PROVINCIA DE SANTA FE

CFI – CONSEJO FEDERAL DE INVERSIONES

INFORME FINAL

BENEFICIOS DE DESARROLLO DE UNA PLATAFORMA NFT/FT (TOKENS FUNGIBLES Y NO FUNGIBLES) Y ESTUDIO DE GRAVABILIDAD DE LOS MISMOS PARA SANTA FE

CONTRATO DE OBRA EX2022-00097431 - -CFI-GES#DCS

Noviembre 2022

Experto: Daniel José Díaz

Índice de contenidos

Unos de los objetivos centrales del presente proyecto, se basa en alinear al gobierno de la Provincia de Santa Fe, con la dinámica y evolución que están tomando las nuevas tecnologías disruptivas del ecosistema de Blockchain. A ese fin se busca poder planear alternativas de acción y estrategias de abordaje de la problemática.

Para lograr ese fin, en este primer informe se realizará un análisis y descripción de la tecnología de Blockchain, su ecosistema, alcance, funcionalidad, beneficios y riesgos.

Entre otros elementos vamos a relevar, distintos tipos de Blockchain (públicas, privadas, de consorcio, híbridas), Contratos Inteligentes, Billeteras digitales, Infraestructura de Claves criptográficas, Tokens criptográficos, ERC20, NFT (Tokens no Fungibles) y FT (Tokens Fungibles).

La tecnología de Cadena de Bloques en contexto

¿Qué es la Blockchain o Cadena de Bloques?

Melanie Swan: quinto paradigma disruptivo en computación

En su libro “Blockchain: Planos para una nueva economía”, Melanie Swan, expone a la tecnología de Blockchain como el quinto paradigma disruptivo de la computación.

Precedido en los años 70, por el uso de las “Mainframe”, en los 80 por la revolución que generó el acceso universal a las PCs (Personal Computer), en los 90 por la globalización basada en el uso masivo de Internet, en la década del 2000 por las redes sociales y aplicaciones móviles, la autora identifica a Blockchain como el siguiente gran cambio disruptivo (next big thing) que marcará la década de 2010.[1]

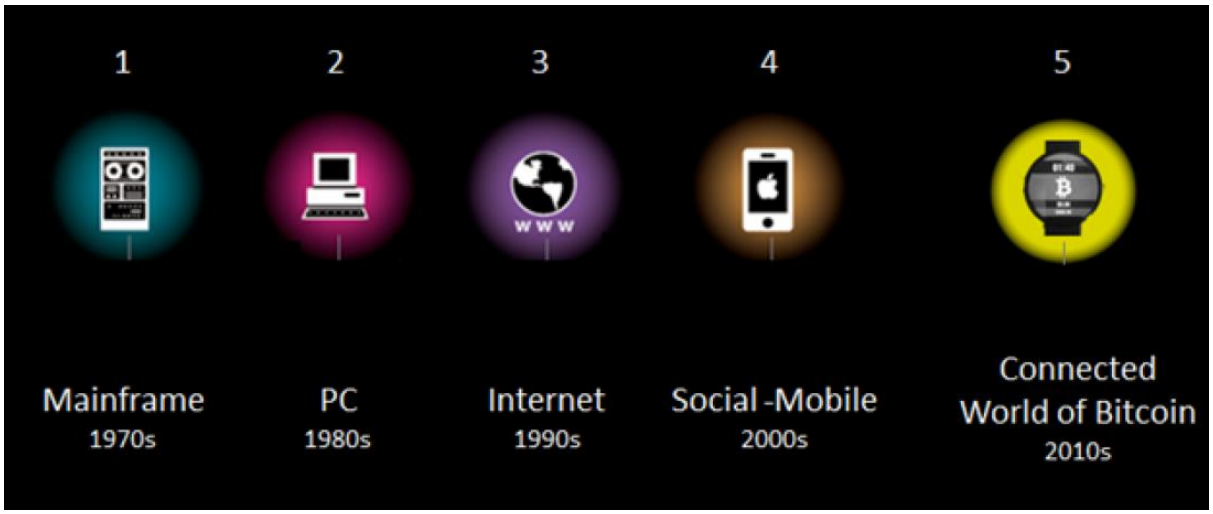


Figura 1 Siguiente gran cambio disruptivo

[1] Swan, M. (2015). *Blockchain: Blueprint for a new economy.* " O'Reilly Media, Inc."

Yuval Harari: 21 lecciones para el siglo XXI

El famoso autor israelí Yuval Harari, autor de “De animales a dioses”, “Homo Deus”, entre otros best sellers, hace referencia en su última obra “21 lecciones para el siglo XXI” acerca de los cambios fundamentales que se espera puedan derivar del uso de las tecnologías vinculadas a la Cadena de Bloques y criptomonedas:

“Mientras tanto, redes de cadenas de bloques entre iguales y criptomonedas como el bitcoin pueden renovar por completo el sistema monetario, de modo que las reformas tributarias radicales sean inevitables. Por ejemplo podría acabar siendo imposible o irrelevante gravar los dólares, porque la mayoría de las transacciones no implicarían un intercambio claro de moneda nacional, o de ninguna moneda en absoluto. Por tanto, quiza los gobiernos necesiten inventar impuestos totalmente nuevos, tal vez un impuesto sobre la información (que será, al mismo tiempo, el activo más importante en la economía y la única cosa que se intercambie en numerosas transacciones). ¿Conseguirá el sistema político lidiar con la crisis antes de quedarse sin dinero?”[2]

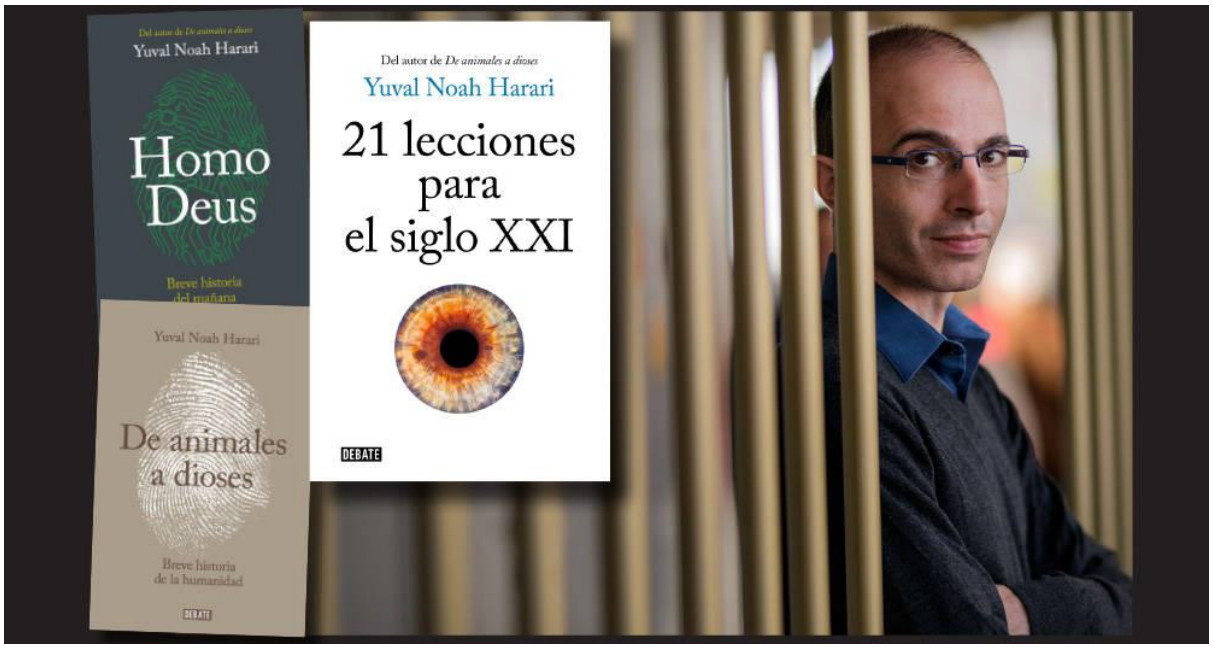


Figura 2 “21 lecciones para el siglo XXI”

Don Tapscott: Internet del valor

Alineado con el planteo de Melanie Swan, en un reportaje, Don Tapscott (uno de los más importantes gurus de IT) definió a la Blockchain, como la segunda era de Internet

[2] Harari, Y. N. (2018). *21 lecciones para el siglo XXI*. Debate.

Tapscott plantea una idea sobre la transformación que está dando en red. Estamos pasando de la "Internet de la Información", hacia la "Internet del Valor".

Tal vez a la fuerza, en este último tiempo, hemos descubierto que todo lo que subimos a Internet, en especial a las Redes Sociales, queda registrado y guardado en forma permanente en algún lugar. Aún con nuestros mejores intentos de borrarlo. Casi sin darnos cuenta, toda nuestra vida, gustos, predilecciones, opiniones, quedan almacenadas en alguna base de datos, para luego ser analizadas.

Pero todo esto es el dominio de la “información”. El nuevo paradigma del que está hablando Tapscott se refiere al dominio del “valor”.

Pensemos en un gigantesco libro contable único, sincronizado, inalterable, validado, copiado y replicado en miles de servidores, donde todas las transacciones financieras que hacemos, quedan asentadas y son accesibles a todo el mundo. Esta es la base de la Internet del Valor. Esta es la Blockchain o Cadena de Bloques

“La tecnología que más parece va a cambiar la próxima década de los negocios no son las redes sociales, el Big Data, la nube, robótica o incluso la Inteligencia Artificial. Es la Cadena de Bloques, la tecnología detrás de las monedas digitales como el Bitcoin”[3]

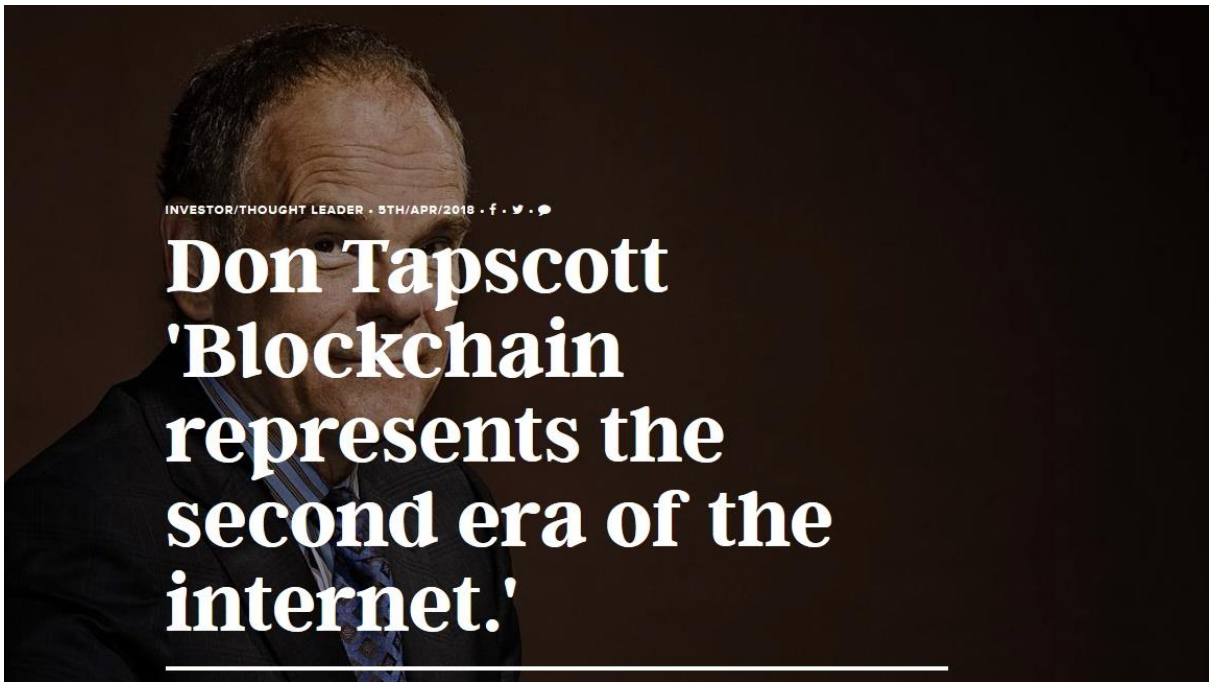


Figura 3 “The impact of the Blockchain goes beyond financial services “

[3] Don Tapscott y Alex Tapscott *“The impact of the Blockchain goes beyond financial services”* Harvard Business Review – 10 de mayo 2016

¿Qué es la Blockchain o Cadena de Bloques?

Podemos comenzar nuestro análisis considerando a la Blockchain o Cadena de Bloques como los PILARES sobre los que se asientan las criptomonedas

Es la tecnología que se desarrolló, originalmente, para poder dar sustento a las criptomonedas. Para que las criptomonedas puedan funcionar.

Es la tecnología que sirve de infraestructura a la funcionalidad de las criptomonedas.

Es importante que iniciemos esta introducción a la Blockchain, desde esta perspectiva, porque vamos a ver que aunque actualmente la tecnología de Blockchain se está utilizando para otras actividades no vinculadas a criptomonedas, los desarrollos que se realizan siguen haciendo uso de elementos propios de funcionamiento de criptos. Por ejemplo, si vamos a desplegar un Contrato Inteligente sobre la Blockchain de Ethereum, deberemos hacerlo por medio de una transacción, tal como cuando transferimos una cantidad de criptomonedas de una cuenta a otra.

¿En qué consiste esa tecnología? vamos a ver una primera aproximación analizandola desde esta perspectiva:

La Blockchain o Cadena de Bloques es:

1. Una red de pares (P2P), totalmente distribuida.
2. Una gigantesca Base de Datos distribuida y sincronizada
3. Un libro contable (Libro Diario) replicado en miles de servidores, y también sincronizado. Se le denomina DLT (Distributed Ledger Technology)
4. Un sistema de registros de transacciones INALTERABLE
5. Un gigantesco computador (procesador) con capacidad de ejecutar programas a los que llamamos Contratos Inteligentes (no todas las Blockchain tiene esta capacidad)

Dejemos estas 5 ideas por ahora. Veamos en esta parte de una introducción básica a como funciona la tecnología de Blockchain.

Monederos o billeteras digitales

La manera más común, con la cual los usuarios van a interactuar con la Blockchain, es por medio de una billetera digital de criptomonedas (Wallet).

Podemos decir que la billetera digital va a ser la “interfaz del usuario”, es decir, lo que la persona va a ver, ya que la Cadena de Bloques no va a ser vista, salvo que se desee acceder en forma directa a la misma, por medio de un software o web especializado.

La billetera digital va a generar y administrar 3 elementos criptográficos básicos:

La clave privada del usuario. Es secreta. Va a quedar almacenada en la billetera, con acceso restringido solamente al usuario, ya que es la que va a permitir firmar las transacciones, es decir, transferir sus criptomonedas.

La clave pública y la dirección (derivada de la anterior), que va a ser la que se difunda por toda la red, y va a servir para identificar la cuenta que va a recibir criptomonedas.

De esta manera, el poseedor de una criptomoneda “firma” con su clave privada (secreta) una transferencia de criptomonedas hacia la dirección de otro usuario. De esta forma se conforma una transacción.

La billetera digital va a preparar y firmar una transacción para enviarla a la Blockchain.

Transacciones

¿En qué consiste una transacción?

En su formato básico, es algo tan sencillo como indicar que cuenta sale una cantidad de criptomonedas, para ir a otra cuenta.

Figura 4 Ejemplo de Transacción

Las transacciones en la Blockchain responden al formato de un asiento contable. En la forma más elemental, con dos cuentas. Una que se debita y otra que se acredita. Pero no necesariamente debe ser así, sino que puede haber varias cuentas de las que salen criptomonedas, las cuales son transferidas a una o varias cuentas distintas.

Figura 5 Ejemplo de Transacción de varias cuentas

En la imagen se puede observar una transacción con 3 cuentas de salida, y 4 cuentas de entrada sobre la Blockchain de Bitcoin.

También se debe considerar que por cada transacción se debe pagar un porcentaje variable a los mineros. Ese porcentaje recibe el nombre de FEE (en el caso de Bitcoin), o de GAS (en el caso de Ethereum), para mencionar solamente a las Blockchains más utilizadas.

Una vez que la billetera preparó y firmó la transacción la va a enviar a la Blockchain. La transacción va a impactar en cualquier servidor de la red y lo que este servidor va a hacer es lo siguiente:

- Leer la transacción
- Validarla
- Registrarla (solo si fue validada)
- Difundirla (va a enviarla a 4 o 5 servidores más de la Blockchain)

Cada nuevo servidor que reciba esa transacción va a volver a hacer lo mismo. Leerla, validarla, registrarla y difundirla. Es decir, la va a enviar a 4 0 5 servidores más, para que vuelvan a hacer lo mismo.

De esta forma, por medio del proceso de divulgación, en pocos segundos todos los servidores de la red van a tener registrada la transacción, quedando esta copiada redundantemente en toda la Blockchain. Al escribir el presente informe la Blockchain de Bitcoin reportaba unas 200.000 transacciones por día.

Mineros

El siguiente paso es la intervención de los mineros en la Blockchain. Pero antes de ver esto, debemos dar una definición, vinculada con las transacciones, y es la de MEMPOOL.

En la Cadena de Bloques, se denomina MEMPOOL al juego de transacciones que fueron validadas y registradas, pero todavía no han pasado por el proceso de mineración, que es una tarea propia a realizar por los mineros.

Para facilitarnos la comprensión, vamos a llamar al MEMPOOL como "la canasta de transacciones pendientes de minerar".

Minería de Bloques

La minería de bloques es el proceso que realizan algunos servidores de la red de Cadena de Bloques a los que, justamente, se los denomina “mineros”.

¿En qué consiste el proceso de minado?

Los mineros seleccionan de la MEMPOOL (lo que denominamos la canasta de transacciones pendientes de minerar) grupos de transacciones pendientes de ser minadas. Sobre ese grupo de transacciones se va a aplicar un considerable poder de cómputo para lograr la resolución de un “acertijo” que solo se puede obtener por medio de “prueba y error”.

Consenso. POW - Prueba de Trabajo

Este trabajo se basa en criptografía avanzada, y tiene como objetivo obtener un “resumen” cifrado, de las transacciones del bloque que se está minando. El resumen se logra por medio de la técnica de encriptación denominada Hash, y constituye la llamada Prueba de Trabajo

(PoW). El minero que resuelva la POW antes, ganará la competencia con otros mineros y podrá incorporar una nuevo bloque a la Blockchain, siendo retribuido con un premio que consiste en obtener nuevos bitcoins generados por la red (programados).

En la actualidad, los nuevos Bitcoins que son asignados a los mineros que ganan la competencia, es de 6,25 BTCs, que son generados aproximadamente cada 10 minutos.

Además de estos nuevos Bitcoins, el minero obtendrá un FEE (Comisión), un premio adicional porcentual al importe por cada una de las transacciones minadas en el bloque. Por medio del mecanismo de consenso un nuevo bloque es agregado a la Cadena de Bloques.

Más adelante mencionaremos que la POW (Prueba de trabajo) no es, actualmente, el único "mecanismo de consenso" que disponen las Blockchains. Especialmente por el impacto que ha tenido recientemente el cambio de consenso de la red Ethereum. Pero para hacer más simple y entendible esta primera aproximación al funcionamiento de la Cadena de Bloques, vamos a dejar este tema para desarrollar más adelante.

¿Cuál es el sentido de pedirles a los mineros este considerable uso de recursos computacionales para realizar el proceso de minado?

Los mineros compiten entre sí, para realizar el proceso de minado antes que los otros mineros, y de esa forma obtener el premio. Este esfuerzo computacional es el que asegura a la red la imposibilidad de ser hackeada y falsificar las transacciones que se registran en la misma.

Si alguien quisiera hackear la Blockchain, necesitaría hacerlo con un poder de cómputo igual o superior al de los mineros, hackear el 50% de los servidores de la red simultáneamente, y todo esto, en menos de 10 minutos, que es el tiempo que la red demora en incorporar un nuevo bloque, y hacer que todo cambie.

Esto nos sirve para perfilar la primera idea que debemos tener en cuenta al evaluar la tecnología de Blockchain: su invulnerabilidad

Visión global de proceso

En este punto podemos considerar lo siguiente:

Pensemos en un gigantesco libro contable único, sincronizado, inalterable, validado, copiado y replicado en miles de servidores, donde todas las transacciones financieras que hacemos, quedan asentadas y son accesibles a todo el mundo.

Fork - Bifurcación de la Blockchain

Por último, en referencia a la Cadena de Bloques, mencionemos que, a veces dos mineros diferentes intentan incorporar bloques diferentes a la Blockchain, al haber sido minados simultáneamente.

En este caso se produce una ramificación temporaria de la Cadena de Bloques que se denomina Fork. Esta ramificación de la Blockchain es temporal y la red termina resolviendo, al minarse el bloque siguiente, cuál de las ramas es la válida, y descarta la otra ramificación.

