STABILA
CADENA PÚBLICA

Descentralizar el Sistema Financiero

LIBRO BLANCO

Construyendo finanzas descentralizadas.

CADENA PÚBLICA STABILA

1. INTRODUCCIÓN

STABILA es un proyecto dedicado a la descentralización del sistema financiero. El protocolo STABILA ofrece servicio público de blockchain y soporte de alto rendimiento, alta escalabilidad y alta disponibilidad para todas las aplicaciones descentralizadas (Dapps, por sus siglas en inglés) en el ecosistema STABILA.

"La transformación digital permite al mundo reinterpretarse a sí mismo, y Moneta se complace en estar entre los impulsores del cambio mediante la habilitación de servicios centrados en el cliente y relaciones duraderas."
www.stabilascan.org

2 TERMINOLOGÍA

Dirección/Billetera

Mediante una clave emparejada, compuesta por una clave privada y una clave pública, se genera una dirección, o billetera, constituida por las credenciales de cuenta en la red STABILA. Generalmente, la clave pública se utiliza para la verificación de firma, encriptado de la clave de sesión y el de aquellos datos que pudiesen ser desencriptados a través de la correspondiente clave privada.

ABI

La interfaz binaria de aplicación (ABI, por sus siglas en inglés) es una interfaz entre dos módulos de programa binario; a menudo, uno de estos módulos es una librería o un sistema operativo en lenguaje de máquina, y el otro es un programa ejecutado por el usuario.

API

La interfaz de programación de aplicaciones (API, por sus siglas en inglés) se utiliza, principalmente, para desarrollos usuario clientes. Con el soporte de API, los propios desarrolladores también pueden diseñar las plataformas que emiten tokens.

Activo

En los documentos de STABILA, activo equivale a token, el cual también se denota como token TRC-10.

Puntos de ancho de banda (BP)

Para mantener el funcionamiento fluido de la red, las transacciones de la red STABILA utilizan puntos de ancho de banda (BP, por sus siglas en inglés) como gas. Cada cuenta recibe 500 BP diarios de forma gratuita y pueden incrementarse cediendo (contratos de depósitos) STB por BP. Ambas transferencias de tokens, STB y TRC-10, son transacciones normales que cuestan BP. Las transacciones de implementación y ejecución de contratos inteligentes consumen tanto BP como unidades de recursos convencionales (UCR, por sus siglas en inglés).

Bloques

Los bloques contienen los registros digitales de las transacciones. Un bloque completo consiste del número, tamaño del bloque, encabezado del bloque, contador de transacciones y datos de la transacción.

Recompensa de Bloque

Las recompensas por la producción de bloques se envían a una subcuenta (dirección/billetera). Los Gobernadores (Governors) y Ejecutivos (Executives) pueden reclamar sus recompensas en stabilascan o directamente a través de la API.

Encabezado de Bloque

El encabezado de bloque es parte del bloque. Los encabezados de bloque de STABILA contienen el hash del bloque anterior, la raíz de Merkle, fecha y hora, versión y la dirección del testigo.

Billetera Fría

La billetera fría, también conocida como monedero offline, mantiene la clave privada completamente desconectada de cualquier red. Usualmente, estas billeteras se instalan en dispositivos "fríos" (por ejemplo, computadoras o teléfonos móviles que permanecen offline) a fin de garantizar la seguridad de la clave privada de STB.

DApp

Una aplicación descentralizada es aquella que no depende de una entidad de confianza centralizada para su funcionamiento. Permite la interacción, acuerdos y comunicación directa entre usuarios finales y/o recursos sin necesidad de intermediarios.

gRPC

La llamada a procedimiento remoto (RPC, por sus siglas en inglés) es un protocolo de código abierto inicialmente desarrollado por Google. Utiliza HTTP/2 como transporte, búfers de protocolo (protobuf) como lenguaje de descripción de interfaz y provee características como autenticación, transmisión bidireccional y control de flujo, vínculos de bloqueo o de no bloqueo, al igual que cancelación y tiempos de expiración. Las llamadas cliente-servidor tienen una estructura multilenguaje y multiplataforma. Los casos más comunes de uso incluyen la conexión de servicios en arquitectura tipo microservicios, así como también la conexión de clientes de dispositivos móviles, y también navegadores, a los servicios backend.

