WHITEPAPER

THINGSCHAIN

step out line - step in chain

THINGSCHAIN

step out line - step in chain

Blockchain for the Internet of Things

Contents

Abstracto

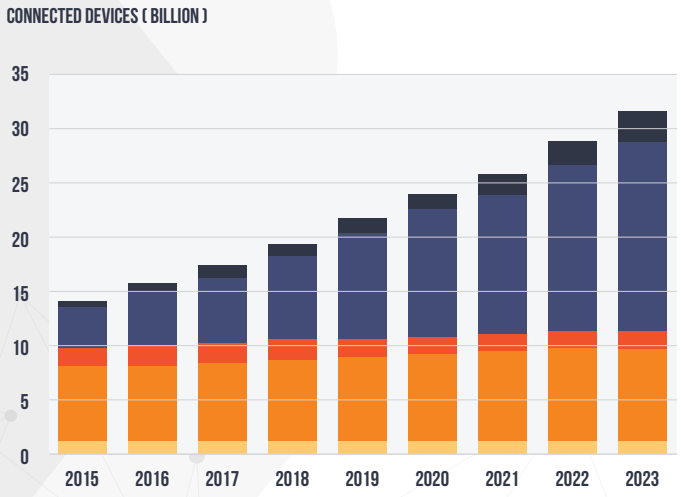
Los dispositivos de IoT son cada vez más importantes en nuestra sociedad digitalizada. Se estima que habrá 20 mil millones de dispositivos de IoT conectados en el mundo para 2023. A pesar de su importancia creciente, los dispositivos de IoT se ven obstaculizados por la falta de interoperabilidad, la poca seguridad y una mayor centralización. Las Blockchains son una posible solución a estos problemas, pero los diseños actuales de blockchain no son adecuados para su aplicación en IoT. Nuestro equipo ha diseñado una solución que ataca estos problemas de interoperabilidad y escalabilidad mediante la creación de una nueva arquitectura de cadena de bloques de varias capas específicamente para la aplicación IoT. ThingsChain es una cadena de bloques de varias capas que resuelve el problema de la escalabilidad y el bajo rendimiento de las transacciones que enfrentan las blockchains actuales. El diseño del protocolo utiliza una arquitectura multicapa con comunicación de cadena cruzada y protocolos de seguridad adicionales para garantizar la seguridad de los datos de IoT en la cadena de bloques.

Introducción

Internet of Things (IoT) es la red de dispositivos físicos, vehículos, electrodomésticos y otros elementos integrados con software y sensores que permiten que estas cosas se conecten e intercambien datos[1]. IoT permite que los objetos físicos sean más inteligentes y se conecten a Internet para proporcionar nuevas capacidades.

Por ejemplo, los termostatos Nest permiten monitorear remotamente la temperatura ambiente y ajustarla automáticamente en base a algoritmos inteligentes. IoT permite una mejor monitorización de máquinas y equipos al tener múltiples sensores para capturar puntos de datos como temperatura, presión, etc. y retransmitirlos continuamente a servidores donde pueden analizarse y actuar sobre ellos. Esto permite la predicción de ruptura inminente y medidas casos de uso que no eran posibles sin IoT. Esto abre una plétora de nuevas oportunidades que aún no se han explorado por completo.

Se estima que para 2023, habrá alrededor de 20 mil millones de dispositivos de IoT conectados en el mundo. Los dispositivos de IoT conectados incluyen automóviles, máquinas, medidores, sensores, terminales de punto de venta, productos electrónicos de consumo y dispositivos portátiles conectados. Entre 2017 y 2023, se espera que los dispositivos IoT conectados aumenten a una CAGR de 19 por ciento, impulsados por nuevos casos de uso y asequibilidad[2]. El mayor crecimiento en dispositivos conectados vendrá principalmente de IoT de área amplia y de corto alcance, como se muestra en la Fig.1 a continuación.



	2017	2023	CAGR
WIDE-AREA IOT	0.6	2.4	26%
SHORT-RANGE IOT	6.4	17.4	18%
PC/LAPTOP/TABLET	1.6	1.7	0%
MOBILE PHONES	7.5	8.8	3%
FIXED PHONES	1.4	1.3	0%
	17.5 BILLION	31.6 BILION	

Fig 1. Number of connected IoT devices (Ericsson Mobility Report, 2017)

A partir de ahora, la mayoría de estos dispositivos de IoT están conectados a servicios centralizados donde registran constantemente los datos generados por sus sensores y obtienen comandos de monitoreo y control. Estos dispositivos de back-end podrían ser servidores alojados en las instalaciones o soluciones de almacenamiento en la nube como AWS S3, Google Cloud, etc. Esto introduce un cierto grado de centralización en dispositivos IoT, que en realidad fueron diseñados para operar de forma descentralizada. Los dispositivos de IoT están limitados por los problemas de escalabilidad de los servidores centralizados a los que están conectados y, por lo tanto, no pueden actuar de forma completamente descentralizada.

La seguridad y la privacidad de los datos generados por dispositivos IoT es otra área de preocupación. Los datos generados por dispositivos IoT se almacenan en servidores centralizados y, a menudo, se presta muy poca atención a la seguridad y privacidad de los datos almacenados. El problema puede ser en múltiples dominios:

1. 1. Falta de seguridad en los datos transmitidos desde el dispositivo al servidor central.

2. 2. La falta de protección de la privacidad de los datos almacenados en los servidores, p. datos de anonimato, etc.

3. 3. No hay protocolos adecuados para garantizar la seguridad de los datos en servidores centralizados.

Esto a menudo lleva a un escenario donde los servidores que almacenan datos de IoT actúan como un honeypot para los hackers. Algunos ejemplos de hacks que usaron dispositivos IoT como su vector son.

1. El ataque de Mirai Botnet: en octubre de 2016, se lanzó el ataque DDoS más grande que se haya lanzado contra el proveedor de servicios Dyn mediante una botnet IoT. Esto llevó a una gran cantidad de Internet en baja, incluidos Twitter, The Guardian, Netflix, Reddit y CNN[3].

