Hdac - Innovación en transacciones (IoT)

LIBRO BLANCO EN ESPAÑOL
https://hdac.io/

Por favor, póngase en contacto con los autores por preguntas o comentarios a:
support@hdac.io

Versión 1.0

RESUMEN EJECUTIVO

La industria de la IoT (Internet de las cosas), está a punto de crecer exponencialmente y la plataforma Hdac serà la que le proporcione los bloques de construcción faltantes que permitirà que los entornos de IoT prosperen, basados en:

1. **Autenticación**: los dispositivos se pueden identificar correctamente por otro
2. **Mapeo**: una vez identificados, se pueden conectar sin problemas
3. **Pago de máquina a máquina**: los dispositivos pueden cobrar entre ellos

Hdac resuelve estos tres problemas combinando **blockchain**, **IoT** y **Fintech**, lo que permite micropagos automáticos, de máquina a máquina, de ultra bajo costo, entre los dispositivos IoT que se autentican, mapean y verifican a través de blockchain.

En su arquitectura, el sistema Hdac usa una combinación de blockchain públicos y privados, lo que permite velocidades de transacción previamente inalcanzables. La tecnología usará la generación de números aleatorios cuánticos para asegurar estas transacciones.

El sistema Hdac garantizará en última instancia la eficiencia y la seguridad del crecimiento exponencial de la industria de la IoT

Introducción

La sociedad en el futuro estará "hiperconectada" y la innovación digital se reintegrará continuamente a los sistemas económicos mundiales. La nueva tecnología se habilitará mediante una combinación adecuada de blockchain (*que tiene su valor como criptomoneda*) y IoT. El mercado y los consumidores demandarán transacciones financieras más confiables y más accesibles. Esto conducirá al desarrollo de cripto monedas, que se pueden implementar para ser utilizadas y dentro de la tecnología blockchain

Creemos que el futuro mundo digital será un mundo en el que la plataforma Hdac operará una red blockchain altamente confiable, que puede utilizar convenientemente los servicios de los numerosos dispositivos IoT del mundo. Se dice que "*la moneda de la nueva economía es la confianza"*, por lo que es primordial que las nuevas tecnologías se basen en la confianza. La plataforma Hdac será una herramienta clave para implementar un sistema de pago más razonable y eficiente a medida que converjan los mundos de blockchain, fintech e IoT.

La filosofía tecnológica que sustenta a Hdac es mejorar dramáticamente los entornos de pago a diario: los contratos, las liquidaciones, los préstamos, las inversiones, los impuestos y las facturas de servicios públicos, todas deberían ser transacciones sencillas y fáciles. Además, creemos que será posible, utilizando nuestra tecnología, promover un consumo razonable y una administración precisa e inteligente para todos los gastos de comunicaciones y servicios.

Se espera que el Blockchain y las criptomonedas funcionen en el futuro cercano, como instrumentos de pago confiables, seguros y eficientes para el entorno de Internet de las cosas [IoT]. Una **Máquina de dinero** será utilizada para el pago de máquina a máquina [M2M] se implementará con pago de igual a igual [P2P] que mejora la estructura de alto costo y baja eficiencia del sistema actual de facturación/depósito/liquidación centralizado que utilizan en las industrias tales como gestión de departamentales y facturación móvil

Sin embargo, también es necesario identificar (*autenticar*) y conectar (*mapear*) al dispositivo apropiado para garantizar que todo esté en un entorno conectado con privilegios previamente aprobados, y para proporcionar funciones de identificación para manejar las tareas solicitadas de forma segura. Estos cambios manejara una cultura de pago que permite micropagos y una liquidación transparente en todas las actividades económicas, como cuando se adquieren bienes de consumo o se utilizan servicios públicos en la vida cotidiana. Por ejemplo, los bienes de consumo se pueden comprar y consumir solo en

cantidades necesarias. Las transacciones serán inmediatas con un bajo costo o riesgo para bienes públicos y privados como electricidad, agua, televisión por cable e Internet.

La sociedad en el futuro estará "*hiperconectada*" y la innovación digital se reintegrará continuamente a los sistemas económicos mundiales. La nueva tecnología se habilitará mediante una combinación adecuada de blockchain (*que tiene su valor como criptomoneda*) y el IoT. El mercado y los consumidores demandarán transacciones financieras más confiables y más accesibles. Esto conducirá al desarrollo de criptomonedas que pueden implementarse para utilizarse dentro de la tecnología blockchain.

El Hdac Token [Hdac*T], un token inteligente basado en blockchain generado en la plataforma Hdac, está diseñado para realizar una tarea determinada bajo las diversas condiciones de comando en el entorno IoT. Hdac proporciona estas funciones de criptomoneda y un entorno de servicio de pago simple, con la racionalidad y eficiencia que persigue la plataforma Hdac, será la plataforma de micropago de elección para su uso con dispositivos IoT.

Además, Hdac se convertirá en una plataforma especializada en fintech basada en criptomonedas, al proporcionar una billetera de hardware que considera la seguridad del usuario y la conveniencia de pago en servicio de la comunicación y los pagos mencionados anteriormente entre los dispositivos M2M y el IoT.

Blockchain y IoT

El uso del Blockchain para admitir aplicaciones de IoT

En un entorno como una casa inteligente o una fábrica, varios dispositivos equipados con sensores, que están estrechamente interconectados mediante un blockchain privado, se pueden configurar para operar de forma más segura y confiable de acuerdo con las condiciones de los demás dispositivos. Un blockchain privado está configurado para realizar no sólo la autenticación de usuario sino también la autenticación mutua entre dispositivos, generando y registrando de forma segura los detalles de operación y los contratos de IoT basados en escenarios.

Estamos creando un ecosistema confiable en el cual los servicios de micropagos se ejecutan en el entorno general de Hdac y en las cadenas de bloques de objetivos privadas, creadas específicamente, al configurar las cadenas de bloques privadas y públicas para que estén interconectadas.

El uso de blockchains privados solo es práctico si pueden interactuar con un blockchain público que ya está en funcionamiento. En este sentido, proporcionamos Hdac, una cadena de bloques pública habilitada para criptomonedas que se puede utilizar de manera efectiva con múltiples blockchains privados. En otras palabras, con nuestro blockchain, los micropagos son posibles más allá de la liquidación P2P de la cadena de bloques pública. En una red blockchain privada controlada, implementamos una máquina de monedas para contratos mutuos y pagos entre dispositivos IoT, lo que permite procesos de pago y consumo más accesibles, confiables y seguros.

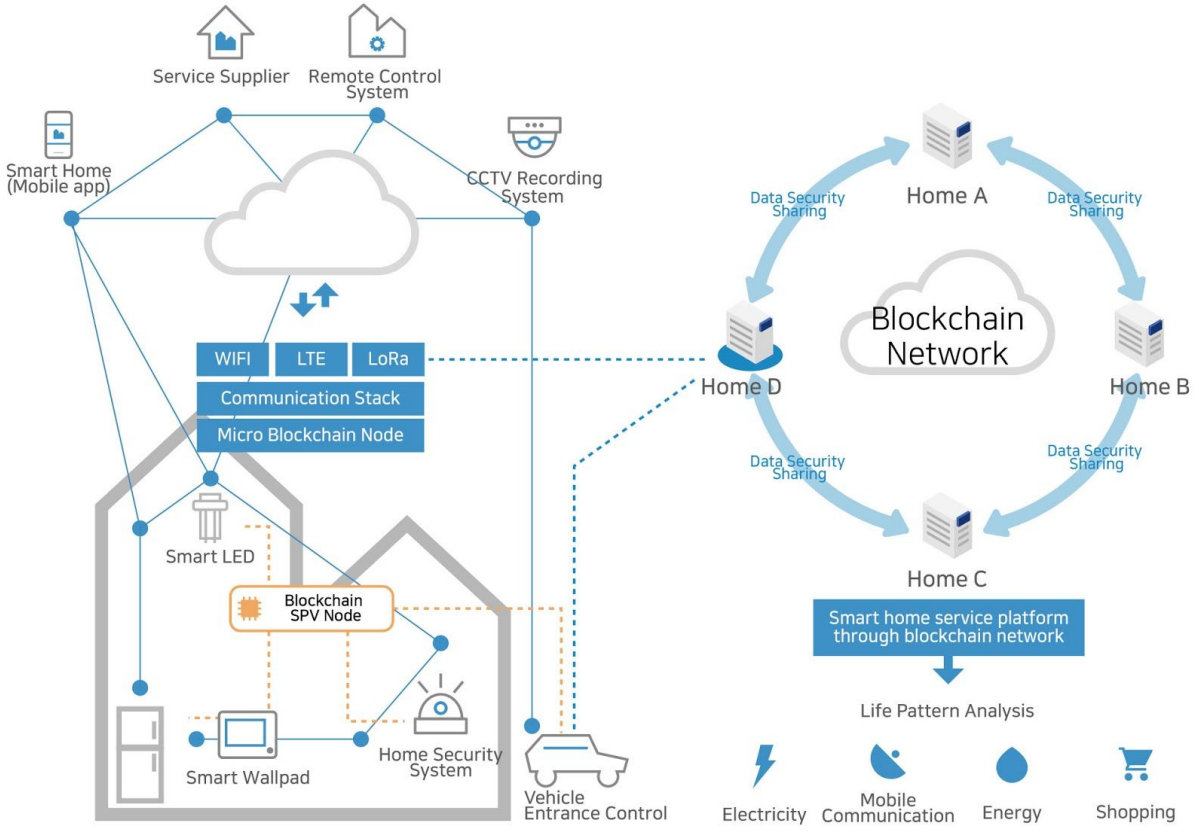

Figura 1:Ejemplo de blockchain privado que permite el uso de IoT

Por ejemplo, supongamos que un usuario desea operar un dispositivo dentro de una capacidad o presupuesto específico. El usuario establece el valor designado (*capacidad o cantidad, aquí se refiere al valor del contrato IoT*) en el dispositivo de control montado en un teléfono inteligente, una computadora, un televisor inteligente o un control remoto y transfiere los datos al dispositivo correspondiente. Luego, la parte de procesamiento de datos de medición del dispositivo transmite el valor de contrato de IoT al dispositivo de medición e inicia la operación. En este momento, el dispositivo activado funcionará hasta que transmita una señal que indique que el valor del contrato IoT especificado ha alcanzado el nivel indicado por el dispositivo de medición. El dispositivo operativo transmite datos cuando se alcanza un valor especificado, o cuando el dispositivo de control del usuario solicita la confirmación del estado de funcionamiento actual para que el usuario pueda confirmar los datos. En este momento, se requiere un proceso de autenticación para confirmar los procesos de comunicación entre los dispositivo de control del usuario, el operativo y el de medición. Si no es un dispositivo autenticado, puede adoptar un esquema de autenticación mutua que no puede enviar o supervisar el contrato de IoT. Además, se

puede usar un contrato de IoT autorizado para realizar un pago y, en el caso de un blockchain privado, un token definido por el usuario se puede usar como un token de pago para activar el dispositivo de IoT.

Los tokens definidos por el usuario pueden tener atributos asignados para pagar sólo para fines específicos en un contrato de IoT, y pueden evitar que el usuario se desvíe a dispositivos o usos no deseados.
Esto juega un papel importante en proporcionar transparencia de uso de tokens mientras se mantiene la seguridad descripta anteriormente. Por ejemplo, cuando los padres transfieren los tokens a un menor, es posible que no quieran que el niño compre alcohol o tabaco en una máquina expendedora donde el token esté disponible. Los tokens pueden llevar atributos que impiden la compra de productos particulares como alcohol o cigarrillos vendidos a través de dispositivos IoT, como máquinas expendedoras, y por lo tanto les dan a los padres más control sobre cómo se gastará el dinero que le dan a sus hijos.

Integración entre Blockchain Networks

Integración entre cadenas de bloques públicas

Como la tecnología blockchain inicial se está volviendo popular debido a sus características de descentralización, transparencia, usabilidad y confiabilidad, la aplicabilidad de blockchain se está expandiendo a través de industrias tales como criptomonedas, verificación de asistencia, mercados pronosticados y finanzas internacionales. Por lo tanto, a medida que aumenta la cantidad de transacciones y datos, es necesario considerar un caso en el que las cadenas públicas de bloques excederán su capacidad natural.

