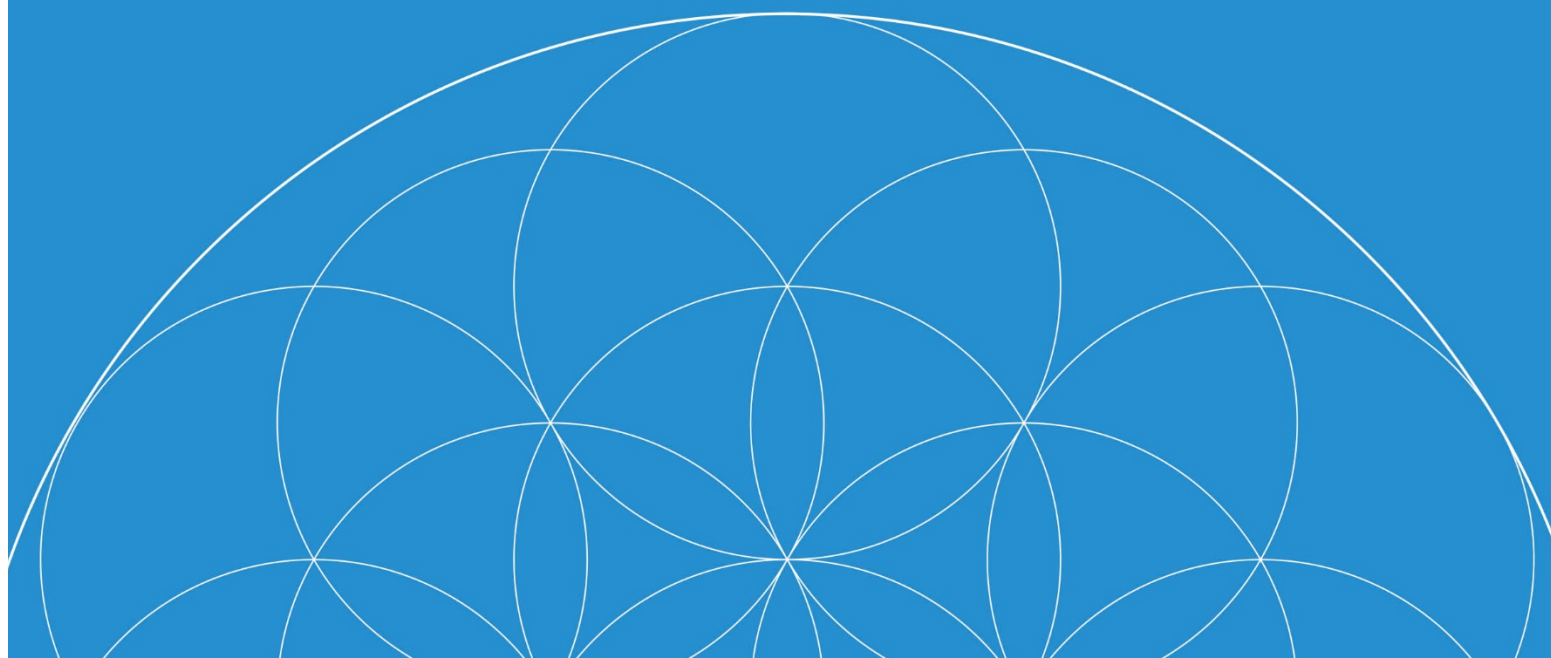




La Moneda de Confianza

Michael Mathias

31 de marzo de 2017



Síntesis

DasCoin se ha diseñado para resolver los problemas clave inherentes a almacenar y a intercambiar valores.

La cadena de bloques de transacciones de DasCoin cuenta con un libro de cuentas de distribución mutua que crea y distribuye activos criptográficos y posteriormente facilita de forma segura su almacenamiento y su intercambio. La cadena de bloques de transacciones de DasCoin forma el núcleo de un sistema de activos digitales conocido como el DasEcosystem, que se ha estructurado para proporcionar un conjunto de soluciones de intercambio de valores que ofrecen seguridad mejorada, gran utilidad, escalabilidad incrementada, mayor aceptación, eficiencia mejorada y mejor desempeño.

En el corazón del sistema está el DasCoin, una moneda híbrida diseñada para combinar las mejores cualidades de las criptomonedas descentralizadas con los mejores aspectos de las monedas centralizadas y eliminar sus respectivas debilidades. El DasCoin es una unidad de "depósito de valor" convertible que sirve como la base del sistema de recursos digitales. El sistema se ha diseñado para incrementar la prosperidad global a través de mejoras en la calidad y la eficiencia del intercambio de valores entre individuos y negocios, instituciones financieras, cooperativas y distribuidores.

En lugar de basar el valor en el apoyo que recibe un bien o en la declaración de un gobierno, el valor de DasCoin se basa en la calidad y la solidez del sistema subyacente. La confianza es fundamental en el sistema y ha sido adaptada al paradigma digital (en lugar de eliminarla sistemáticamente). En última instancia, a través de un sistema de valor con mayor distribución, más eficiente y mejor calibrado, una mayor población diversa y global puede disfrutar de prosperidad.

Introducción

El dinero con base tecnológica se ha convertido en una realidad y está destinado a crecer en las próximas generaciones. El Bitcoin ha sido el pionero en este segmento emergente y ha demostrado cómo es posible dar formato digitalmente a un sistema monetario; ha experimentado un éxito significativo en sus 8 años de existencia. Desde su aparición, han surgido otras criptomonedas, pero pocas han causado un impacto real en el mercado.

El punto de impacto principal ha sido la tecnología innovadora subyacente al Bitcoin, conocida como "blockchain", o cadena de bloques de transacciones. La cadena de bloques de transacciones es una herramienta que puede verificar transacciones con una participación mínima de terceros. Los nombres de compradores y vendedores nunca se revelan, solo sus direcciones en el sistema, y esas direcciones se pueden ocultar. La tecnología de la cadena de bloques forma parte de una categoría conocida como libros de cuentas de distribución mutua. "Mutua" se refiere al hecho de que los nodos son compartidos por la comunidad en lugar de pertenecer a una autoridad central. "Distribución" se refiere al hecho de que los nodos están divididos entre un número de localizaciones. Y "libro de cuentas" en este sistema representa un registro secuencial de transacciones.

Cuando se une, el sistema se convierte en inviolable, es un registro de transacciones inmutable que se comparte en una comunidad de usuarios y se almacena en múltiples localizaciones. Los 2 modelos de criptomoneda dominantes, el de "prueba de trabajo" y el de "prueba de participación", tienen carencias significativas. El modelo de prueba de trabajo del Bitcoin es un sistema brutalmente ineficiente y su estructura descentralizada lleva a problemas serios de gobernabilidad (como muestra el debate continuo sobre el tamaño de los bloques). Las monedas con el sistema de prueba de participación sufren de problemas de pre-distribución (la "pre-minería" puede distribuir monedas sin transparencia o justificación) y una falta inherente de validez (debido al problema del "nada en juego").

Cada sistema de valor debe establecer varios elementos fundamentales. Estos incluyen el definir: la oferta monetaria inicial, la distribución inicial, la base de valor, los mecanismos de expansión/contracción de la masa monetaria, quién controla los medios de producción y la asignación de inflación (y/o asignación de crédito).

DasCoin ofrece una estructura híbrida para resolver los problemas asociados con estos elementos de tipo económico. Se ha incorporado una arquitectura de cadena de bloques de transacciones privada y permissionada por su seguridad mejorada, por su eficiencia inherente y por la capacidad de escalar más fácilmente (a causa del control del despliegue). La fortificación de esta base segura se hace con la autenticación de todos los usuarios según los requisitos de KYC (Conoce al Cliente) de los estándares bancarios y con la implementación de un sistema digital de carteras con requisitos de hardware. Además, el sistema DasCoin integra un mecanismo de marketing potente que incentiva el crecimiento a través de una promoción de referidos basada en el boca a boca. El resultado es un sistema de valor digital con una seguridad óptima, un rendimiento excelente preparado para una adopción global rápida en el gran mercado.

Características clave de diseño

Método de Distribución de "Prueba de Valor"

La garantía de que cualquier persona que esté distribuyendo DasCoins directamente de la cadena de bloques de transacciones de DasCoin ha presentado al sistema una forma de valor definida y reconocida (específicamente en "Ciclos", una moneda con un único fin que solo se puede comprar a través de la compra de una licencia del sistema usando o bien Bitcoins o Euros). No hay agentes (ni ejecutivos ni desarrolladores) que puedan pre-acuñar, pre-minar o pre-distribuir DasCoins a sí mismos. Los Ciclos solo se pueden recibir a cambio de transferir valor al sistema y los Ciclos deben ser enviados al sistema para que haya una distribución directa de DasCoins a través del proceso de acuñación.

Método de Consenso "Prueba de Licencia"

DasCoin incorpora un sistema de licencias en lugar de un equipo de minado. Se llega al consenso a través de un algoritmo que define de forma aleatoria qué nodo con licencia realizará el siguiente bloque.

Suministro Fijo

Una capacidad de 2 a 33, unos 8,5 mil millones de unidades (distribuidas en un periodo indefinido, dependiente de las dinámicas internas del sistema, actualmente proyectado para durar 12 años).

Red Totalmente Autenticada

Cada usuario será autenticado a través del proceso estándar bancario KYC y será realizado por una autoridad central.

Convertibilidad

Los DasCoins se ponen en circulación a través de una conversión de los Ciclos. Una vez acuñados, se pueden transferir directamente o convertirse en una variedad de monedas fiduciarias y en Bitcoins. Los DasCoins existentes se podrán operar en una variedad de intercambios y, en ese punto, será posible el convertir dinero fiduciario directamente en DasCoins.