2. Más tarde, se utilizó una variante de Mirai Botnet para atacar al sector financiero en 2018[4]. El botnet IoT se compone principalmente de enrutadores domésticos comprometidos, televisores, DVR y cámaras IP que explotan las vulnerabilidades en productos de los principales proveedores, incluidos MikroTik, Ubiquiti y GoAhead.

Un informe reciente de Symantec descubrió que el número de ataques IoT aumentó de aproximadamente 6.000 en 2016 a 50.000 en 2017, un aumento del 600% en solo un año[5].

Interoperabilidad de los dispositivos de IoT

Otro problema clave es la falta de interoperabilidad entre dispositivos IoT. Aunque se ha implementado una gran cantidad de dispositivos de IoT, las empresas no han podido obtener muchos beneficios de ellos. La mayoría de estos dispositivos de IoT se comunican utilizando diferentes protocolos y hacer que se comuniquen entre ellos como parte de una red no es trivial. La interoperabilidad entre múltiples proveedores y las preocupaciones de seguridad son los dos obstáculos clave que impiden que los dispositivos de IoT generen valor para las empresas de hoy[6]. Una mayor porción del valor que IoT produce proviene de la interacción, la cooperación y, finalmente, la coordinación autónoma de entidades heterogéneas, que falta hoy en día.

(1) : Internet of Things - Wikipedia

(2) : Ericsson Mobility Report, 2017

(3) : 5 Worst IoT Hacking Vulnerabilities

(4) : Mirai Botnet

(5) : 600% increase in IoT attacks

(6) : Interoperability is the key for IoT

Blockchain

La tecnología Blockchain fue introducida por primera vez por Satoshi Nakamoto en 2008. En 2009, lanzó una implementación de Bitcoin que se concibió como un sistema electrónico de caja peer-to-peer. Bitcoin fue el primer protocolo que utilizó la tecnología blockchain tal como la entendemos hoy en día.

La idea clave detrás de blockchain es que las transacciones en la red se incluyen en bloques y cada uno de estos bloques se refiere a un bloque anterior, creando una estructura tipo cadena. Por lo tanto, blockchain es una lista de bloques unidos individualmente, con cada bloque que contiene una cantidad de transacciones. Proporciona un almacén de datos descentralizado e inmutable que se puede usar en una red de usuarios. También crea activos y actúa como un libro de contabilidad compartido que registra todas las transacciones. Cada transacción se puede consultar fácilmente, brindando mayor transparencia y confianza a todas las partes involucradas[7].

Ethereum es el siguiente paso en la evolución de blockchain. Creado en 2013, se lo considera Blockchain 2.0 y permite la ejecución de código arbitrario para completar procesos computacionales, en lugar de simplemente registrar transacciones. Es una máquina virtual completa de Turing y se ejecuta como una cadena de bloques pública.

(7) : *Introduction to blockchain technology, Hackernoon*

Modelos operacionales Blockchain

Las Blockchains pueden tener diferentes modelos operativos basados en la cantidad de confianza requerida entre los nodos. Hay dos modos principales de operación de blockchains: sin permiso y con permiso. En blockchains sin permisos, cualquiera puede iniciar un nodo y verificar los bloques en la cadena de bloques para contribuir al consenso. No se necesita permiso para unirse a una red de blockchain. Por lo tanto, cualquiera puede comenzar a interactuar con una red sin permiso. Bitcoin y Ethereum son ejemplos de blockchains sin permisos. Tales blockchains necesitan mecanismos de consenso que sean resistentes al ataque de Sybil para evitar que los actores aleatorios se unan a la red y rompan su consenso. Por ejemplo, Bitcoin utiliza PoW consenso que previene el ataque de Sybil pidiendo a los nodos resolver acertijos criptográficos antes de agregar un nodo.

Las blockchains autorizadas, en cambio, son ecosistemas cerrados y monitoreados donde el acceso y las capacidades de cada nodo en la red se basan en los roles que se les asignan. Solo un grupo restringido de actores tiene derecho a validar transacciones en bloque e interactuar con contratos inteligentes en dichas redes. P.ej. Hyperledger Fabric es una cadena de bloques autorizada donde todos los nodos se consideran confiables y tienen identidades criptográficas, por ejemplo, emitidas por servicios de miembros como Public Key Infrastructure (PKI), que los hace altamente escalables con bajo cálculo y un mecanismo de consenso relativamente directo.

Cómo Blockchain es relevante para aplicaciones de IoT

La tecnología Blockchain es adecuada para su aplicación con dispositivos IoT ya que proporciona las propiedades necesarias de descentralización, transparencia e inmutabilidad. Con diferentes dispositivos que forman parte del mismo protocolo de blockchain, también aborda el problema de la interoperabilidad. Exploramos estos temas con más detalle a continuación.

1. Descentralización

La descentralización libera los datos generados por dispositivos IoT del control de las agencias centralizadas. Como vimos anteriormente, si los dispositivos de IoT están controlados por entidades centralizadas, existe el riesgo de que estas entidades intenten utilizar estos datos para su propio beneficio. Por ejemplo, usar datos de sensores para mostrar anuncios específicamente dirigidos a individuos. Además, todos los datos almacenados en servidores centralizados los convierten en el blanco de los ataques. El uso de blockchain proporciona descentralización que hace que los dispositivos de IoT y sus datos sean más seguros contra los ataques.

2. Transparencia

Por su propio diseño, blockchains se distribuyen libros públicos. Si los datos del dispositivo IoT se almacenan en blockchains, entonces cualquiera puede auditarlo y verificar los datos almacenados. Esto proporciona un grado de transparencia que rara vez se ve en entidades centralizadas. Las entidades centralizadas a menudo intentan ocultar sus transacciones y datos, y los detalles solo se revelan a entidades con autoridad o poder.

3. Inmutabilidad

Dado que las transacciones almacenadas en una cadena de bloques son inmutables, los datos almacenados en cadenas de bloques se pueden utilizar para fines de auditoría. Si los datos del dispositivo IoT se almacenan continuamente en blockchains, entonces se pueden auditar fácilmente en cualquier momento mediante el uso de API específicas de blockchain.