Las conexiones entre blockchains públicas ya están implementadas mediante el intercambio de datos a través de los intercambios. Es decir, en el caso de una cadena de bloques registrada en un servicio de Intercambio, este se puede realizar de tal forma que el servicio realice la retransmisión. La ventaja de este enfoque es que las personas pueden identificar y usar fácilmente los servicios porque se realizan de la misma manera que los intercambios entre monedas fiduciarias como el **Won Coreano** y el **Dólar Estadounidense.**

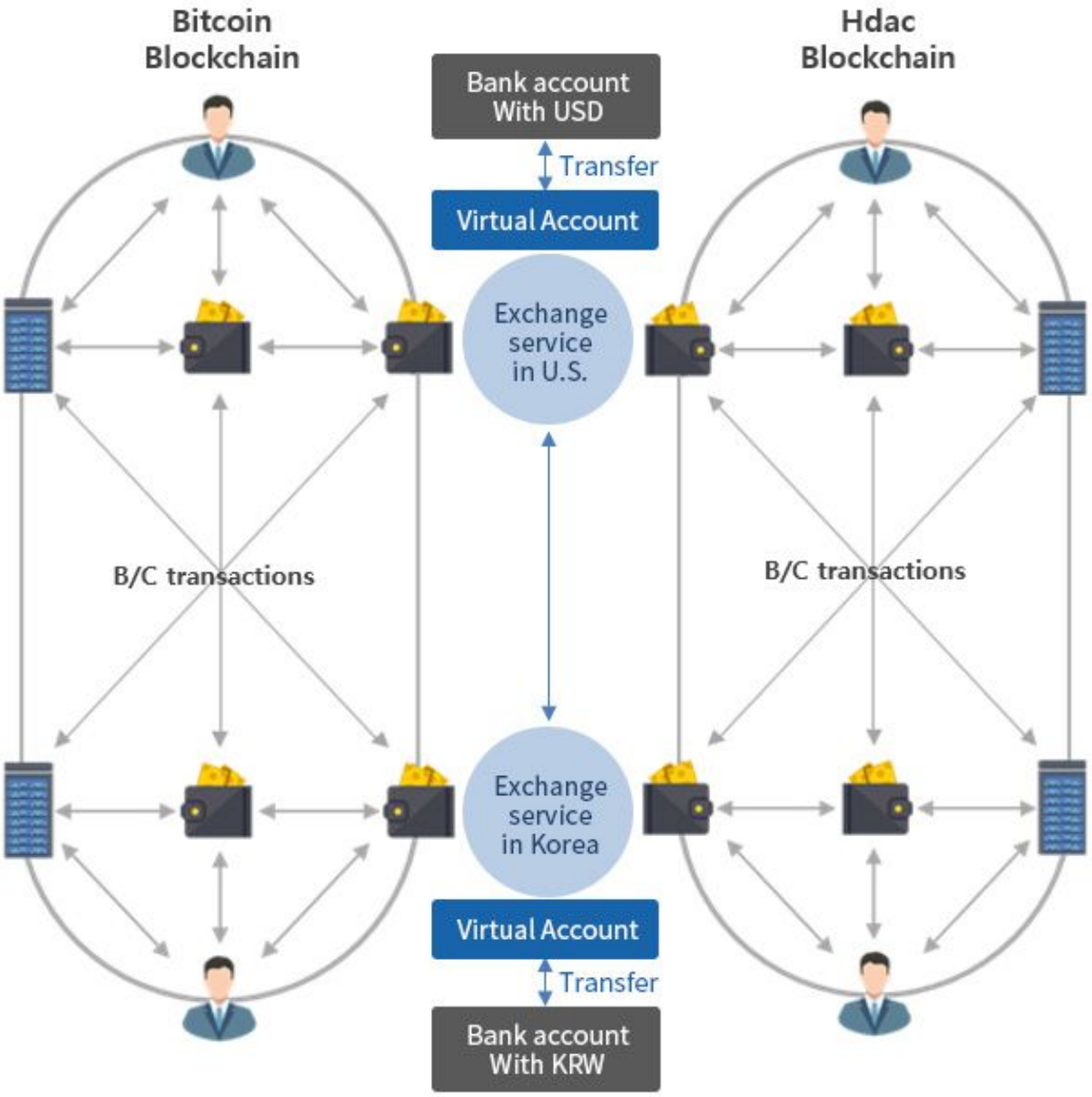

Figura 2: Integración entre blockchain públicos

Las cadenas de bloques públicas también pueden vincularse jerárquicamente. Por ejemplo, hay blockchains de nivel inferior que se pueden votar por distrito o por condado, y los resultados de estos se integran en un blockchain de nivel medio. En este caso, el blockchain de nivel medio, es la escala de una ciudad o provincia, y puede tener múltiples blockchains de nivel inferior. En otras palabras, un resumen de las transacciones recopiladas en la cadena de bloques de nivel inferior se transfiere a la cadena de bloques de nivel medio. La cadena de bloques superior se puede considerar como una estructura en

la que la información de todas las cadenas de bloques de nivel inferior se integra con una cadena de bloques de escala nacional. Aunque este es solo un ejemplo simple, se puede aplicar en varias formas en una red blockchain en forma de un árbol.

En este caso específico, la interconexión entre cadenas de bloques públicas puede interconectarse a través de un servicio separado que actúa como intercambio. Y esta formación puede ser una concatenación dentro de la cadena de bloques.

Integración entre Blockchains Público y Privado

Una red de blockchain privada o una blockchain permitida es una cadena de bloques con privilegios de acceso. Su configuración significa que no puede accederse a cada nodo libremente a diferencia de una cadena de bloques pública. Por lo tanto, para acceder a una cadena de bloques privada desde una pública, se requiere un nodo de puente o un intermediario de retransmisión. Este nodo puente, debe tener toda la información de configuración de la cadena de bloques privada, para permitirle el mismo nivel de acceso que su equivalente privado, al mismo tiempo que le permite publicar en la cadena pública. En resumen, se puede acceder al blockchain privado solo cuando el administrador del blockchain privado, otorga acceso a través de la autenticación previa y registro.

Alternativamente, en el caso de una transacción específica, el administrador puede otorgar un privilegio separado y enviarlo al nodo o dispositivo. Para usar un blockchain privado, fundamentalmente el usuario debe estar registrado después de la misma autenticación con esa blockchain privada.

En términos de transacciones financieras, cuando hay una transacción entre un blockchain público de Bitcoin y un token privado de Hdac no cambia el valor.

Los tokens pueden usarse posiblemente dentro de una empresa específica o para un propósito específico. En este caso, la relación de intercambio entre esos dos se puede determinar a través del intercambio.

Con el fin de encontrar formas de tratar con eficacia las transacciones generadas por los dispositivos de IoT a gran escala, el equipo de Hdac ha investigado la estructura y velocidad de procesamiento de transacciones de IOTA y en la red de próxima generación de Ethereum. En nuestra red de prueba, realizar grandes transacciones de decenas de miles, a cientos de miles de transacciones por segundo, ha demostrado que solo se procesó un número limitado de transacciones, dependiendo de la velocidad de la red física / el rendimiento de la informática física. Por lo tanto, la mejor solución para administrar altos niveles de transacciones es el procesamiento con múltiples blockchains privados e integrando la información a través de un acceso separado a la cadena de bloques

En particular, las cadenas de bloques públicas en un entorno global tienen velocidades de transacción muy limitadas (valores aproximados, Bitcoin=2tx/seg y Ethereum = 5tx/seg)

debido a problemas de red y problemas de sincronización de bloques para muchos nodos. Hdac tampoco puede implementar la velocidad óptima en el entorno global de Internet, debido a los cambios en la velocidad de la red a lo largo del tiempo y los retrasos en la sincronización de bloques. Por lo tanto, en el futuro, una gran cadena de bloques de procesamiento de transacciones puede ser una red de blockchains de una estructura jerárquica o distribuida compuesta de múltiples blockchains privadas para cada propósito. Continuaremos investigando y trabajando para implementar este tipo de blockchain, y nos esforzaremos por desarrollar un ecosistema completo de blockchain compartiéndolo en línea a medida que los resultados estén disponibles.

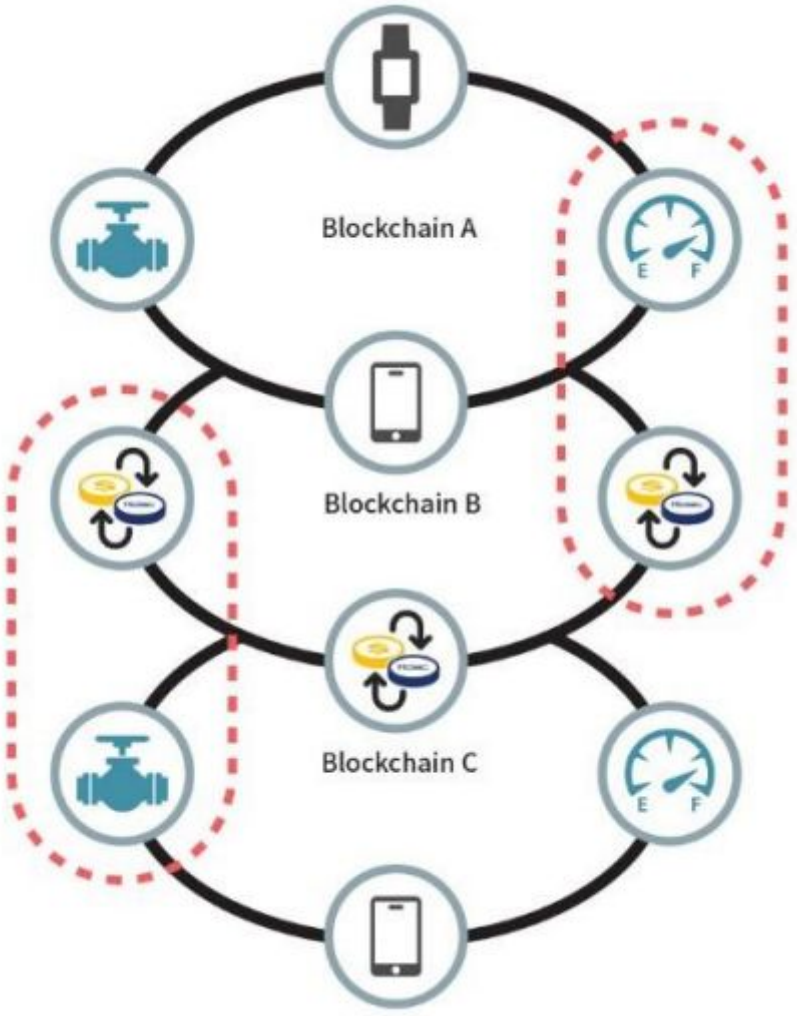

Figura 3: Cadenas de bloques, jerárquicamente integradas

IoT y seguridad

ICBM (IoT, Cloud, Big Data y Mobile) se considera la tecnología central prometedora de la próxima revolución industrial en el mercado global; Se espera que el IoT no solo amplíe el acceso a este mercado, sino también que aumente la eficiencia y la conveniencia para los usuarios con diversos valores económicos.

Sin embargo, para lograr un resultado tan positivo, se debe garantizar la conectividad entre los dispositivos y la confiabilidad. En otras palabras, eliminar la desconfianza y las amenazas a la seguridad implícitas por la conveniencia de la conexión a Internet es la principal prioridad.

Los atributos más atractivos del IoT, son que permite que los dispositivos sean inteligentes y conectados. Los dispositivos que no se crearon para su uso en el blockchain no serán inteligentes ni estarán conectados, y todas las amenazas y vulnerabilidades que puedan ocurrir en el entorno de Internet existente se pueden heredar. Mientras tanto, aparte de la vulnerabilidad de seguridad debido a una infracción externa, los datos recopilados en tiempo real en un servicio basado en Internet pueden conducir a la invasión de la privacidad, y la conexión sin seguridad puede ser un desastre social. Es necesario que la base de esta sociedad hiperconectada pueda contratar y operar entre un sistema de red P2P confiable y los dispositivos IoT en los que confiaremos todos los días. Basado en esto, tiene la capacidad de evolucionar en una red que puede soportar un sistema de micropagos ultra avanzado que puede funcionar de manera segura, confiable e independiente con entradas personalizables de los usuarios.

Innovación en Transacciones y Máquina de dinero

Uno de los aspectos más innovadores de la próxima revolución industrial es el IoT, que se refiere a las tecnologías y servicios inteligentes que conectan todo lo relacionado con Internet y comunican información entre personas y dispositivos, así como entre diferentes dispositivos. Sin embargo, las tecnologías como la conexión en red, que conecta dispositivos entre sí, la tecnología de procesamiento adecuada para diversos servicios, tecnología de interfaz para comunicación y la tecnología de procesamiento distribuido para almacenar y procesar grandes cantidades de datos, son esenciales para el IoT, y todas requieren tecnologías de seguridad para evitar piratería y filtración de información.

Si bien están surgiendo varios servicios basados en este tipo de tecnología de Internet, muchos dispositivos en el blockchain son operados por un contrato tipo IoT, y se espera que este servicio sea posible a través del pago y la liquidación. En particular, los contratos de

IoT no solo controlan dispositivos, acceden y ayudan a comunicarse entre dispositivos, sino que también aseguran el anonimato, con todas las transacciones registradas en el Blockchain. El Libro de registros (blockchain), se utiliza como datos para el aprendizaje automatizado. El ahorro de costos que se espera que proporcione este Big Data[1] e IoT a través de la inteligencia artificial [IA][2] es el objetivo final del ecosistema blockchain IoT[3].

