01 de Junio de 2018
AGETIC/RA/0039/2018
Expediente: 34245

Clasificación : Reservado

RESOLUCIÓN ADMINISTRATIVA

Referencias: AGETIC-UIID/IT/0034/2018 AGETIC/IL/0100/2018

VISTOS:

Que el Parágrafo II del Artículo 103 de la Constitución Política del Estado, establece que el Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación.

Que el Parágrafo I del Artículo 85 de la Ley N° 031, de 19 de julio de 2010, Marco de Autonomías y Descentralización "Andrés Ibáñez", determina que dentro las competencias exclusivas del nivel central del Estado, se encuentra formular y aprobar el régimen general y las políticas de comunicaciones y telecomunicaciones del país, incluyendo el acceso al internet y demás Tecnologías de Información y Comunicaciones–TIC.

Que el Artículo 72 de la Ley No 164, de 8 de agosto de 2011, de Telecomunicaciones, Tecnologías de Información y Comunicación, señala que las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las tecnologías de información, de manera prioritaria, haciendo énfasis en el área de gestión gubernamental.

Que el parágrafo I del Artículo 2 del Decreto Supremo N° 2514 de 9 de septiembre de 2015, dispone la creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), como entidad descentralizada de derecho público, con personalidad jurídica, autonomía de gestión administrativa, financiera, legal y técnica y patrimonio propio, bajo tuición del Ministerio de la Presidencia. A su vez el Artículo 4 inciso f) establece como una de las funciones del Director General Ejecutivo de AGETIC, emitir resoluciones administrativas, en el marco de sus funciones.

Que el Artículo 7 del referido Decreto Supremo N° 2514 , establece que la AGETIC tiene las siguientes funciones: m) Desarrollar e implementar programas, proyectos y servicios de Gobierno Electrónico y Tecnologías de Información y Comunicación.

Que mediante Decreto Supremo Nº 3251 de 12 de julio de 2017 se aprueba el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos, que son aplicables por todos los niveles de gobierno del Estado Plurinacional de Bolivia.

Que el Decreto Supremo N.º 3525 de 4 de abril de 2018, en su articulo 16 establece lo siguiente:

I. La AGETIC será responsable de implementar, gestionar y coordinar un registro descentralizado de orden cronológico e integridad de datos y documentos digitales.

II. Los datos consignados en el registro de orden cronológico e integridad de datos y documentos digitales, tendrán plena validez jurídica respecto a la integridad y temporalidad de los mismos, para asuntos judiciales y administrativos, incluyendo aquellos de ejecución y control gubernamental.

III. La AGETIC establecerá los lineamientos y condiciones técnicas para la implementación y uso del registro de orden cronológico e integridad de datos y documentos.

Que la Disposición Transitoria Quinta del señalado Decreto Supremo N.º 3525, establece que en un plazo máximo de cuarenta (40) días hábiles, computables a partir de la publicación del presente Decreto Supremo, la AGETIC aprobará mediante Resolución Administrativa los lineamientos y condiciones técnicas para la implementación y uso del registro de orden cronológico e integridad de datos y documentos digitales.

Que el Artículo Único de la Resolución Suprema N° 16416 de 14 de septiembre de 2015, designa a Nicolás Laguna Quiroga como Director General Ejecutivo de la Agencia de Gobierno Electrónico y Tecnologías de Información – AGETIC, bajo tuición del Ministerio de la Presidencia.

CONSIDERANDO:

Que mediante Informe Técnico AGETIC-UIID/IT/0034/2018 de 1de junio de 2018 emitido por el Profesional de Investigación en Gestión de Datos e Información, concluye señalando que el documento “Lineamientos y Condiciones Técnicas para la Implementación y Uso del Registro de Orden Cronológico e Integridad de Datos y Documentos Digitales”, fue elaborado por el Área de Investigación de la Unidad de Innovación, Investigación y Desarrollo, en el marco del Decreto Supremo N°3525 y normativa legal vigente.

Que el Informe Legal AGETIC/IL/0100/2018 de fecha 01 de junio de 2018, en sus conclusiones señala que por los antecedentes y normativa legal vigente corresponde la emisión de Resolución Administrativa que apruebe el documento: LINEAMIENTOS Y CONDICIONES TÉCNICAS PARA LA IMPLEMENTACIÓN Y USO DEL REGISTRO DE ORDEN CRONOLÓGICO E INTEGRIDAD DE DATOS Y DOCUMENTOS DIGITALES.

Que asimismo de acuerdo al referido Informe Técnico AGETIC-UIID/IT/0034/2018, el documento “Lineamientos y condiciones técnicas para la implementación y uso del registro de orden cronológico e integridad de datos y documentos digitales” está conformado por 11 Capítulos, con el siguiente detalle:

Nro. de Capítulo	DETALLE
1	Introducción
2	Antecedentes
3	Objetivos
4	Alcance y Ámbito de Aplicación
5	Cadena de Bloques
6	Arquitectura
7	Seguridad
8	Políticas
9	Gestión de la Plataforma
10	Definición de términos y Abreviaciones
11	Referencias

POR TANTO:

El Director General Ejecutivo de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC, designado mediante Resolución Suprema No. 16416 de 14 de septiembre de 2015, en uso de sus atribuciones y facultades;

RESUELVE:

01 de Junio de 2018
AGETIC/RA/0039/2018
Expediente: 34245

ARTÍCULO PRIMERO.- Aprobar los LINEAMIENTOS Y CONDICIONES TÉCNICAS PARA LA IMPLEMENTACIÓN Y USO DEL REGISTRO DE ORDEN CRONOLÓGICO E INTEGRIDAD DE DATOS Y DOCUMENTOS DIGITALES, que forman parte de la presente Resolución Administrativa.

ARTÍCULO SEGUNDO.- Se determina que los LINEAMIENTOS Y CONDICIONES TÉCNICAS PARA LA IMPLEMENTACIÓN Y USO DEL REGISTRO DE ORDEN CRONOLÓGICO E INTEGRIDAD DE DATOS Y DOCUMENTOS DIGITALES, será potestativo para las entidades públicas y privadas que presten servicios públicos delegados por el Estado, de conformidad al parágrafo IV. del artículo 16 (REGISTRO DE ORDEN CRONOLÓGICO E INTEGRIDAD) del Decreto Supremo N° 3525 de 4 de abril de 2018.

ARTÍCULO TERCERO.- Aprobar el Informe Técnico AGETIC-UIID/IT/0034/2018 de 01 de junio de 2018 emitido por el Área de Investigación y el Informe Legal AGETIC/IL/0100/2018 de 1 de junio de 2018 emitido por la Unidad Jurídica, ambos de la AGETIC, que en Anexo forman parte de la presente Resolución Administrativa.

ARTÍCULO CUARTO.- Disponer que la Unidad de Gobierno Electrónico, se encarguen del cumplimiento, difusión y aplicación de los LINEAMIENTOS Y CONDICIONES TÉCNICAS PARA LA IMPLEMENTACIÓN Y USO DEL REGISTRO DE ORDEN CRONOLÓGICO E INTEGRIDAD DE DATOS Y DOCUMENTOS DIGITALES.