Ecosistema Distribuido

Para apoyar el valor del sistema de activos digitales hay una red global de sistemas de hardware y de software, así como productos y servicios asociados que se ofrecen en este sistema (incluyendo funciones de intercambio comercial y soluciones de pago). Esta red de sistemas interconecta muchas jurisdicciones del mundo y tiene redundancias diseñadas para asegurar operaciones fluidas.

Marketing Incentivado

Un sistema de marketing basado en referencias para apoyar el desarrollo de un grupo de afinidad mundial que reconozca el DasCoin y que esté interesado en intercambiar valores a través de este sistema de activos digital.

Características Híbridas

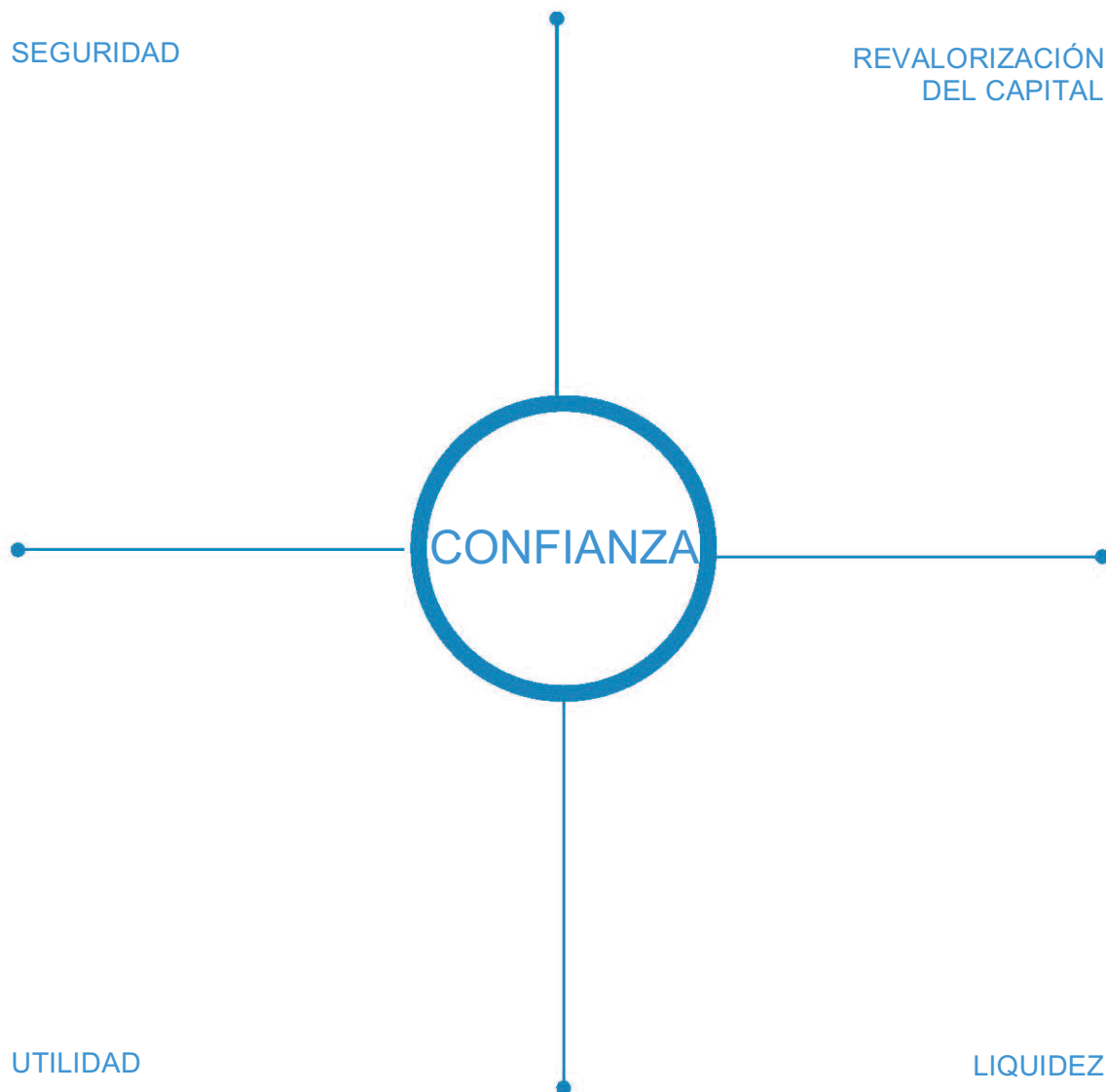
En DasCoin, se han combinado características centralizadas y descentralizadas para resolver problemas y maximizar los beneficios para el usuario.

- Emisiones centralizadas de monedas.
- Distribución descentralizada de monedas.
- Cadena de bloques de transacciones permisionada con verificación independiente.
- Base de usuarios autenticada centralmente a través del proceso estándar bancario KYC para promover la confianza entre los participantes.
- Un ecosistema distribuido, descentralizado.
- Un sistema de carteras digitales descentralizado: Una vez creada, una moneda solo podrá ser controlada a través de la clave privada de la cartera digital del usuario autenticado que posea la moneda. Ninguna otra persona, empresa o autoridad podrá transferir, confiscar o incautar esa moneda.
- Privacidad con transparencia (y sin anonimato) en la forma en que las transacciones se crean y se graban.
- Cumplimiento total de las regulaciones: Cumplimiento con jurisdicciones importantes y desarrollo de estándares de la industria.
- Transacciones inmediatas con una velocidad de validación establecida de 6 segundos.
- Asignación de la inflación descentralizada (a través de la cola de acuñación y del método de distribución de "prueba de valor").

Objetivos Clave

DasCoin se creó con los siguientes objetivos en mente:

- **Seguridad:** Todo el sistema DasCoin debe ser seguro.
- **Liquidez:** Debe haber la posibilidad de intercambiar la unidad DasCoin por otras formas de valor.
- **Utilidad:** Debe haber varias formas de usar el DasCoin en el mercado.
- **Revalorización del Capital:** La unidad debe funcionar como un auténtico depósito de valor. A medida que crezca el valor en el ecosistema, también deberá crecer el valor de la unidad de DasCoin.



Principios Rectores

Confianza: Un objetivo primordial del DasCoin es usar la infraestructura de un sistema de activos digitales para construir una red efectiva de confianza que permita a todos los participantes e interesados el compartir el objetivo común de incrementar el valor de la red y de cultivar su crecimiento. La red conseguirá esto al:

1. Dar confianza a ciertos roles (como el Equipo Directivo de DasCoin y a las autoridades de la cadena) para gestionar la cadena y maximizar la eficiencia y la utilidad de la red.
2. Asegurar programáticamente que cada rol de confianza está bien definido y que no excede los límites de su autoridad.
3. Ofrecer un incentivo por velar por el interés común de la red y asegurarse de que cualquier autoridad que se comporte de forma errónea será apartada de la red y podrá ser sancionada por romper las reglas.
4. Asegurar una firma contable externa verifica la precisión y el nivel de operaciones de la cadena de bloques de transacciones permisionada.
5. Ofrecer un alto nivel de transparencia y asegurar que se preservará adecuadamente la privacidad de todos los participantes del sistema.

Así, el sistema de DasCoin proporciona iteraciones de innovación y permite las actualizaciones necesarias para coincidir con las condiciones tanto de la red como del mundo en general. En definitiva, el sistema creará un conjunto de reglas acordadas para crear y transmitir valor y lo reforzará con el software de la cadena de bloques de transacciones. En una frase: Es el código: La LEY es CLAVE.

Privacidad: El sistema se diseñó para preservar la privacidad de los individuos sin necesitar el anonimato. Se mantiene la transparencia dado que no hay compromiso ni para el sistema de seguridad ni para la preservación de la privacidad de los participantes de la red.

Conveniencia: Cuando sea posible, el sistema incorpora características que mejoran la conveniencia y la facilidad de uso. La seguridad y la conveniencia suelen ser diametralmente opuestas, pero el sistema se ha diseñado para optimizar el equilibrio de esas 2 importantes características.

Simplicidad: Un objetivo que iba más allá era el de mantener el sistema lo más simple posible, sobre todo en lo relativo a todas las interacciones con el usuario.

Definiciones

Clave Privada

Un código secreto que otorga acceso y control de los activos criptográficos. El formato de clave privada del sistema es un número de 32 bytes creado con un método aleatorio de generación.

Clave Pública

Es un código que se puede compartir pero que está emparejado con la Clave Privada. El formato de clave pública del sistema es un punto de la curva elíptica secp256k1.

Ecosistema de DasCoin

Un sistema de activos digital capaz de crear, transferir y considerar de forma segura una variedad de activos cartográficos. El ecosistema contiene la cadena de bloques de transacciones, las carteras y las funcionalidades de intercambio.

DasNet

La red de nodos de alta velocidad en la que existe DasCoin y todo el DasEcosystem.

Cadena de bloques de transacciones DasCoin

Una arquitectura de cadena de bloques de transacciones privada y permissionada que tiene una seguridad mejorada, una eficiencia inherente y una escalabilidad mejorada.

Cuenta de depósito

Una cuenta en el sistema de carteras digital que posee una persona o entidad comercial ya autenticada. Esta cuenta tiene la información de la licencia de esa persona particular o esa entidad comercial.

Licencia

Un certificado criptográfico que permite a una cuenta el participar en la cadena de bloques de transacciones de DasCoin.

