

Fintelum

30 de julio de 2019

Fintelum

Oferta de Token Representativo

Implementación de (STO)

documento técnico¹

¹ Este documento técnico es un trabajo de investigación sobre un problema complejo y la solución que se propone, y no debe confundirse con los documentos técnicos típicos elaborados con el propósito de recaudar fondos mediante una oferta inicial de criptomoneda (ICO).

Contenido

Contenido	2
Glosario	3
Introducción	4
Crypto crowdfunding	5
Tipología de tokens	6
La descentralización como problema	7
Tokens, monedas y contratos inteligentes	8
Emisión y operación	9
Ley aplicable	11
Requerimientos legales	12
Características	14
Compatibilidad	16
Compatibilidad con estándares EIP (ERC)	17
Interoperabilidad e integraciones externas	19
Continuidad del negocio	21
Implementación técnica	22
Preguntas abiertas	23
Conclusión	24
Acerca de	25

Glosario

AML - (Anti-Money Laundering) Contra el Lavado de Activos, es un marco legal que impone obligaciones financieras y otras instituciones para evitar la legalización del producto ilegal.

Bitcoin - blockchain de código abierto y moneda gobernada por un sistema de consenso descentralizado con red criptográficamente segura.

Moneda - unidad de un activo en una cadena de bloques, generalmente conocida como un medio de transferencia de valor para la cadena de bloques subyacente.

Ethereum - plataforma basada en blockchain de código abierto que permite la ejecución de contratos inteligentes y transferibilidad de activos digitales basados en blockchain de Ethereum.

UE - Unión Europea.

ICO (Initial Coin Offering) - Oferta Inicial de Moneda: es una campaña de emisión primaria y distribución de tokens de uso.

KYC (Know Your Customer) - Conozca a su cliente: marco legal que requiere instituciones financieras y de otro tipo para recopilar información de identificación personal sobre sus clientes.

OTC - (Over-The-Counter) Sobre-El-Mostrador se refiere a las transacciones que tienen lugar fuera de las plataformas de intercambios centralizadas.

P2P - (Peer-to-Peer) Parte a Parte: se refiere a la ejecución comercial descentralizada basada en software y a la liquidación comercial en la cadena de bloques Ethereum, con proceso de cumplimiento centralizado de KYC / AML.

PEP - Persona Expuesta Políticamente: se refiere a alguien que tiene una función pública prominente así como a sus familiares y asociados cercanos.

Leyes de valores - un conjunto de reglamentaciones determinadas y de jurisdicción variable centradas en la emisión y transferencia de instrumentos financieros.

Token representativo - activo digital que representa un contrato de inversión (instrumento financiero) y está regulado por las leyes de valores de la jurisdicción respectiva.

Contrato inteligente - protocolo de transacción programable que ejecuta un conjunto de términos como funciones.

Solidity - lenguaje de programación diseñado para crear contratos inteligentes basado en el blockchain de Ethereum.

STO - la oferta de token representativo es una campaña de emisión y distribución primaria de tokens representativos de valor.

Token - unidad de un activo en una cadena de bloques con una funcionalidad de contrato inteligente definida.

Token de uso - activo digital destinado a un uso en una plataforma o red a cambio de un producto o servicio específico del emisor u otros usuarios.

Introducción

La implementación de la Oferta de Token Representativo de Fintelum es un código de Ethereum escrito en Solidity, construido como un protocolo estándar con características modulares que está diseñado para abordar las necesidades de un instrumento compatible para la industria de los mercados de capitales. En particular, para tener una herramienta basada en blockchain que represente un instrumento de valor transferible en una jurisdicción determinada.

Este documento describe la funcionalidad del código en términos de características, y explica la necesidad de dicha implementación según lo han definido las necesidades comerciales de Fintelum, en el marco de las las Leyes de la Unión Europea (UE).

El documento asume que los lectores tienen comprensión básica de cómo funcionan las criptomonedas y qué son las blockchains. También supone que el lector está familiarizado con el funcionamiento básico de los mercados de capitales. y específicamente los métodos de recaudación de fondos y comercio organizado.

Crypto crowdfunding

Desde 2013 hasta finales de 2018, la práctica de financiamiento colaborativo (crowdfunding) en combinación con criptomonedas nacientes permitió a emprendedores recaudar capital en forma de oferta inicial de monedas (ICO). Este crowdfunding basado en recompensas y donaciones fue, en la mayoría de los casos, una Oferta de Token de Ethereum a cambio de un pago en criptomoneda.