Billetera Caliente

La billetera caliente, también conocida como monedero en línea, permite que la clave privada del usuario sea utilizada en línea, por lo que pudiera hacerla susceptible a posibles vulnerabilidades o a ser interceptada por actores maliciosos.

JDK

Java Development Kit es el SDK de Java utilizado en aplicaciones Java. Es el núcleo del desarrollo de Java, comprendiendo el entorno de aplicaciones Java (JVM + librería de clases de Java) y herramientas Java.

LevelDB

LevelDB fue inicialmente adoptado con el fin de alcanzar los requisitos de un R/W veloz y un desarrollo rápido.

Raíz de Merkle

La raíz de Merkle es el hash de todos los hashes de todas aquellas transacciones que forman parte de un bloque del blockchain.

Testnet Pública

Es una versión de la red ejecutada en una configuración de tres nodos. Los desarrolladores pueden conectar y probar funciones sin preocuparse por las pérdidas económicas. Los tokens de Testnet no tienen valor y cualquiera puede solicitar más del grifo público.

RPC

En computación distribuida, una llamada a procedimiento remoto (RPC, por sus siglas en inglés) es un programa codificado como si fuera una llamada a procedimiento normal (local), utilizado por una computadora para ejecutar un procedimiento (subrutina) en otro espacio de direcciones (usualmente, otra computadora en una red compartida) sin que se necesite explícitamente codificar los detalles para la interacción remota.

Escalabilidad

La escalabilidad es una característica del protocolo STABILA. Es la capacidad de un sistema, red o proceso para manejar un aumento del trabajo o su potencial de ampliación a fin de adaptarse a ese crecimiento.

UNIT

UNIT es la unidad más pequeña de STB. 1 STB = 1.000.000 UNIT.

Rendimiento

El alto rendimiento es una característica de STABILA Mainnet. Se mide en transacciones por segundo (TPS). Más específicamente, la máxima capacidad de transacción en un segundo.

Marca de tiempo

El tiempo aproximado en el que se produce un bloque se registra como marca de tiempo Unix, que es la cantidad de milisegundos transcurridos desde las 00:00:00 del 01 de enero de 1970 UTC.

TRC-10

Es un estándar de cripto token en la plataforma STABILA. Se requiere de ciertas reglas e interfaces al momento de llevar a cabo una oferta inicial de monedas en el blockchain STABILA.

STB

STB simboliza a Stabila, la criptomoneda oficial de STABILA.

3 ARQUITECTURA

STABILA tiene una arquitectura de 3 capas.

1. *Capa de almacenamiento.*
2. *Capa de núcleo.*
3. *Capa de aplicación.*

El protocolo STABILA se adhiere al protobuf de Google, el cual intrínsecamente admite extensiones multilenguaje.

Máquina Virtual STABILA (SVM)

La SVM es una liviana y completa máquina virtual de Turing. La SVM se conecta ininterrumpidamente con el ecosistema existente.

Exchange Descentralizado (DEX)

La red STABILA soporta funciones exchange descentralizadas (DEX, por sus siglas en inglés) en forma nativa. Un exchange descentralizado consta de múltiples pares de trading (exchange). Un exchange es un mercado de intercambio entre tokens TRC-10, o entre un token TRC-10 y STB. Todas las cuentas pueden crear un par de trading entre cualquier token.

El código de blockchain de STABILA está implementado en Java y originalmente fue una derivación de STABILA.

4 CONSENSO

Prueba de Participación Delegada (DPoS)

La prueba de participación (PoS, por sus siglas en inglés), como mecanismo de consenso, fue propuesto por muchas redes nuevas. En las redes PoS, los poseedores de tokens bloquean sus saldos en tokens para convertirse en validadores de bloques. Estos se turnan para proponer y votar el siguiente bloque. No obstante, el problema con el PoS estándar es que la influencia del validador está directamente correlacionada con la cantidad de tokens bloqueados. Ello da como resultado el acaparamiento de grandes cantidades de la moneda base de la red por parte de las partes, ejerciendo una influencia indebida en el ecosistema de la red.

