# Documento técnico de Brickblock

Marius Hanne, Jakob Drzazga, Adrian Kizlauskas, Philip Paetz, Martin Mischke

Versión 0.9.3, 17-07-2017

## Índice



Tener en cuenta que este documento es solamente un borrador preliminar; faltan algunos detalles de implementación o pueden estar sujetos a cambios.

El propósito de este documento es comunicar los aspectos técnicos de nuestra visión y ofrecerle al lector una forma de evaluar la factibilidad de nuestro diseño.

Estamos en el proceso de desarrollo para la implementación de una prueba de concepto y emitiremos un primer prototipo antes de nuestra preventa de agosto. Los detalles de la implementación técnica se agregarán tan pronto como se los decida.

Estamos abiertos a los comentarios y sugerencias de la comunidad y haremos lo mejor para evaluar exhaustivamente todas las opciones y no tomar ninguna decisión apresurada.

# Resumen

Este documento describe una plataforma de contratos inteligentes construida sobre una red informática distribuida globalmente tal como Ethereum o Rootstock. El esquema sugerido de prueba de activos (PDA) permitirá a los usuarios comercializar fácilmente los tokens, que representan diferentes tipos de activos extranjeros en todos los mercados ERC20 compatibles.

La idea básica es crear una cantidad de contratos de PDA y que cada uno represente un activo extranjero diferente. Al conectar el contrato del token a un fondo fiduciario digital (Digital Trust Fund, DTF), habrá una paridad cercana al 1:1 entre el valor del token y el activo extranjero.

Los usuarios pueden comprar tokens de pruebas de activos (PDA) a cambio de moneda local, comercializarlos o conservarlos y recibir una participación de cualquier dividendo que el activo pague.

Los inversores pueden canjear sus tokens de PDA pidiéndole al DTF que liquide los activos extranjeros correspondientes y reembolse su valor de mercado actual en moneda local.


# 1 Descripción

Durante un período de contribución, los tokens de Brickblock (Brickblock tokens, BBT) se distribuirán entre los contribuidores participantes.

Los tokens de Brickblock se pueden comercializar en cualquier mercado, o pueden bloquearse para generar los llamados tokens de acceso (Access Tokens, ACT).

Los tokens de acceso se requieren para pagar las tarifas por operar contratos de PDA y para mantenerlos activos en el tiempo.

Los tokens de PDA representan un cierto activo extranjero disponible para comercializar en la plataforma de Brickblock.

Los activos que respaldan esos tokens son conservados por un fondo fiduciario digital auditable públicamente.

Todos estos tokens implementan la especificación ERC20 y se pueden comercializar fácilmente en mercados compatibles de terceros.

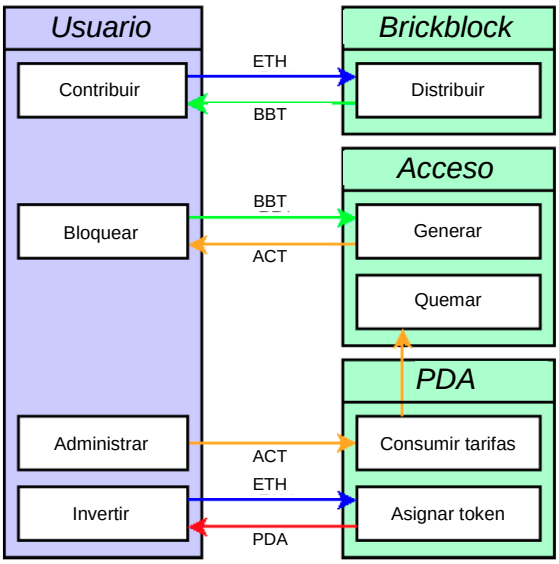


Ilustración 1: Los diferentes tipos de tokens y cómo interactúan

# 2 Brickblock

Brickblock será representada por un contrato inteligente que funciona en la blockchain, la cual maneja el registro de los intermediarios y administra los contratos de PDA individuales.

