BDVE: MANUAL DE OPERACIONES

CAPITULO I: SOBRE LA MACROESTRUCTURA DEL MERCADO

Artículo 1. Definición

El Sistema Descentralizado de Mercados Encriptados, SIDEME, es un conjunto de contratos digitales que componen la plataforma de negociación de la Bolsa Descentralizada de Valores de Venezuela.

Artículo 2. Sobre la descentralización

En todo momento, por registro público distribuido, puede cualquier persona auditar SIDEME.

Artículo 3. Sobre el Contrato Controlador

Con el fin de garantizar la mayor seguridad y transparencia, se establece como centro del mercado electrónico un contrato digital denominado "Controlador", que tiene la capacidad de alterar algunas variables endógenas del mercado.

Artículo 4. Sobre el Contrato Master

Existe un Contrato Master, que tiene la potestad para realizar cambios en el Contrato Controlador. Este Contrato Master, es un contrato cuyos permisos requieren de multiples firmas provenientes de firmantes autorizados designados por BDVE, protegiendo así el sistema de ataques cibernéticos sobre un único punto de fallo. Para que pueda haber un cambio estructural, debe existir consenso entre los firmantes.

Artículo 5. Sobre los tipos de acciones

a. Para el Contrato Master, son acciones ordinarias aquellas que añaden contratos a SIDEME de forma regular, alterando de forma dinámica su estructura durante el normal desempeño de las funciones del mercado.
b. Para el Contrato Master, son acciones extraordinarias aquellas que realizan cambios concretos, pero importantes, en la estructura de SIDEME, solo en caso de sospecha de una posible vulneración de SIDEME por parte de actores maliciosos o en caso de cambios significativos en lógicas de SIDEME para adaptar el mercado a nuevos paradigmas en el ámbito financiero.

Artículo 6. Acciones Extraordinarias en el Contrato Controlador

Son acciones extraordinarias ejecutables en el Contrato Controlador por el Contrato Master las siguientes:

a. SetOwner: Con el argumento "_new", SetOwner ejecuta un cambio en el Contrato Controlador para traspasar la propiedad de ejecutar cambios a un nuevo Contrato Master. En caso de ataque esta función puede congelarse.

b. SetBackend: Con el argumento "_new", la función ejecuta un cambio en la dirección de apuntado del backend del software de uso público para la conexión a SIDEME. En caso de ataque esta función puede congelarse.

c. setSwitcher: Con el argumento "_new", la función ejecuta un cambio en la dirección de las carteras de apagado.

d. setNewAddress: Con el argumento "_kind", se establece un número entero que funciona como identificador para la nueva dirección a apuntar. Con el argumento "_address" se incluye la nueva dirección. Con el argumento "_isfactory", se establece con una variables booleana si la dirección del nuevo contrato proviene de un contrato Factory o no. Esta función se establece para dirigir la cadena de comunicación entre el ecosistema de contratos de SIDEME. En caso de ataque esta función puede congelarse.

e. setTxCommission: Con el argumento "_newCommission" se puede establecer el porcentaje de comisión dentro del ecosistema de contratos de SIDEME. En caso de ataque esta función puede congelarse.

Artículo 7. Acciones Ordinarias en el Contrato Controlador

Son acciones ordinarias ejecutables en el Contrato Controlador por el Contrato Master las siguientes:

a. setNewToken: Con el argumento "_tokenAddress", se establece la dirección de un nuevo activo financiero en SIDEME. Con el argumento "_category", se designa la categoría del activo financiero que se emite. Con el argumento "_is", se designa si está permitida la negociación del activo financiero o no mediante un booleano. Esta función sirve para autorizar la negociación de activos financieros si y solo si estos han sido aprobados por la SUNAVAL. En cualquier caso la SUNAVAL pueden requerir del deslistado, con lo cual se añade la capacidad de retirar el permiso. En caso de ataque esta función puede congelarse.

b. setNewNFToken: Mismos argumentos que el anterior y mismas capacidades, pero referido a activos financieros no fungibles.

c. setNewPNFToken: Mismos argumentos que el anterior y mismas capacidades, pero referido a activos financieros no fungibles con capacidad de empacado.

d. setNewMarket: Con el argumento "_token1" se establece la dirección del activo financiero a ofrecer en el par del contrato Market (intercambio rápido) determinado. Con el argumento "_token2" se establece la dirección del activo financiero a demandar en el par del contrato Market determinado. Con el argumento "_market" se establece la dirección del contrato Market que se utilizará para el intercambio rápido de los activos financieros anteriores. La función sirve para crear mercados rápidos dentro de SIDEME donde los Participantes pueden ofrecer contrapartida directa. En caso de ataque esta función puede congelarse.

Artículo 8. Sobre el Esquema Diamante en SIDEME

a. Con el fin de preservar la ventaja competitiva del sistema, se establece como estructura de cambio en SIDEME un esquema diamante para implementar nuevas funciones o mejorarlas garantizando la constante actualización de metodologías financieras y tecnologías que mejoren la capacidad de negociar de los Participantes.

b. Existe un Diamond Master, que tiene la potestad para realizar cambios en el Esquema Diamante. Este Contrato Master, es un contrato cuyos permisos requieren de multiples firmas provenientes de firmantes autorizados designados por BDVE, protegiendo así el sistema de ataques cibernéticos sobre un único punto de fallo. Para que pueda haber un cambio estructural, debe existir consenso entre los firmantes.

c. El Esquema Diamante está compuesto por tres tipos de contratos:

   i. Tipo Storage: Contiene el valor de las variables locales de cada Contrato del Ecosistema.
   ii. Tipo Logic: Determina la lógica detrás de cada llamada a una función.
   iii. Tipo Diamond: Sirve de guía para determinar la dirección del Contrato Logic en función de la función a la que el Contrato Storage quiera llamar.

d. En SIDEME es el Contrato Tipo Diamond el Contrato Controlador, que direcciona al resto de contratos al Contrato de Lógicas.

e. En SIDEME es el Contrato Tipo Logic el Contrato de Lógicas, que contiene la dirección del Contrato que determina la función a ejecutar.

f. En SIDEME son Contratos Tipo Storage todos aquellos que almacenan variables.

