White paper técnico

(Se pueden agregar algunos detalles)

Sistema financiero descentralizado

CREDITS

Versión 1.5 / 12.09.2017

Abstracto
La plataforma CREDITS es un sistema financiero descentralizado para la interacción directa entre los participantes en los principios de Peer-to-peer (P2P). La plataforma amplía el potencial de utilizar servicios financieros sobre la base de un libro mayor distribuido, contratos inteligentes de autoejecución y criptomonedas CREDITS. El sistema está dirigido a unir a todos los participantes en un sitio, proporcionándoles una plataforma para crear y usar servicios financieros, donde todos pueden ofrecer un servicio y usarlo. Gracias a un sistema tecnológico bien definido y equilibrado, la plataforma CREDITS ofrece una nueva solución técnica y un nuevo modelo conceptual de la interacción de los participantes en la red para el desarrollo de servicios financieros modernos descentralizados.

Introducción

Un acuerdo completamente entre pares para sistemas de prestación de servicios que permite formar servicios financieros: transferencias de dinero, intercambios de divisas y valores, créditos, fondos y otros servicios directamente entre los participantes. Todo se proporciona sin intermediarios adicionales, de acuerdo con un principio, uno de participantes iguales, a otros participantes del sistema. Como resultado, todos obtienen servicios más baratos, más rápidos y mejores.

El mundo se está moviendo hacia la interacción directa entre las personas en los principios de Peer-to-peer - igual a igual. ¡Sucedió una revolución! Esto se ve claramente en la revocación de los medios de comunicación: hasta la década de 1990, los periódicos, las revistas y la televisión fueron los principales proveedores de información. Hoy en día, los líderes de opinión son blogueros, se encuentran en los canales de YouTube y en las redes sociales, el dinero se invierte en crowdfunding e ICO, y la información se almacena en sistemas de nube descentralizados.

La industria financiera, quizás, es una de las pocas industrias rezagadas, que resiste la introducción de la descentralización y la interacción directa entre los participantes. Aunque, técnicamente, es mucho más fácil crear servicios financieros descentralizados que crear vehículos no tripulados.

Se requiere un entorno tecnológico a fin para crear un sistema de productos y servicios financieros descentralizados basados en el libro mayor distribuido:

1. Alta velocidad de ejecución (en segundos), junto con la capacidad de manejar una gran cantidad de transacciones simultáneamente (cientos de miles por segundo) a un bajo costo de cada transacción (para micropagos y transacciones no monetarias).
2. Desarrollo de un sistema donde se combinan todos los participantes y elementos necesarios para los servicios descentralizados financieros cualitativos: personalización de usuarios, KYC, buró de historial de crédito, centros de liquidación de dinero fiduciario, retiro y cobro de criptomonedas, etc. Estas son dos grandes tareas básicas que actualmente obstaculizan el desarrollo de productos financieros peer-to-peer.

Le presentamos una solución para estas tareas, implementada con la ayuda del sistema financiero CREDITS.

CREDITS es la única plataforma tecnológica descentralizada que puede combinar todos los participantes de los servicios financieros, de forma segura, rápida y ejecutar todas las transacciones utilizando los principios de un libro mayor distribuido.
autoejecutar contratos inteligentes y los principios de un sistema de votación federado brindan oportunidades ilimitadas para que todos los participantes creen interacciones únicas de varios productos financieros. La plataforma abre un enorme nuevo mercado y un nuevo potencial para el uso de proyectos y servicios de cadena de bloques en sectores financieros y de otro tipo que no se podían usar anteriormente debido a la velocidad y las limitaciones de los costos de transacción.

1. Libro mayor de la red
Definiciones
1. Un sistema es un conjunto de nodos de red descentralizados que realizan el procesamiento, guardan las transacciones, ejecutan y confirman los términos de los contratos inteligentes, procesan las solicitudes de los sistemas de terceros y proporcionan información cuando se solicita.
2. Un nodo de red es una computadora donde se instala un cliente de red completo, conectado a un sistema común, verificando las transacciones y escribiéndolas en el libro mayor.
3. Un libro mayor es la lista de transacciones confirmadas por el sistema y almacenadas en todos los nodos de la red.
4. Una transacción es el elemento del sistema, que denota una solicitud para realizar un método de contrato inteligente o cualquier acción en la red y registra los resultados en un sistema de cadena de bloques.
5. Un contrato inteligente es el elemento del sistema, los protocolos de la computadora que facilitan, verifican o garantizan el cumplimiento de los términos de la interacción. Usualmente tienen una interfaz de usuario y a menudo emulan la lógica de las relaciones contractuales. La propiedad clave de un contrato inteligente es su descentralización y su independencia de una fuente central.
6. Un método de contrato inteligente es el código del programa responsable de calcular el resultado del trabajo de los términos del contrato inteligente y registrarlo en el libro mayor.
7. Una parte contratante es el participante final de la red y el usuario del sistema.

