuevos contratos implementando código en la cadena de bloqueo.

Las cuentas de contrato sólo realizan una operación cuando una EOA lo instruye. Por lo tanto, no es posible que una cuenta de Contrato ejecute operaciones nativas como la generación de números aleatorios o llamadas de la API. Sólo puede hacer estas cosas si se le solicita un EOA. Esto se debe a que Ethereum requiere que los nodos puedan acordar el resultado de la computación, lo que requiere una garantía de ejecución estrictamente determinista.

Al igual que en Bitcoin, los usuarios deben pagar tarifas de transacción pequeñas a la red. Esto protege la cadena de bloque Ethereum de tareas de computación frivolas o maliciosas, como ataques DDoS o bucles infinitos. El remitente de una transacción debe pagar por cada paso del "programa" que activó, incluyendo el cómputo y almacenamiento de memoria. Estos honorarios se pagan en cantidades del valor nativo de Ethereum, ether.

Estas tarifas de transacción son recopiladas por los nodos que validan la red. Estos "mineros" son nodos de la red Ethereum que reciben, propagan, verifican y ejecutan transacciones. Los mineros entonces agrupan las transacciones -que incluyen muchas actualizaciones del "estado" de cuentas en la cadena de bloques de Ethereum- en lo que se llaman "bloques", y los mineros entonces compiten entre sí para que su bloque sea el siguiente a ser agregado La cadena de bloques. Los mineros son recompensados con éter por cada bloque exitoso que ellos minan. Esto proporciona el incentivo económico para que la gente dedique hardware y electricidad a la red Ethereum.

Al igual que en la red Bitcoin, los mineros tienen la tarea de resolver un complejo problema matemático para poder "minar" con éxito un bloque. Esto se conoce como una "Prueba de Trabajo". Cualquier problema computacional que requiere órdenes de magnitud más recursos para resolver algorítmicamente de lo que se necesita para verificar la solución es un buen candidato para la prueba de trabajo. Con el fin de desalentar la centralización debido al uso de hardware especializado (por ejemplo ASICs), como ha ocurrido en la red Bitcoin, Ethereum eligió un problema computacional de memoria difícil. Si el problema requiere memoria, así como la CPU, el hardware ideal es de hecho la computadora en general. Esto hace que la Prueba de Trabajo de Ethereum sea resistente, permitiendo una distribución de seguridad más descentralizada que los bloqueos cuya minería está dominada por hardware especializado, como Bitcoin.

¿Cómo usar esta guía?

Usando Ethereum: Lo Básico

Esta sección captura las formas básicas en las que un usuario desearía participar en el proyecto Ethereum. En primer lugar convertirse en un nodo en la red que necesita para ejecutar un cliente Ethereum. Múltiples implementaciones se enumeran en la sección Elegir un cliente que también le da consejos qué clientes elegir en varias configuraciones. La conexión a la red proporciona información básica sobre redes, solución de problemas de conectividad y sincronización de bloques. Temas avanzados de la red como la creación de cadenas privadas se encuentra en Redes de prueba.

El Homestead Release

Homestead es la segunda versión principal de la plataforma Ethereum y es la primera versión de producción de Ethereum. Incluye varios cambios de protocolo y un cambio de red que proporciona la capacidad de realizar actualizaciones de red adicionales. La primera versión de Ethereum, llamada Frontier release, era esencialmente una versión beta que permitía a los desarrolladores aprender, experimentar y comenzar a construir aplicaciones y herramientas descentralizadas de Ethereum.

Hitos de la hoja de ruta del desarrollo de Ethereum

La hoja de ruta de desarrollo original establecida antes Ethereum fue en vivo especificó los siguientes hitos:

* Prerelease Paso 0: testnet olímpico - lanzado en mayo de 2015
* Release Paso uno: Frontier - lanzado el 30 de julio de 2015
* Release Paso Dos: Homestead - lanzamientos 14 de marzo de 2016 (Día de Pi)
* Release Paso Tres: Metrópolis - TBA
* Release Paso Cuatro: Serenity - TBA

Aunque todavía es válida, la sustancia detrás de ella ha cambiado algo. La fase testnet olímpica (antes de la liberación Frontier) vio una gran cantidad de mejoras importantes, seguido por Frontier, que se puso en marcha inmediatamente después. Homestead marca la salida de un producto beta a una versión estable. Homestead se introduce automáticamente en el bloque número 1.150.000 que debería ocurrir aproximadamente alrededor del 14 de marzo de 2016, Día del Pi

Si está ejecutando un nodo conectado a la red en vivo, es importante actualizar a un cliente compatible con Homestead. Tales clientes con sus versiones están listados bajo Ethereum Clients. De lo contrario, terminará en el tenedor equivocado y ya no estará en sincronía con el resto de la red.

Una vez que la cadena de bloques Ethereum alcanza el bloque 1.150.000, la red Ethereum sufrirá un hardfork permitiendo algunos cambios importantes como se explica en la siguiente sección.

Cambios en la horquilla dura de Homestead

Ethereum en el sentido formal estrecho es una serie de protocolos. Homestead viene con unos cuantos cambios de protocolo incompatibles hacia atrás, y por lo tanto requerirá un tenedor duro. Estos cambios que hicieron su camino a través del proceso de Propuestas de Mejora Ethereum y se incluyen son:

* EIP 2:
  + El coste para la creación de contratos a través de una transacción se incrementa de 21000 a 53000. La creación de contratos a partir de un contrato que utiliza el opcode CREATE no se ve afectada.
  + Las firmas de transacción cuyo valor s es mayor que secp256k1n / 2 ahora se consideran inválidas
  + Si la creación del contrato no tiene suficiente gas para pagar la tarifa final del gas por agregar el código del contrato al estado, la creación del contrato falla (es decir, sale de gas) en lugar de dejar un contrato vacío.
  + Cambiar el algoritmo de ajuste de dificultad
* EIP 7: DELEGATECALL: Añadir un nuevo código de operación, DELEGATECALL en 0xf4, que es similar en idea a CALLCODE, excepto que se propaga el remitente y el valor desde el ámbito padre al alcance hijo, es decir. La llamada creada tiene el mismo remitente y el mismo valor que la llamada original. Esto significa que los contratos pueden almacenar información de paso a través de msg.sender y msg.value de su contrato principal. Ideal para los contratos que crean contratos, pero no repetir información adicional que ahorra gas. Ver comentarios sobre EIP 7
* EIP 8: devp2p Compatibilidad hacia adelante Compatibilidad con el Principio de Robustez Cambios en el Protocolo de Descubrimiento RLPx y el protocolo de transferencia RLPx TCP para asegurar que todo el software cliente en uso en la red Ethereum pueda hacer frente a futuras actualizaciones del protocolo de red. Para las versiones anteriores de un cliente Ethereum, las actualizaciones del protocolo de red no estaban siendo aceptadas por los clientes más antiguos y se negaría a la comunicación si los paquetes hola no cumplían con las expectativas. Esta actualización significa que todas las futuras versiones del cliente aceptarán las actualizaciones de red entrantes y los apretones de manos.

Los cambios tienen los siguientes beneficios:

* EIP-2/1 elimina el incentivo excesivo para crear contratos a través de transacciones, donde el costo es de 21000, en lugar de contratos, donde el costo es de 32000.
* EIP-2/1 también corrige el protocolo "error" que con la ayuda de reembolsos de suicidio, actualmente es posible hacer una simple transferencia de valor de éter utilizando sólo 11664 de gas.