En términos legales, durante un recaudo de fondos mediante una ICO, el proyecto prevende un producto o servicio. Pero efectivamente realiza un financiamiento colaborativo, llevado a cabo utilizando el nuevo tipo de pago: las criptomonedas.

El token de uso resultante está destinado a ser intercambiable por los servicios o productos, y funciona como una unidad fungible y libremente transferible. Ocasionalmente, el token de uso puede volverse popular y comenzar a ser aceptado como un medio de pago fuera de la red prevista.²

² Sin embargo, esto es cierto para cualquier activo, p. ej., cigarrillos durante la Segunda Guerra Mundial, o fideos Ramen en prisión hoy. <https://bigthink.com/laurie-vazquez/how-ramen-noodles-beat-cigarettes-to-become-a-prison-currency>

Tipología de tokens

Las autoridades financieras se centran principalmente en la distinción y las implicaciones resultantes para dos tipos de tokens: tokens de uso y representativos. Varios reguladores también han distinguido el intercambio/pago y tipos de token híbridos.³

Un token de uso se define por la capacidad inherente de utilizar el token emitido como un servicio o producto canjeable. Por lo tanto, el emisor debe presentar cierta aplicación para el token adquirido, que el comprador podrá usar.

Un token representativo surgió como concepto en el año 2017. Más claridad y reglamentación fueron convocadas en torno a la exuberante práctica de cripto crowdfunding. Esto sucedió porque se consideró que algunos de los proyectos ICO ofrecían más que instrumentos de uso. En particular, la Comisión de Bolsa y Valores (SEC) de Estados Unidos había opinado que todas las ventas de tokens son ofertas de valores.⁴

Para los fines de este documento, continuaremos enfocándonos en el tipo de token representativos.

³ El regulador suizo FINMA fue uno de los primeros reguladores en emitir una guía de clasificación de tokens a principios de 2018 con los siguientes 4 tipos de tokens: pago, uso, activos y tokens híbridos. Malta hizo lo mismo con su Prueba Virtual de activos financieros, en la que todos los activos de DLT (Tecnología de Registro Distribuido) se dividen en una de 4 categorías: token virtual, activo financiero virtual, dinero electrónico o instrumento financiero. La Guía 2019 de la FCA del Reino Unido sobre Criptoactivos menciona 3 tipos: tokens de intercambio, tokens de seguridad y tokens de uso.

Ver más en: <https://www.finma.ch/en/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintecwh/egleitung-ico.pdf?la=en>

Aquí: https://www.mfsa.com.mt/pages/readfile.aspx?f=/files/LegislationRegulation/regulation/VF%20Framework/20180831_VFARFAQs_v1.00.pdf

Y aquí: <https://www.fca.org.uk/publication/consultation/cp19-03.pdf> 4 <https://www.sec.gov/news/speech/peirce-how-we-howey-050919>

⁴ <https://www.sec.gov/news/speech/peirce-how-we-howey-050919>

La descentralización como problema

Las criptomonedas se basan en principios de auto-gobierno sin-necesidad-de-confianza, apertura, y descentralización sin fronteras. Estas cualidades definen fundamentalmente las criptomonedas clásicas,

como bitcoin, litecoin y ether. Sin embargo, los mismos principios se convierten en un problema cuando se trata de hacer cumplir la ley.

Un token conforme a la ley puede existir en un sistema blockchain que posee los principios de

auto-gobierno sin-necesidad-de-confianza, apertura y descentralización sin fronteras. Pero, el contrato inteligente - token que representa un valor - no puede exhibir tales cualidades. De hecho, todo lo contrario por las razones que se describen a continuación.