Artículo 9. Acciones Extraordinarias en el Esquema Diamante

Son acciones extraordinarias ejecutables en el Contrato Controlador por el Contrato Diamond Master las siguientes:

a. SetDiamondOwner: Con el argumento "_new", SetDiamondOwner ejecuta un cambio en el Contrato Controlador para traspasar la propiedad de ejecutar cambios a un nuevo Contrato Diamond Master.

b. diamondCut: Con el argumento "_addresses" se establece un array de direcciones con los Contratos de Lógica permitiendo incluir direcciones para nuevas funciones que el ecosistema pueda utilizar o actualizando las existentes.

c. stopCuts: Sin argumentos, permite al ser llamada la paralización perpétua de toda posibilidad de incluir nuevas funciones en el esquema diamante del ecosistema.

d. stopUpgrades: Sin argumentos, permite al ser llamada la paralización perpétua de toda posibilidad de actualizar las funciones existentes en el esquema diamante del ecosistema.

Artículo 10. Registro de Firmas en SIDEME

Respecto al artículo 4 y 8.b, se establece como firmas ordinarias necesarias para ejecutar una acción de tal tipo, tres registradas en SIDEME; se establece como firmar extraordinarias necesarias para ejecutar una acción de tal tipo, seis registradas en SIDEME.

Se registrará para tal efecto en SIDEME, seis firmas ordinarias y nueve extraordinarias divididas entre diferentes responsables en BDVE cuya identidad permanecerá oculta.

Tanto las firmas ordinarias como las extraordinarias, serán generadas a través de un script diseñado para tal efecto, offline, con claves mnemónicas individuales por cartera firmante, que deberán mantener en secreto los firmantes de forma individual, y offline.

Artículo 11. Uso de Firmas en SIDEME

Para firmar transacciones ordinarias o extraordinarias a través de los Contratos Master y Diamond Master, los firmantes deberán acceder a una serie de scripts y activar ciertos comandos siguiendo reglas estrictas de ejecución.

Primero, uno de los firmantes suscribe un cambio en SIDEME y genera un identificador de transacción para con una función del Contrato Controlador.

Segundo, estando conectado a internet, el firmante debe ejecutar el script "nonce checker" para visualizar el nonce de la cartera firmante que se vaya a utilizar.

Tercero, el firmante deberá acceder al script "offline-signer" para entrar en el módulo de firmas. En ese momento deberá desconectarse de internet, incluir en el formulario las mnemónicas de la cartera firmante y el identificador de la transacción contra la función del Contrato Controlador. Se generará una firma electrónica offline.

Cuarto, el firmante debe borrar las mnemónicas y después, volver a conectarse a internet.

Quinto, el firmante debe acceder al script "send-transaction" para enviar la transacción, interponiendo el identificador de la firma electrónica offline generada en el párrafo Tercero.

Artículo 12. Inmunidad a ataques cibernéticos

Con el fin de garantizar la inmunidad a ataques cibernéticos en SIDEME, se ejecuta el siguiente protocolo para Acciones Extraordinarias:
Primero, las Acciones Extraordinarias podrán aceptar solo una firma cada 24 horas hasta completar las seis firmas.

Segundo, la firma de cualquier tipo de acción, genera eventos que emiten emails a los firmantes, con el objeto de alertar sobre un posible robo o desencriptación de las carteras firmantes.

Tercero, los firmantes siempre deberán ejecutar cambios inconclusos hasta un mínimo de cuatro firmas para las funciones setOwner y setDiamondOwner, con el fin de cambiar de Contrato Master o Diamond Master antes de que se ejecute un cambio en cualquier otra función.

Cuarto, para efectos del párrafo Tercero, los firmantes deberán haber generado Contratos Master y Diamond Master suplentes, así como firmas suplentes para estos previo al funcionamiento de SIDEME.

Quinto, de ser informado un evento relacionado a una acción no consensuada, deberán los firmantes terminar de ejecutar los cambios inconclusos expresados en el párrafo Tercero, inhabilitando los cambios indeseados.

Sexto, en el momento del cambio de los Contratos Master y Diamond Master, deberán los firmantes generar nuevos Contratos Master y Diamond Master suplentes y ejecutar nuevos cambios inconclusos.

CAPITULO II: SOBRE LAS IDENTIDADES DIGITALES

Artículo 13. Sobre los Participantes en SIDEME

Podrán utilizar SIDEME, todos los Participantes definidos en el Reglamento de BDVE, que generen una identidad digital bajo los lineamientos del Reglamento de BDVE.

Artículo 14. Sobre la Identidad Digital en SIDEME

La Identidad Digital en SIDEME, se denomina SmartID. Es un sistema compuesto por una variedad de Contratos que permiten al individuo garantizar que su identidad digital es única y que su capital está asegurado y segregado.

Artículo 15. Componentes Núcleo del SmartID

Son Componentes del Núcleo del SmartID aquellos con potestades transaccionales, siendo estos:

a. Contrato SmartID
b. Contrato Caja

Artículo 16. Componentes Satélite del SmartID

Son Componentes del Satélite del SmartID aquellos que generan Contratos o que sirven como base de datos de la Identidad Digital, siendo estos:

a. Contrato de Registro
b. Contrato Fábrica de Identidades
c. Contrato Fábrica de Cajas
d. Contrato Comprobación de Estado
e. Contrato Servicio de Nombres

Artículo 17. El Contrato de Registro

El Contrato de Registro contiene un registro bidireccional del SmartID y sus hashes. Estos hashes son:

a. El hash de identidad simple: conformado por el registro inicial del Participante, donde tiene que registrar un email o nickname.
b. El hash de identidad completa (hash due diligence o HDD): conformado por el registro completo del usuario.

En el momento de la creación del SmartID, se crea el primer hash, que es inalterable e irreplicable. En el momento de la consignación toda la documentación, se añade el HDD que tiene las mismas propiedades de inalterabilidad e irreplicabilidad del primero.