El mecanismo de consenso de STABILA utiliza un innovador sistema de prueba de participación delegada (DPoS, por sus siglas en inglés) en el que 21 Gobernadores (G) producen bloques para la red. Cada 6 horas, los titulares de cuentas STB que hayan creado contratos de depósitos pueden votar por una selección de Ejecutivos, considerándose Gobernadores a los 21 Ejecutivos más votados.

La red de protocolo STABILA genera un bloque cada tres segundos.

5 CUENTA

Tipos de cuentas de la red STABILA.

1. *Regular: cuentas utilizadas para transacciones habituales.*
2. *Token: cuentas utilizadas para almacenar tokens TRC-10.*
3. *Contrato: cuentas de contrato inteligente creadas por cuentas regulares, las cuales pueden también activarse por cuentas regulares.*

Creación de Cuenta

Existen tres formas de crear una cuenta STABILA:

1. *A través del API.*
2. *Por transferencia de STB a una nueva dirección de cuenta.*
3. *Por transferencia de tokens TRC-10 a una nueva dirección de cuenta.*

Generación de Claves Privadas y Direcciones

Pueden generarse claves offline emparejadas, las cuales constan de una dirección (clave pública) y una clave privada. El algoritmo para la generación de las direcciones de usuario consiste en generar una clave emparejada, para luego extraer la clave pública (arreglo de bytes de 64 bytes que representa las coordenadas x, y). Hacer el hash de la clave pública usando la función SHA3-256 (el protocolo SHA3 adoptado es KECCAK-256) y extraer los últimos 20 bytes del resultado. Añadir 3F al inicio de la matriz de bytes y asegurar que la longitud de la dirección inicial sea de 21 bytes. Hacer un hash doble de la dirección usando la función SHA3-256 y tomar los primeros 4 bytes como código de verificación. Agregar el código de verificación al final de la dirección inicial y obtener la dirección en formato Base58Check, mediante la codificación base58. Una dirección Mainnet codificada comienza con S y tiene una longitud de 34 bytes.

6 TRANSACCIÓN

Firma

El proceso de firma de las transacciones de STABILA sigue un algoritmo criptográfico ECDSA estándar, con una curva de selección SECP256K1. Una clave privada es un número aleatorio y la clave pública es un punto en la curva elíptica. El proceso para la generación de esta última consiste en generar primero un número aleatorio como clave privada y después multiplicar el punto base de la curva elíptica por la clave privada para así obtener la clave pública. Al producirse una transacción, primero se convierten a formato de bytes los datos sin procesar de esta para después someterlos a un hash SHA-256. Luego, la clave privada correspondiente a la dirección del contrato firma el resultado del hash SHA256, y el resultado de la firma se añade a la transacción.

7 ANCHO DE BANDA

Modelo de Ancho de Banda

Las transacciones ordinarias solo consumen puntos de ancho de banda, pero las operaciones de los contratos inteligentes consumen tanto unidades de recursos convencionales (UCR) como puntos de ancho de banda (BP).

Tipos de Puntos de Ancho de Banda Disponibles

Los usuarios pueden ganar puntos de ancho de banda mediante la creación de contratos de depósitos (CD) con STB, en tanto que diariamente también están disponibles 500 puntos de ancho de banda gratuitos. Cuando se emite una transacción STB, esta se transmite y almacena en forma de arreglo de bytes a través de la red.

Puntos de ancho de banda consumidos por una transacción = Número de bytes de la transacción multiplicado por la tasa de puntos de ancho de banda.

***Ejemplo**:*

Si la longitud del arreglo de bytes de una transacción es 200, entonces la transacción consume 200 puntos de ancho de banda.

No obstante, si una transferencia STB o token resulta en la creación de la cuenta de destino, solo los puntos de ancho de banda consumidos para crearla serán deducidos y no se deducirán los adicionales.

En el caso de la creación de cuentas, la red primero consumirá los puntos de ancho de banda que el iniciador de transacción obtuvo al crear CDs de STB. Si esta cantidad fuese insuficiente, la red entonces consumirá el STB del iniciador de transacción. En los casos estándar de transferencia de STB entre una cuenta STB y otra, la red primero consumirá los puntos de ancho de banda ganados por el iniciador de transacción por crear CDs STB. Si eso fuese insuficiente, consumirá de los 500 puntos de ancho de banda diarios gratuitos. Si aún así continuase siendo insuficiente, entonces la red consumirá el STB del iniciador de transacción.