Nodos de red
Usamos varios tipos de nodos, dependiendo de su propósito de construir una red descentralizada basada en el acceso libre y la conexión de nodos:
1. Un nodo común (ОУ) es el nodo que participa en la verificación de transacción para la validez pero tiene un factor de confianza mínimo. También es un candidato para el rol de un nodo confiable y el nodo del procesamiento actual en el próximo ciclo de selección de roles de nodo en la red.
2. Un nodo de confianza (ДУ) es el nodo que participa en la verificación de transacción y tiene el factor de confianza máximo (1), es un candidato para el rol del nodo del nodo actual de procesamiento y común. Este nodo no puede convertirse en confiable durante una cantidad calculada matemáticamente de ciclos de selección y votación entre nodos El cálculo matemático depende de la cantidad de nodos y la complejidad de la red.
3. El nodo principal (ГУ) de la red es el nodo que participa en la verificación y es responsable de agregar transacciones al bloque del libro mayor de transacciones. Este nodo no puede convertirse en confiable o el nodo del procesamiento actual durante un

número matemáticamente calculado de ciclos de votación, cuyo cálculo matemático depende de la cantidad de nodos y la complejidad de la red.
El sistema usa un factor de confianza, un valor numérico fraccionario absoluto de 0 a 1, expresado en términos matemáticos de la cantidad de nodos de confianza +1 al número total de nodos en la red. La cantidad máxima de nodos de confianza no puede superar el 50% de los nodos de red.

El último bloque guardado
El Libro mayor común de Bloques (CRB) es el estado sincronizado de todo el Libro mayor común de bloques en todos los nodos del sistema.
Según el contenido del bloque de libro mayor, nos referimos a una unidad de información almacenada que contiene un código hash del bloque anterior y una lista de datos relacionados con este libro mayor con el número asociado del bloque anterior. Al recibir el bloque de otro nodo, toma su lugar en el libro de contabilidad común de bloques según el número. Esto ahorra ancho de banda de red.
Durante la sincronización, solo se verifica primero el número de bloque. Si falta el bloque en este nodo, se descarga y se guarda.
Como resultado, el sistema en cualquier momento contiene la última copia actualizada del libro mayor. Lo llamamos el último libro mayor (LR). Es automáticamente creado por el nodo responsable de la formación del libro mayor al llegar a un consenso. Este bloque se envía a todos los nodos del sistema para mantener la uniformidad actualizada del estado del Libro mayor en todos los nodos del sistema.
Cada nodo está asociado con todos los otros nodos de la red y constantemente intercambia nuevos bloques con transacciones con ellos, a fin de mantener siempre la información relevante. Todos los bloques forman un conjunto de candidatos de transacciones que esperan ser agregados al libro mayor. Al mismo tiempo, cada servidor genera conjuntos supuestos de los candidatos para otros servidores y el conjunto propuesto de transacciones. Se toma una decisión al verificar, ya sea para agregarlos al libro mayor.
Como resultado, es posible almacenar los datos del libro de contabilidad varias veces en varios servidores: los nodos del sistema y toda la información está protegida. Cuantos más nodos hay en el sistema, más confiable e independiente es.

Sincronización de nodos
Cada nuevo nodo se inicia y sincroniza después de la definición de la determinación y la verificación completa de la confianza. Para mejorar la velocidad de procesamiento de la información, todos los procesos se manejan simultáneamente, independientemente el uno del otro. Si no hay variables entrantes, se crea un almacén contable vacío: se reserva un espacio en la RAM para un acceso simplificado adicional. En el caso de que el libro mayor requerido no esté disponible, se envía una solicitud a los nodos de confianza para recibir todas las transacciones realizadas para la cuenta sincronizada.
Si el parámetro de entrada es un objeto que caracteriza la transacción, entonces se inicia la búsqueda en todos los hilos de sincronización en ejecución. La operación da como resultado un código numérico: el número de posición en el libro mayor de nodos confiable para el hilo actual o el número de error si el valor es menor que cero. Si el método de subproceso finaliza con un error de conexión, el hilo termina por completo.
2. Consenso de la red
El consenso en CREDITS es un método de toma de decisiones grupales.
Con el objetivo de desarrollar soluciones finales aceptables para todos los nodos de red.

