ESP

ORBIS
YELLOW PAPER

BLOCKCHAIN – ORBIS, COMO LA SUPERIORIDAD SOBRE EL FUTURO.

Reseña histórica

En 1982, D. Chaum propuso un algoritmo de firma ciega e introdujo el concepto de dinero digital. S. Haber y S. Stornetta presentaron en 1991 una descripción teórica de un sistema para certificar la inmutabilidad de los documentos basado en marcas de tiempo. El mecanismo de prueba de trabajo (PoW) fue propuesto por A. Back en el proyecto Hashcash para prevenir envío de correo basura. La idea de contratos inteligentes fue propuesta por N. Szabo en 1996. N. Szabo también propuso un protocolo para el dinero digital Bitoro en 1998, que fue publicado en 2005; se basó en el cálculo de la cadena de bits y utilizó el mecanismo de consenso PoW. Pero el sistema no se implementó en la práctica y fue propenso a los ataques Sybil.

Blockchain ORBIS es una organización autónoma descentralizada DAO ORBIS.

La organización autónoma descentralizada (DAO) es una forma organizacional, en la que la coordinación de las actividades de participantes y la gestión de recursos se realizan de acuerdo con un conjunto de reglas acordadas y formalizadas de antemano, el control de su ejecución se realiza automáticamente.

Blockchain ORBIS es un protocolo BaaS (Blockchain-as-a-Service) descentralizado orientado a servicios para capturar hechos de creación y rotación de derechos sobre valores digitales.

Modelo tokenómico

Blockchain ORBIS prevé la emisión de monedas de tres tipos:

1. **ORB Coin (ORBC) es la moneda básica del Blockchain ORBIS. Mediante la moneda ORBC los usuarios reciben los productos y servicios digitales de ORBIS.**

Datos de la moneda ORB Coin

Nombre: ORB Coin.
Símbolo: ORBC.
Volumen máximo de emisión: 42 000 000.
Valor de bits: 10^{-8}.

Comisión por transacción: 0% hasta que se realice la votación de DAO, pero no antes de 1 año desde el lanzamiento del Blockchain ORBIS.
Costo inicial: 1$ por 1 coin.

2. ORB Mining (OM) es el token, la posesión del cual da los derechos a:

- Ser miembro de DAO ORBIS.
- Recibir ORBC como resultado de minería del 62% de ORBC emitidos.
- Recibir el 38% de ORBC emitidos por la validación de las transacciones en la red ORBIS.
- Participar en la gestión de DAO ORBIS.

Datos del token ORB Mining

Nombre: ORB Mining.
Símbolo: OM.
Volumen máximo de emisión: no limitado.
Valor de bits: 1.
Minería: 0,314 % cada semana de las monedas restantes en el contrato inteligente de minería. En total, se supone emitir 42 millones de ORBC.
Condición de obtención de un token: transacción en el contrato inteligente de minería en la cantidad de 10 000 ORBC por 1 OM. Cuando el usuario recibe OM, las monedas ORBC se devuelven en volumen total de las monedas no minadas.

Cuando en un contrato de minería inteligente se alcanza un saldo de 10 000 000 ORBC, DAO puede cambiar los porcentajes de distribución de la minería entre los validadores y los titulares de OM.

Los ORBC minados son las monedas que se minan el sábado de cada semana a las 24:00 GMT con ayuda de tokens de minería ORB Mining.

La minería se lleva a cabo una vez a la semana y se calcula según la fórmula:

$$V_i = K*((V_{start} - \sum_{i=0}^{N} V_{i-1}) + \sum_{i=0}^{N} V_{OM_i} + \sum_{i=0}^{N} (V_{K1_i} + V_{K2_i} + V_{K3_i} + V_{K4_i} + V_{K5_i}))$$