El monto se calcula multiplicando por 6 UNIT el número de bytes en la transacción. De ahí, que para muchos de los poseedores de STB que no crean CDs para participar en la votación de Gobernadores, el primer paso se omite automáticamente (pues el balance CD de STB = 0) y es el ancho de banda diario gratuito de 500 lo que impulsa la transacción.

Para las transferencias de tokens TRC-10, la red primero verifica si es suficiente el total de puntos de ancho de banda gratuitos del activo token emitido. De no serlo, se consumirán los puntos de ancho de banda obtenidos por crear CD STB. Y si aún no fuesen suficientes, entonces consumirá el STB del iniciador de transacción.

8 COMISIÓN

Comisión

Generalmente, la red STABILA no cobra comisiones por la mayoría de las transacciones; empero, debido a restricciones del sistema y la equidad, el uso del ancho de banda y las transacciones sí pagan ciertas comisiones.

1. *Las transacciones normales cuestan puntos de ancho de banda.*
2. *Los contratos inteligentes cuestan UCR, pero también requerirán puntos de ancho de banda para que la transacción se emita y confirme.*
3. *Todas las transacciones de consulta son gratuitas. No cuestan UCR ni ancho de banda.*

La red STABILA también tiene establecido un conjunto de comisiones fijas para las siguientes transacciones:

1. *Creación de un nodo testigo: 1000 STB*
2. *Emisión de un token TRC-10: 1000 STB*
3. *Creación de una nueva cuenta: 1385 UNIT*
4. *Creación de un par de exchange: 14 STB*

Confirmación de Transacción

Una transacción se incluye en un bloque futuro luego de emitirse en la red. La transacción se confirma después de haberse minado 19 bloques en STABILA (incluyendo el propio). Cada bloque se produce por uno de los 21 Gobernadores y tarda 3 segundos en ser minado al blockchai.

9 MÁQUINA VIRTUAL STABILA

Máquina Virtual STABILA (SVM)

La SVM es una liviana y completa máquina virtual de Turing desarrollada para el ecosistema de STABILA. Su objetivo es proveer un servicio blockchain eficiente, conveniente, estable, seguro y escalable. La SVM inicialmente derivó de STABILA y puede conectarse ininterrumpidamente con el ecosistema existente de desarrollo de contratos inteligentes Solidity.

Adicionalmente, la SVM soporta consenso DPoS y emplea el concepto de UCR. Las operaciones de transacciones y contratos inteligentes en SVM son gratuitas, sin consumo de STB.

El compilador primero traduce el contrato inteligente Solidity a un código de bytes legible y ejecutable en la SVM. Después, la SVM procesa los datos por medio del código de operación, equivalente a operar la lógica de una máquina de estados finitos basada en pilas.

10 CONTRATOS INTELIGENTES

Compatibilidad

La SVM es compatible con EVM y en el futuro también lo será con más máquinas virtuales prevalecientes. Sin embargo, debido a la naturaleza fraudulenta de los contratos inteligentes, se propone un proceso de autorización, o licencia, antes de que cualquier usuario pueda implementar un contrato inteligente.

Licencia de los Contratos Inteligentes

Los contratos inteligentes son inútiles y continuarán siéndolo en el futuro próximo. Carecen de un mecanismo para probar el respaldo de activos y no pueden comunicarse con el mundo exterior. El modelo de licencias, o autorizaciones, propuesto es para permitir únicamente aquellos contratos inteligentes que tengan un uso real y estén respaldados por activos a través de la lógica subyacente y la estructura corporativa. En caso de que el propietario del contrato inteligente no pueda continuar manteniéndolo, un tercero asumiría la responsabilidad, de tal forma de proteger a los clientes en la red STABILA.

Modelo de Unidades de Recursos Convencionales (UCR)

El límite máximo de UCR para implementar y activar un contrato inteligente es una función de varias variables:

- *UCR dinámico por crear CD de 1 STB = 30.000.000.000 (Límite total de UCR) / (Peso total de UCR).*
- *El límite de UCR es el límite diario de UCR de la cuenta por la creación del CD de 1 STB.*
- *El restante UCR diario de la cuenta por la creación del CD de STB se calcula como: UCR Límite - UCR Usado.*
- *El límite de la comisión en STB se establece en la implementación del contrato inteligente/llamada de activación.*
- *El restante STB utilizable en la cuenta.*

La funcionalidad del contrato inteligente se activará en febrero de 2022.