## 2.1 Token de Brickblock (Brickblock Token, BBT)

El contrato de Brickblock en sí mismo implementa un token compatible con ERC20, el cual será distribuido a los contribuidores de nuestro recaudador de fondos.

Además de ser comercializables, estos tokens se necesitan para generar nuevos tokens de acceso.

## 2.2 Token de acceso (Access Token, ACT)

Los tokens de acceso se requieren para pagar tarifas para operar los contratos de PDA y mantenerlos activos. Solo pueden ser generados al bloquear el BBT en el contrato del token de acceso.

Mientras los BBT estén bloqueados, el contrato acreditará nuevos ACT a la cuenta de los remitentes. La tasa a la cual se generan los ACT aumenta con el tiempo mientras los BBT estén bloqueados. Los ACT generados pueden ser retirados en cualquier momento, sin embargo, hacer esto pone en cero la edad del BBT bloqueado que los generó.

Los tokens de acceso se requieren para operar ciertas funciones de los contratos de PDA, y se destruyen después de su uso. El contrato de PDA informará al contrato del token de acceso la dirección del usuario y el número de ACT requerido. Si el usuario tiene tokens suficientes en su cuenta, la suma solicitada se sustraerá y la operación podrá continuar. Si el saldo no es suficiente, entonces la solicitud arrojará una excepción, y evitará que el contrato de PDA ejecute la función solicitada.

## 2.3 Fondo fiduciario digital (Digital Trust Fund, DTF)

Brickblock configurará un fondo fiduciario digital que conserve los activos que estén respaldando los tokens de PDA en una cuenta de inversión con un custodio.

El custodio certificará las actividades en la cuenta del DTF y publicará las pruebas que permitirán que todos verifiquen que se contabilizan todas las obligaciones.

## 2.4 Tarifas

A lo largo de su duración, un contrato de PDA requiere que varias partes paguen tres tipos de tarifas diferentes como ACT: tarifas por creación, tarifas por liquidación y tarifas por existencia.

Las tarifas por creación las debe pagar un intermediario para crear un nuevo contrato de PDA y ofrecérselo a los inversores.

Las tarifas por liquidación las deben pagar los usuarios en caso de querer canjear sus tokens por moneda local.

Las tarifas por existencia las debe pagar toda persona interesada en la operación continua de los contratos. En caso de no haber interés suficiente para cubrir las tarifas, el contrato suspenderá su operación hasta que se paguen tarifas suficientes para revivirlo. Esto ayudará a eliminar contratos obsoletos y no deseados, y brinda un incentivo adicional a los intermediarios para hacer ofertas atractivas.

El ACT pago se eliminará y, por consiguiente, se retirará de circulación. Brickblock no los guarda ni los comercializa después de que se hayan usado.

## 2.5 Contract Discovery y actualizaciones

Para permitir la actualización de funciones, se podrá acceder a todos los contratos inteligentes a través de un contrato de proxy con una dirección fija.

Los contratos individuales también se pueden suspender, como medida de emergencia, en caso de que se descubra un error informático.

Reconocemos la pérdida parcial de la descentralización real al ser la única parte que controla el mecanismo de actualización. Sin embargo, los tenedores de BBT tendrán la capacidad de vetar y por lo tanto de demorar cualquier cambio que se implemente en la red de producción.

## 2.6 Registro del intermediario

Los intermediarios deben ser aprobados por el equipo de Brickblock y someterse a procedimientos de diligencia debida antes de que se les permita comercializar en la plataforma. El contrato de Brickblock contiene una lista de todos los intermediarios activos actualmente y le permite a la administración de Brickblock agregarlos y eliminarlos. Para agregar un intermediario a la lista, se deben pagar las tarifas de ACT.