Tokens, monedas y contratos inteligentes

Un token es una script (anotación) criptográfica. Se utiliza como la funcionalidad de la segunda capa, o contrato inteligente. Es diferente de la moneda blockchain subyacente. Una moneda, como bitcoin o ether, funciona

como la unidad monetaria inherente de la respectiva cadena de bloques dentro de la cual opera. Acciona la cadena, y la cadena está definida por la moneda y su programabilidad. Por ejemplo, Ethereum blockchain fue diseñada para permitir secuencias de comandos más completas. A diferencia de las secuencias de comandos del blockchain de Bitcoin, Ethereum fue construido como una plataforma de contrato inteligente Turing Complete.⁵

El término contrato inteligente define la programabilidad de la cadena subyacente y fue acuñado, mucho antes de que Bitcoin fuera inventado, por el científico informático Nick Szabo. Él describió un "contrato inteligente" como:

Un protocolo de transacción computarizado que ejecuta los términos de un contrato. Los objetivos generales diseñados del contrato inteligente son para satisfacer condiciones contractuales comunes (como condiciones de pago, gravámenes, confidencialidad y incluso la aplicación), minimizar las excepciones tanto maliciosas como accidentales, y minimizar la necesidad de intermediarios de confianza. Los objetivos económico relacionados incluyen, reducir la pérdida por fraude, los arbitrajes y los costos de ejecución, y otros costos de transacción.⁶

La cadena de bloques Ethereum permite reducir los costos administrativos y automatizar los términos de contrato según lo descrito por Nick Szabo. Pero, para efectos de emitir un token representativos de valor, algunos de los principios fundamentales de auto-gobierno sin-necesidad-de-confianza, apertura, y descentralización sin fronteras, deben reducirse a un conjunto de limitaciones funcionales que puedan ser programados en el contrato inteligente.

Hay otras cadenas de bloques viables construidas con Turing Completeness. Con el propósito de Implementación de STO Fintelum, sin embargo, la cadena de bloques Ethereum fue elegida como una plataforma de contrato inteligente a prueba de batalla, segura y fácilmente accesible.⁷

⁵ <https://github.com/ethereum/wiki/wiki/White-Paper#computation-and-turing-completeness%20y>

⁶ Véase Nick Szabo, Smart Contracts, 1994, <http://www.virtualschool.edu/mon/Economics/SmartContracts.html>

⁷ Vea más información cuantitativa sobre la cadena de bloques Ethereum aquí: <https://media.consensys.net/ethereum-by-the-numbers-3520f44565a9> y aquí <https://media.consensys.net/the-state-of-the-ethereum-network-949332cb6895>

Emisión y operación

El modelo comercial de Fintelum promueve la recaudación de fondos ordenada y conforme a la norma. La oferta en la venta del token debe constituir un Instrumento emitido a los participantes, basado en blockchain, que sea conforme a la ley. Además, El negocio de Fintelum requiere que el token representativo final se pueda intercambiar entre los participantes aprobados o incluidos en la lista blanca, tanto en bolsas de intercambio centralizadas como descentralizadas. Para lograr el arbitraje y la aplicación de la ley, Fintelum se mantiene como la contraparte centralizada para el cumplimiento de KYC / AML.

A continuación se describe la emisión y el funcionamiento del Token Representativo de Fintelum para

emisiones primarias y comercio secundario entre pares (P2P) a cambio de criptomonedas:

1. Se crea a nombre del emisor un contrato inteligente con cierto conjunto de características (ver más adelante, sección: Implementación de STO: características). El contrato inteligente contiene una lógica de transferencia de token, donde todas las demás comprobaciones de datos / transacciones son almacenadas en sus respectivos contratos inteligentes dedicados.
2. El contrato inteligente representa los términos del contrato de venta o accionista / acuerdo del propietario. También exige una lista blanca de los participantes antes de la inversión.
3. Cada participante de la recaudación de fondos primero pasa por una verificación de cumplimiento y luego se registra en una lista blanca, relacionada con el correspondiente contrato inteligente. Este paso es realizado por Fintelum.
4. Cuando se concluye la emisión, los tokens, que representan los términos del contrato, son publicado y distribuido a los respectivos participantes de la lista blanca. Los tokens son enviado a las direcciones indicadas de Ethereum, administradas por los participantes.
5. Después de la distribución del token, el emisor puede optar por incluir el token en el mostrador comercial P2P de Fintelum. Si enseguida de la emisión principal se enlista el token, no hay requisitos adicionales. Si se aplica el listado para usar otra implementación de STO, un intercambio de tokens puede ser necesario, y se requerirá una lista blanca entre otros criterios de acuerdo los requisitos enumerados por Fintelum.
6. Un titular de token listado puede colocar pedidos y ofertas en el mostrador comercial P2P.
7. Una contraparte puede aceptar pedidos / ofertas en cantidades totales o parciales.
8. Se supone que las partes han dado su consentimiento para ejecutar una transacción cuando ha ingresado el pedido / oferta y cuando el otro ha aceptado el pedido / oferta.