4. Interoperabilidad

Un problema clave con los dispositivos IoT es la interoperabilidad. Los sensores de IoT de diferentes proveedores a menudo no siguen el mismo protocolo de comunicación y es difícil hacerlos hablar entre ellos. Pero si blockchain se usa como la capa subyacente, entonces cada dispositivo IoT puede guardar transacciones en la cadena de bloques y, por lo tanto, un dispositivo puede comunicarse con el otro ya que todos los dispositivos guardan datos y transacciones en la misma cadena de bloques subyacente.

5. Interacciones automáticas con contratos inteligentes

Algunos blockchains como Ethereum proporcionan una plataforma para ejecutar 'contratos inteligentes'. Los contratos inteligentes son lógicas programables o contratos que se pueden codificar y desplegar en cadenas de bloques públicas. Los usuarios o entidades pueden interactuar con estos contratos inteligentes pagando algunas tarifas de gas. Estos contratos inteligentes permiten así la ejecución automatizada de contratos en la cadena de bloques

Los casos de uso que combinan contratos inteligentes con dispositivos IoT abren muchas nuevas posibilidades. Por ejemplo, un sensor de temperatura IoT se puede conectar a una caja que contiene frutas frescas que se transportan. El sensor IoT enviará periódicamente su lectura de temperatura a un contrato inteligente. Mientras la temperatura esté por debajo de un cierto umbral, no hay acción. Pero tan pronto como cruza el umbral, el contrato inteligente penaliza el depósito hecho por el transportista por la incapacidad de mantener la temperatura acordada durante el transporte del producto.

Este proceso está completamente automatizado y no hay ningún ser humano involucrado. El contrato inteligente que se implementa en blockchain asegura que no haya problemas de confianza, y si alguna parte trata de alterar este proceso, lo mismo será capturado inmutablemente en la cadena de bloques.

¿Por qué las soluciones de blockchain actuales no son adecuadas para IoT?

Aunque las blockchains proporcionan propiedades que son beneficiosas para el ecosistema de IoT, no significa que cada blockchain sea adecuada para IoT. A continuación se presentan algunos problemas potenciales con la aplicabilidad de las soluciones actuales de blockchain para IoT.

1. Problemas con la escalabilidad

Las plataformas de blockchain populares actuales como Bitcoin y Ethereum no son adecuadas para las transacciones de IoT ya que el número de transacciones admitidas en estas cadenas de bloques es muy pequeño. Los dispositivos IoT, por otro lado, necesitan un número muy elevado de transacciones, ya que miles de sensores se pueden usar para capturar diferentes puntos de datos para una entidad, p. fábrica.
Existen pocas soluciones especializadas de IoT que utilizan la tecnología de contabilidad distribuida, pero están diseñadas específicamente para dispositivos de IoT. IoTA, por ejemplo, usa DAG para habilitar el libro mayor descentralizado y la alta tasa de rendimiento de transacción. Pero el diseño actual de IoTA introduce cierto grado de centralización debido al uso de nodos coordinadores ejecutados por la fundación IoTA.

2. 2. Los nodos IoT son livianos y no pueden hacer minería, almacenar blockchain, etc.

A. Los dispositivos de IoT generalmente son pequeños dispositivos de sensores y no están equipados para hacer cálculos pesados como minería de prueba de trabajo, etc.

B. Los dispositivos de IoT no tienen espacio para almacenar cadenas de bloques completas y verificarlas de manera independiente. Por ejemplo, el tamaño de la cadena Bitcoin y Ethereum actualmente es más de 100 GB. Ningún dispositivo IoT tiene tanta capacidad de almacenamiento.

C. Los dispositivos de IoT no pueden conectarse con sus compañeros todo el tiempo. Su conexión con sus pares depende de su conectividad y tiempo de actividad. Sin embargo, la mayoría de las cadenas de bloques actuales necesitan conectividad constante para obtener bloques más nuevos y actualizarse.

Debido a las limitaciones mencionadas anteriormente, la mayoría de las cadenas de bloques actuales son demasiado pesadas para dispositivos de IoT.

Visión general y visión de ThingsChain

ThingsChain: Blockchain 4.0

ThingsChain es una plataforma de próxima generación para dispositivos IoT basados en tecnología blockchain. Utiliza una arquitectura de varias capas que proporciona una solución a los problemas que enfrentan las cadenas de bloques actuales, como la falta de escalabilidad y la baja tasa de rendimiento de las transacciones.

¿Cómo puede ThingsChain resolver el problema?

ThingsChain utiliza un enfoque de varias capas para almacenar datos del dispositivo IoT. La capa principal se llama Webchain y la capa secundaria se llama NestChains. Las cadenas de servicio Nest son las capas que interactúan con los servicios y tienen un alto rendimiento. Solo los cambios en el estado cada 10 minutos se actualizan en NestChain. Por lo tanto, NestChain actúa como la fuente final de la verdad, mientras que WebChains almacena información transitoria.

WebChain podría ser una cadena de bloques privada y dependería de NestChain para retransmitir transacciones entre capas secundarias. La capa secundaria proporciona flexibilidad y extensibilidad para adaptarse a requisitos diversificados de diferentes aplicaciones de IoT. Por lo tanto, esta arquitectura permite una alta escalabilidad que es necesaria para manejar transacciones desde dispositivos IoT.

Algunos proyectos que trabajan en dominios relacionados

1. IoTA - IoTA se enfoca en permitir la comunicación del dispositivo IoT a través de una tecnología ledger distribuida llamada Tangle. Es único en el sentido de que se deshace de conceptos como bloques y mineros. En IoTA, cada transacción debe aprobar dos transacciones previas. Por lo tanto, este mecanismo evita los problemas inherentes a la tecnología de blockchain, como la escasa escalabilidad y la baja tasa de rendimiento de las transacciones.