donde

V_i - Volumen de minería de ORBC en la semana i;
K - Coeficiente de minería equivalente a 0.314%;
V_{start} - Constante: volumen total de emisión de ORBC (42 000 000);
$\sum_{i=0}^{N} V_{i-1}$ - Suma de ORBC minados antes de la semana i;
$\sum_{i=0}^{N} V_{OM_i}$ - Volumen de ORBC recibidos de la generación de ORB Mining (OM), a la semana i;
V_{K1_i} - Comisión por la transferencia de ORBC en la semana i;
V_{K2_i} - Comisión por la transferencia de token a ORBC en la semana i;
V_{K3_i} - Comisión por la transacción de servicio en ORBC en la semana i;
V_{K4_i} - Comisión por el registro de tokens utilitarios en ORBC en la semana i;
V_{K5_i} - Comisión por el registro de servicios en ORBC en la semana i;

3. Tokens que pueden ser emitidos por los participantes de la red ORBIS para organizar un servicio digital en Internet.

Datos de los tokens

Nombre: cualquier nombre en letras latinas.
Símbolo: no más de 4 letras latinas mayúsculas.
Volumen máximo de emisión: el número de dígitos significativos de un token emitido es de 18 dígitos, incluidos los dígitos después del punto. Al mismo tiempo, la coma puede estar en cualquier lugar entre los caracteres del 10 al 17. Valor de bits: hasta 10
Comisión por emisión de tokens: 1 ORBC (el importe de la comisión puede ser cambiado por la decisión de DAO)

Comisión por transacción: 0, hasta que se realice la votación de DAO, pero no antes de 1 año desde el lanzamiento del Blockchain ORBIS.

4. Además del uso de tokens en la red ORBIS, existe la posibilidad de que los usuarios creen productos y servicios digitales, cuyo propósito es utilizar los datos almacenados en Blockchain ORBIS y almacenar los datos generados por los servicios de usuario a través de transacciones de datos.

Datos de los servicios de usuario

Nombre: cualquier nombre
Lenguaje de programación: cualquier lenguaje
Canal de comunicación con nodos de ORBIS: Rest API ORBIS
Volumen de datos en una transacción: ~ 500 bytes
Comisión por transacción de datos: 0, hasta que se realice la votación de DAO, pero no antes de 1 año desde el lanzamiento del Blockchain ORBIS.
Comisión por registro del Servicio: 1 ORBC (el importe de la comisión puede ser cambiado por la decisión de DAO).

Todas las comisiones cobradas en la red Blockchain ORBIS se envían al contrato inteligente de minería.

Administración de DAO ORBIS

La administración en DAO ORBIS se realiza por los titulares de OM, que autoriza para la minería y la gestión en Blockchain ORBIS. Para hacerse un titular de 1 OM es necesario enviar 10 000 ORBC al contrato inteligente OM del sistema.

Todos los miembros de DAO ORBIS tienen la oportunidad de desarrollar una organización descentralizada.

Solo los titulares de OM, miembros de DAO ORBIS, tienen el derecho a adoptar decisiones en cuestiones de organización, administrativas y tokenómicas. La votación se lleva a cabo en forma postal vía Internet. Se determina el periodo de 8 días para los procedimientos de la votación.

El quorum o la idoneidad de la decisión se aceptan en una cantidad superior al 50% del número total de los titulares de OM. La decisión se considera como adoptada si más del 50% de los titulares de OM que hayan participado en la votación votaran a favor.

La votación de participantes de DAO ORBIS se lleva a cabo en dos etapas:

1. Cualquier participante de DAO ORBIS, titular de OM, puede iniciar la votación pero no más de 1 vez al año. En la primera etapa el participante que ha iniciado la votación forma el quorum de participantes de la votación. En esta etapa de la votación el quorum se hace idóneo si más del 50% del número total de los participantes de DAO ORBIS ha votado “a favor” de la votación.

2. En la segunda etapa a los participantes se les propone a aceptar una seria de parámetros de administración que se usan por contratos inteligentes de la red ORBIS:

- Importe de la comisión de la transacción de ORBC.
- Importe de la comisión de la transacción de tokens en ORBC.
- Importe de la comisión de la transacción de datos de servicios en ORBC.
- Importe de la comisión de la emisión de tokens.
- Otros parámetros relacionados con el desarrollo de Blockchain ORBIS.