9. Ambas contrapartes reciben instrucciones para crear una transacción desde sus billeteras.
10. El remitente de los tokens recibe instrucciones sobre la dirección de custodia del contrato inteligente donde debe enviar los tokens y qué datos debe incluir. No incluye los datos que resultan de una transacción fallida.
11. El remitente de la criptomoneda basada en blockchain de Ethereum recibe instrucciones a qué dirección de depósito de contacto inteligente debe enviar los fondos. En caso de éter (ETH), el remitente también recibirá información sobre los datos que deben incluirse en la transacción para garantizar una ejecución válida de la transacción.
12. Las transacciones se verifican por contratos inteligentes de respuesta, con la inclusión en la lista blanca de ambas partes y los fondos quedan consignados en garantía en los contratos inteligentes de depósito.
13. El controlador del contrato de depósito en garantía inicia más transferencias de fondos o reembolsos, si es necesario.
14. La transacción y liquidación P2P se concluye y se registra en el blockchain de Ethereum.
15. Si alguna de las partes no cumple con las obligaciones de transferir fondos o tokens a la dirección de depósito en garantía en un período de tiempo determinado, se aplica una multa y se paga una compensación a la otra parte. Los fondos o tokens enviados al contrato de depósito en garantía se devuelven a la dirección de reembolso especificada por el remitente.

Ley aplicable

La emisión de un token representativo requiere el cumplimiento de las leyes de valores. Como regla de emisión y venta de valores al público en general (es decir, inversores no profesionales) requiere de un prospecto (documento de oferta) aprobado por la autoridad financiera, un proceso costoso que toma mucho tiempo.

La Unión Europea, en 2017 adoptó el nuevo Reglamento de Prospecto 2017/1129, que se aplica plenamente a partir del 21 de julio de 2019 y reemplaza el régimen actual de la Directiva sobre prospectos. Esta iniciativa de la Unión de los Mercados de Capitales de la UE tiene como objetivo eliminar el arbitraje regulatorio y garantizar protección de los inversores, y al mismo tiempo promueve un acceso más fácil al capital para las pequeñas y medianas empresas en Europa.

El Reglamento de Prospecto proporciona varias exenciones cuando libera a los emisores de tener que producir un prospecto a gran escala. Cada estado miembro de la UE puede establecer un límite nacional para Emisión libre de prospectos, dentro del rango de emisión de 1 millón de euros a 8 millones de euros anuales (sin embargo, puede haber otros requisitos nacionales de divulgación que aplican). El crowdfunding de capital como una emisión de valores de escala relativamente pequeña actualmente depende en esta exención.⁸

Otra iniciativa de la UE se encuentra actualmente en el proceso legislativo, a saber, el Reglamento de Crowdfunding que crearía un marco a nivel de la UE para crowdfunding por debajo del límite de 8 millones de euros. La adopción final y la entrada en vigor tomarán algunos años más. Hasta entonces crowdfunding se basa en la exención del Reglamento del Prospecto y las normas nacionales de cada estado miembro de la UE.⁹

⁸ Lea más sobre el Reglamento (UE) 2017/1129 del Parlamento Europeo y del Consejo de 14 de junio de 2017 sobre el prospecto que se publicará cuando los valores se ofrezcan al público o se admitan a negociación en un mercado regulado y la Directiva que lo deroga 2003/71 / CE: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R1129>

⁹ Lea más sobre la propuesta de Reglamento de Crowdfunding en Europa. Posición del Parlamento Europeo aprobada en primera lectura el 27 de marzo de 2019 con vistas a la adopción del Reglamento del Parlamento Europeo y del Consejo de Proveedores Europeos de Servicios de Crowdfunding (CECA) para Empresas: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0301_EN.pdf

Requerimientos legales

A la luz de la protección del inversor, un simple estándar de token de blockchain de Ethereum no es suficiente

para garantizar el alcance completo de los requisitos legales. Debe contener las garantías otorgadas por el emisor al inversionista hacia el cumplimiento de los términos del contrato. La ley requiere que los inversores estén protegidos en la medida en que el contrato / acuerdo estipule los derechos de los inversores a ciertos beneficios. Estos pueden ser:

- derechos de propiedad y obligación del emisor de proteger y restablecer el artículo perdido o robado (siguiendo una prueba de propiedad);
- derechos de voto y obligación del emisor de tener en cuenta el voto;
- derecho a la renta (dividendos, beneficios o participación en los ingresos) y obligación del emisor de pagar;
- derecho de herencia de propiedad y obligación del emisor de administrar;
- derecho a la información y obligación del emisor de proporcionar información verdadera y sin obstáculos;
- derechos de litigio;
- distribución de activos en caso de liquidación;
- otros derechos contractuales específicos que emanan de los términos del contrato.