Ciclos

Un activo criptográfico definido en la cadena de bloques de transacciones de DasCoin. Los Ciclos representan la capacidad almacenada en DasNet y se pueden usar o bien a cambio de servicios de la red o pueden cambiarse por DasCoins.

DasCoin

Una unidad de "depósito de valor" convertible que está en el centro del sistema de activos digitales. Los DasCoins se producen y se distribuyen a cambio de Ciclos enviados a DasNet.

Frecuencia

El factor de conversión que determina la cantidad de Ciclos que producirán un DasCoin en el proceso de acuñación.

Acuñación de DasCoin

El proceso de producir y distribuir DasCoins a cambio de los Ciclos enviados. Se forma una cola con los Ciclos enviados al sistema. Entonces se crea un cierto número de DasCoins cada 10 minutos y se distribuyen según la Frecuencia y los parámetros relevantes de la cola.

Definiciones

Cola de acuñación de DasCoin

La cola de usuarios que han enviado sus Ciclos a cambio de DasCoins. La cola funciona según un sistema de primera entrada, primera salida.

Bloque de acuñación de DasCoin

La cantidad de DasCoins distribuidos al final de cada intervalo de acuñación.

Intervalo de Acuñación de DasCoin

El periodo de duración de 10 minutos entre Bloques de Acuñación de DasCoin.

Índice de Acuñación de DasCoin

El número de DasCoins que serán distribuidos durante el transcurso del Intervalo de Acuñación de DasCoin.

WebEuro

Un activo criptográfico definido en la cadena de bloques de transacciones de DasCoin que representa la denominación Euro.

Libro de cuentas de Transacciones

Operaciones

Las operaciones son la base para crear transacciones. Se definen usando un lenguaje de programación C++ que permite la creación de actividades dinámicas y expansivas que se desarrollan en la cadena de bloques de transacciones. Las operaciones describen la lógica potencial de la que puede hacer uso una persona o los nodos. Se pueden añadir y actualizar en tiempo real tras la aprobación de las actualizaciones del software. Esto significa que es posible ofrecer contratos digitales personalizados que se refuercen mediante programación con la cadena de bloques de transacciones y su red de nodos.

Transacciones

Las transacciones son el resumen de las operaciones previstas para alguna actividad. Cuando el conjunto de operaciones está definido, el participante de la transacción debe firmar adecuadamente la operación correspondiente con su clave privada. Estas se comprobarán y se verificarán e incluirán una fecha de vencimiento, un número de bloque y una referencia del resumen criptográfico del número de bloque. Solo cuando todos los campos requeridos estén rellenos y cada operación esté firmada con las claves respectivas se podrá incluir con éxito en un bloque y anotarse en el historial del Libro de cuentas de la Cadena de bloques de transacciones.

Bloques

Un bloque es un grupo de transacciones que actualiza el estado del Libro de cuentas de la Cadena de bloques de transacciones. Los bloques son el elemento fundamental de la Cadena de bloques de transacciones. Cada bloque es creado por una entidad de autoridad llamada Nodo Maestro ("Master Node") y cada bloque está enlazado criptográficamente con el bloque anterior.

Esta continuidad criptográfica asegura la integridad de los saldos que se modifican en el libro de cuentas. Al reproducir la secuencia de bloques se revela el estado existente actual y la aplicación secuencial de bloques significa que no puede haber incoherencias entre el saldo de las cuentas que hay en la cadena de bloques de transacciones.

Los bloques son inmutables porque contienen sellos de tiempo, tienen la firma del Nodo Maestro que lo aprobó y se enlazan a los futuros bloques. Esto significa que cuando la gente hace transacciones, son irreversibles y no se pueden modificar sin afectar totalmente todos los demás aspectos del sistema. Se rechazará cualquier firma inválida y por tanto, nadie puede cambiar o modificar fácilmente el historial existente de la cadena de bloques de transacciones.

Bloques de Acuñación

Un Bloque de Acuñación es la distribución directa de DasCoins recién acuñados que ocurre al final de cada Intervalo de Bloques de Acuñación (actualmente establecido en 10 minutos). Cada Bloque de Acuñación es creado por un Nodo Maestro y se enlaza criptográficamente al Bloque de Acuñación anterior. Los DasCoins resultantes se transfieren directamente a los depósitos WebWallet según la Cola de Acuñación.

Libro de cuentas de Transacciones

Contrato de Caja Fuerte

Un Contrato de Caja Fuerte es un contrato inteligente que existe en la Cadena de Bloques de Transacciones de DasCoin. Requiere que el dueño del Depósito WebWallet transfiera un cierto número de DasCoins para almacenamiento seguro durante un periodo de tiempo acordado (el término del contrato). Una vez en el almacenamiento seguro, los DasCoins no pueden ser transferidos hasta que haya expirado el periodo de tiempo y luego se transferirán automáticamente de vuelta al depósito original a no ser que el titular del contrato acuerde prorrogar el saldo durante otro periodo de tiempo.

Como incentivo por aceptar el almacenar cierta cantidad de DasCoins, el dueño de los DasCoins recibe un porcentaje del Fondo de Incentivos. Los incentivos se transfieren directamente de la Cadena de bloques de transacciones de DasCoin a la caja fuerte del titular del contrato. Caja Contrato de Caja Fuerte inicial recibe una parte del Fondo de Incentivos y el incentivo se comparte entre todos los titulares de contratos actuales durante ese periodo.

Hay 3 tipos de Contratos de Caja Fuerte. Cada uno requiere una Transferencia Admisible diferente, un Plazo de Compromiso diferente y cada uno trabaja con un Fondo de Incentivos diferente. Cada uno concede al titular del contrato también con una cierta proporción de influencia de voto en el sistema.

Contrato de Votación

Este contrato requiere que se comprometan 10.000 DasCoins durante un periodo de 2 años. El Fondo de Incentivos para este contrato es un 10% adicional del total de DasCoins acuñados cada semana y se entrega de forma semanal. No hay límite en el número de Contratos de Votación que puede tener una persona o entidad.

Contrato de Libro de Cuentas

Este contrato requiere que se comprometan 100.000 DasCoins durante un periodo de 3 años. El titular del contrato también debe tener 10 Nodos de Libro de Cuentas para poder participar en el Fondo de Incentivos del Libro de Cuentas. El sistema verificará que esos nodos han estado activos durante el periodo anterior al momento de distribuir la parte de los incentivos al titular del contrato. El Fondo de Incentivos de este contrato es un 6% adicional de todos los DasCoin acuñados en un periodo de 2 semanas y se distribuye cada 2 semanas. No hay límite en el número de Contratos de Libro de Cuentas que una persona o entidad puede tener.

Libro de Cuentas de Transacciones

Contrato Maestro

Este contrato requiere que se comprometan 1.000.000 DasCoins durante un periodo de 5 años. El titular del contrato también debe tener un Nodo Maestro para poder participar en el Fondo de Incentivos de Maestros. El sistema verificará que ese nodo ha estado activo durante el periodo anterior al momento de distribuir la parte de los incentivos al titular del contrato. El Fondo de Incentivos de este contrato es un 3% adicional de todos los DasCoin acuñados en un periodo de 3 semanas y se distribuye cada 3 semanas. Hay un límite de 3 Contratos Maestro por persona, entidad o partes vinculadas.

Contrato	Transferencia Admisible	Plazo de Compromiso	Fondo de Incentivos	Votos
Contrato de Votación	10.000 DasCoins	2 años	10%	1
Contrato de Libro de Cuentas	100.000 DasCoins	3 años	6%	20
Contrato Maestro	1.000.000 DasCoins	5 años	3%	300

Prórroga

Se entregará un incentivo extra a cada titular de un contrato por aceptar comprometerse a un término adicional antes de que expire el periodo en curso. Al "prorrogar" su contrato, el titular del contrato obtendrá 2 partes del Fondo de Incentivos, en lugar de la parte habitual. Cada compromiso subsecuente vendrá acompañado de una parte adicional del fondo, así que al acordar una segunda prórroga, el titular del contrato recibiría 3 partes, en lugar de una sola parte, en ese periodo. Cada acuerdo de prórroga añade otra parte del Fondo de Incentivos según los términos próximo contrato.

Libro de Cuentas de Transacciones

Súper Bloques

Un Súper Bloque es una transacción de distribución grande que actualiza el estado del Libro de Cuentas de la Cadena de bloques de transacciones en un intervalo específico. Cada Súper Bloque es creado por un Nodo Maestro de acuerdo con una serie de contratos inteligentes y cada Súper Bloque se integra en la Cadena de bloques de transacciones de DasCoins a través de un enlace criptográfico con el anterior bloque estándar. La producción de Súper Bloques no retrasa ni interfiere con la producción de Bloques de Acuñación y, por tanto, no impacta en la Cola de Acuñación.

Bloques de Votación

10% de la producción del Bloque de Acuñación durante un periodo de 1 semana. Se introduce directamente a las cuentas de caja fuerte.

Bloques de Libros de Cuentas

6% de la producción del Bloque de Acuñación durante un periodo de 2 semanas. Se introduce directamente a las cuentas de caja fuerte.

Bloques Maestros

3% de la producción del Bloque de Acuñación durante un periodo de 3 semanas. Se introduce directamente a las cuentas de caja fuerte.

Bloques de Tesorería

1% de la producción del Bloque de Acuñación durante un periodo de 4 semanas. Se introduce directamente en una Cuenta de Tesorería controlada por la Junta de DasCoin. Las ganancias de estos bloques se han diseñado para pagar por la administración del sistema (Director Ejecutivo, personal y Junta Directiva), así como para financiar las campañas de marketing.