Una visión gráfica del funcionamiento de la Blockchain

La siguiente figura nos muestra un esquema simplificado de los procesos descriptos:

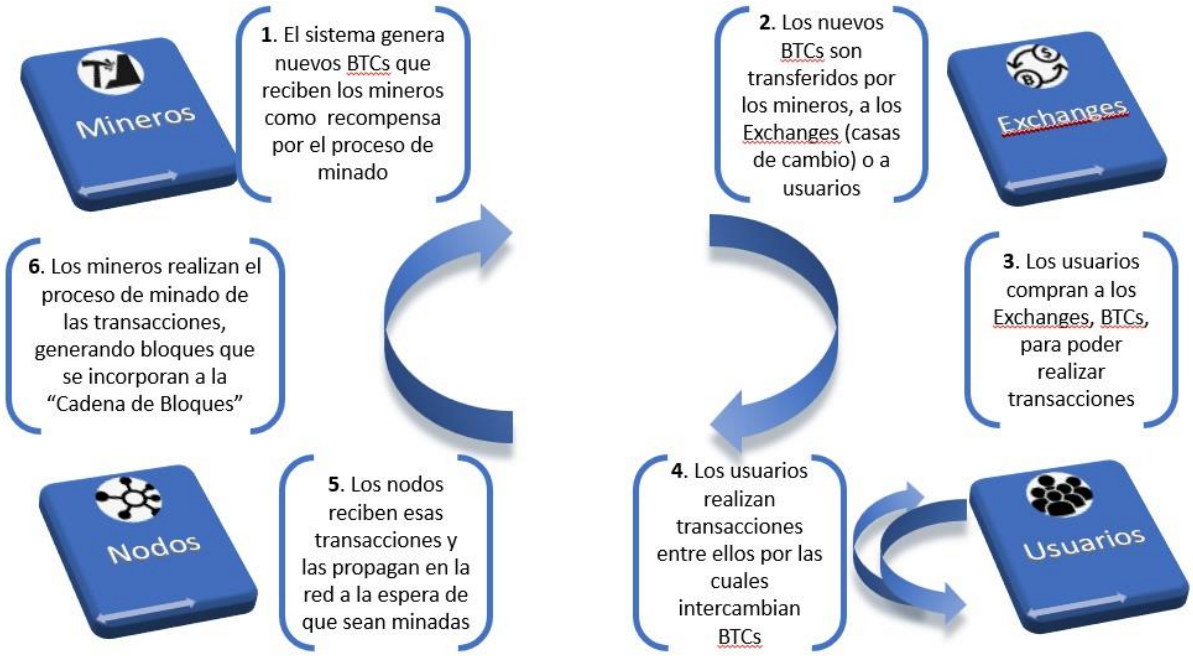


Figura 6 Esquema simplificado de los procesos

El gráfico tiene algunas simplificaciones que corresponde aclarar:

En el punto 2, vale destacar que no necesariamente los mineros van a transferir los nuevos Bitcoins generados por la red, "solamente" a los exchanges, sino, que también podrían ser transferidos a otros usuarios regulares de la red.

En el punto 5, debemos aclarar que las transacciones a ser minadas, no son solamente las transferencias entre usuarios, sino que también incluyen las transferencias de los mineros a los exchanges, y las compras de Bitcoins que los usuarios hacen a los exchanges. Es decir, todas las transacciones que se realizan en la red, de cualquier tipo, van a ser minadas.

Contratos Inteligentes

Hasta aquí vimos el funcionamiento básico de la Cadena de Bloques en criptomonedas, especialmente, en el Bitcoin. Ahora vamos a incorporar a estas definiciones el funcionamiento de la Cadena de Bloques para soportar los contratos inteligentes y sus derivaciones.

En el año 2015, un joven de 23 años canadiense (de padres rusos) llamado Vitalik Buterin propuso el desarrollo una red de Cadena de Bloques específica denominada Ethereum. La red sustenta su propia criptomoneda, el Ether, pero la característica que la distingue es su capacidad de ejecutar contratos inteligentes.

Vale decir, incorpora la capacidad a los servidores de la red de ejecutar lógica contenida en pequeños programas. En las propias palabras de Vitalik:

"funciona de la misma manera que funciona Bitcoin, excepto que, la diferencia es que Ethereum tiene un lenguaje de programación incorporado" Vitalik Buterin

El lenguaje de programación al que hace referencia Vitalik se denomina "solidity" (no es el único, pero sí el más utilizado para desarrollar contratos inteligentes), y su principal objetivo es el de poder programar la lógica de un contrato inteligente, es decir, transacciones sobre la Blockchain, que se ejecutarán si se cumplen determinadas condiciones, se produce un evento, o simplemente en el plazo del tiempo.

Este tipo especial de Cadena de Bloques, abre una nueva dimensión al desarrollo de Aplicaciones Distribuidas (DAPP) ya que estas gozan de la infraestructura necesaria para que todos los servidores ejecuten los contratos que se han registrado en la Cadena de Bloques. Por otra parte, y al mismo tiempo, cuentan con la infraestructura de una base de datos distribuida, implementada por los registros almacenados en la Blockchain.

Las Blockchains que soportan Contratos Inteligentes, como Ethereum, permiten crear Tokens. Podemos definir, en el ámbito de Blockchain a un Token como la representación digital, sobre una Blockchain, de un bien, derecho o servicio. En la mayoría de las ocasiones los tokens se vinculan a la creación de nuevas criptomonedas, pero como vemos, su definición es tan amplia, que puede abarcar la representación digital de cualquier bien o derecho sobre la Cadena de Bloques.

Al poder crearse una nueva criptomoneda, por medio de un Contrato Inteligente, se han desarrollado sistemas de financiación por medio de las denominadas ICO (Initial Cryptocurrency Offering - Oferta Inicial de criptomoneda). Por medio de este tipo de desarrollos se vincula una nueva criptomoneda a un proyecto de inversión o a un emprendimiento determinado.

El desarrollo de este tipo de Cadenas de Bloques, ha dado origen a "marcos de trabajo" (Frameworks), con capacidad de facilitar el acceso y el desarrollo de contratos inteligentes para diferentes usuarios. Tal vez, el más reconocido de estos proyectos (en realidad incluye a varios proyectos) es "Hyperledger", el cual es soportado por la Fundación Linux, y posee apoyo e impulso de IBM.

Podemos también mencionar a otros Framework como Corda R3, o Quorum.

La promesa más ambiciosa, que se deriva de la implementación de contratos inteligentes, es el desarrollo de las denominadas DAO (Organizaciones Autónomas Descentralizadas), organizaciones basadas en contratos inteligentes que se autoejecutan inexorablemente.

Por último, cabe mencionar que, de acuerdo a las necesidades específicas por las cuales se va a utilizar una Cadena de Bloques, podemos encontrarnos en la necesidad de realizar cambios en la programación del “core” (el núcleo de programación) de la misma.

Más adelante veremos, que al modificar el "core" de programación de una Blockchain, podemos generar redes públicas, privadas o de consorcio, según el fin específico y los requerimientos funcionales que definamos para las mismas.

Para finalizar esta primera visión resumida del ecosistema de la Blockchain, vamos a esbozar una definición. Podemos decir que la cadena de bloques es:

“Una cadena de bloques es un libro contable abierto, transparente y distribuido que permite a los usuarios transferir de forma segura unidades de propiedad y puede registrar de manera eficiente y permanente las transacciones entre los usuarios. Blockchain es una red de dispositivos llamados "nodos" conectados entre sí a través de Internet.”[4]

Analicemos esta definición paso por paso:

Una cadena de bloques es un libro contable abierto, transparente y distribuido: en inglés se utiliza el término “distributed ledger” que hace referencia a un libro contable distribuido.

que permite a los usuarios transferir de forma segura unidades de propiedad: este registro o libro contable, va a guardar todas las transacciones que se realizan entre individuos, indicando cada cantidad de criptomonedas que pasan de una mano a otra. Es de destacar que la Blockchain puede guardar cualquier tipo de información, y no solamente transacciones entre usuarios como lo hacen las criptomonedas. Por este motivo, cuando hablemos de BTC (Bitcoins), estaremos hablando de una Blockchain específica que brinda infraestructura tecnológica a ese criptomoneda, pero no de la generalidad de todas las Blockchains.

puede registrar de manera eficiente y permanente las transacciones entre los usuarios: las transacciones que mencionamos como ejemplo, en el párrafo anterior, se agrupan en bloques. Cada bloque de transacciones que se registra en el Blockchain, hace referencia al último bloque, que previamente al que se va a registrar, fue registrado. De este modo, todos los bloques hacen referencias al bloque anterior, uno a uno, de modo que se compone una cadena de eslabones de información.

Blockchain es una red de dispositivos llamados "nodos" conectados entre sí a través de Internet: parece tal vez una obviedad, pero no está demás destacar que la Blockchain es una tecnología desarrollada para correr sobre la infraestructura de Internet. Es decir, no es una red independiente de Internet. El carácter particular que reviste es el de ser una red distribuida, donde todos los nodos tienen igual importancia, sin que exista un servidor central que dirija la red.

---

[4] Panda, S. K., Elngar, A. A., Balas, V. E., & Kayed, M. (Eds.). (2020). *Bitcoin and blockchain: History and current applications*. CRC Press.

Billeteras digitales

Una billetera es un software, que puede integrar componentes de hardware, y que se encarga de:

- Gestionar el acceso al dinero criptográfico que posee el usuario
- Manejo de claves y direcciones
- Conducir el balance las criptomonedas
- Crear y firmar transacciones

Como ya mencionó anteriormente la red de Cadena de Bloques, en nuestro caso la de Bitcoin (recordemos que existen diferentes criptomonedas y cada una tiene su propia Bockchain), corre sobre la red Internet e implementa un protocolo propio. El modo con el cual los usuarios van a interactuar con la Blockchain de Bitcoin, es por medio de sus billeteras, es decir que la billetera actúa como “interfaz” del usuario. Es decir, son las ventanas, que el programa le va a mostrar y con las que el usuario va a interactuar.

Cabe en este punto aclarar, que, si bien las billeteras o monederos digitales son la forma más común de interactuar con una Cadena de Bloques específica, no es la única forma de hacerlo.

Podemos accesar en forma directa a una Cadena de Bloques, por medio de una API específica y también podemos realizarlo por medio de llamadas JSON-RPC

Tipos de billeteras de criptomonedas

Podemos clasificar a las billeteras de criptomonedas según la plataforma en que corren en:

Billeteras de escritorio: las billeteras de escritorio fueron las primeras en ser desarrolladas. Corren como un programa instalado en la computadora. Al igual que cualquier otro programa stand-alone que corre en la computadora, las billeteras de criptomonedas interactúan y dependen en sus funciones del sistema operativo en que corren. Esto vincula a la billetera con las posibles vulnerabilidades que posea el sistema operativo con el que interactúan.

Billeteras móviles: son desarrollos hechos para correr en dispositivos móviles, como Smartphones o tablets. En general su diseño es intuitivo y de facilidad de uso, a fin de que los usuarios puedan utilizar estas billeteras para realizar rápidamente pagos.

Billeteras web: basadas en aplicaciones de interfaz web, es decir, que debemos accederlas por medio de un navegador Web. En este caso los datos y claves e identidades quedan en un sitio web gestionado por un tercero de nuestra confianza.

Este es el tipo de billeteras que comúnmente nos va a ser ofrecido por los Exchanges que realizan “custodia” de las criptomonedas que nos venden.

Billeteras de Hardware: a diferencia de los otros tipos de billeteras, estas basan su fortaleza y seguridad en gestionar las claves, identidades e información de criptomonedas por medio de dispositivos autónomos de propósito específico.

Billeteras de papel: parece una incoherencia el hecho de gestionar moneda electrónica por medio de papel. Sin embargo, el fundamento de este tipo de tipo de billetera radica en que las claves que se generan quedan únicamente respaldadas en el papel impreso, y de esta manera, no están expuestas al riesgo de poder ser hackeadas. El procedimiento para trabajar con este tipo de billeteras es el siguiente:

1) Se debe preparar un disco de booteo con un sistema operativo (preferentemente Linux) completamente limpio, es decir, descargado o comprado sin ningún software adicional instalado.

2) Iniciado el sistema operativo, se debe navegar por internet a una página web que posea capacidad de generar claves para gestionar criptomonedas, desde el lado del cliente, es decir sin necesidad de comunicarse con el servidor. Por ejemplo la página: https://www.bitaddress.org

3) Una vez que se esa página se cargó en el navegador, se debe cerrar la conexión con Internet para así asegurarnos que ningún malware capture la información de las claves que se van a generar.

4) Desde la página, sin conexión, se debe generar las claves e imprimirlas. De este modo la información de las claves generadas no quedará almacenada en el disco rígido de la computadora, ni en el servidor ya que la página web trabajará solo del lado cliente sin intercambiar información con el servidor. El único respaldo de las claves que se generaron será el papel impreso con las mismas, el cual deberemos llevar a un Exchange para poder comprar o vender nuestras criptomonedas.

De las características que describimos se puede deducir que las billeteras papel tienen un alto grado de seguridad para no poder ser hackeadas, ya que el único respaldo de las claves generadas con las mismas son el papel impreso.

A diferencia de las billeteras móviles o basadas en hardware, las billeteras papel, son claramente muy incómodas, o prácticamente inútiles, para realizar transacciones recurrentes con criptomonedas. Por ejemplo, si quiero usar mis criptomonedas para comprar un café, contratar un servicio, o adquirir cualquier bien en negocios que reciban criptomonedas, deberé introducir mi clave privada, que se encuentra impresa en papel, en alguna computadora donde por medio de una billetera de software se genere la autorización para realizar la transacción.

Aparte de la incomodidad de esto, estaré exponiendo mi clave privada a una vulnerabilidad de hackeo, que es claramente lo que trato de evitar con este tipo de billeteras.

Por todo esto es que las billeteras papel son recomendadas para “atesoramiento” de criptomonedas.

El segundo tipo de billetera que se puede considerar más seguro son las billeteras de tipo hardware. En este tipo de billeteras la gestión de claves se realiza por medio de hardware de uso específico y autónomo, que elude las posibilidades de ser hackeado desde la computadora en que corren. Este tipo de billeteras, a diferencia de las billeteras papel, son apropiadas para realizar transacciones (compra, venta, transferencia) de criptomonedas.

Siguiendo un ordenamiento de las billeteras más seguras, podemos mencionar a las billeteras web. En este caso se puede pensar en la aplicación de consistentes políticas de seguridad informática integrada, en los servidores que nos brindan el servicio de almacenamiento y gestión de claves. Otro factor por considerar en beneficio de este tipo de soluciones es la facilidad de actualización e implementación de mejoras que las firmas que ofrecen este servicio nos pueden brindar.

Por último, tenemos las billeteras de escritorio y las móviles. Estas últimas conllevan una clara facilidad de uso, al poder incluirse como una aplicación más en el teléfono inteligente, y por medio de la misma poder realizar compras en forma rápida y directa.

Tipos de Blockchain – Criterios

Antes de realizar una clasificación y explicación de los distintos tipos de Blockchains nos parece importante analizar:

1. El criterio que aplicaremos para definir las categorías de la clasificación

2. La utilidad que esta clasificación tiene para poder analizar el desarrollo e implementación de Contratos Inteligentes.

En referencia al criterio que utilizaremos para desarrollar la clasificación de diferentes tipos de Blockchains, debemos tener en cuenta, como hilo conductor, el concepto de DLT – Distributed Ledger Technology (Tecnología de Registro Contable Distribuido).

Podemos considerar a la Blockchain desde tres perspectivas:

1. Una gigantesca base de datos distribuida y sincronizada, que mantiene un registro actualizado de todas las transacciones de criptomonedas que se realizan en la misma.

2. Una red gobernada por un protocolo específico

3. Un software que corre distribuido en miles de servidores

Si ponemos foco en la primera perspectiva, la de “una gigantesca base de datos distribuida”, debemos tener en consideración que todos los nodos (servidores) de la Blockchain, tendrán una copia actualizada y sincronizada de la totalidad de las transacciones que se hicieron en la Cadena de Bloques, desde su inicio. Cada Blockchain, prevé el mecanismo mediante el cual se llega a un consenso para aceptar los nuevos bloques de transacciones que se incorporan a la cadena, y de este modo, se mantienen actualizadas y sincronizadas todas las copias de Cadena de Bloques, en todos los servidores.

A este mecanismo es el que hace referencia el concepto DLT, con la sigla D proveniente de Distributed.

La segunda mención que se hace en el término DLT, es referida a “Ledger Technology” o Registro Contable. Si bien se ha generalizado la denominación de “contabilidad distribuida” para designar a las Cadenas de Bloques, no creemos que la misma se pueda identificar con un sistema contable robusto, como con los que estamos acostumbrados a interactuar. La mención, más bien, hace referencia al registro de movimientos de determinadas criptomonedas, entre diferentes cuentas, lo cual dista de ser una verdadera contabilidad integral.

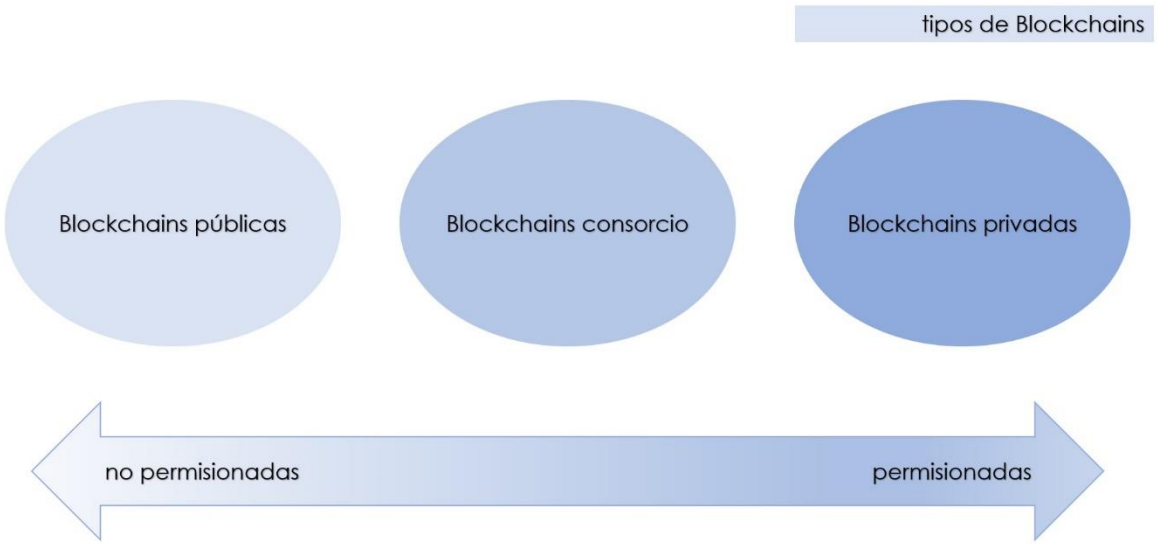
Pero volviendo a la temática de considerar al concepto de DLT como hilo conductor de la clasificación de Blockchains, podemos mencionar que dicha clasificación la haremos en función de los permisos que cada tipo de Cadena de Bloques haga para que sus miembros:

- puedan ser aceptados para poder realizar transacciones,

- quien tendrá gobierno de validar esas transacciones, y

- cuál será el mecanismo para validar, aceptar e incorporar bloques nuevos a la Cadena de Bloques, es decir el mecanismo de consenso.

De esta forma, la primera clasificación de Blockchains, podemos decir que distingue entre Blockchains permisionadas y no permisionadas. Y en ese recorrido podemos distinguir, aplicando un segundo criterio, entre públicas, de consorcio, y privadas.



Fuente: Mukhopadhyay, M. (2018). *Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity*. Packt Publishing Ltd.

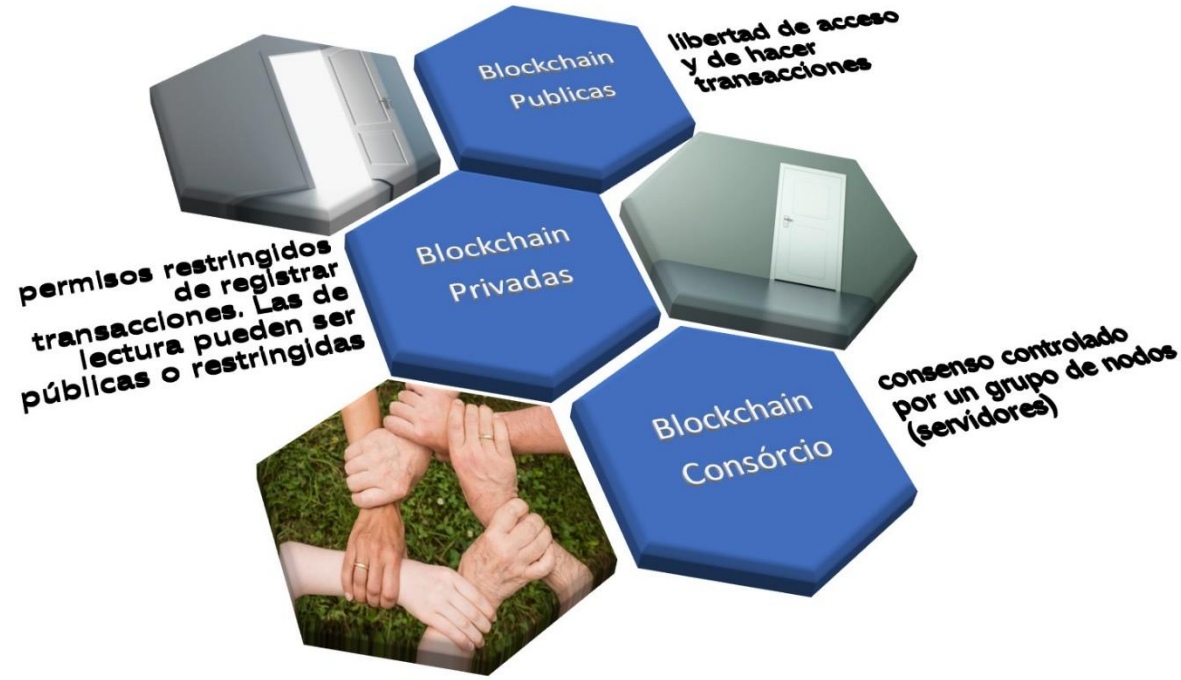
Figura 7 Tipos de Blockchains permisionadas y no permisionadas

Mencionamos también que esta clasificación nos iba a ser de utilidad para poder analizar el desarrollo e implementación de Contratos Inteligentes.

En el caso de las redes privadas, según como se configure la misma, un único, o algunos nodos específicos, tendrán la atribución de leer o escribir transacciones en la Blockchain. Como veremos, los contratos inteligentes son desplegados en la Cadena de Bloques, por medio de un tipo especial de transacciones, por lo cual, los nodos administradores en las redes privadas, tendrán el gobierno de aceptar o no el registro de un Smart Contract en la red.

En el caso de las Blockchains de Consorcio, existirán nodos administradores, que pertenezcan a diferentes organizaciones y “nodos selladores”, que solamente podrán validar y registrar Contratos Inteligentes, previamente aprobados por los nodos administradores.