Además de los derechos de los inversores, el emisor debe cumplir con conocer a su cliente (KYC) y tomar medidas contra el lavado de activos (AML). Estos se imponen sobre el inversor participante y puede incluir:

- identificación de los principales beneficiarios con métodos de identificación telemáticos o presenciales;
- verificar la información personal;
- identificar si los beneficiarios son personas políticamente expuestas (PEP) o incluidas en cualquier lista de sanciones públicas;
- garantizar la verificación de la fuente de riqueza y el capital invertido en moneda corriente (fiat) y criptomonedas

De los requisitos legales anteriores se deduce que la emisión del token que se considera representar un instrumento representativo no puede ser:

- libremente transferible;
- aceptar inversores no verificadas;
- aceptar fondos no verificados;
- libremente negociado en el mercado secundario;
- emitido anónimamente;
- falta de supervisión y control.

Por lo tanto, la transferibilidad descentralizada y la emisión no verificada deben reemplazarse por cumplimiento mandatorio de KYC / AML y características inherentes que permitan controles exógenos y estricto cumplimiento de la ley pertinente.

Cada jurisdicción puede requerir un conjunto de características diferentes. Por lo tanto, el estándar del STO Fintelum es modular y flexible en su implementación.

Fintelum es un proveedor de cumplimiento y tecnología para las entidades emisoras. El emisor del token,

por lo tanto, puede delegar los requisitos legales mencionados a una plataforma como Fintelum.

Características

El siguiente conjunto de características define la implementación de un STO Fintelum, según la definición de necesidades empresariales establecidas por Fintelum, dentro del marco reglamentario de la Unión Europea (UE), ver arriba.

Verificación

Capacidad para verificar de antemano que la transferencia de tokens de seguridad será exitosa. Si la transferencia no tuviera éxito, los datos que indican la razón de falla esperada serán devueltos.

Transferibilidad

El controlador de contrato puede forzosamente congelar y transferir tokens representativos, en caso de un evento de recuperación de activos o si se requiere una acción legal.

Modificaciones

Permite especificar datos que se procesarán en el momento de la transacción. Esta información luego se puede usar para realizar varias operaciones, dependiendo de la implementación del contrato inteligente.

Categorización

Subconjunto de activos de token que puede tener estado/metadatos especiales asociados con ellos, es decir, la clase de acciones, los derechos de los accionistas, las restricciones de transferencia.

Leyendo

Si un nodo Ethereum está escuchando eventos específicos de contratos inteligentes, puede leer actualizaciones relacionadas

Suscribirse

Soporte para suscribirse a actualizaciones relacionadas con la documentación, donde el suscriptor debe tener acceso al nodo Ethereum que está escuchando un evento específico del contrato inteligente.

Dividiendo

Posibilidad de dividir las existencias del propietario de un token representativo en varias billeteras.

Bloqueos

Permite que se impongan restricciones basadas en el tiempo (recuento de bloque) en el momento de la emisión o en cualquier caso de la ejecución de la transacción del token, p. ej., vender tokens o comprar tokens adicionales

Lista blanca

Las personas identificadas y sus respectivas billeteras Ethereum están vinculadas y registradas en la cadena de bloques en forma ofuscada. Soporte para restringir el rango de clases de activos entre jurisdicciones y propiedad de tokens y transferencia solo entre personas incluidas en la lista blanca.

Expiración KYC

Cumplimiento de la fecha de vencimiento de KYC mediante la suspensión de transacciones, p. ej., mediante metadatos que solicitan un código de error más específico.

Pagos por adelantado

Capacidad para distribuir a las billeteras de los propietarios de tokens otros tokens (por ejemplo, monedas estables) como dividendos.