ARTÍCULO QUINTO.- Se abrogan y derogan todas las disposiciones contrarias a la presente Resolución Administrativa.

LINEAMIENTOS Y CONDICIONES TÉCNICAS PARA LA IMPLEMENTACIÓN Y USO DEL REGISTRO DE ORDEN CRONOLÓGICO E INTEGRIDAD DE DATOS Y DOCUMENTOS DIGITALES

1. INTRODUCCIÓN

En el mundo digital son las computadoras y sistemas de información realizan transacciones entre sí, muchas de estas de forma automática o con participación de humanos para poder realizar registros, en estos se intercambian bienes, dinero o se realizan simples registros administrativos. Por esto se hace necesario contar con herramientas que permitan verificar que esa transacción fue realizada en un momento determinado y poder verificar la integridad de los datos de la misma a cada uno de los actores involucrados en la misma.

Por esto se plantea la implementación de un registro de orden cronológico e integridad distribuido donde el lineamiento base de operación del mismo se establece en este documento. Este registro se implementa en esta primera versión sobre tecnología de cadena de bloques por los niveles de seguridad que tiene y la arquitectura distribuida que presenta en su diseño.

Los lineamientos establecen la forma de gestión de la plataforma y las responsabilidades de los actores para garantizar la auditabilidad y transparencia necesarias para dar un servicio de calidad a ciudadanos e instituciones que usen la misma.

Esta plataforma al ser distribuida requiere de la participación de varias entidades, donde las responsabilidades son compartidas y siguen el espíritu de integración de entidades públicas para la implementación de tecnología con soberanía basada en herramientas libres.

Esta primera implementación de una cadena de bloques por parte del Estado es un paso más hacia la Bolivia Digital que se llevando adelante con la implementación de gobierno electrónico, para brindar un mejor servicio a los ciudadanos y la dotación de herramientas a las entidades como apoyo en este proceso.

2. ANTECEDENTES

El país está implementando el Plan de Implementación de Gobierno Electrónico y llevando adelante de la construcción de la Bolivia Digital al año 2025, en este proceso requiere de la participación de todas las entidades del Estado integrándose al mundo digital como parte del fenómeno que se lleva en el mundo.

Para esto se ha elaborado una ruta de trabajo definida desde la Ley de Telecomunicaciones y Tecnologías de Información y Comunicación Nro. 164 y sus decretos reglamentarios. Para la implementación de gobierno electrónico se requiere contar con herramientas que permitan garantizar las transacciones electrónicas que son producto de la digitalización de los procesos administrativos para poder dar seguridad y garantizar las mismas. Tanto para el lado del ciudadano como la misma entidad.

Desde su creación, la AGETIC en coordinación con diferentes entidades del Estado, ha llevado adelante proyectos de gobierno electrónico, donde el factor principal de los mismos es el análisis de procesos y procedimientos para su posterior digitalización utilizando diversas herramientas que se han ido desarrollando como respuesta a los problemas encontrados en este camino, algunas de estas son, la plataforma de interoperabilidad para apoyar el intercambio de agil y rapido de datos entre entidades, la plataforma de pagos para facilitar el pago de trámites estatales y la conciliación en línea de los mismos, la firma digital como medida de seguridad para la certificación de documentos digitales.

Estas herramientas se integran a los sistemas de información de las entidades apoyando la digitalización completa de los procesos.

En este contexto es necesaria otra herramienta que permita dar confianza a las transacciones que se realizan en las entidades con los ciudadanos, garantizando el contenido de la transacción, el momento exacto en el que se realizó, los participantes de la misma.

Para esto se ha elaborado el D.S. 3525 del 04 abril de 2018 donde se establece la creación de REGISTRO DE ORDEN CRONOLÓGICO E INTEGRIDAD para datos y documentos digitales, este registro tiene validez jurídica para asuntos judiciales y administrativos, incluyendo aquellos de ejecución y control gubernamental.

Una de las características principales de este registro es que debe ser descentralizado lo que permite tener diversos actores que generen una cadena de confianza y disponibilidad del mismo. La descentralización en el ámbito de las TIC desde la aparición de la tecnología de cadena de bloques ha demostrado ser una forma transparente para los registros de transacciones electrónicas entre diversos actores.

3. OBJETIVO

El presente documento tiene como objetivo establecer los lineamientos para la implementación del servicio de REGISTRO DE ORDEN CRONOLÓGICO E INTEGRIDAD descentralizado de datos y documentos digitales por parte de las entidades del sector público y privadas que tengan servicios delegados del Estado Plurinacional de Bolivia, mismo que estará a cargo de la AGETIC.

4. ALCANCE Y ÁMBITO DE APLICACIÓN

En este documento se formulan los lineamientos y condiciones técnicas para la implementación y uso del registro de orden cronológico e integridad de datos y documentos digitales para el estado, basado en cadena de bloques, para generar transacciones confiables y automáticas basado en software libre. Pueden ser partícipes las entidades del sector público de nivel central, entidades descentralizadas, entidades desconcentradas, autárquicas, empresas públicas estratégicas y mixtas, autoridades de regulación sectorial, Ministerio

Público y Procuraduría General del Estado y empresas que prestan servicios públicos delegados por el Estado.

Los lineamientos contenidos en este documento establecen estándares técnicos mínimos a ser implementados para el uso de registro cronológico e integridad de datos y documentos digitales en el Estado. Tomando en cuenta la naturaleza dinámica de la tecnología, se puede implementar versiones superiores y/o con mejores características, sin dejar de considerar todos los puntos que se detallan en el documento.

Los lineamientos contenidos en este documento deberán ser asumidos por todas las entidades del sector público que participen del registro de orden cronológico e integridad, sin perjuicio del trabajo desarrollado por aquellas que hayan asumido como parámetros rectores, normas y estándares nacionales e internacionales vigentes o de otra naturaleza en materia de registro de orden cronológico e integridad de datos y documentos digitales, los cuales no deberán ser contrapuestas a los lineamientos establecidos en el presente documento.

La AGETIC analizará periódicamente la necesidad de actualización de este documento.

5. CADENA DE BLOQUES

Las cadenas de bloques tuvieron su mayor impacto en su uso en las criptomonedas, sin embargo, su uso se ha extendido a diversas áreas por las características técnicas y potencialidades que presenta. La forma de trabajo distribuida y la capacidad de participación de diversos actores hacen de esta tecnología una forma ideal de trabajo para dar garantía y asegurar las transacciones de datos e información que realizan los sistemas en línea.

5.1 Sistemas distribuidos de orden cronológico

Los sistemas distribuidos de orden cronológico nacen con la creación de criptomonedas y sistemas digitales distribuidos de libros mayores para registro de transacciones entre participantes con valores para negociar, tratando de encontrar solución al problema del doble gasto simultáneo y el registro de existencia de cada transacción que sea inmutables.