Comparación de consenso
La definición de los principios del libro de CREDITS descentralizados para comparar diferentes tipos de consenso:
● disponibilidad del libro mayor (los nodos pueden escribir datos en el libro mayor y leerlos en cualquier
hora);
● Modificabilidad por todos los nodos de red participantes;
● Consistencia de todos los nodos del sistema (todos los nodos ven una versión absolutamente idéntica del libro mayor, que se actualiza después de los cambios);
● Resistencia a la separación (si un nodo se vuelve inoperable, esto no afecta el operación de todo el libro mayor).

Parámetro comparado	Créditos específicos PoW y PoC	PoW	PoS
El principio de identificar el nodo que generó el bloque.	Cálculo de la función matemática. Confirmación de almacenamiento de la última copia del libro mayor.	Realizando un cálculo iterativo de la función matemática, con complejidad variable.	Busque la pila máxima entre los participantes (nodos competidores)
Ataque 51%.	Improbable, ya que es necesario tener un libro contable completo en recursos y una potencia de cálculo para calcular, y los nodos de confianza se seleccionan dinámicamente.	Probable, pero será muy costoso en términos de uso de recursos.	Probable, pero costoso, debido a la necesidad de aumentar la propia pila.
Compensación por el trabajo realizado en el sitio para agregar al ledger / blockchain.	Calculado automáticamente, depende de la comisión por operación.	Proporcionado arreglo para la minería de bloques.	Proporcionado arreglo para la minería de bloques.

El concepto del nodo de la red principal
Todos los nodos de red están descentralizados y ninguno de ellos tiene prioridad. Se requiere definir un nodo de red que procese la cola de transacciones almacenadas en diferentes nodos de red. Después de eso, debe ingresar un bloque de transacción recién generado en el libro mayor.
La plataforma CREDITS usa su propio protocolo combinado para aumentar la velocidad del procesamiento de transacciones, para proporcionar seguridad completa de almacenamiento de datos, procesamiento y transferencia de transacciones. El protocolo se basa en el cálculo de la función matemática de todas las transacciones contables, aplicando los

principios de Prueba de trabajo. Determina con precisión el almacenamiento de la última copia actualizada del libro mayor y el software en este nodo (Comprobante de capacidad), al calcular la suma de comprobación de los valores de todo el contenido: el código hash. El tamaño de los archivos también se determina como la prueba de que esta es la última copia actualizada y un código hash de la última transacción registrada en el sistema.
Para convertirse en el nodo principal de la red, el nodo busca el valor de la función hash que calcula en función del último libro almacenado. Organizamos un entorno competitivo saludable entre los nodos de red para tener la oportunidad de convertirnos en el nodo principal, generar y almacenar un nuevo libro mayor.
Después de calcular la función y obtener el resultado, se envía a todos los nodos de la red para su verificación. El resultado contiene una marca de tiempo del cálculo y un valor basado en el cálculo de la función de los archivos del libro mayor y el software. Todos los nodos reciben el valor calculado, comparan el tiempo de cálculo asignado para la búsqueda del servidor de red principal, lo verifican y confirman el factor de confianza del nodo, y también confirman su oportunidad de participar en la competencia: convertirse en el nodo principal de la red.
Después de recibir la aprobación de todos los nodos de la red, se forma la lista de nodos que calculó correctamente el valor de la función y contiene una marca de tiempo. El nodo que recibió el resultado correcto y lo aprobó en el tiempo más rápido, se convierte en el nodo de red principal del momento.
El concepto del algoritmo SHA2 se usa para calcular la suma hash del archivo.
Las funciones hash de la familia SHA2 se basan en la estructura MerkleDamgard.
El mensaje inicial después de la adición se divide en bloques, cada bloque se divide en 16 palabras.
El algoritmo pasa cada bloque de mensajes a través de un ciclo con 64 u 80 iteraciones (rondas). En cada iteración, se convierten 2 palabras, y el resto de las palabras definen la función de conversión. Los resultados de cada proceso de bloque se resumen. La suma es el valor de la función hash. Sin embargo, el estado interno se inicializa en función de los resultados del procesamiento de bloques anterior. Por lo tanto, es imposible procesar bloques de forma independiente y resumir los resultados.
Equipo de nodos de red
Nos esforzamos por crear una plataforma con las características de procesamiento de transacciones más rápidas posibles, por lo que proponemos utilizar un incentivo material para mantener los nodos de red en las mejores condiciones: equipos de servidor de alto rendimiento y ancho de banda de Internet elevado.
Como compensación material, el propietario del nodo de la red principal recibirá la remuneración en CREDITS de una serie de comisiones por transacciones de este libro procesado. El resto (½) está destinado al presupuesto general de desarrollo del proyecto para el soporte del usuario, las características actuales y el desarrollo de nuevos productos. El porcentaje puede cambiarse, así como separarse al sistema de formación de tasa a través de la votación federada por los nodos de la red, después de la oferta de moneda inicial durante al menos tres años.
Como resultado, alentamos a los propietarios de servidores a mantener este servidor en el hardware de mayor rendimiento y mantener un canal de comunicación de alta calidad y alta velocidad.