La producción de Súper Bloques es simplemente la redistribución de la distribución definitiva del número total de DasCoins. En lugar de distribuir la cantidad final de DasCoins simplemente a través de la producción de Bloques de Acuñación, el sistema incentiva a los titulares de DasCoins para que almacenen (o guarden) una porción de sus activos. Esta dinámica beneficia la estabilidad general del sistema. El sistema también se beneficia de los nodos de Comunidad creados por los Súper Bloques. Esto crea una mayor descentralización y mejora la estabilidad general de la infraestructura DasNet.

Consenso Descentralizado

Nodos Maestros

El papel del Nodo Maestro es agregar transacciones con el fin de producir Bloques. Solo los Nodos Maestros tienen la autoridad de escribir transacciones en el historial del libro de cuentas de la cadena de bloques de transacciones. Cada Nodo Maestro conoce la existencia de los demás y debe haber sido votado en el sistema de gobierno. Los Nodos Maestros son innovadores por el hecho de que su autoridad está representada por claves criptográficas. Esto significa que cada Nodo Maestro debe haber registrado su Clave Pública y firmará con su Clave Privada durante la Producción de Bloques. Por lo tanto, es posible responsabilizar a un Nodo Maestro en particular por sus acciones.

Nodos del Libro de Cuentas

Los Nodos del Libro de Cuentas son mantenedores sin autoridad de la Cadena de bloques de transacciones de DasCoin. Es decir, los Nodos del Libro de Cuentas no producen bloques, pero agregan transacciones y se las pasan a los Nodos Maestros para su inclusión en los Bloques. Los Nodos del Libro de Cuentas pueden verificar transacciones y, por tanto, son útiles tanto para reforzar la impronta de la Red de Consenso del DasCoin como para permitir la conectividad y llegar más lejos sin necesidad de asignar autoridad al nodo. La propagación de las transacciones se acelera por los Nodos del Libro de Cuentas.

Nodos de Votación

Los Nodos de Votación son influyentes sin autoridad en la Cadena de bloques de transacciones de DasCoin. Estos nodos no controlan ninguna de las funciones diarias del sistema DasCoin, pero controlan totalmente quién forma parte de la Junta de DasCoin y qué proposiciones llegan al sistema. Los Nodos de Votación representan a accionistas importantes que han demostrado (a través de su compromiso de mantener al menos 10.000 DasCoins durante un periodo de 2-5 años) que tienen una visión a largo plazo para el DasCoin y, por tanto, reciben el privilegio de influir en la gobernanza de la cadena. Cada Nodo de Votación podría firmar una transacción con su clave privada correspondiente y, así, expresar su opinión sobre asuntos de la gobernanza de la cadena.

La votación tiene lugar en una sección especializada de WebWallet y requiere autenticación con un dispositivo de hardware especializado de 2 factores (es decir: el "Validator"). Los votos pueden realizarse individualmente o en bloques de multi-voto, como cuando la cuenta de una cartera específica tiene varios Contratos de Caja Fuerte o uno o más Contratos de Caja Fuerte de mayor nivel. Cualquier Nodo de Votación cualificado puede iniciar una propuesta. La Junta de DasCoin es responsable de organizar y presentar las propuestas al grupo de Nodos de Votación. También hay un mecanismo en el sistema de votación que permite a los Nodos de Votación el presentar directamente un referéndum a sus miembros sin pasar por el proceso de revisión de la Junta (para evitar que la Junta deniegue cierta propuesta de los Nodos de Votación).

Cada titular de una cuenta podrá comprometerse con tantos Contratos de Votación como desee y tener toda esa cantidad de votos en el sistema. Cada voto es de igual importancia en las elecciones de la cadena y en los referéndums. El propósito de los Contratos de Votación es hacer que los usuarios tengan un saldo bloqueado de DasCoin en el sistema como inversión y, por tanto, que tengan un interés personal en seguir con su compromiso.

Consenso Descentralizado

La duración del contrato (2 años) se establece con la expectativa de que los votos tengan un objetivo racional de conseguir un crecimiento del valor a largo plazo en lugar de tener ganancias a corto plazo, ya que las participaciones están bloqueadas y no se pueden sacar para beneficiarse de la dinámica del mercado a corto plazo.

Producción de Bloques

Cada Nodo Maestro tiene una oportunidad equitativa para producir un bloque. Hasta que cada Nodo Maestro haya participado en producir un bloque, su orden es aleatorizado de nuevo. Esto evita que cualquier Nodo Maestro domine la producción de bloques, lo que podría llevar potencialmente a la inestabilidad de la red y de las transacciones por no estar confirmadas en el libro de cuentas. Cada 6 segundos, otro Nodo Maestro es seleccionado y es responsable de producir el bloque de ese índice. Si no puede producir un bloque, entonces el siguiente Nodo Maestro se encarga de producir el bloque de ese mismo índice. Se sigue este protocolo para la producción de todos los tipos de bloques dentro de la cadena de bloques de transacciones.

Actualizaciones del software

Las actualizaciones puntuales para implantar mejoras y nuevas características deberán incorporarse al software de la cadena de bloques de transacciones. Por lo tanto, es posible el mejorar la tecnología, aunque ya esté funcionando. Al menos el 51% de los Nodos Maestros deben aprobar un cambio de software para incorporarlo en el uso general de la red. Esto permite que los accionistas del DasCoin puedan incorporar peticiones para características y que los desarrolladores optimicen el desempeño del software.

Debido a la estructura híbrida del sistema, se puede realizar una implementación centralizada cuando al menos un 51% de los Nodos Maestros hayan aprobado una actualización del software. La implementación centralizada suprime la posibilidad de que haya la conocida como "bifurcación dura", que tiene lugar cuando el sistema monetario se divide en 2 redes diferentes. Ese es el resultado de un desacuerdo interno entre los nodos de producción del sistema y causa muchas consecuencias negativas. La bifurcación dura es estadísticamente inevitable para todas las criptomonedas descentralizadas a causa de su estructura operativa. Por otro lado, una bifurcación dura es imposible en el sistema de DasCoin. Tras la aprobación de una actualización de software, se actualizan todos los Nodos Centrales y también los Nodos de Comunidad conformes. Ese grupo será responsable de al menos el 51% de los Nodos Maestros y seguirá operando la Cadena de bloques de transacciones del DasCoin. Cualquier Nodo de Comunidad sobrante que rechace la actualización del software ya no será reconocido en la operación de la Cadena de bloques de transacciones del DasCoin y ya no recibirá Distribuciones del Súper Bloque.

Privacidad

La Cadena de Bloques de Transacciones de Dascoin es un sistema permissionado, es decir, todas las cuentas de usuario deben ser verificadas y aprobadas por una autoridad registradora (que, en el caso de las cuentas de usuario, es gestionado a través del sistema de carteras digital).

Definimos el "estado" como el consenso sobre los datos de usuario (cuentas, saldos, etc.). A diferencia de los derivados del Bitcoin, el estado del usuario existe en todos los nodos en memorias de datos y se puede acceder a él libremente.

Consenso Descentralizado

El estado se mantiene a través de un consenso de red al seguir la cadena de bloques más larga disponible. Los nodos pueden reproducir la vía más larga al poner cada transacción grabada por orden y llegar al estado actual (o el estado en el momento de cada bloque en el pasado).

Como se accede al estado de forma regular y es modificado por la aplicación de nodos, no puede almacenarse en un formato encriptado en el disco (de hecho, los datos deben estar en la RAM por razones de rendimiento, lo que hace que el control de acceso sea más complicado).

La premisa de la Cadena de bloques de transacciones del DasCoin es que todos los datos en la cadena de bloques son públicos. Las cuentas de usuario (y, por tanto, los saldos enlazados a la identificación de la cuenta) no almacenan información de identificación personal. Todos los datos confidenciales se almacenan en servidores de autenticación independientes y privados en un almacenamiento en frío encriptado. Por lo tanto, solo los usuarios pueden conocer la identificación de sus cuentas y pueden mantener así su privacidad ante observadores externos.

Para conseguir transparencia de operación, la Cadena de bloques de transacciones de DasCoin debe estar abierta al público. Esto requiere que el explorador de los bloques (es decir: DasCoinExplorer.com) muestre los bloques sin filtrar con todos los datos de las transacciones. Al participar en Contratos de Caja Fuerte, los usuarios pueden implementar sus propios Nodos de Libro de Cuentas para observar la Cadena de bloques de transacciones y consultar el estado (saldos, cuentas y otros datos).

El servidor de autenticación puede revelar datos de usuario para la validación KYC para cumplir con las normativas legales. Los usuarios pueden ser avisados de este hecho (y de la necesidad de cumplir con la ley).

En este modelo de privacidad se deberá confiar en el servicio de autenticación de la red DasCoin. El usuario podrá esperar seguir teniendo una privacidad razonable en el sistema ya que su saldo no podrá ser consultado por fuentes externas. La información KYC también se proporciona en los sistemas actuales de intercambios de criptomonedas por causas legales. El servicio de autenticación tiene un fuerte incentivo para no divulgar la información privada a externos, ya que dañaría la valía de la red. También reduce el nivel de confianza que el usuario debe invertir en la red. Como todas las transacciones son públicas, no cabe la posibilidad de que se manipulen los saldos ni el estado de usuario.

El único requisito es que los servidores de autenticación se mantengan seguros contra intrusiones. Esto, sin embargo, es una tarea mucho más sencilla que asegurar toda la red, ya que la superficie de ataque es mucho más pequeña y el control de acceso se puede regular más. Si los datos se aseguran y se comparten adecuadamente, una posible intrusión no significa una pérdida total de privacidad, ya que el atacante solo consigue una cierta cantidad de datos privados.