En las Blockchains públicas, existe total acceso de cualquier nodo, o servidor, para recibir, validar, registrar o desplegar Contratos Inteligentes. Por otra parte, en las Blockchains públicas, los usuarios interactúan con la Cadena de Bloques, por medio de claves públicas anónimas, ya que no es necesario realizar la identificación de a que organización o persona, pertenece esa clave pública.



Tipos de Blockchain - comparativa

Principales características de los tipos de Blockchains

	Blockchain Pública	**Blockchain de Consorcio**	**Bockchain Privada**
Acceso	Cualquiera	Grupos de organizaciones afines o con un interés en común	Una única organización gobernante
Permisos	Permiso libre	Permisos restringidos a un grupo de usuarios	Permiso restringido a una autoridad
Identidad	Anónima	Identidad requerida	Identidad requerida
Modelo de negocios generalmente implementados	Criptomonedas / Criptoactivos	Asociaciones de empresas o organizaciones afines	Empresas o grupos de empresarios particulares

Consensos	POW – Prueba de trabajo	Por votación	Consenso único basado en autoridad o distribuido en administradores designados
Velocidad de las transacciones	Lenta	Rápida	Rápida
Ejemplos	Bitcoin, Ethereum	Corda, Hyperledger	Quorum (Blockchain originalmente desarrollada por J. P. Morgan)

Tabla 1 Comparativa principales características de los tipos de Blockchains

Blockchains híbridas

En el punto anterior desarrollamos una clasificación clásica de los tipos de Blockchains, basada en el caracter de permisionadas (Blockchains privadas) o no permisionadas (Blockchains públicas).

Vimos también un tipo de Cadena de Bloques particular, entre estas dos tipologías puras, que es la que denominamos "Blockchains de Consorcio o Federadas". Si bien las Bockchains de consorcio responden al modelo de Blockchains privadas, tienen un tratamiento distintivo ya que su gobierno no se encuentra centralizado en una sola organización, sino que reponde a un gobierno compartido entre varias organizaciones que proveen al funcionamiento de la Cadena de Bloques, nodos maestros.

Vamos a analizar un modelo particular de Blockchains que se han desarrollado recientemente, y que si bien, no son muy difundidas, creemos que puede ser significativo su estudio, en especial bajo el ámbito de servicios financieros, como la del ejemplo que vamos a mencionar.

Estas Blockchains reciben la denominación de "Blockchains híbridas", y según algunos autores pretenden obtener lo mejor de los dos mundos, en referencia a que implementan Cadenas de Bloques púbicas y privadas, al mismo tiempo. De esta forma se puede combinar, aunque parezca contradictorio, acceso libre y controlado simultaneamente.

¿Cómo se implementa esto?

Al igual que en las Blockchains privadas, el código fuente en las Blockchains híbridas es completamente configurable, por lo cual su modelo de funcionamiento puede variar de una a otra.

Esencialmente lo que las Cadenas de Bloques híbridas hacen es restringir el acceso a determinados usuario, al igual que las Blockchains privadas o las de Consorcio. Sin embargo una vez que el usuario es admitido, puede manejarse con libertad como si operase en una Blockchain Pública.

Otras de las funcionalidades que las Blockchains Híbridas pueden implementar es la facultad de los nodos maestros (o administradores) de definir cuales transacciones se van a hacer públicas y cuales no. O, en su caso, para quienes esas transacciones se van a hacer públicas. Esto con independencia de que las transacciones sean verificables e inmutables, condición sin la cual, sería dudoso pensar en términos de que se pueda considerar una Blockchain.

A los fines de perfeccionar lo que mencionamos en el párrafo anterior, la dinámica de la Blockchain Híbrida, sería semenjante a la siguiente:

- tomemos en cuenta que la Blockchain Híbrida es una combinación de una Blockchain Pública y una Privada. Por lo tanto, los usuarios podrán manejarse en ambos ámbitos, considerando los permisos necesarios.

- al registrarse el usuario, su identidad quedaría almacenada en el ámbito de la Blockchain Privada.

- una vez admitido, el usuario, puede empezar a interactuar con la Blockchain, en el ámbito de la Blockchain Pública. Es decir, con total libertad de operar realizando las transacciones que quiera.

- será potestad de los nodos administradores de la Blockchain Privada, el revelar la identidad del usuario que está registrada en el ámbito de la Blockchain Privada. Esto, a criterio de los nodos administradores, podría efectuarse al realizar determinados tipos de operaciones, operaciones que excedan un monto determinado, o cualquier otro criterio que se quiera implementar.

- otra variante, sería la delegar al usuario la potestad de que él decida en que transacciones revele su identidad.

Este modelo de funcionalidad de las Blockchains Híbrida, podría considerarse de interés para la implementación de sistemas KYC (Conozca su cliente), o AML (anti-lavado de dinero).

Vamos a mencionar, como ejemplo, una Blockchain Híbrida, XDC, basada en un protocolo propio, y desarrollada por una compañia de Singapore.

En el gráfico se puede observar el protocolo de la Blockchain XDC en su funcionamiento.

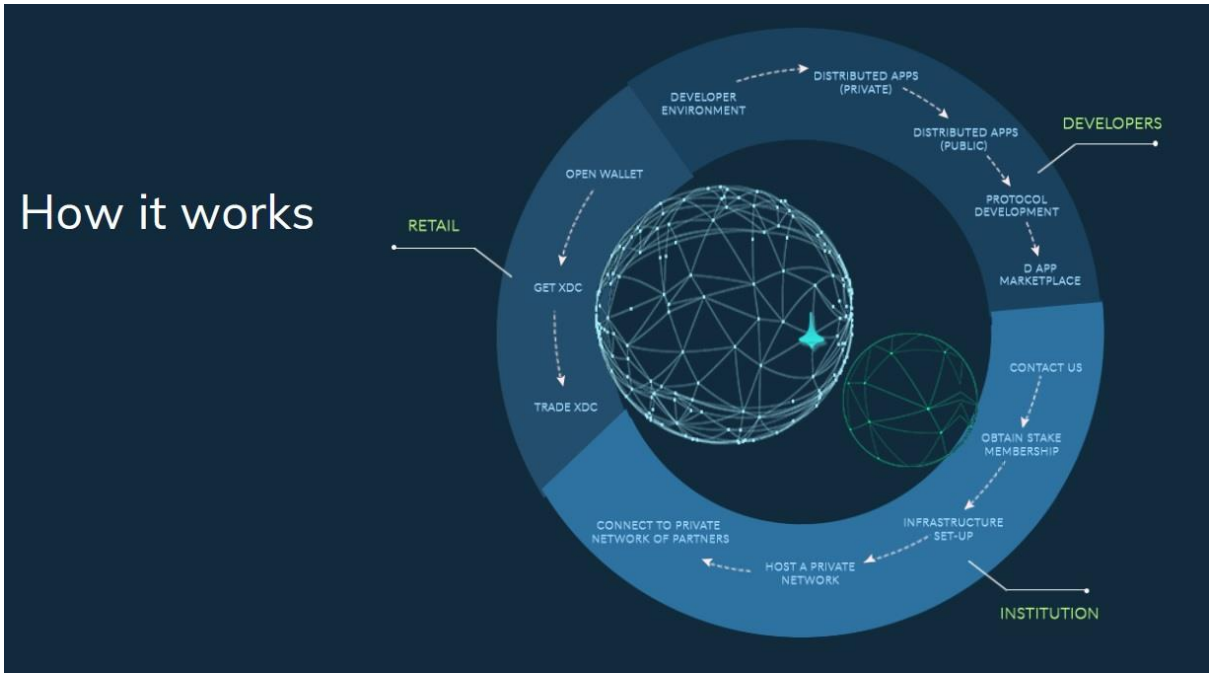


Figura 8 Protocolo de la Blockchain XDC

El modelo de Cadena de Bloques Híbrida XDC maneja dos ámbitos: uno de Blockchain Pública y otro de Blockchain Privada. Los usuarios minoristas pueden interactuar libremente, usando sus billeteras, e intercambiando tokens de XDC dentro del ámbito de la Blockchain Pública.

Los usuarios mayoristas, o institucionales pueden desarrollar dentro del ámbito de Blockchain Privada, sus propias sub-cadenas de bloques. Dentro de estas sub-blockchains los participantes tienen acceso restringido, de modo que sus transacciones, mensajerias y datos no son accesibles por usuarios de la Blockchain Pública.

En ese ámbito de Blockchain Privada, es donde los usuarios mayoristas o institucionales, pueden desarrollar la infraestructura de base para implementar sus DAPPS o sus aplicaciones empresariales.

En esta imagen se puede observar una aproximación del eco-sistema de la Blockchain Híbrida XDC.

Algunos de los beneficios que podemos observar de las Cadenas de Bloques Híbridas son:

Ecosistema cerrado: en su modelo más común las Blockchains híbridas permiten configurar un ecosistema cerrado donde los usuarios deben ser registrados y autorizados para operar sobre la Cadena de Bloques. Si bien luego de registrarse pueden realizar transacciones libremente como en una Blockchain Pública, la Cadena de Bloques mantiene el control de quienes son los usuarios que operan en ella.

Ambiente de desarrollo más amigable: desde que la Blockchain Híbrida, en su modelo tradicional, admite el desarrollo de Contratos Inteligentes en el ámbito de BCT Privada, esto permite un mejor acceso controlado a infraestructura tecnológica de Blockchain, para las aplicaciones que los usuarios deseen generar.

Gestión de privacidad y de identidad de usuarios: la Blockchain Híbrida suma como ventaja la identidad digital de sus usuarios, pero simultaneamente permite que estos mantengan su privacidad controlando el acceso de quienes pueden ver sus transacciones.

Por último, como resumen, queremos compartirles un infograma que muestra en forma sintética, características relevantes de los diferentes tipos de Blockchains:

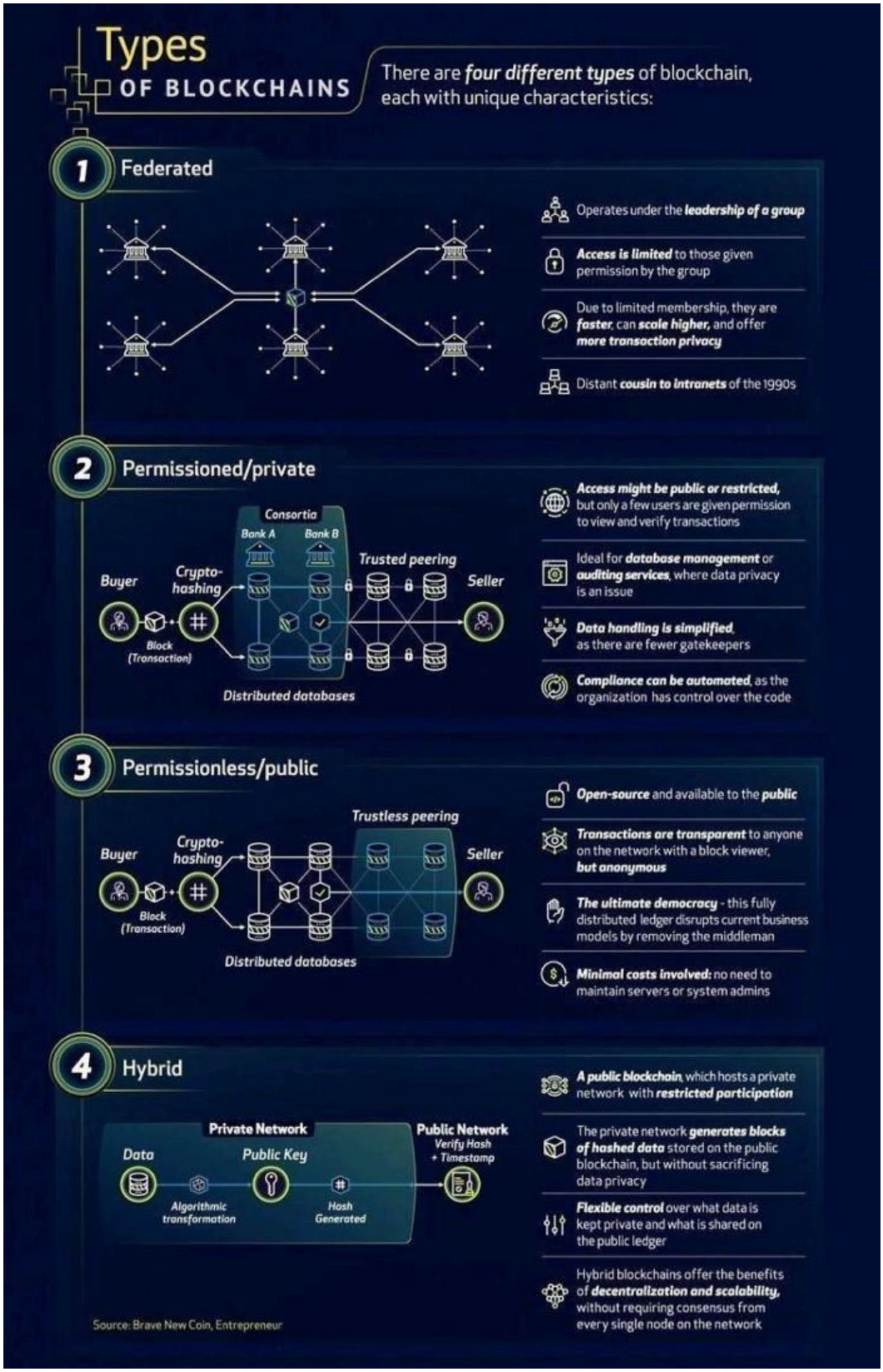


Figura 9 características relevantes de los diferentes tipos de Blockchains. Fuente: Brave New Coin

Contratos Inteligentes

La idea de “contratos inteligentes” es previa al desarrollo de la tecnología de Blockchain.

En el año 1996, Nick Szabo publicó un paper donde delineaba una propuesta para desarrollo y análisis de Contratos Inteligentes. Para ese momento no se contaba todavía con la infraestructura tecnológica de la Blockchain, que como mencionamos anteriormente, fue pensada en función del soporte de las criptomonedas.

Recién en enero de 2009, se lanza la primera Cadena de Bloques, la que va a sustentar hasta ahora a la principal criptomoneda, el Bitcoin.

Seis años después, Vitalik Buterin, junto con otro grupo de entusiastas, propone el desarrollo de la Blockchain Ethereum, pensada para soportar una criptomoneda específica, el Ether, y con capacidad de registrar y ejecutar Contratos Inteligentes.

Por esto, vamos a conceptualizar a los Contratos Inteligentes, basándonos en la definición que dio Szabo, en 1996, pero iremos realizando consideraciones que entendemos procedentes para adecuar esa definición, a la perspectiva de su implementación en Cadena de Bloques.

Definición:

“Un Contrato Inteligente es un juego de promesas, especificadas en un formato digital, incluyendo protocolos con los cuales las partes, pueden perfeccionar estas promesas”

Veamos algunos de los conceptos que se incluyen en esta definición:

juego de promesas: el contrato contempla prestaciones a realizarse en tanto se cumplan “condiciones de negocio”. En el caso particular de Contratos Inteligentes sobre Blockchain, veremos que podemos clasificar esas condiciones en intrínsecas y extrínsecas, a la Blockchain.

Dentro de las intrínsecas podemos mencionar aquellas promesas que disparan acciones vinculadas al plazo de tiempo. En este caso la misma Blockchain va a ejecutarlas, sin necesidad de ninguna acción externa.

Dentro de las extrínsecas podemos mencionar a las comunicaciones que el contrato puede recibir de usuarios, como por ejemplo el voto en los Contratos Inteligentes de “democracy”. También en esta categoría (extrínsecas) podemos incluir a las notificaciones que el Contrato puede recibir de “oracles”. Por ahora podemos mencionar que lo que se denomina en la Blockchain “oracles”, hace relación a sensores externos (Internet de las cosas), que poseen la capacidad de comunicarse con el contrato, o responder solicitudes realizadas por este, enviando mensajes.

especificadas en formato digital: podríamos decir que un Contrato Inteligente es una representación en código de programa (una representación digital) de un acuerdo aceptado entre diferentes partes. El código es la forma en que vamos a introducir la lógica de negocio con la que se van a ejecutar las condiciones de negocio.

Vamos a ver que, tomando en consideración, la diferenciación o la complementariedad que haya entre el “contrato en lengua natural” (mundo real), y su “contrato en código de programa” (Blockchain), vamos a poder distinguir distintas tipificaciones de contratos en el “espectro” de desarrollo de contratos inteligentes.

incluyendo protocolos: en IT utilizamos a diario el término “protocolo” para referirnos al software que posibilita la comunicación dentro de una red, por ejemplo el protocolo TCP/IP que nos permite comunicarnos en Internet. Pero en la definición de Contratos Inteligentes que estamos analizando, el término protocolo adopta otra perspectiva. En este caso hace referencia a un juego de reglas, que ya se encuentran codificadas en forma de software, corriendo en la Blockchain, y que van a disparar acciones que impactaran en las partes intervinientes en el contrato, como, por ejemplo, la generación de una transacción que transfiera criptomonedas entre cuentas de usuarios.

con los cuales las partes pueden perfeccionar estas promesas: esta es tal vez la parte más relevante de la definición, en relación con los Contratos Inteligentes que desplegamos sobre la Blockchain. La definición hace referencia a que los protocolos que mencionamos en el apartado anterior permiten que se perfeccionen el juego de promesas del contrato. La esencia de los Contratos Inteligentes que corren sobre la Blockchain, y su característica distintiva, es que una vez que son desplegados en la Cadena de Bloques, son “irrevocables”, vale decir, inexorablemente se van a ejecutar. Vamos también a desarrollar este punto, ya que, en el diseño del contrato, esto será tal vez, el factor más preponderante que deberemos tomar en cuenta.

A fin de poder analizar sistemáticamente las diferentes etapas en que podemos dividir, el planeamiento, desarrollo, despliegue y ejecución de un Contrato Inteligente, vamos a seguir el marco general de desarrollo de Contratos Inteligentes propuesto por la organización Digital Chambers of Commerce.[5]

El marco de desarrollo mencionado distingue 6 etapas en el desarrollo de Smart Contracts:

[5] Digital Chambers of Commerce - https://digitalchamber.org/ Observado: noviembre 2022

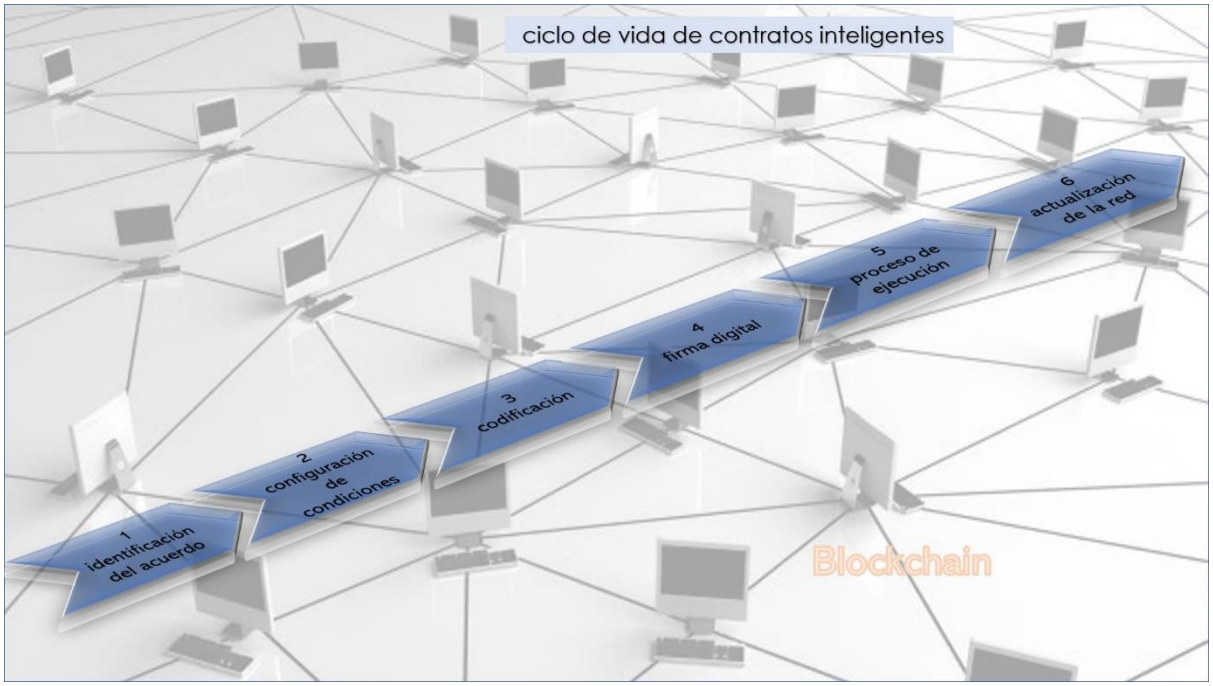


Figura 10 Ciclo de vida de Contratos Inteligentes

Identificación del acuerdo:

En esta primera etapa se debe identificar con claridad la oportunidad de negocio, o la acción social que se quiera gestionar por medio del Contrato Inteligente en el caso de una actividad sin fin de lucro. En relación con esto, los objetivos que se desea alcanzar por medio de la ejecución del contrato, en especial desde el enfoque del iniciador del mismo.

Algunos de los aspectos más relevantes a definir en esta etapa, son:

- Participantes
- Relaciones que se presentarán entre ellos, en el marco y alcance del contrato
- Derechos, prestaciones y valores que se van a transferir
- Plazos
- Definición en abstracto de condiciones:

Condiciones generales

Oracles: mencionemos que por medio de los “oracles” el Contrato Inteligente recibe mensajes de afuera de la Blockchain.

Condiciones de ruptura: podemos mencionar, que dentro de las condiciones de ruptura, deberemos considerar, que en virtud de ser los Contratos Inteligentes inmutables e imposible de ser detenidos, en algunas situaciones deberíamos plantearnos la posibilidad de incluir en el Smart Contract, cláusulas para su disolución o para que se detenga su ejecución.