La creación de consenso

Como resultado, tenemos el nodo de red principal seleccionado por todos los nodos. Las principales tareas del nodo principal son: obtener transacciones en el estado del candidato para agregarlas al libro mayor desde todos los nodos, procesarlas, crear el último libro de contabilidad relevante y enviar un libro mayor recién creado a todos los nodos de la red. El proceso de manejo de transacciones y construcción del último libro de contabilidad relevante es precisamente la búsqueda de una solución de consenso. El resultado de la construcción del último libro de contabilidad relevante es la solución de consenso.
Todo el proceso se puede dividir en las siguientes etapas:
1. Busqueda del nodo principal de la red;
2. Construcción de nodos de confianza;
3. Recibir la lista de transacciones y crear una lista de candidatos para agregar a la libro mayor;
4. Procesamiento de la lista de candidatos, votación de nodos (nodos confiables y comunes tienen diferentes factores de peso (factor de confianza);
5. La eliminación de la lista de candidatos de transacciones no confirmadas que no han sido verificadas o que tienen una confirmación negativa;
6. Elaborar una lista de transacciones confirmadas para agregar al libro mayor;
7. Agregar transacciones al libro mayor con la marca de tiempo y el código hash del bloque que contenía la transacción;
8. Envío del bloque con transacciones a todos los nodos de red. Cuando se recibe, se agrega a los registros de todos los nodos.

Construyendo e Iniciando el libro mayor
Todo el proceso se puede describir en la siguiente secuencia:
1. El usuario final de la red en el sistema genera una transacción.
2. Cuando se cumplen todas las condiciones del contrato inteligente especificado en el mismo, el usuario inicia la acción (transacción) llamando al método requerido utilizando el software de la plataforma.
3. Para seguir los principios fundamentales de blockchain, el kernel de validadores realiza un seguimiento de la sincronización y la invariancia de la última versión del libro mayor.
4. Al momento de elaborar el consenso, todas las transacciones recibidas durante el ciclo se recopilan en el bloque.
5. Se asigna un número al bloque, que consiste en una marca de tiempo y un identificador de nodo convertido en un código hash, y luego el bloque se coloca en el módulo de consenso.
6. Después de la compilación de la lista blanca de candidatos, no solo se graba el hash de la transacción en el libro mayor, sino también el hash del bloque, para certificar siempre la fuente en función del mismo.
7. Este hash es un tipo de firma del bloque y el que creó este bloque con transacciones.
8. Después de crear consenso utilizando un algoritmo de búsqueda federativo, las transacciones agregadas al bloque se pasan al kernel del validador para escribirse en el libro mayor.

Transacciones no incluidas en el registro
Las transacciones no incluidas en la lista de transacciones preparadas se marcan como rechazadas. La información sobre esto se muestra inmediatamente en el emisor (iniciador) de la transacción.

Las transacciones no incluidas en el libro mayor permanecen en el conjunto de candidatos y se almacenan en los nodos de la red. Todas las nuevas transacciones recibidas por el servidor en el momento del consenso también llegan allí, y luego el proceso de búsqueda comienza de nuevo. Dicha operación cíclica continua de la red permite realizar transacciones durante un período de tiempo relativamente corto, manteniendo un alto grado de fiabilidad y relevancia de la información.

Transacciones

Una transacción es la unidad mínima del sistema que informa a la plataforma sobre la ejecución de métodos contractuales o transferencias directas entre cuentas sin crear un contrato inteligente, seguido de la colocación del resultado en la red peer-to-peer.

La creación de consenso

El sistema usa un modelo federado para construir un consenso - votación de nodos de validación de confianza, y también el algoritmo de creación de consenso - un algoritmo para el paso de un autómata de estado finito. El consenso funciona por ciclos (pasos de tiempo), por paso de tiempo, las transacciones se extraen y se colocan en un grupo (matriz unidimensional). Después de colocarse en el grupo, todas las transacciones se envían a nodos de confianza para recibir una respuesta. Si se recibe la respuesta, entonces la transacción para la cual se envió la solicitud para agregar puede agregarse al libro mayor de este validador. Después de eso, se envía al siguiente validador en la red. Cuando se genera consenso, al final de la cadena donde la legalidad de la transferencia se confirma por completo, la transacción se envía a validación con una marca para escribir y guardar en el libro mayor.