# 3 Prueba de activo

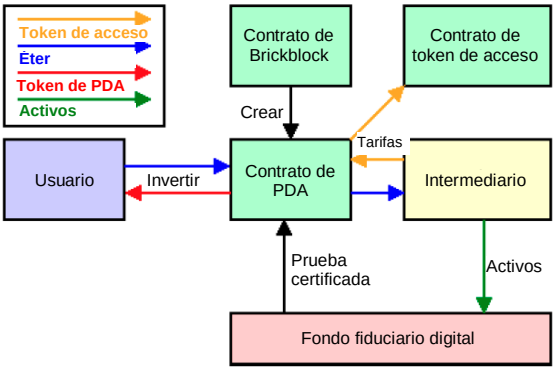


Ilustración 2: El esquema de prueba de activos

El mecanismo de prueba de activos funciona mediante el establecimiento de un "triángulo de la confianza" entre el usuario, el DTF y un intermediario, que se rigen por un contrato inteligente en el que confían todas las partes.

Un usuario paga en moneda local al contrato. El intermediario puede reclamar esta suma una vez que haya enviado los activos solicitados al DTF.

El DTF prueba la recepción de los activos al contrato inteligente, el cual libera la moneda local al intermediario y el token de PDA recientemente creado al usuario.

El usuario puede confiar en que el contrato se active solamente cuando se reciba una prueba de activos válida, o cuando se reembolse el monto inicial.

De la misma manera, el intermediario puede confiar en que el contrato libere los fondos, y debe confiar en que el DTF envíe la prueba de recepción al contrato. La prueba de recepción real será proporcionada públicamente por ese custodio, en quien se debe confiar que no se apropiará indebidamente de los fondos en ningún caso.

Hasta que este proceso haya establecido la confianza con los intermediarios, el DTF asumirá un microcrédito para hacer un atomic swap con el intermediario a través del custodio. En lugar del intermediario, el DTF recibirá la moneda local del contrato inteligente, y la convertirá para cancelar el microcrédito.

El custodio certifica y publica todas las transacciones y saldos de la cuenta del DTF. Esto le permite a los usuarios verificar de manera independiente que todas las responsabilidades del DTF siguen siendo contabilizadas en algún punto en el tiempo. En caso de que haya alguna diferencia, el usuario puede enviar una prueba de fraude al contrato de PDA, lo que generará un bloqueo y suspensión de todas las transacciones.

Los usuarios que deseen comprar tokens de forma inmediata a un precio fijo pueden hacerlo en los mercados externos y arbitrarios de tokens compatibles con ERC20. Esto alivia la carga de adquirir y manipular una cesta con todas las diferentes monedas y le permite a los usuarios simplemente comprar tokens de PDA con una única moneda y sin ningún período de espera, especialmente en el caso de fondos comercializados con monedas (Coin-Traded Funds, CTF).

## 3.1 Creación

Al crear un nuevo contrato PDA, el intermediario define sus parámetros (ver Tabla 1).

Los contenidos de estos campos varían entre los diferentes tipos de contratos de PDA, los cuales se detallan a continuación.

Por ejemplo, un contrato CTF normalmente requiere solo una provisión mínima insignificante. De esta forma, no tiene etapa de financiamiento y no requiere ninguna extensión del contrato, dado que sus nuevos tokens se activan tan pronto son creados.

La información del custodio para un contrato de activos del mundo real es una clave pública del custodio, la cual se usa para firmar las pruebas de activos. Un contrato de activos encriptados requiere una lista de todas las cuentas usadas para mantener las diferentes monedas.

## 3.2 Activación

Para activar un contrato de PDA, debe recibir una prueba válida del custodio sobre la recepción de los activos por parte del DTF.

Para contratos de activos del mundo real, esta prueba es una firma del custodio, que certifica el saldo actual de la cuenta del DTF.

Para contratos de activos encriptados, la prueba se basa en validar la inclusión de una transacción de financiamiento en el blockchain extranjero.