- Otros

En el caso que el proceso de negocio que se desee gestionar por medio del Contrato Inteligente tuviese un alto grado de complejidad, deberíamos plantearnos en esta etapa, la posibilidad desagregar la lógica de negocio del problema a resolver, modelando diferentes Contratos Inteligentes conectados entre sí. Dentro de las capacidades de los Contratos Inteligentes desplegados sobre la Blockchain, podemos mencionar las de hacer llamadas entre ellos, o “heredarse” unos a otros en forma jerárquica.

También en esta etapa y, en relación con la complejidad del proceso de negocio que se mencionó en el párrafo anterior, deberíamos considerar el modelado del Contrato Inteligente, en función de la posibilidad de tener que volver a utilizarlo para relaciones de negocio futuras, o en función de su escalabilidad para relaciones de negocio derivadas de la actual, y con mayor grado de complejidad.

Configuración de condiciones:

En esta etapa se debe identificar, catalogar y configurar las condiciones que impactarán en la lógica del contrato a modelar. Podemos clasificar las condiciones que van a impactar en un Contrato Inteligente en:

- Condiciones intrínsecas al Contrato: son las que no requieren de ser “invocadas” por un actor externo al contrato, por medio de un mensaje enviado al mismo. Por ejemplo, si establecí en un Contrato Inteligente, que el contrato transfiera una cantidad de criptomoneda de una cuenta a otra, en un plazo de 30 días.
- Condiciones extrínsecas al Contrato: son las que requieren un mensaje de un actor externo al contrato para activarse. Las podemos subclasificar en:
    - Mensajes generados por usuarios de la Blockchain (cuentas de EOA - External Owners Accounts), por ejemplo, la manifestación de voluntad que comunica cada usuario designado en un Contrato Inteligente de votación (comúnmente conocido como “democracy contract”)
    - Mensajes generados por sensores con los que se comunica el contrato. El uso más común de esta modalidad de contrato lo encontramos en el campo de IoT (Internet de las Cosas), disciplina que estudia dispositivos sensores que generan flujos constantes de información transmitida por Internet. Por ejemplo, en el caso que tenga un Contrato Inteligente de “auto-aseguro” de una cooperativa agrícola, para cubrir el riesgo se granizo de los asegurados. En este caso el contrato va a monitorear un sensor certificado, como puede ser el del Servicio Meteorológico Nacional, y al detectar que se produjo el siniestro en el campo de un asegurado, va a disparar una clausula de pago de la prima, por medio de la transferencia de un monto de criptomonedas desde la cuenta del contrato a la cuenta del usuario asegurado.

Codificación

Una vez definido el modelo del contrato, su lógica, partes intervinientes, líneas de tiempo, condiciones, y otros tenemos que volcar ese modelo abstracto a la codificación para que pueda ser gestionado y ejecutado por la Blockchain.

Este es el punto donde se debe observar el trabajo interdisciplinario entre profesionales de negocio (gerentes, contadores, abogados) y profesionales de IT (programadores, arquitectos de sistemas, analistas). El punto crítico se centra en que la lógica, escenarios, condiciones que define el contrato modelado en abstracto, coincidan con las definidas en el código de programación del contrato inteligente.

En ese aspecto, Mukhopadhyay, M. (2018) define un espectro de relaciones entre contratos inteligentes y contratos en lenguaje natural.[6]

Figura 11 Espectro de Contratos Inteligentes

Bajo este análisis, el autor mencionado, define toda una gama de posibles combinaciones de complementariedad, entre los Contratos Inteligentes y los Contratos en Lenguaje Natural.

Esta complementariedad se presenta según sea el grado mayor o menor grado de automatización del contrato inteligente, y la mayor o menor preponderancia del contrato escrito en lenguaje natural. Tipifica 4 casos que pueden ser significativos para que conceptualicemos los niveles de complementariedad de estos contratos:

- Enteramente digital.

[6] Mukhopadhyay, M. (2018). *Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity*. Packt Publishing Ltd.

- En código de programa, con versión en lenguaje natural.
- Contrato en lenguaje natural, con ejecución por código de programa.
- Contrato en lenguaje natural, con mecanismos de pago por código de programa.

En referencia al código de programa en sí, como ya mencionamos anteriormente, Ethereum soporta un lenguaje de programación específico denominado “Solidity”. Solidity es un lenguaje orientado a objetos, de alto nivel, con sintaxis basada en JavaScript, phyton, y C++, y desarrollado especialmente para la codificación de contratos inteligentes sobre Ethereum. Ethereum actualmente también soporta programación de Smart Contracts por medio de Vyper, otro lenguaje específico para el desarrollo de Contratos Inteligentes sobre Ethereum. En este caso, vyper, tiene una sintaxis basada en Python.

Otro aspecto que consideramos relevante, y que debe tomarse en cuenta en esta etapa del ciclo de vida de Contratos Inteligentes, es el referido a la seguridad de Smart Contracts, en especial a las vulnerabilidades de código. Tema, que si bien, es propio de profesionales de IT, no se puede dejar de analizar, y validar por expertos de negocio, en especial por las consecuencias indeseadas, estudio de auditoría de contratos, y análisis de riesgos relevantes.

Firma digital

Las Blockchains utilizan activamente la infraestructura criptográfica de firma digital con la finalidad de definir identidad criptográfica y permisos de sus usuarios.

Cuando hablamos de identidad criptográfica nos estamos refiriendo al registro que se realiza en la Blockchain de las operaciones realizadas por las direcciones de usuarios, vinculadas a sus claves públicas, y en el caso de las Cadenas de Bloques públicas, estas claves son anónimas ya que no requieren de un proceso de identificación de los usuarios (personas) que las detentan.

También vimos, al desarrollar la historia de la Blockchain Ethereum, su diferencia con la Blockchain de Bitcoin. Bitcoin fue pensada y desarrollada para gestionar una criptomoneda específica, y soporta transacciones con esa finalidad, mientras que Ethereum adiciona a esta funcionalidad la capacidad de soportar contratos inteligentes.

Esto toma relevancia en relación con las consideraciones que debemos hacer sobre el uso de firma digital, en el sentido que en Ethereum vamos a diferenciar dos clases de tipos de cuentas:

EOA: Externally owner accounts – propietarios de cuentas externas, quienes son los usuarios tradicionales que detentan criptomonedas (Ethers). Sus cuentas se vinculan con sus claves privadas, las que utilizan para poder firmar transacciones, y de esta forma detentar sus tenencias de criptomonedas.

Las EOA tienen estas características:

- Poseen “balance”, la función que nos permite conocer la cantidad de criptomonedas asociada a esa cuenta, a un momento determinado (consultar su saldo).
- Pueden enviar transacciones a la Blockchain
- Son controladas por medio de sus claves privadas
- No tienen un código de programa asociado a ellas

Cuentas del contrato: son las cuentas creadas al realizar la implementación del contrato, para poder identificarlo. De esta forma, por ejemplo, el contrato puede ser receptor de criptomonedas que se transfieran a él.

Las cuentas de contrato poseen estas características:

- Poseen “balance”, podemos consultar en cualquier momento el saldo de Ethers que posee la cuenta del contrato.
- Pueden disparar transacciones por medio de la ejecución de su código de programa
- No poseen claves privadas asociadas
- Tienen código de programa asociado, que se ejecuta por medio de transacciones o mensajes invocados por otros contratos. Este código puede a su vez realizar operaciones complejas, manipula la información que el contrato almacena en la Blockchain, y tiene su propio estado de persistencia.

Esta distinción que hacemos entre cuentas EOA (cuentas externas) y Cuentas de contrato, toma importancia en cuanto analizamos el diferente tratamiento que la Blockchain hace, al no usar las cuentas de contrato, claves privadas para poder firmar las transacciones que pueden generar. ¿Como es esto? ¿Quién me garantiza en ese caso que la transacción que generó un contrato inteligente esté firmada por él?

Para comprender la dinámica de como esto opera, a nivel de contratos inteligentes, debemos hacer foco en la cuarta característica que mencionamos recién, en el apartado de cuentas del contrato: “tienen código de programa asociado”.

Ya vimos la lógica que tiene, y como funciona, la EVM (Ethereum Virtual Machine), el motor que se va a encargar de ejecutar los contratos inteligentes que desplegamos en Ethereum.

Ethereum va a hacer uso de las transacciones para registrar y para ejecutar eventos en los contratos inteligentes. Como los bloques que se incorporan a la Blockchain, contienen las transacciones que van a impactar en diferentes cuentas cambiando sus estados, podemos decir que los bloques contienen las “transiciones” que al impactar, producen los cambios de “estados”.

¿Y como juega esto con el contrato inteligente? El código de programa del contrato, ya se encuentra registrado en la Blockchain. Supongamos entonces, que por medio de una transacción un usuario, envía un mensaje al contrato, invocando un método de este (llamando al contrato para que realice una acción determinada). Lo que la EVM va a hacer es comprobar si ese mensaje (y su transacción) es válido, y verificar la acción que se solicita al contrato que

ya se encuentra registrado en la red, y si todo está correcto, va a ejecutar esa acción, cambiando el estado de ese contrato.

Por dicho motivo es que el contrato no necesita de una clave privada para realizar una transacción. Porque lo que vendría a sustituir a esa firma de la transacción, es el código de programa que ya se encuentra registrado (y validado) en la Blockchain.

Veámoslo en un ejemplo, para clarificar un poco más este aspecto.

Supongamos que Juan desea realizar una transferencia de valor a María. Lo que simplemente Juan va a hacer es, por medio de su billetera digital, va a firmar una transacción donde indica a Ethereum que transfiera 5 Ethers, desde su cuenta a la cuenta de María. La transacción firmada va a viajar a la red, va a ser validada y registrada en un primer servidor. Por el método de divulgación se va a propagar por toda la red, donde todos los nodos que la reciban van a volver a validarla y registrarla. Posteriormente un minero va a extraer esa transacción desde el mempool de red, y la va a minar dentro de un bloque, que va a pasar a formar parte definitiva de la Blockchain.

Ahora, veamos la misma operación, pero con más complejidad. Vamos a suponer que Juan es el gerente financiero de una empresa, y María presta un servicio a dicha empresa. Para que se realice el pago del servicio prestado por María, se necesita de la conformidad de la mayoría de un comité compuesto por Pedro, Gabriel y Gustavo.

En esta situación Juan decide registrar un contrato inteligente en Ethereum y desde su cuenta, envía una transacción firmada con su firma digital, hacia la cuenta del contrato, por el monto total de 5 Ethers. Es decir, en lugar de transferir directamente a María, transfiere a la cuenta del contrato. Al mismo tiempo, registra en la Blockchain, ese contrato, cuyo código de programa contiene una lógica semejante a esta:

- Almaceno en la Blockchain, en forma permanente, la información de las cuentas de María (prestadora del servicio), por un lado, y de Pedro, Gabriel y Gustavo (miembros del comité).
- Si 2 de los 3 miembros del comité, por medio de mensajes en transacciones válidas (validando sus identidades), manifiestan su conformidad de perfeccionar el pago: doy por válida la transferencia desde la cuenta del contrato hacia la cuenta de María.

¿Cuál es entonces la “firma digital” de la transacción por la que el contrato envía a la cuenta de María los 5 Ethers? La respuesta a esto es “el cumplimiento de las condiciones que estipulo el contrato, o parte de él”.

Por este motivo es que las cuentas de Contratos en Ethereum, poseen direcciones (claves públicas), pero no claves privadas, sino que poseen códigos de programas asociados, que al cumplir sus condiciones actúan como la firma digital autenticando las transacciones.

Proceso de ejecución

Una vez que se haya desarrollado el código del programa del Contrato Inteligente deberemos “deployarlo” (hacer el despliegue) del mismo en la la Blockchain de Ethereum.

Solo unas breves consideraciones técnicas que debemos tomar en cuenta aquí.

La mayoría del software con que interactuamos a diario pasa por dos momentos de implementación.

Primero: la escritura del código fuente del mismo, legible y entendible por el ser humano, aunque para su comprensión se debe conocer la sintaxis del lenguaje de programación que se ha utilizado (podríamos decir que es legible por el ser humano, pero de alguien especializado en el tema – un programador).

Segundo: la compilación de ese programa fuente, para obtener un programa ejecutable, codificado de tal forma que sea entendible por la computadora. Este es el programa ejecutable que tenemos en nuestras computadoras (el que corre cuando clickeamos en el ícono de Word, por ejemplo).

Como ya mencionamos Ethereum gestiona y ejecuta los contratos inteligentes programados, por medio de la EVM (Ethereum Virtual Machine). Y como su nombre lo indica, adiciona a lo que mencionamos antes una capa adicional, del proceso de compilación. De este modo podemos encontrar para un contrato inteligente:

- Su código fuente, escrito en un lenguaje de programación (generalmente solidity).
- La compilación de este en OPCODES.
- La compilación para ejecución en BYTECODES.

¿Por qué es esto relevante al funcionamiento de los Contratos Inteligentes?

Cuando vimos la dinámica de la Blockchain y estudiamos las transacciones, vimos que el formato de una transacción es muy semejante a un asiento contable, donde tenemos cuentas que se debitan (ingresos), y cuentas que se acreditan (salidas), y la transacción debe estar balanceada, siendo igual el total de ingresos al total de salidas.

Sin embargo, el monto que sale de una cuenta de un usuario no es el mismo que ingresa a la cuenta del otro, sino que la diferencia entra ambas está dada por un porcentaje que se asigna como retribución al minero que realiza el proceso de mineración de esa transacción.

Siguiendo esta lógica, los contratos inteligentes también pagan a los mineros, por el trabajo de mineración que van a hacer sobre ellos.

La diferencia entre este pago que realiza el contrato, con el pago de una transacción común, está dado en que el pago que destina el contrato a los mineros se calcula en función de las operaciones que el contrato realiza.

Este pago que el contrato hace a los mineros, en Ethereum se denomina “GAS”.

El “yellow paper” de Ethereum contiene una tabla específica a utilizar para el cálculo del GAS de un contrato inteligente.

Appendix G. Fee Schedule

The fee schedule G is a tuple of 31 scalar values corresponding to the relative costs, in gas, of a number of abstract operations that a transaction may effect.

Name	Value	Description*
G_{zero}	0	Nothing paid for operations of the set W_{zero}.
G_{base}	2	Amount of gas to pay for operations of the set W_{base}.
$G_{verylow}$	3	Amount of gas to pay for operations of the set $W_{verylow}$.
G_{low}	5	Amount of gas to pay for operations of the set W_{low}.
G_{mid}	8	Amount of gas to pay for operations of the set W_{mid}.
G_{high}	10	Amount of gas to pay for operations of the set W_{high}.
$G_{extcode}$	700	Amount of gas to pay for an EXTCODESIZE operation.
$G_{extcodehash}$	400	Amount of gas to pay for an EXTCODEHASH operation.
$G_{balance}$	400	Amount of gas to pay for a BALANCE operation.
G_{sload}	200	Paid for a SLOAD operation.
$G_{jumpdest}$	1	Paid for a JUMPDEST operation.
G_{sset}	20000	Paid for an SSTORE operation when the storage value is set to non-zero from zero.
G_{sreset}	5000	Paid for an SSTORE operation when the storage value's zeroness remains unchanged or is set to zero.
R_{sclear}	15000	Refund given (added into refund counter) when the storage value is set to zero from non-zero.
$R_{selfdestruct}$	24000	Refund given (added into refund counter) for self-destructing an account.
$G_{selfdestruct}$	5000	Amount of gas to pay for a SELFDESTRUCT operation.
G_{create}	32000	Paid for a CREATE operation.
$G_{codedeposit}$	200	Paid per byte for a CREATE operation to succeed in placing code into state.
G_{call}	700	Paid for a CALL operation.
$G_{callvalue}$	9000	Paid for a non-zero value transfer as part of the CALL operation.
$G_{callstipend}$	2300	A stipend for the called contract subtracted from $G_{callvalue}$ for a non-zero value transfer.
$G_{newaccount}$	25000	Paid for a CALL or SELFDESTRUCT operation which creates an account.
G_{exp}	10	Partial payment for an EXP operation.
$G_{expbyte}$	50	Partial payment when multiplied by $\lceil \log_{256}(exponent) \rceil$ for the EXP operation.
G_{memory}	3	Paid for every additional word when expanding memory.
G_{txcreate}	32000	Paid by all contract-creating transactions after the *Homestead* transition.
$G_{txdatazero}$	4	Paid for every zero byte of data or code for a transaction.
$G_{txdatanonzero}$	68	Paid for every non-zero byte of data or code for a transaction.
$G_{transaction}$	21000	Paid for every transaction.
G_{log}	375	Partial payment for a LOG operation.
G_{logdata}	8	Paid for each byte in a LOG operation's data.
G_{logtopic}	375	Paid for each topic of a LOG operation.
G_{sha3}	30	Paid for each SHA3 operation.
$G_{sha3word}$	6	Paid for each word (rounded up) for input data to a SHA3 operation.
G_{copy}	3	Partial payment for *COPY operations, multiplied by words copied, rounded up.
$G_{blockhash}$	20	Payment for BLOCKHASH operation.
$G_{quaddivisor}$	20	The quadratic coefficient of the input sizes of the exponentiation-over-modulo precompiled contract.

Tabla 2 “ yellow paper” de Ethereum contiene una tabla específica a utilizar para el cálculo del GAS de un contrato inteligente

Las operaciones que se mencionan en la primera columna de la tabla son las que se obtienen del proceso de primera compilación del código fuente para transformarlo en OPCODE. En la figura siguiente, podemos ver una muestra de los 3 estados de un Smart Contract, en código fuente, compilado en OPCODE y compilado en BYTECODES.

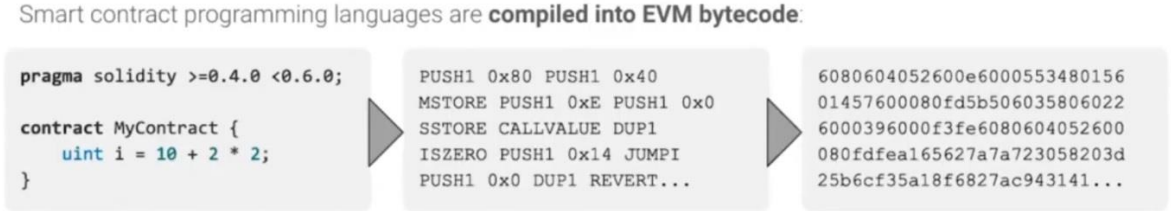


Figura 12 Tres estados de un Smart Contract

Resumiendo, estas ideas, podemos aplicar este ejemplo, para intentar una mejor comprensión:

- La Blockchain de Ethereum vendría funcionar como nuestro auto.
- Lo que llamamos GAS en Ethereum sería semejante a la nafta que nuestro auto necesita para funcionar
- En Ethereum tenemos que pagar con Ethers para comprar GAS. Así como en nuestra vida real, pagamos con dinero para adquirir la nafta.
- Ejecutar un Contrato Inteligente, es como si quisiéramos realizar un viaje con nuestro auto. Para ejecutar ese Contrato Inteligente, podríamos decir que tenemos que cubrir una cierta distancia, lo que sabemos que nos va a consumir una cantidad de nafta.
- Es decir, que la ejecución de un Contrato Inteligente vendría a ser el costo en que vamos a incurrir, para poder realizar ese viaje.

¿Por qué tenemos que pagar para ejecutar un Contrato Inteligente? Básicamente por dos razones:

1. Para recompensar a los mineros, que deben tomar el trabajo de registrar ese contrato inteligente, y sus estados, en la Blockchain

2. Para evitar los ataques DoS (Denied of Service). Imaginemos por un momento, que los contratos inteligentes fueran gratuitos y no tendríamos que pagar el GAS para ejecutarlos. Un grupo de actores maliciosos podrían subir una gran cantidad de contratos que realicen una cantidad extraordinaria de operaciones, y de esta forma sobrecargar la red para que funcione muy lenta, o se desborde y colapse. La idea de pagar el GAS como condición a la ejecución del contrato, tiene como sentido cubrirse ante esta posibilidad de ataques.

Actualización de la red

Lo último que tomaremos en consideración, es que una vez desplegado el Contrato Inteligente sobre la Blockchain, la EVM – Ethereum Virtual Machine será la encargada de ir ejecutando la parte correspondiente de su código de programación.

Ya anteriormente mencionamos lo importante que es para esto, entender la dinámica de los pasos de un estado a otro estado, en la Blockchain, y el concepto de transiciones (que es lo provoca los cambios de estados).

En este caso, las transiciones que la Blockchain debe dar, se encontrarán en los bloques que se van a incorporar a la misma. Estas transiciones pueden ser simples transacciones de criptomoneda (Ethers), o ejecución del código del Contrato Inteligente.

Una vez que el minero verifica la ejecución correspondiente del código, va a enviar el nuevo estado del contrato a todos los otros nodos de la red, que van a verificar las condiciones, ejecutar la parte correspondiente del código, y controlar si se llega al mismo estado del contrato propuesto por el minero. De ser así, se dará por bueno ese bloque, incorporándose a la Cadena de Bloques.

Modificaciones adicionales al modelo de Contratos Inteligentes

El modelo de ciclo de vida y desarrollo de Contratos Inteligentes que propone el Digital Chambers of Commerce, es sin duda de mucha utilidad para poder ordenar metodológicamente los aspectos más relevantes que deberemos tener en consideración al momento de realizar un desarrollo sobre Ethereum.

Sin perjuicio de esto, nos animamos a sugerir dos etapas adicionales, que por la importancia que tienen en el ciclo de vida y desarrollo, consideramos que sería oportuno su tratamiento como etapas del proceso por separado, en lugar de considerarlas dentro de algunas de las etapas más amplias, que propone el modelo.

Configuración de la Plataforma de Blockchain

La primera de estas etapas adicionales la podríamos ubicar entre “1. identificación del acuerdo” y su siguiente etapa “2. Configuración de condiciones”.