Procesamiento de transacciones

Para lograr la naturaleza descentralizada del sistema, cada servidor debe tener almacenamiento en el libro mayor y ser un manejador de todas las transacciones.

El sistema usa el concepto de núcleos del sistema. Por núcleos, nos referimos a un manejador de datos que realiza una tarea de producción específica, independientemente de la disponibilidad y operatividad de los componentes restantes del sistema. Cada kernel, en la entrada, en el momento en que se ejecuta la tarea, recibe una lista de variables para procesar. Y siempre obtiene un resultado en la salida - positivo, cualquier otro o un error. Como resultado, el kernel del sistema siempre contiene el código de respuesta, además del conjunto de datos principal. Esta estructura es necesaria para la mayor velocidad posible de cada proceso, que debe funcionar independientemente el uno del otro.

Estructura de entrada del libro mayor

Para lograr un rendimiento significativo del libro mayor, pero al mismo tiempo, sin comprometer la seguridad, proponemos utilizar una base de datos contable sin construir el árbol Merkle a partir del código hash del bloque anterior y el resultado de la transacción.

Árbol Merkle (*TTH - Tiger Tree Hashing*) es un tipo de función hash utilizada para verificar la integridad de los datos, obtener un identificador único de la cadena y restaurar la secuencia. Los datos se dividen en partes pequeñas: bloques que se procesan en hash individualmente utilizando *Leaf Tiger Hash*; a continuación, se calcula el Hash de tigre interno a partir de cada par de hashes onebyone.

Si el hash no tiene un par, entonces se transfiere a la nueva cadena sin cambios. A continuación, se calcula Hash de *Tiger* interno nuevamente en la cadena para cada par. Este procedimiento se repite hasta que queda un hash.

Cuando el ledger se opera con árboles Merkle, la velocidad de procesamiento de la transacción es muy baja y la carga en los recursos informáticos es muy alta. En nuestra opinión, este no es un uso racional del almacenamiento de datos.

Estructura de libro mayor CREDITS

Ofrecemos abandonar los árboles Merkle y usar el libro mayor de transacciones en el sistema CREDITS, con cada entrada que consiste en un código hash del bloque de transacción para agregar a la lista de candidatos además del libro mayor. Además, la entrada tiene el identificador de nodo y la marca de tiempo cuando se generó. La entrada del libro mayor contiene la dirección de la transacción, sus cuentas iniciales y finales, el tipo de cancelación, el número de cancelaciones de unidades, el tipo de depósito y el número de unidades de depósito. Este principio aumenta la velocidad del procesamiento de transacciones, aumenta la complejidad del cambio en el libro mayor ilegítimo y excluye posibles cambios en la entrada del libro mayor en retrospectiva.

Tamaño de bloque

La unidad de tiempo es el ciclo de búsqueda de los nodos principales y de confianza, y el tiempo del ciclo se calcula según la complejidad de la red. Por unidad de tiempo, la red contiene N transacciones generadas y transferidas para su procesamiento a la red desde el final del ciclo anterior, hasta el inicio del siguiente ciclo, para obtener el estado de "Candidato que se agregará al libro mayor". Las transacciones seleccionadas de la red N se colocan en el bloque. El tamaño del bloque depende de la cantidad de transacciones en él.

Buscar participantes en la transacción

La red peer-to-peer de CREDITS se puede representar como un gráfico, con cuentas de usuario en forma de vértices y una multitud de posibles transacciones en forma de bordes dirigidos que conectan dos vértices (cuenta). Como todos los bordes tienen un vértice inicial y uno terminal, siempre puede construir un gráfico orientado (orgraph).

Si tomamos las siguientes condiciones para la identificación:

● Cualquier transacción siempre tiene un emisor y un receptor;

● Cualquier vértice (cuenta) siempre se puede conectar a otro vértice con un borde dirigido (transacción);

● Cualquier vértice del gráfico (cuenta) tiene un número finito de bordes dirigidos (transacciones entrantes y salientes). En relación con lo anterior, podemos decir que la gráfica contiene la ruta requerida para cumplir con las condiciones de transacción necesarias y construir una cadena simple. Dado que es una secuencia finita de vértices, donde cada vértice (excepto el último) está conectado al siguiente vértice en la secuencia por un borde.

Canal de transmisión de datos

Cada canal de comunicación entre el nodo principal de la red y el nodo común de la red CREDITS es un hilo separado (multihebra), dentro del cual los datos se envían en forma encriptada cuando se ejecuta la transacción.