2. Iotex - IoTeX pretende convertirse en el sistema nervioso centrado en la privacidad y escalable para IoT. Utiliza una arquitectura única de blockchain dentro de blockchain para contrarrestar los problemas de escalabilidad que enfrentan las blockchains tradicionales como Bitcoin y Ethereum. También le da mucho énfasis a la privacidad de los datos almacenados en la cadena de bloques y utiliza la tecnología de firma de anillo para permitir esto.

3. Iotchain - Iotchain es un proyecto de blockchain de China que también permite que los dispositivos de IoT interactúen entre sí. Usan tecnología DAG, similar a IoTA.

4. HDAC - HDAC es un proyecto de cadena de bloques que está trabajando en la creación de una red blockchain altamente confiable que puede utilizar convenientemente los servicios de los numerosos dispositivos IoT del mundo. Se enfocan en campos específicos en IoT como transacciones M2M (máquina a máquina) y autenticación de dispositivo. Tienen su base en Corea y se han asociado con Hyundai.

Descripción general del diseño y la arquitectura

El objetivo de ThingsChain es crear un sistema descentralizado y sin confianza en el que las transacciones sean similares a las transacciones en el mundo real. ThingsChain lo logra diseñando su red como una cadena de bloques de múltiples capas con un algoritmo de consenso doble para permitir que las transacciones se vinculen con información adicional en la cadena. Los usuarios, desarrolladores, operadores de nodo, organizaciones, empresas, intercambio de cifrado, socios y otras blockchains y cryptos pueden participar en el desarrollo de ThingsChain como se describe anteriormente. En este documento, discutiremos los componentes de la red y los roles de cada participante en todo el ecosistema de ThingsChain.

Como se discutió anteriormente, ThingsChain blockchain tendrá una estructura de varias capas. La capa principal se llamará Webchain y la capa secundaria se llamará Nestchain. Cada 10 minutos, las transacciones reales o la información importante se almacenarán en la cadena Nestchain.

pBFT (Practical Byzantine Fault Tolerance)

pBFTpBFT es un algoritmo de replicación que fue diseñado para tolerar fallas bizantinas. El objetivo de la tolerancia a fallas bizantinas es poder defenderse contra fallas de los componentes del sistema con o sin síntomas que impiden que otros componentes del sistema lleguen a un acuerdo entre ellos, cuando tal acuerdo es necesario para el correcto funcionamiento del sistema. El algoritmo pBFT proporciona replicación de máquina de estado bizantino de alto rendimiento, procesando miles de solicitudes por segundo con aumentos de latencia de menos de milisegundos[8].

DAG (Directed Acyclic Graphs).

Como se discutió anteriormente, las cadenas de bloques efectivamente tienen una estructura ligada como lista. Los bloques en una cadena de bloques deben agregarse uno después del otro como una lista. Esta estructura lleva a problemas de escalabilidad y un bajo número de transacciones por segundo que inhiben la adopción generalizada de blockchains. Bitcoin y Ethereum, ambos sufren de estos problemas.

Esta desventaja inherente de blockchain ha llevado a una exploración de formas alternativas de mantener bases de datos descentralizadas. El gráfico acíclico dirigido (DAG) es una de esas alternativas. Un gráfico acíclico dirigido es una implementación de un gráfico, y permite a las redes que lo utilizan eludir algunas de las limitaciones más desalentadoras del blockchain.

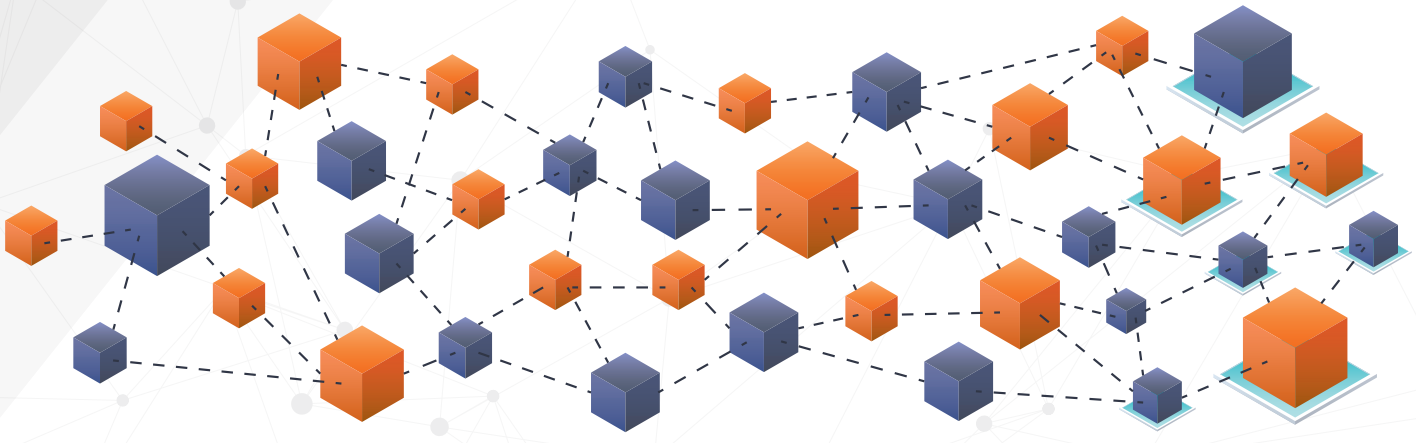


Fig 2. The "Tangle" in DAG: Each node represents a new transaction[9].

IOTA es la criptomoneda que más se habla sobre DAG. El uso de DAG ha eliminado por completo la necesidad de los mineros y las tarifas de transacción para mantener un consenso distribuido.

En Bitcoin, los mineros compiten en la resolución de un acertijo matemático por la oportunidad de escribir en la historia de la cadena de bloques. En IOTA, sin embargo, todos son mineros; todos son responsables de emitir y validar transacciones[10].

Presentación de gráficos de bloques radiantes

Los gráficos de bloques radiantes son similares a los DAG. Un DAG es un gráfico dirigido finito sin ciclos dirigidos. Consiste en finitos muchos vértices y bordes, con cada borde dirigido de un vértice a otro[11].