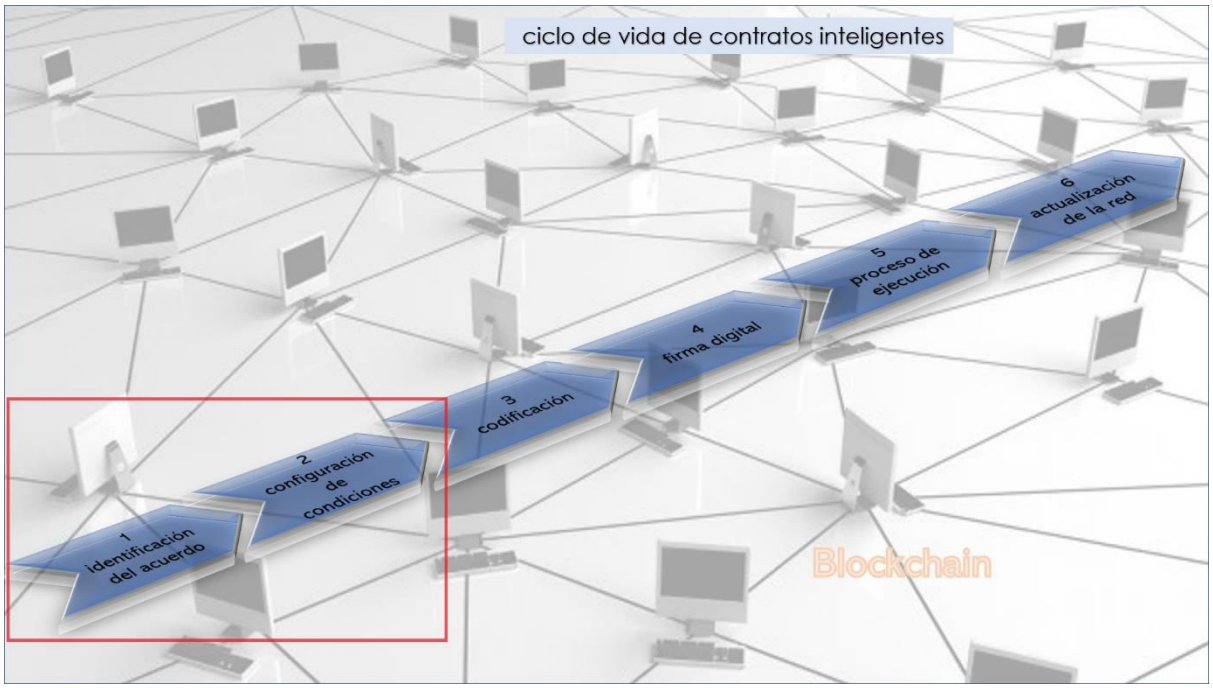


Figura 13 Ciclo de vida Contrato Inteligente Etapas 1. identificación del acuerdo” y 2. Configuración de condiciones

La etapa que sugerimos incorporar para su análisis hace referencia a la “configuración plataforma Blockchain”. Aquí deberíamos analizar las diversas alternativas, acerca de la plataforma de Blockchain que utilizaremos para alojar nuestros contratos inteligentes

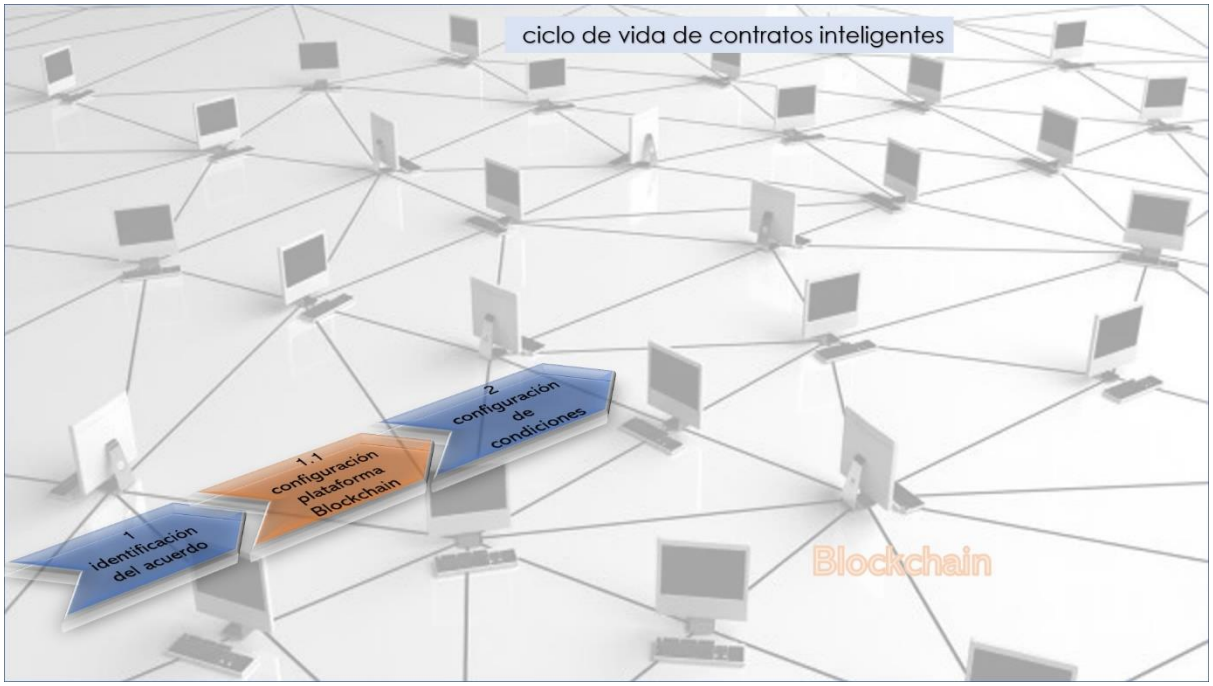


Figura 14 Ciclo de vida Contrato Inteligente Incorporación etapa “configuración plataforma Blockchain” entre etapas 1 y 2

Ya mencionamos previamente la clasificación de los tipos de Blockchain, dividiéndolas entre permisionadas y no permisionadas. Y a su vez, a las permisionadas en Blockchains privadas, y Blockchains de consorcio.

La razón por la que creemos que esta distinción toma relevancia en el desarrollo de nuestros contratos inteligentes, tiene que ver con el hecho de que en las redes públicas no existen restricciones para que cualquier persona desarrolle y despliegue un contrato inteligente en la misma.

Por el contrario, en las redes permisionadas, el acceso de nuevos nodos y usuarios está restringido a que los nodos administradores los admitan. Así también la aceptación de que puedan desplegar contratos inteligentes. Por lo cual, la decisión acerca de la plataforma de Blockchain que se va a utilizar, pasa a ser estratégica, y vinculada directamente a las capacidades, permisos y restricciones que van a poder tener nuestros contratos inteligentes, es decir, al éxito o fracaso del desarrollo que se quiera realizar.

Blockchains modificadas

De acuerdo con la magnitud del proyecto que queramos realizar, una de las opciones que se debería evaluar es la de crear nuestra propia Blockchain, basándonos en el desarrollo ya realizado por otras Cadenas de Bloques.

Todas las Blockchains públicas son desarrollos open-source, es decir, que ponen a disposición del público el código fuente con el cual se desarrollaron. Además de esto se facilita documentación conformada acerca de funcionamiento y aspectos técnicos de las mismas, por medio de la publicación de yellow papers, o de white papers, y suelen tener fuertes

participaciones de la comunidad de desarrolladores y usuarios que interactúan con el proyecto fundacional de la misma.

En el caso que se desee desarrollar con fines particulares una Blockchain privada o de consorcio, que soporte una gran cantidad o complejidad de contratos inteligentes y otras aplicaciones (DAO, DAPPs), se debería analizar la factibilidad de descargar y modificar el código fuente de una Blockchain pública, para adaptarla y convertirla en una Cadena de Bloques permisionada, donde se diferencien nodos administradores de nodos validadores, por ejemplo.

Esta opción no es muy frecuente, en especial por el esfuerzo de análisis, desarrollo, implementación y testing que conlleva. Además que las redes privadas o de consorcio que se encuentran disponibles como frameworks (plataformas de desarrollo), como las que mencionamos (Corda, Hyperledger, Quorum), tienen la capacidad y amplitud para adaptarse y parametrizarse, a una amplísima gama de casos de usos.

Sin embargo, si la complejidad del proyecto lo demandase, el desarrollo de una Blockchain propia, modificada de alguna de las Cadenas de Bloques públicas, es una opción por evaluar.

Verificación del contrato inteligente desarrollado

A la siguiente etapa que sugerimos incorporar para hacer un proceso de análisis específico, la podemos situar entre “4. firma digital” y “5. proceso de ejecución”.

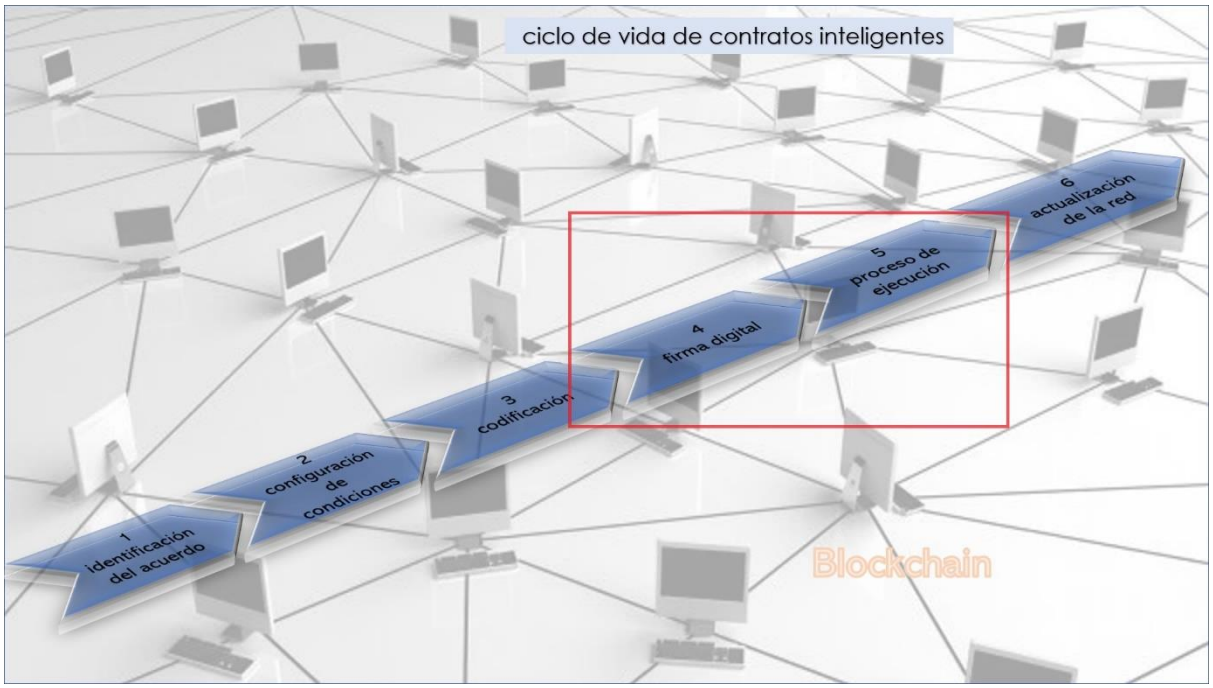


Figura 15 Ciclo de vida Contrato Inteligente Etapas “4. firma digital” y “5. proceso de ejecución”

Entendemos que, ante la inmutabilidad e irreversibilidad que poseen los Contratos Inteligentes, es prioritario y relevante al ciclo de vida y desarrollo, tratar por separado todas

acciones y procesos vinculados a la verificación y testeo de estos, antes de desplegarlos en la Blockchain, ya que una que vez que hayamos hecho esto, es imposible detenerlos y evitar que se ejecuten.

Al ser los contratos inteligentes que desarrollamos, inalterables e imposibles de detener en su ejecución, es muy importante someterlos a un fuerte proceso de testing en diferentes estados de stress, vulnerabilidades y verificación funcional.

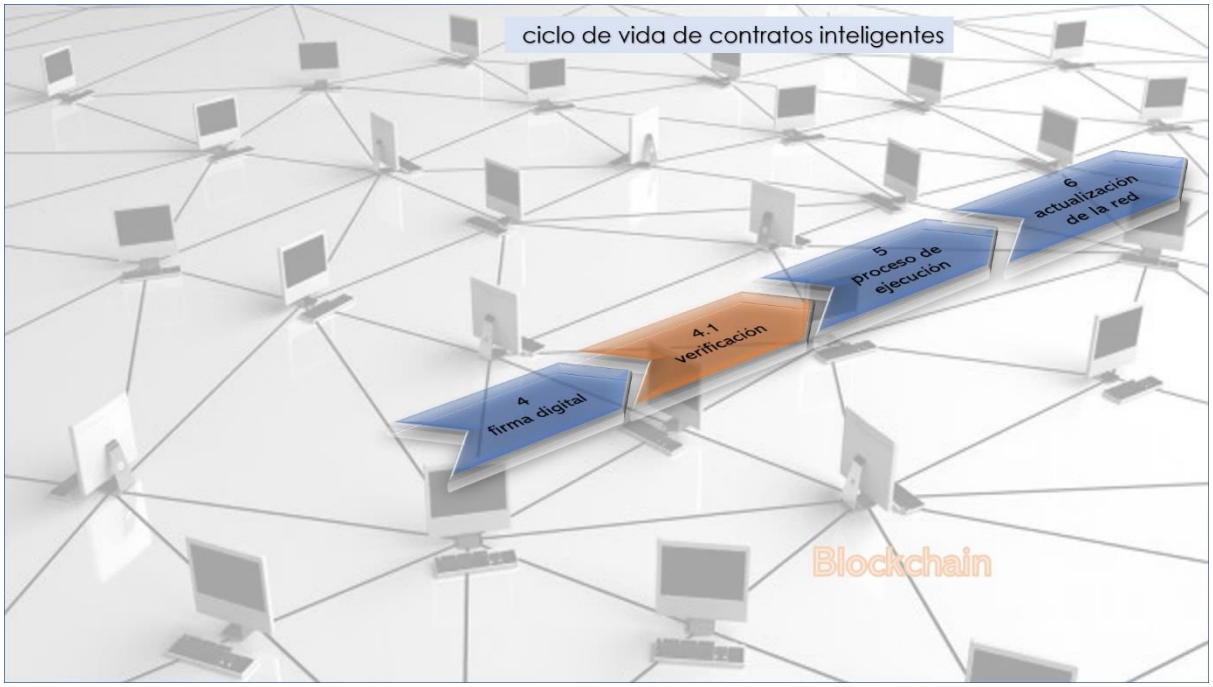


Figura 16 Ciclo de vida Contrato Inteligente Incorporación etapa “verificación” entre etapas 4 y 5

Algunas de las herramientas que los analistas y desarrolladores tienen para poder desarrollar los procesos de testing son:

Editores de código: se puede desarrollar el código de los contratos inteligentes en cualquier editor de texto. Algunos editores disponen de correctores de sintaxis específicos para verificar la correcta escritura de Solidity. Por ejemplo: Visual Studio Code, Sublime Text, Atom, entre algunos de los gratuitos y de amplia difusión. Algunos de estos, como VS Code, integran el compilador al editor de modo, de poder realizar la edición del programa y compilarlo (transformarlo en programa ejecutable) en un mismo entorno.

Editores/Compiladores: como mencionamos en el punto anterior, algunos editores de código traen integrado el compilador de Solidity. Si decidimos hacer este proceso por separado, del sitio de Ethereum podremos descargar “solc”, el compilador desarrollado específicamente para la Cadena de Bloques.

También dentro de esta categoría podemos mencionar “Remix”, framework integrado de editor, compilador y despliegue de contratos inteligentes basados en Ethereum, el cual corre desde la web, y dentro del site de Ethereum Organization[7]

También podemos destacar a Open Zeppelin, otro framework integrado, pero preferido por programadores, arquitectos y desarrolladores de Contratos Inteligentes, por su alta capacidad de detección y corrección de vulnerabilidades.[8]

Emuladores locales de la Blockchain Ethereum: se pueden descargar en forma libre y gratuita “emuladores” de la red Ethereum, para hacer correr en forma local (en nuestra máquina) nuestros desarrollos de contratos inteligentes, antes de desplegarlos en la Blockchain Ethereum. En este caso el emulador nos va a permitir trabajar como si estuviésemos conectados con la Blockchain, emulando en forma local todos los procesos vinculados a la Cadena de Bloques, tales como consultar saldos de cuentas, minerar bloques, realizar transacciones, y desplegar y ejecutar contratos inteligentes.

Redes de prueba (TestNets): son Blockchains clonadas de Ethereum, pero con determinadas modificaciones que nos habilitan a poder desplegar en ellas nuestros contratos y testearlos, de manera de poder contar con un entorno de testing, tal como si interactuamos con la red Ethereum real.

Algunas de las más divulgadas son: Sepolia, Goerli.

Estas redes de testing son gratuitas, no debemos pagar con Ethers para ejecutar transacciones, o desplegar contratos inteligentes, como lo hacemos en la mainnet de Ethereum (red principal).

Sin embargo, y para cumplir con todos los aspectos funcionales que tiene Ethereum, cada operación que hacemos en ellas consumen GAS (el pago que se hace a los mineros en Ethers). La diferencia es que la adquisición de los Ethers con que vamos a trabajar en estas redes, es gratuito. Hay que solicitarlos por medio de algún método de autenticación, como informar un email, o publicar durante un día una clave en Facebook, la cual nos es suministrada por la red de pruebas.

Esto permite la red de testing no se sature (se entrega cada vez que se solicita una cantidad chica de Ethers, 5 o 10), y tampoco esté expuesta a los ataques maliciosos de DoS, que mencionamos anteriormente.

Dentro de las comunidades de Blockchain, se suele asignar estos nombres a las Cadenas de Bloques que mencionamos:

Ownnet: es lo que designamos en los párrafos anteriores como Emuladores locales de la Blockchain. Emula el funcionamiento completo de la Blockchain, pero corriendo local, en mi computadora.

---

[7] Ethereum Remix - http://remix.ethereum.org - Observado: noviembre 2022
[8] Open Zeppelin - https://www.openzeppelin.com/ - Observado: noviembre 2022

Testnet: las redes de prueba, totalmente funcionales y copiadas de Blockchains públicas, con la salvedad que mencionamos de poder adjudicarnos gratuitamente criptomonedas, para poder realizar las pruebas

Mainnet: la Blockchain propiamente dicha, donde circula su criptomoneda específica, y se perfeccionan transacciones con sus correspondientes transferencias de valor.

Una vez que nuestro contrato haya sido testeado, bajo stress y en profundidad, estará listo para que lo despleguemos en la Blockchain de Ethereum, o en la Blockchain privada o de consorcio que hayamos decidido utilizar.

Vulnerabilidades

Un campo amplio y de gran desarrollo potencial en la actualidad es el de la auditoría de contratos inteligentes. Podemos diferenciar dos ramas claras, en ese aspecto.

La auditoría técnica del contrato, vinculada a funcionalidad y vulnerabilidades en la ejecución de los contratos inteligentes. Por otro lado, la auditoría funcional de estos, vinculada a si los contratos realizan aquello para lo cual fueron creados, y si en la lógica de los procesos y acciones que ejecuta, hay vulnerabilidades intrínsecas al contrato.

Solo para mencionarlo, las vulnerabilidades que se presentan en desarrollo de contratos inteligentes, se suelen clasificar en:

- Ataques externos: cuando un actor externo, malicioso, se aprovecha de una vulnerabilidad del contrato.

- Ataques de entorno: cuando un actor externo, malicioso, ataca el “front-end” del contrato inteligente (por ejemplo las billeteras de los usuarios) para hacerse de las claves privadas de los participantes, y suplantarlos, beneficiándose con esta maniobra.

- Vulnerabilidades intrínsecas del contrato: cuando la lógica de ejecución del programa que gobierna el contrato, posee errores que pueden llevar a generar acciones no deseadas, o directamente el quiebre o caída del contrato inteligente.

- Vulnerabilidades de minería: cuando los mineros se valen de errores en la codificación del programa para beneficiarse con estas acciones.

Nos parece relevante mencionar que, al momento de controlarse vulnerabilidades técnicas del desarrollo de software del contrato, es importante verificar las vulnerabilidades conocidas y publicadas por la comunidad de la Blockchain con la que trabajaremos.

En el caso particular de Ethereum, la Blockchain más utilizada para desplegar contratos inteligentes, es de utilidad controlar si el contrato cumplimenta las vulnerabilidades consignadas en SWC Registry:[9]

[9] SWC Registry - https://swcregistry.io/ - Observado: noviembre 2022

https://swcregistry.io/

SWC Registry

Smart Contract Weakness Classification and Test Cases

The following table contains an overview of the SWC registry. Each row consists of an SWC identifier (ID), weakness title, CWE parent and list of related code samples. The links in the ID and Test Cases columns link to the respective SWC definition. Links in the Relationships column link to the CWE Base or Class type.

ID	Title	Relationships	Test cases
SWC-136	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method	• odd_even.sol • odd_even_fixed.sol
SWC-135	Code With No Effects	CWE-1164: Irrelevant Code	• deposit_box.sol • deposit_box_fixed.sol • wallet.sol • wallet_fixed.sol
SWC-134	Message call with hardcoded gas amount	CWE-655: Improper Initialization	• hardcoded_gas_limits.sol
SWC-133	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay	• access_control.sol • access_control_fixed_1.sol • access_control_fixed_2.sol
SWC-132	Unexpected Ether balance	CWE-667: Improper Locking	• Lockdrop.sol
SWC-131	Presence of unused variables	CWE-1164: Irrelevant Code	• unused_state_variables.sol • unused_state_variables_fixed.sol • unused_variables.sol • unused_variables_fixed.sol
SWC-130	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	• guess_the_number.sol
SWC-129	Typographical Error	CWE-480: Use of Incorrect Operator	• typo_one_command.sol • typo_safe_math.sol • typo_simple.sol
SWC-128	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	• dos_address.sol • dos_number.sol • dos_simple.sol
SWC-127	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality	• FunctionTypes.sol
SWC-126	Insufficient Gas Griefing	CWE-691: Insufficient Control Flow Management	• relayer.sol • relayer_fixed.sol

Tabla 3 Vulnerabilidades consignadas en SWC Registry

ECOSISTEMA BLOCKCHAIN

Como ya mencionamos, la Blockchain es la tecnología disruptiva e innovadora, que se desarrolló para dar sustento al funcionamiento de las criptomonedas, esencialmente al Bitcoin.