Los resultados de la votación se consideran aceptados si más del 50% de los miembros de DAO ORBIS que participaron en la segunda etapa de la votación votaron “a favor” de los parámetros propuestos.

Todos los resultados de la votación y los parámetros aceptados se guardan en la cadena de Blockchain ORBIS correspondiente.

Parte técnica

Se puede distinguir 4 módulos principales dentro de la parte técnica de ORBIS:

1. TreeChain.
2. Consenso.
3. Criptografía.
4. API orientada a servicios.

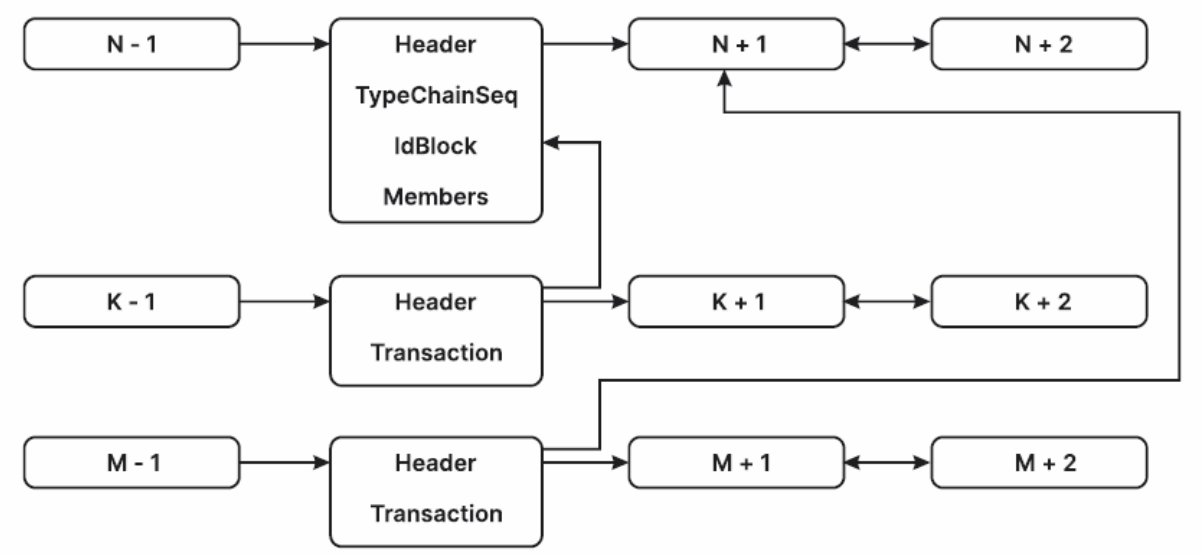
Estos módulos son básicos en Blockchain ORBIS.

TreeChain

TreeChain es una tecnología de almacenamiento de datos, basada en la tecnología blockchain, que permite acceder al cualquier bloque en un período de tiempo mínimo posible, si comparamos con la selección de datos estándar de una cadena habitual (Dibujo 1).

Si hay una gran acumulación de datos, la solución presentada acelera el trabajo de la emisión de datos de los nodos, manteniendo el índice del bloque y su participante.

TreeChain almacena cada transacción como un bloque separado, que tiene hash, firma y confirmación propios. Este enfoque permite deshacerse de la necesidad de construcción del árbol de Merkle y validar cada transacción que ha sido realizada en un momento de tiempo definitivo.