En esencia un sistema distribuido se apoya en una base de datos distribuida y compartida que es replicada y sincronizada entre los participantes de una red. Los participantes acuerdan el consenso de la actualización de la información de la base de datos de cada participante cuando se produce una nueva transacción.

Los registros del sistema distribuido cuentan con una firma criptográfica para cada transacción y que es unida a otras firmas criptográficas mediante un árbol de Merkle que se realiza hasta completar un bloque donde la firma criptográfica raíz se encadena al siguiente bloque de la cadena.

Una cadena de bloques permite garantizar la integridad de la información contenida en cualquier documento digital, como también la certeza sobre el momento en que dicho documento se creó y obtuvo vigencia.

5.2 Ejemplo de Uso: Criptomonedas y Registro de Orden Cronológico

A nivel mundial existen criptomonedas que cotizan y realizan transacciones utilizando billeteras digitales y se basan en sistemas de orden cronológico con cadenas de bloques para confirmar la validez de transacciones en tiempo y contenido.

Varios países latinoamericanos han comenzado a usar las mismas como parte de la política de estado, ante las capacidades de esta tecnología. Venezuela a lanzado el Petro como medida economica, en Argentina se habilitó el uso de una moneda local y México ha comenzado a

realizar estudios para admitir criptomonedas activas a nivel mundial.

La plataforma estatal de sistema de orden cronológico no utiliza criptomonedas y no tiene necesidad de incentivos ya que se basa en un sistema de admisión mediante permiso en el cual el sistema de ordenamiento realiza el consenso y añade los bloques para todas las transacciones aprobadas que se envíe.

Otros países como México han implementado cadenas de bloques para apoyar la gestión pública. En este caso este mecanismo tecnológico permite garantizar la integridad de los documentos como también el orden cronológico de su existencia. En el caso de México se utiliza para transparentar las adquisiciones estatales, permitiendo a todos los ciudadanos acceder a información sobre las contrataciones cuya integridad y temporalidad se certifican utilizando la cadena de bloques.

5.3 Tipos de sistemas distribuidos de orden cronológico

Existen dos tipos de sistemas distribuidos de orden cronológico: abiertos y mediante permiso de admisión.

Los sistemas abiertos son aquellos que son utilizados en las criptomonedas que permiten la participación de cualquier persona. El uso del sistema distribuído cronológico mediante cadenas de bloques debe ser realizado por los denominados mineros de bloques que reciben compensación económica en criptomoneda por su participación creando bloques a la cadena.

Todos pueden participar del minado de bloques pero solo el primero en remitir la solución correcta de la ecuación criptográfica gana el premio económico.

Los sistemas de orden cronológico con permiso de admisión, solo permiten la participación de aquellos que han sido identificados especialmente y posteriormente autorizados con diferentes roles como segunda instancia.

Los sistemas distribuidos de orden cronológico con permiso de admisión permiten crear una ruta de confianza de eventos que quedan registrados y son inmutables, que pueden ser verificados en el tiempo y contenido por los participantes de la red.

5.4 Elección de Hyperledger Fabric para la plataforma estatal

La implementación de la plataforma requiere enmarcarse en la política de Estado de uso de software libre como parte de la soberanía tecnológica. Por esto la plataforma debe responder a la necesidad de cumplir con los lineamientos del plan de software libre.

En la actualidad existen pocos proyectos de software libre completos que implementen todos los aspectos de una plataforma de sistemas distribuidos cronológicos mediante cadenas de bloques. Si bien existen proyectos de software libre derivados de las criptomonedas, estos están basados en mecanismos de recompensa monetaria.

Hyperledger (del inglés hiper libro maestro) es un esfuerzo colaborativo creado para promover tecnologías de cadena de bloques basadas en código abierto e implementables en distintos sectores. Es una colaboración global, creada por la Linux Foundation, que incluye varias empresas líderes en tecnologías digitales y tiene el objetivo de proponer herramientas de alta calidad para la implementación de cadenas de bloques. Fabric es la plataforma para cadenas de bloques desarrollada por el proyecto Hyperledger y es la herramienta elegida para la implementación del servicio de cadena de bloques del Estado.

Fabric cumple con el Plan de Implementación de Software Libre siendo distribuido bajo licencia de software Apache 2.0 que provee el código permitiendo su modificación y el uso del nombre

del proyecto con características descriptivas no con fines comerciales.

Fabric también implementa una arquitectura independiente de criptomonedas.

En sus características generales tenemos:

Diseño para redes privadas con restricción de miembros.

Creación de códigos de cadena en varios lenguajes de programación.

Flexibilidad de crear diversas formas de consenso entre los miembros de la plataforma.

5.5 Definición de canal y participantes

El sistema descentralizado de orden cronológico está basado en una infraestructura de cadena de bloques que agrupan las transacciones. Las transacciones son añadidas por clientes del sistema.

Existen participantes del sistema distribuido que son denominados nodos y que forman el grupo entre el cual se realizan transacciones mediante canales de transacción predefinidos que se realizan entre miembros de la red. Estos canales pueden abarcar a todos los participantes o sólo determinados nodos.

5.6 Bases de datos distribuidas

Cada nodo participante del sistema guarda dos bases de datos del sistema: una base de datos del estado actual del sistema y otra base de datos como un registro de las actividades de la cadena.

5.7 Código de cadena

Los nodos dentro del sistema distribuido interactúan con un libro mayor a través del “código de cadena”. El libro mayor está construido con la base de datos distribuida en los nodos. Los códigos de cadena automatizan la ejecución de las transacciones sobre el libro mayor de acuerdo a condiciones establecidas previamente entre los participantes.

El código de cadena puede estar escrito en diferentes lenguajes de programación ya sea NodeJS, Go, C/C++.

5.8 Abstracciones operativas dentro del sistema de cadena de bloques

Para una mayor comprensión del sistema distribuido de orden cronológico mediante cadenas de bloques se establecen abstracciones operativas que se describen a continuación para explicar el funcionamiento del sistema en general.

5.8.1 Capa de consenso

Responsable de generar un acuerdo en el orden y confirmación del set de transacciones dentro del bloque. En la herramienta utilizada para el consenso se utilizan algoritmos de tolerancia a faltas bizantinas de los nodos participante del endorsamiento y el módulo de consenso utilizado se implementa de forma modular. Aunque el software base de Hyperledger Fabric contiene por defecto el módulo de consenso denominado “solo”, no se debe utilizar en producción y debe ser reemplazado por un módulo de consenso como Apache Kafka.

5.8.2 Capa de código de cadena

Es el código que interactúa con el libro mayor del sistema de cadena de bloques mediante su ejecución. En su estructura que se programa antes de iniciar la cadena se concibe la lógica de

negocios del sistema global y se definen ciertas políticas normativas de uso de la cadena de bloques.

5.8.3 Capa de comunicación

Responsable del transporte de los mensajes P2P entre los nodos participantes de un canal de transacciones. En la tecnología implementada se hace la abstracción para comunicarse con los nodos participantes mediante nombres de hosts y redes virtuales creadas entre los participantes.