Si no se recibe una prueba válida dentro del tiempo especificado, el contrato devuelve todos los fondos cobrados a los inversores.

## 3.3 Comercialización

Todos los tokens de PDA son comercializables en mercados externos compatibles con ERC20, como con cualquier otro token.

Tabla 1: Parámetros de contratos de pruebas de activos

| | |
|---|---|
| Id. del activo | Identificación del activo, como Número internacional de identificación de valores (International Security Identification Number, ISIN) |
| Nombre y símbolo | Nombre y símbolo del token dentro del ecosistema de contratos inteligentes |
| Provisión mínima | Monto mínimo de financiación inicial requerida |
| Información del custodio | Datos requeridos para validar la prueba del custodio |
| Plazo | Plazo durante el cual se cancela la etapa de financiación si no alcanza el objetivo |

## 3.4 Pago de dividendos

Cuando el activo rastreado por el contrato de PDA rinde cualquier dividendo, estos serán convertidos a moneda local por el DTF, enviados al contrato de PDA y distribuidos entre todos los tenedores de tokens. Los usuarios pueden entonces reclamar su parte de las ganancias en cualquier momento.

## 3.5 Canje

Los usuarios pueden, en cualquier momento, canjear sus tokens de PDA activos por su valor actual en moneda local.

Para hacer esto, el usuario primero debe completar un proceso obligatorio de conocimiento del cliente (Know-Your-Customer, KYC) con Brickblock.

Cuando el usuario devuelve tokens de PDA al contrato, estos recibirán el valor actual del activo rastreado en moneda local. El contrato notificará al DTF, el cual proporciona la moneda local solicitada y liquida la suma apropiada de acciones a través del intermediario.

## 3.6 Extensión

Para extender la base de activos de un contrato de PDA, se puede crear un subcontrato, el cual implementa una nueva ronda de financiación idéntica al contrato principal. Ante la activación, el subcontrato enviará la prueba de activos al contrato principal y le solicitará fusionar los nuevos saldos.

Tener en cuenta que esto solo será necesario cuando la nueva ronda de financiación por sí misma tenga una restricción de provisión mínima. En la mayoría de los casos, los usuarios pueden simplemente comprar nuevos tokens del contrato mientras que el DTF adquiere los activos adicionales necesarios.

## 3.7 Pruebas de fraude

Todas las responsabilidades del DTF serán contabilizadas públicamente de manera que le permita a todos identificar una discrepancia para probar este hecho al contrato de PDA.

Cuando el contrato recibe una prueba de fraude válida, automáticamente bloquea y suspende cualquier actividad.

Salvo que el contrato tenga una prueba de activos nueva y válida dentro de un determinado tiempo, se autodestruirán e invalidarán todos sus tokens.

El contrato volverá a sus operaciones normales después de que haya sido desbloqueado nuevamente.

# 4 Fondos de activos del mundo real

El contrato de fondos de activos del mundo real implementa fondos que están compuestos por activos extranjeros, tales como fondos negociados en la bolsa (Exchange-Traded funds, ETF) y fondos inmobiliarios (Real Estate Funds, REF).

## 4.1 Financiación

El contrato de PDA inicialmente vende sus tokens a inversores a cambio de moneda local, hasta que se alcance la meta de financiación especificada.

## 4.2 Fallido

Si la meta de financiación no se alcanza dentro del tiempo especificado o si la activación caduca, entonces el contrato pasa a la etapa fallida.

Los inversores pueden devolver al contrato sus tokens de PDA comprados y recibirán a cambio su moneda local.

## 4.3 Pendiente

Si se alcanza la meta de financiación, el contrato entra en la etapa pendiente y le informa al intermediario que asegure los activos extranjeros.

El intermediario asegura los activos extranjeros y los transfiere a la cuenta del DTF con el custodio.