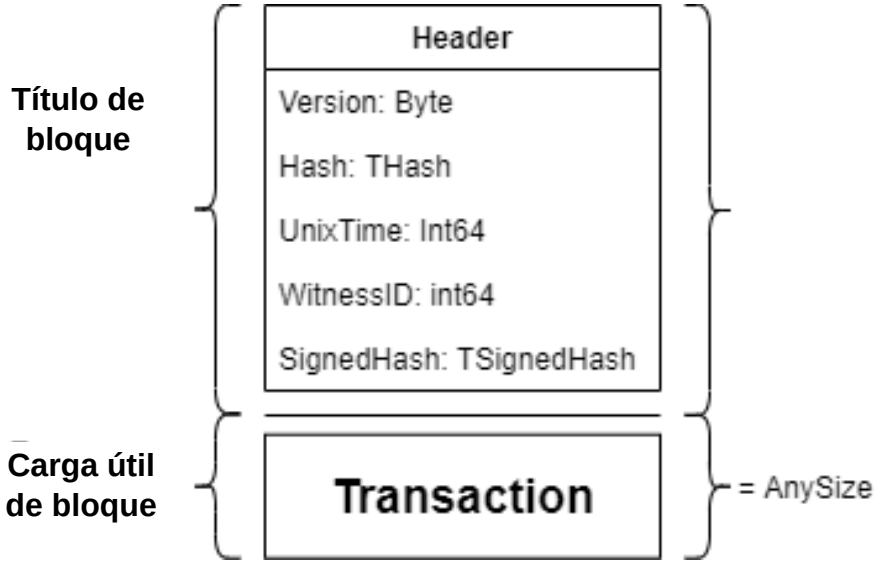


Dibujo 1. Algoritmo de estructura de TreeChain

Cada bloque tiene la arquitectura básica:

1. Título.
2. Carga útil.

El título siempre tiene la dimensionalidad de ~100 bytes (Dibujo 2), que nos dice que el tamaño mínimo del bloque puede ser de 101 bytes.

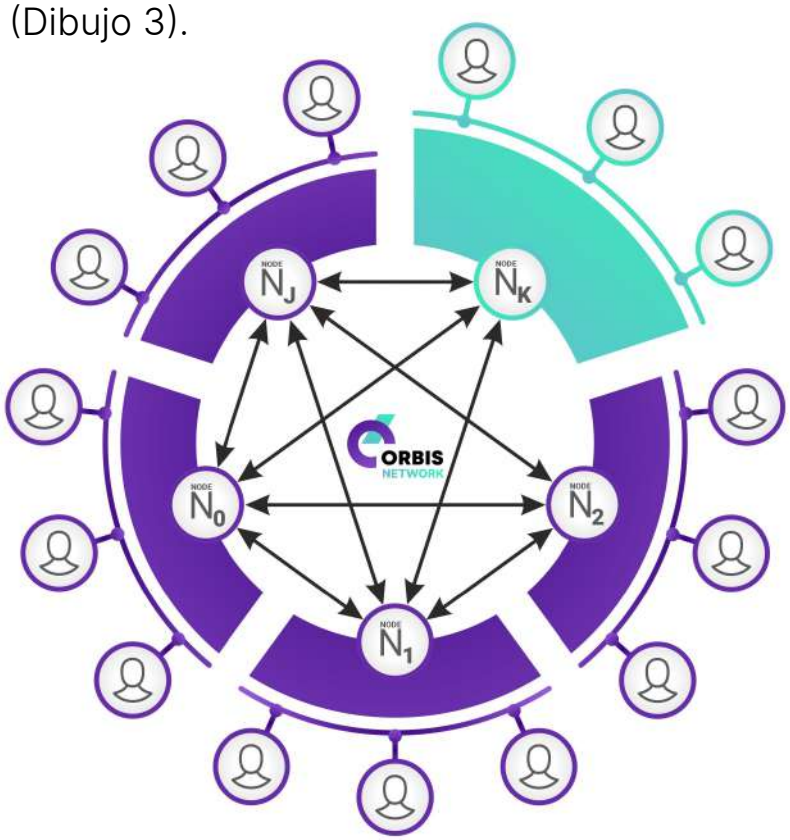


Dibujo 2. Estructura de bloque

Consenso

ORBFT(Optimized Recognized Byzantine Fault Tolerance) es un algoritmo de consenso, basado en dos mecanismos del consenso PoS & dBFT, que permite seleccionar claramente los delegados y oradores de aquellos nodos, que poseen OM y tienen la dirección IP estática.