La estructura clave que hace que los DAG funcionen es un enredo. The Tangle es un tipo particular de gráfico dirigido, que contiene transacciones. Cada transacción se representa como un vértice en el gráfico. Cuando una nueva transacción se une al enredo, elige dos transacciones previas para aprobar, agregando dos nuevos bordes al gráfico[12].

Los gráficos de Radiating Block también funcionan en un concepto similar con múltiples nodos y conexiones directas entre ellos.

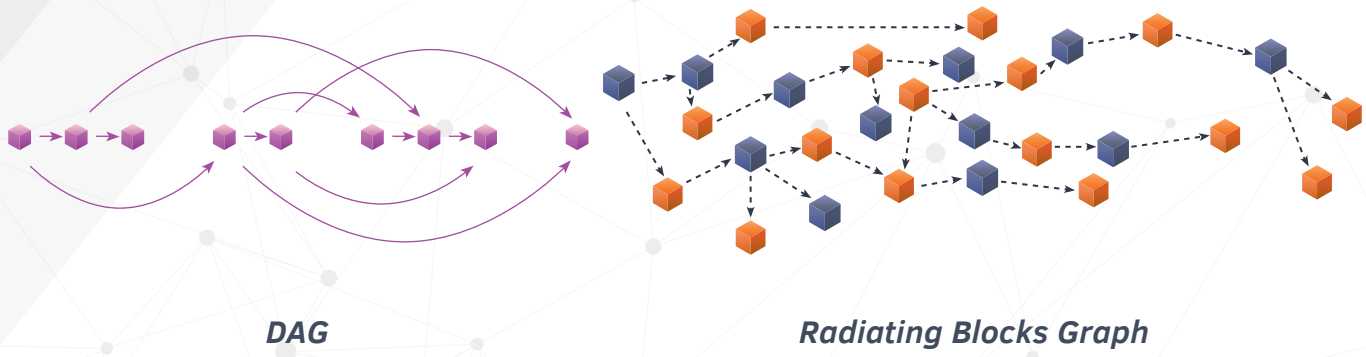


Fig 3. Illustration of DAG and Radiating Blocks Graph

Blockchain multicapa

ThingsChain propone tener una estructura de cadena de bloques multicapa. La capa principal se llamará WebChain y la capa secundaria se llamará NestChain. Esta estructura aumentará la capacidad de almacenamiento, procesará más confirmaciones de transacciones por segundo y proporcionará más seguridad. Una estructura de dos capas también disminuirá el tamaño de la cadena de bloques que los nodos son necesarios para almacenar.

Solo las transacciones finales se almacenarán en la cadena secundaria que es NestChain. Las transacciones transitorias se almacenarán en WebChain y una vez que se finalice un conjunto de transacciones, el efecto neto de esas transacciones sobre el estado de la cadena de bloques se actualizará en NestChain.

El uso de un DAG como Radiating Block también hace que el sistema sea más seguro ya que no hay ningún problema de ataque por parte de los mineros con una concentración de potencia hash. Como cada nueva transacción que se une al enredo aprueba otras dos transacciones anteriores, no hay mineros necesarios para verificar las transacciones en el sistema.

(8) : Byzantine Fault Tolerance, Wikipedia

(9) : IoTA Whitepaper

(10) : Introduction to DAG and cryptocurrencies

(11) : Directed Acyclic Graphs - Wikipedia

(12) : The Tangle - An Illustrated Introduction

WebChain and NestChain

WebChain

WebChain es la capa principal de ThingsChain que usa Radiating Blocks Graph. El nuevo concepto de Radiating Blocks Graph aumentará la tasa de transacción en comparación con la tecnología blockchain actual. Se considera una gran mejora para la industria de IOT.

WebChain usa prueba delegada del modelo de stake como mecanismo de consenso. Los nodos pueden votar sobre quiénes serían los validadores de bloque. La cantidad de votos que tiene cada nodo depende de la cantidad de tokens que hayan estacado en la red.

NestChain

Esta es una idea de tecnología completamente nueva en la que los bloques están controlados por Supernode. En Webchain, el número de bloques es alto y no siguen un orden determinado, por lo tanto, el almacenamiento necesario y los datos redundantes podrían ser enormes. Por lo tanto, el objetivo principal de Nestchain es filtrar los datos importantes y necesarios y luego almacenarlos en WebChain cada 10 minutos. Con esta tecnología, los datos del usuario serán más seguros, la tasa de transacción aumentará y el 51% de ataque podría evitarse.

NestChain usa el mecanismo de consenso Prueba de la verdad. El consenso es que solo las transacciones reales o la información confirmada son confirmadas por supernodos y almacenadas en NestChain.

Podría haber diferentes NestChain para diferentes propósitos. Estos se llamarían como Service Nestchains. Podría haber NestChains por separado para diferentes sectores. Un ejemplo es para el gobierno. Las identificaciones de civiles se pueden almacenar en NestChains, pero el gobierno puede controlar qué identificadores civiles se agregan a la capa principal, WebChain. Solo aquellos identificadores que son verificados por las agencias gubernamentales pueden almacenarse en la capa principal, que es la WebChain. Servicio similar Se pueden implementar NestChains para casos de uso médico, inmobiliario o bancario, pero solo se permite actualizar los datos verificados en la capa principal.

Comunicación de Cadena Cruzada

La comunicación de Cross Chain es muy importante para una red de múltiples capas, especialmente cuando está diseñada para dispositivos IoT. Los dispositivos IoT producen datos a una velocidad muy alta ya que son sensores que capturan datos todo el tiempo. Esto podría ser cada segundo o cada milisegundo. Siempre hay una necesidad de que un dispositivo IoT en una capa secundaria se comunique con un dispositivo IoT en otra capa secundaria. Para habilitar esto, las Nestchains se han diseñado de manera que puedan intercambiar datos y transacciones con otras NestChains a través de WebChain. Como los dispositivos IoT tienen capacidades de computación y almacenamiento bajas, es imperativo que la comunicación entre ellos sea ligera, de modo que no restrinja sus recursos.

