Universidad de Valladolid

Facultad de Ciencias Económicas y Empresariales

Trabajo de Fin de Grado

Grado en Finanzas, Banca y Seguros

Tecnología de bloques aplicada al mercado de valores

Presentado por:

David Sanz de León

Tutelado por:

Félix J. López Iturriaga

Valladolid, 28 de Julio de 2022

RESUMEN

Tras la aparición de Bitcoin en 2008 y otras criptomonedas, en los últimos años han surgido las denominadas ICO[1], que se basan en la tecnología DLT[2] que sustenta la mayoría de las criptomonedas, para respaldar la emisión de otros tipos de instrumentos. Principalmente consiste en la emisión de tokens de utilidad[3] en un entorno no regulado. Más recientemente, hemos visto surgir un nuevo tipo de token en forma de tokens de valores[4] (o de inversión) que esencialmente, y una serie de los reguladores han comenzado a confirmar que deben ser equivalentes a los valores, es decir, equivalentes a los valores tradicionales pero que se emiten, mantienen y transfieren en una infraestructura DLT. Una de las características más importantes de los tokens de valores es, a diferencia de los tokens de utilidad, que se debe considerar que se les aplican las leyes y prácticas de valores existentes y, entre otras cosas, todos los requisitos reglamentarios KYC y AML. Estas regulaciones existen para controlar quién posee el título y quién lo transfiere para detectar y prevenir el lavado de dinero, la financiación del terrorismo y otras actividades ilegales o fraudulentas.

Palabras clave: tecnología de bloques, mercado de valores, criptomonedas, CBDC.
Clasificación JEL: G12, G15, G18.

---

1 **ICO**: *Initial Coin Offering*, Oferta Inicial de Moneda: Se trata de una forma de búsqueda de financiación para una iniciativa o proyecto, mediante la emisión de una moneda basada en la tecnología blockchain, es decir, una criptomoneda.

2 **DLT**: *Distributed Ledger Technology* o Tecnología de Contabilidad Distribuida es un sistema electrónico o base de datos para registrar información que no es ejecutada por una sola entidad. Esta nos permiten almacenar y usar datos que pueden ser descentralizados (almacenados en varios lugares) y distribuidos (conectados y, por lo tanto, pueden comunicarse) tanto de forma privada o pública.

3 **Tokens de utilidad** (*Utility tokens*): son una representación en la cadena de bloques de un derecho específico sobre bienes o servicios que el emisor del token ha creado o está en proceso de crear. Generalmente restringiremos el uso del término "ICO" para referirnos a la emisión de tokens de utilidad.

4 **Tokens de valores** (*Security tokens*) o, más genérico, tokens de inversión): son activos que representan una expectativa de (y un derecho sobre) flujos de efectivo futuros (que no sean un simple aumento en el precio de mercado) resultantes de la actividad del emisor. Pueden ser considerados como valores "tradicionales" y representan, por ejemplo, deudas/préstamos, acciones o fondos de inversión (pueden también representan valores tales como terrenos, inmuebles, aeronaves, etc.). Generalmente usaremos el término "STO" (*Security Token Offering*, IPO tokenizada) para referirse a la emisión de tokens de valores.

ÍNDICE

1. INTRODUCCIÓN

En este trabajo vamos a ver como implementar la tecnología de la cadena de bloques al mercado de valores prestando especial interés en la regulación.

El mercado de valores y la tecnología de cadena de bloques a priori son muy diferentes. La filosofía de las criptomonedas contradice la legislación relativa al mercado de valores respecto a temas como el anonimato o la libre transferencia. A lo largo de este trabajo vamos a ver cómo con las propias herramientas de la blockchain de Ethereum podemos realizar cambios para cumplir la legislación. De este modo podemos incorporar los beneficios de la tecnología blockchain, especialmente la solidez de un sistema distribuido, el registro inalterable de transacciones y la seguridad de la criptografía asimétrica al mercado de valores.

Para realizar este estudio se ha revisado la legislación de la CNMV, la ESMA y la SEC. También se han analizado papers que explican como funcionan las diferentes herramientas de la cadena de bloques.

En este trabajo primero explicaremos como funciona la tecnología de bloques después analizaremos el marco regulatorio aplicado a los valores tradicionales. Seguidamente implementaremos esta regulación a la tecnología de bloques especialmente a las monedas digitales, acciones, bonos y otros instrumentos derivados. Finalmente veremos como establecer un mercado secundario para los valores en la tecnología de bloques.

2. TECNOLOGÍA *BLOCKCHAIN*

2.1. Fundamentos de las criptomonedas, cadenas de bloques y billeteras

Para realizar este estudio hemos utilizado una versión modificada de la red Ethereum. Ethereum es una tecnología para crear aplicaciones y organizaciones, mantener activos, realizar transacciones y comunicarse sin estar controlado por una autoridad central. No es necesaria la entrega de todos los datos personales para usar Ethereum: cada usuario mantiene el control de sus propios datos y de lo que se comparte. Ethereum tiene su propia criptomoneda, Ether, que se utiliza para pagar ciertas actividades en la red Ethereum. (Ethereum Foundation, n.d.-c)

La criptomoneda es una nueva forma de dinero digital impulsada por la criptografía. Todo comenzó en 2008 con Bitcoin desarrollado por Satoshi Nakamoto (Nakamoto, 2008). Las criptomonedas inicialmente se usan para enviar dinero a cualquier persona en cualquier lugar del mundo. La diferencia principal entre las criptomonedas y las transferencias bancarias normales u otros servicios

financieros como Paypal es que no existen intermediarios (autoridad central como un banco o gobierno que interviene en una transacción entre el remitente y el destinatario). Estos intermediarios tienen el poder de vigilar, censurar o revertir transacciones y pueden compartir los datos confidenciales que recopilan sobre los usuarios con terceros. También suelen dictar a qué servicios financieros tiene acceso los usuarios.

Las cosas son diferentes con las criptomonedas. Las transacciones conectan directamente al remitente y al destinatario (peer to peer, P2P) sin tener que tratar con ninguna autoridad central. Ninguna autoridad tiene acceso a los fondos de los usuarios ni pueden decidir qué servicios pueden utilizar. Esto es posible gracias a la tecnología blockchain sobre la que operan las criptomonedas. (Ethereum Foundation, n.d.-c)

Las criptomonedas están basadas en la tecnología de la cadena de bloques (*blockchain*). Una cadena de bloques es una base de datos de transacciones que se actualiza y comparte entre un gran número de ordenadores en una red. Cada vez que se agrega un nuevo conjunto de transacciones, se denomina “bloque”, de ahí el nombre de cadena de bloques. La mayoría de las cadenas de bloques son públicas y solo se puede agregar datos, no eliminarlos es decir son inmutables, se puede entender como un registro inalterable de datos. Si alguien quisiera alterar la información o engañar al sistema, tendría que tomar el control del 51% de los ordenadores de la red (ataque del 51% o de doble gasto). Esto hace que las cadenas de bloques sean altamente seguras.

Las cadenas de bloques utilizan técnicas criptográficas para garantizar la seguridad de los fondos. Se utilizan técnicas similares en la industria bancaria para garantizar la seguridad de las transacciones monetarias. Podemos decir que las criptomonedas tienen un nivel de seguridad bancario. (Ethereum Foundation, n.d.-c)

Los usuarios interactúan con la cadena de bloques de Ethereum por medio de las billeteras. Podemos considera la billetera como una aplicación de banca por Internet pero sin el banco. La billetera permite interactuar con la cuenta Ethereum p.e. leer el saldo, enviar transacciones y conectarse a aplicaciones. (Ethereum Foundation, n.d.-a)

La billetera es solo una herramienta para administrar una cuenta Ethereum. Eso significa que se puede cambiar de proveedor de billetera en cualquier momento. Muchas billeteras también permiten administrar varias cuentas de Ethereum desde una sola aplicación. Las billeteras no custodian los fondos. Son solo una herramienta para interactuar con la red de Ethereum.

Podemos hacer un paralelismo con las cuentas bancarias para entender como funcionan las billeteras. La billetera está formada por una dirección[1] y una clave privada (criptografía asimétrica de clave pública y clave privada). La dirección sería el equivalente al número de cuenta bancario para la transferencia de fondos y la forma de identificarse en la cadena de bloques. La clave privada sería el PIN para acceder en una aplicación bancaria. Los fondos no se almacenan en la billetera sino en la cadena de bloques y para poder interactuar con esos fondos los usuarios se identifican con la dirección y la clave privada por medio de una billetera. Para enviar fondos a otro usuario solo es necesario saber la dirección del usuario.

En resumen:

- Una cuenta de Ethereum es una entidad que puede enviar transacciones y tiene un saldo.
- Una cuenta de Ethereum tiene una dirección de Ethereum, como una bandeja de entrada tiene una dirección de correo electrónico asociada. Puede usarse para enviar fondos a una cuenta o como identificación.
- Una billetera es un producto que permite administrar una cuenta Ethereum. Permite ver el saldo de su cuenta, enviar transacciones y otras funciones.

2.2. ¿Qué son los *smart contract* o contratos inteligentes?

Los contratos inteligentes son los componentes básicos de las aplicaciones de Ethereum. Son programas informáticos almacenados en la cadena de bloques que nos permiten convertir los contratos tradicionales en análogos digitales. Los contratos inteligentes tienen una estructura condicional lógica: si se cumple la condición, entonces se realiza una acción. Esto significa que se comportan exactamente como se programaron y no se pueden cambiar.

Nick Szabo acuñó el término “contrato inteligente”. En 1994, escribió una introducción al concepto (Szabo, 1994) y, en 1996, una exploración de lo que podrían hacer los contratos inteligentes (Szabo, 1996).

Nick Szabo imaginó un mercado digital basado en estos procesos automáticos y criptográficamente seguros. Un lugar donde las transacciones y las funciones comerciales pueden realizarse sin confianza, sin intermediarios. Los contratos inteligentes en Ethereum ponen en práctica esta visión.

---

1 En este documento vamos a utilizar la palabra billetera y dirección de forma equivalente ya que aunque no son lo mismo, en la practica son una representación de la identidad de un usuario.

Para la mayoría de las personas, los contratos traen a la mente acuerdos de términos y condiciones innecesariamente largos o documentos legales aburridos.

Los contratos son solo acuerdos. Es decir, cualquier forma de acuerdo puede encapsularse dentro de las condiciones de un contrato. Los acuerdos verbales o los contratos en papel y lápiz son aceptables desde un punto de vista social y legal, pero no están exentos de fallos. Uno de los mayores problemas con un contrato tradicional es la necesidad de que las partes cumplan con los resultados del contrato.

Podemos ver los fallos en los contratos con un ejemplo. Alicia le apuesta a Pedro 10€ a que le ganará una carrera en bici. Pedro confía en que será el ganador y acepta la apuesta. Al final, Alicia termina la carrera muy por delante de Pedro y es la clara ganadora. Pero Pedro se niega a pagar la apuesta, alegando que Alicia debe haber hecho trampa.

Este ejemplo sencillo ilustra el problema de los contratos tradicionales. Incluso si se cumplen las condiciones del acuerdo (en este caso, Alicia es la ganadora de la carrera), aún hay que confiar en que la otra persona cumpla el acuerdo (es decir, el pago de la apuesta).

Aunque las partes incumplan el contrato existe la ley de responsabilidad contractual que obliga a las partes a cumplir el contrato. Esta ley del derecho civil protege a las partes del contrato pero en la práctica es poco efectiva, bien porque las costas procesales hacen que no compense reclamar el importe del contrato o, porque los plazos procesales se extienden en el tiempo y cuando se cumple de forma forzosa el contrato resulta irrelevante p.e. cuando finalmente se paga una deuda a la empresa esta ya se encuentra en concurso de acreedores.

Los contratos inteligentes digitalizan los acuerdos al convertir los términos de un acuerdo en un código de ordenador que se ejecuta automáticamente cuando se cumplen los términos del contrato.

Una metáfora simple para un contrato inteligente es una máquina expendedora, que funciona de manera similar a un contrato inteligente: las entradas específicas garantizan salidas predeterminadas:

- Seleccionas un producto
- La máquina expendedora devuelve el importe necesario para adquirir el producto
- Introduces la cantidad correcta

- La máquina expendedora verifica que hayas introducido la cantidad correcta
- La máquina expendedora dispensa el producto elegido.
- La máquina expendedora solo dispensará el producto deseado una vez que se hayan cumplido todos los requisitos. Si no seleccionas un producto o no insertas suficiente dinero, la máquina expendedora no entregará el producto.