Consenso es la tecnología de construcción de la arquitectura de la red ORBIS y de la resolución de problema de la inscripción de datos en Blockchain según el algoritmo ORBFT (Dibujo 3).



Dibujo 3. Arquitectura de la red ORBIS

Aquí:

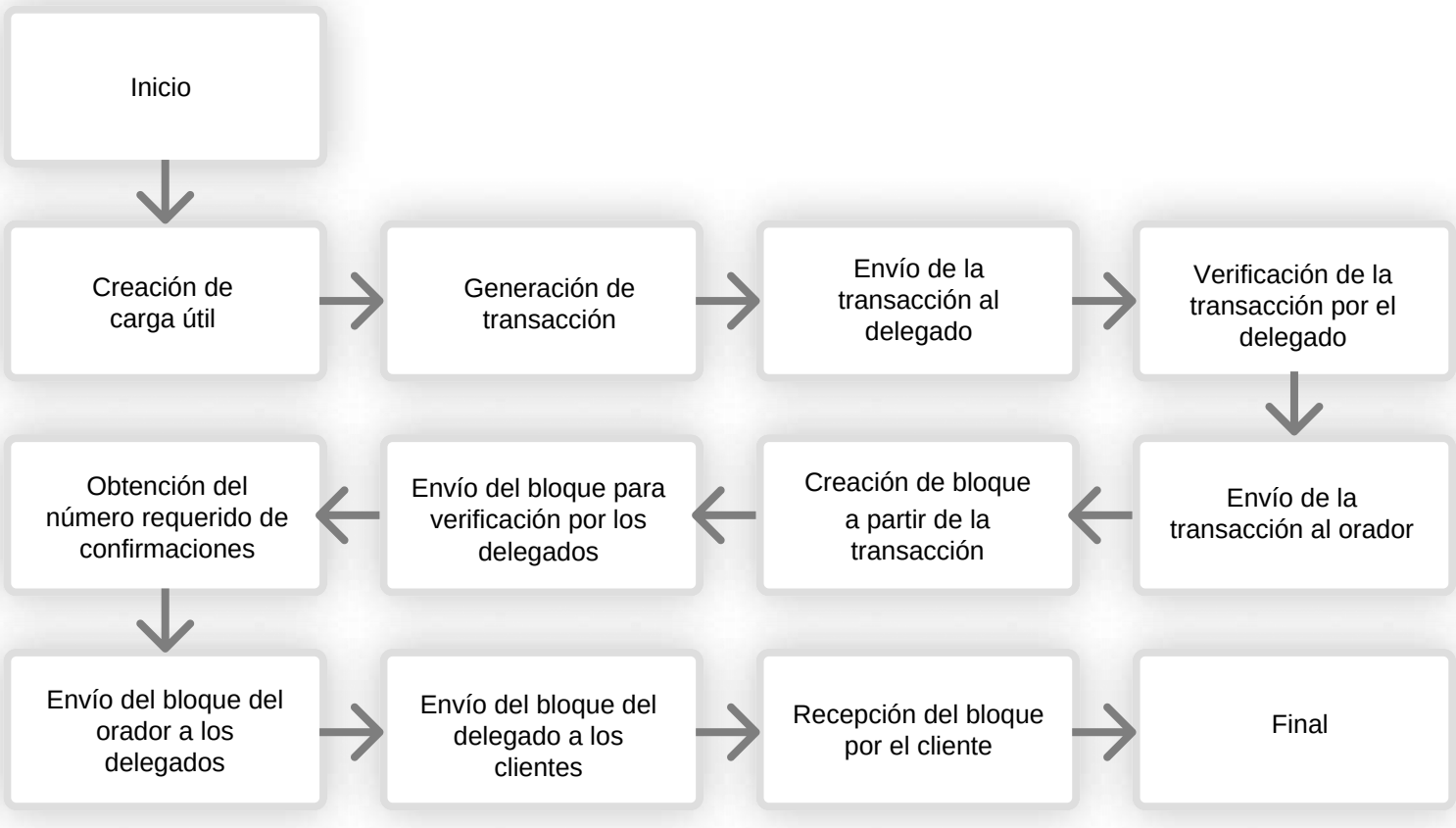
Los usuarios son las aplicaciones cliente que no tienen OM y un nodo completo.