En la actualidad, y como lo hemos destacado, su uso no se ve limitado al soporte de criptomonedas abiertas (permissionless). Cada día hay más desarrollo de proyectos de sistemas distribuidos basados en Blockchain, vinculados con las más dispares áreas de actividades, tales como salud, identidad digital, FinTech, y otros.

Este crecimiento continuo de desarrollos y variantes que se presentan sobre la tecnología de Blockchain, induce a tener que realizar un periódico relevamiento de las herramientas, artefactos, y posibilidades que tenemos a disposición en referencia a la misma.

A todos esos elementos, damos a llamar el ecosistema de la Blockchain.

Es importante esta visión, para poder conceptualizar y clasificar, elementos, herramientas y oportunidades que se nos presentan para encarar el desarrollo de soluciones basadas en esta tecnología.

Modelo de Ecosistema de Blockchain IMDA-MAS (2020)

La dinámica impresa por los desarrollos vinculados a la tecnología de Blockchain, parece a veces muy variante, incorporando permanentemente nuevas ideas, implementaciones y procesos de desarrollos. Por esta razón, nos parece conducente presentar un último modelo de Ecosistema Blockchain, más actualizados a los dos anteriores. Si bien, el tiempo transcurrido desde los dos modelos anteriores que presentamos, hasta la actualidad, no es mucho (3 y 4 años), con la vertiginosidad de los cambios que se dan en desarrollos, artefactos, y elementos del Ecosistema, hacen sugerible incorporar este nuevo modelo.

El modelo que presentamos fue desarrollado por IMDA - Infocomm Media Development Authority y MAS - The Monetary Authority of Singapore, recientemente en el año 2020.

La siguiente imagen presenta la visión y clasificación de elementos del modelo:

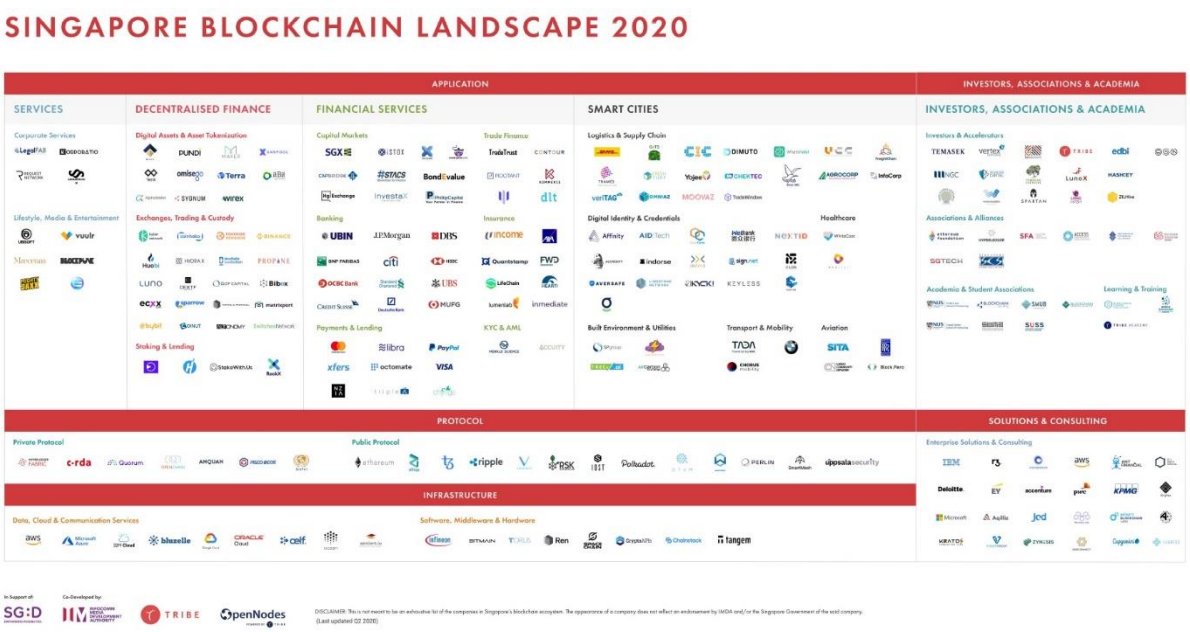


Figura 17 Modelo de Ecosistema de Blockchain IMDA-MAS (2020)

FINANCIACIÓN EMPRESARIAL POR MEDIO DE BLOCKCHAIN

Vamos a analizar las prácticas más comunes que se han desarrollado para que pequeñas, medianas empresas y emprendedores accedan a autofinanciación por medio del uso de la Blockchain y Contratos Inteligentes.

Para esto vamos a hacer un enfoque inductivo, yendo desde el desarrollo más atómico o particular, hacia los desarrollos más amplios o abarcativos.

Veremos en esta secuencia los siguientes elementos:

- ✓ Tokens
- ✓ Nueva criptomoneda
- ✓ ICO: oferta inicial de criptomonedas
- ✓ DAO: organizaciones autónomas descentralizadas

Desde el punto de vista del acceso a autofinanciación empresarial por medio de Blockchain

- Contratos Inteligentes, nuestro enfoque va a estar centrado principalmente en el desarrollo de ICOs (ofertas iniciales de criptomonedas), ya que el desarrollo posterior en esta secuencia, es decir, las DAO (organizaciones autónomas descentralizadas) tienen más relación con la gestión de procesos de negocio internos de las organizaciones, que con las estrategias de financiación de estas.

La siguiente imagen muestra el enfoque incremental de conceptos mencionado:

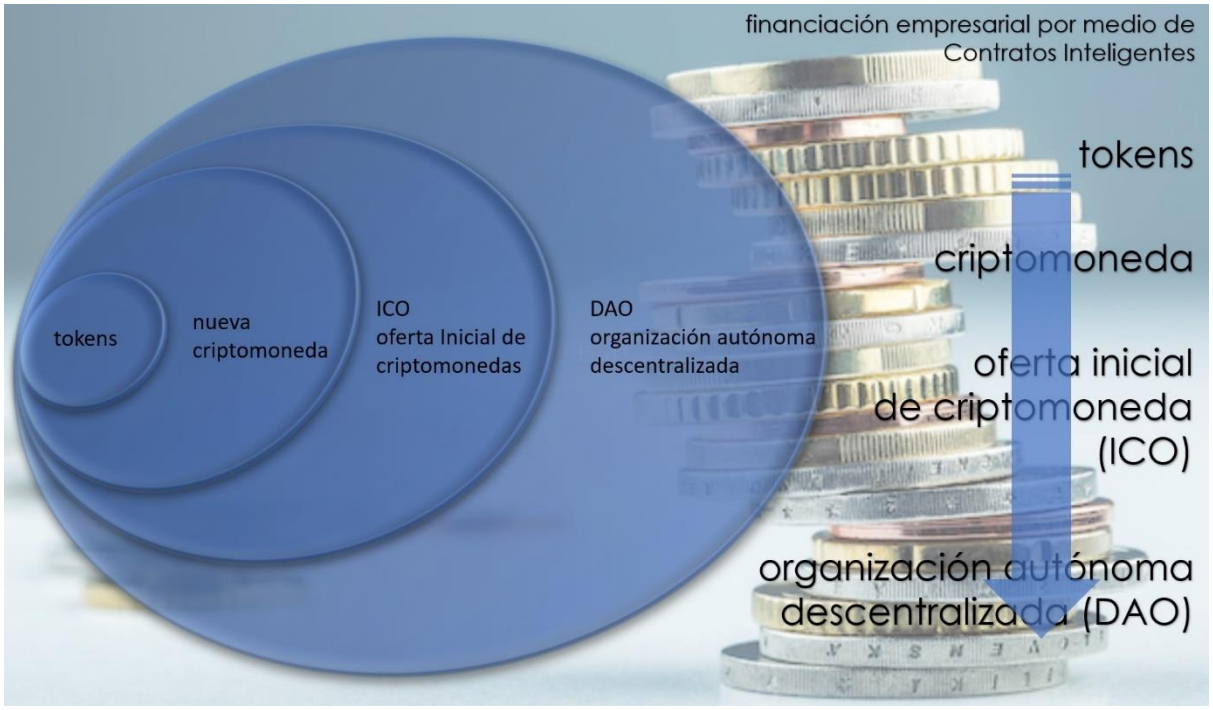


Figura 18 Financiación empresarial por medio de contratos inteligentes

Tokens: es un concepto fundamental que debemos ver en el desarrollo de Contratos Inteligentes.

Si vamos a una definición genérica de Tokens, podríamos decir que son:

"*Una representación digital, sobre una Blockchain, de un bien, derecho o servicio*".

La definición es muy amplia y abarcativa.

La idea que gobierna al concepto de token es la posibilidad de desarrollar sobre la Blockchain, un código de programa que permita gestionar valores, identificándolos inequívocamente, y de esta manera poder utilizarlos para representar, bienes, servicios o derechos. También, ligado a esta posibilidad se encuentra la capacidad de los tokens de fraccionar esos valores, y transferirlos con facilidad.

Límites difusos de conceptos

Como mencionamos al principio, vamos a ver que los límites en las definiciones que vamos a analizar aquí, son difusos. No son blancos y negros, sino grises. Veamos algo derivado de esta definición de tokens.

Unos de los tokens de los que vamos a hablar cuando desarrollemos la clasificación de estos, son los tokens de criptomonedas.

Ethereum permite desplegar contratos inteligentes. Por medio de ellos puedo ejecutar la lógica de un programa. Se han desarrollado plantillas específicas de contratos inteligentes, que corran sobre la Blockchain de Ethereum, que permiten crear y gestionar mis propias criptomonedas. La más común y difundida de estas plantillas es la que se denomina Token ERC20.

La cuestión es que estas "nuevas" criptomonedas que uno puede crear sobre Ethereum, pueden tener las mismas características y funcionalidades que el Ether, la criptomoneda propia de Ethereum. De allí que algunos autores afirman que las criptomonedas propias de las Blockchains (Ethereum, Bitcoin, …) son en sí, tokens. Por esa razón es que, para estos autores, o en muchas publicaciones, vamos a encontrar el término tokens utilizado como sinónimo de criptomonedas. En nuestra opinión esto lleva a una confusión innecesaria.

Para cerrar esta idea, deberíamos destacar que, si bien las funcionalidades de los tokens de criptomonedas son las mismas de las "criptomonedas nativas", estas corren sobre el software propio de la Blockchain (fueron creadas al crear la Blockchain correspondiente), mientras que los tokens de criptomonedas son desarrollos hechos por usuarios de la Blockchain, que se despliegan sobre esa Cadena de Bloques. Por ejemplo, si yo genero un contrato inteligente, que despliego sobre Ethereum, para que cree y gestione una nueva criptomoneda.

Más adelante vamos a ver que también encontraremos límites difusos entre los conceptos de Tokens de criptomonedas y ICOs, y en entre los conceptos de ICOs y DAOs. Sin embargo, estas distinciones de términos, que algunas veces resultan sutiles, no nos tienen que hacer perder la finalidad de comprender la dinámica de todos estos desarrollos de avanzada realizados sobre contratos inteligentes.

Características de los tokens

Veamos algunas características distintivas de los tokens**:**

Liquidez: pueden con relativa facilidad ser canjeados por efectivo, o por otras criptomonedas que tengan mercados transparentes y accesibles

Divisibilidad: al igual que las criptomonedas nativas desarrolladas al crear las Blockchains, los tokens utilizan un fraccionamiento muy atómico de los valores que representan. La idea, tras esta característica es la de facilitar transacciones chicas, y evitar tener que lidiar con la problemática de manejo de decimales y redondeos en las transferencias de tokens. A modo de ejemplo, mostramos la división que hace el Bitcoin de su valor unitario, en “Satoshis”, la unidad de medida en que se expresan sus transacciones

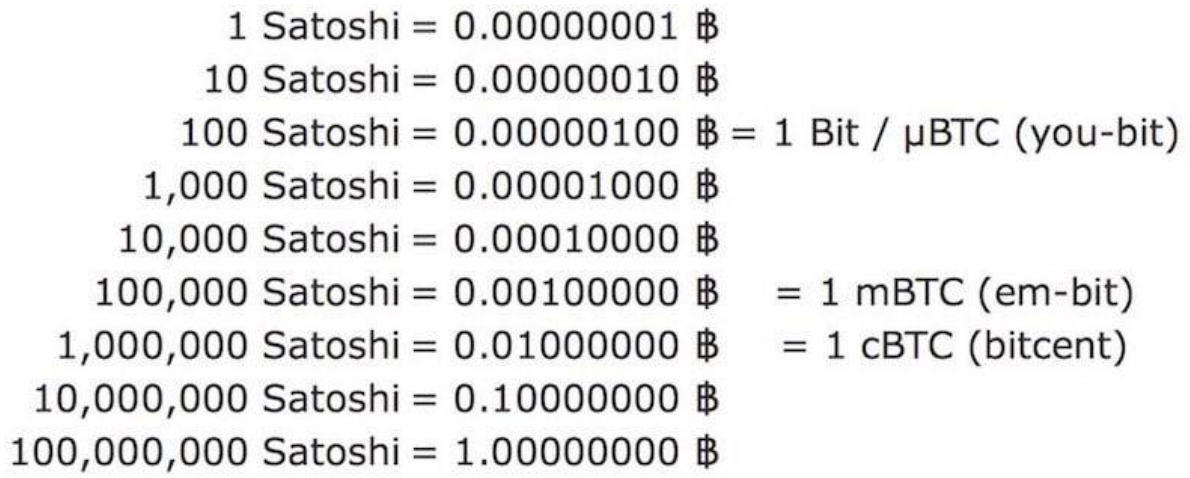


Figura 19 Características de los tokens “Divisivilidad”

Comercializables y de fácil transferencia: los tokens hacen uso de la infraestructura de la Blockchain en la que se despliegan, y de esta manera pueden transferirse sus valores, con rapidez y transparencia, por medio de transacciones volcadas en esa Cadena de Bloques.

Titularidad: es una de las condiciones esenciales de un token, identificar inequívocamente los derechos, servicios o bienes que representan. Para esto los contratos inteligentes que soportan los tokens, hacen uso de toda la infraestructura de encriptación que utiliza la Blockchain para asegurar identidad, propiedad y derechos de los tokens

Clasificación de tokens

Muchos autores han propuesto diferentes clasificaciones para identificar tipologías de tokens.

Nuestro abordaje aquí no pretende ser un mero ensayo académico de la cuestión, sino que pensamos, que por medio del estudio de estas clasificaciones podemos brindar una visión más amplia de las diversas funcionalidades que se le puede dar al desarrollo de tokens por medio de Contratos Inteligentes.

La clasificación más sencilla e intuitiva sobre el tema es la que desarrollaron Luis Oliveira, Liudmila Zavolokina, Ingrid Bauer and Gerhard Schwabe, en un trabajo de la Universidad de Zurich . Ellos clasifican a los tokens en:

Clasificación de Universidad de Zurich

Tokens de criptomonedas:

En estos casos el token desarrollado actúa como una criptomoneda pura, que puede ser transferida libremente, y su adquisición se puede realizar en un mercado al precio determinado por su demanda. Estos tokens son desarrollados con la aspiración de convertirse en criptomonedas populares y de amplia circulación en el mundo.

Tokens de acciones:

Estos tokens emulan el funcionamiento de las acciones de sociedades anónimas en la vida real. Representan una participación en el capital, y otorgan derecho al cobro de utilidades sobre el mismo, en función de un reparto de utilidades.

Tokens de fondeos o capital:

Pensados en términos de ser una forma de financiamiento para el desarrollo de proyectos o iniciativas empresariales, y tienen como objetivo actuar como instrumento de financiamiento a largo plazo.

Tokens de consensos:

Diseñados para ser el medio de pago de recompensas prestablecidas, para los nodos que colaboren dentro de la Blockchain, en la validación y gestión de transacciones y en la generación de consensos. Al igual que en el caso de los tokens de criptomonedas y teniendo en cuenta la salvedad que hicimos al respecto, deberíamos separar aquellas criptomonedas que la Blockchain genera en forma “nativa” para retribuir a los mineros, de los tokens que se puedan desplegar sobre la Blockchain, por medio de contratos inteligentes (forma no nativa), para recompensar a los gestores de validación y consensos.

Tokens de trabajo:

Son usados como medio de compensación o incentivo para determinados usuarios que realizan una actividad o denotan algún comportamiento que se desea estimular.

Tokens de votación:

Son aquellos tokens que les permiten a determinados usuarios de la Blockchain votar en determinadas decisiones. Están ligados, en general, a lo que se denominan los contratos inteligentes de “democracy”, y se encuentran vinculados con los derechos de votos asignados por el Smart Contract. En algunos casos, serán de un solo voto por usuario, cantidad de votos en función del capital aportado, juego de votos simples y votos privilegiados y otros.

Tokens de activos:

Tokens creados como representación de activos del mundo real. Aquí entra en juego, en la mayoría de los casos, la figura del “trusted”, es decir quien dará fe en el mundo real de la disposición de ese bien, en favor del propietario del token.

Tokens de pagos:

Instrumentos de pago, en representación digital, dentro de un sistema de plataforma o un ecosistema tecnológico determinado.

Clasificación de Euler

Al ser la definición de tokens tan amplia, permite la representación por medio digital de todo tipo de bienes, derechos y servicios, creando un amplísimo abanico de posibilidades.

Un enfoque interesante para abordar este tema es la clasificación que propone Thomas Euler, clasificando los tokens de Blockchain según diferentes dimensiones

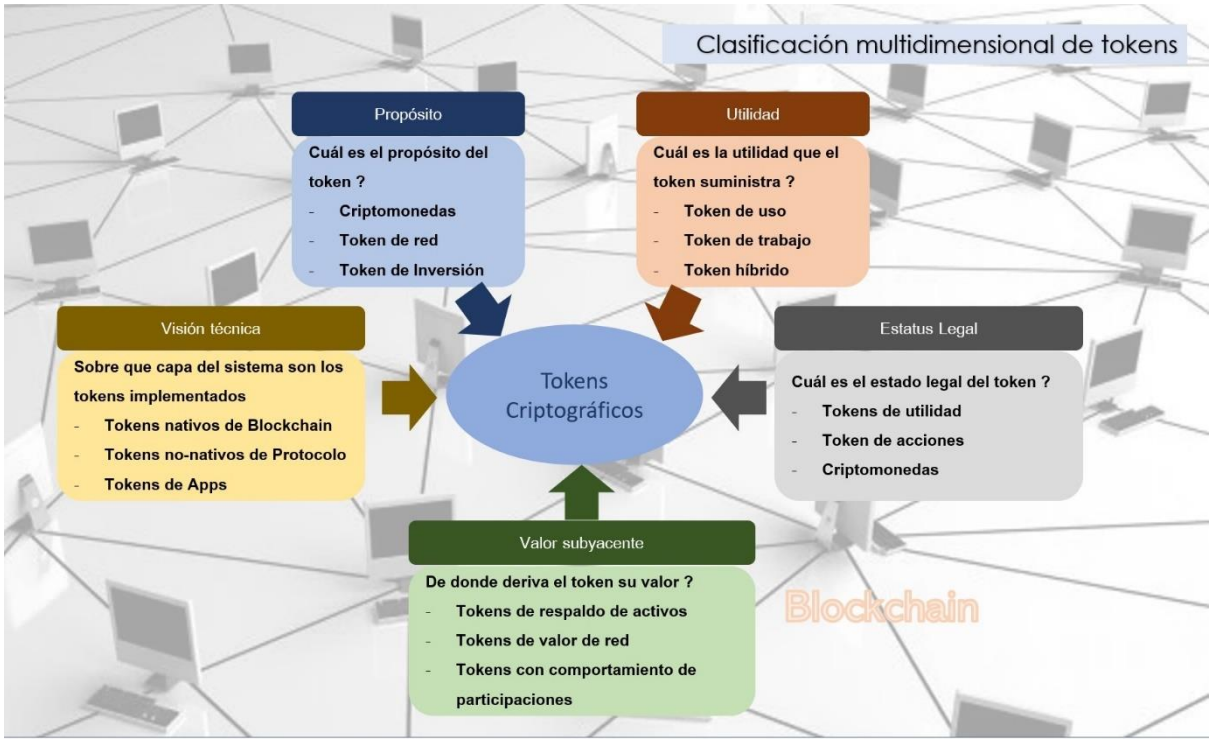


Figura 20 Clasificación multidimensional de tokens

Tokens ERC20:

Como vimos en estas clasificaciones de tipos de tokens que se desarrollan sobre la Blockchain, unos de los tipos más destacados son los tokens de criptomonedas y los de fondeos o capital.

En el tema siguiente vamos a adentrarnos en el tipo de tokens de fondeo o capital, que se utilizan como recurso de financiación empresarial para nuevos proyectos o emprendimientos.

Reciben el nombre de ICOs (Initial Coin Offering), haciendo una referencia tácita a las siglas IPOs (Initial Public Offering), que se utilizan en las Bolsas para designar el momento en que empresas comienzan a hacer oferta pública de sus acciones.

La mecánica básica del lanzamiento de una ICO en una Blockchain, se centra en desarrollar un Contrato Inteligente que pueda emitir una nueva criptomoneda. Esa criptomoneda es ofrecida al público en general, para ser canjeada por una criptomoneda de uso generalizado y mercado transparente, por ejemplo: Ethers.