Algunas de las mejoras que incorporan los contratos inteligentes son:

a.) Ejecución automática: Uno de los beneficios más significativos que tienen los contratos inteligentes sobre los contratos tradicionales es que el resultado se ejecuta automáticamente cuando se cumplen las condiciones del contrato. No es necesario esperar a que un persona ejecute el resultado. En otras palabras: los contratos inteligentes eliminan la necesidad de confianza.

Por ejemplo, podemos escribir un contrato inteligente que retenga fondos en depósito de inversión para un niño, permitiéndoles retirar fondos después de una fecha específica. Si intentan retirar los fondos antes de la fecha especificada, el contrato inteligente no se ejecutará. O bien, un contrato que automáticamente proporciona una versión digital de la titularidad de un automóvil cuando se paga el importe del automóvil al concesionario.

b.) Resultados predecibles: El factor humano es uno de los mayores puntos donde fallan los contratos tradicionales. Por ejemplo, dos jueces individuales pueden interpretar un contrato tradicional de diferentes maneras. Sus interpretaciones podrían llevar a que se tomen decisiones diferentes y a resultados dispares. Los contratos inteligentes eliminan la posibilidad de diferentes interpretaciones. Los contratos inteligentes se ejecutan con precisión en función de las condiciones escritas en el código del contrato. Esta precisión significa que dadas las mismas circunstancias, el contrato inteligente producirá el mismo resultado.

c.) Registro Público: Los contratos inteligentes también son útiles para auditorías y seguimiento. Dado que los contratos inteligentes de Ethereum están en una cadena de bloques pública, cualquiera puede rastrear instantáneamente las transferencias de activos y otra información relacionada. Se puede verificar por ejemplo si una persona realizó una transferencia de dinero.

d.) Protección de la privacidad: Los contratos inteligentes también pueden proteger la privacidad. Dado que Ethereum es una red seudanónima (las transacciones están vinculadas públicamente a una dirección criptográfica única, no a su identidad).

e.) Términos visibles: Al igual que los contratos tradicionales, se puede verificar qué hay en un contrato inteligente antes de firmarlo (o interactuar con él). Gracias a la transparencia pública de los términos del contrato cualquiera puede examinarlo.

3. MARCO REGULATORIO

Hay varias formulaciones que revelan el concepto de “valores”. Cada uno se centra en alguna característica clave de los “valores”:

- Un valor es un documento, que posee un valor legal, a menudo en relación con las finanzas o con cualquier propiedad.
- Un valor es un tipo de activo básico en forma de una de las formas de capital. Se puede cambiar por bienes en lugar de dinero y usarse en el mercado, obteniendo ganancias.
- Un valor es un documento que confirma los derechos del titular.

La comodidad de los valores radica en su universalidad. Por ejemplo, si se utiliza un valor en forma de un determinado capital o producto, entonces la presencia física de este producto simplemente no es necesaria. Se puede comprar o vender simplemente usando el “valor” como su sustituto directo. Por lo tanto, el valor en sí, es una mercancía. Además, los valores pueden usarse como una demostración de la evidencia de inversión en una empresa.

En varios países existen leyes especiales, que controlan todos los aspectos del manejo de los valores, desde su emisión hasta todas las transacciones en el mercado que se producen con ellos.” (FIBO Group, n.d.)

Tipos de valores:

a.) Acciones: “Valor mobiliario que representa una parte proporcional del capital social de una sociedad anónima. Los tenedores de acciones son por tanto socios propietarios de la sociedad, en proporción a su participación. Las acciones pueden estar representadas por títulos físicos o por anotaciones en cuenta; la representación por anotaciones en cuenta es obligatoria si la sociedad está admitida a cotización en Bolsas de valores.” (CNMV, n.d.)

b.) Valores representativos de deuda:

- Bonos: Valores de renta fija que pueden ofrecer un tipo de interés fijo que se abona mediante cupones periódicos. La rentabilidad para el inversor viene determinada por la diferencia entre el precio de adquisición y el precio de reembolso mas los cupones si los hubiese. Es habitual que se emitan al descuento. (CNMV, n.d.-a)
- Dinero fiat[2]: bono cupón cero perpetuo al portador emitido por el estado o una entidad autorizada que se compra y vende a la par (valor nominal). La rentabilidad para el propietario proviene del efecto de la inflación[3].
- Obligaciones: Valor mobiliario que representa una parte proporcional de un empréstito. La sociedad emisora se compromete a retribuir a los tenedores de los valores (obligacionistas) con un interés que puede ser fijo o variable, y a devolver el capital aportado, en la fecha establecida para el vencimiento de los títulos. (CNMV, n.d.-a)

c.) Productos derivados: "instrumentos financieros cuyo valor deriva de la evolución de los precios de otro activo, denominado "activo subyacente"." (CNMV, n.d.-b)

Para la aparición de valores, es necesario llevar a cabo una emisión, es decir, emisión y distribución. El emisor en este caso es una empresa que, por ejemplo, se beneficia al atraer nuevos fondos. El estado a menudo se convierte en el emisor, deseando alcanzar objetivos similares. Además, la emisión de valores puede ser una entidad jurídica o un individuo, así como algunas autoridades.

La regulación mas importante trata sobre los temas relativos a la identidad de los inversores.

3.1. Know your client (KYC)

Conozca a su cliente (KYC) es un estándar en la industria de inversión que

2 Sería mas correcto usar la definición moneda de curso legal (forma de pago decretada por un estado sin valor intrínseco que si un deudor la ofrece como pago de deuda, la deuda se extingue legalmente. Aunque el acreedor no esta obligado a aceptar la moneda de curso legal, el acto de ofrecer la moneda de curso legal es suficiente para saldar la deuda) pero este estudio no se centra en el dinero como forma legal de cancelar deudas sino en el dinero como valor financiero y por tanto la definición de dinero fiat (forma de pago decretada por un estado que no esta respaldada por ninguna mercancía) es suficiente.

3 Cuando hacemos referencia a la inflación como rentabilidad el signo es inverso, una inflación de +2% equivale a una rentabilidad de -2%.

garantiza el conocimiento de información detallada sobre la tolerancia al riesgo de los clientes: es el grado de variabilidad en los rendimientos de inversión que un inversor está dispuesto a soportar en su planificación financiera: conocimiento de inversión y posición financiera.

La regulación KYC protege tanto a los clientes como a los asesores de inversiones: los clientes están protegidos al informar a sus asesores de inversiones qué inversiones se adaptan mejor a sus situaciones personales; mientras que los asesores de inversión están protegidos sabiendo lo que pueden y no pueden incluir en la cartera de sus clientes. El cumplimiento generalmente involucra requisitos y políticas como gestión de riesgos, políticas de aceptación de clientes y monitoreo de transacciones.

La regla *Know Your Client* (KYC) es un requisito ético para aquellos en la industria de valores que tratan con clientes durante la apertura y el mantenimiento de cuentas. Hay dos reglas que se implementaron en julio de 2012 que cubren este tema: Autoridad Reguladora de la Industria Financiera (FINRA) Regla 2090 (Know Your Customer) y Regla FINRA 2111 (Suitability):

- Conozca a su cliente Regla 2090: cada corredor de bolsa debe hacer un esfuerzo razonable al abrir y mantener cuentas de clientes. Todos los datos y hechos esenciales deben registrarse y si alguna autoridad actúa en nombre del cliente, deben identificarse.
- Reglas de prácticas justas de FINRA, 2111: un corredor de bolsa debe tener motivos razonables al recomendar lo que es adecuado para un cliente en función de la situación financiera y las necesidades del cliente. Esta responsabilidad significa que el corredor de bolsa ha realizado una revisión completa de los hechos actuales del cliente e, incluso, de otros valores antes de realizar cualquier compra, venta o intercambio de valores.

La Red de Ejecución de Delitos Financieros de EE. UU. (FinCEN) ha establecido requisitos básicos para KYC junto con los requisitos básicos para el programa de diligencia debida. Para prevenir el lavado de dinero, las instituciones financieras deben realizar evaluaciones más profundas de los perfiles de riesgo de sus clientes.

Los asesores de inversión y las empresas son responsables de conocer la situación financiera de cada cliente al explorar y recopilar la edad del cliente, otras inversiones, estado fiscal, necesidades financieras, experiencia de inversión, horizonte temporal de inversión, necesidades de liquidez y tolerancia al riesgo. A este respecto, la SEC requiere que un nuevo cliente proporcione

información financiera detallada que incluya nombre, fecha de nacimiento, dirección, situación laboral, ingreso anual, valor neto, objetivos de inversión y números de identificación, antes de abrir una cuenta.

Aunque las criptomonedas tienen la ventaja de ser descentralizadas y un medio de intercambio que promueve la confidencialidad, estos beneficios también presentan desafíos en la prevención del lavado de dinero. Los delincuentes ven las criptomonedas como un medio para promover sus actividades ilegales y como un vehículo para lavar dinero; como resultado, los órganos rectores están buscando formas de imponer KYC en los mercados de criptomonedas, requiriendo plataformas de criptomonedas para sus clientes al igual que las instituciones financieras. De hecho aunque aún no es obligatorio, muchas plataformas han implementado prácticas KYC.

Debido a que los intercambios de cripto a cripto no se ocupan de la moneda tradicional, no tienen las mismas presiones para emplear los estándares KYC que los intercambios que se ocupan de la moneda fiat.

Los intercambios de fiat a cripto facilitan las transacciones que involucran monedas fiat y criptomonedas. Dado que la moneda fiat es la moneda oficial de una nación, la mayoría de estos intercambios emplean algunas medidas de KYC. Afortunadamente, las instituciones financieras ya deberían haber examinado a sus clientes de acuerdo con los requisitos de KYC. (European Digital Assets Exchange, n.d.)

3.2. Anti Money Laundering (AML)

Anti lavado de dinero (AML) se refiere a las leyes, reglamentos y procedimientos destinados a evitar que los delincuentes disfracen los fondos obtenidos ilegalmente como ingresos legítimos.

Se convirtió en una prominencia mundial en 1989, cuando un grupo de países y organizaciones de todo el mundo formaron el Grupo de Acción Financiera Internacional (GAFI en inglés, *Financial Action Task Force*, o FATF). Su misión es diseñar estándares internacionales para prevenir el lavado de dinero y promover su implementación. En octubre de 2001, luego de los ataques terroristas del 11 de septiembre, el GAFI amplió su mandato para incluir la lucha contra la financiación del terrorismo.

Otro organismo importante en la lucha contra el lavado de dinero es el Fondo Monetario Internacional (FMI) que también ha presionado a sus países miembros para que cumplan con los estándares internacionales para impedir la financiación del terrorismo.

Las leyes y reglamentos AML se enfocan en actividades delictivas que incluyen la manipulación del mercado, el comercio de bienes ilegales, la corrupción de fondos públicos y la evasión de impuestos, así como los métodos utilizados para ocultar estos delitos y el dinero derivado de ellos.

Una regla vigente es el período de retención AML, que requiere que los depósitos permanezcan en una cuenta durante un mínimo de cinco días de negociación. Este período de retención está destinado a ayudar en la lucha contra el lavado de dinero y la gestión de riesgos.

Los departamento de cumplimiento normativo a menudo son designados para supervisar las políticas contra el lavado de dinero y garantizar que los bancos y otras instituciones financieras lo cumplan.

Depende de las instituciones financieras supervisar los depósitos de los clientes y otras transacciones para asegurarse de que no sean parte de un esquema de lavado de dinero. Las instituciones deben verificar el origen de grandes sumas, supervisar actividades sospechosas y reportar transacciones en efectivo superiores a $10,000. Además se deben mantener extensos registros de casi todas las transacciones financieras significativas. Por otro lado, las instituciones financieras deben asegurarse de que los clientes conozcan las leyes AML.

Una técnica común para lavar es pasar el dinero a través de un negocio legítimo basado en efectivo que sea propiedad de la organización criminal o sus aliados: el negocio supuestamente legítimo deposita el dinero, que luego los delincuentes pueden retirar. De lo contrario, los lavadores de dinero también pueden infiltrar dinero en efectivo en países extranjeros para depositarlo, depositar dinero en efectivo en incrementos más pequeños para evitar despertar sospechas o usar dinero ilícito para comprar otros instrumentos de dinero en efectivo. A veces invertirán el dinero, utilizando corredores dispuestos a ignorar las reglas a cambio de grandes comisiones. (European Digital Assets Exchange, n.d.)