Nodos con la numeración individual son los nodos que tienen OM, la dirección IP estática: pueden participar en la generación y la confirmación de los bloques.

Flecha del cliente al nodo es la vinculación que implica que el cliente puede solo enviar una transacción o aceptar un bloque.

Flecha bidireccional es la vinculación bilateral cuando los nodos pueden comunicarse las transacciones almacenadas para generar bloques y enviarlos de vuelta.

En este algoritmo la vía desde la creación hasta la inscripción de la transacción en el bloque será la siguiente (Dibujo 4):



Dibujo 4. Ciclo de vida de una transacción

En el marco del consenso ORBFT existen dos papeles claves:

1. Orador es un nodo que genera los bloques a partir de las transacciones y los envía para su verificación a los delegados.

2. Delegado es un nodo que agrega las conexiones de los clientes y, en consecuencia, las transacciones, así como se ocupa de la validación de bloques y los retransmita a los clientes.

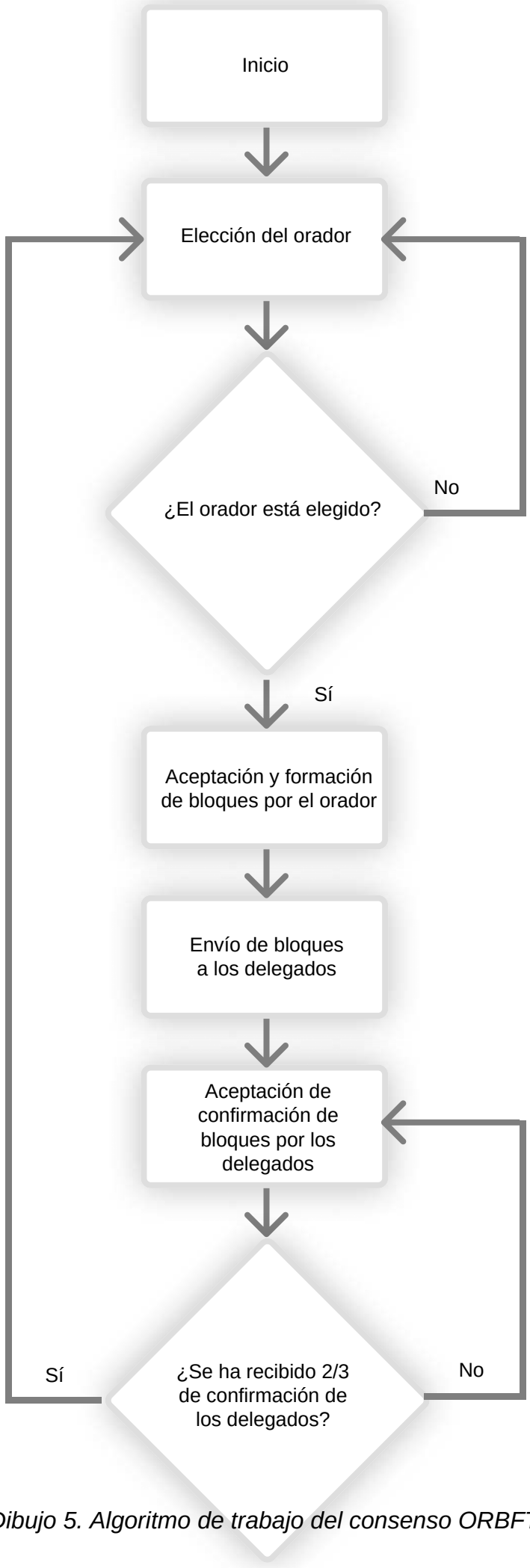
Para participar en el consenso ORBFT es necesario cumplir con los criterios:

1. A nivel programático: existencia de cuenta, que tiene al menos un OM.
2. A nivel de sistema: existencia de la dirección IP estática.