5.8.4 Capa de abstracción de almacenamiento de datos

Están disponibles diferentes clases de almacenes de datos para ser usada por otros módulos del sistema que necesitan tener acceso a los datos almacenados en nodos diferentes.

5.8.5 Capa de abstracción criptográfica

Esta capa permite utilizar diferentes algoritmos criptográficos que se intercambian entre módulos en sus firmas sin afectar a los demás componentes del sistema.

5.8.6 Servicio de Identidad

El servicio de identidad está implementado mediante un servicio proveedor de membresía MSP interno que establece un sistema de confianza mediante una autoridad CA interna que otorga certificados para poder participar a los nodos, para el enrolamiento y registro de entidades o sistemas de entidades durante la operación de la red y la administración de cambios, tales como eliminaciones, altas y revocaciones. El establecimiento de identidades y permisos de participantes es el paso inicial para comenzar el canal de transacciones.

5.8.7 Políticas del grupo

Se establecen políticas administrativas en el sistema, tales como, la política de aprobación, la de consenso, la de gestión de grupo. Estas políticas deben estar establecidas previamente a la creación del canal de transacciones. La interacción entre los módulos están acorde a las las diversas políticas establecidas.

5.8.8 Capa de API de interacción con las clientes

La interacción de los clientes que desean efectuar transacciones en el libro mayor debe hacerse mediante un SDK que proporciona una API que permite interactuar con el código de cadena a nombre de los clientes mediante los nodos.

5.9 Definición de roles de los participantes del sistema

Las entidades participantes forman parte de un comité que puede tener a varios nodos participantes de la red de cadenas de bloques. Cada uno de los nodos participa de la red y pueden tener diferentes roles dentro la red. Existe la posibilidad de tener una autoridad de certificación CA en cada entidad o tener una sola para todas las entidades.

La definición de los papeles para los participantes está establecida en las políticas de la cadena de bloques que se elabora previamente a la creación del canal de transacciones de los miembros participantes.

Los roles que pueden adquirir los participantes son los siguientes:

5.9.1 Participante administrador

Se encarga de inscribir a otros participantes y otorgarles privilegios dentro la red frente a la

autoridad de certificación de la plataforma. El participante administrador se crea al inicializar la autoridad de certificación. El participante administrador es responsable de la plataforma.

5.9.2 Participante como verificador (endorsador)

De acuerdo a la política establecida, el participante verificador recibe la propuesta de transacción y ejecuta la simulación de la transacción en su base da datos del estado del libro mayor para sacar un resultado que se enviará al sistema de ordenamiento con una firma criptográfica adherida.

5.9.3 Participante del sistema de ordenamiento

Se encarga de realizar la tarea de agrupar las transacciones en bloques, aplicando el algoritmo de consenso sobre estas para que sean sido enviadas a todos los demás nodos para su validación final. Los participantes del sistema de ordenamiento no tienen conocimiento del estado actual del libro mayor ni ejecutan el código cadena.

5.9.4 Nodos miembros con almacenamiento

Pueden solicitar realizar una transacción en la cadena de bloques como los demás participantes, mediante la ejecución del código de cadena mediante los endorsadores. Tienen la obligación de ejecutar la verificación final cuando se propone una transacción y de añadir el resultado a su libro mayor en caso de confirmación.

6. ARQUITECTURA

La arquitectura propuesta se basa sobre la plataforma Fabric [1], un framework desarrollado bajo el auspicio de la Linux Foundation y publicado con licencia de código abierto. La plataforma implementa una arquitectura de tipo “Ejecución Ordenamiento Validación” (EOV) en contraposición a las arquitecturas estándar denominadas “Ordenamiento Ejecución” (OE) [2].

6.1 Partes

La arquitectura se compone de dos partes fundamentales:

Un código de cadena, denominado chaincode. Es el programa que implementa la lógica de la aplicación y se usa en la fase de ejecución. El programa permite simular una transacción hasta generar un resultado deterministico comparable con el resultado de otras simulaciones. El código de cadena puede ser implementado por actores que no sean de confianza para la plataforma.

Una política de verificación (endorsamiento) utilizada en la fase de validación. Estas políticas no pueden ser establecidas o modificadas por actores que no sean de confianza. Una política de endorsamiento define cuántos y cuáles participantes de la plataforma se necesitan para poder avalar una transacción.

Cada una de las partes mencionadas tiene que ser definida en fase de implementación de la plataforma. En este sentido el framework Fabric es agnóstico y no impone una única solución en mérito al código de cadena y a la Política de Endorsamiento.

6.2 Nodos

La arquitectura se compone de participantes denominados nodos los cuales juntos forman una red. La participación es otorgada por el servicio proveedor de membresía MSP. Los nodos pueden ser de tres tipos:

El Cliente. El cliente el nodo que envía la solicitud inicial de transacción para que pueda ser ejecutada, ordenada y validada.

El Participante (Peer). Los nodos de tipo Peer tienen la función de ejecutar (simular mediante la ejecución del chaincode) las transacciones propuestas por un Cliente para poderlas avalar. También tienen la función de validar las transacciones verificando los productos de las simulaciones. Los participantes de tipo peer también tiene el rol de mantener una copia de la cadena de bloques. Es importante mencionar que solo un sub-grupo de los peers está autorizado para endorsar una transacción, los miembros de este grupo se definen como Peers Endorsadores.

El Nodo de Servicio de Ordenamiento. Los nodos de este tipo participan en la implementación del Servicio de Ordenamiento. Es el servicio que se hace cargo de ordenar cronológicamente todas las transacciones enviadas por los nodos endorsadores. Las transacciones endorsadas incluyen el producto de la ejecución y a las firmas digitales de cada nodo que las ha avalado.

6.3 Fases

Cualquier interacción de lectura o escritura con el libro maestro es considerada una transacción. La inmutabilidad de la cadena no permite modificaciones posteriores, las transacciones de escritura son siempre nuevas (append only) y la información de la cadena no puede ser modificada para conservar la característica de confiabilidad de la información.

El ciclo de vida de una transacción se articula en las siguientes tres fases distintas:

6.3.1 Ejecución

En esta fase un Cliente crea una propuesta de transacción, la firma y la envía a varios nodos establecidos como endorsadores. Cada nodo endorsador reciben la propuesta de transacción y la ejecuta, es decir que simula la transacción mediante la ejecución del código de cadena y devuelve el resultado al Cliente sin alterar el libro maestro. La devolución del resultado se define como respuesta de la propuesta.

La propuesta de transacción es un objeto JSON que contiene al menos los siguientes datos:

La identidad del Cliente, de acuerdo al Servicio Proveedor de Membresía.

La carga útil. Contiene la operación que caracteriza la transacción (ej, Juan Perez compra un servicio del proveedor Perico de los Palotes). En caso no se pueda estructurar la carga útil en términos de texto plano, se podría almacenar el documento transformado en cadena (ej, mediante base64). Tambien se podria realizar un almacenamiento fuera de la cadena (off-chain storage) [6].