Los Ethers que el generador de la ICO reciba, serán utilizados para financiar el desarrollo de una actividad económica planificada. Y seguramente ofrecerán un rendimiento, a pagar a futuro, sobre la inversión que la persona que transfiere al Contrato Inteligente haga.

Esta práctica, muy discutida y polémica, ha tenido un gran crecimiento y desarrollo en el ecosistema de Blockchain, especialmente en Ethereum donde se han desarrollado la mayor cantidad de ICOs.

¿Qué vendría a ser entonces el token ERC20?

Podemos explicarlo por medio de un ejemplo. Supongamos que queremos crear un documento nuevo de Word, para realizar un informe empresarial. Cuando clickeamos en la opción “nuevo documento”, Word nos va a ofrecer crear un nuevo documento en blanco, o nos va a sugerir, entre un juego de “templates”, elegir la plantilla que mejor se adecue a nuestra necesidad.

Si, por ejemplo, quisiéramos unificar determinados informes que los empleados de una empresa deben confeccionar, podríamos generar nuestro propio “template” con formato, estructura de información, tablas, etc…

Algo semejante es lo que ocurre con el Token ERC20.

Podríamos decir que el Token ERC20 es un contrato inteligente estándar, que actúa como una plantilla, para que otros desarrolladores de contratos inteligentes puedan utilizarlo para desarrollar, básicamente nuevas criptomonedas, u otras implementaciones más avanzadas como ICOs, DAOs, etc…

ERC20 funcionalidad

Desde el punto de vista de negocio el Token ERC20, lo podemos comparar a una plantilla predefinida con las funciones elementales que debe tener una nueva criptomoneda. Desde el enfoque de sistemas, y más específicamente, desde la óptica de programación orientada a objetos, el Token se puede equiparar a una interfaz.

Las funcionalidades (métodos y eventos) que expone son:

Métodos requeridos:

totalSupply(): expone la cantidad total de tokens de un tipo que se han emitido.

balanceOf(): esta funcionalidad recibe como información una cuenta, y devuelve el total de tenencia de tokens de un tipo que esa cuenta posee.

allowance(): recibe como información una cuenta, y devuelve como dato el total de tokens de un tipo que esa cuenta ha sido autorizada a transferir. La autorización fue realizada por la cuenta propietaria de esos tokens.

transfer(): esta función es la transacción base donde se identifica la cuenta destino y la cantidad de tokens a transferirle. Devuelve un binario (un si o no), de acuerdo a si la transferencia se pudo realizar o no.

approve(): esta función perfecciona la aprobación de la cuenta propietaria de tokens, en favor de una cuenta autorizada para que esta pueda disponer de gastar un número determinado de tokens. En el caso de allowance() la función devuelve el total de tokens que se han autorizado por este método (en el caso que se hayan hecho varias autorizaciones en el tiempo).

transferFrom(): funciona igual que transfer(), con la única diferencia que en este caso se debe suministrar la cuenta origen y la cuenta destino, además de la cantidad de tokens a transferir. Se pueden hacer transferencias simples por este método, pero se lo usa específicamente, cuando la cuenta origen no es la cuenta propietaria, sino que es una cuenta autorizada previamente por el método approve().

Eventos:

Los eventos sirven en programación para que el desarrollador asigne un código que el contrato va a ejecutar ante el suceso de ese evento. De esta manera se puede controlar el comportamiento del contrato, cuando ocurren determinadas circunstancias.

Los eventos con que expone el Token ERC20 son:

Transfer(): captura el evento de la transferencias de tokens de un cuenta a otra.

Approval(): captura el evento de la aprobación que la cuenta propietaria de determinados tokens, da a la cuenta autorizada para poder transferirlos.

Métodos adicionales, optativos:

El token ERC20 también posee tres métodos adicionales, que no son obligatorios de implementar, pero pueden resultar de utilidad al desarrollador. Ellos son:

name(): el nombre asignado al nuevo token que se está creando

symbols(): el nombre corto, que se va a utilizar para identificar a es token

decimals(): cantidad de decimales que el token tendrá para su manejo

Por último, queremos destacar que no es necesario utilizar el Token ERC20 de Ethereum, si deseamos desarrollar un Contrato Inteligente que genere una nueva criptomoneda, o en un caso más avanzado, sustente una ICO. Sin embargo, por el hecho de ser un template que expone funcionalidades básicas de cualquier criptomoneda, estar debidamente probado para su uso, y tener una divulgación masiva en la comunidad Ethereum, ha pasado a ser considerado por los desarrolladores como parte de la infraestructura de la Blockchain. Simplemente, nadie quiere reinventar la rueda.

ICO – Initial Coin Offering

No existe una clara definición ICO (Initial Coin Offering), sino que la mayoría de los autores optan por conceptualizarlas mediante la descripción de su alcance y funcionamiento.

Juntando algunas descripciones otorgadas por varios autores (Henri Arslanian, David Kuo Chuen y otros…), podemos intentar una definición como la siguiente:

ICO (Initial Coin Offering) es un intercambio dado entre nuevos tokens de criptomonedas y criptomonedas de mercados líquidos y accesibles, que permiten a iniciativas, proyectos y start-ups basadas en Blockchain financiar la ejecución de sus actividades.

Por ejemplo, si una start-up desea fondear un proyecto de desarrollo de una aplicación, puede desplegar sobre Ethereum una ICO. De esta forma emitir un nuevo token de criptomoneda, es decir, su propia criptomoneda, ligada a ese proyecto.

Cada unidad de la nueva criptomoneda, tendrá una paridad asignada contra Ehters, la criptomoneda de Ethereum.

El contrato inteligente que regula esa ICO que se ha creado, puede estar desarrollado sobre el Token ERC20, que como vimos, identificará la cantidad total de la nueva criptomoneda emitida. Ese será el total del capital que se espera sea integrado.

Cada aportante a la ICO, transferirá a favor del Contrato Inteligente que gobierna esa ICO, una cantidad de Ethers, recibiendo por medio de la paridad establecida, una cantidad de la nueva criptomoneda.

La Start-up con los Ethers recaudados, podrá recurrir a un Exchange de criptomonedas (una casa de cambio), y cambiar esos Ethers por dólares, para poder comenzar a financiar su actividad.

Esa es la dinámica básica y más común que posee una ICO.

Vamos a analizar con más detenimiento los pasos que se deben dar para el desarrollo e implementación de una ICO, pero por el momento es importante destacar dos aspectos.

1. Las dos diferencias más destacables entre este tipo de financiación (ICO), en lugar de la tradicional IPO (Initial Public Offering – Oferta Pública de acciones inicial), están dadas por el alcance del crowfunding de la ICO, el cual es global, y la falta de regulación de la ICO, en contraste con la extremada cantidad de regulaciones de una emisión de acciones.

2. Mencionamos en nuestro ejemplo que el contrato inteligente que va a gobernar la ICO, “puede” estar desarrollado sobre el estándar del Token ERC20. Hoy en día, el token ERC20 ha sido prácticamente incorporado a la infraestructura de la Blockchain Ethereum, al punto que es muy poco probable que una ICO tenga éxito si no lo utiliza. Es prácticamente un estándar “de facto”.

La mayoría de los reguladores de mercados de capitales, han emitido “warnings” (advertencias) acerca de como manejarse con financiamientos realizados por medio de ICOs, estando el planes de muchos de ellos (algunos ya lo han hecho) la emisión de normas de regulación. Para citar solo algunos, podemos mencionar, USA, Inglaterra, Canada, Australia, Hong Kong, Dubai, Singapur, China, Brasil y otros.

En el caso de Argentina, la CNV ha emitido una advertencia en fecha diciembre de 2017. Dicha advertencia destaca 7 riesgos inherentes a una inversión en ICO:

(a) falta de regulación específica,

(b) volatilidad de los precios y riesgos de liquidez,

(c) potencial fraude,

(d) inadecuado acceso a información relevante,

(e) proyectos en etapa inicial,

(f) fallas tecnológicas y de infraestructura y

(g) Carácter trasnacional de las negociaciones con ICOs.

Análisis comparativo de ICOs con IPOs

Como ya mencionamos las siglas ICO fueron adoptadas en relación a las siglas utilizadas para designar la primera venta de acciones que realiza una compañía que abre su capital en la Bolsa – IPO Initial Public Offering.

Para empezar a adentrarnos en el concepto y funcionamiento de las ICOs podemos realizar una comparación entre ambos métodos de financiamiento empresarial, las ICOs, y IPOs.

Cuadro comparativo Financiación empresarial por medio de ICOs y IPOs[10]

Aspecto evaluado	**ICOs**	**IPOs**

[10] Algunos criterios fueron extraídos de:
Lee, D. K. C., & Low, L. (2018). Inclusive fintech: blockchain, cryptocurrency and ICO. World Scientific.
Monitor Deloitte: IOCs – The new IPOs. Deloitte & Touche Tohmatsu Limited

Propósito del inversor	Rentabilidad por obtener. La propiedad sobre la inversión puede ser considerada secundaria	Rentabilidad por obtener. Ejercicio de la propiedad y poder de voto.
Propósito del desarrollador	Fondeo de una nueva iniciativa o proyecto	Consolidación del negocio. Acceso a financiamiento más económico por medio del mercado de capitales.
Iniciadores	Nuevos desarrolladores de negocio. Plan de negocio expuesto por medio de un White Paper.	Negocios establecidos y consolidados. Activos comprobados y certificados por profesionales
Costo de desarrollo y divulgación	Mediano a bajo. El foco se suele poner en poder transmitir con claridad la idea de negocio a potenciales inversores	Alto. Al tener regulaciones estrictas, el plan de desarrollo de una IPO incluye altos costos de consultoría especialmente en aspectos de compliance.
Regulación	Actualmente no reguladas, o con regulaciones incipientes.	Fuertemente reguladas por autoridades definidas.
Inversores	Entusiastas, partidarios, que esperan retorno de su inversión	Inversores institucionales y privados. Generalmente inversores profesionales.
Alcance de los inversores	Global.	Regional, generalmente vinculado al mercado específico en que se realice la oferta pública.

Verificación de inversores	Al no ser reguladas, o tener regulación incipiente, no se realiza generalmente la verificación del inversor.	Reguladas por normativas fiscales y de combate al fraude y lavado de dinero.
Tamaño de las transacciones	Pequeñas y medianas. Vinculadas al tipo de ICO específica	Grandes o medianas, dependiendo del mercado
Facilidad de transferencia	Alta facilidad de transferencia con costo de transacción mínimos	Alta facilidad de transferencia con costos medianos a altos de intermediación en mercados
Riesgos	Alto nivel de riesgo. Actualmente la protección del inversor es baja	Mediano. Dependiente de las regulaciones del mercado en que se negocien.

Tabla 4 Comparativo financiación empresarial por medio de ICOs y IPOs

ICO – Hoja de ruta

Hay muchos trabajos desarrollados en aspectos relativos a los pasos metodológicos que se deben tener en cuenta para la implementación exitosa de una ICO, como así también códigos de buenas prácticas vinculadas a esos aspectos.

Vamos a orientarnos en esta parte, con un trabajo desarrollado por Ezequiel Djeredjian, con algunos agregados y sugerencias derivadas de otros autores.[11]

Hoja de ruta para el desarrollo de una ICO

Conceptualización del proyecto: Como cualquier startup tradicional, todo parte de una idea para solucionar un problema.

Armado del equipo central de trabajo (core): el fundador o los fundadores reúnen a los miembros del equipo central que impulsarán el proyecto.

[11] Ezequiel Djeredjian (2018) ICO Checklist: How to Setup a Successfun Initial Coin Offering from Idea to Funding – Medium.com

https://medium.com/blockchain-review/ico-checklist-how-to-setup-a-successful-initial-coin-offering-from-idea-to-funding-b7fdf035dc68

Observado: Junio 2020

Planificación del producto: Con un equipo de diversos miembros capacitados se definen decisiones importantes como la tecnología a utilizar, la funcionalidad del producto, las características del token / ICO, etc.

Definir estrategias de protección de los intereses de inversores: ante la volatilidad y falta de regulación robusta con que se desarrollan las ICOs, es crucial definir las estrategias de resguardo del aporte que realizarán los inversores, para poder comunicarles esta con claridad en propuesta.

Conseguir asesores: se debe superar las deficiencias de su equipo con personas experimentadas que puedan brindar asesoramiento, tutoría y conexiones.

Definir estrategias de mercado: se debe analizar detalladamente el mercado de inversores al que se apunta y las estrategias para abordarlo exitosamente

Marketing de producto / comunidad: comenzar a promover una comunidad comprometida y, lograr introducir el proyecto en la comunidad. Crear un plan de comunicación para presentar el producto y la visión de la iniciativa.

Definición de aspectos técnicos del desarrollo: plataforma de Blockchain sobre la cual desplegar la ICO, arquitectura de software, buenas práctica de programación y despliegue del contrato inteligente y otros.

Desarrollo de un White Paper: crear un White Paper para presentar el problema, la solución, el producto y su tecnología, el token y la ICO, equipo, negocio, etc.

Publicación de una hoja de ruta: presentar un plan de acción demostrando la factibilidad de propuestas, desarrollos e hitos, y de esta forma mostrar el compromiso del equipo responsable ante la comunidad y los entusiastas.

Buscar consejo y encuadre legal: Definir la jurisdicción y conformar el comité legal que asesorará sobre la legislación correspondiente, incluyendo estructura corporativa, impuestos, valores, normativas de lavado de dinero, etc.

Marketing de venta de tokens: se buscará en este paso realizar el anuncio y desarrollo de una estrategia de comunicación para informar a las personas sobre la venta de tokens, los detalles del token, su distribución, términos de venta, etc.

Publicación de código y auditorías: comparta su código de programas de Contratos Inteligentes para su revisión e idealmente haga que un servicio de auditoría específico de revisión.

Venta de tokens (preventa opcional): se ejecutará la venta colectiva real o una preventa (pública o privada) para recolectar algo de dinero "inicial" para el desarrollo.

Conversión de ganancias: los equipos liquidan parte del dinero recibido para asegurar efectivo y financiar la construcción del equipo, la tecnología y el negocio.

Lanzamiento de prototipo: cuanto antes se presente un prototipo, mejor. Si es antes del ICO aún mejor.

Informes de transparencia y posventa: después de que se completa el fondeo de una ICO, comienza el trabajo real y la responsabilidad hacia su comunidad. Ser transparente, mostrar avances y mantener actualizaciones constantes es fundamental.

Evaluación de desarrollo de mercados secundarios: si la ICO resulta exitosa, se deberá analizar la promoción de venta secundaria de tokens (la forma que tendrán los inversores de vender a otros usuarios sus tokens) y los aspectos vinculados a divulgación por medio de exchanges.

Pilares y buenas prácticas:

1. Alineación del desarrollo proyectado para la ICO, con la idea de negocio
2. Elección del equipo central (core) de trabajo
3. Comunicación eficiente de la propuesta
4. Claras estrategias de protección de intereses de los inversores
5. Rendiciones de cuentas y gestión, periódicas y detalladas

DAO – Organizaciones Autónomas Descentralizadas

"El problema es encontrar una forma de asociación que defienda y proteja con toda la fuerza común la persona y los bienes de cada asociado, y en la que cada uno, aun uniéndose a todos, pueda obedecer a sí mismo solo y permanecer tan libre como antes." Jean Jacques Rousseau. El contrato Social

La primera idea que queremos retomar, debido a que ya fue mencionada con anterioridad, es la relativa a los límites difusos que podemos observar en los tres tipos de desarrollos avanzados de Contratos Inteligentes que estamos estudiando: Tokens, ICOs y DAOs.

Ya definimos a los Tokens como una representación digital de un activo, un derecho o un servicio. Como vimos, existen diferentes tipos de Tokens que podemos desarrollar por medio de Contratos Inteligentes, sobre la Blockchain. Si nos enfocamos a dos tipos de estos Tokens, los de criptomonedas y los Tokens de fondeo o capital, podemos ver que estos son las base donde podemos desarrollar una ICO.

La definición que dimos de ICO, refiere al financiamiento empresarial que podemos obtener, por medio de la Blockchain, para un nuevo proyecto de una organización en funcionamiento, o para desarrollar desde cero una StartUp.

¿Hasta donde a una ICO se la puede definir como tal, y no solamente como un Token? Como ya lo dijimos, entramos en la discusión (tal vez sin mayor importancia), sobre los límites difusos que hay entre estos conceptos.

Ahora vamos a ver otro desarrollo avanzado de Contratos Inteligentes, y es lo que se denomina DAO – Organización Autónoma Descentralizada. La idea de DAO, la podríamos atribuir a Christoph Jentzsch, quien en 2016 escribió un White Paper donde propuso el desarrollo, por medio de Contratos Inteligentes, de una organización que gestionara su autogobierno sin la intervención humana de gerentes o directores.

Lamentablemente, esta idea verdaderamente disruptiva e innovadora en gestión, terminó empañada por lo que se denominó "el incidente DAO", que como vimos en la historia de Ethereum, se puede considerar una de las horas más negras que tuvo la Blockchain.

Pero volviendo a la cuestión de los límites difusos, podríamos decir que una DAO es un paso más delante en el desarrollo de ICO, donde, además de recaudación de fondos para llevar adelante un proyecto, la gestión de ese proyecto también es gobernado por Contratos Inteligentes desplegados en la Blockchain. ¿Cuál es el límite exacto en que a una ICO dejamos de considerarla como tal, y podemos decir que es una DAO? Hay algunos parámetros que podemos tomar para evaluar esto, pero, una vez más, los límites de esa frontera no son del todo claros.

La idea de DAO

La idea de organizaciones autónomas ha estado presente por años en el diseño de estructuras administrativas y modelos de procesos de negocio. Desde la década del 90, en la que Internet tiene un crecimiento exponencial acompañando el proceso de globalización de mercados, las organizaciones han ido mudando de paradigmas de administración.

Sin dudas, que la plataforma tecnológica que brinda la Blockchain, y su "filosofía" de red de pares, totalmente distribuida, va a generar un impacto en la adopción de nuevos modelos de estructuración de organizaciones basadas en la descentralización. Sin embargo, esta idea ya se viene afianzando, incluso antes del nacimiento de las Blockchains.

Un ejemplo de esto, lo podemos ver en el reconocido libro "La estrella de mar y la araña" de Ori Brafman y Rod A. Beckstrom[12]. En esta obra los autores analizan organizaciones clasificándolas en centralizadas, descentralizadas e híbridas. Comparan a las centralizadas con una araña, que posee 8 patas y una cabeza, y al perder la cabeza, la araña muere. En cambio, las organizaciones descentralizadas se asemejan a la estrella de mar, que no posee una cabeza y al perder una de sus patas, ninguna de las otras lo sufre y la estrella de mar puede volver a regenerarla.

Lo particular de este libro es que fue escrito en el 2006, antes de que Satoshi Nakamoto, lanzase la primer Blockchain, el Bitcoin, y antes de que Vitalik Buterin propusiera el desarrollo de Contratos Inteligentes sobre la Blockchain Ethereum

DAO – Organizaciones Autónomas Descentralizadas

La irrupción que provocaron las Blockchains públicas, en especial la de Ethereum, trajo consigo la posibilidad de contar con una infraestructura tecnológica probada para el desarrollo de sistemas descentralizados. La lógica por la cual la Blockchain valida y registra y sincroniza transacciones en forma descentralizada, y el despliegue de una red de pares (peer-to-peer), brindan el soporte ideal para la implementación de soluciones descentralizadas.

Con esa visión, Christoph Jentzsch propuso en 2016 el desarrollo de una DAO – Organización Autónoma Descentralizada, montada sobre la infraestructura de la Blockchain Ethereum. Pero antes de analizar el lanzamiento de la primer DAO, y su fracaso, con las consecuencias que provocó y que impactan hasta la actualidad, vamos a ver algunas de las definiciones que se les ha dado a la DAO:

"Una organización autónoma descentralizada (DAO), también conocida como corporación autónoma descentralizada (DAC), es una organización que se ejecuta a través de reglas codificadas como contratos inteligentes".[13]

---

[12] Brafman, O., & Beckstrom, R. A. (2006). *The starfish and the spider: The unstoppable power of leaderless organizations*. Penguin.

[13] Bambara, J. J., Allen, P. R., Iyer, K., Madsen, R., Lederer, S., & Wuehler, M. (2018). *Blockchain: A practical guide to developing business, law, and technology solutions.* McGraw Hill Professional.

Ralph Merkle habla de una DAO como una entidad que detenta una propiedad interna, la cual tiene valor, puede actualizar su estado interno, responde a los miembros y ejecuta contratos inteligentes.[14]

Tal vez nos ayude para tener un concepto más definido de lo que es una DAO, o mejor aún, de su potencialidad, echar una mirada a las ventajas que pueden brindar este tipo de desarrollo:

- Coordinar recursos cuando las partes involucradas no se conocen (o no se conocen lo suficientemente bien como para confiar profundamente entre sí)
- Alinear un gran número de contribuciones de partes interesadas, hacia objetivos compartidos
- Dirigir organizaciones de una manera que sea resistente a la censura
- Seguimiento y validación de la participación y contribución a un proyecto
-
- Gestionar una variedad de diferentes niveles de contribución
- Permitir que las personas y entidades contribuyan con el trabajo de una manera independiente sin vinculación con la jurisdicción a la que pertenezcan e independientemente de las reglas de la ubicación física desde la que contribuyan
- Configuración ágil, especialmente en relación con las estructuras organizativas tradicionales

El incidente DAO y sus consecuencias

En su libro Blockchain Revolution, Don Tapscott compara a la industria financiera en su estado actual con la máquina de Rube Goldberg. Una máquina extremadamente compleja, para hacer una función completamente sencilla.[15]

[14] Dhillon, V., Metcalf, D., & Hooper, M. (2017). *Blockchain enabled applications: understand the blockchain ecosystem and how to make it work for you*. Apress.

[15] Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin.