Esto está dictado por la necesidad de:
1. Eliminarse de los nodos malintencionados.
2. Dar a los clientes la oportunidad de conectarse y trabajar con ORBIS.

Representación algorítmica del consenso ORBFT paso a paso (Dibujo 5):

1. Elección del orador:
   a. Si el orador está elegido, pasamos al paso 2.
   b. Si el orador no está elegido, pasamos al paso 1.
2. Recolección de las transacciones de los delegados y formación de los bloques.
3. Envío de los bloques a los delegados para la verificación.
4. Espera de la confirmación de los bloques por los delegados (hasta 5 segundas dependientemente del número de los bloques recibidos simultáneamente);
   a. Si 2/3 de los delegados han votado afirmativamente, entonces colectamos sus firmas e inscribimos en el bloque de firmas.
   b. Si 2/3 de los delegados no han votado, entonces incrementamos el indicador de intentos:
      i. Si el indicador de intentos es 3, pasamos al paso 1 sin inscribir los bloques generados en el blockchain.
      ii. Si el indicador de intentos no es 3, pasamos al paso 4.



Dibujo 5. Algoritmo de trabajo del consenso ORBFT

Criptografía

La criptografía es una tecnología de creación de las claves, el hashing, la firma, el cifrado y descifrado de datos. Esta funcionalidad se crea utilizando:

1. RSA.
2. AES.
3. BIP39.
4. SHA256.

RSA se utiliza para generar un par de claves con tamaño de exponente privado igual a 512 bits.

AES se utiliza para cifrar un par de claves con una contraseña que solo el usuario sepa. Si guardar el resultado AES como matriz de bytes en un archivo, habrá un criptocontenedor con un par de claves.

BIP39 se utiliza para crear 47 palabras con las que se puede recuperar la clave privada.

SHA256 se utiliza para generar los hash de bloques, así como para crear la dirección a partir de la clave pública.

API orientada a servicios

API orientada a servicios es la tecnología que da a cualquier titular del servicio la oportunidad de conectarse a ORBIS usando REST API, que incluye el nodo ORBIS e inscribir en el Blockchain cualquiera información necesaria (Gráfico 1).