El identificador del código de cadena. El código será usado en la fase de ordenamiento por parte de los participantes endorsadores.

Un valor aleatorio. Tiene que ser usado una sola vez por cada cliente.

Un identificador de la transacción. Se compone sobre la base del valor aleatorio y del identificador del Cliente.

La respuesta de la propuesta contiene los siguientes datos:

El writeset (set de escritura). Contiene los estados del libro mayor que se actualizarán en base al resultado de la simulación.

El readset (set de lectura). Contiene los estados del libro mayor antes de la ejecución de la

simulación.

El identificador de la transacción.

El identificador del endorsador.

La firma de la respuesta por parte del participante endorsador.

6.3.2 Ordenamiento

Cuando el Cliente ha recibido un número suficiente de respuestas entonces las ensambla en una transacción y las envía con firma al Servicio de Ordenamiento.

La transacción contiene los siguientes datos:

La carga útil de la propuesta de transacción.

Los metadatos de la transacción

El conjunto de respuestas de la propuesta de transacción.

El Servicio de Ordenamiento recibe la transacción con los resultados de los varios endorsamientos, la ordena dentro de las demás transacciones recibidas y aplica el algoritmo de consenso. Si se establece el consenso de la transacción entonces el Servicio de Ordenamiento pública la transacción a todos los participantes (endorsadores y no endorsadores) para que procedan con la fase de validación.

El servicio de ordenamiento ensambla varias transacciones en bloques para optimizar la eficiencia de la difusión.

6.3.3 Validación

Los bloques ensamblados por el Servicio de Ordenamiento llegan a todos los participantes para que se pueda realiza la validación final de cada transacción. La validacion esta basada en los productos generados en la fase de ejecución y no necesita la ejecución del chain code. Por esta razón todos los nodos, no solo los endorsadores, pueden tomar parte en el proceso de validación. Una vez terminada la validación de la transacción esta es añadida al libro mayor que cada participante tiene en su base de datos. Es importante notar que de acuerdo a esta arquitectura se anotan en el libro mayor también las transacciones que no han resultado válidas. La transacciones no válidas son marcadas oportunamente para poder ser identificadas dentro del bloque.

7. SEGURIDAD

La seguridad involucra varios aspectos de la cadena de bloques que se deben tomar en cuenta.

7.1 Seguridad de arquitectura de la cadena de bloques

La arquitectura de la mayoría de las cadenas de bloques está conformada por una arquitectura de ordenamiento y ejecución sin ninguna verificación adicional. Este arquitectura tiene varias desventajas para un sistema con permisos de admisión.

La ejecución secuencial de las transacciones en todos los nodos limita el rendimiento de salida que puede realizarse en la cadena de bloques. Particularmente debido a que el rendimiento es inversamente proporcional a la latencia de ejecución esto representa un cuello de botella para la mayoría de códigos de cadena.

La cadena de bloques representa una máquina de computo universal y sus cargas de cómputo pueden ser desplegadas por adversarios. Esto es susceptible a un ataque de denegación de servicios que puede destruir o interrumpir de forma permanente el sistema de cadena de bloques introduciendo un código de cadena que toma demasiado tiempo en ejecutarse.

Para considerar este riesgo la arquitectura considera la ejecución previa, el ordenamiento y la validación final para evitar ataques por tipo de arquitectura.

7.2 Modelo de confianza y falla

El sistema de cadena de bloques debe ser flexible en la presunción de confianza y fallas. En general cualquier cliente debe ser considerado potencialmente malicioso o denominado bizantino. Los participantes están agrupados en organizaciones y cada organización forma un dominio de confianza tal que los participantes confían en los demás participantes de su organización pero no en los participantes de otras organizaciones. El servicio de ordenamiento con su algoritmo de consenso considera a todos los participantes como potencialmente maliciosos.

Por este motivo la integridad de la plataforma depende en la consistencia del servicio de ordenamiento.

7.3 Integridad del código de cadena

La integridad del código de cadena depende de su correcta instalación e instanciación en el nodo participante.

La seguridad contra inyecciones maliciosas en el código de cadena de un nodo puede verificarse mediante los dos sistemas de comprobación inicial y final de la plataforma de bloque de cadenas.

7.4 TLS

El protocolo TLS permite la identificación y autenticación de la comunicación de los nodos de las entidades con el servidor de autoridad de certificación del sistema de cadena de bloques logrando confidencialidad e integridad de la información.

Es recomendable habilitar siempre en los archivos de configuración del servidor de la autoridad de certificación el uso de TLS.

7.5 Independencia del sistema de ordenamiento

El servicio de ordenamiento verifica que los bloques enviados por el sistema de ordenamiento estén totalmente ordenados. Más aún el sistema de ordenamiento está separado de ejecutar o validar las transacciones y no mantiene ningún registro del estado actual de estado del bloque de cadenas.

7.6 Zona horaria

Las entidades que participen en el sistema de cadena de bloques deben utilizar la misma zona horaria, con el fin de que todas las entidades conciban los tiempos de la misma manera. Para el caso del Estado Plurinacional de Bolivia se utiliza GMT-4.

7.7 Sellado de tiempo y versionamiento

El sellado de tiempo de cada transacción invocada en la plataforma de cadenas de bloques se realiza en el tiempo de ejecución por los endorsadores al momento de ejecutar la transacción.

En este tiempo de ejecución también se incrementa el número de la versión de la transacción sobre el par llave y valor sobre la cual está actuando la transacción para la verificación de coherencia de versiones en la validación final por parte de todos los nodos participantes del canal de transacciones.

7.8 Firma digital

Asocia un mensaje entre nodos a un firmante con autenticidad, integridad y no repudio. Identifica un certificado digital con la identidad de un cliente o un nodo participante. Permite verificar si la información de los mensajes entre nodos ha sido modificada.

7.9 Protección de certificados

Los certificados otorgados a los participantes del cadena de bloques pueden ser protegidos desde hardware con la utilización de HSM con APIS de PKCS11. La configuración para este caso está configurada en la sección BCCSP (BlockChain Crypto Service Provider) de la configuración de un cliente o servidor miembro de la plataforma.

8. POLÍTICAS

8.1 Actores y roles en la plataforma

Cada participante de la plataforma puede tener diferentes perfiles dentro la misma, se definen las políticas generales para cada uno de los miembros.

8.1.2 Miembros de la plataforma

Los miembros de la plataforma son los que tienen un rol activo dentro de la misma y realizan tareas para garantizar su funcionamiento. Los mien

8.1.2.1 Miembro administrador

El administrador de la plataforma tiene la responsabilidad de incorporar nuevos miembros a la misma definiendo su rol y el tiempo de permanencia, previa postulación al comité y aprobación del mismo.

8.1.2.2 Miembro autoridad de certificación

Responsable de emitir certificados para la participación de los miembros aprobados por el comité. Tiene como requisito indispensable contar con políticas y protocolos de seguridad para emisión de certificados digitales.