Para garantizar la seguridad de la red, todos los datos entre los nodos de validación se transmiten de forma encriptada, y cada conexión entre nodos es de bajo nivel en función de la biblioteca de red. Si la transferencia de datos ocurre con un error, el hilo debe interrumpirse automáticamente, la entrada correspondiente se coloca para escribir en el sistema de registro y luego en el archivo de registro. Los datos se transmiten a través de variables tipificadas.

Los datos transmitidos se cifran utilizando el algoritmo RC4 simétrico. Dado que este algoritmo funciona bajo una clave secreta común, esta clave se transfiere cuando se crea una conexión entre nodos y se transmite de forma encriptada de acuerdo con el algoritmo DiffieHellman.
El algoritmo RC4, como cualquier cifrado de flujo, está construido sobre la base de un generador de bits pseudoaleatorio. La clave se escribe en la entrada del generador, y los bits pseudoaleatorios se leen en la salida. La longitud de la clave puede ser de 40 a 2048 bits. Los bits generados tienen una distribución uniforme.
El algoritmo DiffieHellman permite que dos partes reciban una clave secreta común utilizando un canal sin protección de escucha, pero protegido del cambio del canal de comunicación. La clave recibida se puede usar para intercambiar mensajes usando encriptación simétrica. El algoritmo se basa en la complejidad de calcular logaritmos discretos. En él, como en muchos otros algoritmos con una clave pública,
los cálculos se realizan módulo a un cierto número primo grande P.
Primero, se selecciona un cierto número natural A, más pequeño que P, de una manera especial. Si queremos encriptar el valor X, entonces calculamos

$$Y = AX \bmod P.$$

Y es fácil calcular que Y tenga X. El problema inverso de calcular X a partir de Y es bastante complicado. El exponente X se llama exactamente el logaritmo discreto Y. Por lo tanto, conociendo la complejidad de calcular el logaritmo discreto, el número Y puede transmitirse públicamente en cualquier canal de comunicación, ya que con un gran módulo P, el valor inicial X será casi imposible de seleccionar. El algoritmo DiffieHellman para generar una clave se basa en este hecho matemático.
Cualquier acción en el sistema está relacionada con la marca de tiempo, el número del bloque anterior, el inicio de sesión del usuario y la identificación del contrato inteligente. Esto permite encontrar duplicados al ejecutar. Si se encuentra un duplicado, tomamos la primera transacción del grupo, el resto se considera ilegítimo.

Acción en el sistema
Una acción en el sistema es una transacción que caracteriza la transferencia más simple del valor de una cuenta a otra o la transferencia del resultado del método del contrato al validador, para la posterior búsqueda de una solución en el subsistema de búsqueda de consenso.
Para evitar la duplicación de la transacción en el mismo bloque con el mismo identificador, el sistema acepta un acuerdo de que la única transacción verdadera y correcta es la que vino primero al subsistema del validador para su procesamiento. Dado que ya está registrado en el sistema de validación que ya se ha realizado una transacción desde la cuenta actual y que no quedan valores en la cuenta para realizar la transacción, no se puede encontrar un consenso. Por lo tanto, se resuelve el problema del doble desperdicio.
Cuando se ejecuta la transacción, la información se recibe en el validador y se confirma, la información sobre el cambio de estado del libro mayor se distribuye automáticamente a todos los nodos de la lista de confianza, después de lo cual el libro mayor se sincroniza.
Para tener siempre un diario de transacciones actualizado entre todos los nodos de confianza para el nodo validador actual, es necesario sincronizar la transacción recién llegada en el libro mayor de todos los nodos cada vez. Para resolver este problema, se

debe usar un puerto separado para la sincronización (si existe tal oportunidad). Esta oportunidad aumentará la velocidad de procesamiento de la información entrante al núcleo del validador debido a la distribución de la carga en el puerto. El hilo de sincronización siempre se ejecuta, es cíclico. La prioridad para la asignación de carga de RAM y CPU (usando ciclos de CPU) es menor que la media. La memoria almacena las últimas 1,000 operaciones y el estado de las cuentas para ellas (de forma encriptada usando un algoritmo síncrono), esto aumenta la velocidad de respuesta a las solicitudes de otros nodos validadores.

Agregar una transacción para validación

La adición de transacciones al libro mayor solo se realiza desde el subsistema del validador inmediatamente después de crear consenso y compilar una lista blanca con el resultado del ahorro de transacciones en el libro mayor.

Llamar desde sistemas de terceros es imposible, para mejorar la seguridad.