El custodio certificará y publicará todas las transacciones en la cuenta del DTF, junto con la correspondiente dirección de contratos de PDA.

El custodio hará eso para activar el contrato de PDA, al firmar criptográficamente una declaración que consiste en lo siguiente:

| | |
|---|---|
| Dirección | La dirección del contrato |
| ISIN | La identificación del activo extranjero |
| Monto | La cantidad de acciones transferidas |

## 4.4 Activación

Si la prueba es válida, el contrato pasa a la etapa activa. Si el contrato no se activa dentro de un determinado espacio de tiempo, pasa a la etapa fallida.

El contrato verifica que la declaración firmada consta de los datos esperados y tiene una firma válida del custodio. Para hacer esto, primero recrea desde su memoria los datos de la declaración esperados y luego utiliza estos datos en combinación con la firma recibida para recuperar la dirección de firma. Si la dirección recuperada es igual a la del custodio, se demuestra simultáneamente que la información es correcta y que la firma fue ciertamente hecha por el custodio. Si los datos de la declaración son diferentes a la información que el custodio utilizó para crear la firma, la recuperación brinda una dirección diferente y el contrato no se activa.

El contrato de PDA notifica al intermediario que sus fondos se compensan. El intermediario puede ahora reembolsar desde el contrato de PDA y recibirá la moneda local cobrada.

## 4.5 Pago de dividendos

Toda vez que el activo rastreado rinda cualquier dividendo, estos serán convertidos a la moneda local y enviados al contrato de PDA.

Los inversores pueden entonces reclamar su participación de los dividendos en cualquier momento.

## 4.6 Canje

Los inversores pueden canjear sus tokens de PDA por el precio de mercado actual del activo rastreado.

Los tokens devueltos al contrato se eliminan, y el DTF solicita al intermediario que liquide los activos asociados.

El DTF convierte a moneda local los fondos recibidos y los envía al contrato, para que el usuario los reclame.

## 4.7 Extensión

Un intermediario puede decidir extender la base de activos de un contrato de PDA existente.

Para hacerlo, el contrato de PDA crea una nueva instancia de sí mismo, la cual se ejecutará a través del mismo proceso de financiación y activación descrito previamente. También compartirá naturalmente con el contrato principal ciertas propiedades, tales como el ISIN y el símbolo.

Una vez que el subcontrato haya completado la financiación, pasa a la etapa absorbida, y el principal se fusiona con los saldos de sus tokens. Dado que el subcontrato sigue exactamente las mismas reglas que el contrato principal, este último puede aceptar los nuevos tokens como válidos e intercambiables con los propios.