La comunicación de cadena cruzada se puede lograr mediante el uso de la tecnología de vinculación de cadena lateral propuesta por Adam Back[13] . Esto funciona de la siguiente manera: para transferir monedas de la cadena principal a monedas de cadena lateral, las monedas de la cadena principal se envían a una salida especial en la cadena principal que solo se puede desbloquear mediante una prueba de posesión de SPV en la cadena lateral.

(13) : *Enabling Blockchain Innovations with Pegged Sidechains*

Para sincronizar las dos cadenas, se deben definir los siguientes dos períodos de espera:

1. El período de confirmación de una transferencia entre cadenas laterales es una duración para la cual una moneda debe estar bloqueada en la cadena principal antes de que pueda transferirse a la cadena lateral. El propósito de este período de confirmación es permitir que se cree suficiente trabajo de manera que un ataque de denegación de servicio en el siguiente período de espera se vuelva más difícil.

2. El usuario debe esperar el período del concurso. Esta es una duración en la que una moneda recién transferida no puede gastarse en la cadena lateral. El propósito de un período de concurso es evitar el gasto doble transfiriendo monedas previamente bloqueadas durante una reorganización.

Mientras está bloqueado en la cadena principal, la moneda se puede transferir libremente dentro de la cadena lateral sin interacción adicional con la cadena principal. Sin embargo, conserva su identidad como moneda de cadena matriz, y solo puede transferirse a la misma cadena de la que proviene.

Por lo tanto, la vinculación de cadenas laterales se puede utilizar de manera efectiva para lograr una comunicación de cadena cruzada similar a la descrita anteriormente.

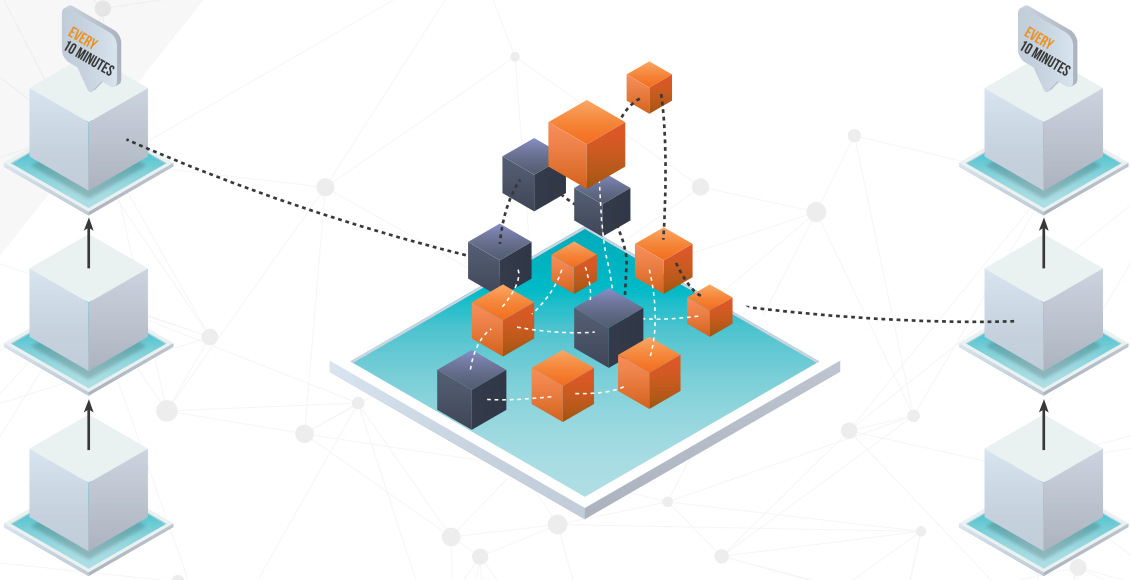


Fig 4. Communication between 2 NestChains

Red de ThingsChain

Los mecanismos de consenso son un aspecto importante del diseño de cualquier sistema basado en cadenas de bloques. Define cómo los nodos de la red interactúan entre sí y cómo deben actuar para contribuir a la confianza en la red. Algunos de los mecanismos de consenso popular que se utilizan hoy en día son Prueba de trabajo, Prueba de participación y Prueba delegada de participación. En la red de ThingsChain, WebChain utilizará un mecanismo de consenso de prueba delegada de estaca (DPoS) mientras que NestChain usará la prueba de la verdad como mecanismo de consenso. A continuación damos una breve descripción de estos mecanismos de consenso.

Proof of Work (PoW) (Prueba de trabajo)

El mecanismo de consenso de prueba de trabajo se utiliza para confirmar nuevas transacciones y producir nuevos bloques en la cadena de bloques. Los mineros resuelven un rompecabezas criptográfico relacionado con las transacciones incluidas en el bloque. Si pueden encontrar una solución correcta, se dice que han "extraído" un bloque y este bloque se envía a otros nodos de la red para su validación e inclusión en el blockchain. La prueba de trabajo actúa así como un mecanismo de prevención de "ataque de Sybil", ya que cualquiera que quiera agregar un bloque a la cadena de bloques tiene que resolver un enigma criptográfico antes de que su bloque pueda agregarse a la cadena de bloques. Blockchains basados en este mecanismo de consenso son Bitcoin, Litecoin, etc.

Proof of Stake (PoS) (Prueba de estaca)

Los sistemas de Prueba de Estaca tienen el mismo propósito de validar las transacciones y lograr el consenso, sin embargo, el proceso es bastante diferente que en los sistemas de Prueba de Trabajo. Con Prueba de Estaca, no hay un acertijo matemático, en cambio, el creador de un nuevo bloque se elige de forma determinista en función de su apuesta. La apuesta es cuántas monedas/fichas uno posee. Por ejemplo, si una persona fuera a apostar 10 monedas y otra persona estacara 50 monedas, la persona que aposte 50 monedas tendría 5 veces más probabilidades de ser elegida como el siguiente validador[14] de bloque. Casper (protocolo PoS de Ethereum), TON (red abierta de Telegram), etc. se basan en el mecanismo de consenso de Prueba de Estaca.