Artículo 18. Funciones del Contrato de Registro

Las funciones que presenta el Contrato Registro son:

i. SetNewIdentity, que con el argumento "_identity" asocia la dirección del SmartID y "_dataHash" que asocia el hash de identidad simple y de esta forma ambos quedan empatados. El Contrato que tiene privilegios sobre esta función es la Fábrica de Identidades, la cual es controlada por la/las carteras que se asocian al backend de la DApp. De esta forma, cuando un usuario se registra en SIDEME, automáticamente la Fábrica de Identidades activa esta función y crea el vínculo que se almacena en el Contrato Registro.

ii. setNewIdentityDD, que con el argumento "_identity" asocia la dirección del SmartID y "_dataHashDD" que asocia el hash de identidad completa HDD a la identidad del usuario. Son la/las carteras que se asocian al backend de la DApp quienes la ejecutan automáticamente una vez se aprueba el registro completo del Participante.

Ambas funciones pueden ser congeladas en caso de ataque para prevenir el aumento de reputación del Participante.

Artículo 19. El Contrato Fábrica de Identidades

El Contrato Fábrica de Identidades despliega el SmartID y da las órdenes para la creación del resto de registros asociados a un SmartID a través del Contrato Registro. El despliegue se produce de la siguiente forma:

i. Una vez el Participante accede a SIDEME con su correo o nickname, se despliega de forma automática el SmartID.
ii. Se da la orden al Contrato Fábrica de Cajas para que despliegue el Contrato Caja asociado a ese SmartID.
iii. Se registra el correo o nickname en el Contrato de Servicio de Nombres que actúa como peer para el Contrato Caja que se acaba de desplegar.
iv. Se registra el hash simple en el Contrato de Registro para el SmartID que se acaba de desplegar.

Artículo 20. Función del Contrato Fábrica de Identidades

Las función que presenta el Contrato Fábrica de Identidades es "deployIdentity" y tiene cuatro argumentos.

a. "_identityOwner" registra la dirección de una cartera externa creada de forma aleatoria denominada Owner, que es la que representa la voluntad de la identidad. Con esta cartera externa, el usuario ejecuta transacciones a través del SmartID hacia el mercado. Dichas transacciones son acciones ordinarias y dicha cartera se almacena de forma descentralizada en el dispositivo de cada uno de los Participantes en particular, solo durante el periodo de tiempo en el que el usuario está conectado a SIDEME, para borrarse del sistema cuando éste cierra sesión en la DApp.

b. "_identityRecovery" registra la dirección de una segunda cartera externa creada de forma aleatoria, que es la que mantiene el control de acciones extraordinarias. Estas son, todas las acciones pertinentes relativas al Contrato Caja, la variabilidad del Contrato Comprobación de Estado y el cambio de Owner. Esta cartera no se almacena en el dispositivo del Participante y queda siempre offline a no ser que el usuario desee realizar algún tipo de acción extraordinaria.

c. "_dataHash" crea el primer hash asociado al SmartID simple del Participante.

d. "_name" registra el nickname asociado al SmartID cuando el Participante se registra.

La función es controlada por la/las carteras que tienen privilegios al backend de la DApp y puede ser congelada en caso de ataque.

Artículo 21. Contrato Fábrica de Cajas

El Contrato Fábrica de Wallet despliega el Contrato Wallet mediante orden de la Fábrica de Identidades en el momento en el que se crea un SmartID. Tiene una única función "deployWallet" que contiene un único argumento "_identityAddress" que crea el vínculo entre el Contrato Wallet y el SmartID, proporcionando la dirección de este último.

Artículo 22. Contrato Comprobación de Estado

El Contrato Comprobación de Estado realiza las comprobaciones pertinentes para saber si un SmartID puede o no realizar una determinada operación en base al destino de la llamada.

Artículo 23. Estados almacenados en el Contrato de Comprobación de Estado

Tres tipos de Estado son almacenados en el Contrato de Comprobación de Estado:

a. Control de Identidad: El Participante tiene la capacidad de desactivar temporalmente toda la actividad de su SmartID.
b. Bloqueo Transaccional: El usuario puede permitir o bloquear llamadas a Contratos que no formen parte de SIDEME.
c. Control de Caja: Bloquea el nexo entre el SmartID y el Contrato Caja inhabilitando el movimiento de activos.

Artículo 24. Funciones del Contrato de Comprobación de Estado

El Contrato almacena el estado de las variables e indica al SmartID si la transacción es viable o no. Presenta la función "checkState" que tiene tres argumentos. "_state" hace referencia al estado del SmartID desde el cual se hace la comprobación. "_identityDestinationKind" verifica si el contrato al cual se dirige la llamada pertenece al ecosistema SIDEME o no. Si pertenece presenta un número distinto de cero, si no, presenta como identificador cero. "_destination" verifica el estado de la dirección destino de la retransmitida por el SmartID.

El Contrato Comprobación de Estado puede congelarse en caso de ataque.

Artículo 25. Contrato de Servicio de Nombres

El Contrato Servicio de Nombres, es aquel que realiza la conexión entre el Contrato Caja y el nickname. Dicha conexión es determinada en el primer registro por el Contrato Fábrica de Identidades cuando se despliega el SmartID. La función del Contrato es hacer intercambiable el nickname por la dirección Contrato Caja.

Artículo 26. Propiedad del Nickname

Cada nickname posee un propietario. Dicho propietario tiene el derecho de cambiar la dirección del Contrato Caja a la que el nickname apunte, cambiando la naturaleza de su SmartID.

Artículo 27. Funciones del Contrato de Servicio de Nombres.

La función principal del Contrato Servicio de Nombres es "createName", cuyo argumento "_name" registra el nickname del Participante, "_wallet" registra la dirección del Contrato Caja asociado al SmartID del cual proviene el nickname, y "_owner" registra el SmartID del participante.

Artículo 28. Sobre el Contrato SmartID

El SmartID es el puente entre las llamadas que se envíen a un contrato en SIDEME y que identifica la transacción con la identidad del usuario. Es por tanto el factor definitorio de la identidad del Participante en SIDEME.

Artículo 29. Gobernanza del Contrato SmartID

El Contrato SmartID tiene asociadas dos Carteras Externas, que se denominan *cartera propietaria* y *cartera de recuperación*. Estas son creadas de forma aleatoria en el momento del registro de la identidad a través del Contrato Fábrica de Identidades y su definición está expresada en el artículo 20(a)(b).

Tanto la cartera propietaria como la cartera de recuperación pueden recuperarse con un código mnemónico compuesto de 12 palabras, que el Participante deberá custodiar con la debida diligencia offline. Dicho código es proporcionado en la DApp en el momento del registro.