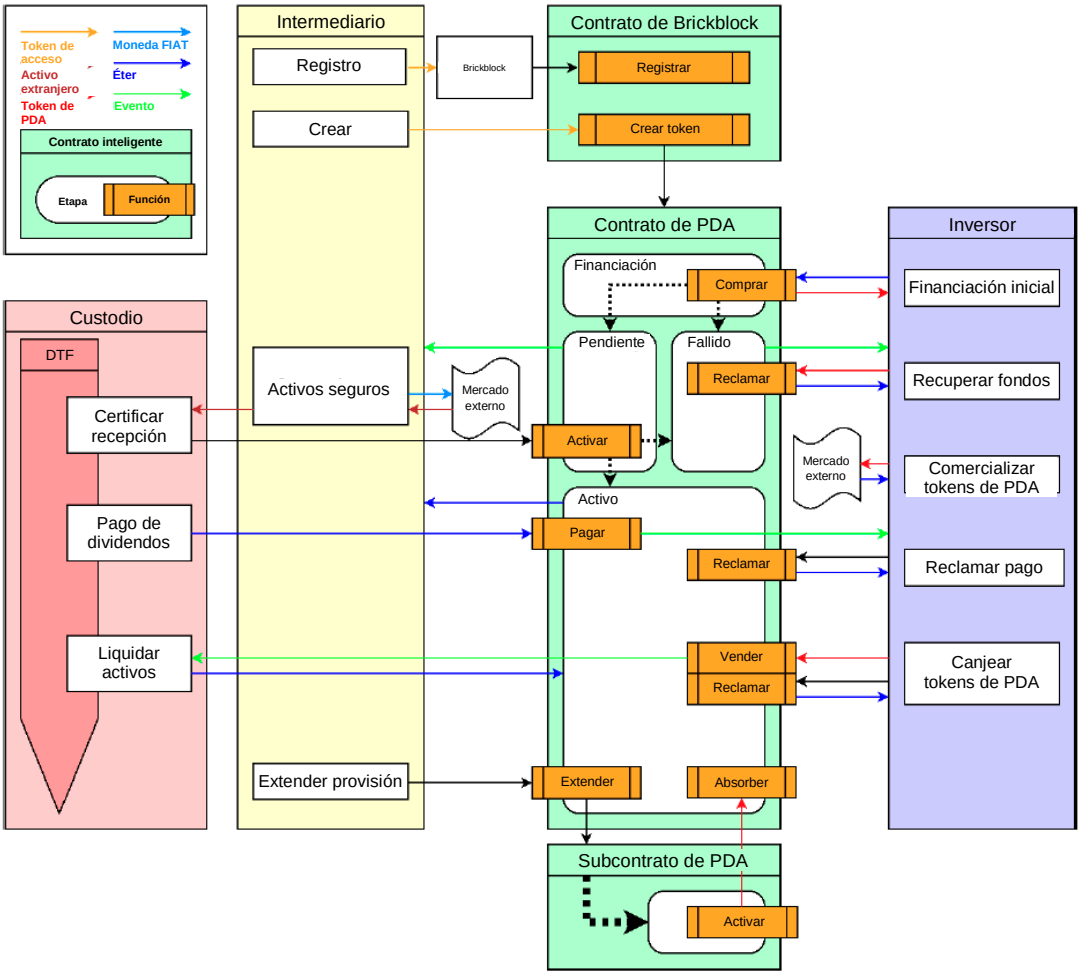


Ilustración 3: Ciclo de vida de un token de prueba de activo para ETF y REF

# 5 Fondos de criptodivisas

Los contratos de fondos de criptodivisas constan de diferentes monedas criptográficas o tokens, tales como Bitcoin, Litecoin, Dash, Ethereum, Golem e incluso BBT o ACT en sí mismas.

Existen tres tipos de contratos: fondos comercializados en monedas (Coin-Traded Funds, CTF), fondos administrados en monedas (Coin-Managed Funds, CMF), y fondos autónomos de monedas (Autonomous Coin Funds, ACF).

Los usuarios pueden comprar tokens de PDA que representen una cierta cesta o monedas extranjeras o locales y tokens.

Esos fondos pueden ser CTF pasivos, que operen bajo reglas predefinidas, o CMF activos, comercializados por un intermediario en mercados asegurados o no asegurados.

En el futuro, esperamos agregar fondos completamente autónomos de monedas que implementen toda la lógica de comercialización dentro del contrato.

## 5.1 Pasivo (CTF)

El contrato pasivo de fondos comercializados con monedas cuenta con una cierta composición de diferentes monedas criptográficas, basada en un conjunto de reglas predefinidas.

Al cambiar la composición de la cesta de creación y canje, el contrato ajusta sus valores en cartera al mercado cambiante.

El custodio responde las solicitudes de cotizaciones (Requests for Quotes, RFQ) para la composición actual de la cesta.

## 5.2 Administrado (CMF)

El contrato de fondos administrados en monedas permitirá a los administradores de fondos comercializar los fondos recibidos en sus propias cuentas o en mercados de terceros.

Los usuarios pueden pagar en cualquier moneda y el administrador del fondo las convierte a la composición deseada.