Asegurar la confianza entre los dispositivos de IoT en Blockchain

La estructura conectiva del IoT y la estructura de red de las blockchains son muy similares, como se puede observar en la siguiente figura:

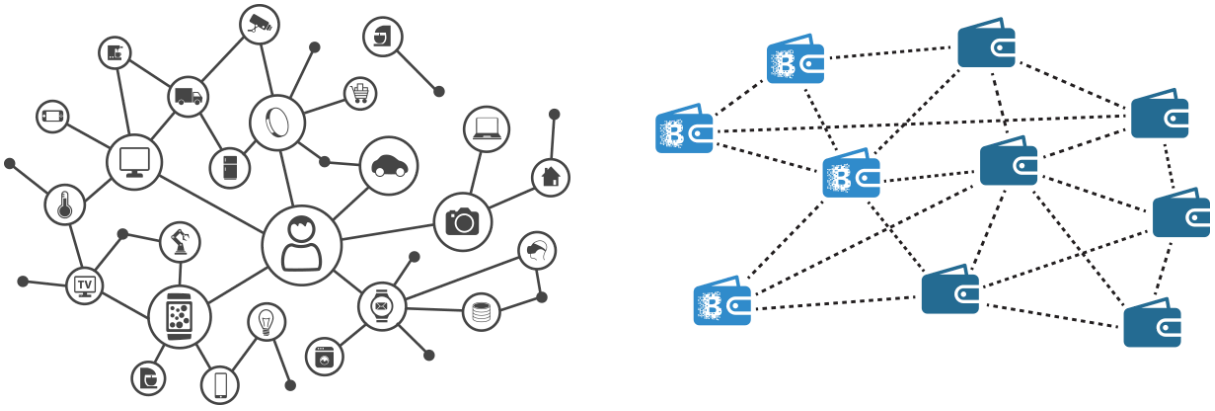

Figura 4: Comparación de la estructura de red entre IoT y blockchains

La integración de blockchains con IoT hace que sea fácil implementar la confidencialidad con integridad, una condición necesaria para garantizar conexiones confiables y un procesamiento seguro entre dispositivos. Para hacerlo, los dispositivos conectados responden a los ataques de fabricación y modificación, mejorando así la fiabilidad mutua de la comunicación. En particular, la cadena de bloques contiene una capacidad para hacer frente a los ataques externos a través de encriptación matemática compleja del libro mayor de transacciones contenido dentro del bloque. Además, el blockchain usa un método descentralizado en lugar de centralizado, que tiene la ventaja de dificultar que los hackers determinen el objetivo de ataque. Estas características minimizan el impacto de los ataques individuales en los dispositivos de IoT en todo el contexto.

Los servicios fiables proporcionados entre dispositivos IoT se pueden resumir de la siguiente manera:

- P2P y una estructura descentralizada distribuye los objetivos de ataque, lo que dificulta que el hacker identifique a los usuarios individuales como objetivos.

    ○ En el caso de una cadena de bloques privada, si el desarrollo de la informática distribuida se vuelve limitado, los problemas de seguridad se pueden resolver

[1] *Big data: Gigantesco conjunto de datos que las app tradicionales no logran manejar.*
[2] *IA: Inteligencia Artificial*
[3] *IoT: Internet de las cosas*

protegiendo la red a través del método de "*IP segura*", por lo que la amenaza de ataques externos disminuye mucho.

- Es posible mejorar la transparencia en todos los aspectos de las transacciones registrándolas en un libro mayor distribuido como una cadena de bloques, donde son fácilmente accesibles para futuras referencias si fuera necesario.

  ○ Esto garantiza la integridad de los detalles de la transacción para responder a los ataques de falsificación y alteración, lo que minimiza los costos de resolución de disputas, ya que todos los participantes prueban los detalles de la transacción.
- Se requieren procedimientos de autenticación y autorización para los dispositivos de IoT que son objeto de transacciones.

- En el caso de una cadena de bloques pública, es posible aumentar la eficiencia de la construcción y el mantenimiento de acuerdo con la distribución. Además, la descentralización generalizada del libro público mejora la eficiencia al reducir los costos transaccionales, por lo tanto, asigna de manera más eficiente los recursos públicos y privados.

Como resultado, la red que usa blockchain proporcionará un entorno confiable para ambos el administrador y el usuario para intercambiar una gran variedad de datos y valores.

Características de Hdac

Características principales de la plataforma Hdac

Las principales características de la plataforma Hdac son las siguientes:

Los activos digitales personalizados (tokens) se pueden crear y usar sin limitaciones, y el nombre del activo se puede definir o crear y distribuir libremente por un administrador autorizado. Este activo puede circular y usarse de manera similar a la moneda nativa existente.

Además, los activos que se generan para un negocio en particular o para fines específicos pueden intercambiarse con monedas nativas en una proporción adecuada según sea necesario.
Existen varias funciones de gestión de derechos, y un administrador que construye el primer nodo de cadena de bloques puede otorgar autorización a otros nodos. Los tipos de autorización pueden ser derechos de acceso, permisos de transmisión y/o recepción, derechos de minería, derechos para generar activos, etc., y pueden modificarse de manera efectiva durante la operación.

La plataforma Hdac proporciona las funciones adecuadas de instalación y configuración, y la cadena de bloques se puede configurar fácilmente según lo definido por el usuario. Además, esta nueva configuración de nodos se puede hacer simplemente con un solo comando de línea y ser parte de la cadena de bloques existente como un nodo completo y todas las configuraciones se copian y comparten automáticamente. En el caso de una cadena de bloques privada, esto puede ayudar a la minería de una manera más eficiente, a diferencia del enfoque relativamente antieconómico, como un sistema de prueba de trabajo [PoW][4].

Se proporcionan firmas multiusuario mejoradas, para servicios de soporte tales como liquidación segura de depósito en garantía. También proporciona la capacidad de comunicarse creando canales encriptados entre dos usuarios específicos. Junto con esto, también estamos planeando proporcionar funciones y control de IoT para el blockchain privado especializado en varios campos de aplicaciones, ideas e infraestructura para conectar los blockchains. Los detalles relacionados con el IoT se especifican en el "**Hoja de ruta de la tecnología Hdac**" en la página nro 21.

Hdac se basa en blockchains y acomoda todas las características de una blockchain típica. Las limitaciones del blockchain en sí mismo están evolucionando una por una a lo largo del tiempo.
Hdac difiere de otras plataformas basadas en blockchains, al haber modificado o complementado varias funciones para distinguirlas en términos de capacidad, seguridad, funcionalidad y velocidad.

La capacidad limitada del bloque y la parte de datos adicionales del blockchain existente, se modificaron para usarlos de manera flexible en la parte de carga de datos. Esto permite varias aplicaciones usando el blockchains.

En el caso de una cadena de bloques privada respaldada por la plataforma Hdac, se debe mejorar la seguridad. Al generar números aleatorios para crear claves de identificación a través de un generador de números aleatorios cuánticos, es posible eliminar la posibilidad de piratear a través del análisis de patrones numéricos, lo que mejora en gran medida la seguridad de la tecnología y las transacciones asociadas.

Además, proponemos un algoritmo de ePoW para el algoritmo de consenso para desarrollar el esquema de PoW existente para inducir el uso eficiente de la energía y la distribución equitativa. Además, al agregar un concepto de permiso que puede otorgar derechos administrativos, solo un usuario específico en una cadena de bloques privada puede participar como un nodo completo de una cadena de bloques. Si la plataforma existente usa unidades token comunes, Hdac puede construir múltiples blockchains de acuerdo con el uso, y además, proporcionará un modelo de servicio que se puede usar para crear y distribuir tokens personalizados.

[4] *Es un sistema que, para evitar comportamientos indeseados (por ejemplo ataques de denegación de servicio o spam), requiere que el cliente del servicio que se realice algún tipo de trabajo que tenga cierto costo y que es verificado fácilmente en la parte del servidor.*

Hemos examinado varias cadenas de bloques que son adecuadas para implementar entornos de IoT desarrollados para el procesamiento en tiempo real. Es difícil implementar esto con Bitcoin. Ethereum tiene un modelo más útil para entornos de IoT, pero la mayoría de los dispositivos se desarrollan principalmente en lenguaje C, por lo que examinamos blockchain en C.
Sin embargo, puede desarrollarse para ser compatible con Ethereum en el futuro. El token IOTA tiene el potencial para hacer frente a grandes volúmenes de transacciones, pero no es una tecnología de cadena de bloques estándar a la que nos dirigimos y, por lo tanto, la excluimos. Después de revisar muchas otras plataformas, elegimos **MultiChain**, que efectivamente puede implementar blockchains privados basados en el Bitcoin más comúnmente utilizado.

Hdac está basado y mejorado a partir de MultiChain, que es una cadena de bloques mejorada de Bitcoin. Hdac ha explorado específicamente varias blockchains para apoyar de manera eficiente los entornos de IoT y para proporcionar diversos servicios de manera rápida y efectiva a blockchains privados. También hemos establecido la cadena de bloques apropiada como Multichain e hicimos mejoras. Por lo tanto, Hdac tiene algunas de las características del Bitcoin, así como las características optimizadas de MultiChain para blockchains privados. Hdac proporciona una base para actuar como una plataforma para el IoT. Se puede aplicar a diversos campos de servicios, como finanzas, IoT, distribución, logística y gestión de datos públicos, basados en velocidades de procesamiento de transacciones rápidas y escalabilidad de transacciones.

Bitcoin genera un bloque cada 10 minutos, y Ethereum genera un bloque cada 12 segundos. Cuando se considera el tiempo que se comparte en la red, toma de uno a dos minutos o más para verificar el resultado de la transacción de transferencia.

Considerando esto, Bitcoin procesa aproximadamente 7 transacciones por segundo [**TPS**] y Ethereum procesa aproximadamente 25 TPS. En particular, Bitcoin está limitado a un máximo de 1 MB en el tamaño de bloque actual, y se propone una alternativa para aumentar el tamaño del bloque a través de SegWit2x.

Features	Bitcoin	Hdac	Ethereum
Principales características	Transacciones financieras (Script de Bitcoin)	"Blockchains amistosos del IoT Bloqueines públicos / privados"	Contratos Inteligentes C Contratos Inteligentes (Solidity, Serpent,etc.)
Algoritmo de consenso	PoW	ePoW, basado en al confianza	Actual: PoW Futuro: CASPER PoS
Velocidad de transacción	7 tx/sec	~160 tx/sec (public)	25 tx/sec
		~ 500tx/sec (privado)	
		1000 tx/sec (Objetivo)	
Tiempo De Bloque	10 minutos	3 minutos	12 segundos
Tamaño de Bloque	1 MB	Dinàmico (Max. (MB)	Dinámico
Datos Extra	80 Byte (OP_RETURN)	Dinámico (Máx. 4 Kb)	Dinámico (5 gas /byte)
		Dinámico (5 gas / byte)	
Topología	Blockchain público	Publico/Privado Blockchains	Blockchain Públique
		Blockchain Autorizado	Blockchain sin Permiso

Tabla 1. Comparación de las propiedades de criptomonedas

Hdac ha compensado estas deficiencias y ha asignado el tiempo de bloqueo a tres minutos, lo que representa la velocidad del tráfico rezagado del Tercer Mundo. El tamaño máximo de bloque es de hasta 8 MB y es variable.

El motivo de esta cifra es que la velocidad media del tráfico de Internet en el Tercer Mundo es de solo 1 ~ 2 Mbps. Por lo tanto, si Hdac puede acomodar solo una fracción de esta velocidad, se sugiere crear un entorno que pueda operar un nodo completo de la cadena de bloques de Hdac. Las transacciones a través de billeteras generales también están disponibles en entornos de poco tráfico. Las pruebas en un entorno interno limitado han demostrado que las transacciones estables se pueden lograr en grandes transacciones de aproximadamente 20 veces o más, lo que es más cercano al valor teórico en comparación con Bitcoin.

Hdac proporciona una forma de almacenar grandes cantidades de datos adicionales en una transacción como cadena de bloque orientada a IoT en el futuro. Además, el tamaño de la transacción se puede adaptar dinámicamente si es necesario para la seguridad de IoT y la expansión del servicio de aplicación.

Algoritmo de consenso

El Blockchain tiene las condiciones básicas necesarias para que todos los nodos que participan en la red, acuerden en cada paso de verificar que el bloque sea válido para conectar un nuevo bloque. Todos los nodos participantes (nodo completo) deberían poder identificar el mismo resultado con el mismo procedimiento, y todos los procesos de

verificación deben determinar el mismo valor. Además, el valor determinado debe ser el propuesto por un nodo específico.

Hdac blockchain, se basa en el método PoW como cadena de bloques pública. También es compatible con el método de minería para una cadena de bloques privada basada en confianza: esto es, un algoritmo de consenso basado en confianza para una cadena de bloques autorizada.