Artículo 30. Comprobaciones del Contrato SmartID

El SmartID comprueba en cada transacción si la retransmisión de la llamada está permitida o no con el Contrato de Comprobación de Estado.

Con cada llamada que se realiza se comprueba si existen los saldos necesarios para ejecutar transacciones en la cartera propietaria. La cartera propietaria deberá tener siempre un saldo mayor a 0.01 unidades de divisa. Si no tuviere al menos 0.01 unidades de divisa, se transferirá, si existieran los fondos, 0.1 unidades de divisa de forma automática desde el Contrato Caja.

Artículo 31. Comprobaciones del Contrato SmartID

El Contrato SmartID tiene las siguientes funciones principales, que son ejecutadas bien por la cartera propietaria o la de recuperación, siguiendo cada caso en particular:

a. Forward: con el argumento "_destination" se incluye la dirección destino de la llamada a retransmitir. Con el argumento "_data" se incluye la función a ejecutar en SIDEME y los argumentos de apoyo en la misma. Permite al SmartID retransmitir una llamada a otro Contrato de forma que el origen sea este preciso SmartID. Esta función, previo a ser ejecutada, comprueba el estado de la permisología de la misma ejecutando la función checkState del Contrato de Comprobación de Estado. Solo puede ser ejecutada por la cartera propietaria.

b. setOwner: con el argumento "_newOwner" establece la dirección de una nueva cartera propietaria del SmartID. Esto permite modificar la cartera propietaria en caso de sustracción del dispositivo, prevención de robo de identidad y otras situaciones de similares consecuencias. Puede ser ejecutada por la cartera propietaria actual o por la cartera de recuperación.

c. setRecovery: con el argumento "_newRecovery" establece la dirección de una nueva cartera de recuperación del SmartID. Esto permite modificar la cartera de recuperación. Solo puede ser ejecutada por la cartera de recuperación actual.

d. setState: con el argumento "_newState" permite un nuevo estado del SmartID, que se registra en el Contrato de Comprobación de Estado y que la función checkState corrobora cuando se va a ejecutar la función Forward.

Artículo 32. Sobre el Contrato Caja

El Contrato Caja es una bóveda digital, descentralizada y customizable, que hace la función de Caja de Valores individualizada, de una forma segura y eficaz. El Contrato Wallet está dominado por el SmartID y solo puede comunicarse con él, creando una capa de protección inviolable y solo traspasable con las llaves privadas de las carteras asociadas.

Artículo 33. Funciones Ejecutables por la Cartera Propietaria del Contrato Caja

Las funciones ejecutables por la cartera propietaria respecto al Contrato Caja:

a. Transfer: Con el argumento "_tokenAddress" se especifica el identificador del activo financiero a transferir. Con el argumento "_to" se especifica la dirección destino de la transferencia. Con el argumento "_value" se especifica el monto de la transferencia". Con el argumento "_data" se puede especificar un concepto a la transferencia. Con el argumento "_kind" se especifica el tipo de transferencia a realizar.

Esta función permite realizar tranferencias de activos financieros entre Participantes. Antes de realizar la transferencia consulta los Estados y la permisología que haya impuesto el Participante a través de otras funciones.

b. exchange: Con el argumento "_sendingToken" se especifica el identificador del activo financiero que se desea intercambiar. Con el argumento "_receivingToken" se especifica el identificador del activo financiero que se desea recibir. Con el argumento "_amount" se define el monto a intercambiar. Finalmente con el argumento "_kind" se clasifica el tipo de intercambio.

   La función exchange emite una órden dirigida específicamente a los Contratos Market.

c. forwardValue: Con el argumento "_tokenAddress" se especifica la dirección del Contrato o activo financiero que se va a transferir. Con el argumento "_amountOrId" se especifica el monto a transferir en el caso de que el activo financiero sea simple (fungible) o el ID del activo financiero a transferir en el caso de que el activo financiero sea complejo (no fungible). Con el argumento "_destination" se especifica la dirección destino de la llamada a retransmitir, y con el argumento "_data" se codifica la función que se va a ejecutar la llamada con los argumentos de la misma.

   Esta función se ejecuta cuando el Participante desea transferir activos financieros a un contrato donde también en la llamada viene especificada la órden requerida por el Participante en dicho contrato.

d. forwardValuePNFT: Con los mismos argumentos que la anterior, forwardValuePNFT es una función que ejecuta el mismo patrón que forwardValue con la especialidad de que está dedicada a los activos financieros complejos empacables.

Artículo 34. Funciones Ejecutables por la Cartera de Recuperación del Contrato Caja

Las funciones ejecutables por la cartera de recuperación respecto al Contrato Caja:

a. limitValue: Con el argumento "_tokenAddress" se especifica la dirección del activo financiero sobre el que va a recaer una limitación transaccional. Con el argumento "_limit" el Participante especifica el monto máximo permitido para transferencias del activo financiero denotado por transacción.

   La función unlimitValue, funciona de forma contraria a la anterior, donde especificando el _tokenAddress se elimina el limite impuesto.

b. limitTo: Con el argumento "_receiver" el Participante especifica la dirección de un SmartID o SmartIDs a los que se vaya a poner una permisión de transaccionalidad. Con el argumento "_isAllowed" puede autorizar o desautorizar las transferencias a un SmartID o SmartIDs específicos, con una variable booleana..

   La función unlimitTo, funciona de forma contraria a la anterior, donde la simple llamada elimina cualquier restricción impuesta a todos los destinatarios.

c. limitDaily: Con el argumento "_tokenAddress" se especifica la dirección del activo financiero sobre el que va a recaer una limitación transaccional. Con el argumento "_limit" el Participante especifica el monto máximo diario permitido para transferencias del activo financiero denotado por transacción. De esta forma el Participante puede controlar mejor sus finanzas, planificar gastos diarios y protegerse de ataques específicos limitando la cantidad de activos transpasables diarios.

   La función unlimitValue, funciona de forma contraria a la anterior, donde simplemente especificando el _tokenAddress se elimina el limite de gasto diario impuesto.

Artículo 35. Responsabilidad del Participante sobre el uso del SmartID

Dado el carácter descentralizado del SmartID y el Contrato Caja, el Participante se hace plenamente responsable de su uso y seguridad, aceptando las condiciones dispuestas para ello en el Reglamento.