4. SISTEMA DE IDENTIFICACIÓN EN LA CADENA DE BLOQUES

La gestión de transacciones acordes a la legislación a través de tokens de autorización se basará en 4 pilares principales creando una autoridad validadora descentralizada (Tokeny Solutions, 2020):

- ONCHAINID: un sistema de gestión de identidad basado en blockchain, que permite la creación de una identidad, accesible globalmente para cada usuario.
- Un conjunto de certificados de validación (técnicamente hablando, estos

certificados son los *claims* (fragmento de información sobre el usuario), descritos en los estándares ERC-734 y ERC-735 utilizados por ONCHAINID (para una mejor comprensión, los nombraremos como certificados) emitido por terceros de confianza y firmado on-chain, cada uno de ellos vinculados a un único ONCHAINID.

- Un sistema de verificación de elegibilidad (*Eligibility Verification System*, EVS) cuya función es actuar como un filtro de todas las transacciones de valores tokenizados y verificará los certificados de validación de las partes interesadas. Esencialmente, el EVS verificará que el receptor tenga los derechos para recibir los tokens siguiendo las reglas de cumplimiento específicas y los requisitos del emisor aplicables para este activo específico. El EVS bloqueará la transacción si el receptor no tiene un certificado obligatorio y le notificará el motivo del bloqueo. El validador on-chain se implementa en el contrato inteligente del Registro de Identidad a través de la función “isVerified”.
- Un conjunto de reglas de Cumplimiento que garantizan que se respeten las reglas de la oferta, p.e. el máximo de inversores por país de distribución, el máximo de tokens en poder de un solo inversor, etc. Estas reglas no solo están vinculadas a la identidad del receptor de una transacción sino también a la distribución global de tokens en un momento determinado.

Estos 4 pilares permiten a los emisores utilizar una autoridad validadora descentralizada para controlar las transferencias y exigir el cumplimiento de los titulares del token de valores. El Validador incluye reglas para toda la oferta (p. ej., gestionar el número máximo de titulares permitidos en un mercado específico, cuando se aplique dicha regla), y reglas para cada inversor (p. ej., KYC o criterios de elegibilidad definidos por el emisor) gracias al sistema de gestión de identidad.

4.1. Sistema de Validación Descentralizado

Una transferencia de tokens ERC-20 generalmente ocurre de la siguiente manera en la cadena de bloques de Ethereum, con la implementación estándar de ERC-20:

Figura 1: Ilustración de una transacción ERC-20 (Tokeny Solutions, 2020)

Las transacciones se ejecutan entre 2 pares, sin restricciones y sin ningún control, la libertad de transacción es completa y pseudoanónima, las comprobaciones AML/KYC solo se realizan cuando las criptomonedas se convierten en monedas fiat y viceversa. Hay un muchas formas de evitar esto a través de intercambios no regulados, intercambios directos entre pares, etc.

En comparación, una transacción en un token de valores autorizado ERC-20 acorde con la legislación se procesará de la siguiente manera:

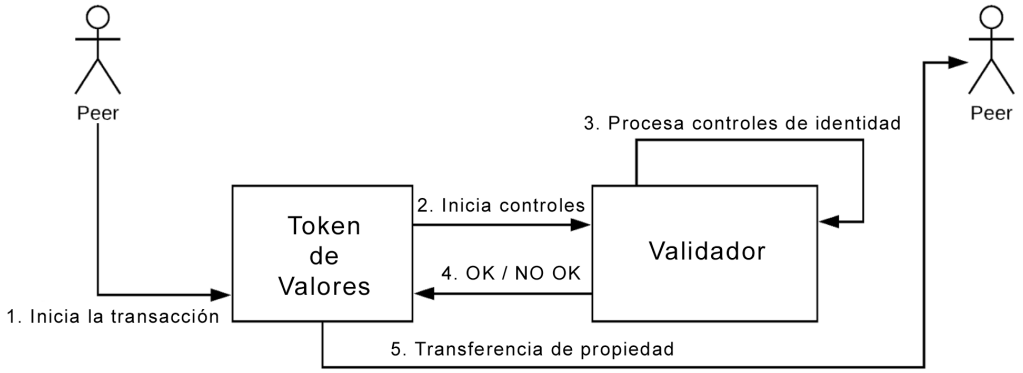

Figura 2: Ilustración de una transacción de token autorizada (Tokeny Solutions, 2020)

Los tokens de valores permiten transacciones entre pares después de una verificación de cumplimiento completa. El titular de los tokens inicia la transacción a través del contrato inteligente de token de valores (1.). A diferencia de un token ERC-20 estándar, la función de transacción del contrato inteligente se modifica, la función de transferencia del contrato inteligente llama al validador (2.) para iniciar comprobaciones en el ONCHAINID del receptor para asegurarse de que tiene los permisos necesarios o certificados para recibir el token en cuestión y que la transferencia cumple con las reglas de cumplimiento establecidas en el contrato inteligente de cumplimiento (3.). Si el ONCHAINID del receptor tiene los certificados requeridos (datos personales validados por terceros de confianza (por ejemplo, KYC, AML, entidad soberana,...) Y si la transferencia no viola ninguna de las reglas de cumplimiento establecidas en el contrato inteligente de cumplimiento, la transferencia de los tokens puede continuar (4.) y ejecutarse (5.) Si no tiene los certificados necesarios en su ONCHAINID O si la transferencia viola una regla de cumplimiento implementada en el contrato inteligente de cumplimiento, la transferencia se rechaza y se entrega un mensaje de error para explicar los pasos necesarios para obtener los certificados que faltan o la razón por la cual la transferencia fue rechazada por el contrato de cumplimiento (4.).

4.2. Gestión de identidades on-chain

Un token de valor está sujeto a una gobernanza estricta, su distribución tiene que seguir toda la normativa aplicable y, en particular, aquellos aspectos relacionados con las reglas KYC. En ese sentido, la gestión de la identidad es clave para implementar dicho cumplimiento en la cadena de bloques.

Dado que la propiedad de un token de valores se registra en la cadena de bloques, es necesario tener una forma de rastrear la propiedad del token y prohibir las transacciones ilícitas directamente en la cadena de bloques. Es por eso que existe la necesidad de vincular las direcciones de las carteras y las identidades para administrar los derechos a través de un contrato ONCHAINID (basado en ERC734-735) directamente en la cadena de bloques. Además, también debemos garantizar la privacidad de esas identidades para cumplir con las reglamentaciones relacionadas con la protección de datos personales. Por esta razón, los datos personales no deben almacenarse directamente en la cadena de bloques, sino solo los certificados de validación emitidos por terceros de confianza (proveedor de KYC, gobierno, notarios,…) que hayan verificado estos datos. Esos certificados (claims), almacenados en las identidades de cada usuario, serán utilizados por el validador descentralizado para validar si esas partes pueden o no poseer o transferir un token de valores específico.

Vincular la cartera de un inversor a un ONCHAINID puede aportar un valor añadido significativo a los usuarios en el incipiente mercado de tokens de valores. Por ejemplo, permitirá que un emisor de tokens reemplace los tokens de un inversor si el inversor pierde el acceso a su cartera (lo que sucede con bastante frecuencia y generalmente resulta en la pérdida de los activos del propietario), al verificar que sus datos personales proporcionados durante el proceso de recuperación se ajustan a los datos off chain vinculados al contrato ONCHAINID correspondiente a la cartera perdida. Una vez confirmada la identidad del inversor, el agente del emisor de tokens puede activar la función de recuperación que forzará una transferencia de tokens entre la billetera perdida y la nueva billetera y actualizar el registro de identidad así como el contrato ONCHAINID.

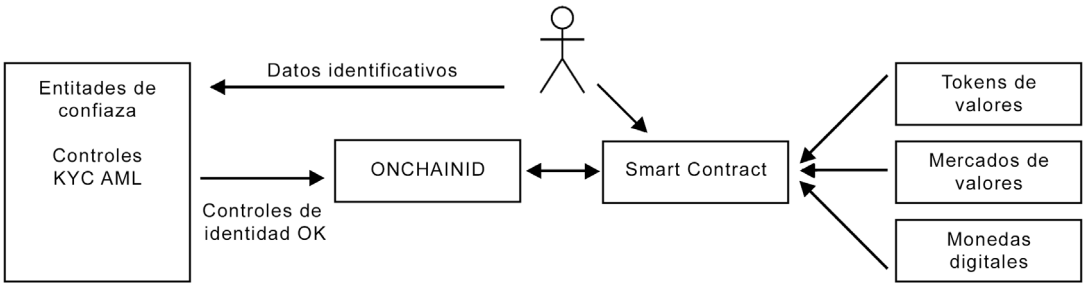

Figura 3: Modelo simplificado del protocolo ONCHAINID

Además, los ONCHAINID y los certificados (claims) que almacenan se pueden reutilizar potencialmente para pasar KYC para otros tokens de valores distintos a aquellos para los que se proporcionaron originalmente esos certificados o incluso en situaciones distintas a las inversiones (por ejemplo, apertura de cuenta en un servicio de cambio de moneda, identificación con servicios web compatibles, …). Si las cuentas de Google y Facebook son las identidades de la mayoría de las personas en el Internet de la información, la Web 2.0 , los ONCHAINID pueden ser los del Internet del valores, Web 3.0.

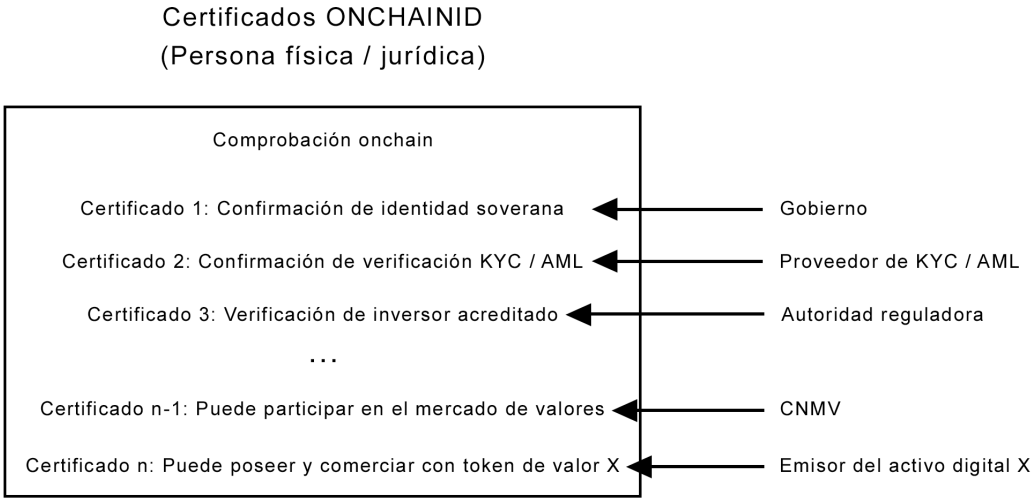

Figura 4: Sistema de certificados ONCHAINID (simplificación)

5. VALORES TOKENIZADOS

Los denominados *security tokens*, sirven como medio de inversión, generando en el adquirente unas expectativas de obtención de beneficios económicos. Debido a la consideración de estos tokens como instrumentos financieros (conforme al articulo 2 del texto refundido de la Ley del Merado de Valores), se tiene que aplicar

la Directiva 2014/65/EU – MIFID II, el Reglamento UE 600/2014-MIFIR, como también lo dispuesto en el Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores. En este caso se deberá contar con las autorizaciones exigidas para su emisión y someterse a la supervisión de la CNMV, considerándose dicha emisión como una STO (Security Token Offering).

En el plano de la Unión Europea, la European Securities and Markets Authority (ESMA) define los tokens como "Cualquier representación digital que pueda tener valor, ser un derecho a recibir un beneficio, o por contrario que no tenga un propósito o uso especifico". Por otro lado, el Banco Central Europeo (ECB) los define como "meras representaciones digitales de activos existentes, que permiten registrar esos activos mediante una tecnología diferente". Es decir, un activo digital emitido por una entidad, que puede tener valor en sí mismo o representar cualquier activo dentro de una comunidad, como pueden ser los activos financieros.

Acudiendo a la legislación española nos encontramos con el comunicado conjunto de la CNMV y del Banco de España con fecha de 8 de febrero de 2018 en donde se establecen las diferencias entre un *utility token* y un *security token*. Este comunicado se refuerza mediante la publicación de un nuevo documento por parte de la CNMV, en la misma fecha, mediante el cual se recogen los principales criterios a modo de revisión y actualización, denominado "Consideraciones de la CNMV sobre "criptomonedas" e "ICOs" dirigidas a los profesionales del sector financiero".