Compatibilidad

Garantizar la compatibilidad con las Propuestas de Mejora de Ethereum (EIP), anteriormente el estándar de Solicitud de Comentarios de Ethereum (ERC)¹⁰, es importante para poder utilizar la plataforma de cadena de bloques Ethereum existente, bien establecida, segura y descentralizada. Ante todo, la implementación STO Fintelum garantiza las siguientes características de compatibilidad:

Transferibilidad

Capacidad para transferir activos entre cualquier dirección / billetera de Ethereum.

Asignación de terceros

Disponibilidad para agregar permiso para transferir cierta cantidad de tokens a Dirección / billetera de Ethereum no relacionados.

Transferencia de asignaciones

Capacidad para mover la asignación entre cualquier dirección / billetera Ethereum.

Consultas

Permiso para consultar direcciones / billeteras para saldo / asignación.

Disponibilidad de información del contrato

Proporcionar información básica de token, como el suministro, los decimales y el número total de Direcciones del titular.

¹⁰ A menudo hay confusión con respecto al uso de las designaciones EIP y ERC para los estándares Ethereum. Los Autores consideran que EIP es la designación más apropiada para los estándares Ethereum ya establecidos.

Compatibilidad con estándares EIP (ERC)

#1410

Este estándar describe la capacidad de ordenar activos en diferentes categorías y cantidades. Esto permite rastrear el saldo total y el saldo de cada categoría de activos, así como cualquier información arbitraria sobre cada grupo de tokens individuales.

Analogía: una baraja de cartas que se clasificarían en cuatro grupos, y el valor de cada grupo sería la cantidad de cartas de cada pila: 15 cartas con 7 espadas, 3 corazones, 2 tréboles y 3 diamantes. Esto se debe a que en un contrato de token estándar EIP-20, solo se puede reconocer que hay 15 cartas, pero no el grupo de cada carta. El estándar #1410 permite varias características importantes:

- (1) consulta los saldos por grupo de activos y que grupos de activos pertenecen a una dirección específica. A partir del ejemplo de analogía, podríamos preguntar cuántas espadas propias tiene una dirección o qué grupo son propiedad de la dirección;
- (2) permite transferencias de categorías de activos específicos;
- (3) agrega una capa de administración en la que los administradores de la categoría de activos pueden administrar categorías de activos según sus derechos. Por ejemplo, el gerente de la categoría de los activos de clubes no pueden realizar operaciones en activos de categoría de diamante. Los gerentes son determinado por cada titular individual de token;
- (4) agrega una capa de gestión de transferencia que impide la transferencia en caso de que la transferencia esté prohibida, dependiendo de la categoría de activos o metadatos asociados y devuelve datos sobre el motivo del error de transferencia.

Algunas de estas características fueron anuladas por los requisitos estándar EIP-1400 STO. Por ejemplo, dado que el estándar # 1400 debe cumplir con el token EIP-20, esto significa que debe integrarse un algoritmo que determinará qué categoría de activo es transferido, cuando se solicita la operación de transferencia sin especificar la categoría.

#1594

Este estándar define la funcionalidad requerida para emitir nuevos tokens y canjear fichas existentes. Proporciona la capacidad de verificar si la transferencia sería exitosa o fallaría por varias razones. El # 1594 define la transferencia que puede tener offchain datos que pasen a la llamada de función de transferencia que luego pueden ser verificados / procesados (ejemplo: las transferencias solo se pueden realizar si la firma de un tercero, que se pasa como datos con solicitud de transferencia, se pueden verificar). Entre las características, el estándar # 1594:

- (1) agrega la capacidad de verificar si la transferencia fallará / tendrá éxito y devolverá el estado de la razón del fracaso;
- (2) incluye la capacidad de realizar transferencias que tienen datos fuera de la cadena proporcionados como parte de solicitud de transferencia;
- (3) aplica métodos nativos de EIP-20, tales como: ver el suministro total; ver saldo de la dirección; agregar asignaciones; ver asignaciones; transferencia de asignaciones; hacer transferencia simple (no transferencia de datos sobre clases de activos);
- (4) admite la capacidad de emitir / canjear tokens, y proporciona estado si el token puede ser emitido o no.