Artículo 36. Procolo de registro responsable en SIDEME

Para garantizar la máxima seguridad en el proceso de registro y creación del SmartID, el Participante puede seguir los pasos descritos a continuación:

i. El Participante debe cerciorarse de que no se está registrando haciendo uso de un dispositivo al que se le haya realizado un jailbreak u otros métodos de liberación.
ii. El Participante debe cerciorarse de que no está registrándose en el dispositivo de una tercera persona.
iii. El Participante debe guardar las palabras mnemónicas en lugar seguro, offline.
iv. El Participante debe cambiar la cartera de recuperación por una creada offline no perteneciente a la rama mnemónica de las carteras generadas en el registro simple, previo a realizar un envío de activos financieros al Contrato.

Artículo 37. Procolo de uso responsable de las carteras de recuperación

Para garantizar la máxima seguridad en la firma de cambios donde intervenga la cartera de recuperación, el Participante puede seguir los pasos descritos a continuación:

i. El Participante debe declarar el cambio que desea realizar al SmartID a través de un script habilitado para ello.
ii. El Participante puede activar el script dipuesto para obtener el nonce de la cartera que vaya a utilizar.
iii. El Participante entonces accede al script que habilita la firma offline.
iv. El Participante deberá desconectar el dispositivo de internet y una vez realizado este paso, completar el formulario con las mnemónicas, el nonce y el ID de la transacción.
v. Al firmar offline, se le descargará un archivo txt en el dispositivo con la firma digital. Debe borrar las mnemónicas y volver a conectarse a internet.
vi. El Participante entonces accede al script que ejecuta la firma, inserta en el campo habilitado la firma digital y ejecuta dicha firma, propagando el cambio.

Artículo 38. Procolo de seguridad para el uso de los SmartID

El Protocolo de seguridad descrito a continuación es el recomendado para instituciones financieras, personas jurídicas con diferentes requerimientos de firmantes, carteras controladas por dos o más personas naturales o por representantes de estas donde deba existir consentimiento para la disposición de activos.

i. Siguiendo el Artículo 36(iv), el Participante puede cambiar la cartera de recuperación por un contrato multifirma cuyas carteras firmantes asociadas tengan claves mnemónicas disociadas.
ii. La Identidad Digital del Participante puede estar conformada por dos SmartIDs, uno que el Participante utilice para realizar transacciones con el mercado en general y otra para custodiar los fondos.
iii. En el caso de que el punto 38(ii) sea efectivo, entonces el SmartID que sea utilizado como custodio de los fondos debiera ejecutar la función limitTo del Contrato Caja para limitar las transacciones de dicho custodio al SmartID operativo.

De esta forma, teniendo el Participante solo aquellos fondos de los cuales requiera para hacer efectivas sus operaciones ordinarias en el SmartID transaccional, la posibilidad de un ataque sobre los fondos es reducida significativamente.

Artículo 39. Sobre la emisión de HDDs y las operaciones sujetas

La normativa contenida en el presente manual y el manual de prevención es de aplicación a todos los que trabajan en la BDVE en lo que se refiere a las siguientes operaciones sujetas:

a. cuando se registren SmartIDs completos con HDDs.
b. cuando se deba verificar una cuenta bancaria registrada por un Participante.

Artículo 40. Debida Diligencia en la emisión de HDDs

Todas las medidas que se detallan en los siguientes apartados se refieren a operaciones sujetas. Para la emisión del HDD, el estudio del Participante se inicia con la comprobación de su identidad mediante documentos fehacientes, que permitan conocerle. En ningún caso se podrá asumir un asunto sin haberse seguido previamente las normas de identificación que se establecen a continuación.

Se recabará del Participante su documento de identidad y se conservará copia en el expediente. Se recogerá la manifestación sobre la titularidad real de la operación (personas físicas con posesión o control, directo o indirecto, de más de un 25% del capital o de los derechos de voto de un cliente persona jurídica o que por otros medios ejerzan el control de su gestión). En caso de no existir tales personas, se considerará titulares reales a sus administradores.

Se hará constar si el Participante o sus familiares y allegados desempeñan responsabilidades públicas en la actualidad o durante los dos años precedentes.

Se recabará del Participante con el objeto de verificar la información suministrada la documentación complementaria que, para cada caso, se indica:

a. Participante personas jurídicas:

    - Documentación fehaciente acreditativa de su denominación, forma jurídica, domicilio y objeto social (escrituras, consulta al Registro Mercantil y otros similares).
    - Poderes y la identidad de las personas que actúen en su nombre.

b. Participante personas físicas:

    - Documento Nacional de Identidad, tarjeta de residencia, tarjeta de identidad de extranjero, pasaporte o documento de identificación válido en el país de procedencia que incorpore fotografía de su titular,
    - Documento Acreditativo de Residencia que pudiere ser una factura donde a nombre de la persona donde se muestre la dirección de residencia o cualquier otro documento que muestre dicha información.
    - Poderes e identidad de las personas que actúen en su nombre.

c. Participante Casa de Bolsa y Sociedades de Corretaje de Valores deberán presentar, además de la documentación requerida para las personas jurídicas, el número de providencia expedido por la SUNAVAL.

Se debe mantener una copia de toda la documentación relativa a la identificación de Participantes, incluido el formulario de identificación de Participantes, y deberá ser debidamente archivada y custodiada en un expediente especial.

Se deberá realizar un seguimiento del Participante y, en el caso de Participantes de riesgo superior al promedio, con carácter anual.

Tales medidas consistirán en el establecimiento y aplicación de procedimientos de verificación de las actividades declaradas por los Participantes, según el nivel de riesgo.

No obstante, el empleado de BDVE procederá a identificar al Participante y al titular real en todos aquellos casos no incluidos en los supuestos que le hacen sujeto obligado, si advierte una vez iniciada su intervención circunstancias indicativas de las actividades reales del cliente o del origen de los fondos o de su patrimonio que pudieran inducirle a suponer la existencia de alguna ilegalidad previa.