La CNMV y el Banco de España a través del comunicado conjunto citado anteriormente, definen como utility token a aquellos tokens que "dan derecho a acceder a un servicio o recibir un producto, sin perjuicio de lo cual con ocasión de la oferta se suele hacer mención a expectativas de revalorización y de liquidez o a la posibilidad de negociarlos en mercados específicos ". Por otro lado, los security tokens "generalmente otorgan participación en los futuros ingresos o el aumento del valor de la entidad emisora o de un negocio."

En este sentido, el Comunicado de la CNMV publicado en febrero 2018 estimó relevante los siguientes factores, para valorar si una ICO ofrece valores negociables:

- "Que los tokens atribuyan derechos o expectativas de participación en la potencial revaloración o rentabilidad de negocios o proyectos o, en general,

que presenten u otorguen derechos equivalentes o parecidos a los propios de las acciones, obligaciones u otros instrumentos financieros incluidos en el articulo 2 del TRLMV."

- "En el caso de tokens que den derecho a acceder a servicios o a recibir bienes o productos que se ofrezcan haciendo referencia, explicita o implícitamente, a la expectativa de obtención por el comprador o inversor de un beneficio como consecuencia de su revalorización o de alguna remuneración asociada al instrumento o mencionando su liquidez."

UTILITY TOKEN	SECURITY TOKEN
Regulado por las normativas de consumo y de publicidad, además de lo contemplado en el Código Civil.	Regulado por MIFID II/ MIFIR y la Ley del Mercado de Valores (LMV).
Rápida implementación.	Implementación y emisión lenta (se requiere aprobación de la CNMV).
Por lo general, su tenencia conlleva, el canje de servicios y productos, o incluso descuentos o ventajas en los servicios prestados por el emisor del token.	Activo que representa parte del patrimonio neto de la empresa emisora del token.
Valor especulativo en mercados no organizados.	Valor que puede negociarse, principalmente, en mercados organizados.
No brindan participación o poder de voto dentro del emisor del token.	Podría permitir al comprador tener participación directa y voto dentro de la empresa emisora del token.
En la medida en que exista un servicio de cambio del Criptoactivo por dinero fiat, o un servicio de custodia de las carteras o monederos, precisará cumplir con la normativa de AML, KYC	Precisa cumplir con la normativa de AML, KYC.

Tabla 1: Comparación entre la regulación de los tokens de utilidad y tokens de valores

También se podrán tener en cuenta los criterios marcados por el Test de Howey, los cuales fueron aplicados por primera vez en 1933 por la SEC (U.S. Securities and Exchange Commission), para determinar que nos encontramos ante un instrumento financiero (security token) si se cumplen los siguientes supuestos:

- Existe una inversión económica.
- Existe una participación en una empresa común.
- Existe una expectativa de obtener beneficio.
- El rendimiento proviene del trabajo de un tercero distinto al inversor.

Asimismo, debemos hacer alusión al borrador de la propuesta del Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de critptoactivos (MiCA), el cual tiene como objetivo final determinar unas pautas comunes y, consecuentemente, aportar seguridad jurídica a los operadores, poniendo el foco en el proceso de emisión y negociación y a la prestación de servicios sobre criptoactivos. El documento mencionado, aclara que los utility token o también denominadas “fichas de servicio”, no tienen la consideración de e-money tokens o de asset referenced tokens, por lo que a comparación de los security tokens, representan un menor riesgo para los usuarios por lo que no están sujetos a un régimen de autorización previo, sino a un régimen de notificación al supervisor. Los objetivos regulatorios que pretende la propuesta MICA, se centran principalmente en:

- la emisión de criptoactivos como la prestación de servicios de criptoactivos por parte de los proveedores, aplicando los requisitos de transparencia y divulgación de información.
- la autorización y supervisión de proveedores de criptoactivos y de emisores de tokens específicos.
- los medios de protección al consumidor frente a la emisión, negociación, intercambio y custodia de criptoactivos.

Teniendo en cuenta lo explicado en el presente articulo, es probable que con los criterios establecidos hoy en día por el regulador a la hora de diferenciar entre los diferentes tipos de token, puedan surgir dudas para determinar si queda dentro del ámbito de supervisión de la CNMV. Especialmente cuando el emisor no haga referencia explicita a la revalorización del token y esta se produzca por el crecimiento natural del mercado o del servicio, siendo imposible prever que el token se pueda revalorizar en función de la oferta y demanda.

Hemos implementado un contrato inteligente basado en CMTA token (The Capital Markets and Technology Association, 2022) y en el estándar EIP-3643 (Lebrun, Malghem, Thizy, Falempin, & Boudjemaa, 2021)

Este contrato inteligente es retrocompatible con ERC-20 e interactúa con un

contrato ERC-735 para validar los certificados enlazados con ONCHAINID, basado en ERC-734 y ERC-735.

Proporciona interfaces estándar para tokens de valores emitidos en Ethereum, a través de los cuales cualquier tercero podría interactuar con el token de valores. Las funciones descritas por estas interfaces varían y permiten a los usuarios apropiados realizar una variedad de acciones diferentes, como transferencias forzadas, congelar tokens (parcial o totalmente en una billetera o incluso congelar el token completo), acuñar, quemar, recuperar tokens perdidos (si un inversor pierde el acceso a su monedero), etc.

Se hizo un estudio con instituciones financieras que buscan emitir valores en una infraestructura DLT como ethereum y se llegó a los siguientes requisitos:

- Debe ser compatible con ERC-20.
- Debe usarse en combinación con un sistema de identificación en cadena (ONCHAINID)
- Debe poder aplicarse cualquier regla de cumplimiento requerida por la entidad reguladora o por el emisor del token
- Debe tener una interfaz estándar para verificar previamente si una transferencia se aprobará o fallará antes de enviarla a la cadena de bloques
- Debe tener un sistema de recuperación en caso de que un inversor pierda el acceso a su clave privada
- Debe poder congelar tokens en la billetera de los inversores si es necesario, parcial o totalmente
- Debe tener la posibilidad de pausar el token
- Debe poder acuñar y quemar tokens
- Debe poder eliminar el token
- Debe definir un rol de Agente (persona autorizada) y un rol de Propietario (emisor del token)
- Debe poder forzar transferencias desde una billetera de Agente
- Debe poder emitir transacciones en lote (para tener todas las transacciones realizadas en el mismo bloque)
- Debe ser actualizable (el código del contrato inteligente debe ser actualizable sin cambiar la dirección del contrato inteligente del token)

Este sistema esta formado por varios contratos inteligentes:

a.) Los tokens autorizados ERC-3643 se basan en una estructura ERC-20 estándar, pero se agregan algunas funciones para garantizar el cumplimiento en las transacciones de los tokens de valores. Las funciones transfer y transferFrom se implementan de forma condicional, lo que les permite proceder con una transferencia solo si la transacción es válida. Los tokens autorizados pueden transferirse solo a contrapartes validadas, para evitar que los tokens se mantengan en billeteras/ONCHAINID de inversores no elegibles/no autorizados. El estándar ERC-3643 también admite la recuperación de tokens de valores en caso de que un inversor pierda la clave privada de su billetera. Se mantiene un historial de tokens recuperados en la cadena de bloques por razones de transparencia. Los tokens ERC-3643 están implementando muchas funciones adicionales para brindarle al propietario o a su agente la posibilidad de administrar la oferta, las reglas de transferencia, los Lock-up[4] y todo lo que pueda requerirse en la administración de un valor.

Para poder realizar una transferencia se deben cumplir varias condiciones:

- El remitente debe tener suficiente saldo disponible (saldo total - tokens congelados, si los hay)
- El receptor debe estar incluido en la whitelist[5] en el Registro de Identidad y verificado (mantener los certificados necesarios en su ONCHAINID)
- La billetera del remitente no puede estar congelada
- La billetera del receptor no puede estar congelada
- La transferencia debe respetar todas las reglas de cumplimiento definidas en el contrato inteligente de Cumplimiento. Esto se realiza mediante la función isVerified que verifica si el receptor es un inversor válido y la función canTransfer que verifica si la transferencia cumple con las reglas de cumplimiento global aplicadas al token.

4 Periodo durante el cual no es posible realizar una determinada operación. Los motivos y características de estos “periodos de cierre” varían según el tipo de producto. Por ejemplo, en las ofertas públicas de venta (OPV) algunos accionistas pueden firman un compromiso de lock-up, por el que se obligan a mantener sus acciones durante un periodo determinado; el objetivo es facilitar la colocación entre el público, eliminando la incertidumbre y el descenso de precios que se produciría si algún accionista significativo optara por deshacerse de sus acciones.

5 Una lista blanca (en inglés, whitelist) es una lista o registro de usuarios /entidades que, por una razón u otra, pueden obtener algún privilegio particular, servicio, movilidad, acceso o reconocimiento. Es una lista de usuarios permitidos cuando todos están denegados por defecto.

Ademas de las funciones relativas a la transferencia, el contrato inteligente incorpora otras funciones según el tipo de valor que veremos mas adelante.

b.) El Registro de Identidad enlaza una dirección, un ONCHAINID y un código de país correspondiente al país de residencia del inversor. También comprueba la validez de los certificados (según los requisitos del token de valores) en el ONCHAINID del usuario. El Registro de Identidad es administrado por el agente y/o el propietario. Una vez que se realizan las comprobaciones de los certificados se añade la dirección, el ONCHAINID y el código del país del inversor a una lista blanca de identidades. Una vez que la dirección esta en la lista blanca el inversor puede ser titular del token. Existe un registro de identidad específico para cada token de valor.

c.) El Cumplimiento se utiliza para establecer las reglas de la oferta en sí y garantiza que estas reglas se respeten durante todo el ciclo de vida del token, p.e. el contrato de cumplimiento definirá la cantidad máxima de inversores por país, la cantidad máxima de tokens por inversor, los países aceptados para la circulación del token (utilizando el código de país correspondiente a cada inversionista en el Registro de Identidad). El contrato inteligente de cumplimiento es un contrato hecho a medida que se implementa de acuerdo con los requisitos legales y siguiendo las indicaciones del emisor del token.

d.) El Registro de emisores de confianza almacena las direcciones de todos los emisores de certificados de confianza para un token de valores específico. El ONCHAINID de los propietarios del token (los inversores) debe tener certificados firmados por los emisores de certificados almacenados en este contrato inteligente para poder tener el token. La propiedad de este contrato se otorga al emisor del token, lo que le permite administrar este registro según sus requisitos.

e.) El Registro de certificados almacena todos los certificados de confianza para el token de valores. El ONCHAINID de los propietarios de tokens debe contener los certificados almacenados en este contrato inteligente. La propiedad de este contrato se otorga al emisor del token, lo que le permite administrar este registro según sus requisitos.

6. MONEDAS DIGITALES

6.1. CBDC

Central Bank Digital Currency (CBDC) es un tipo de moneda digital emitida por un banco central y es una representación digital de la moneda fiat. Por tanto, tiene la propiedad de ser una forma de moneda regulada por un estado o una unión

de estados. Esta propuesta pretende solucionar el problema, especialmente de costos e infraestructura, que involucra la versión física del dinero fiat (monedas y billetes). (Solé, 2021)

Según el Banco de Inglaterra, las CBDC son dinero electrónico emitido por un banco central. Esto permite a los estados indicar que esta moneda digital es de curso legal. La emisión y registro de transacciones se realiza a través de algún tipo de sistema de base de datos centralizado. Las CBDC buscan expandir las características y la usabilidad del dinero fiduciario, especialmente en Internet, así como competir con Bitcoin y otras criptomonedas.

Los mecanismos de funcionamiento de las CBDC depende mucho de la tecnología utilizada para su creación y de las necesidades que pretendan cubrir. No tienen por qué estar todas creadas de la misma manera ni contar con las mismas características.

Muchos de los bancos centrales actualmente muestran interés por la tecnología blockchain y la variante DLT (Distributed Ledger Technology, Tecnología de Contabilidad Distribuida), para su desarrollo. Se apuesta por estas tecnologías para minimizar el riesgo de desarrollar sistemas monetarios que funcionan solamente en entornos digitales.

Blockchain y DLT son dos soluciones tecnológicas que simplifican la construcción de sistemas de interoperabilidad con otras monedas. Actualmente se trabajan en integraciones dentro de las criptomonedas que permiten el intercambio instantáneo entre criptomonedas con consensos diferentes. Pero además se podrían beneficiar del uso de smart contracts para crear o desplegar diferentes soluciones.