Aquí, la tarea de crear un bloque se conoce como "minería", y los nodos que participan en la minería se denominan "mineros". Cuando comienza una transacción de Hdac, transmite a los mineros datos informándoles sobre la transacción y fomentar la participación. Los mineros luego realizan cálculos aritméticos para verificar el bloque generado. El algoritmo de consenso de blockchain incluye PoW, prueba de participación [PoS][5] y prueba de participación delegada [DPoS][6]. Ese algoritmo de consenso determina aquellos que generarán un bloqueo a través de la realización de un proceso de cálculo que toma una cierta cantidad de tiempo entre numerosos participantes.

Este algoritmo de consenso desperdicia energía al consumir potencia de hash, para obtener una compensación de bloque en el competitivo proceso de minería. Además, el método PoW o PoS tiene el problema de que cuanto mayor es el poder de hash, o más participación hay, más se puede concentrar la acumulación de compensación o riqueza en un solo lugar.

De hecho, la minería se concentra en ciertas áreas de llamadas granjas de minería.

Hdac usa ePoW como un algoritmo de consenso para crear nuevos bloques y conectarlos a la cadena de bloques. ePoW se refiere a "PoW basado en oportunidades equitativas y ahorro de energía". El algoritmo de Hdac considera estos dos como su filosofía básica.

El algoritmo de consenso ePoW puede reducir el número de nodos que participan en PoW y motiva la participación de múltiples nodos de minería. Como resultado, pretendemos evitar el desperdicio de energía debido al excesivo poder de dispersión para la competencia minera y distribuir oportunidades equitativas de minería.

[5] *[PoS] es un protocolo de consenso distribuido para redes distribuidas que asegura una red de una criptomoneda mediante la petición de pruebas de posesión de dichas monedas.*

[6] *[DPoS] Es una variante del PoS, y permite que los nodos propietarios de monedas deleguen sus privilegios para construir nuevos bloques en un nuevo tipo de nodos llamados representantes.*

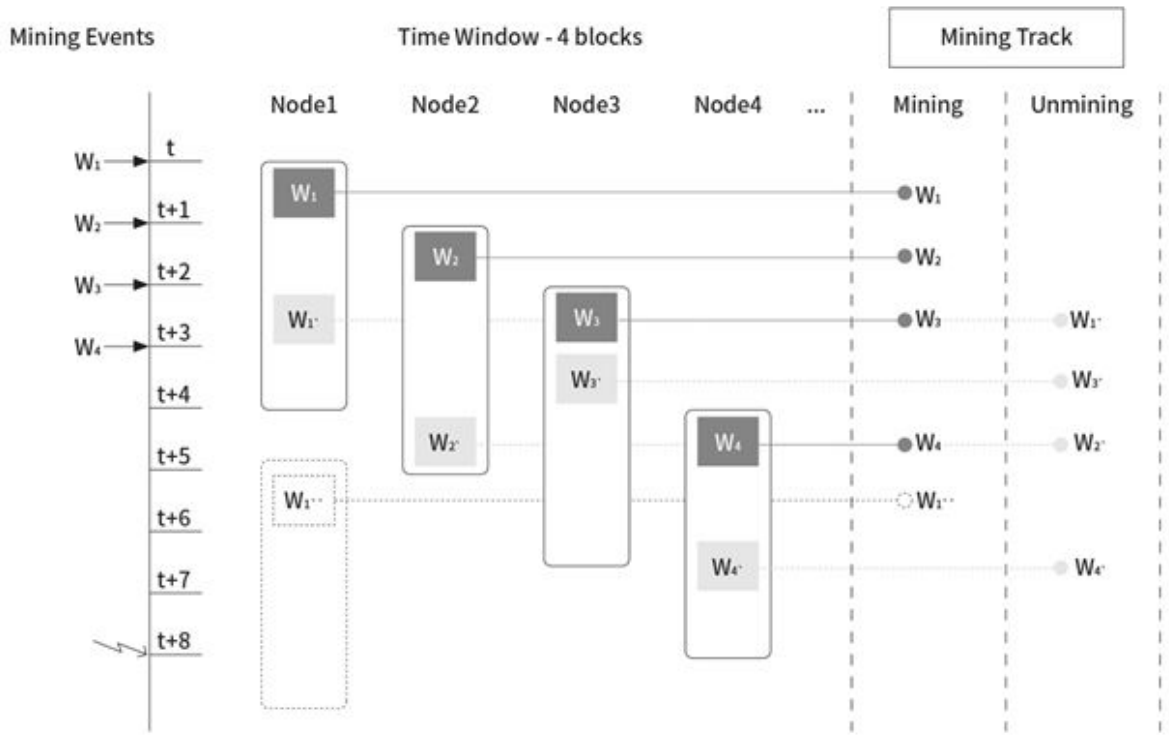

Figura 5: Algoritmo de consenso ePow

Hdac ePoW, es un algoritmo de consenso que reduce el monopolio de la minería aplicando el concepto de ventana de bloque. Reduce la energía perdida que se consume en en el cálculo de hash al evitar los intentos espontáneos de minería durante el período de aplicación de ventana de bloque una vez que la extracción es exitosa. Si un nodo tiene éxito en la minería, no se puede extraer ningún bloque nuevo durante el período de aplicación de la ventana de bloque. Incluso si un nodo codicioso descuida este mecanismo y logra minar un nuevo bloque, no se reconocerá como un bloque válido en toda la red blockchain de Hdac, eliminando así la necesidad de tratar de encontrar un bloque no válido.

El hash de bloque, debe cumplir con la especificación de datos de acuerdo con el grado de dificultad y no debe estar dentro de una ventana de bloque determinada (espaciamiento de tiempo). Este tamaño de ventana de bloque se puede expresar en la forma de una función de tiempo, Ws = f (t). "F (t)" es una función que aumenta en proporción al tiempo y, por lo tanto, el tamaño de la ventana también aumenta gradualmente con el tiempo. Esto significa que hay una gran oportunidad para los participantes iniciales, y con el tiempo cada nodo de minería se hace cada vez más difícil de monopolizar la minería y se puede lograr una distribución más equitativa.

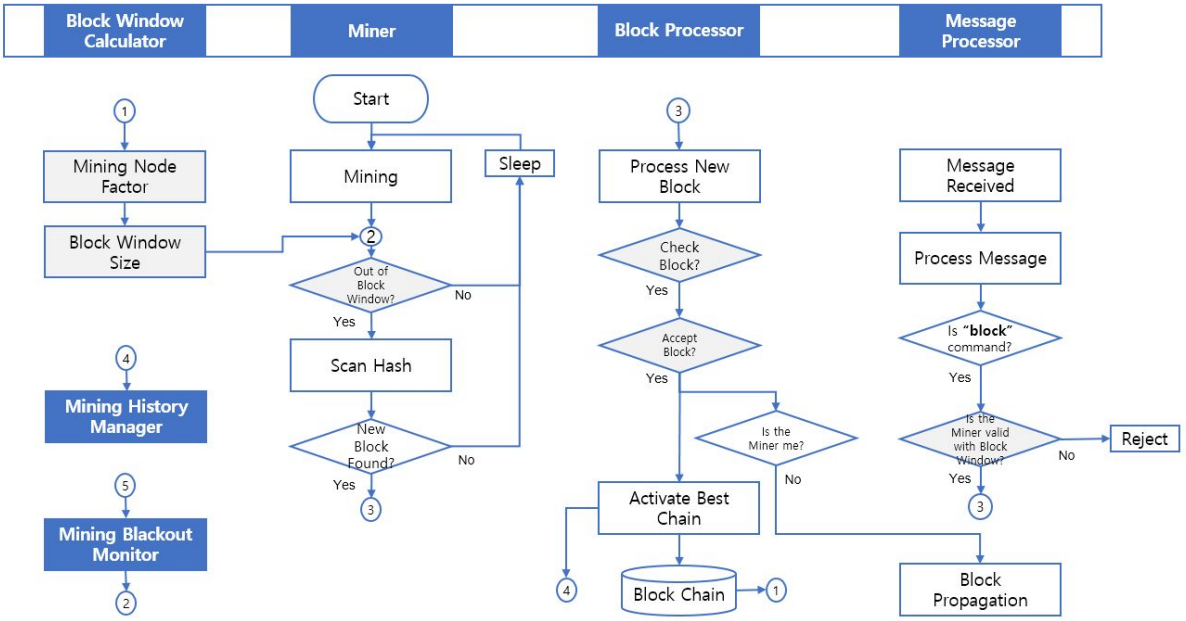

Figura 6: Diagrama de flujo de ePoW

La ventana del bloque ePoW es un sistema que da ciertas restricciones a los intentos de minería después de tener éxito en la minería en un cierto ciclo PoW.

El tamaño de la ventana de bloque (Ws) se define como,

*f(t)=[(N*0.7)x(nro acumulativo de bloques actuales (t))] / (nro de bloques acumulativo durante 10 años (tm))*

El nodo el factor (N) se calcula a partir de la lista de nodos de minería exitosos recientes. La razón por la que el tiempo de llegada del tamaño máximo de ventana de bloque (Wm) es de 10 años es porque está configurado para alcanzar el punto de más del 80% de la generación de token total en ese momento.

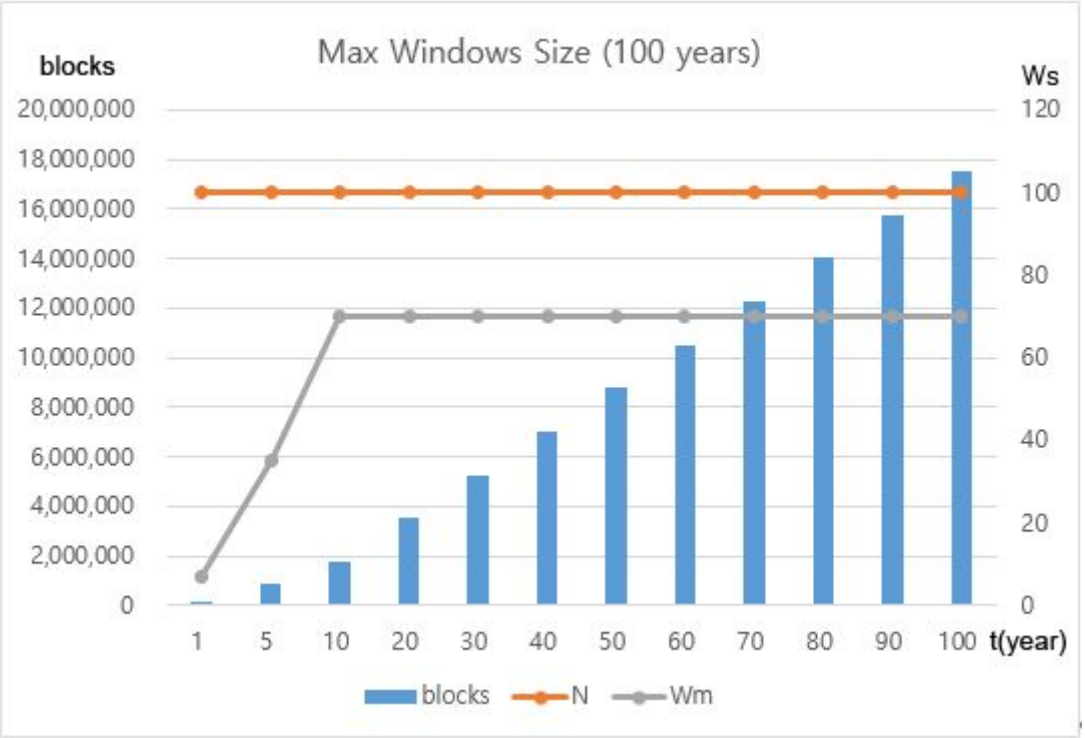

Figura 7: Simulación de ventana de bloque (100 años)

Si el tamaño de la ventana del bloque se simula durante 100 años con un factor de nodo de minería de 100, como se muestra en la figura 7. La ventana del bloque aumenta gradualmente desde el momento en que se inicia el bloqueo desde la génesis de su creación, y el tamaño aumenta o disminuye según el factor del nodo después del punto (tm) cuando se alcanza el tamaño máximo de la ventana del bloque.
Hemos completado el desarrollo de ePoW, y los resultados de la distribución de la minería de bloques de ePoW y los niveles de consumo de energía se publicarán por separado en el sitio web más adelante.

El algoritmo de consenso ePoW de Hdac apoyará una variedad de métodos técnicos para crear un entorno de minería saludable. Se está desarrollando un módulo de seguridad de hardware por separado [HSM] para mejorar la seguridad del nodo de minería, donde esta será una opción disponible para seleccionar.