Red de Nodos de Alta Velocidad

El DasEcosystem muestra un nuevo poder y posibilidad como Cadena de bloques de transacciones y Criptomoneda ya que los Nodos Maestros solo deben almacenar sus claves de firma privadas y autenticarse con el resto de la red. Esto significa que los Nodos Maestros solo deben validar las transacciones en el historial antes de producir un bloque. Cuanto antes el Nodo verifique todas las firmas y los saldos, antes podrá producir un bloque y seguir adelante. Por lo tanto, la confirmación y las operaciones pueden llevar un ritmo más rápido que nunca.

La calidad del hardware y de la configuración de red permiten una mejor captación de las transacciones de todo el mundo y mejora la confianza y la estabilidad del comercio. A causa de todos estos adelantos, la red puede confirmar las transacciones y permitir actualizaciones de saldo en tan solo 6 segundos. La optimización del software de la Cadena de bloques de transacciones reducirá considerablemente el tiempo requerido para confirmar y propagar bloques.

Middleware

DasNet es una red sofisticada que se ha pensado para alojar la Cadena de bloques de transacciones y para el acceso global para la captación y verificación de transacciones. Por este motivo, DasCoin está construido sobre una arquitectura de red de vanguardia específicamente diseñada que trabajar como una red segura y adaptada a escala mundial.

Infraestructura del hardware

Los Nodos Maestros están alojados exclusivamente en centros de datos con el requisito de que el acceso al armario de servidores esté físicamente asegurado. Están conectados de forma compatible con otros centros de datos del mundo con líneas directas arrendadas que garantizan un ancho de banda fiable y altamente conectado. Este planteamiento da a DasNet el control de toda la ruta entre centros de datos y permite evitar los ataques de intermediarios así como los ataques de denegación de servicio y de denegación de servicio distribuido entre los nodos que mantienen la Cadena de bloques de transacciones y su conectividad con el servicio.

DasNet tiene 2 capas adicionales para manejar la captura de transacciones y la conectividad de red además de las características de la infraestructura central mencionadas anteriormente. La configuración del servidor tiene componentes de vanguardia y de calidad y protección y prevención para amenazas superiores. Además, tiene una solución de cortafuegos de hardware que suele ser utilizada por los bancos y por otros ambientes de alta seguridad. Además, DasNet está alojado en unos servidores potentes que operan con 44 centrales por servidor, lo que ofrece un espacio y un consumo de energía eficiente con mucho tráfico y un uso global.

DasNet tendrá un total de 33 Nodos Maestros Centrales que operarán en centros de datos en 33 jurisdicciones diferentes de todo el mundo. La instalación de los Nodos Maestros Centrales tendrá lugar a un ritmo de aproximadamente 2 por mes. También habrá aproximadamente 3.000 Nodos de Libros de Cuentas Centrales en DasNet. Además, los Contratos de Caja Fuerte traerán miles de Maestros de Comunidad y Nodos de Libros de cuentas que se añadirán a la infraestructura de DasNet.

Infraestructura del software

La conectividad a la Cadena de bloques de transacciones de DasCoin también funciona con un servicio de software que permite el acceso a los servicios centrales sin dejar de mantener su alto aislamiento y seguridad. Estos servicios ofrecen y apoyan un equilibrio de carga del servicio base así como una redundancia y facilidad para escalar, ya que se podrían necesitar recursos de red con un uso mayor de la misma.

El acceso a la Cadena de Bloques de Transacciones de DasCoin requiere una configuración para las partes autorizadas para que transmitan información relevante de la Cadena de bloques de transacciones y sus operaciones internas. También contiene monitorización 24/7 y soporte para mantener tanto los servicios externos como los parámetros clave de los servicios centrales. Cada uno de esos componentes y servicios permite un índice de producción de bloques de alta velocidad, así como el mantenimiento de su integridad de operación. La inmutabilidad y la conexión criptográfica entre todas las actividades defienden los principios de la Cadena de bloques de transacciones de DasCoin y de DasNet.

Middleware

Equipo central de desarrollo

La infraestructura de hardware es implementada y preservada por el Equipo central de desarrollo. Toda la infraestructura de software ha sido desarrollada y preservada por el Equipo central de desarrollo. La Junta es responsable de asegurar que el Equipo central de desarrollo vele por el interés general de todo el ecosistema. Los Nodos Maestros tienen el control de los directivos del ecosistema, los Directores Ejecutivos, y de los accionistas importantes de la comunidad DasCoin. Ningún individuo o empresa podrá controlar más de 3 Nodos Maestros en la infraestructura de DasNet.

Inducción del Sistema de Licencias

Para que una persona o entidad se convierta en un participante activo de esta red autenticada, deberá obtener una Licencia. El software de la Cadena de bloques de transacciones permite que un servicio esté autorizado para conectar y registrar nuevas cuentas. El Valor (en forma de Euros o Bitcoins) que se aportó determinará el nivel de la Licencia que determina la escala con la que una persona o entidad puede participar en la red. Una vez se haya comprado una licencia, el recipiente deberá crear una Cartera para aprovechar al completo de las oportunidades que le otorga la Licencia.

Cuentas de Depósito

Las Cuentas de Depósito tienen información personal del usuario y son las cuentas que reciben las licencias. Se registra la cuenta en la Cadena de bloques de transacciones de DasCoin y la Autoridad Expedidora de Licencias asigna la licencia. Una vez que se conceda la licencia, la Cuenta de Depósito recibirá Ciclos. Las Cuentas de Depósito tienen restricciones de transferencias dependiendo del nivel de licencia y del nivel de autenticación. Para poder usar una Cuenta de Depósito, se deberá conectar a una Cuenta Cartera. La Cuenta de Depósito también es la cuenta con la que se pueden enviar los Ciclos a la Cola de Acuñación de DasCoin.

Cuentas Cartera

Las Cuentas Cartera ofrecen la posibilidad de operar a los participantes de DasNet. Esta cuenta puede aceptar transferencias de la Cuenta de Depósito y realizar transacciones externas así como transferir fondos a otra Cartera y Cuentas de Depósito de la red. El titular de una Cuenta Cartera también puede acceder a una variedad de funciones a través de la Cartera, incluyendo las votaciones y la operación de los Nodos Comunitarios de Libros de Cuentas o los Nodos Comunitarios Maestros (correspondiente a los Contratos de Caja Fuerte).

Conexión

Todas las Cuentas de Depósito deberán estar conectadas a una Cuenta Cartera. Ambos tipos de cuentas se conectan y permanecen estrechamente vinculadas. Una Cuenta Cartera se puede conectar a tantas Cuentas de Depósito como un usuario quiera compartir. El proceso de conexión requiere una firma simultánea tanto de la Cuenta de Depósito como de la Cuenta Cartera para realizar una transacción de conexión con éxito. Este proceso se inicia con una invitación segura que es enviada por la entidad que expide las licencias a través de una combinación de mensajes por email y SMS.

KYC y AML (Conoce al Cliente y Ley Contra el Blanqueo de Capitales)

Cada Cuenta de Depósito debe tener una licencia otorgada a una persona o entidad para acceder a DasNet. El nivel de la licencia y los niveles correspondientes de KYC también determinan las cantidades diarias que una Cuenta de Depósito puede transferir a la Cuenta Cartera. Una licencia con un nivel más alto permite a la persona o entidad el incrementar su nivel de autenticación y, por tanto, incrementa su acceso a más capacidad en el sistema y mayores privilegios de retirada. Así, la Cadena de Bloques de Transacciones de DasCoin y de DasNet puede cumplir totalmente con las regulaciones globales que requieren que los titulares de las cuentas sean identificados y que tengan una buena posición antes de comerciar con otros participantes del DasEcosystem. Este tipo de protocolo de autenticación resulta en un mayor nivel de integridad entre los participantes y seguramente lleve a una mayor aceptación entre las jurisdicciones reguladas del mundo.

WebWallet

El WebWallet es un punto de acceso seguro para que los usuarios accedan a datos relevantes de la Cadena de bloques de transacciones de DasCoin e interactúen con el estado global al firmar transacciones. Es una cartera criptográfica electrónica que tiene el acceso para el cliente en el navegador del usuario y el *backend* del servidor de la aplicación está alojado en un servidor web en internet. La WebWallet sirve como el punto de entrada para el usuario en la Red Dascoin segura. Cada cuenta WebWallet enlaza a los usuarios con sus depósitos y carteras y se usa para almacenar y validar la información personal KYC y AML. Los usuarios autenticados pueden acceder a través de WebWallet a su información importante en la cadena de bloques global: el saldo de los depósitos, la compra de licencias, el historial de transacciones, etc.

WebWallet cuenta con un hardware de almacenamiento criptográfico para gestionar claves y firmar de forma segura transacciones en la cadenas de bloques. Este dispositivo de hardware propio es conocido como el "Validator" y tiene la capacidad de generar y almacenar claves privadas ECDSA correspondientes a los usuarios de los depósitos de las cadenas de bloques. El Validator también está asegurado con un PIN/frase de contraseña que evita el uso inadecuado y el robo de claves.

Al firmar las transacciones de la cadena de bloques de transacciones, WebWallet se comunica con el dispositivo de hardware del Validator. El usuario debe primero desbloquear su Validator antes de que la clave privada ECDSA requerida pueda ser transferida a la memoria del navegador de la aplicación del cliente de javascript tras la confirmación de una transacción. No se puede realizar ninguna transacción de DasCoin sin la validación a través de este dispositivo de hardware criptográfico. Este sistema ofrece el mayor nivel de seguridad y protección para la autenticación de transacciones. La clave se almacena en la memoria durante el menor tiempo posible requerido para firmar la transacción y luego se expulsa de la memoria del cliente. La clave privada nunca es "rápida": nunca cruza el cable, ni siquiera de forma encriptada.