#1644

El #1644 proporciona un interfaz estandarizado que se utiliza para verificar si el token puede ser gestionado unilateralmente por un controlador autorizado. También proporciona un interfaz para el controlador, si existe, para hacer las transferencias necesarias. Dado que los tokens representativos están sujetos a supervisión legal y regulatoria (los detalles de ¿qué? variarán según la jurisdicción, el marco regulatorio y el activo subyacente) en muchos casos el emisor (o una parte delegada por el emisor que actúa como controlador, p. ej., un regulador o agente de transferencia) deberá retener la capacidad de forzar tokens de transferencia entre direcciones. El estándar #1644:

- (1) permite al controlador forzar la transferencia / canjear tokens entre diferentes titulares de tokens;
- (2) agrega la capacidad de verificar si dicho controlador existe para el token de seguridad;
- (3) registra todas las acciones del controlador y garantiza que se puedan proporcionar datos fuera de la cadena con cada operación del controlador (para proporcionar razonamiento detrás de una acción específica).

#1643

El estándar #1643 agrega la capacidad de asociar documentos con contratos inteligentes y consultar sus estados y modificaciones. Ejemplos de documentación podrían incluir ofrecer documentos y leyendas asociadas con tokens representativos. Esto incluye las siguientes características:

- (1) agrega referencia a un documento publicado, especificando dónde está el documento ubicado (URL), su nombre y cifra de verificación (usando un algoritmo de hash seguro);
- (2) recupera la información del documento por nombre;
- (3) enumera todos los documentos;
- (4) elimina los documentos.

Este estándar de contrato inteligente no menciona como la gestión de Los derechos de documentos están controlados.

#1066

Este estándar define cómo un contrato inteligente devuelve códigos de estado para indicar solicitud de estado y / o razones de falla. De lo contrario, no proporciona ninguna característica distinta, ya que la idea ya está incorporada por los métodos de transferencia #1410 y #1594. En lo que respecta a las STOs, todavía hay una discusión en curso sobre los códigos de estado que serán utilizados.

Interoperabilidad e integraciones externas

Interoperabilidad con proveedores de servicios externos, como plataformas de intercambio o agentes de transferencia, es factible en la medida en que se cumpla con las normas KYC / AML del emisor. Dependiendo en la jurisdicción, cada emisión puede tener una configuración de token modular, que consiste en Las características anteriores en su totalidad o en parte. Sin embargo, la característica más destacada consiste en exigir

Cumplimiento KYC / AML y permitir controles exógenos para un cumplimiento estricto con la ley correspondiente.

La implementación actual de STO Fintelum puede integrarse con servicios externos. Hay dos escenarios básicos:

Como cliente de Fintelum

Una entidad, como un creador de mercado autorizado para una plataforma de intercambio que desee enumerar un proyecto que ha utilizado la implementación STO Fintelum, puede convertirse en propietario de una porción de los tokens. Los tokens adquiridos permitirán al creador de mercado hacer pedidos y ofertas en la plataforma de intercambio. Para obtener derechos de propiedad, el creador de mercado y todos los participantes involucrados en el comercio de tokens se registran como clientes de Fintelum y se someten al mismo procedimiento KYC / AML que todos los demás titulares de tokens. El cumplimiento los niveles pueden variar en los requisitos de un proyecto a otro.

Como operador independiente o agente de transferencia

Una entidad, como una plataforma de intercambio autorizada, puede necesitar convertirse en el único agente de transferencia de token y, por lo tanto, un operador independiente del título emitido. En este escenario, Fintelum cedería sus responsabilidades hacia el emisor como un agente externo de transferencia de tokens. El nuevo agente de transferencia debe garantizar la inclusión en la lista blanca de acuerdo con los requisitos de cumplimiento KYC / AML del token emitidos. Para migrar los derechos de la agencia de transferencia, Fintelum realizará el cambio del controlador u operador cotidiano en el blockchain. El nuevo agente de transferencia proporcionará su propio conjunto de direcciones de transacciones. Fintelum eliminará todos los derechos y responsabilidades de operar los contratos inteligentes y los servicios de custodia relacionados. Tal transacción garantiza la elección de un nuevo operador diario o agente de transferencia de tokens.

Continuidad del negocio

Un token de seguridad es una representación criptográfica de un acuerdo. Es la segunda capa representativa para facilitar la gestión de un acuerdo / contrato legal entre dos o más partes. El token en sí no debe considerarse un objeto del acuerdo, sino un mera representación de los términos allí establecidos. La implementación de STO Fintelum se basa en la cadena de bloques Ethereum debido a la seguridad y robustez de esta Plataforma de secuencias de comandos Turing completa.