Parámetros entrantes: el objeto que caracteriza la transacción. El valor resultante ResultValue <0 - la ejecución se cancela con un error, el valor resultante es un posible código de error / 0 <ResultValue - la función se ejecutó sin errores, el resultado es el número de la entrada en el libro mayor.

Parámetro entrante: el objeto que contiene la etiqueta única de la transacción, el remitente, el destinatario, el valor transferido, la correspondencia de valores, el valor deseado, la cantidad del valor transferido, la cantidad del valor deseado y otra información del sistema que puede cambiarse si es necesario.

Costo de las transacciones

El sistema usa la moneda CREDITS, que sirve:

- Como medio interno de pago para el uso del sistema;
- Para intercambiar diferentes monedas dentro del sistema;
- Intercambiar varios valores dentro del sistema;
- Para crear y procesar operaciones bajo contratos inteligentes;
- Para comprar información de terceros

fuentes de servicios dentro del sistema.

El costo de una transacción puede variar en función de la carga de la red, en un usuario particular del sistema, que teóricamente puede dirigir un gran flujo de transacciones en un determinado momento punta. Sugerimos usar el método material y el impacto en los usuarios del sistema para controlar la carga de la red.

El costo de realizar transacciones en los primeros tres años de la operación del sistema se establecerá individualmente para diferentes tipos de transacciones y operaciones. En el futuro, se desarrollará un algoritmo para la generación automática del costo de transacción.

4. Contratos inteligentes

Introducción

Un contrato inteligente en el sistema CREDITS es un algoritmo electrónico que describe un conjunto de condiciones mediante las cuales se pueden asociar acciones y eventos en el mundo real o sistemas digitales.

Para implementar contratos inteligentes autocontrolados, se requiere un entorno descentralizado que excluya por completo el factor humano, y para usar la transferencia del costo de un contrato inteligente, se requiere una criptomoneda independiente de la autoridad central.

Entidades

Un contrato inteligente en CREDITS consta de las siguientes entidades:
1. Propiedad (variables públicas): la entidad del sistema que almacena los datos públicos necesarios para el trabajo del contrato en el sistema CREDITS .
2. Método es la entidad del sistema de CREDITS responsable de observar la lógica y la secuencia de acciones al realizar la transacción (acciones bajo el contrato).
Los participantes en el sistema CREDITS firman los contratos inteligentes utilizando la llamada al método que modifica las propiedades del contrato, iniciando los procesos para verificar el cumplimiento de las condiciones y la coordinación.
Un contrato inteligente entra en vigor después de la firma de las partes. Para garantizar el cumplimiento automático de las obligaciones, se requiere un entorno de existencia que automatice por completo la ejecución de los términos del contrato.
Esto significa que los contratos inteligentes pueden existir solo dentro de un entorno que tenga acceso libre al código ejecutable a los artículos del contrato inteligente.
Todos los términos del contrato deben tener una descripción matemática y una lógica clara de ejecución. Por lo tanto, el principio principal de un contrato inteligente es la automatización completa y la fiabilidad de las relaciones contractuales entre las partes.

Método de contrato inteligente
El método de contrato inteligente CREDITS es la entidad del sistema responsable del cumplimiento de la lógica y la secuencia de acciones durante la transacción (acciones en virtud del contrato).
La lógica y la secuencia de acciones se describen mediante un código de programa (módulo) que contiene comandos, su ejecución secuencial permite obtener el resultado deseado. Este código puede manejar comandos de sistema (por ejemplo, el comando de asignación), comandos de usuario (funciones escritas por separado), propiedades de contrato (variables inicializadas de forma estática o dinámica disponibles a partir de cualquier método de contrato),
y métodos de cualquier otro contrato de terceros disponibles solo para el propietario del contrato conectado (tercero). Para una mayor divulgación, el desarrollo se proporciona en lenguajes de scripting (por ejemplo, JavaScript).
El método (código de programa) permite el uso de todos los operadores de lenguaje de scripting ampliamente utilizados (comandos) (asignación, saltos condicionales e incondicionales), la creación de funciones y procedimientos (subrutinas), la conexión de bibliotecas de terceros.
Máquina Ejecutable Virtual
El método de contrato del sistema CREDITS se ejecuta en el entorno virtual del sistema (Máquina virtual, en lo sucesivo, VM). Cuando se llama a un método para un contrato en particular, VM asigna un área de memoria y carga el bytecode del contrato que contiene los métodos y las variables inicializadas (o redefinido cuando llama a otros métodos de contrato). VM comienza a procesar el bytecode del método, en tiempo de ejecución, las variables y el código se cargan en su área de memoria, y los comandos se ejecutan sucesivamente, su resultado se transfiere a la red peer-to-peer para su posterior ubicación en el libro.
El iniciador del método de ejecución es el usuario del sistema, en nombre del cual se lanza este método.
Término de valor
La criptomoneda CREDITS también es un indicador del término de valor de una unidad contractual para comparar dos unidades completamente diferentes y generar un consenso