Entre las funciones de las CBDC podemos indicar las siguientes:

a.) Usabilidad: Lo que buscan es hacer las transacciones mucho más rápidas y fáciles. Poder realizar pagos instantáneos o realizar transferencias instantáneas son parte de los objetivos actuales.

b.) Reemplazar efectivo: Una de las principales desventajas del efectivo para un gobierno o banco central es su producción, transporte, mantenimiento y recaudación. Además, los billetes y las monedas se deterioran y también pueden ser un mecanismo para la transmisión de enfermedades (involuntariamente, por supuesto). La idea es desarrollar una moneda digital accesible al mayor número de usuarios. Debe cumplirse la característica de universalidad, aunque esto puede ser muy difícil de lograr en la práctica.

c.) Limitar el impacto social de las crisis bancarias: El objetivo es lograr que no existan crisis bancarias, o al menos reducir su frecuencia e impacto social. Las monedas digitales de este tipo pueden ofrecer depósitos a los usuarios para desvincular la provisión de pagos de la provisión de créditos.

d.) Reducir el crimen: Una de las desventajas de la moneda fiat física es que puede usarse para actividades ilícitas. Las monedas digitales emitidas por un organismo competente eliminan o minimizan esta posibilidad. Hay un registro de todas las transacciones, lo que permite rastrear el origen y el destino de las transacciones. Esto podría reducir o eliminar muchas actividades criminales como el narcotráfico o la prostitución. Más importante aún, podría tomar medidas drásticas contra la corrupción entre empresarios y políticos o la economía sumergida.

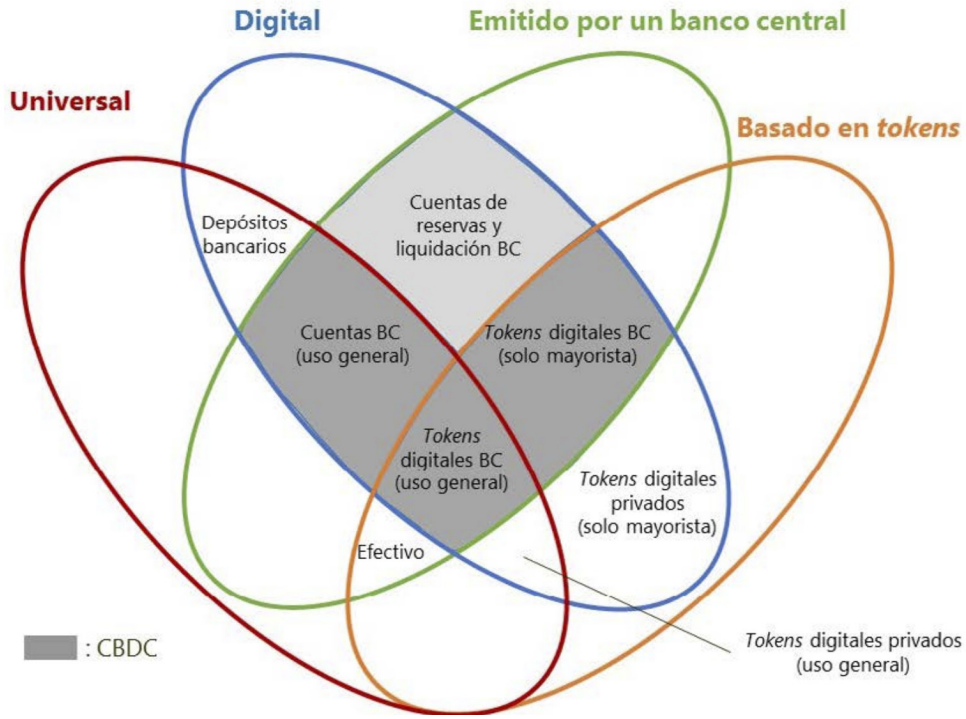

Figura 5: La flor del dinero: una taxonomía del dinero (BIS, 2018, pp. 6)

Las CBDC presentan tanto ventajas como desventajas. Entre las primeras podemos citar las siguientes:

- Creación de sistemas de pago más eficientes y emisión y control de mecanismos de emisión de fondos. Elementos que el actual sistema económico no permite alcanzar.

- Podrían ofrecer una mayor inclusión financiera a los usuarios de un estado. La creación de billeteras digitales para CBDC sería simple y llevaría los servicios bancarios a las personas que actualmente son rechazadas por el sistema bancario.
- Esto permitiría una mayor competencia entre las empresas de pago, permitiendo ajustes a la baja en las comisiones y tarifas.
- Desarrollar una política más justa y transparente para las personas.
- Reducir la corrupción política y la comisión de delitos, como el narcotráfico o la explotación sexual.

Tenemos los siguientes problemas o riesgos para el titular:

- Censura: el emisor de la moneda puede cancelar una transacción a voluntad o tomar los fondos del titular sin el consentimiento del titular por cualquier motivo
- Emisión: Los emisores pueden agregar a la circulación tantas monedas nuevas como deseen. Este es un proceso instantáneo y sin coste, mucho más fácil que emitir nuevos billetes y monedas.
- Público: No hay información pública sobre las transacciones realizadas con esta moneda digital. Esto implica que toda confianza depende de un tercero que asumimos como confiable y que no realizará acciones maliciosas.
- Auditable: El código proviene de un organismo público, pero dicho código no es público. Evita que los usuarios puedan analizar el código en busca de defectos o realizar mejoras en el código.
- Confidencialidad: Todas las transacciones son monitoreadas por un banco central y/o gobierno, por lo que no tenemos confidencialidad con respecto al uso del dinero. Esto es lo mismo que usar la tarjeta de crédito. Actualmente, si queremos privacidad al realizar transacciones, podemos hacerlo con efectivo, que no es rastreable.
- Acceso: Se podrían imponer sanciones a los usuarios que les impidan acceder a este tipo de dinero, realizar transacciones con el dinero que tienen en mente o simplemente apoderarse de él (lo que equivale a robarlo).
- Canjeable: Efectivamente, podemos enviar dinero a cualquier persona autorizada para acceder a este tipo de dinero. Las transacciones también pueden ser canceladas o el dinero retenido.

- Universalidad: No son realmente universales, ya que un banco central, un gobierno o una empresa puede decidir no aceptar este tipo de moneda. Si vamos a la tienda de conveniencia con dólares americanos, lo más normal es que no los acepten como forma de pago. Así de sencillo es dejar de ser una moneda universal.

6.2. Stablecoins

Es un término que se refiere a un token que tiene una paridad de 1:1 con la moneda fiat en una cadena de bloques. Tehter, por ejemplo, tiene un valor estable de un dólar por moneda Theter.

Las Stablecoins son tokens, no criptomonedas, y tienen una emisión cerrada o abierta. Esto significa que se emite una cierta cantidad y no se puede agregar más (emisión cerrada), o que se pueden agregar cantidades adicionales indefinidamente (emisión abierta). Cabe señalar que estos suelen ser emitidos por empresas. (Solé, 2021)

Hay distintos tipos de stablecoins. Por un lado tenemos las respaldadas por dinero fiat. Básicamente, un pagaré (IOU, *I owe you*) por una moneda fiat tradicional (generalmente dólares). Se utiliza moneda fiat para comprar una stablecoin que luego se puede canjear por la moneda original. (Ethereum Foundation, n.d.-b)

Existen también stablecoins respaldadas por metales preciosos. Al igual que las monedas con respaldadas por dinero fiat, estas monedas estables utilizan recursos como el oro para mantener su valor.

Tanto las stablecoins respaldadas por fiat como con metales preciosos necesitan auditorias externas para garantizar que la empresa emisora tenga suficientes reservas para mantener la paridad.

Otro tipo son las respaldadas por criptomonedas. Estas monedas estables están respaldadas por otros criptoactivos, como Ether. Su precio depende del valor del activo subyacente (o colateral), que puede ser volátil. Debido a que el valor de ETH puede fluctuar, estas monedas estables están sobregarantizadas para garantizar que el precio se mantenga lo más estable posible. Esto significa que es mas correcto decir que una moneda estable *respaldada por criptomonedas* de $ 1 tiene un activo criptográfico subyacente que vale al menos $ 2. Entonces, si el precio de ETH cae, se debe usar más ETH para respaldar la moneda estable, de lo contrario, las monedas estables perderán su valor. Este tipo de stablecoins no necesita custodios, los activos se almacenan en los smart contracts por lo que no se necesita auditoría externa.

Finalmente, también hay stablecoins respaldadas por Algoritmos o, más estrictamente, no están respaldadas por ningún activo. Un algoritmo venderá tokens si el precio cae por debajo del valor deseado y proporcionará tokens si el valor supera la cantidad deseada. Dado que la cantidad de estos tokens en circulación cambia regularmente, la cantidad de tokens que posee cada usuario cambiará, pero siempre reflejará el mismo porcentaje del total. A Julio de 2022 no se ha conseguido implementar con éxito este sistema y las stablecoins respaldadas por algoritmos terminan perdiendo la paridad.

Las stablecoins y las CBDC tienen algunos aspectos comunes, siendo el más importante la falta de privacidad. Las stablecoins se crean para su uso en intercambios centralizados donde tenemos que pasar controles KYC y AML. Las CBDC al estar vinculados a nuestra identidad, se elimina la privacidad.

También comparten la propiedad de emisión ilimitada. Aunque hay monedas estables que tienen emisión cerrada, la mayoría tienen emisión abierta. Esto significa que se pueden agregar tantos tokens nuevos como los desarrolladores lo consideren necesario. Las CBDC son lo mismo, los bancos centrales o los gobiernos creadores pueden generar tantas monedas nuevas como quieran.

Las monedas estables suelen ser emitidas por empresas, mientras que las CBDC son creadas por bancos centrales o gobiernos.

6.3. Funciones del token de valor aplicadas a monedas digitales

Algunos ejemplos prácticos de las funciones citadas aplicadas a las monedas digitales son:

- Transfer: permite el intercambio de la moneda digital entre usuarios.
- batchTransfer: puede ser utilizada para transferir ayudas sociales a una lista determinada de usuarios o transferir el salario a una lista de empleados.
- setAddressFrozen: seria el equivalente a congelar una cuenta bancaria debido a actividades ilícitas o deudas impagadas.
- Las funciones mint y burn permiten de forma sencilla controlar la oferta monetaria añadiendo o retirando monedas en circulación.
- Las funciones snapshot permiten mantener un registro de los balances de las carteras para facilitar sistemas de auditoría y pago de impuestos.

7. ACCIONES

Las transferencias de valores pueden tener restricciones por una variedad de razones. Esto contrasta directamente con los tokens de utilidad, de los cuales generalmente solo se requiere que el remitente tenga un saldo suficiente. Estas condiciones pueden estar relacionadas con el estado de la billetera de un inversor, la identidad del remitente y el receptor de los valores (es decir, si han pasado por un proceso KYC / AML, si están acreditados o son afiliados de la entidad emisora) o por razones no relacionadas con la transferencia específica, sino que se establece a nivel de token (es decir, el smart contract del token impone un número máximo de inversores o un límite en el porcentaje en poder de un solo inversor). Para los tokens ERC-20, las funciones de balanceOf (balance de la billetera) y allowance (permisos de acceso a tokens) brindan una forma de verificar que es probable que una transferencia tenga éxito antes de ejecutar la transferencia, que se puede ejecutar tanto *on-chain* como *off-chain*. Para tokens que representan valores, se introduce una función canTransfer (puede transferir) que proporciona una forma más general para realizar las transferencias p.e. cuando los motivos de restricción de la transferencia están relacionados con las reglas de cumplimiento del token y la función isVerified (esta verificado) que permite verificar el estado de elegibilidad de la identidad del inversor.

Podemos especificar en el contrato inteligente atributos tales como el nombre de la acción, el código ISIN o la documentación relativa a la acción por ejemplo el Documento de datos fundamentales para el inversor DFI, en ingles KID recogido en el REGLAMENTO (UE) no 583/2010.

Otras funciones relativas a las acciones son:

a.) Splits y contra-splits

Esta implementación no permite administrar splits de acciones y contra-splits on-chain (es decir, redefinir la unidad de noción de un token). Más bien, tales acciones corporativas deben llevarse a cabo a través de las funciones “Mint” y “Burn” descritas anteriormente, para garantizar que la cantidad de tokens siempre sea igual a la cantidad de acciones tokenizadas.