Delegated Proof of Stake (DPoS) (Prueba delegada de estaca (DPoS)

La prueba delegada de la participación como su nombre indica es una variante del mecanismo de consenso de PoS. La única diferencia es que en los sistemas DPoS, los usuarios 'votan' para seleccionar 'testigos' (otros usuarios en quienes confían para validar transacciones) y el nivel superior de testigos (que han acumulado la mayor cantidad de votos) se gana el derecho de validar las transacciones. Los usuarios incluso pueden delegar su poder de voto a otros usuarios, en quienes confían para que voten por los testigos en su nombre.

Los votos se ponderan según el tamaño de la apuesta de cada votante. Un usuario no necesita tener una apuesta grande para ingresar al nivel superior de testigos. Por el contrario, los votos de los usuarios con grandes apuestas pueden hacer que los usuarios con apuestas relativamente pequeñas se eleven al nivel superior de los testigos[15].

(14) : *Consensus Mechanism - PoW vs PoS*

(15) : *What is Delegated Proof of Stake*

Prueba de verdad

ThingsChain usará un mecanismo de prueba de consenso que garantizará que solo se almacenen datos correctos en NestChain. Es un mecanismo de consenso que permite almacenar solo transacciones reales o información confirmada por supernodo en Nestchain.

La red ThingsChain consta de 3 tipos de nodos:

1. Full Node – Este nodo es parte de WebChain. Full Node es una computadora que participa en la red WebChain y tiene conexiones con otros nodos completos. El nodo completo garantiza la corrección e integridad de la capa de NestChain. También pueden proporcionar servicios adicionales en la red y garantizar que la red funcione correctamente. Esto garantiza que la mayoría de las transacciones de alto rendimiento se manejen en la propia WebChain y solo una vez cada 10 minutos los cambios en los estados se actualizan en NestChain.
Las transacciones se enviarán a nodos completos y se enviarán a los delegados. Un Delegado es un Nodo Completo que ha sido votado por otros Nodos Completos (Votantes) para ser el validador del siguiente bloque. Los votantes son nodos completos que apuestan su TIC (token de ThingsChain) para obtener los votos. Para votar por un Delegado, un Nodo Completo debe crear una transacción llamada Transacción de Voto y el total de Votos se contará con pesos que son el saldo de replanteo actual de los Votantes. Los nodos completos pueden ser ejecutados por cualquier computadora y juegan un papel vital en la sostenibilidad de la red de Thingschain. Para promocionar nodos completos para apostar TIC y unirse al proceso de votación, Thingschain tiene el sistema de recompensas de bloque para los delegados y sus votantes. Thingschain recompensa a los generadores de bloques con una cantidad fija de TIC por bloque.

2. Super Node – este nodo es parte de Main NestChain. El objetivo principal de los Nodos Super es hacer que las transacciones en ThingsChain sean ricas en información. Los Supernodos ejecutarán la capa NestChain en ThingsChain. Los nodos Super aprobarán los bloques de NestChain que contengan transacciones y propaguen las transacciones de NestChain a otros nodos Super y nodos completos en toda la red de ThingsChain. Un Super Node deposita una gran cantidad de tokens como apuesta para respaldar su compromiso con la red. Para incentivar a los Super Nodes a participar en la red ThingsChain, la red los recompensa con los honorarios dados por los usuarios para procesar la información adjunta. Esto actúa como un interés ganado para Super Nodes por depositar una gran cantidad de tokens como participaciones en la red.
3. Nodo de servicio: este nodo forma parte de Service NestChains, como la cadena de servicios gubernamentales, la cadena de servicios médicos, la cadena de servicios inmobiliarios, etc. Los nodos de servicio forman el servicio NestChains que se desarrollan para casos de uso específicos.

3. Service Node – No es necesario actualizar todos los datos transaccionados en los nodos de servicio en NestChain, solo se actualizan los cambios confiables y verificados en el estado de NestChain. ThingsChain está descentralizado en la capa Nodo completo y Supernodo, pero no en la capa del nodo de servicio. Si un servicio particular NestChain ejecutado por los nodos de servicio se interrumpe, la red no puede proporcionar el servicio. Esto también modela el escenario de la vida real donde si una agencia gubernamental en particular se retira de una plataforma, entonces los datos sobre esa agencia gubernamental no están disponibles en la plataforma común. Los nodos de servicio avanzado proporcionan servicios como la verificación de Nestchain, el sistema de pago instantáneo o el sistema de pago privado.

La red debe confiar en los Nodos de Servicio. Después de completar el proceso para probar las identidades y autoridades, los nodos de servicio se convierten en nodos de confianza y pueden comenzar a proporcionar sus servicios a la red. Los nodos de servicio trabajan en conjunto siguiendo el mecanismo de la prueba de la verdad para mantener el consenso de la red. Los nodos de servicio pueden ser administrados por gobiernos, hospitales, universidades, bancos y empresas. Los servicios en la red de Thingschain son provistos por ciertos Nodos de Servicio y no están descentralizados. Por ejemplo, solo el gobierno de China puede proporcionar el servicio de verificación a los pasaportes chinos. Thingschain está diseñado para ser descentralizado en la cadena web y la cadena Nest y no para los servicios adicionales. Cada vez que un nodo completo, un delegado o un súper nodo sale de la red, Thingschain sigue siendo ejecutado por otros nodos. Sin embargo, si un nodo de servicio sale de la red, se suspenderá el servicio proporcionado por ese nodo de servicio. Esa es la realidad del mundo real y el diseño de ThingsChain es llevarlo a la red, no romperla

Como se muestra en la Fig. 5, cada 10 minutos, las transacciones reales o la información importante se almacenarán en la cadena Nest. Es por eso que las transacciones transitorias no se almacenarán en NestChain. Solo se seleccionará la información necesaria dependiendo del propósito de cada industria, como el servicio KYC (Conozca a su cliente) para el gobierno, la información de los pacientes para los registros médicos de salud, etc.