al ejecutar o aceptar el contrato por las partes. En lugar de registrar cada combinación separada de valor / puerta de enlace, la criptomoneda de CREDITS sirve como un grupo para efectuar transferencias de valores. Esto es posible porque cualquier valor es líquido con respecto a la moneda de CREDITS, lo que significa que cualquier valor puede ser líquido con respecto a cualquier otro valor.

Realización de los términos del contrato inteligente
El término del contrato en el sistema de CREDITS son los valores de los campos desencadenantes (marcados) necesarios para cerrar (completar) el contrato.
El cumplimiento de los términos del contrato inteligente es un procedimiento cuando los campos del disparador (deseado) se comprueban para un valor deseado equivalente. Hay tres formas posibles de encontrar una solución para cumplir con los términos del contrato:
1. El contrato se celebra entre dos o más partes para la transferencia de valor. En este caso, el cumplimiento del contrato es la provisión del costo equivalente del valor para la parte que realiza la transferencia desde la parte receptora.
2. El contrato se celebra entre las partes para la transferencia de valor, pero el pago debe realizarse al cumplir una cierta cantidad de condiciones (por ejemplo, la entrega de valor a la parte receptora).
3. Un contrato para la conversión de un valor a otro con un costo equivalente en forma de CREDITS se coloca en el sistema. En este caso, la plataforma comienza a buscar el camino más corto posible para intercambiar un valor por otro a través de la conversión en otros contratos. Se puede proporcionar cualquier cumplimiento del contrato por una transacción, o por varias transacciones, lo que brindará la oportunidad de cobrar la cantidad requerida de unidades de valor para completar el contrato.

Fuentes de datos
Para un trabajo correcto y completamente funcional, verificando y proporcionando información adicional, para hacer una solución más equilibrada y óptima, CREDITS utiliza proveedores de datos de terceros. La necesidad de introducir fuentes de datos adicionales en el sistema se debe a la insuficiencia de información pública sobre una o varias partes contratantes (por ejemplo, obtener el estado de crédito del prestatario para tomar la decisión de emitir un crédito).
Para trabajar con sistemas de información de terceros, la plataforma puede llamar a un bus de integración, que mediante acceso remoto genera una solicitud a un sistema de terceros (sitio) en un formato para la presentación de datos pagados para los participantes del sistema con pago en CREDITS.
La solicitud se envía en forma cifrada a los puertos y direcciones proporcionados por sistemas de información distintos de los estándar. El resultado de la solicitud puede ser cualquier respuesta al servicio que contiene la información necesaria para tomar una decisión, o un código de error que caracteriza la imposibilidad de recibir la respuesta requerida y los posibles pasos para eliminar el error.

5. Plan de implementación
Plan técnico de implementación del proyecto

	S1	S2	S3	S4	S5
	Pre-Alpha	Alpha	Beta	Lanzamiento candidato	Lanzamiento
Almacenamiento, Consenso mFA Consenso	FA: implementación, Diseño clave	mFA: implementación de diseño clave, PoW + PoC	Optmizacion mFA	–	Optimización
Almacén de datos	Ledger de descentralización, Implementación de la tienda NoSQL	Historial de MessagePack	Respaldo de cadena de bloques		–
CVM (máquina virtual de créditos)	Diseño y Implementación	Integración con ecosistema	Optimización	Revisión de errores	-
Sistema de terceros	-	Diseño e implementación	Integrar al sistema completo	-	Optimización
Máquina de inferencia	Especificación formal y elementos clave de diseño	Integración de Reasoner con cadena de bloques	Optimización de Reasoner	-	-
Interfaz de usuario	Implementación	Diseño web UX	-	-	-
Monedero	Especificación formal del monedero		Prueba de aplicación de diseño UX	Android, iOS, monederos de escritorio	
RPC & REST API	Especificación formal	Explorador de cadena	-	Explorador de terceros	

		de bloques			

CREDITS cryptocurrency
Después de emitir la versión de lanzamiento del sistema, una cantidad fija de 1,000,000,000 de CREDITS serán emitidos. Se cambiarán por tokens estándar ERC20, emitidas en la venta inicial del token. Ellos se intercambiarán a una tasa de cambio fija: 1 token estándar ERC20 = 1 unidades monetarias CREDITS.