Artículo 41. Requisitios de emisión de HDDs

Con carácter general, se aplicarán las siguientes medidas de debida diligencia:

- Identificación formal en los términos establecidos en el artículo 38.
- Identificación del titular real.
- Información sobre el propósito e índole prevista de la relación de negocios.
- Información sobre el ejercicio por el cliente o sus familiares o allegados de funciones públicas importantes en el extranjero o en Venezuela, en cargos políticos o equivalentes, actualmente o en los dos años anteriores.
- Será requerida una entrevista telemática para comprobara la identidad formal y la titularidad real con posterioridad al establecimiento de una negociación, sin que transcurran más de 3 meses, cuando se trate de operaciones superiores a cien mil (100.000,00) Euros o equivalente.
- Se revisará la documentación aportada cada cinco años.
- Se realizará el seguimiento de la relación de negocios cada dos años.

Si en el proceso de admisión del cliente concurrieran indicios o certeza de blanqueo de capitales o de financiación del terrorismo, o de riesgos superiores al promedio, no podrán aplicarse estas medidas sino las que correspondan en adelante en el presente artículo.

Con carácter especial, se aplicarán las siguientes medidas de debida diligencia al Participante que presente un riesgo superior al promedio, o sean personas con responsabilidad pública, o sociedades cuyo capital no sea suficiente para la realización de pactos por ciertas cantidades salvo que las fuentes de financiación sean conocidas, o sociedades que hayan sido preconstituidas y la titularidad cambiada:

- Se revisará la documentación obtenida en el proceso de aceptación del cliente cada año.
- Se obtendrá documentación adicional a fin de determinar el origen del patrimonio y de los fondos con los que se llevará a cabo la operación.
- Se obtendrá documentación o información adicional sobre el propósito de las operaciones.
- Se examinará y documentará la lógica económica de la operación.
- Se examinará y documentará la congruencia de las operaciones con la documentación e información disponibles sobre el cliente.
- Se realizará un seguimiento reforzado de la relación de negocios cada año.

Artículo 42. Protocolo de Control de SmartIDs con HDD

El Departamento de Cumplimiento de BDVE efectuará el siguiente protocolo a la hora de ejecutar la debida diligencia:

i. Todo miembro de la Compañía tiene la obligación de examinar con especial atención cualquier operación sujeta, que pudiera arrojar indicios de estar relacionada con el blanqueo de capitales o la financiación del terrorismo, trasladándolo al Departamento de Cumplimiento para que éste decida si procede su comunicación a las autoridades competentes en dicha materia.
ii. Quien hubiera detectado alguna de estas circunstancias lo pondrá, de inmediato, en conocimiento del Departamento de Cumplimiento.
iii. Efectuada la comunicación al Departamento de Cumplimiento, el comunicante quedará exento de responsabilidad. Cualquiera que sea el criterio adoptado por el Departamento de Cumplimiento con respecto a las comunicaciones realizadas, se informará al comunicante del curso que se le dé.
iv. El Departamento de Cumplimiento llevará a cabo las gestiones adicionales de investigación sobre las operaciones detectadas con la máxima profundidad y rapidez posible, mediante la obtención de toda la información y documentación disponibles, y la investigación global de la operativa de los Participantes, contemplando la posible relación con otros clientes o sectores de actividad.
v. A la vista de toda la documentación recabada, el Departamento de Cumplimiento decidirá sobre la procedencia de su comunicación a las autoridades competentes. En caso afirmativo, la operación será comunicada, junto con la documentación que soporte las gestiones realizadas.
vi. De los análisis de operaciones de riesgo (anormales, inusuales o potencialmente constitutivas de indicio o certeza), de las deliberaciones habidas, así como de las comunicadas, se guardará constancia. En especial, dichos registros harán referencia a cada operación estudiada, Participante, identificación, motivo de la alerta, ampliación de datos efectuada si resultara preciso, decisión adoptada de remisión o de archivo y motivo, así como cualquier otro dato o antecedente que, a la vista de la operación concreta, se mostrare relevante para su evaluación.

Artículo 43. Régimen Reputacional de los SmartIDs

Los SmartIDs tendrán un régimen reputacional valorado entre cero y veinte dependiendo de los hashes adheridos a su Identidad Digital, siendo estos:

a. Hash de Identidad Simple: Confiere cinco puntos de reputación.
b. Hash de Identidad Completa: Confiere diez puntos de reputación.
c. Hash de Comprobación de Cuenta Bancaria: Confiere cinco puntos de reputación.

Los tres hashes agregados suman la reputación total de veinte.

CAPITULO III: BDVE EN SIDEME

Artículo 44. Definición

Las presentes disposiciones regulan el funcionamiento de la negociación de los Participantes en BDVE, asi como los procedimientos mediante los cuales se negocian por su medio los valores y documentos representativos de distintos bienes, servicios o productos cuyo origen provienen de cualquier industria permitida por la Ley y son aprobados por la SUNAVAL.

Artículo 45. Tipos de Mercado

En SIDEME se encuentran dos tipos de mercado:

i. El Mercado Primario, donde emisores autorizados pueden ofertar los Valores de forma exclusiva.
ii. El Mercado Secundario, donde cualquier Participante puede ofertar libremente los Valores que tenga en su haber.
iii. El Mercado de Derivados, donde cualquier Participante puede ofertar o demandar diferentes tipos de derivados financieros.

El Mercado Primario se caracteriza por ser uno permisionado, donde BDVE autoriza y da permiso a emisores para que oferten los Valores en divisas específicas que la SUNAVAL haya previamente aprobado.

El Mercado Secundario se caracteriza por ser uno libre, donde los Participantes pueden ofertar o demandar Valores en diferentes divisas sin la necesidad de estar permisionados para tal fin.

Artículo 46. Tipos de Activos

Actualmente SIDEME presenta la capacidad para listar una gama amplia de activos, entre aquellos que representan un determinado activo, o aquellos que representan un valor equidistante a estos. Estos activos subyacentes y sus derivados pueden en la actualidad ser:

b. Derivados sobre Divisas, siendo estos principalmente swaps de tipo de cambio.
c. Materias Primas: Entre estas, metales, minerales, agropecuarios o ganaderos, entre otros posibles, siendo estos principalmente obligaciones o contratos de propiedad reembolsables.
d. Construcción: Entre estos materiales y edificaciones, siendo estos principalmente contratos de propiedad o de servicios.
e. Acciones: Entre estos índices financieros, grandes compañías y pequeñas y medianas empresas, siendo estos principalmente acciones desmaterializadas, derivados financieros sobre estas y fondos cotizados (ETFs).
f. Bonos: Entre estos convertibles, grandes compañías y pequeñas y medianas empresas, siendo estos principalmente obligaciones, papeles comerciales, títulos de participación, pagare bursátil así como cualquier otro valor autorizado por la SUNAVAL y derivados financieros sobre estos.