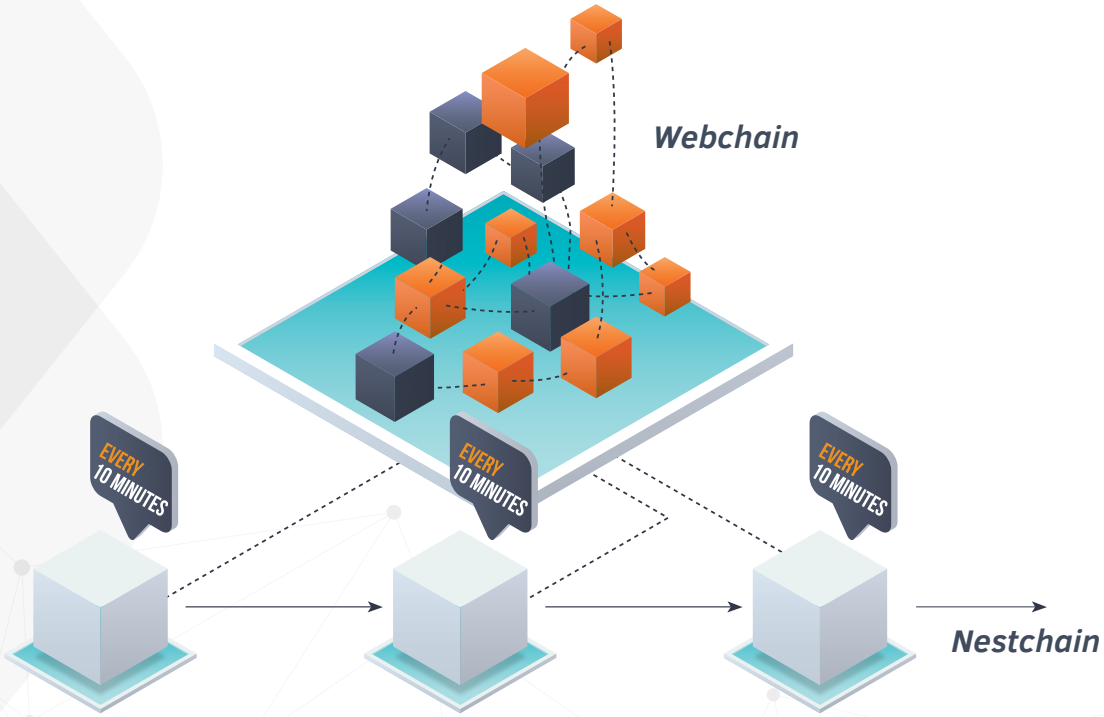


Fig 5. Interaction of WebChain and NestChain

Security

Seguridad debido a la descentralización

Las redes descentralizadas son mucho más seguras ya que no hay un servidor centralizado donde se almacenan todos los datos y transacciones que pueden ser atacados para robar la información. Existe el riesgo de que se piratee el lado del cliente o el servicio en la nube, lo que ocasiona el robo de los datos del usuario.

Junto con la descentralización, ThingsChain está utilizando algunas de las últimas tecnologías para mejorar la seguridad y el rendimiento. Pocos de ellos se mencionan a continuación.

Criptografía de curva elíptica

Criptografía de curva elíptica (ECC) se utiliza en la criptografía de clave pública para ThingsChain. ECC ofrece el mismo nivel de seguridad cuando lo compara con RSA. Algunas ventajas de ECC son que tiene un tamaño de operando mucho más corto y implementaciones más eficientes. Con los años, se ha convertido en un estándar de facto para proteger la seguridad y la privacidad de los sistemas emergentes de IoT y las redes de criptomonedas[16].

(16) : *Elliptic Curve Cryptography, IoT Security and Cryptocurrencies*

Cuentas de firma múltiple

ThingsChain admite cuentas con varias firmas. Una cuenta de firma múltiple es una cuenta que requiere varias firmas para firmar transacciones. Los usuarios pueden especificar los firmantes que se necesitarán para operar una cuenta en particular.

Esto proporciona una mejor seguridad, ya que protege contra el escenario donde el operador de la cuenta se vuelve pícaro. Supongamos que hay una cuenta que se usa para enviar datos en el blockchain por una agencia del gobierno. Si una sola persona tiene acceso a esta cuenta, existe el riesgo de que se vuelva deshonesto y, potencialmente, ingrese datos incorrectos. Tal situación se previene mediante el uso de cuentas con varias firmas, ya que ahora se necesita el consentimiento de varias personas para operar esa cuenta.

Almacenamiento de datos en forma cifrada en blockchain

Los datos sobre la cadena de bloques ThingsChain se almacenarán en forma encriptada de manera predeterminada. Esto evitará que los atacantes simplemente lean los datos almacenados en la cadena de bloques por los dispositivos IoT. En una cadena de bloques pública, cualquier persona puede acceder a los datos almacenados. Por lo tanto, para proteger la privacidad y proporcionar confidencialidad, ThingsChain almacena todos los datos confidenciales en forma cifrada.

Resumen

ThingsChain es un intento de crear una plataforma basada en blockchain de próxima generación para aplicaciones IoT que resuelve los problemas actuales de escalabilidad, bajo rendimiento de transacciones e interoperabilidad. Hemos diseñado un protocolo basado en cadenas de bloques multicapa donde diferentes capas se pueden comunicar entre sí según sea necesario. Las diferentes capas manejan las transacciones para las cuales están diseñadas y solo las transacciones más importantes se actualizan en la cadena principal. También utilizamos protocolos de seguridad avanzados para garantizar que los datos de IoT se almacenen de forma segura en blockchain. Nuestra visión es permitir un futuro en el que los dispositivos de IoT puedan interactuar entre sí de una manera interoperable y sin confidencias sin preocuparse por la seguridad de los datos almacenados.


THINGSCHAIN
step out line - step in chain
www.thingschain.network