Mejora de la seguridad cuántica de números aleatorios

Las plataformas basadas en Blockchain ya han sido verificadas con resultados de alta seguridad. La clave privada, la clave pública y la dirección de la billetera utilizadas en las transacciones basadas en cadenas de bloques se crean utilizando un número pseudo aleatorio. En casos recientes, se ha encontrado una vulnerabilidad de seguridad de número pseudoaleatorio mediante el análisis de los patrones de esos números y la creación de valores para fines específicos. Ha habido varios intentos de compensar estas debilidades, y ha surgido un método de número aleatorio cuántico que no puede analizarse teóricamente.

Hdac propone un método para reemplazar la generación de números aleatorios con números aleatorios cuánticos para un blockchains privado.

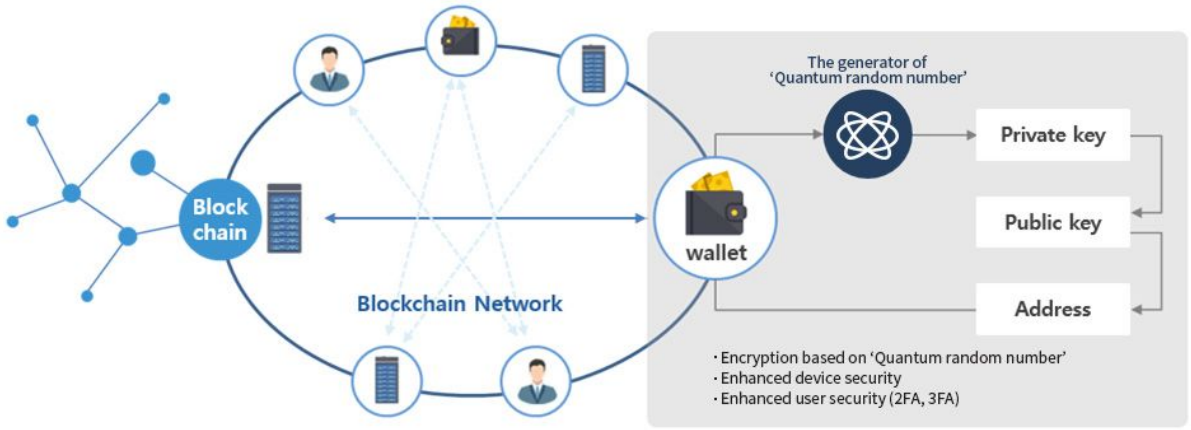

Figura 8. Seguridad mejorada del dispositivo usando números aleatorios cuánticos

El Blockchain utiliza números pseudoaleatorios cuando crea claves privadas, claves públicas y direcciones de billetera. Las direcciones de monedero creadas por este proceso están representadas por valores hash a través de la tecnología de incriptación hash tipo SHA256. Además, de acuerdo con la notación, la letra de inicio de la dirección se compone de la siguiente manera, y Hdac usa "H." De esta manera, los diferentes caracteres en el primer carácter de cada dirección se pueden considerar como un tipo de sistema de protección que impide a un usuario específico de enviar un token con una moneda diferente.

Si una moneda específica usa las mismas iniciales, puede haber errores de transmisión debido a otras monedas porque el primer carácter de la dirección se duplicará. Por lo tanto, Hdac agregó la cadena "Hdac" a la suma de comprobación para evitar esto.

Generación de Tokens, minería y sistema de recompensas

En comparación con el Bitcoin, la política de emisión de Hdac es la siguiente:

La cantidad total de tokens de Hdac es de 12 billones de **DAC**. La primera recompensa de bloque comienza con 5,000 DAC antes de dividir el token. El ciclo de generación de bloques es de 3 minutos, se establece para reducir la recompensa a la mitad por cada 1,032,000 bloques. Es decir, la recompensa del bloque se reduce a la mitad aproximadamente cada 71 meses desde que se creó el bloque inicial.

Un 7% de los tokens se usará para crear infraestructura y un ecosistema para implementar la tecnología Hdac, impulsar su transacción y también para la administración de la liquidez. Otro 7% se distribuirá a los participantes que donaron a la Fundación Hdac en preventa y el evento de generación de fichas.

Tal mecanismo es una política destinada a mantener el valor intrínseco del token al reducir su suministro. La cantidad total de tokens generados es fija, en lugar de tokens inflacionarios donde el activo generado aumenta hasta el infinito y el valor del activo disminuye. Es importante ver si el precio de equilibrio se puede mantener en el punto donde el comprador y los objetivos de resguardo o holdeo, del vendedor se encuentran.

Los mineros que quieran extraer tokens vía minado utilizando la red blockchain de Hdac recibirán recompensas por cada bloque logrado, junto con las tarifas de transacción como recompensas. La recompensa por cada bloque, se reduce a la mitad aproximadamente cada 6 años, esto aumenta gradualmente el número de transacciones incluidas en un bloque, logrando así la cantidad para la recompensa necesaria y logrando una tarifa más baja para cada transacción.

Hoja de ruta de la tecnología Hdac

Configuración de IoT Blockchain Network

La red blockchain de IoT es una cadena de bloques privada autorizada que se registra después de ser autenticada y puede operar en una red blockchain. Por lo tanto, se puede decir que su personalidad es diferente de un blockchain público que tiene acceso a la red.

Los componentes de la red blockchain de IoT son los siguientes.:

- **Nodo de Blockchain**: Registra todos los bloques de transacción como un nodo completo. Almacena la información de configuración relacionada con el dispositivo del usuario, el control del dispositivo a dispositivo, la facturación y la administración realizada por el administrador.

- **Administrador**: Es una persona que registra usuarios, puertas de enlace y dispositivos en blockchain y otorga acceso entre ellos. La configuración se almacena de forma segura en el nodo completo de la cadena de bloques y se transmite a los siguientes usuarios, puertas de enlace y dispositivos a través de la red. Cada usuario y dispositivo, mantiene la última configuración relacionada con ellos. También se puede integrar sistemáticamente con el entorno operativo IoT existente.

- **Usuario**: Es una persona o dispositivo con un programa que se ejecuta como un nodo simple que no almacena bloques.

- **Gateway**: Es una unidad utilizada para controlar muchos dispositivos o sensores reales o simulados. Puede analizar detalles del contrato IoT y luego transmitir a dispositivos simulados o sensores. Cada dispositivo o sensor está conectado con una dirección individual.

- **Dispositivo**: Es un dispositivo que está conectado a una puerta de enlace o un nodo simple que no almacena bloques. Corresponde a direcciones individuales y también puede analizar los detalles del contrato de IoT y operar con ellos.

Como se ilustra en la Figura 7 a continuación, el usuario envía el contrato de IoT que está conectado con un programa a la puerta de enlace o a un dispositivo. El dispositivo analiza y opera el contrato IoT recibido. El usuario puede enviar transacciones que acceden o controlan puertas de enlace o dispositivos explícitamente autorizados.

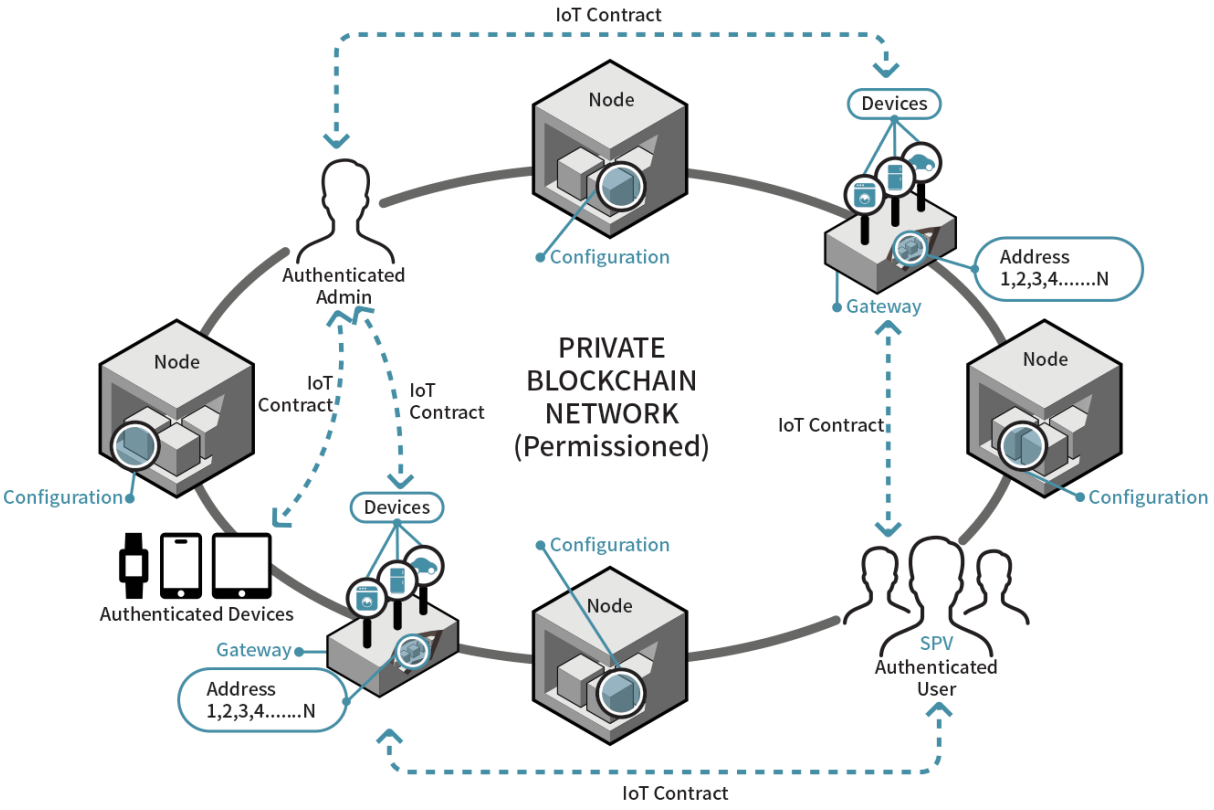

Figura 9: Estructura de la red blockchain de IoT

Mapeo de dispositivos de usuario en la cadena de bloques IoT

El usuario en la cadena de bloques IoT debe poder acceder al dispositivo de acuerdo con las reglas de derechos de acceso para controlar el dispositivo. El usuario también debería poder controlar el equipo específico de acuerdo con la configuración o solo leer el estado del equipo, también debería ser posible hacer que los usuarios generales no puedan acceder a ciertos equipos. Esto permite al administrador establecer permisos de acceso usando las direcciones de los usuarios, dispositivos o puertas de enlace. Esta configuración de acceso correcto se almacena en todos los nodos completos de la red blockchain, y también se comparte entre todos los nodos, puertas de enlace y dispositivos.

El acceso y control de usuarios y dispositivos, y la autorización de pago, se registran de forma segura en el blockchain. El contrato de IoT, puede llevarse a cabo después de que se verifique la autorización mediante la comparación con este registro cuando se produce la transacción.

En los entornos operativos generales de IoT, a menudo se otorgan estos permisos.

Por lo tanto, la cadena de bloques de IoT puede ser útil para usar en combinación con el entorno de IoT existente.

Los tipos de asignación de autorización son los siguientes:

- Asignación de dispositivo de usuario y puerta de enlace.
- Asignación de usuario a usuario.
- Asignación de dispositivo a dispositivo vía puerta de enlace.

Los derechos de asignación son los siguientes.

- **Derechos de acceso:** Otorga el derecho de acceso al equipo. Podrá especificar una calificación o nivel de acceso mínimo. Un usuario o dispositivo tendrá una calificación, lo que significa que solo se puede acceder a una calificación o nivel, específica o superior. Si el acceso no es posible, todos los derechos a continuación no están disponibles.

- **Derecho de lectura:** Es un derecho para leer el estado actual, y la autorización detallada se puede especificar como una cadena separada, y el dispositivo puede interpretarla para determinar si es aplicable o no.

- **Derecho a controlar / escribir:** Es el derecho a controlar el dispositivo o cambiar el estado. La autorización detallada se puede especificar por separado, y el dispositivo puede interpretarla para determinar si es aplicable o no.

- **Derechos de pago**: Especifica los derechos configurables relacionados con pagos pendientes y/o automáticos. La autorización detallada se puede especificar por separado, y el dispositivo puede interpretarla para determinar si es aplicable o no. El método de limitar el monto máximo de pago y el monto máximo de pago único durante un período específico es posible.

- **Otros derechos (que especifican los derechos detallados por dispositivo):** otros derechos detallados se pueden especificar como un código o cadena separada, y el dispositivo puede interpretarlos para determinar si son aplicables o no. Como este detalle es un método para depender del dispositivo, aquí no se especifican medidas de control específicas para todos los dispositivos.

Se determina que todas las transacciones que se usan esta red blockchain se transmitan según el derecho de acceso. Es decir, si un usuario A no tiene acceso a un dispositivo B pero aún se produce una transacción de A a B, el dispositivo B y todos los nodos de cadena de bloques rechazarán esta transacción. En este caso, el error puede ser reportado al nodo de detección de intrusos en el blockchain, y el administrador puede verificar inmediatamente los detalles y actuar en consecuencia..