Un split de acciones se puede llevar a cabo ya sea “quemando” los tokens existentes y “acuñando” otros nuevos (por ejemplo, “acuñando” dos nuevos tokens por cada token “quemado”) o “acuñando” tokens adicionales y asignando esos nuevos tokens a todas las direcciones del libro mayor (utilizando las funciones snapshot y batch). Los splits de acciones y los contra-splits requieren enmiendas a los documentos constitutivos del

emisor relevante (estatutos de asociación y, potencialmente, los términos de tokenización).

b.) Distribución de dividendos o intereses

Puede que los emisores tengan que realizar distribuciones a los titulares de los valores (por ejemplo, pagos de dividendos para valores de renta variable o pagos de intereses para valores de deuda). Los emisores pueden decidir realizar las distribuciones off chain (es decir, transfiriendo moneda fiat a la cuenta bancaria de los titulares de valores). Sin embargo, si el emisor tiene la intención de realizar dichas distribuciones on chain, esto puede requerir la distribución de monedas digitales (dividendo activo) o la distribución de nuevos tokens (dividendo en acciones) a los titulares de tokens existentes, sobre la base de una snapshot realizada en el momento en que surge el derecho legal a la distribución. No todos los poseedores de tokens pueden ser elegibles para distribuciones. Los eventos de distribución generalmente se realizan de acuerdo con un calendario de fechas predefinido[6] y de acuerdo con la distribución de tokens en un momento determinado, que puede determinarse mediante una Snapshot.

c.) Votación

Gracias a la implementación ERC20Votes y ERC20VotesComp los titulares de un token pueden emitir una propuesta (si cumplen los requisitos necesarios p.e. contar con un 10% de todas las acciones) y votar esa propuesta.

---

6 Las fechas claves en relación con los dividendos de acciones son las siguientes:

1. Fecha de declaración: fecha en la que la junta de directores de la empresa aprueba el pago de dividendos y designa la fecha de pago y la fecha de cierre de registro.

2. Fecha de cierre de registro: la fecha que determina los accionistas con derecho a recibir el pago del dividendo. Debe ser titular de acciones al final del día de la fecha del cierre de registro para recibir el dividendo.

3. Fecha ex-dividendo: la fecha en la que las acciones se negociarán sin el derecho a recibir el dividendo. Debido a que la mayoría de las operaciones en acciones en Estados Unidos se liquidan de forma regular, es decir tres días hábiles tras la operación, una persona física debe comprar las acciones tres días hábiles antes de la fecha de cierre de registro para cualificarse para el dividendo. La fecha ex-dividendo es, por lo tanto, dos días hábiles anterior a la fecha de cierre de registro.

4. Fecha de pago: fecha en la que el dividendo declarado se paga a todos los accionistas que tengan acciones en la fecha de cierre de registro.

Ademas si esta propuesta esta relacionada con el contrato inteligente, como emitir un dividendo o realizar un split de las acciones, se puede implementar en la propuesta el código relativo para realizar los cambios en el contrato inteligente. De esta forma una vez que la propuesta consigue los votos necesarios, cualquier titular de los tokens, no solo el creador de la propuesta, puede ejecutar la propuesta y automáticamente se realizaran los cambios en el contrato inteligente sin la necesidad de una autoridad central.

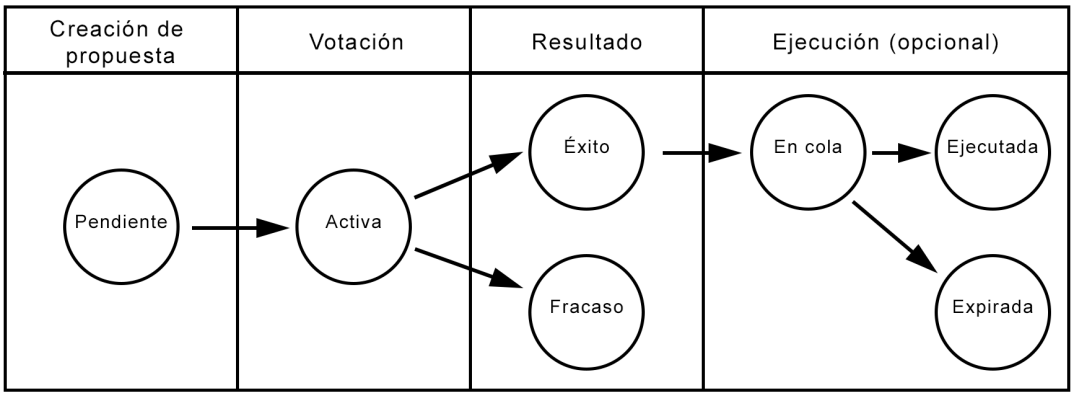

Figura 6: Ciclo de vida de una propuesta.

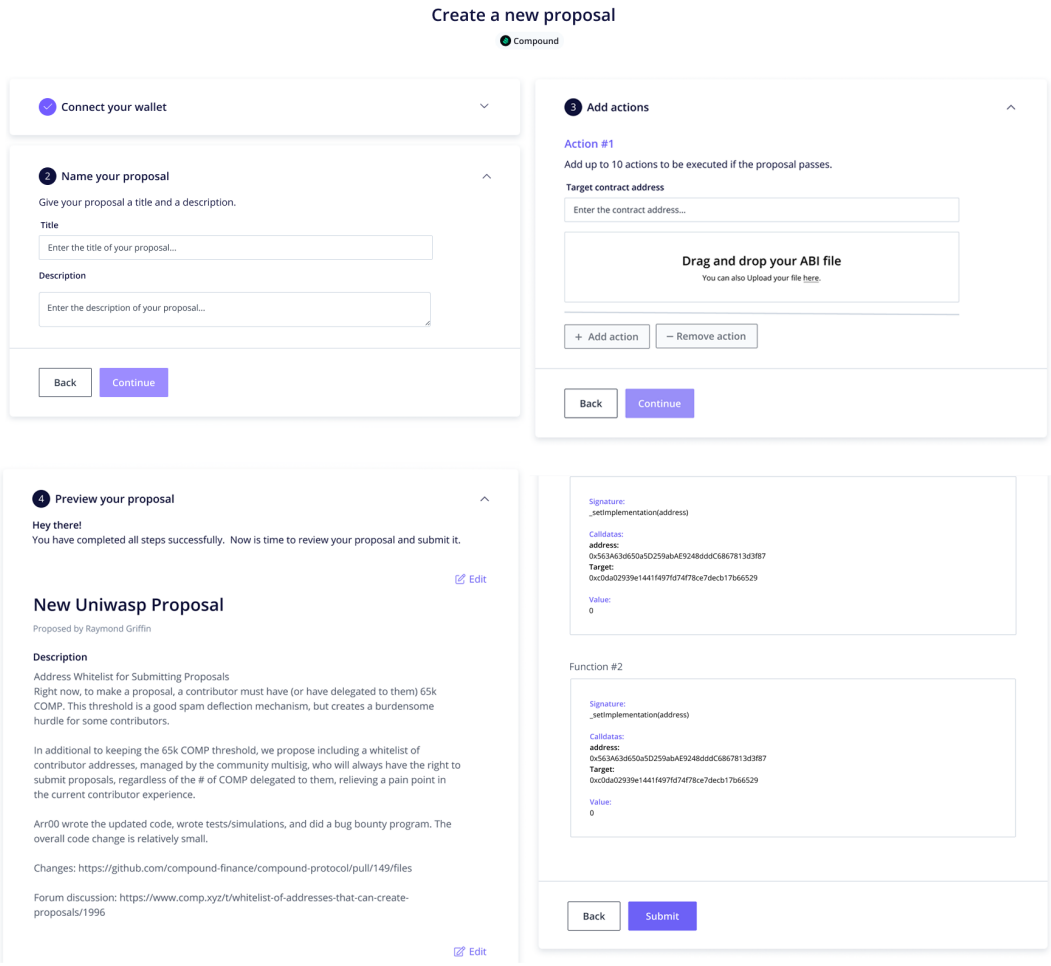

Figura 7: Interfaz de creación de propuestas de tally.xyz

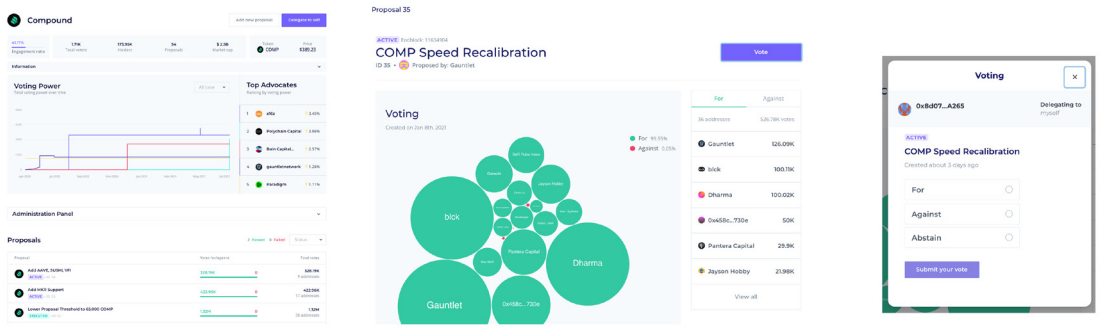

Figura 8: Interfaz de votación de propuestas de tally.xyz

8. TOKENS DE VALORES DE DEUDA

Los tokens de valores de deuda se refieren a instrumentos de deuda como bonos corporativos, hipotecas inmobiliarias o bonos del Estado. El valor de un token de valor de deuda depende de dos factores clave: riesgo e intereses. El riesgo implica los sucesos inesperados a los que están sujetos los tokens de valores de deuda, como cambios drásticos en el valor de la deuda o incumplimiento de los deudores. Mientras que el interés, por otro lado, se refiere a una forma de ingreso regular que el instrumento de deuda subyacente está estructurado para generar.

En términos de blockchain, el contrato inteligente que representa un token de valor de deuda debe incluir información relativa como la identidad del titular del bono, la fecha de vencimiento, el valor nominal, la rasa de interés y la fecha de devengo y pago de los intereses.

También el contrato inteligente posee funciones utilizadas por las agencias calificación de riesgos como indicar la calificación del bono o indicar el impago del bono por parte del emisor.

Finalmente el contrato inteligente incorpora funciones que automáticamente cuando llega la fecha para realizar los pagos se retira el importe de los intereses y/o el principal de la dirección del emisor y se pone a disposición de los titulares del bono. De forma similar a los dividendos, los titulares del bono pueden reclamar su parte correspondiente. Si el deposito no tuviese fondos suficientes se emitiría un evento en la blockchain indicando el impago del bono.

9. PRODUCTOS DERIVADOS

Podemos utilizar estos módulos para crear otros tipos de productos derivados. Aunque en este estudio no se han implementado de forma practica procedemos ha explicar a grandes rasgos algunos de ellos:

9.1. Préstamo hipotecario

Existen implementaciones para tokenizar bienes inmuebles (Token Factory Switzerland, 2018). Podemos diseñar el préstamo hipotecario como un token bono emitido por el propietario del inmueble y los intereses serían la cuota hipotecaria. Si el deudor no pudiese pagar el interés una vez pasado el periodo de gracia se puede transferir el token que representa la propiedad al acreedor de forma automática. Estos tokens inmobiliarios también se pueden usar como llave, una cerradura electrónica puede escanear una cartera y solo abrirse si detecta el token asociado a la vivienda.

9.2. Póliza de seguros

Los seguros se pueden programar como un smart cotract con la dirección del asegurado y del beneficiario y genera un token para el asegurador. El asegurado paga la prima acorde al calendario establecido utilizando el mismo sistema que los intereses de los bonos al poseedor del token asegurador. Si se produce el evento cuyo riesgo es objeto de cobertura a indemnizar que puede ser verificado mediante un oráculo por la propia compañía de seguros, una entidad tercera o una entidad gubernamental (para los certificados de defunciones) entonces automáticamente el poseedor del token asegurador realiza el pago de la indemnización a la dirección beneficiario. De este modo podemos permitir la negociación de los seguros en el mercado secundario: los inversores pueden comprar el token asegurador y recibir las primas y pagar la indemnización.

9.3. Opciones

Para este ejemplo nos vamos a referir a la call o opción de compra. Podemos implementarlo como dos contratos inteligentes entrelazados. El contrato obligación con su token asociado cuyo propietario es la persona que ha emitido la call. El contrato derecho con su token asociado guarda las condiciones de la call como la cantidad de acciones subyacentes o la fecha de ejecución en el caso de opciones europeas, en el caso de opciones americanas el contrato permite al poseedor del token derecho ejercitar la call cuando quiera. Cuando se ejercita la call el proceso sería el siguiente: el contrato derecho llama al contrato obligación que ejecuta la transferencia de las acciones (o el equivalente monetario del valor de las acciones mediante un oráculo) de la dirección propietaria del token

obligación a la dirección propietaria del token derecho. Mediante la transferencia de los tokens obligación y derecho podemos establecer en el mercado secundario de la call posiciones cortas y largas.