11 GOBERNANZA

Gobernadores

Todas las cuentas de la red STABILA pueden postularse y tener la oportunidad de convertirse en Ejecutivo (E). Todos pueden votar por los Ejecutivos. Los 21 Ejecutivos más votados se convertirán en Gobernadores (G), los cuales tendrán el derecho y la obligación de generar bloques. Los votos se cuentan cada 6 horas y los G cambiarán consecuentemente. Para prevenir ataques maliciosos, el convertirse en Ejecutivo trae aparejado un precio: al aspirante se le cargarán 1000 STB a su cuenta al momento de postularse. Logrado esto, dicha cuenta puede unirse a la elección de los G.

Elección

Se necesita STABILA Power (SP) para votar y la cantidad de SP depende de los activos del votante creados por CD (STB). El SP se calcula de la siguiente manera: 1 SP = 1 STB CD para obtener ancho de banda.

Todas las cuentas de la red STABILA tienen derecho a votar por sus propios Gs. Después del lanzamiento (sin cd, disponible después de 3 días), los usuarios no tendrán ningún activo en CD y, consecuentemente, pierden todos los SP. Como resultado, todos los votos se invalidarán para las rondas de votación en curso y futuras, a menos de que nuevamente se cree CD de STB para votar.

Recompensa de los Ejecutivos

También conocido como Executive Reward, los 79 Ejecutivos más votados, actualizados una vez por ronda (6 horas), compartirán 78 STB como minado. La recompensa se dividirá conforme al peso de los votos que cada Ejecutivo reciba.

Recompensa E total por ronda = 10.972 Unit/bloque × 20 bloques/min × 60 minutos/hora × 6 horas/ronda.

Anualmente, se otorgará un total de 28.834 STB a los 79 Es.

Recompensa por Bloque

También conocido como Governor Reward, los 21 Ejecutivos más votados (G), quienes serán electos cada ronda (6 horas), compartirán un aproximado de 1.596 STB minados. La recompensa se dividirá a partes iguales entre los 21 Gs.

Recompensa total por ronda = 221.714 Unit/bloque x 20 bloques/min x 60 minutos/hora x 6 horas/ronda.

Anualmente, se otorgará un total de 2.330.657 STB a los 21 Gs

12 CONFIGURACIÓN DE LA CADENA STABILA

Suministro Circulante *Cantidad de monedas STB disponibles públicamente y circulando en el mercado.*	**20.000.000**
Suministro total *Cantidad de STB existente actualmente que está bien sea en circulación o bloqueada para los mineros.*	**30.000.000**
Suministro Máximo *Número máximo de monedas STB que se crearán.*	**30.000.000**
Velocidad de producción de bloques *Segundos por 1 bloque producido.*	**3**
Mineros/Gobernadores *Nodos productores de bloques.*	**21**
Consenso *70% de los 21 gobernadores para lograr un consenso sobre la producción del próximo bloque.*	**15**
1 STB = () Units *UNIT es la unidad más pequeña de STB*	**1.000.000**

GRACIAS

“Lo que tenemos es una maduración del mercado cripto, y encontramos a inversionistas y operadores sintiéndose más cómodos al entender los fundamentos en torno a lo que están comprando.”

Daniel Varzari, CEO

“Blockchain es un nuevo paradigma tecnológico de nuestro tiempo. Fundamentalmente, cambiará los principios laborales de todo el mundo financiero.”

Igor Scvortov, CFO

“Un día, en nuestro futuro cercano, todo será ‘tokenizado’ y conectado utilizando blockchain.”

Anastasia Kovaleva, VP Asia

STABILA

MONETA HOLDINGS LLC

San Vincente y Las Granadinas

Primer piso
Edificio First St. Vincent Bank Ltd.
James Street
Kingstown

BLOCKCHAIN TECHNOLOGY

Construyendo finanzas descentralizadas.

info@moneta.holdings

info@stabilascan.org