El usuario puede guardar una clave mnemónica que consiste de 24 palabras usadas como entropía para generar la clave privada. En caso de robo o pérdida del dispositivo de hardware, el usuario puede usar la mnemónica para reconstruir la clave privada original y restaurar el acceso a su cuenta.



Acuñaación de DasCoin

El proceso de producir y distribuir nuevos DasCoins es conocido como Acuñaación. Esto permite a una persona o entidad el almacenar valor en forma de DasCoins. Para conseguir DasCoins, la gente puede enviar Ciclos a la red y luego conseguir que se le asigne una plaza en la Cola de Acuñaación de DasCoin. Con una base de primera entrada, primera salida, los DasCoins se envían a la cuenta que está la siguiente en la cola de distribución. En cada Intervalo de Distribución de DasCoin se distribuye una cantidad específica de DasCoins entre los miembros de la cola.

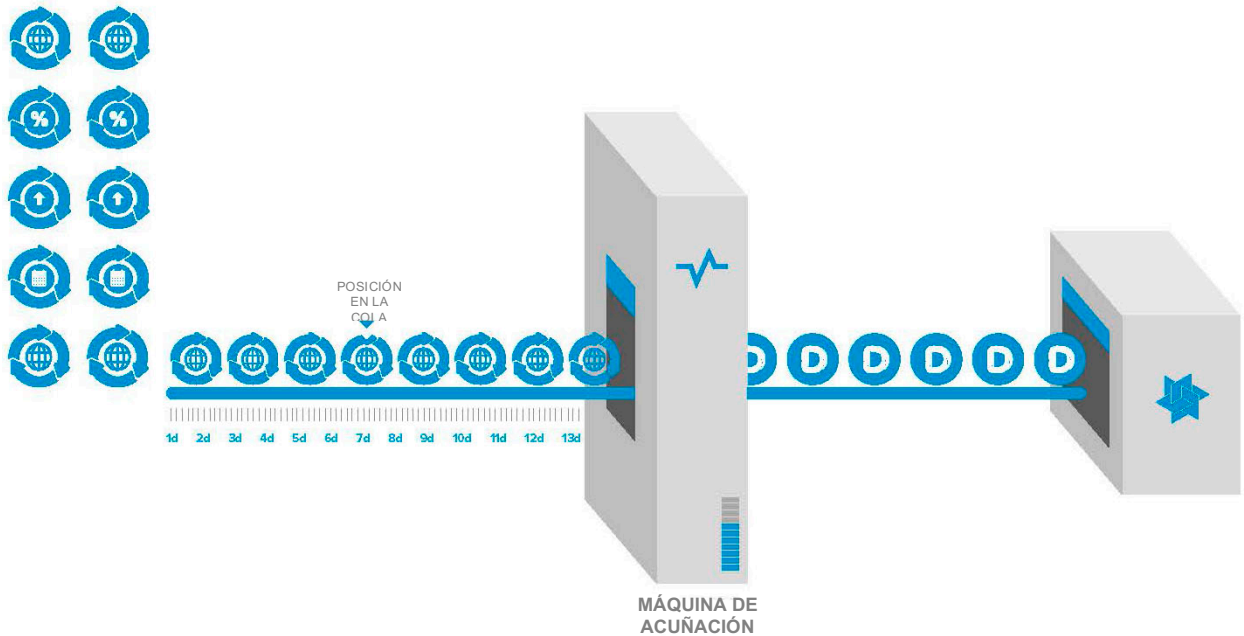
La cantidad de DasCoins a recibir está regulada por un factor de conversión ajustable llamado Frecuencia de forma que la cantidad de Ciclos enviada dividida por la Frecuencia resulta en el número de DasCoins que serán enviados a esa persona. Se restan los Ciclos de la cuenta en el momento del envío y en el momento de la entrega de los DasCoins, éstos son enviados automáticamente a la cuenta con el software de la cadena de bloques de transacciones.

La distribución se realiza según el siguiente algoritmo:

```
While amount_to_distribute > 0 and not queue.empty() do
  element = queue.front()
  If element.frequency_lock exists then
    Dascoin = element.cycles/element.frequency_lock
  Else
    Dascoin = element.cycles/global_frequency
  End if
  If amount_to_distribute >= dascoin then
    queue.pop_front()
    issue dascoin to element.accaunt_id
    amount_to_distribute = amount_to_distribute - dascoin
  Else
    If element.frequency_lock_exists Then
      cycles_to_remove = amount_to_distribute * element.frequency_lock
    Else
      cycles_to_remove = amount_to_distribute * global_frequency
    Endif
    issue amount_to_distribute to element.account_id
    element.cycles = element.cycles - cycles_to_remove
    queue.update_front(element)
  Endif
Loop
```

Acuñación de DasCoin

Periódicamente, según un Intervalo de Mejora predeterminado, todos los saldos de Ciclos experimentarán una Mejora y esos saldos de las cuentas se duplicarán. Si los Ciclos ya están en la Cola de Acuñación de DasCoin, esos Ciclos permanecerán intactos (a no ser que estén asociados con una cuenta que tenga un Bloqueo de Frecuencia).



Intercambio Interno en la Cadena de Bloques de Transacciones

La Cadena de bloques de transacciones de DasCoin también incorpora un sistema de intercambios descentralizado que opera, liquida y libera la Cadena de bloques de transacciones de forma autónoma. Así, los usuarios con licencia no tienen que elegir el transferir su moneda a cuentas de custodia en cambios centralizados para realizar ciertos tipos de operación. Por ejemplo, los WebEuros también son activos criptográficos de una forma similar a los DasCoins y, por tanto, sin sacarlo de su cuenta, el titular puede cambiar DasCoins por denominaciones de Euro directamente en la cadena de bloques de transacciones.

A causa de esto, el nivel de robos por parte de externos se reduce considerablemente y la operación y la conversión a las monedas fiduciarias nacionales es simple y directo. A través de la característica de Transacción Externa, un usuario con licencia de la Cadena de bloques de transacciones de DasCoin puede pasar Euros directamente a su cuenta bancaria desde su cuenta de WebWallet.

Gobernanza de la Red

Nodos de Votación

La gobernanza del DasCoin empieza con Nodos de Votación que son operados en cuentas cartera que contienen al menos 10.000 DasCoins y que se han comprometido a mantener esos DasCoins durante al menos 2 años en un Contrato de Caja Fuerte. Todos los Nodos de Votación podrán opinar sobre el funcionamiento de la red al votar en elecciones regulares para la Junta del DasCoin, al ser activos proponiendo miembros para la Junta del DasCoin y al participar en futuros referendos sobre asuntos de vital importancia.

La Junta de DasCoin

La Cadena de bloques de transacciones del DasCoin permite que la junta directiva regule los parámetros de la red. La Junta de DasCoin estará compuesta de miembros elegidos por los Nodos de Votación. La función de la Junta es:

1. Proponer y modificar los parámetros de la cadena para mantener el funcionamiento y el crecimiento normal de la red.
2. Delegar ciertos papeles ejecutivos a ciertos directivos de la cadena (como expedir licencias y autenticar dichas licencias).
3. Actuar como control del poder de dichos ejecutivos al tener la capacidad de interrumpir su acceso a la red.

La propia Junta no tiene control sobre el estado de la base de datos o de la construcción de la Cadena de bloques de transacciones del DasCoin y está programáticamente impedida para realizar cambios en ella. Como la misma red gestiona y mantiene el estado y el libro de cuentas de transacciones, la única forma de realizar un cambio no deseado es subvertir la mayoría de los Nodos Maestros.

La Junta está diseñada para consistir de 7 Directores individuales, cada uno de los cuales tiene privilegios totales de votación. Generalmente, cada Director estará al mando durante un período de 6 años, aunque los Directores iniciales lo estarán durante períodos escalonados (de 2-6 años) para asegurar la continuidad de la experiencia. Se requiere un mínimo de 3 Directores para gobernar el ecosistema DasCoin y hasta 9 podrían trabajar en la Junta.

Además, habrá un miembro mediador en la Junta que no votará y no tendrá ningún tipo de responsabilidad en la Junta, pero atenderá a todas las reuniones de la Junta y aportará un grado de independencia y de transparencia al proceso de gobernanza de la Junta.

Por último, hay un Director Ejecutivo que trabaja para la Junta y que es responsable de asegurar que todas sus decisiones e iniciativas se aprueben y se apliquen. El Director Ejecutivo atiende a todas las reuniones de la Junta pero no puede votar. El Director Ejecutivo es responsable de supervisar directamente a todas las Autoridades de la Cadena.

Gobernanza de la Red

Autoridades de la Cadena

Los papeles de autoridad de la red existen para asegurar una entrada fluida en la Cadena de bloques de transacciones de los datos de usuario que existen fuera del sistema. El problema con los sistemas totalmente descentralizados es el hecho de que no pueden tener contribuciones fiables: por ejemplo, el Bitcoin se crea internamente en la cadena de bloques de transacciones del Bitcoin y simplemente se transfiere. Para que funcione la Prueba de Valor, debe haber una certeza de que el usuario aporta valor a la red. El valor no puede existir sin un observador independiente: por lo tanto, la única forma de verificar que el usuario ha aportado valor al sistema es mantener a un observador imparcial.