Artículo 47. Tipos de Contratos

Todos los Valores en BDVE en la actualidad están configurados de tres posibles formas:

i. ERC223: Equivalente al protocolo ERC20 pero con una mejora de seguridad que comprueba que la dirección de envío puede gestionar activos financieros digitales.
ii. ERC721: Especiales para activos no fungibles. Capaces de poder definir diferentes características para un mismo tipo de activo financiero.
iii. Packable: Solución especial desarrollada por el equipo de BDVE que comparte gran parte del código con ERC721, pero añade una capa para que dentro de cada tipo de ERC721 se pueda tener cierto saldo fungible y se pueda gestionar saldos con distinta tipología.

No obstante BDVE podrá aprobar otros tipos de protocolos electrónicos dependiendo de las necesidades específicas de cada activo en particular.

Artículo 48. Sobre el mercado p2p

BDVE es un mercado descentralizado. El traspaso efectivo de valores y capitales se realiza en formato peer-to-peer (p2p), a través de un Contrato de mismo nombre, que actúa como cámara de compensación, garantizando el buen desempeño de las operaciones efectuadas. La estructura del Contrato p2p depende de la naturaleza del activo y su relación con el resto de activos en SIDEME.

Artículo 49. Funciones del Contrato p2p

Son funciones del Contrato p2p, las siguientes:

a. Offer: Con el argumento "_tokens" se especifica un array de direcciones con las direcciones de los activos financieros que compongan el par ofertado. Con el argumento "_tokenId", que solo está disponible para tipos de contratos packable, se establece la clase de activo a ofertar. Con el argumento "_amounts", se establece un array de números enteros con las cantidades ofertadas y demandadas de ambos activos, que luego se traducirá en el precio. Con el argumento "settings", se establece un array de booleanos, donde la primera componente indica si la oferta admite pactos parciales o no, y la segunda componente hace referencia a transferencias de fiat o no. Con el argumento "_limits", se establece un array de números enteros que establece los límites de la oferta; la primera componente indica el mínimo importe permitido por pacto y la segunda el máximo; la tercera indica la mínima puntuación reputacional requerida por el ofertante para que un demandante pueda pactar con su oferta. Con el argumento "_auditor", se selecciona el auditor para la operación en el caso de que esta sea un intercambio por fiat. Con el argumento "_description", el Participante puede optar por aportar información extra en texto plano sobre la operación. Con el argumento "_metadata" se establece un array de enteros de usos varios para la configuración de la oferta en la DApp, como puede ser el país o el medio de pago.

   Esta función permite que el Participante pueda interponer a través de su SmartID cualquier tipo de oferta en los mercados p2p.

   Salvo en el Mercado Primario, donde la opción para interponer la oferta si es permisionada, cualquier Participante puede hacer uso de esta función.

b. cancelOffer: Con el argumento "_offerID" se identifica la oferta a cancelar. Solo puede ser ejecutada por el oferente que haya interpuesto la orden y permite que pueda cancelar la orden.

c. updateBuyAmount: Con el argumento "_offerID" se identifica la oferta a modificar. Con el argumento "_buyAmount" se puede expresar la nueva cantidad demandada, lo que provoca una actualización del precio en la oferta. Solo puede ser ejecutada por el oferente que haya interpuesto la orden y permite modificar una orden existente.

d. Deal: Con el argumento "_offerID" se identifica la oferta a pactar. Con el argumento "_buyAmount" se expresa la cantidad que se pretende demandar dentro de una oferta, si esta admite pactos parciales. Esta función permite que un Participante pueda pactar una oferta en el mercado.

e. voteDeal: Con el argumento "_dealID" se identifica el pacto pendiente. Con el argumento "_vote" el Participante puede definir si ya ha realizado su obligación para con la contrapartida, con un uno;

con un dos el Participante opta por cancelar el pacto. Solo pueden ejecutar esta función el oferente y demandante de una oferta ya pactada pero cuyas obligaciones y derechos no han sido ejercitados.

Artículo 50. Protocolo de Ofertas en el Mercado Secundario p2p

Un Participante puede realizar una oferta en el Mercado Secundario p2p a través de la DApp, a través del siguiente protocolo:

i. El Participante debe especificar el activo financiero que quiere ofertar, teniendo en cuenta las siguientes restricciones:
    a. En el caso de que el activo sea dinero fiat o criptodivisas de una sidechain, solo podrán ser demandados Valores.
    b. En el caso de que el activo ofertado sea tipo ERC721 o Packable, solo podrá demandar el Participante activos tipo ERC223, dinero fiat o criptodivisas de una sidechain.

ii. El Participante debe especificar el activo financiero que quiere demandar, teniendo en cuenta las siguientes restricciones:

    a. En el caso de que el activo demandado sea dinero fiat o criptodivisas de una sidechain, solo podrán ser ofertados Valores.
    b. En el caso de que el activo demandado sea tipo ERC721 o Packable, solo podrá ofertar el Participante activos tipo ERC223, dinero fiat o criptodivisas de una sidechain.

iii. Una vez seleccionado los activos financieros, el Participante deberá especificar qué cantidad desea ofertar del activo ofertado y qué cantidad desea demandar del activo demandado.

iv. Si el Participante seleccionó como oferta o demanda dinero fiat deberá seleccionar entonces:

    a. Si el dinero demandado lo requerirá en efectivo y,
    b. En el caso de no requerirlo en efectivo, deberá incluir una cuenta de banco verificada o no desde donde emitirá o donde recibirá el pago respectivamente.

v. Si el Participante seleccionó como oferta un activo tipo ERC223 o Packable, podrá activar la capacidad de ejecución parcial de la orden, delimitando los montos máximos y mínimos a pactar por la contrapartida.

vi. En el caso de demandar dinero fiat en efectivo, el Participante tendrá la opción de

    a. Especificar el país donde requiere el efectivo.
    b. Especificar la reputación mínima que requiere del demandante.
    c. Especificar el Auditor que requiere para evaluar el pacto en caso de conflicto.

vii. Adicional al punto (vi) y en cualquier otro caso, el Participante podrá definir detalles adicionales en una caja de texto.