8.1.2.3 Miembro verificador (endorsador)

Responsable de recibir las transacciones hacia la plataforma, realizar la simulación en la cadena y proponer las transacciones a la misma.

Tiene como requisitos:

Poder dedicar infraestructura en servidores y comunicaciones con alta disponibilidad.

Contar con personal técnico a cargo del mantenimiento de esta infraestructura.

Contar con políticas y lineamientos de seguridad institucionales para la gestión de tecnologías de información y comunicación.

8.1.2.4 Miembro de control de orden

Responsable de escribir las transacciones en la cadena, es imprescindible la capacidad de

cómputo para realizar esta tarea.

Tiene como requisitos:

Poder dedicar infraestructura en servidores y comunicaciones con alta disponibilidad.

Contar con personal técnico a cargo del mantenimiento de esta infraestructura.

Contar con políticas y lineamientos de seguridad de la entidad para la gestión de tecnologías de información y comunicación.

8.1.2.5 Miembros de almacenamiento

Responsables de mantener una copia de las transacciones escritas en la plataforma. Es necesario tener capacidad de crecimiento tecnológico en el tiempo.

Tiene como requisitos:

Poder dedicar infraestructura en servidores y comunicaciones con alta disponibilidad.

Contar con personal técnico a cargo del mantenimiento de esta infraestructura.

Contar con políticas y lineamientos de seguridad entidades para la gestión de tecnologías de información y comunicación.

8.2 Usuarios de la plataforma

Los usuarios de la plataforma son las entidades que pueden solicitar la inscripción de transacciones en la plataforma.

Requisitos para ser usuario de la plataforma:

Firmar la norma de adhesión

Contar con un certificado válido y vigente

8.3 Solicitud de transacción en la cadena

Los usuarios o miembros de la cadena pueden realizar solicitudes para iniciar transacciones en la plataforma a través de una miembro verificador.

8.4 Inicialización de la plataforma de cadena de bloques estatal

8.4.1 Solicitud de participación

El funcionamiento del sistema inicia mediante la solicitud de las entidades que deseen participar en el sistema de bloques de cadenas estatal para formar un comite en conjunto con la AGETIC, con el fin de crear un sistema de orden cronológico descentralizado de integridad para documentos digitales.

8.4.2 Creación de la autoridad de certificación

El sistema interno de autoridad certificadora CA se crea en primera instancia con creación de su certificado y registro del administrador.

La AGETIC como administrador de la autoridad certificadora CA ejecuta el software que pone en funcionamiento al sistema interno de infraestructura de clave pública utilizando un imagen de sistema operativo Linux que ejecuta código de autoridad de certificación.

8.4.3. Establecimiento del servicio de provisión de membresía

La autoridad de certificación de la AGETIC está encargada del registro y autorización de participantes y es el primer paso para establecer el servicio de provisión de membresía del sistema de cadenas de bloques.

8.4.4 Inicialización de los nodos participantes

Las entidades admitidas como participantes del sistema de cadena de bloques reciben el manual de instrucciones de la AGETIC para la instalación de software libre para el funcionamiento de los nodos participantes.

Una vez que los nodos participantes de las entidades autorizadas están funcionamiento establecen una capa de comunicación segura con el administrador del sistema de cadena de bloques y con los servicios de provisión de membresía para su enrolamiento.

8.4.5 Bloque inicial y configuración del canal de transacciones

La creación del canal de participantes de la cadena de bloques está determinada por la creación de un bloque inicial que contiene la información inicial de valores iniciales del libro mayor de la cadena de bloques.

La AGETIC invoca la configuración del canal de transacciones y la creación del primer bloque de la cadena de bloques con valor inicial de depósito del primer documento digital como primera transacción.

8.4.6 Inicialización de bases de datos distribuidas

Los nodos participantes inscritos y enrolados en el sistema de bloques de cadenas proceden a continuación de acuerdo al manual entregado por la AGETIC, a inicializar sus bases de datos de registro del libro mayor de transacciones.

Este paso comprende la ejecución de instrucciones en software libre para invocar la creación de bases de datos adjuntas al nodo participante.

La base de datos está adjunta al nodo y está compuesta de software libre para almacenamiento en formato tipo JSON, para el uso de pares de llaves y valores en cadenas.

8.4.7 Instalación del código de cadena

Cuando los nodos participantes de las entidades han inicializado sus bases de datos, se debe instalar el código de cadena. Lo mismo está descrito en el manual de instalación provisto por la AGETIC.

Esta instalación la realiza la AGETIC como entidad de administración del sistema de cadenas de bloques mediante la capa de comunicación con el nodo de la entidad. El software será invocado por el nodo participante al momento de solicitar una transacción con el sistema de cadena de bloques.

El código de cadena es un programa que contiene la lógica de negocio del sistema de cadena de bloques estatal.

8.5 Adhesiones a roles de los participantes

Los roles de los participantes serán designados por el comité de la plataforma. El rol de endorsamiento será asignado a la AGETIC con posibilidad de tener nodos participantes de otras entidades.

9. GESTIÓN DE LA PLATAFORMA

9.1 Comité de la plataforma de registro

El comité de la plataforma de registro tiene a cargo la gestión de la misma y está conformado por la entidades miembros del mismo, bajo el siguiente esquema:

Presidencia del comité estará a cargo del Director(a) General Ejecutivo(a) de la AGETIC, cuyas atribuciones serán:

Actualizar los lineamientos de la plataforma

Definir y aprobar las actualizaciones técnicas

Convocar a sesiones ordinarias y extraordinarias del comité

Velar por el cumplimiento de la normativa aplicable a la plataforma

Aprobar y gestionar la normativa recomendada por los miembros del comité

Elaborar y aprobar el reglamento de funcionamiento interno como condición necesaria para la operación de la plataforma.

Aceptar el ingreso de miembros

Miembros del comité. Son todos los miembros de la plataforma que cumplen un rol de verificación, ordenamiento, almacenamiento, certificación, administradores, cuyas atribuciones serán:

Formular propuestas de políticas y normativa relacionada a la plataforma, para consideración de la presidencia.

Sugerir a la presidencia nuevos miembros.

Sugerir actualizaciones técnicas.

9. 2 Autoridad certificadora

La designación de la autoridad certificadora en la fase inicial de la plataforma es emitida por la presidencia del comité.

9.2.1 Procedimientos

La entidad certificadora necesita definir y aprobar con el comité los siguientes procedimientos para poder habilitarse en la plataforma:

Procedimiento de generación de certificado raíz, debe incluir la participación de la presidencia del comité como veedor del proceso.

Procedimiento de otorgación, renovación y revocación de certificados a los miembros.

Procedimiento de otorgación, renovación y revocación de certificados a los usuarios.