Cada papel de autoridad está configurado de tal forma que:

1. La autoridad no tiene forma de realizar un impacto significativo no deseado en el estado de la red, ya que la red puede retroceder a un estado seguro.
2. Las acciones de la autoridad son comprobadas por una autoridad de autenticación independiente y hay medidas programadas para asegurar que hay una posibilidad mínima de colusión.
3. Hay incentivos por trabajar en beneficio de la red.
4. Cualquier acto malicioso por la autoridad de la cadena será transparente y llevará a que esa cuenta sea marcada como poco fiable, expulsada de la red y penalizada.



Gobernanza de la Red

Operaciones

La Junta fija el procedimiento y asegura la adecuada ejecución de lo siguiente: el nivel de Frecuencia en cada intervalo de 2 semanas; el tamaño de los Bloques de Acuñación al principio de cada Intervalo de Mejora; el tamaño de los Súper Bloques y de los Bloques de Tesorería; las propuestas a enviar a los Nodos de Votación, el uso de los fondos de los Bloques de Tesorería; la autorización de los Nodos Maestros y de los Nodos de Libros de cuentas en la infraestructura de DasNet; la intervención en tiempos de crisis y otros elementos (listados más abajo en los Parámetros de la Junta).

El Director Ejecutivo supervisa el desempeño de todas las autoridades de la cadena y las funciones KYC, gestiona el flujo de propuestas para que las tenga en cuenta la Junta, facilita los referéndums si se han pasado los umbrales adecuados, es responsable de implementar todas las iniciativas y decisiones de la Junta y es totalmente responsable ante la Junta de todas las operaciones dentro del sistema.

Las autoridades de la cadena revisan la emisión y autenticación de las Licencias y de los WebEuros bajo la supervisión del Director Ejecutivo.

La frecuencia se ajusta cada 2 semanas. El proceso implica que la Junta elija cual de una serie de algoritmos refleja mejor el estado de crecimiento actual de la red. Los factores primarios considerados incluyen: la cantidad general de Ciclos en el sistema; la cantidad de Ciclos autorizados en el período más reciente de 2 semanas; la velocidad de crecimiento de los Ciclos en los períodos anteriores y el crecimiento proyectado del Ciclo en el sistema.

Las mejoras ocurren automáticamente en todo el sistema en fechas específicas, empezando por 108 días después del lanzamiento de la Cadena de bloques de transacciones de DasCoin. Es poco probable que ese intervalo se vea alterado en cualquier punto del futuro, pero la Junta podrá hacer ese ajuste si lo considera necesario. Todos los Contratos de Caja Fuerte funcionan también de forma automática. Básicamente, tanto el proceso de acuñación, las Mejoras como los Contratos de Caja Fuerte son contratos inteligentes que se ejecutan automáticamente y se forman directamente en el ecosistema de DasCoin.

Parámetros Globales

A continuación se encuentra el conjunto de parámetros sobre el que la Junta de DasCoin puede proponer cambios:

Autoridad de Expedición de Licencias: El privilegio de asignar una Licencia a una Cuenta de Caja Fuerte y determinar el nivel de la licencia.

Autoridad de Autenticación de Licencias: La capacidad de cancelar la expedición de una nueva Licencia para una cuenta en caso de error.

Autoridad de Expedición de WebEuro: El privilegio de transferir un saldo WebEUR a una Cuenta de Caja Fuerte.

Gobernanza de la Red

Autoridad de Autenticación de WebEuro

La capacidad de cancelar la expedición de un saldo WebEUR a una cuenta en caso de error.

Fecha e Intervalo de Mejora del Ciclo

La fecha exacta de una Mejora y el Intervalo de Mejoras. El Intervalo de Mejoras está actualmente establecido en 108 días y no se espera que sea modificado.

Frecuencia

El factor de conversión por el que los Ciclos pueden ser intercambiados por DasCoins como parte del proceso de acuñación.

Bloque

Una medida de transacciones acumuladas. El sistema registra actualmente un bloque según un período designado conocido como Intervalo de Bloques.

Intervalo de Bloques

El tiempo que tarda en crear una confirmación de un bloque individual de transacciones.

Por defecto, las transacciones se confirman cada 6 segundos. En el futuro, ese tiempo disminuirá a medida que la base de código se optimice.

Bloque de Acuñación

La cantidad de DasCoins distribuidos al completar cada intervalo de acuñación.

Intervalo de Acuñación

El tiempo que un Bloque de Acuñación tarda en crearse. El Intervalo de Acuñación por defecto del sistema es de 10 minutos y no se espera que cambie.

Período de Mantenimiento

El número de bloques que se deben crear antes de que se realice un mantenimiento en la Cadena de bloques de transacciones.

Intervalos Omitidos durante el Mantenimiento

Durante un período de mantenimiento, algunos bloques serán omitidos: este parámetro define cuántos debería omitir el sistema al realizar un Período de Mantenimiento.

Súper Bloque

La cantidad de DasCoins distribuidos al final de cada tipo de Intervalo de Súper Bloques. El tamaño de los Súper Bloques se extrae de un porcentaje de los DasCoins acumulados distribuidos por los Bloques de Acuñación en ese Intervalo de Súper Bloques. Hay 3 tipos de Súper Bloques y cada uno corresponde a un Contrato concreto de Caja Fuerte: Súper Bloques de Votación, Súper Bloques de Libros de cuentas, Súper Bloques Maestros.

Gobernanza de la Red

Intervalos de Súper Bloques

El tiempo que tardan en crearse los Súper Bloques. Hay 3 Intervalos de Súper Bloques en el sistema y cada uno corresponde con un tipo de Súper Bloque. Los Intervalos de Súper Bloques de Votación duran 1 semana, los Súper Bloques de Libros de cuentas duran 2 semanas y los Súper Bloques Maestros duran 3 semanas.

Bloque de Tesorería

La cantidad de DasCoins distribuidos al final de un Intervalo de Bloque de Tesorería. Como los Súper Bloques, los Bloques de Tesorería se extraen de un porcentaje de los DasCoins acumulados distribuidos por los Bloques de Acuñación en el Intervalo de Bloques de Tesorería.

Intervalo de Bloque de Tesorería

El tiempo que tarda en crearse un Bloque de Tesorería. Los Intervalos del Bloque de Tesorería duran 4 semanas.

Tamaño Máximo del Bloque

Tamaño máximo en bytes que puede tener un bloque que está dentro de la Cadena de bloques de transacciones.

Tamaño Máximo de la Transacción

Es el tamaño máximo admisible en bytes para una sola transacción.

Número Máximo de Testigos

Es el número máximo de Nodos Maestros que pueden estar activos en la red.

Hash de cuenta/longitud del nombre:	entre 3 y 63 caracteres
Tamaño de la transacción:	1024B
Tiempo entre bloques:	6 segundos.
Tiempo entre intervalos de mantenimiento:	1 día
Duración del mantenimiento (número de bloques omitidos):	3 bloques
Tiempo entre Mejoras:	108 días
Tiempo entre acuñación (intervalo de acuñación):	10 minutos

Eficiencia General del Sistema

El Bitcoin y las cadenas basadas en las bifurcaciones del Bitcoin se apoyan en una base de datos de objetos UTXO para seguir la pista a los saldos de las monedas de cada dirección/cuenta. En el Bitcoin, cada transacción consume (gasta) el saldo de las transacciones anteriores y produce un nuevo saldo para ser consumido en futuras transacciones, formando así un nuevo Saldo de Transacción Sin utilizar (UTXO) que solo puede ser consumido una vez. Aunque este modelo tiene ciertas propiedades matemáticas beneficiosas y se usa para evitar gastar el doble en bitcoins, también sufre de graves restricciones: es innecesariamente complicado y no tiene un estado inherente y, por tanto, no está capacitado de forma natural para aplicaciones con un estado inherente, como la manipulación de activos personalizados y guardar el estado de ejecución de contratos inteligentes.

La Cadena de bloques de transacciones de DasCoin cuenta con un estado de cadena compartido: una memoria de la base de datos sobre el estado de los objetos relacionados con los datos de usuario como por ejemplo la cuenta, los saldos de DasCoin (y, posiblemente, otros activos), la información de acuñación (como la Cola de Acuñación de DasCoin), información sobre la ejecución de contratos inteligentes, etc. Los nodos de la Cadena de bloques de transacciones forman el estado al aplicar las transacciones de los bloques anteriores. El consenso de estado se consigue al seguir la cadena más larga de bloques que encuentra el nodo. El estado de la Cadena de bloques de transacciones es totalmente reproducible al aplicar las transacciones en orden.

Uno de los objetivos principales de la Cadena de bloques de transacciones del DasCoin es tener transacciones rápidas. Como cada nodo almacena el estado compartido en la memoria, las transacciones pueden ser validadas rápidamente por toda la red. Esto aumenta enormemente el número de transacciones que se pueden incluir en un bloque e incrementa el rendimiento general de la red. Como no se solicita una Prueba de Trabajo para firmar un bloque, cada testigo puede recolectar y verificar rápidamente las transacciones con el estado global, formar un bloque de transacciones válidas, firmarlas con su clave de firma de bloques y enviar el bloque firmado al resto de la red. Los nodos también pueden restaurar las transacciones en caso de que haya un fallo de consenso, tanto en caso de que se rechace el bloque (a causa de que haya habido una bifurcación más corta en una resolución de bifurcaciones) o a causa de que la transacción caduque sin ser incluida en ninguno de los bloques.