Si la cadena de bloques Ethereum falla por cualquier motivo, el token se puede replicar en otras cadenas de bloques, siguiendo los mismos requisitos comerciales y legales, y de conformidad con la decisión del emisor. Por lo tanto, la implementación de STO Fintelum se puede considerar independiente de la cadena, en la medida en que se cumplen los requisitos legales relativos y las necesidades comerciales de Fintelum.

Implementación técnica

La implementación de Fintelum STO se conforma de varios componentes:



1. Módulo principal de transferencia de STO: este es el componente central que une todas las otras partes. Recibe solicitudes de dos módulos subordinados y analiza estas solicitudes para una función específica. Todas las solicitudes pasan a través de este módulo principal.
2. STO Módulo de datos: este es el lugar donde todos los datos se almacenan, datos como los saldos.
3. STO Administrador de verificación de transacciones - este módulo analiza la solicitud en la que se realizan comprobaciones específicas requeridas para una transacción. También se puede usar para eliminar y agregar controles adicionales, según sea necesario.
4. Verificación de transacciones de módulos individuales: estos módulos subordinados realizan funciones específicas como se describe en el capítulo llamado "Características" de este documento. Cada una de estas funciones son intercambiable y flexible para ser agregado o eliminado, según sea necesario.

El código base se publicará y mantendrá en el repositorio de Git: <https://github.com/Fintelum/STO>

Preguntas abiertas

Los mercados de capital establecidos están gobernados centralmente, donde solo inversores participantes profesionales, calificados, del mercado tienen amplio acceso a plataformas de intercambio reguladas. Los Bancos y los corredores de valores aseguran el cumplimiento de KYC / AML, y las transacciones se realizan con moneda legal corriente o fiduciarias.

En el contexto de la estructura actual de los mercados de capitales, algunas de las preguntas abiertas se refieren a la aplicabilidad de la implementación de STO Fintelum. ¿Existe una demanda para valores del mercado de capitales ser representados por tokens criptográficos? ¿Hay una necesidad de inversores no profesionales para acceder a los mercados de capitales para la emisión de valores primarios y comercio secundarios?

Esto se puede demostrar con un caso de negocios exitoso que no entra en conflicto con la ley aplicable. Una empresa debe poder realizar una emisión ordenada de títulos valores y su comercialización secundaria como un servicio profesional. La rendición de cuentas puede garantizarse con divulgaciones y transparencia voluntaria.

Conclusión

En este documento, hemos abordado la descripción técnica de la implementación de un STO Fintelum, y también se revelaron como un protocolo estándar las necesidades comerciales que requiere un STO Fintelum. Hemos examinado un conjunto de características modulares que pueden constituir dicho token representativo y se propuso una determinada base de protocolo para un instrumento basado en el blockchain de Ethereum en cumplimiento de la norma, utilizable en la industria de los mercados de capitales. También hemos abordado la interoperabilidad y posibles integraciones externas que los participantes de la industria deben tener en cuenta. Además, hemos obtenido la implementación técnica y hemos proporcionado un enlace para la base completa del código fuente.

Con este documento, en Fintelum esperamos haber logrado contribuir al avance de la industria de la tokenización en general. Somos conscientes de que nuestra propuesta de implementación es una de varias posibilidades, y anticipamos que habrá otras.

Sin embargo, es notable demostrar nuestra comprensión de los requisitos del proceso y su legalidad al sugerir la implementación de token representativos.

Si nuestras presunciones son correctas, esta implementación estándar puede servir como punto de referencia para la industria en general.

Acerca de

Fintelum es una empresa de desarrollo de TI, autorizada por la Unidad de Inteligencia Financiera de Estonia (UIF) para proporcionar billetera de custodia de criptomonedas y servicios de intercambio de activos digitales, en conformidad con las leyes AML de la UE. El producto principal de Fintelum es una plataforma de lanzamiento de tokens, especializada en emisión de token representativos (STO) y emisión de moneda inicial (ICO), emisión primaria y comercio secundario P2P, con énfasis en cumplimiento de conozca a su cliente (KYC) y medidas contra el lavado de activos (AML), tecnología y servicios de asesoramiento.

Para más información, visite <https://fintelum.com>

Puedes seguir a la empresa en [Twitter](#), [Telegram](#), [LinkedIn](#) y en [Facebook](#).