Después de que el administrador configura la autoridad entre el primer dispositivo de usuario o dispositivo a dispositivo, los derechos de cada usuario y dispositivos se pueden ajustar si se realizan cambios en la red de blockchain. Además, cuando se agrega o elimina

un dispositivo, se debe realizar una asignación correspondiente. Los derechos básicos se pueden especificar en los casos en que se agrega un nuevo dispositivo según la configuración prevista.

El proceso de asignación de derechos de acceso según el dispositivo, puede ser bastante complejo en algunos casos. Por lo tanto, es posible intentar agrupar usuarios o puertas de enlace con dispositivos en grupos específicos para manejar de manera efectiva dicha asignación de derechos, y también, puede proporcionar una interfaz de programación de aplicaciones de usuario [**API**] o un comando en forma de script, para controlar los complejos mapeos. En algunos casos, la asignación de dispositivo de usuario puede expresarse en formas más complejas con respecto a la ubicación y el estado de tiempo y espacio. En esta sección, solo se presenta la forma genérica de asignación de dispositivos.

Este método de mapeo de dispositivo de usuario ya se está utilizando en la industria de la IoT, y será posible operar mediante el sistema de gestión existente para tener el máximo efecto mientras se minimiza la modificación a través del enlace comercial apropiado con la cadena de bloques.

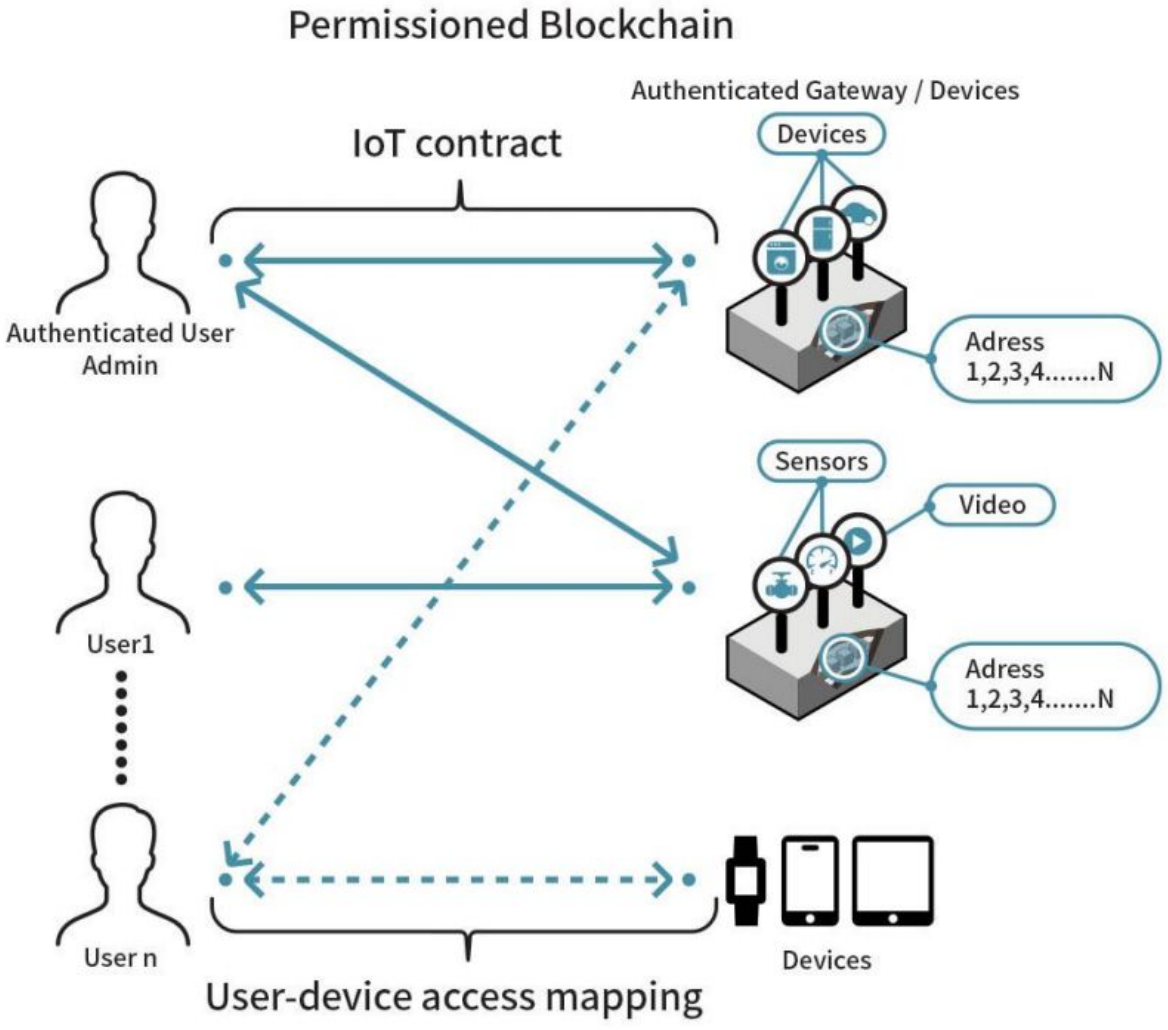

Figura 10: Ejemplo de mapeo entre el usuario y un dispositivo en la cadena de bloques privada

Contrato de IoT

El contrato de IoT es un concepto donde el objeto del contrato inteligente se propaga a los dispositivos del IoT. Esto permite que un programador puede crear un programa que controle la operación del dispositivo del IoT. Es decir, crea un contrato inteligente para el IoT y envía un contrato del IoT a un dispositivo específico para realizar trabajos, pagos y liquidaciones automatizados. El contrato de IoT es una transacción que transfiere comandos de control entre el dispositivo del usuario o entre dos dispositivos, que podrán usar esta transacción en relación a un dispositivo de usuario o también dos dispositivos, por ejemplo de autenticación, que se describiremos más adelante.

Antes de usar esta transacción, el usuario y el dispositivo deben estar registrados en la red blockchain a través del procedimiento de autenticación. En el caso del usuario, solo el usuario autorizado a través de la autenticación de dos factores, debería poder acceder a la red blockchain. Como método de autenticación de usuario, se puede agregar una identificación, o una contraseña, o una autenticación biométrica (huella digital, iris, reconocimiento facial, etc.) y la verificación se realiza a través de estos métodos..

Dado que el dispositivo es difícil de registrar por sí mismo, el administrador primero debe identificarlo y registrarlo. Se están considerando varios métodos para determinar la identificación unívoca del dispositivo. Primero, no hay problema si el dispositivo tiene una identificación única (como podrìa ser un chip de seguridad). Sin embargo, si este no es el caso, puede registrar el hash de información único, o la dirección MAC, o el ID de la CPU, como también el ID del disco, o una imagen del sistema operativo, también es posible, utilizar la dirección del monedero electrónico, y otros varios métodos, para que el dispositivo pueda desconectarse automáticamente de la red blockchain e informar al administrador si ha sido manipulado.

Dependiendo del contrato IoT, cuando cambia el estado de un programa que se ejecuta en el dispositivo, puede ocurrir que manipule el mismo, y realizar pagos automáticos entre dispositivos o transmitir información de estado o datos a una ubicación predeterminada. En este momento, el pago automático entre dispositivos se denomina “Machine Currency”, y el pago se puede realizar solo a las direcciones permitidas de antemano. El dispositivo A, que recibe los comandos, puede transmitir información de estado o de control a otro dispositivo llamado B, de acuerdo con el contenido del programa y también puede controlar el dispositivo B.

El control solo es posible cuando la configuración está registrada y tiene derechos en la red blockchain. Al proporcionar el servicio de contrato IoT a través de Hdac, es posible el control, el pago y la administración entre usuarios y dispositivos, así como también entre dispositivos. A través de esto, se puede proporcionar el pago entre máquina ya máquina.

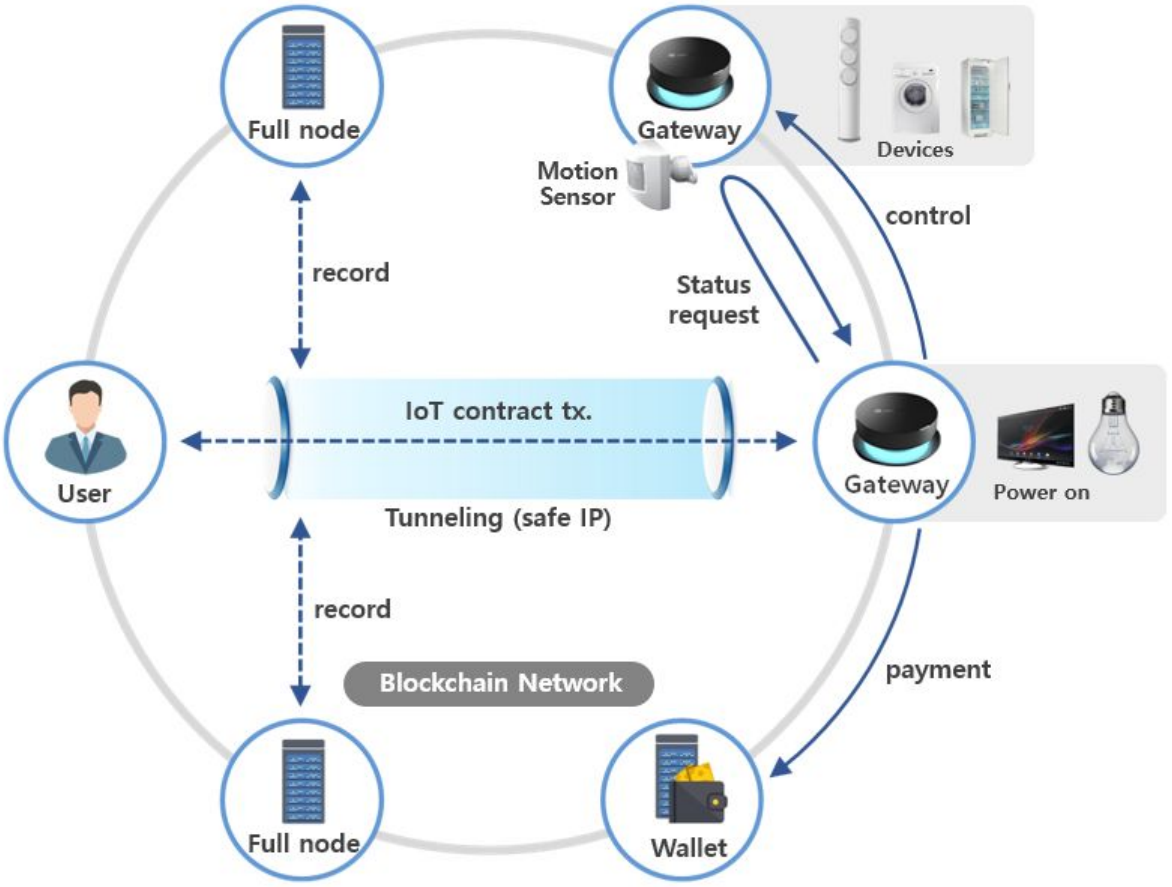

Figura 11: Estructura del servicio de contrato de IoT

Se puede agregar un programa automatizado al contrato IoT para que el dispositivo funcione y pueda ser controlado por el el usuario, se le informe sobre el estado del mismo, proceda automáticamente con los pagos si se cumple una determinada condición, etc. Este programa puede ofrecer datos formateados en JSON simples de acuerdo con las condiciones del dispositivo, y se puede proporcionar con un tipo de API programable que puede manejar información más compleja.

En dispositivos de mayor rendimiento, se agrega una programación de alto nivel más compleja y sofisticada al contrato IoT y se entrega al dispositivo, y puede ser interpretada y procesada a través de un intérprete o máquina virtual que opere dentro del dispositivo.

La forma más efectiva y conveniente de controlar los dispositivos de IoT en términos de velocidad y seguridad, es usar una API para desarrollar la programación del dispositivo.

En términos de flexibilidad, un intérprete o una máquina virtual pueden ser muy efectivos. En el caso de un intérprete o una máquina virtual, no es necesario cambiar el dispositivo, esto se soluciona cambiando el programa de control en el lado del usuario, para que se pueda aplicar de manera fácil y flexible. Sin embargo, el uso de un intérprete o una máquina

virtual requiere un nivel relativamente alto de potencia de cálculo y memoria, por lo que no se puede cargar directamente en los dispositivos de bajo rendimiento.

Por ejemplo, si hay 100 dispositivos de tipo A y se cambia la política para administrar este dispositivo, es mucho más eficiente y seguro cambiar el contrato de IoT del lado del usuario, que tiene derechos de control, en lugar de modificar o actualizar los 100 dispositivos. .