9.3 Portal de la plataforma

La AGETIC está a cargo de implementar y mantener el portal de la plataforma que debe tener mínimamente:

Portal de información general de la plataforma

01 de Junio de 2018
AGETIC/RA/0039/2018
Expediente: 34245
Módulo de verificación de la integridad y cronología de los documentos

Lineamientos actualizados

Estado técnico de la plataforma y sus nodos

9.4 Procedimiento de adhesión por por roles en la plataforma

La adhesión a la plataforma la puede solicitar cualquier entidad público o instituciones privadas que prestan servicios públicos delegados por el Estado, mediante la designación de un responsable para la coordinación con el administrador de la plataforma. Dependiendo del tipo de rol se tiene los siguientes requisitos.

9.4 .1 Para miembro administrador

El Miembro administrador de la plataforma será la AGETIC, la cual tiene las siguientes responsabilidades:

La AGETIC registra a las entidades públicas como nuevo miembro definiendo su rol, previa postulación al comité y aprobación del mismo.

Monitorear el funcionamiento y disponibilidad de los nodos.

Gestionar los accesos.

Mantener el portal con la información técnica mínima para cada uno de los roles.

9.4.2 Para miembro autoridad de certificación

El miembro autoridad de certificación será la AGETIC, la cual tiene las siguientes responsabilidades:

Emitir certificados para la aprobación del comité.

Deberá de contar con políticas y protocolos de seguridad para la emisión de certificados digitales.

9.4.3 Para miembro verificador (endorsador)

El miembro verificador puede ser cualquier entidad pública , previamente registrada y contar con los certificados aprobados por el comité.

La entidad que quiera ser miembro verificado (endorsador) deberá enviar una solicitud al comité indicando que cuenta con lo siguiente:

Infraestructura en servidores y comunicaciones con alta disponibilidad.

Personal técnico a cargo del mantenimiento de esta infraestructura, indicar el o los nombres de las personas a cargo.

Políticas y lineamiento de seguridad institucionales para la gestión de tecnologías de información y comunicación

Poder dedicar infraestructura en servidores y comunicaciones con alta disponibilidad.

9.4.4 Para miembro de control de orden

El miembro control de orden puede ser cualquier entidad pública, previamente registrada y contar con los certificados aprobados por el comité.

La entidad que quiera ser miembro de control de orden deberá enviar una solicitud al comité indicando que cuenta con lo siguiente:

Infraestructura en servidores y comunicaciones con alta disponibilidad.

Personal técnico a cargo del mantenimiento de esta infraestructura, indicar el o los nombres de las personas encargadas.

Políticas y lineamientos de seguridad institucionales para la gestión de tecnologías de información y comunicación.

9.4.5 Para miembros de almacenamiento

El miembro de almacenamiento puede ser cualquier entidad pública, previamente registrada y contar con los certificados aprobados por el comité.

La entidad que quiera ser miembro de control de orden deberá enviar una solicitud al comité indicando que cuenta con lo siguiente:

Infraestructura en servidores y comunicaciones con alta disponibilidad.

Personal técnico a cargo del mantenimiento de esta infraestructura, indicar el o los nombres de las personas encargadas.

Políticas y lineamientos de seguridad institucionales para la gestión de tecnologías de información y comunicación.

9.5 Seguridad y disponibilidad

9.5.1 Seguridad

Todos los servicios que operan en la plataforma se publican bajo el protocolo TLS (Transport Layer Security), que permite la identificación y autenticación de las entidades a nivel de la capa de transporte, lo que permite que la comunicación sea confidencial y que los datos enviados y recibidos sean íntegros.

Todos los servicios de la plataforma cuentan con mecanismos de control de ingreso que permiten identificar a los usuarios y si fuera necesario, revocar los accesos a la plataforma.

Permite mantener la confidencialidad de los datos cuando estos son sensibles. Para este propósito se puede utilizar algoritmos de cifrado como AES con una clave de 128 bits o más, o RSA con una clave de longitud mínima de 2048 bits.

Todas las solicitudes y respuestas que pasan a través de la plataforma se almacenan en un registro de eventos para su posterior análisis y aplicación de medidas preventivas y/o correctivas en los servicios si así fuera necesario.

Realiza bloqueo de consultas en base a direcciones físicas para mejorar el control de de acceso a la plataforma.

9.5.2 Disponibilidad

Cada miembro de almacenamiento tiene servicios de consulta en la plataforma dispone de mecanismos de consulta para poder verificar los datos y documentos.

Se realizan pruebas de carga y de estrés de manera periódica para verificar que los servicios fiables y utilizan sus recursos de manera eficiente.

01 de Junio de 2018
AGETIC/RA/0039/2018
Expediente: 34245
Se publica una página web para mostrar el estado de los servicios y nodos de la plataforma, lo que permite verificar el estado de los servicios y nodos de manera sencilla.

Se informará cualquier suspensión o mantenimiento en la plataforma de interoperabilidad para tomar previsiones al respecto con el tiempo necesario.

9.6 Faltas y sanciones

9.6.1 Faltas

El incumplimiento por parte de las entidades usuarias o miembros a cualquiera de las disposiciones establecidas en las políticas y lineamientos de la plataforma, se constituye como falta, de acuerdo a la siguiente catalogación:

1. FALTAS GRAVES. - Son catalogadas como faltas graves a incumplir con cualquiera de los preceptos señalados en el presente documento.

2. FALTAS MUY GRAVES. - Serán catalogados como faltas muy graves:

a. La reincidencia en las faltas graves.

b. Utilizar los servicios de la plataforma para fines no concertados previamente y que afecten al rendimiento de la misma.

9.6.2 Sanciones

La AGETIC en cualquier caso, se reservará el derecho de interrumpir a las entidades usuarias o miembros el acceso a la plataforma sin previo aviso si considera suficientemente probado cualquier tipo de riesgo a la seguridad de los plataforma.

Las sanciones serán aplicadas, ante el incumplimiento a cualquiera de las disposiciones establecidas en los lineamientos, la misma que derivará en las siguientes sanciones, sin que medie trámite o aviso previo alguno:

a. Sanciones por faltas graves: Interrupción del acceso, sin previo aviso, la misma será levantada una vez resuelta la causal que propició la observación en cuestión; y

b. Sanciones por faltas muy graves: Revocatoria de la autorización, sin previo aviso a los usuarios de la entidad que incurrió en las faltas establecidas.

9.6.3 Revocatoria de acceso

Para aquellos casos donde la AGETIC advirtió faltas por parte de la entidad usuaria o miembro, podrá revocar los accesos a los servicios de la plataforma.

Cuando exista una falta muy grave, la AGETIC notificará a la Máxima Autoridad Ejecutiva de los incidentes y procederá a la interrupción y suspensión del servicio. Además solicitará el cambio del responsable y notificará a la entidad publicadora para que la misma asuma las acciones legales correspondientes según el perjuicio, gravedad o daño ocasionado.

La AGETIC en cualquier caso, se reserva el derecho de interrumpir a las entidades consumidoras el servicio, sin previo aviso si considera suficientemente probado cualquier tipo de riesgo a la seguridad de los servicios, los datos y/o información transferidos u otros.