### 5.2.1 Cuentas aseguradas

Brickblock ofrecerá cuentas aseguradas, en las que los administradores de fondos pueden comercializar en bolsas verificadas y confiables. Estas cuentas tendrán funcionalidad limitada y solo pueden usarse para comercializar. Solo se permiten los retiros hacia el DTF. Esto les permitirá a los administradores de fondos menos confiables ofrecer sus servicios de forma controlada para establecer un registro de seguimiento y ganar credibilidad.

### 5.2.2 Cuentas no aseguradas

Para ofrecer a los administradores de fondos la flexibilidad total que necesitan para desempeñarse bien, se les puede permitir comercializar en sus propias cuentas. Se les proporciona la propiedad total de los fondos y pueden administrarlos de la forma que elijan. Los administradores de fondos pueden opcionalmente proporcionar pruebas de activos si su configuración las soporta, pero esto no es obligatorio.

Los usuarios siempre estarán al tanto del tipo de cuenta y administrador de fondos que aseguran sus inversiones y pueden factorizar esta información en su cálculo de riesgos.

En el futuro, Brickblock proveerá el seguro para las cuentas de custodia o administradores de fondos confiables.

### 5.2.3 Dividendos

Si un fondo rinde dividendos, el administrador de fondos los cobra, los convierte a moneda local y los envía al contrato. Los tenedores de tokens son notificados y pueden reclamar su participación en cualquier momento.

### 5.2.4 Canje

Los inversores pueden canjear sus tokens en cualquier momento y enviarlos de regreso al contrato. El administrador de fondos liquidará las posiciones, las convertirá a moneda local y las enviará al contrato para que el usuario las reclame.

## 5.3 Autónomos (ACF)

También deseamos explorar los contratos totalmente automáticos que se comercializan de forma autónoma entre múltiples blockchains.

Hasta tanto se implemente una vinculación de la moneda de dos vías confiable entre la mayoría de las monedas criptográficas, la única opción para hacerlo es por medio de un intercambio con terceros. El contrato podría interactuar con un programa de aplicación por interfaz (Application Program Interface, API) como shapeshiftbot e intercambiar monedas por sí mismo.

Al permitir a los usuarios enviar algoritmos de comercialización y modelos de mercado implementados como contratos inteligentes, apuntamos a crear un mercado para robots que se comercialicen. Los desarrolladores pueden ofrecer sus resultados y los usuarios pueden elaborar el desempeño e invertir en los contratos preferidos.

# 6 Compatibilidad

Todos los contratos de tokens serán compatibles con la especificación ERC20, la cual hace trivial comercializarlos en bolsas y billeteras compatibles.

Estamos evaluando diferentes opciones para el descubrimiento y la actualización de contratos, y esperamos encontrar una solución común junto a otros proyectos.

Bitcoin y los blockchains derivados serán verificables por el contrato inteligente a través de una verificación de pagos simplificada (Simplified Payment Verification, SPV), por ejemplo BTCRelay.

El motor del contrato inteligente subyacente aún no se ha decidido. Actualmente estamos usando como prototipo el blockchain Ethereum y también evaluaremos sistemas comparables como el Rootstock, Tezos y EOS.

# 7 Glosario

- **Base de activos**: La suma de activos extranjeros administrados por el contrato de PDA.
- **Custodio**: Una organización confiable que conserva las carteras de activos extranjeros del DTF.
- **Fondo fiduciario digital (DTF)**: Una entidad financiera estrictamente regulada que tiene la propiedad legal de los activos en nombre de sus inversores.
- **Activo extranjero**: Un activo que existe fuera del ecosistema Ethereum, es decir, no Ether pero REF, ETF o CTF.
- **Moneda local**: Una moneda local de la plataforma de blockchain, como Ether (ETH) para Ethereum.
- **Tokens de PDA**: Un token inteligente según ERC20, que representa un valor igual a un determinado activo extranjero.