Artículo 51. Estructura del Ticket de Oferta para el Ofertante

El ofertante, al tener privilegios sobre el ticket de la oferta, puede acceder a su oferta y cancelarla o cambiar los montos requeridos, alterando el precio. En el Ticket de la oferta verá:

i. Activo ofertado.
ii. Activo demandando.
iii. Cantidad ofertada actualizada, dependiendo de si ya ha habido parte de la oferta pactada.
iv. Cantidad demandada, dependiendo de si ya ha habido parte de la demanda pactada.
v. Precio / tipo de cambio.
vi. Límites mínimo y máximo de la oferta.
vii. En el caso de ser una oferta de o por dinero fiat o criptodivisa de una sidechain, entonces el ofertante podrá ver los requerimientos de recepción de los fondos.

Artículo 52. Estructura del Ticket de Oferta para el Demandante

El demandante puede acceder a su oferta y pactarla. En el Ticket de la oferta verá:

i. Nickname del Ofertante
ii. Reputación por verificación del Ofertante.
iii. Número total de pactos cumplidos e incumplidos.
iv. Número total de cantidades pactadas.
v. Activo ofertado.
vi. Activo demandando.
vii. Cantidad ofertada actualizada, dependiendo de si ya ha habido parte de la oferta pactada.
viii. Cantidad demandada, dependiendo de si ya ha habido parte de la demanda pactada.
ix. Precio / tipo de cambio.
x. Límites mínimo y máximo de la oferta.
xi. En el caso de ser una oferta de o por dinero fiat o criptodivisa de una sidechain, entonces el ofertante podrá ver los requerimientos de recepción de los fondos.
xii. En el caso de ser una oferta de o por dinero fiat o criptodivisa de una sidechain, Auditor del Pacto.
xiii. Detalles adicionales en texto plano.
xiv. Identificador de la oferta.

Artículo 53. Protocolo de Pactos en el Mercado Secundario p2p cuando la oferta y demanda está compuesta por dos activos

Un Participante puede pactar una oferta en el Mercado Secundario p2p a través de la DApp entre activos financieros que no sean fiat o criptodivisas en una sidechain, siguiendo el protocolo descrito a continuación:

i. El Participante localiza una oferta que desea pactar y muestra su interés en la DApp.
ii. En el caso de que la oferta sea por monto completo, el Participante puede aceptar la oferta directamente y pactar, siendo el intercambio de los activos automático.
iii. En el caso de que la oferta sea por monto parcial, el Participante estipula un monto a pactar entre el mínimo y máximo requerido por el ofertante y acepta la oferta, siendo el intercambio de los activos automático.

Artículo 54. Protocolo de Pactos en el Mercado Secundario p2p cuando la oferta o la demanda está compuesta por dinero fiat o criptodivisas en una sidechain.

Un Participante puede pactar una oferta en el Mercado Secundario p2p a través de la DApp, siguiendo el protocolo descrito a continuación:

i. El Participante localiza una oferta que desea pactar y muestra su interés en la DApp.
ii. Si las condiciones son favorables en el ticket y el Participante acepta, se genera un email con los datos de pago y especificaciones de la operación tanto para el demandante como para el oferente, con los datos contenidos en el SmartID de dichos sujetos, y pueden encontrar el pacto pendiente de votación positiva o negativa en la DApp.
iii. El Participante puede revisar los datos de pago en el ticket del pacto pendiente.
iv. Los Participantes pueden establecer contacto por email o por el chat de la DApp.
v. El Participante responsable de la transferencia de dinero fiat o criptodivisas en una sidechain, realiza la transferencia correspondiente y vota a favor del pacto.
vi. El Participante que recibe el fiat o la criptodivisa en la sidechain, confirma la transferencia correspondiente y vota a favor del pacto, liberando los activos financieros bloqueados.

Artículo 55. Protocolo de Pactos en conflicto en el Mercado Secundario p2p.

Puede ocurrir que un pacto, tal y como se describe en el artículo 50, entre en régimen de conflicto cuando:

i. Uno de los Participantes no entre en consenso sobre el status del pacto.
ii. Uno de los Participantes no responda a la aceptación o denegación del pacto, paralizando la operativa.

De esta forma y para evitar el sabotaje del mercado por parte de entes nefarios, solo es permitido un pacto por cada tipo de dinero fiat o criptodivisa en una sidechain.

Si un pacto entra en conflicto, el Participante que no esté de acuerdo o que no reciba respuesta por la contraparte, puede reclamar la ayuda de un Auditor que intervenga en la liberación de los activos financieros bloqueados.

El Auditor se pondrá en contacto con ambas partes del conflicto y requerirá de las suficientes pruebas para definir su postura referente al pacto, que puede ser:

a. A favor del pacto: Liberar los activos financieros bloqueados en favor de la contraparte emisora del pago en finero fiat o criptodivisa en una sidechain, si se comprueba que efectivamente el pago se emitió correctamente.
b. En contra del pacto: Liberar los activos financieros bloqueados en favor del Participante al cual se le bloquearon, por la imposibilidad de efectivamente verificar el pago debido por la contraparte.

Artículo 56. Independencia de los Auditores.

Podrán ser Auditores en BDVE, todos los Participantes considerados Casas de Bolsa o Sociedades de Corretaje. Los Auditores son independientes, en tanto en cuanto asumirán la responsabilidad de la elaboración de Manuales de Auditoría, que serán publicados en la página web de BDVE y que presentarán en contenido los procedimientos que utilicen para verificar las transacciones realizadas entre Participantes.

Artículo 57. Penalizaciones en situación de conflicto.

Serán registrados de forma cumulativa, el número de pactos cumplidos y el número de pactos no cumplidos, así como el número de fondos pactados. Serán considerados como pactos no cumplidos aquellos donde el Auditor decida en contra del voto del Participante en una situación de conflicto. Será considerado como voto en contra la no votación por parte del Participante.