9.6.4 Actualización de las políticas.

Tomando en cuenta la naturaleza dinámica de la tecnología, se debe realizar la revisión y actualización de las políticas de la implementación del uso de registro cronológico en

integridad de datos y documentos digitales en el Estado.

Para la actualización de las políticas se tiene que realizar el siguiente procedimiento:

El comité realizará la evaluación de la actualización de las políticas, previamente a un informe técnico que describa las razones por la que se tienen que realizar la actualización a las políticas de implementación de uso de registro cronológico en integridad de datos y documentos digitales en el Estado y lo remitirá a la AGETIC para su consideración.

9.7 Exención de responsabilidad de la AGETIC

La AGETIC no asumirá las responsabilidades que sean atribuibles a las entidades usuarias o miembros participantes en la plataforma, respecto a:

Problemas con el servicio, debido a factores diversos como la interrupción del servicio de proveedores de internet, falla en los sistemas o redes, cortes de energía, fallas humanas y otros.

Problemas o interrupción en la prestación del servicio debido a causas de fuerza mayor o caso fortuito.

Problemas atribuibles a la mala configuración de los servicios por parte de los miembros de la plataforma.

Uso de la plataforma para fines que no sean de gobierno electrónico u otros procesos del Estado legítimamente acreditados.

Uso de la plataforma para fines que no se establecieron con la AGETIC.

Problemas derivados de la negligencia, errores, acciones u omisiones de los miembros de la plataforma.

Las entidades usuarias de la plataforma son responsables del contenido y gestión de los documentos, la plataforma solo es un registro de orden cronológico y la integridad de los datos o documentos.

De la misma forma, toda posible controversia referente a la calidad, validez e integridad de los datos e información, se resolverá de manera directa entre las entidades usuarias. Las entidades asumirán frente a los destinatarios o ciudadanos toda la responsabilidad por el uso, destino y gestión que dé a los datos e información. La AGETIC y los miembros de la plataforma que no participan del proceso, gestión, transacción o trámite deslindan de toda responsabilidad respecto a cualquiera de estos aspectos.

9.8 Gestión técnica

La gestión técnica de la plataforma está a cargo de la AGETIC, que comprende las siguientes tareas:

Definir los procedimientos de ejecución automática en los miembros de la plataforma.

Actualizaciones de configuración.

Revisiones periódicas de seguridad.

Prever la disponibilidad de la plataforma, realizando análisis de riesgos de forma periódica e implementando medidas para mitigar los mismos.

Brindar capacitación y transferencia tecnológica a entidades públicas.

10. Definición de términos y Abreviaciones

Criptomoneda.- Tipo de moneda no regulado, digital, emitido y controlado por sus creadores. Es utilizada y aceptada entre los miembros de una comunidad virtual sin un banco central emisor que lo respalde pero es corroborada por un sistema de cadena de bloques.

Libro mayor.- El libro mayor o mayor contable es un libro que recopila todas las transacciones registradas de valores de manera cronológica.

Firma criptográfica.- Denominada también firma digital es un mecanismo criptográfico que permite al

receptor de un mensaje firmado digitalmente identificar a la entidad originadora de dicho mensaje con seguridad de que el mensaje original no fue alterado en su contenido.

Árbol de Merkle.- Un árbol de Merkle se denomina también árbol de hash, es una construcción en forma de árbol de valores en donde cada nodo interior, es el resultado de aplicar una función de hash sobre el valor de los nodos hijos hasta llegar a un nodo raíz llamado Merkle root del árbol.

Mineros de bloques.- En sistemas de cadenas de bloques de tipo abierto, los mineros de bloques añaden nuevos bloques de transacciones a la cadena después de ejecutar un algoritmo de consenso realizando una prueba de trabajo, generalmente resolviendo una ecuación criptográfica compleja en el menor tiempo posible.

Hyperledger.- Marca registrada del esfuerzo colaborativo en software libre de sistemas de cadenas de bloques. Fue creado por la Linux Foundation para el desarrollo de sistemas distribuidos de bases de datos con comprobación cronológica.

Endorsamiento.- El endorsamiento o verificación inicial, representa una tarea asignada a un nodo o más nodos en conjunto que son participantes de un sistema de cadena de bloques para simular una transacción propuesta por un cliente del sistema y enviar su resultado simulado de vuelta al cliente junto con su firma criptográfica.

Host.- Nombre del nodo participante en un sistema de cadenas de bloques, en la capa de comunicación mediante el cual los otros nodos pueden visualizarlo y comunicarse con él directamente.

Redes Virtuales.- Una red virtual en un sistema distribuido representa una abstracción de una capa de comunicación que permite el envío de mensajes entre diferentes nodos conectados a una red en común.

Código de Cadena.- El código de cadena es un denominativo de la plataforma Hyperledger que señala al programa, escrito en código NodeJS, Go o C/C++, que interactúa con el libro mayor. Es el único intermediario entre la cadena de bloques y el nodo solicitante de una transacción.

Framework fabric.- El Framework fabric puede ser considerado como un sistema operativo distribuido para la creación de plataformas de cadenas de bloques con diferentes características programadas al momento de su inicialización.

Sistema de ordenamiento.- Es un grupo de nodos con la tarea de realizar bloques agrupando transacciones y aplicando algoritmos de consenso sobre las transacciones enviadas al sistema. Es agnóstico del contenido de las transacciones.

Consenso.- Acuerdo entre los nodos delegados sobre la forma de construcción de un bloque nuevo de transacciones para añadirlo al libro mayor de una cadena de bloques.

Abreviaciones

P2P.- Entre iguales o entre pares es una comunicación entre nodos.

MSP.- Servicio proveedor de membresía de una plataforma de cadena de bloques

CA.- Autoridad certificadora de un sistema de cifrado de clave pública

SDK.- Kit de desarrollo de software para hacer interfaz a un software interno.

API.- Interfaz de programación de aplicaciones.

EOV - Ejecución Ordenamiento Validación

OE - Ordenamiento Ejecución

11. Referencias

[1] Hyperledger Fabric, https://www.hyperledger.org/projects/fabric .

[2] E. Androulaki et al., Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains, EuroSys 2018.

[3] CTIC-EPB. Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia. "Lineamientos para la implementación de servicios de interoperabilidad para las entidades del sector público".

[4] Androuaki Elli. Cachi Christian. Ferris Christopher, et al. "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains" EuroSys ´18. Abril 2018.

[5] Sousa, Joao. Bessani, Alysson. Vukolic, Marko. "A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform". 20 Sep 2017. pp. 1-10.

[6] Zyskind, Guy. Nathan, Oz. Pentland, Alex. "Descentralizing Privacy: Using Blockchain to Protect Personal Data". 2018.

[7] Lamport, Leslie. Shostak, Robert. Pease, Marshall. "The Byzantine Generals Problem". ACM Transactions on Programming Languages and Systems. Vol 4. No. 3, July 1982. pp. 382-401.

[8] Decreto Supremo 3525 del 4 de abril de 2018

Regístrese, comuníquese, cúmplase y archívese.

Fdo.-

LAOV

Cc.:archivo