Verificación de la Integridad de la Cadena de bloques de transacciones

La Cadena de bloques de transacciones de DasCoin es una serie de bloques enlazados criptográficamente. Estos bloques establecen un registro permanente de transacciones que han sido verificadas y confirmadas por los Nodos Maestros que mantienen y registran los privilegios de la Cadena de bloques de transacciones. Por lo tanto, cada acción almacenada en la Cadena de bloques de transacciones tiene un identificados permanente y único.

Por estas características, el historial completo de actividades de la Cadena de bloques de transacciones puede ser reproducido y se puede comprobar su integridad en cualquier momento. Se puede autorizar que un auditor utilice herramientas programáticas que evalúen y comprueben que los saldos de todas las acciones sean consistentes y correctos. Esto excluye la capacidad de que cualquier actor central, operador de la Cadena de bloques de transacciones o intruso pueda manipular los contenidos de la Cadena de bloques de transacciones. Todas las acciones requieren la firma del propietario del contenido para impulsar un nuevo cambio. Los propietarios de la cuenta son los únicos que pueden hacer que haya cambios en sus saldos y los operadores no pueden realizar transferencias maliciosas o forzadas o modificar los saldos.

Como parte del protocolo de supervisión de la Junta responsable, se requiere que una firma contable externa e independiente sea contratada para verificar la autenticidad de todas las actividades de la Cadena de bloques de transacciones. Se pagará a esa firma con los fondos de Tesorería que son controlados por la Junta y tendrá acceso a al menos 2 Nodos de Libro de cuentas, para los que tendrán acceso completo para consultar y analizar según el protocolo de verificación que han diseñado. La verificación de la precisión y de la integridad de la Cadena de bloques de transacciones del DasCoin tendrá lugar de forma mensual y el resultado de esos protocolos de pruebas estará disponible para todos los participantes del sistema DasNet.

El propósito del protocolo de verificación de integridad mensual de la Cadena de bloques de transacciones es incrementar la fiabilidad del sistema. El protocolo se ha diseñado para proteger la seguridad de la red y la privacidad de sus participantes al dar a una firma de contabilidad externa un acceso completo a Nodos de Libro de cuentas activos del sistema y ofrecer una transparencia completa sobre las operaciones generales de la Cadena de bloques de transacciones de DasCoin.

Expansión y Adopción

El sistema incrementará su valor de utilidad a medida que más y más gente participe en la red. Para conseguir el objetivo de expandir la red, se ha creado un sistema de marketing basado en referencias en el software de la red para premiar la contribución de cada participante según su impacto individual en el crecimiento de la red. Por tanto, en lugar de usar recursos para cubrir los costes del minado en base a la prueba de trabajo, la red ofrece incentivos a sus participantes por expandir la red.

Este tipo de sistema de incentivos es posible por las eficiencias inherentes del modelo de consenso de Prueba de Licencia. En lugar de incurrir en la carga financiera de proteger una red de configuración abierta con servidores entre pares, la Cadena de bloques de transacciones de DasCoin emplea el método significativamente más eficiente de llegar a un consenso.

Al equilibrar aspectos de la centralización con elementos de la descentralización, el sistema es capaz de auto-gestionarse a través de un método de consenso adecuadamente aleatorio pero muy eficiente. Como incorpora una arquitectura de sistema cerrado, la red puede beneficiarse de todas las ventajas del protocolo de cadena de bloques de transacciones pero sin todas los problemas de gastos, ineficiencias y seguridad de una arquitectura descentralizada de sistema abierto. La eficiencia resultante de este modelo de cadena de bloques de transacciones permissionado combinado con los acuerdos de licencia permite que la red ofrezca incentivos para que los participantes promuevan y expandan los beneficios de la red por el mundo.

El sistema está diseñado para tener en cuenta los riesgos inherentes de una nueva red y para premiar a los participantes según su impacto en el crecimiento de la red. Esta dinámica proporciona un potente marketing de confianza a la expansión de la red.

Conclusión

Hasta ahora, no ha habido un énfasis suficiente en los requisitos de infraestructura en la fundación de las cadenas de bloques de transacciones, específicamente en los elementos relativos a la fiabilidad, la disponibilidad, la escalabilidad y el mantenimiento. Éstos son factores cruciales para asegurar que la cadena de bloques de transacciones puede jugar un papel viable en las vidas financieras de los usuarios generales. A la tecnología de las cadenas de bloques de transacciones le faltaba todo un nivel de garantía de calidad sobre todo a causa de las limitaciones inherentes de la naturaleza descentralizada de la mayoría de tecnologías de cadena de bloques de transacciones.

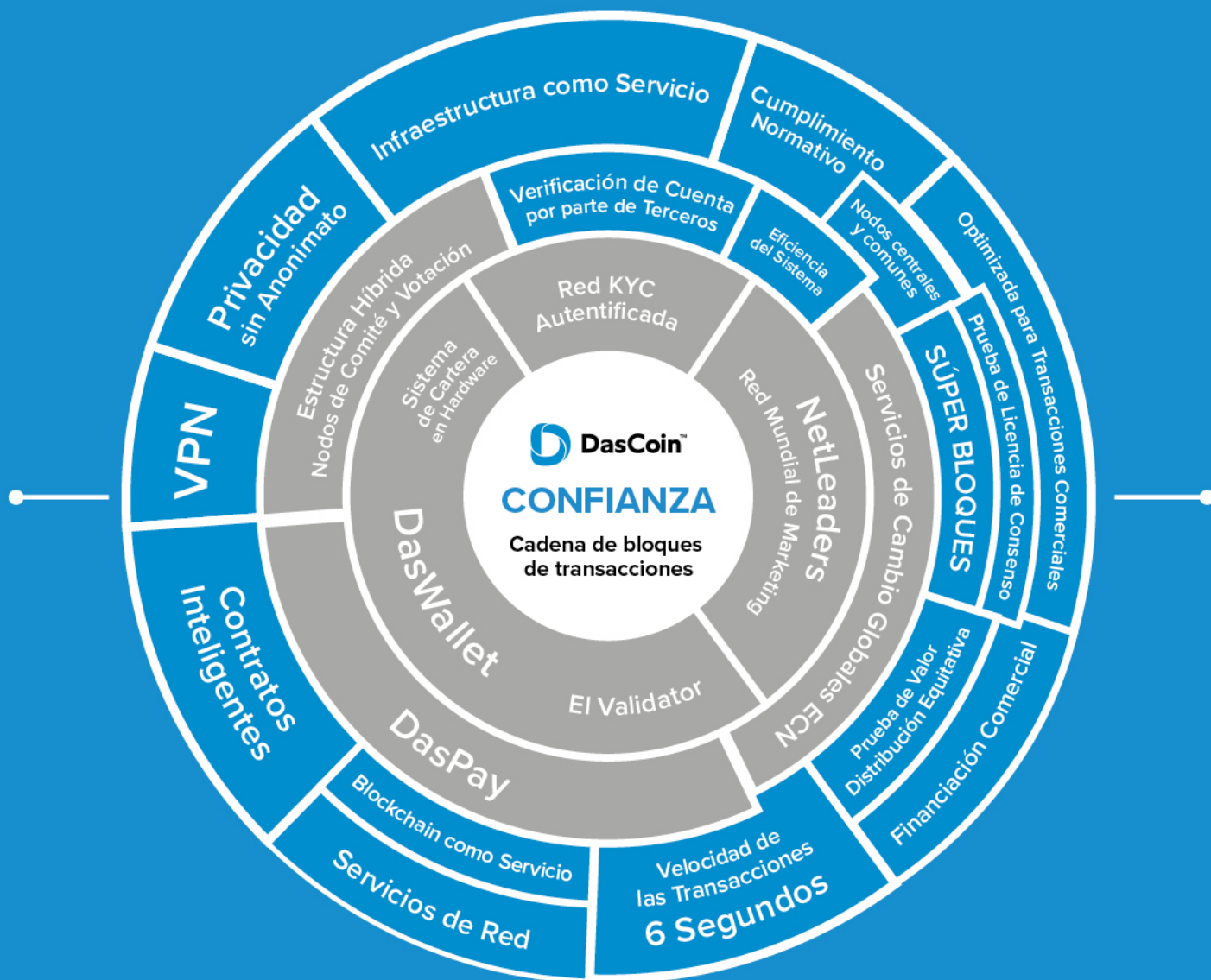
DasCoin ha sido diseñado para abordar los problemas que han evitado que las monedas digitales sean adoptadas por todos los usuarios en general. DasCoin está estructurado para ofrecer mayor seguridad, eficiencia, rendimiento y escalabilidad. El ecosistema DasCoin también potencia la eficiencia de su infraestructura para incentivar su expansión. El resultado es un sistema de valor digital que ha sido construido en las bases de una moneda sólida y está perfectamente preparado para atraer a usuarios generales de todo el mundo.

La consecuencia del sistema DasCoin es la realización completa del Internet de Confianza, en el que los usuarios autenticados pueden intercambiar todo tipo de activos en una red virtual privada especializada. Lo que se hace posible es un mundo lleno de transacciones transfronterizas realizadas con todo tipo de activos digitales diferentes y completadas en cualquier parte del mundo, en cualquier momento del día o de la noche y de forma instantánea, segura y sin ningún coste. Y este no es más que el principio de lo que es posible realizar con el ecosistema DasCoin.

Al adaptar la confianza al paradigma digital, podemos acceder a todas estas posibilidades. La confianza es la moneda de DasCoin y DasCoin es la moneda de confianza. A medida que se haga realidad, DasCoin desbloqueará niveles de prosperidad sin precedentes en el mundo.

SEGURIDAD

REVALORIZACIÓN DE CAPITAL



UTILIDAD

LIQUIDEZ



DasCoin™

Copyright 2017
DasCoin.com