10. MERCADO SECUNDARIO DE TOKENS

Vamos a utilizar el protocolo 0x para establecer el mercado secundario en la cadena de bloques. 0x es una infraestructura de intercambio descentralizada de código abierto que permite el intercambio de activos tokenizados en múltiples cadenas de bloques. Este sistema permite transacciones mediante un libro de órdenes o fuera del mercado como OTC. El protocolo 0x es, en esencia, un conjunto de contratos inteligentes seguros que facilitan el intercambio entre pares de activos basados en Ethereum.

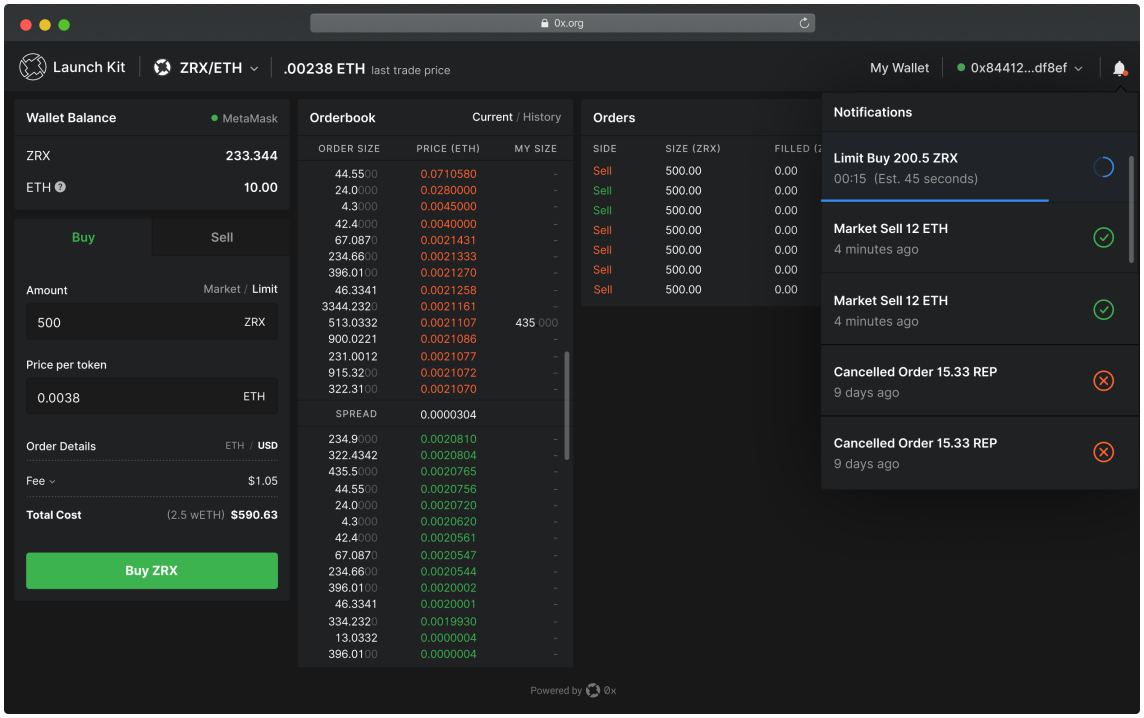

Figura 9: Interfaz del libro de órdenes de 0x

Dentro del ecosistema 0x, hay dos lados. Oferentes, esta es la entidad que crea órdenes 0x y proporciona liquidez al sistema para que la consuma el lado de la Demanda. Demandantes, esta es la entidad que quiere el activo del oferente. Los demandantes acuerdan cambiar su activo por el activo del oferente; en otras palabras, consumen la liquidez 0x.

Para realizar el intercambio de los tokens la API de 0x primero realiza una consulta de los precios de múltiples mercados y agrega la liquidez de las fuentes consultadas para proporcionar el mejor precio posible. Funciona de forma similar al servicio de vuelos de Google que agregan de diferentes páginas los precios de

los vuelos para una fecha y hora determinadas para encontrar el mejor precio. De manera similar 0x encontrar el mejor precio en todas las fuentes de liquidez.

El algoritmo de enrutamiento de pedidos inteligentes de 0x divide la transacción en diferentes fuentes para maximizar el rendimiento general del intercambio.

Las respuestas de la API se devuelven en un formato que se puede ejecutar fácilmente utilizando las bibliotecas Web3.

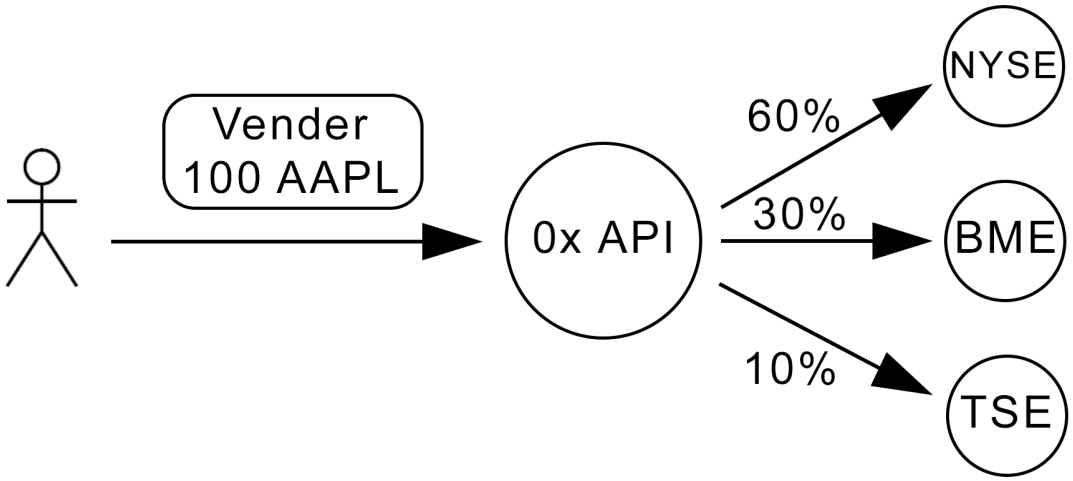

Figura 10: Funcionamiento de la API de 0x

11. CONCLUSIÓN

Podemos ver que se puede implementar la tecnología de bloques al mercado de valores cumpliendo toda la regulación. Esto nos permite incorporar las mejoras de la tecnología de bloques al mercado de valores. Algunas de estas mejoras son:

- Transparencia: El registro inalterable de transacciones facilita las labores contra el fraude y el blanqueo de capitales. Actualmente ya existen herramientas como Crystal blockchain y TRM labs que permiten rastrear los movimientos de las criptomonedas. Si vinculamos las direcciones con una identidad, con el sistema ONCHAINID, entonces realizar el seguimiento de transacciones sería trivial.

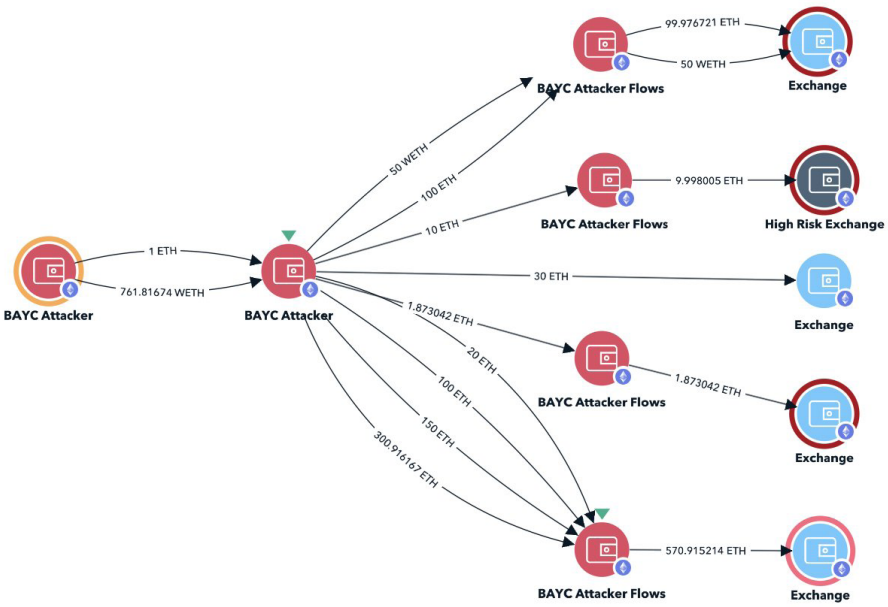

Figura 11: Historial de transacciones de TRM labs.

- Velocidad de las transacciones: Actualmente las transacciones entre bancos mediante el sistema swift se realizan mediante intermediarios, esto produce una demora de las transacciones. Utilizando la tecnología de bloques podemos establecer transacciones directas e instantáneas entre los bancos. Este sistema también facilita las transacciones de mercancías. Con el sistema actual los participes (el comprador, aduanas, transporte, bancos, etc) tienen que recibir y enviar documentación relacionada con la compra de las mercancías. Con la tecnología de bloques podemos poner a disposición de todos los participantes la documentación necesaria para reducir el tiempo de la transacción.

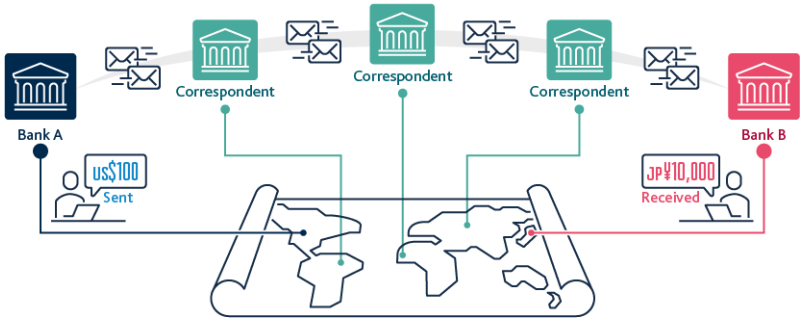

Figura 12: Sistema actual de transferencias bancarias internacionales.

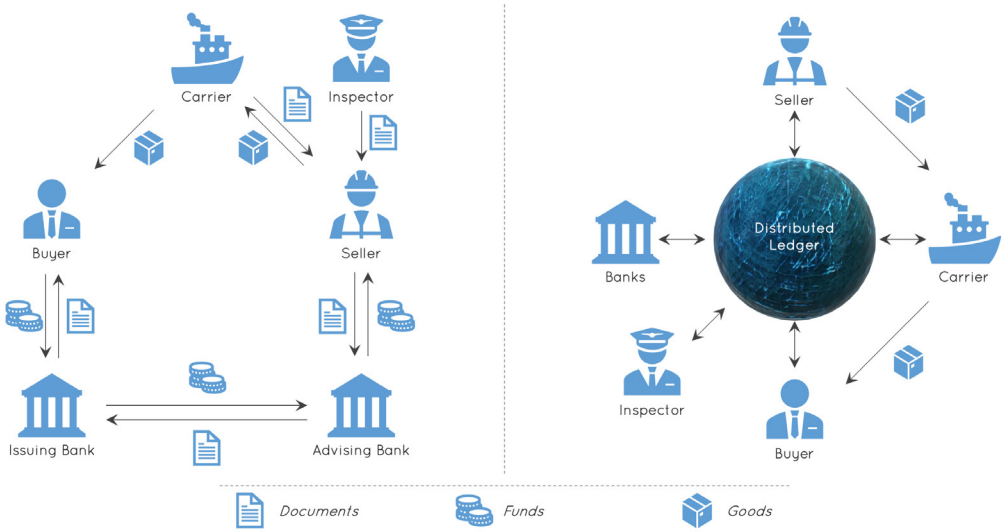

Figura 13: Comparación entre el sistema actual y el sistema con la tecnología de bloques para las transacciones de mercancías.

- Fiabilidad: la tecnología de bloques opera entre varios nodos esto permite que aunque uno de los nodos falle, el sistema sigue funcionando.
- Seguridad: la criptografía asimétrica aporta seguridad a los inversores y evita problemas como la apropiación indebida de fondos o el robo de identidad.