En el IoT, dado que una transacción debe realizarse en tiempo real, se registra una cantidad adecuada de dispositivos en la cadena de bloques. Si es el caso donde la red garantiza un rendimiento de procesamiento apropiado, puede procesar aproximadamente 500 tx/seg.
La cantidad de transacciones o el tiempo de respuesta que se puede manejar puede depender en gran medida del rendimiento de la red y del dispositivo.

En particular, cuando una transacción requiere alta seguridad, puede transferirse al dispositivo a través de un canal seguro completamente separado de la red normal, como una **VPN**. En otras palabras, puede hacerse inaccesible a través de la red pública intermedia. En el blockchain privado, el dispositivo y el nodo completo se pueden organizar en una relación N:1 donde los dispositivos de seguridad se utilizan para mejorar la seguridad del segmento de red. Si es necesario, el programa de usuario y el bloque de datos pueden encriptarse y transmitirse contemplando las cuestiones de seguridad del dispositivo.

Las especificaciones detalladas del contrato IoT son las siguientes.

- Transacción básica de blockchain
- Encabezado JSON definido por el usuario.
  - Consiste en información del usuario, tipo de usuario, contenido autorizado, comando y datos de procesamiento, método de respuesta, etc.
- Programa de usuario
  - Datos JSON adicionales, o lenguaje de programación de alto nivel, o información de objeto para ejecutar
  - Puede ser procesado por API, intérprete o máquina virtual
- Datos o flujo para ser utilizado en el programa de usuario
-

Encriptado	Transacción predeterminada de Blockchain	
	Encabezado JSON definido por el usuario	
	(Info de Usaurio.,Tipo de Usuario, Permiso, Codigo de Operación, Codigo de datos, Tipo de envio, etc.)	
	Programa de usuario (Script)	User Data (Binary)

Tabla 2: Estructura del contrato del IoT

El programa de usuario es un lenguaje de alto nivel, y puede interpretarse a través de un intérprete o una máquina virtual que tienen una sintaxis similar a C, que es familiar para los desarrolladores de IoT.

En este proceso, usaremos un intérprete de programa específico o máquina virtual para interpretar programas de usuario, pero mantendremos el código fuente y la interfaz lo más simple posible, para que los usuarios puedan agregar fácilmente un nuevo tipo de intérprete o máquina virtual.

Seguridad para el Blockchain del IoT

La principal preocupación del IoT es, un problema de seguridad para dispositivos IoT. La mayoría de estos problemas de seguridad se pueden resolver adaptando cadenas de bloques IoT. Sin embargo, dado que la cadena de bloqueo IoT no puede resolver el ataque de denegación de servicio [DoS], la denegación de servicio distribuida [DDoS] y los ataques de rastreo, se debe considerar la conexión con otras tecnologías de seguridad.

Para blockchains privados, la seguridad podría mejorarse mediante el uso de un canal seguro separado, esto separa la red entre nodos y dispositivos o entre nodos de blockchain y usuarios. Este método se puede implementar mediante hardware o software blockchain, que se puede montar en un dispositivo. Este método tiene la ventaja de que no es necesario cambiar un nodo existente de blockchain o la configuración del dispositivo. Esos dispositivos generales que no pueden transferir el código blockchain, se pueden controlar a través de un nodo adaptador de dispositivo por separado.

En este caso, la transacción se puede controlar cambiando la señal para controlar directamente el dispositivo. Además, si es necesario, pueden instalarse otros diversos métodos de seguridad dentro del servidor para evitar amenazas. Actualmente, los dispositivos inteligentes tienen protocolos integrados tales como **Transport Layer Security** [TLS] o **Secure Sockets Layer** [SSL].

También tienen varios sistemas de seguridad contra señales de control. Un contrato de IoT, que es una transacción encriptada entre usuarios y dispositivos, puede admitir dispositivos mediante TLS y/o SSL y varios protocolos. Un Contrato de IoT, una transacción encriptada entre usuarios y dispositivos, puede admitir dispositivos que usan TLS y/o SSL y varios protocolos. Además, los dispositivos de bajo rendimiento que tienen dificultades para realizar un cifrado complejo pueden usar selectivamente **IDEA** (algoritmo internacional de cifrado de datos) o **ARIA** (algoritmo criptográfico genérico de 23 bloques con estructura SPN revolucionaria y optimizada para entornos livianos e implementación de hardware) o con **AES128** a **AES256** algoritmo estándar de cifrado de clave simétrica, todo ello considerando el tipo de dispositivo.

Debido a que el programa dentro del dispositivo necesita ser cambiado, este método es difícil de aplicar a un dispositivo que ya ha sido creado. Por lo tanto, estos dispositivos de muy bajo rendimiento se pueden clasificar como dispositivos simulados y se pueden administrar mediante puertas de enlace que operan a través de canales seguros independientes.

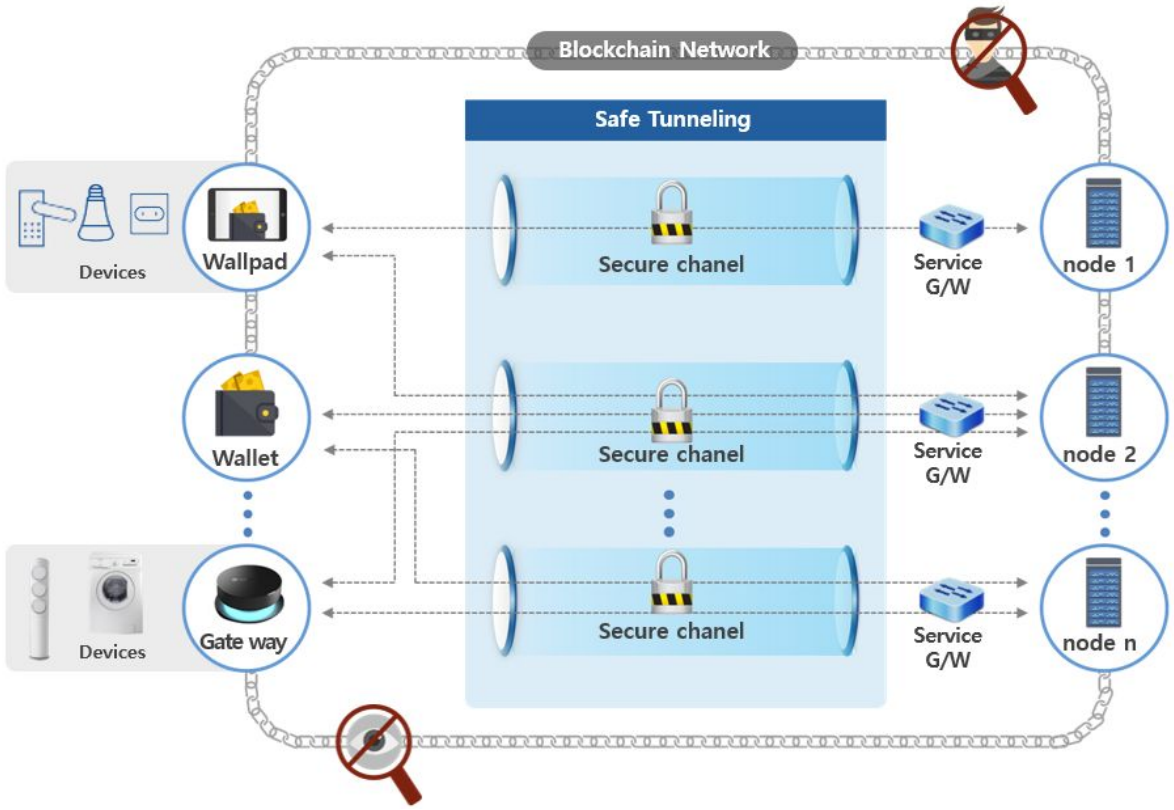

Figura 12: Seguridad de red mejorada mediante una cadena de bloques

Incluso si el blockchain del IoT está bien integrado con los procesos de seguridad existentes, aún puede haber vulnerabilidades de seguridad inesperadas. Por lo tanto, es necesario no sólo supervisar constantemente los cambios de configuración de usuario, la adiciones de dispositivos, los cambios de configuración y los cambios de asignación entre el usuario y el dispositivo en la cadena de bloques de IoT, sino también comparar con las configuraciones anteriores y detectar los cambios de contenidos. Estos grandes datos se pueden buscar y analizar utilizando herramientas equipadas con aprendizaje automático.

Además, si los contenidos principales cambian, es necesario promulgar el proceso de intentar la autenticación secundaria para el administrador, y debería poder hacer frente a varios ataques de red, incluidos los DoS y DDoS realizados en la red. Por lo tanto, uno o más nodos deben operar como watchdogs, para detectar transacciones anormales y generar eventos. En cada nodo, la función de supervisar el estado del servidor se puede agregar y notificar al administrador, que puede actuar antes de que la cadena de bloques se vuelva difícil de operar.

Los siguientes eventos pueden ser detectados por el nodo watchdog:

- **Transacciones anormales:** Son las transacciones que no tienen una dirección de destino y que causan tráfico excesivo anormal, las transacciones no autorizadas y contratos de IoT.
- **Detectando el estado de cada nodo**: Si es un nodo completo, monitorea la capacidad del disco, el estado del servidor y el estado de la red, y notifica al watchdog ,cuando se alcanza un cierto nivel.
- **Supervisión de cambio de asignación de dispositivo a dispositivo**: Detecta cuándo se cambian los contenidos. Realiza un seguimiento de los cambios cuando están prohibidos los cambios en la asignación.

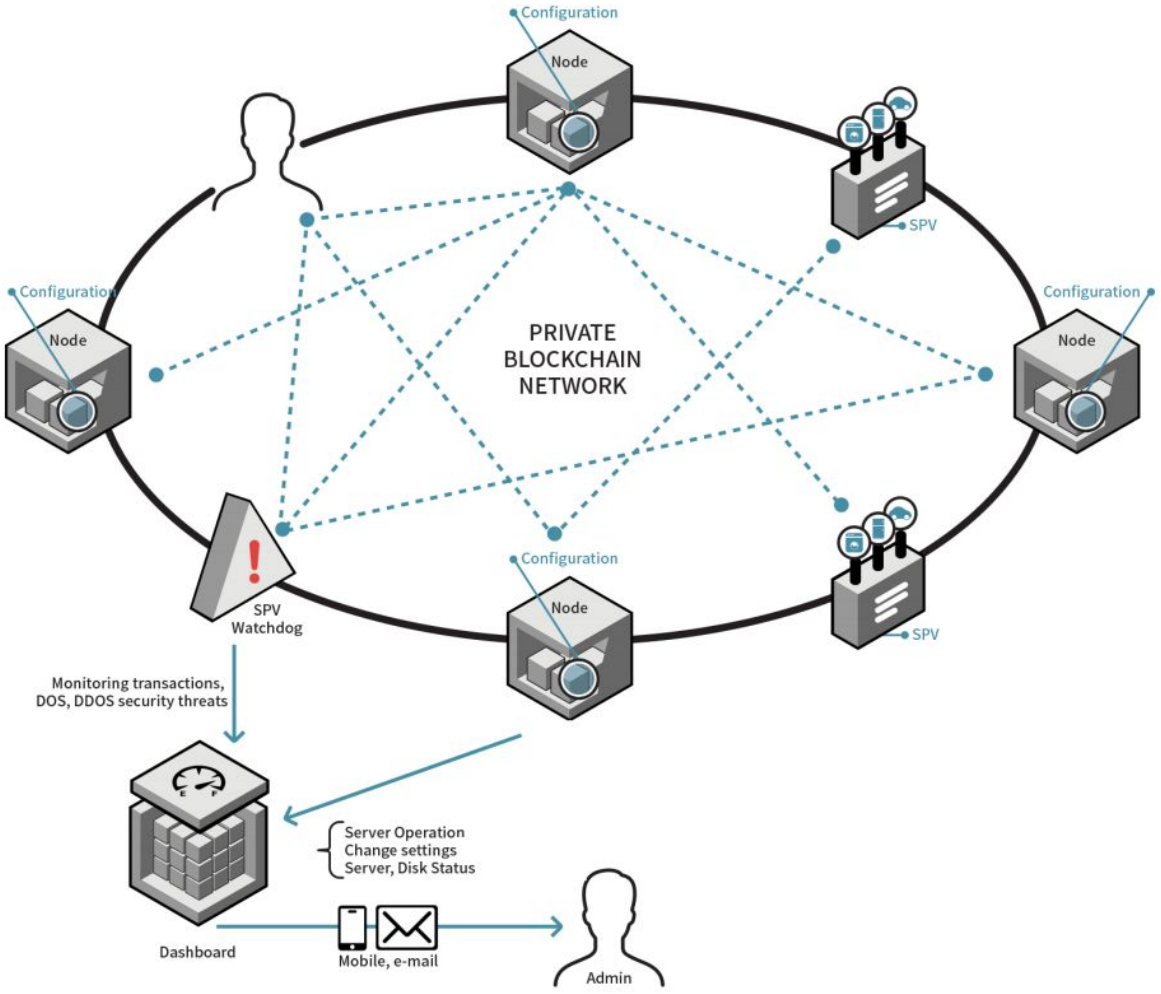

Figura 13: Detección de amenazas en la cadena de bloques privada IoT

Ecosistema Hdac

Estrategia del desarrollo del ecosistema Hdac

Para que Hdac evolucione de forma continua y estable, la **Fundación Hdac** realizará actividades de marketing y relaciones públicas, mientras que **HDAC Technology AG** implementará **Hdac Core Technology,** desarrollando la plataforma de última generación de fintech. Estos equipos se esforzarán juntos para desarrollar el progreso tecnológico y el ecosistema de sinergia de Hdac con el fin de crear un entorno de círculo virtual para el desarrollo tecnológico global, como se muestra a continuación.