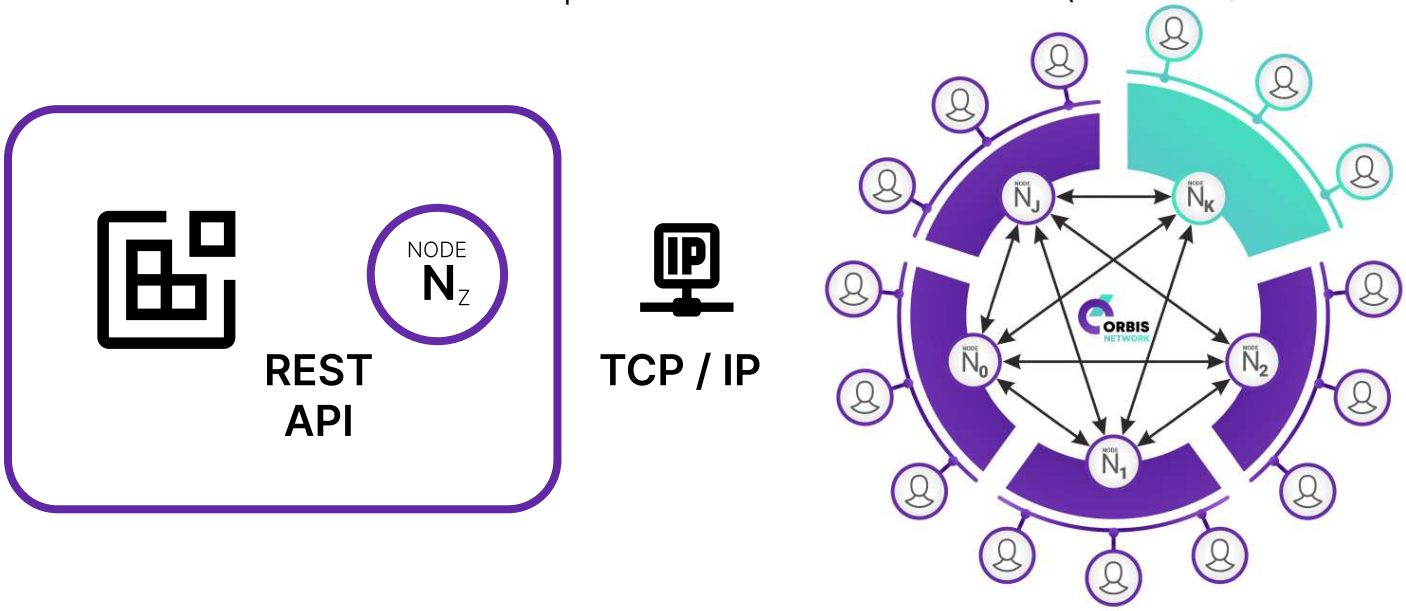


Gráfico 1. Colaboración de los servicios con ORBIS

Para trabajar en calidad de servicio es necesario instalar un nodo completo al cual el servicio podrá conectarse.

La **arquitectura de red** es la combinación de nodos de la red así como el conjunto de reglas, de acuerdo con las que se transmitan los mensajes en la red. Las redes Blockchain pueden ser de una capa y de dos capas, públicas o privadas, pueden tener distribución de los nodos por papeles.

El **mecanismo de consenso** es un protocolo que permite llegar a un acuerdo entre los participantes de iguales derechos de la red descentralizada. Existe una gran cantidad de realizaciones, pero los consensos más populares son PoW, PoS, dPos, aBFT, dBFT.

El **bloque** es la estructura de datos que se utiliza para almacenar los datos en el Blockchain. El bloque almacena la transacción, el estado de la red, los contratos inteligentes, el permiso de acceso a los datos y otra información.

La **cadena** es la estructura de datos construida mediante la combinación consecutiva de los bloques en la cadena. Mediante el almacenamiento de la función hash del bloque anterior, todos los bloques son estrictamente secuenciales, tienen la numeración pasante, el bloque secundario siempre hace referencia a un solo bloque primario.

La **transacción** es una operación mínima lógicamente significativa de transferencia o intercambio de activos que tiene sentido y solo puede realizarse en su totalidad. La transacción puede llevar a cabo la transmisión de mensajes, acciones, crear un contrato y otros.

La **dirección** es un medio para identificar un objeto activo en la red.
Las direcciones definen unívocamente al remitente y al receptor de los valores transferidos en la red Blockchain, todas las acciones del usuario en la red están asociadas con la dirección. Dependiendo de Blockchain, la dirección puede ser tanto una cadena como una estructura de datos, puede asociarse con un usuario o con un contacto inteligente.

El **ciclo de vida de una transacción** es un proceso de firma de la transacción; envío de amplia difusión en la red; verificación de la transacción; finalización de la transacción. Incorporación de la transacción en un bloque: proceso de toma de las transacciones para un bloque.

Validación de una transacción: proceso de verificación y firma.

Referencias bibliográficas:

1. Chaum, D. “Blind Signatures for Untraceable Payments”. //Advances in Cryptology Proceedings of Crypto 82, Plenum. 1982. pp. 199-203, 1982.
2. Haber, S., Stornetta, W.S. How to time-stamp a digital document. //J. Cryptology 3. 1991. pp. 99–111.
3. Back, A. Mail “Hash cash postage implementation”. //The Cypherpunks Mailing List. URL: https://cypherpunks.venona.com/date/1997/03/msg00774.html.
4. Szabo, N. Smart Contracts: Building Blocks for Digital Markets. //A partial rewrite of the article which appeared in Extropy No 16. 1996. URL: http://www.alamut.com/subj/ economics/nick_szabo/smartContracts.html.

ORBIS – ¡Piensa globalmente!


@orbismoney_official