BIBLIOGRAFÍA

CNMV. (n.d.-a). CNMV - Glosario Financiero. Retrieved July 9, 2022, from www.cnmv.es website: http://www.cnmv.es/Portal/inversor/Glosario.aspx

CNMV. (n.d.-b). CNMV - Productos derivados. Retrieved July 9, 2022, from www.cnmv.es website: http://www.cnmv.es/Portal/inversor/Derivados.aspx

Ethereum Foundation. (n.d.-a). Ethereum wallets. Retrieved from ethereum.org website: https://ethereum.org/en/wallets/

Ethereum Foundation. (n.d.-b). Stablecoins. Retrieved from ethereum.org website: https://ethereum.org/en/stablecoins/

Ethereum Foundation. (n.d.-b). What is Ethereum? Retrieved from ethereum.org website: https://ethereum.org/en/what-is-ethereum/

FIBO Group. (n.d.). Glossary | Valores. Retrieved July 9, 2022, from www.fibogroup.mx website: https://www.fibogroup.mx/clients/glossary/securities/

Nakamoto, S. (2008). Bitcoin: a Peer-to-Peer Electronic Cash System. In bitcoin.org. Retrieved from https://bitcoin.org/bitcoin.pdf

Tokeny Solutions. (2020). T-REX (Token for Regulated EXchanges). Retrieved from https://tokeny.com/wp-content/uploads/2020/05/Whitepaper-T-REX-Security-Tokens-V3.pdf

EUR Lex. (2022). EUR-Lex - 32010R0583 - EN - EUR-Lex. Retrieved July 10, 2022, from Europa.eu website: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32010R0583

European Digital Assets Exchange. (n.d.). What do you need to know: KYC & AML. Retrieved July 22, 2022, from EDSX - European Digital Assets Exchange website: https://www.edsx.ch/blog-news/what-do-you-need-to-know-kyc-aml

Lebrun, J., Malghem, T., Thizy, K., Falempin, L., & Boudjemaa, A. (2021, July). EIP-3643: T-REX - Token for Regulated EXchanges. Retrieved July 18, 2022, from Ethereum Improvement Proposals no. 3643 website: https://eips.ethereum.org/EIPS/eip-3643

Fernández De Lis, S., & Gouveia, O. (2019). Monedas digitales emitidas por bancos centrales: características, opciones, ventajas y desventajas. Retrieved from https://www.bbvaresearch.com/wp-content/uploads/2019/03/WP_Monedas-digitales-emitidas-por-bancos-centrales-ICO.pdf

Solé, R. (2021, July 11). CBDC: qué son y en qué se diferencian de las criptomonedas. Retrieved July 22, 2022, from Profesional Review website: https://www.profesionalreview.com/2021/07/11/que-es-cbdc/

Szabo, N. (1994). Smart Contracts. Retrieved July 6, 2022, from www.fon.hum.uva.nl website: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Szabo, N. (1996). Nick Szabo -- Smart Contracts: Building Blocks for Digital Markets. Retrieved July 6, 2022, from Hum.uva.nl website: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Comité de Pagos e Infraestructuras del Mercado, & Comité de los Mercados. (2018). Comité de Pagos e Infraestructuras del Mercado Comité de los Mercados Monedas digitales emitidas por bancos centrales. In Bank for International Settlements. Bank for International Settlements. Retrieved from Bank for International Settlements website: https://www.bis.org/cpmi/publ/d174_es.pdf

The Capital Markets and Technology Association. (2022). CMTAT Functional specifications for the Swiss law compliant tokenization of securities. Retrieved from https://cmta.ch/content/15de282276334fc837b9687a13726ab9/cmtat-functional-specifications-jan-2022-final.pdf

Token Factory Switzerland. (2018). FACILITATING AN ACCESSIBLE & STREAMLINED REAL-ESTATE MARKET. Retrieved from blockimmo.ch website: FACILITATING AN ACCESSIBLE & STREAMLINED REAL-ESTATE MARKET

APÉNDICE 1: GLOSARIO

- Token: Un bien virtual negociable definido en un contrato inteligente en la cadena de bloques de Ethereum. En algunos casos el titular del token puede acceder a funciones exclusivas del contrato inteligente como emitir un voto o recibir dividendos.
- Interfaz de un token: conjunto de funciones accesibles por los usuarios (pueden poseer el token o no)
- Token standars: conjunto de especificaciones (funciones) de forma que los tokens definidos con dichos estándares tenga propiedades comunes y sean interoperables. Por ejemplo, cuando un nuevo proyecto emite un token, sigue siendo compatible con los intercambios descentralizados existentes.
- Oráculos: son fuentes de datos que conectan Ethereum con información del mundo real fuera de la cadena para poder consultar datos en los contratos inteligentes. Por ejemplo se puede apostar quien será el próximo presidente de los Estados Unidos y usar un oráculo para confirmar el resultado y el pago a los ganadores.
- Transacciones *On-Chain* (en cadena o dentro de la cadena)*:* se refieren a transacciones que se registran y verifican en la cadena de bloques. Las transacciones en cadena se consideran válidas solo cuando la cadena de bloques se ha actualizado para reflejar las transacciones en el libro mayor público. Las transacciones en cadena ofrecen seguridad y transparencia, ya que no se pueden modificar una vez que se verifican y registran en la red. Sin embargo, existen algunos inconvenientes en las transacciones en cadena, que incluyen tarifas más altas y tiempos de procesamiento lentos.
- Transacciones *Off-Chain* (fuera de la cadena): se refieren a transacciones que ocurren fuera de la cadena de bloques. Las transacciones fuera de la cadena pueden implicar tarifas más bajas, tiempos de procesamiento inmediatos y mayor anonimato que las transacciones dentro de la cadena. Dependiendo del método utilizado, es posible que las transacciones fuera de la cadena eventualmente deban registrarse dentro de la cadena.

APÉNDICE 2: FUNCIONES DE LOS CONTRATOS INTELIGENTES

Tabla 2: Funciones comunes de los tokens de valores	
Nota: las funciones marcadas con asterisco solo pueden ser utilizadas por el emisor, las otras pueden ser usadas por usuarios[1]	
setName*	establece el nombre del token
setSymbol*	establece el símbolo del token
setupDecimals*	establece el número de decimales. Especialmente útil para las acciones ya que algunas legislaciones permiten acciones fraccionarias y otras no
pause*	pausa el contrato del token, cuando el contrato está en pausa, los inversores no pueden transferir tokens
unpause*	reanuda el contrato del token, cuando el contrato no está en pausa, los inversores pueden transferir tokens
setAddressFrozen*^	si la dirección esta congelada no se pueden transferir los tokens
freezePartialTokens*^	congela una cantidad de tokens especificada para una dirección dada
unfreezePartialTokens*^	descongela una cantidad de tokens especificada para una dirección dada
forcedTransfer*^	forzar una transferencia de tokens entre 2 billeteras
mint*^	genera tokens en una billetera
burn*^	destruye los tokens de una billetera
batch*	Esta función combinada con las funciones con acento circunflejo permiten realizar acciones con una lista de direcciones. P.e. batchTransfer transfiere una cantidad determinada de tokens a cada una de las direcciones de una lista dada.
recoveryAddress*	función de recuperación utilizada para forzar la transferencia de tokens desde un billetera perdida a una nueva billetera de un inversor.
Kill*	autodestrucción del smartcontract y como consecuencia de los tokens, impidiendo así cualquier transferencia u otra operación.

1 Emisor significa la entidad legal que ha emitido el valor representado por los tokens o una persona o entidad autorizada por dicho emisor para realizar ciertas acciones en los tokens.

Usuario significa cualquier entidad o persona que controla una dirección en el blockchain en el que se registran los tokens (pero no necesariamente tiene que poseer los tokens).

ScheduleSnapshot*	permite programar la creación de una instantánea (snapshot)[2] en un momento determinado. La hora de la nueva instantánea programada no puede ser anterior a la hora de la última instantánea programada, pero aún no creada.
RescheduleSnapshot*	cambia la hora de una instantánea programada. La nueva hora programada no puede ser anterior a la hora de la instantánea programada anteriormente ni posterior a la hora de la siguiente instantánea programada (es decir, las instantáneas programadas no pueden ser reordenadas).
UnscheduleSnapshot*	cancela una instantánea programada anteriormente. La instantánea programada anulada debe ser la última instantánea programada y su hora debe ser en el futuro.
TotalSupply	para un token en particular, cualquier persona puede conocer la cantidad total de tokens en circulación en cualquier momento.
BalanceOf	para un token en particular y un usuario en particular, cualquier persona puede saber la cantidad de tokens registrados actualmente en la dirección del blockchain del usuario.
Transfer	los usuarios pueden transferir algunos o todos sus tokens a alguna otra dirección de registro (que el cedente no necesariamente controla).
SnapshotTime	para una instantánea particular programada, pero aún no creada, cualquiera puede conocer la hora de la instantánea.
SnapshotTotalSupply:	para una instantánea creada en particular, cualquiera puede saber la cantidad total de tokens que estaban en circulación en el momento de la creación de la instantánea.
SnapshotBalanceOf:	para una instantánea creada en particular y una dirección en particular, cualquiera puede saber la cantidad de tokens registrados en la dirección correspondiente en el momento de la creación de la instantánea.

2 La función Snapshot (instantánea) determina el número de tokens registrados en las diversas direcciones del blockchain en un momento específico

Tabla 3: Atributos obligatorios, aplicables a todas las acciones tokenizadas	
Name	Nombre del token
Symbol	Símbolo del token
ID del token	ISIN o equivalente
Documentación	incluyen un enlace web a los términos de tokenizacion, los términos de la acción, y otros documentos relevantes (por ejemplo, Documento de datos fundamentales para el inversor (DFI en ingles KID) recogido en el REGLAMENTO (UE) no 583/2010)
Compliance	enlaza el contrato de Cumplimiento vinculado al token, p.ej. el contrato de cumplimiento definirá la cantidad máxima de inversores por país, la cantidad máxima de tokens por inversor, los países aceptados para la circulación del token, etc.
identityRegistry	enlaza el contrato de Registro de Identidad vinculado al token

Tabla 4: Funciones para la distribución de dividendos	
DistributionCreateParameters*	Define el token de liquidación (es decir, el token que se distribuirá), la snapshot (pasada o futura) usada para la distribución y la cantidad que se distribuirá.
DistributionSetEligibility*	Define las reglas para que un inversor pueda recibir el dividendo con una snapshot (equivalente a la fecha de cierre de registro)
DistributionSetDeposit*	establece un deposito con los tokens que van a ser distribuidos (importe total del dividendo en moneda o acciones)
DistributionClaimDeposit	Permitir que los titulares de tokens reclamen su parte de un depósito, de acuerdo con el saldo del token en la instantánea creada en la fecha de cierre de registro

Tabla 5: Funciones para realizar una votación	
propose	cualquiera con suficientes votos (por ejemplo, el 1 % de los tokens en circulación) puede proponer una propuesta. La propuesta incluye una descripción de la misma y opcionalmente un enlace web con otros documentos
castVote	cualquier titular de tokens puede emitir un voto ponderado por los tokens en su posesión sobre una propuesta que se somete a votación
delegate	los titulares pueden ceder su voto a cualquier persona
cancel	cualquiera puede cancelar una propuesta si el proponente deja de tener suficientes votos y se ha pasado el plazo de votación

Tabla 6: Atributos obligatorios aplicables a los bonos	
Guarantor identifier	Identidad del avalista-garante (si lo hubiese)
Bondholder representative identifier	Identidad del titular del bono (opcional)
Maturity date	Fecha de vencimiento
Interest rate	Tasa de interés
Par value	Valor nominal
Interest schedule format	las fechas en las que se devengan el pago de intereses (si los hubiese)
Interest payment date	Fecha del pago de intereses si es diferente a la fecha del devengo

Tabla 7: Funciones usadas por las agencias de 'rating' o agencias de calificación de riesgos	
FlagDefault*	Indica el impago de un bono por parte del emisor (habitualmente después del periodo de gracia[3])
FlagDefaultRemove*	Revoca el estado de impago del bono
FlagRedeemed*	Establece que el bono ha sido redimido
SetRating*	Indica la calificación del bono

3 Un período de gracia es un período de tiempo establecido después de la fecha de vencimiento durante el cual se puede realizar el pago sin penalización.

Tabla 8: Funciones para el pago de intereses y principal (complementadas con las funciones de pagos de dividendos)	
DistributionSchedule	Definir un calendario para el pago de intereses (y el reembolso del valor nominal al vencimiento)
DistributionUnschedule	Cancelar el calendario previamente establecido para el pago de intereses (y reembolso del importe del principal al vencimiento)