Construction of Hdac Blockchain Core Plataform	>	Construcción del servicio Hdac Plataform	>	Composición de Hdac Eco-system
Construction of HDac Block chain plataform		Desarrollo del servicio global de pago Iot (promoción del servicio de plataforma de primer paso).		Blockchain para el pago IoT.
Establishement of mind to long term bussines vision through ster by ster implementation plan.		Finalización del desarrollo de la convergencia de Blockchain y IoT, y asegurando el poder económico y el crecimiento estableciendo las bases de la estandarización internacional.		estandarización global de la plataforma y crecimiento como operador de I + D
Progress of Hdac PoC and global ICO		Derivación y quetificación de la nueva perspectiva de negocio.		Establecimiento de una imagen global de Hdac Pagos por promoción global del servicios de la plataforma de pago de IoT.
Successful entrey of cryptocurrrency market		Aspectos legales, institucionales y regulatorios.		Establecimiento de un ecosistema de pago Hdac IoT a través de la vinculación y la expansión de servicios de plataforma de pago IoT
Listed on the cryptocurrency international exchange		Nuevo aspecto tecnológico del pago IoT		Expansión de la convergencia y descubrimiento de una nueva BM para la construcción y expansión de ecosistemas
		Temas relativos a negocios digitales		
		Mercado global y temas relativos aBigData.		

Figura 14: Estrategia del desarrollo del ecosistema Hdac

Miembros y Socios del Ecosistema

La Fundación Hdac, **Doublechain**, **Hyundai Pay** y **DEXKO** han formado la Comunidad de Transformación Digital para el desarrollo de tecnología/aplicaciones centrales de Hdac, así como su activación. Además, estamos en proceso de cooperación con varios socios: como:

- **WisBase**, que se especializa en el diseño y ajuste de grandes bases de datos;
- **PnP Secure**, que es una compañía de soluciones de protección de información;
- **EYL**, que es un desarrollador de chips de números aleatorios cuánticos;
- **INTO Information**, un desarrollador de tecnología original y desarrollo de servicios para diversas industrias; proveedor de solución lógica de red cerrada
- **ARAD**; Socio de tecnología de dispositivo
- **IOT MODA; y Mill Corp.**

También estamos colaborando con Intel para desarrollar IoT y soluciones de seguridad de acceso de reconocimiento facial.
En diciembre de 2016, **Hyundai BS&C** y **Doublechain** firmaron un MOU para lanzar un negocio de tecnología financiera basado en blockchain. Y estamos persiguiendo un proyecto conjunto para maximizar la eficiencia del desarrollo / operación de la plataforma basada en blockchain, y desarrollando las soluciones de convergencia IoT y blockchain.

En junio de 2017, se lanzó **HyundaiPay**, la compañía de fintech especializada en blockchain, para el avance de la tecnología blockchain y el lanzamiento temprano de varios servicios.

El 20 de julio de 2017, **HyundaiPay** y **Doublechain** firmaron una alianza estratégica con **Elasticsearch Korea**, una gran compañía de datos y aprendizaje automático, para el codesarrollo de un negocio de fintech/blockchain basado en Hdac.

Abriremos el primer café blockchain de Corea en diciembre de 2017 y planeamos operar una variedad de servicios basados en Fintech on/off-line utilizando Bitcoin

Ecosistema	Socios	Acuerdos y Roles
DTC (Comunidad de Transformación Digital)	Hyundai Pay	DTC (Comunidad de Transformación Digital) Soporte de desarrollo central Hyundai Pay Blockchain, Mejora y activación del valor Hdac
	Doublechain	Blockchain Core / Platform Development, Virtual account development
	Korea Digital Exchange (DEXKO)	Digital Asset Exchange (inc. Hdac)
IoT Laboratorio de tecnología de convergencia	Hyundai BS&C	Smart IoT (HERIOT, etc.), Smart IoT Home Technology Research Collaboration
Aplicación de la tecnología	EYL	Tecnología Quantum random number, soporte de plataforma
	INTO Information	Web Firewall, Soporte de cumplimiento de seguridad
	MODA	IoT dispositivo Gateway desarrollo y construcción
	WisBase	DB / tuning de gran capacidad
	ARAD Networks	Technical Support for safe IP
	Elasticsearch	Search engine, Big data preprocessing, Technical Support for machine Learning

	Ripple	Fabricación de productos IoT y PC Industrial

Tabla 3: Miembros del Ecosistema

Línea de tiempo del desarrollo del ecosistema Hdac

Año	OBJETIVOS
2017	Evento de creación de Hdac - Lanzamiento del algoritmo de consenso de Hdac - Finalización del entorno operativo Hdac Prueba de campo (ASM mining pool, Wallet1.0, Explorer, etc.) - Versión H / W Wallet (KASSE 1.0), ASM (Advanced Security Module) Ver 0.9 - Liberar la API de aplicaciones de Hdac (ASM mining, Wallet, Explorer)
2018	Lanzamiento del entorno operativo Hdac (ASM 1.0 mining pool, wallet2.0, etc.) - Hdac IoT Contract PoC - Autenticación IoT y control de dispositivos (Smart Home PoC) - Private Blockchain PoC (Game Token, sitio POS Hdac * T) - Smart Poo difusión IO
2019	Lanzamiento de la Aplicación práctica de Hdac IoT Contract & Smart Home (HerIoT) - Lanzamiento Aplicación práctica de Hdac IoT Contract & Smart Factory (control de Mando) - Hdac Public-Private Hybrid Blockchain Uso-desarrollo de casos
2020	Desarrollo de la blockchain de procesamiento de transacciones de alta velocidad IoT Blockchain - Lanzamiento de mejoras privadas de Blockchain Security, módulo de seguridad avanzada versión Ver 2.0 - Hybrid (público-privado) Blockchain Network Live Operation (Máquina de monedas y micropagos)

Tabla 4. Cronograma para crear el ecosistema Hdac

APÉNDICE A - Ejemplos

Ejemplo de un contrato inteligente

El encabezado JSON puede contener los siguientes comandos de control simples. Los datos JSON se pueden pasar a la función de definición del usuario, luego los usuarios pueden controlar el dispositivo interpretando esos datos JSON:

```
// Light on (if the IoT contract comes with the address of the light)

{ “operation” : “on”, “rerun” : “yes” } // If the response is returned after executing the command

{ “operation” : “off” }
```

```
// Turn on the air conditioner, set the temperature to 22 degrees Celsius, and set the wind to natural wind. Return temperature

{ “operation” : “on”, “temperature” : “22c”, “wind” : “natural”, “return” : “temperature” }

// Turn on the air conditioner, set the temperature to 70 degrees Fahrenheit, auto off after 60 minutes{ “operation” : “on”, “temperature” : “70f”, “timer” : “60 minute” }
```

Ejemplo de un programa de contrato IoT

El siguiente ejemplo es un programa simple de contrato de IoT que activa el aire acondicionado cuando el usuario está en casa, lo que le permite limitar la transacción automáticamente para cubrir solo la cantidad del servicio utilizado:

```
#include "hdac.h"
NodeAlias AC = "75578a276a3b2d50a1b4ddae16724185ae2d6d25"; // Air conditioner
NodeAlias TV = "1BZDfv3gjrFi2YpZ4FnPWhgRovbyM5coFmAAEA"; // TV
NodeAlias IS = “Infrared Sensor”; // Infrared Sensor
NodeAlias MO = “Management Office”;
hdac_t *hdac = NULL;
time_t PowerOnTime = 0;

main()
{
  hdac = HdacInit();
  IS.AddEvent(hdac, ProcessISEvent)
```

```
  ExecuteContract(hdac); // Wait until the IoT Contract end signal
  HdacExit(hdac);
}

// Process Event
void ProcessISEvent(hdac_t *hdac, NodeAlias node, NodeEvent ev)
{
  if (hdac == NULL || hdac->disabled == true)
    return;
  if (ev.GetStatus("motion") == 0 && PowerOnTime > 0)
  {
    AC.SetStatus(“power”, “off”); // AC OFF
    TV.SetStatus(“power”, “off”); // TV OFF
    int elapsed = time() - PowerOnTime;
    if (node.balance > 1) // If the balance is sufficient, pay
      MO.Pay(0.0001 * elapsed / 60); // Pay exact amount
    else
      node.Alert("Low Balance"); // Notify the user
      PowerOnTime = 0;
  }  else if (ev.GetStatus("motion") == 1 && PowerOnTime <= 0)  {
    AC.SetStatus(“power”, “on”); // AC operation
    TV.SetStatus(“power”, “on”); // TV operation
    PowerOnTime = time();
  }
}
```

APÉNDICE B - Descargo de responsabilidad legal

La información contenida en este documento está sujeta a cambios o actualizaciones sin previo aviso y no debe interpretarse como un compromiso por parte de HdacTech.AG. Este documento es solo para fines informativos y no constituye una oferta o solicitud para vender acciones o valores en Hdac.io o cualquier empresa relacionada o asociada. Dicha oferta o solicitud se realizará únicamente a través de un memorando de oferta confidencial y de acuerdo con los términos de todos los valores y demás leyes aplicables.

APÉNDICE C - Referencias

Antonopoulos, Andreas, Mastering Bitcoin: Programming the Open Blockchain, O'Reilly Media Inc. (California: 2017).

Arad Networks, "Why SPN Solutions?" http://www.aradnetworks.com/spn_why, (March 2017).

Banafa, Ahmed, "Internet of Things (IoT): Security, Privacy and Safety," Datafloq, https://datafloq.com/read/internet-of-things-iot-security-privacy-safety/948.

Beecham Research Limited, "IoT Security Threat Map," http://www.beechamresearch.com/download.aspx?id=43, (2015).

Belson, David [Ed.], "The State of the Internet / Q3 2015," Akami, https://www.akamai.com/us/en/multimedia/documents/report/q3-2015-soti-connectivity-final.pdf, (December 2015).

Boldt, Bill, "Without Security, is the Internet of Things Just a Toy?" Pubnub, https://www.pubnub.com/blog/2015-01-30-without-security-internet-things-just-toy/, (January 2015).

Buterin, Vitalik, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," https://github.com/ethereum/wiki/wiki/White-Paper, (2014).

Elasticsearch, "Heart of Elastic Stack," https://www.elastic.co/kr/products/elasticsearch, (2017).

EYL Partners, "Product Overview" http://www.eylpartners.com/index.php/product-overview/, (2017).

Greenspan, Dr. Gideon, "MultiChain Private Blockchain - White Paper," Coin Sciences, http://www.multichain.com/download/MultiChain-White-Paper.pdf, (2014).

Intel Software, "Intel Realsense Camera SR300," https://software.intel.com/en-us/realsense/sr300, (June 2016).

La Marca, Daniela, "Gartner: hype in 2015 around the internet of things (iot) and wearables," Mediabuzz,

http://www.mediabuzz.com.sg/asian-emarketing-latest-issue/210-asian-e-marketing/digital-marketing-trends-a-predictions-week-1/2504-gartner-hype-in-2015-around-the-internet-of-things-iot-and-wearables, (Jan. 2015).

Modacom, "Smart IoT Gateway (Hub)," http://web.modacom.co.kr/ko/product/product_view.php?cate=IoT%20Products, (Feb. 2017).

Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf, (2008).

P&P Secure, "Domestic DB Security # 1 'P & S Secure,'" http://www.pnpsecure.com/NEWS--NOTICE/page-4, (Sept. 2017).

Postscapes, “Internet-of-Things Software Guide: Find and compare the best IoT Software development tools, OS, language platforms, and frameworks,” https://www.postscapes.com/internet-of-things-software-guide/, (2017).

Sandoval, Kristopher, “Blockchain: Beyond Cryptocurrency,” NordicAPIs, https://nordicapis.com/the-uses-of-blockchain-beyond-cryptocurrency/, (May 2016).

Waterman, Shaun, “Report: IoT security products face huge challenges,” Cyberscoop, https://www.cyberscoop.com/forrester-iot-security-report-q1-2017/, (Jan. 2017).