Según plantea Tapscott, el sistema de criptomonedas sustentadas en la Blockchain ha venido a sustituir ese sistema extremadamente complejo, por una red accesible a todo el mundo que puede realizar transferencias en pocos segundos, en forma eficiente y sin tener que incurrir en los elevados costos y comisiones de los sistemas de pagos internacionales.

Este cambio disruptivo que propone la adopción de criptomonedas inspiró a Chirstoph Jentzsch, un físico alemán, a pensar en desarrollar un sistema tanto o más revolucionario que el del Bitcoin: una organización auto-gobernada.

La idea, muy ambiciosa, por cierto, fue generar una organización montada sobre la Blockchain, guiada por Contratos Inteligentes, que pudiese autogestionarse en las decisiones rutinarias y repetitivas, y recurriese a votaciones que realicen los propietarios de las participaciones para aquellas decisiones no rutinarias. De esta manera se eliminaría la intermediación de costosos y gerentes y directores.

De esta forma en marzo de 2016 Jentzsch publicó un White Paper del proyecto, con el nombre de DAO – Decentralized Autonomous Organization y en abril de ese año comenzó la campaña de inversores. Tal como vimos en el apartado de Tokens, el sistema contemplaba intercambiar el token específico de la DAO, por Ethers, la criptomoneda por default de la red Ethereum.

Según declaró Jentzsch su idea era recaudar un par de millones de dólares, pero para su sorpresa la DAO en mayo de 2016 ya había recaudado 150 millones de dólares.

Todo parecía hasta allí una situación de festejo, pero el éxito de la campaña con 150 millones de dólares recaudados, era una tentación muy grande para los hackers.

EL 26 de mayo 2016, antes que la DAO cerrase su periodo de recaudación de fondos, Emin Gün Sirer, un científico de computadoras experto en Blockchain de Cornell University, publicó un artículo sugiriendo que la DAO cesara su actividad ya que había detectado 9 errores graves en el código de su Contrato Inteligente.

En Junio 17, a las 3 semanas que la DAO había comenzado a funcionamiento operativo, un hacker disparó un ataque valiéndose de una vulnerabilidad que tenía el programa del Contrato Inteligente de la DAO.

El código de la DAO contemplaba la posibilidad de un participante pudiese retirarse de DAO, recibiendo un reembolso de su inversión en Ethers. La cláusula había sido pensada para evitar que inversionistas con participación mayoritaria, pudiesen tomar decisiones en detrimento de los inversionistas con participación minoritaria. De esta forma, estos últimos (los inversionistas con participación minoritaria) contaban con la posibilidad de retirarse de la organización si estaban en desacuerdo con las decisiones que imponían los que detentaban la mayoría en votaciones.

El problema del que se valió el hacker, fue un error de programación donde el código del contrato inteligente tenía una demora en descontar el retiro que hacia el inversor de su cuenta. De esta manera el hacker, podía invocar al contrato un nuevo retiro antes de que el contrato actualizara su saldo. Se valió del bug para crear otro contrato que fuese goteando la cuenta y drenando unos 4.000 USD cada 3 minutos.

Por increíble que parezca, Jentzsch explicó con el tiempo, que el error fue tan simple como haber consignado en una variable una letra T (con mayúscula), en lugar de una t (con minúscula).

Para cuando se decidieron tomar medidas contra el desfalco que se había producido, el hacker ya había extraído 4 millones de Ethers, que al valor de ese momento llegaban a unos 55 millones de dólares. Era un tercio de los fondos que la DAO había recaudado. Pero el impacto del hackeo era más significativo. Implicaba la caída del proyecto DAO, que en ese momento contenía el 16% de los Ethers totales emitidos. No peligraba la seguridad del proyecto DAO, sino que ponía sobre la cuerda floja de la falta de credibilidad a la red Ethereum misma.

Toda la comunidad de Ethereum pedía una solución, para que el hacker no pudiese salirse con su cometido.

El problema es que, como vimos, una vez enviada una o una serie de transacciones a la Blockchain, no hay manera de volverlas atrás. Quedan registradas y salvaguardadas criptográficamente de forma invulnerable.

Solo había una solución al problema. Crear un hard-fork, es decir una bifurcación de la red.

La idea que se propuso, y el mismo Vitalik Buterin se encargó en consultar en la comunidad Ethereum, fue la de volver al momento anterior del despliegue del contrato inteligente que

soportaba la DAO, y volver a minerar todas las transacciones siguientes, eliminando selectivamente todas aquellas vinculadas a la DAO. Todo esto sobre una nueva bifurcación de la Blockchain. La consulta se realizo sobre los tenedores de Ethers con el criterio de 1 Ether = 1 voto. De modo de salvaguardar los derechos de los usuarios que mayor tenencia de Ethers ostentaran. El resultado fue aplastante: 87% a favor de resetear la red creando una nueva bifurcación, contra 13% que votaron por la negativa.

De esta forma el 20 de julio de 2016 se produjo la bifurcación de la Bockchain de Ethereum, manteniendo el nombre de Ethereum la red principal sobre la que se hicieron los cambios para poder devolver los Ethers a los inversores de la DAO, y Ethereum Classic, para quienes siguieron actuaron sobre la red original donde se había desplegado la DAO.

La pregunta que podemos hacer es, ¿qué propósito pueden llevar los usuarios que se quedaron en Ethereum Classic, cuando conocen que en esa bifurcación se benefició al hacker que realizó la maniobra de vaciar fondos de la DAO?

El tema pasa por una discusión fuerte que existe en la comunidad de Blockchain sobre quienes piensan que la falta de credibilidad que conlleva aceptar la generación de una bifurcación de la red, es un costo más alto que aceptar el daño provocado por el hackeo.

Un artículo que tuvo, y tiene aún hoy, mucho peso sobre esta postura es el de Bruce Fenton, miembro de la Fundación Bitcoin:

“Es mejor perder su inversión que perder su blockchain”. El título solo, define claramente su postura. En ese artículo Fenton dice: "la fuerza de la tecnología Blockchain está en que la misma es un registro, una declaración de verdad. Ese registro es tan bueno como su resistencia a la censura, el cambio, las demandas o los ataques”.[16]

Consideraciones

El incidente DAO marcó uno de los momentos más críticos en la comunidad de desarrolladores y entusiastas de la tecnología Blockchain.

Hasta el día de hoy la controversia de la solución que se buscó para poder salvar la red Ethereum de un posible quiebre por falta de confianza, sigue creando polémica y ruido entre:

- quienes sostienen que la solución que se buscó erosiona el pilar fundamental de la Blockchain, que es la confianza en su inmutabilidad, y

- quienes valoran la solución adoptada como una forma de sobrellevar un daño irreparable que el hackeo al contrato inteligente de la DAO hubiese provocado

[16] It’s Better to Lose Your Investment than Lose Your Blockchain - https://medium.com/@brucefenton/its-better-to-lose-your-investment-than-lose-your-blockchain-2907a59d5a40
Observado: noviembre 2022

De todas maneras, sea cual fuese la postura que se adopte, el incidente DAO creó una sombra de sospecha sobre la confianza que se puede depositar en un desarrollo de este tipo de Contratos Inteligentes.

Actualmente existen iniciativas tendientes a retomar la idea que originalmente Jentzsch planteó, y que no deja de ser innovadora. Se han desarrollado proyectos que ofrecen plantillas pre-programadas y debidamente probadas para poder desarrollar DAOs como soluciones organizacionales, especialmente para procesos de crowdfunding. Vamos a ver una de ellas, dentro de las más destacadas.

Proyecto ARAGON

Proyecto Aragon es una iniciativa generada por Luis Cuende y Jorge Izquierdo en 2017. A mayo de 2020 contaba con 1.500 organizaciones creadas por medio de sus contratos inteligentes, unos 28.000 usuarios vinculados a estas, y el capital total de esas organizaciones generadas asciende a unos 10.000 millones de dólares.

No se conocen al momento, ataques de hackers que hayan podido vulnerar la integridad de sus desarrollos.

Aragon ofrece una variedad de Contratos Inteligentes pre-programados que pueden utilizarse como plantillas para desarrollar funciones básicas de una DAO:

1. Asignación de tokens
2. Sistemas de votación
3. Finanzas
4. Pagos

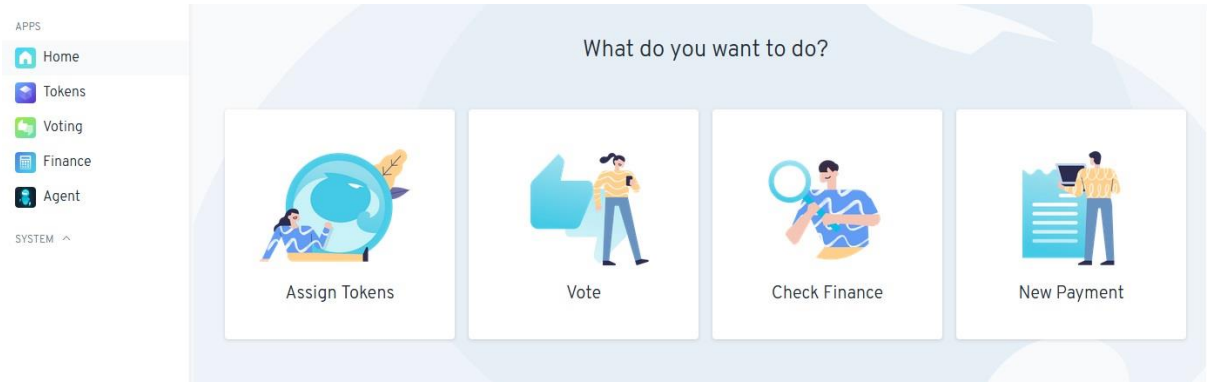


Figura 21 Aragon Court

El servicio más destacado, pero también más polémico que la comunidad de Aragon viene desarrollando es el que se denomina “Aragon Court”.

La idea de este servicio que provisto por la plataforma Aragon, es que al momento de desarrollarse una nueva DAO, los iniciadores tengan la opción de configurar la misma de

modo que sus futuros miembros e inversores queden sometidos a la resolución de disputas por medio del sistema de Aragon Court.

El Aragon Court consta con jueces, que son usuarios del sistema los cuales pueden postularse para esta tarea transfiriendo a contrato inteligente que gobierna el Argaon Court, una cantidad determinada de tokens, los que quedarán en custodia de la corte.

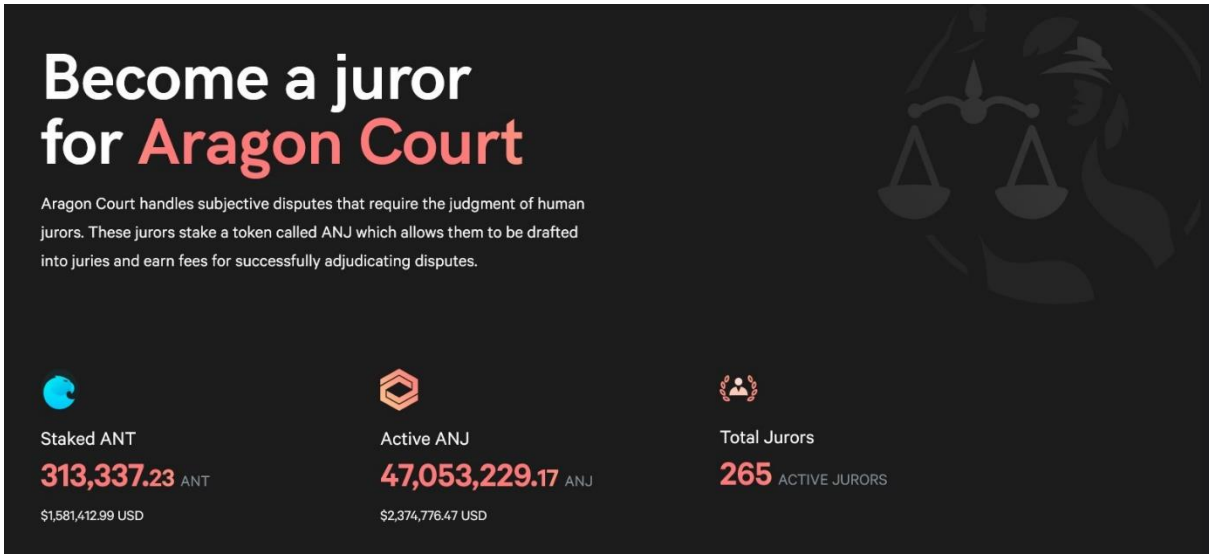


Figura 22 Jueces en el Aragon Court,

Cada vez que los miembros de una nueva DAO, la cual haya decidido someterse a este sistema de resolución de conflictos, presenten una disputa, el contrato inteligente de Aragon Court designará 3 jueces de los inscriptos, en forma aleatoria para resuelvan la disputa amigablemente.

Los litigantes presentaran a la corte sus argumentos de defensa y los jueces realizan un primer veredicto, el cual quedará a consideración de los litigantes de ser aceptado o no. Destaquemos que todo este servicio está basado en Contratos Inteligentes, desplegados sobre la Blockchain de Ethereum, por lo cual, todos estos pasos y las votaciones están automatizados y registrados en la Blockchain.

Si los litigantes no aceptan la resolución de los tres jueces, se podrá pasar a una segunda instancia, donde el caso será presentado a todos los jueces inscriptos en la corte del proyecto Aragon, decidiéndose por simple mayoría de votos de estos. Esta decisión será inapelable y se instrumentará automáticamente, también por un contrato inteligente de votación.

Por último, tanto en la primera, como en la segunda instancia, los jueces intervinientes serán recompensados en su labor por medio de tokens que la DAO les transferirá.

Por supuesto, que así como un desarrollo innovador y dinámico, este tipo de servicio desplegado como Contrato Inteligente, abre también una fuerte polémica en la disputa que se puede presentar entre jurisdicciones de las DAOs que se constituyan, leyes aplicables y en situaciones donde estas disputas virtuales se lleven a tribunales regulares (mundo real).

Sin duda una controversia apasionante con la que vamos a lidiar en los próximos años.

Conclusiones – rumbos

Hemos realizado un recorrido sobre la tecnología de Blockchain o Cadena de Bloques, describiendo los factores fundamentales que sustentan la misma.

De esta manera hemos podido arribar, explicando sus funcionalidades, las características distintivas de la tecnología.

Su invulnerabilidad, por medio de uso intensivo de criptografía y métodos de consensos. Hemos descripto como impacta en este factor la denominada POW -Prueba de Trabajo que los mineros de la Blockchain deben observar para desarrollar su función.

El registro ordenado y redundante de transacciones, las cuales son replicadas en miles de servidores, garantizando la disponibilidad de la información integral de la red en todo momento.

Todo esto para garantizar la propiedad de los activos financieros que se representan en la Blockchain. Dando accesibilidad a la propiedad de esos criptoactivos por medio de billeteras digitales criptográficas.

Vimos que esta tecnología, pensada originalmente para ser autogobernada sin una autoridad monetaria centralizada, se está mudando en muchos casos a Blockchains permisionadas, con nodos administradores (con permisos) y nodos selladores. Mencionamos y analizamos en este aspecto a Blockchains no permisionadas (públicas), permisionadas (privadas), de consorcio e híbridas.

Explicamos la dinámica de Contratos Inteligentes, especialmente en su desarrollo sobre la infraestructura de la Blockchain Ethereum. La tecnología de Smart Contracts, o Contratos Inteligentes, es clave para poder entender el desarrollo y la evolución que va tomando el ecosistema de la Blockchain.

Por último, nos adentramos en el objetivo principal de este informe, que es la evaluación de los desarrollos que se han estado haciendo sobre la tecnología de Cadena de Bloques y configuran lo que globalmente llamamos el ecosistema de la Blockchain. Nuestro foco en este aspecto se ha centrado en los desarrollos y aplicaciones que se desenvuelven para el financiamiento empresarial por medio de esta tecnología.

La comprensión y conceptualización de la infraestructura que brinda la Blockchain para el desarrollo de este tipo de aplicaciones y artefactos es fundamental para poder adentrarnos en evaluar la conveniencia, riesgos, alcance y futuras implementaciones de una plataforma Blockchain de la provincia de Santa Fe, no solo para desenvolvimientos propios del gobierno, como abierta y supervisada para desarrollos de organizaciones, empresas y particulares.

Marco normativo

Introducción

En función del objetivo “evaluar críticamente el impacto, oportunidades y riesgos que conllevan los nuevos medios digitales de financiación, basados en el ecosistema de la tecnología Blockchain.”, que nos planteamos en la implementación de la propuesta de evaluar los “BENEFICIOS DE DESARROLLO DE UNA PLATAFORMA NFT/FT (TOKENS FUNGIBLES Y NO FUNGIBLES) PARA SANTA FE”, vamos a desarrollar en esta tarea una descripción y análisis del marco jurídico de criptoactivos.

Nuestro enfoque comenzará desde la base de las definiciones que da la Constitución Nacional, para la emisión y gestión de dinero circulante en el país. Las normas de la carta orgánica del Banco Central de la República Argentina (BCRA), como así también las circulares de este organismo. Algunas vinculaciones con el Código Civil y Comercial, y luego analizaremos en particular, el marco impositivo de monedas digitales, a nivel nacional.

Vamos a relevar las normativas provinciales, en lo referente a Impuestos a los Ingresos Brutos, y en particular, vamos a hacer enfoque más detallado, de la reciente Ley provincial de San Luis, que promueve el desarrollo del uso de Blockchain como tecnología que impulse la Innovación Financiera para la Inversión y el desarrollo socio-económico.

Es de nuestro entender, que la iniciativa de la provincia de San Luis, es un antecedente fundamental a tener en cuenta con el objeto de nuestra propuesta de evaluación de beneficios del desarrollo de la plataforma referente para Santa Fe.

Por último, y para enmarcar el marco normativo con los adelantos que se hacen a nivel internacional, vamos a poner foco en la propuesta de Reglamento del Parlamento Europeo sobre Criptoactivos. La razón de poner foco en esta propuesta, es que consideramos que a nivel internacional es una de las normativas más avanzada, estructurada e abarcativa de todo el ecosistema de la tecnología de Blockchain.

Constitución Nacional

Siguiendo un orden lógico de prelación, iniciaremos el enfoque del marco normativo vigente en Argentina en que podemos situar a los cripto-activos, analizando lo establecido en la Constitución de Nación Argentina.

German Bidart Campos (2000) realiza una diferenciación entre lo que denomina la Constitución material, vigente y eficaz, y la Constitución formal, escrita y codificada. Consideramos que esta diferenciación escapa al foco del análisis normativo que queremos realizar en este trabajo.

Sin embargo, tomaremos como guía la caracterización que el autor propone para definir la Constitución formal (codificada), en especial para destacar la supremacía y prelación de la Constitución Argentina, sobre el resto de leyes y normativas que analizaremos.

Bidart Campos G. (2000), establece las características elementales de la Constitución formal o codificada como:

"Si la pensamos en su tipo clásico de constitución escrita o codificada, podemos describirla conforme a las siguientes características:

a) *La Constitución es una Ley.*
b) *Por ser ley suprema, se considera como super ley.*
c) *Esa ley es escrita.*
d) *La formulación escrita está codificada, cerrada,o reunida en un texto único y sistematizado.*
e) *Por su origen, se diferencia de las leyes ordinarias o comunes en cuanto es producto de un poder constituyente que, también formalmente, aparece elaborándola."*[17]

Habiendo destacado la jerarquía normativa de la Constitución, podemos analizar que establece en referencia a la moneda, su valor, emisión y demás aspectos relevantes. Luego analizaremos si por su naturaleza las criptomonedas y demás cripto-activos que se definen en el ecosistema de Blockchain, pueden ser consideradas o equiparadas a la definición de moneda que surge de la Constitución Nacional y leyes vinculadas.

En el Capítulo 4 de la CNA - Atribuciones del Congreso, artículo 75, inciso 11), encontramos como potestad de este órgano, el de hacer sellar moneda y fijar su valor

"*Artículo 75:*

….

11) Hacer sellar moneda, fijar su valor y el de las extranjeras; y adoptar un sistema uniforme de pesos y medidas para toda la Nación".[18]

La primera consideración que se puede realizar es vinculada a la extemporaneidad de la norma en el sentido de hablar de "hacer sellar moneda". En la actualidad la mayoría (por no considerar la totalidad) de la acuñación de moneda física se hace en billetes, habiendo quedado por causa del proceso inflacionario que vivimos, prácticamente en desuso el uso de la moneda metálica.

---

[17] BIDART CAMPOS, G. (2000). Manual de la Constitución Reformada, Tomo I, Ediar. Buenos Aires. Capítulo I - LA ESTRUCTURA, EL CONTENIDO Y LAS FUENTES DEL DERECHO CONSTITUCIONAL punto 15

[18] CONSTITUCION DE LA NACION ARGENTINA. sancionada en 1853 con las reformas de los años 1860, 1866, 1898, 1957 y 1994. Texto ordenado según Ley Nº 24.430. Sancionada: Diciembre 15 de 1994. Promulgada: Enero 3 de 1995.
Cita: Capítulo 4 - Atribuciones del Congreso - artículo 75, inc 11

Aún en años anteriores, se ha observado una prevalencia de la moneda-billetes sobre la moneda-metal. Esta salvedad toma dimensión al considerar la diferencia de usos y costumbres, entre el texto original de la CNA realizado en 1853, con la época actual.

Otra consideración en referencia a la extemporaneidad del artículo que estamos analizando tiene que ver con la mención que se realiza como una atribución del Congreso, de "fijar su valor y el de las extranjeras".

Antes de 1881, cuando en la presidencia de Julio A. Roca se sancionó la Ley 1130 de unificación de moneda nacional, existían en circulación y se reconocían como de curso legal, monedas extranjeras. Al entrar en vigencia la ley mencionada se unificó una única moneda nacional de curso legal. En ese sentido se hace mención en la CNA, según su texto original de 1853, a la potestad de fijar el valor de monedas extranjeras. No debe interpretarse como facultad del Congreso el fijar el tipo de cambio, ya que esa atribución establecida por la CNA refería al momento en que se reconocía a determinadas monedas extranjeras como de curso legal[19].

El artículo 75 de la Constitución de la Nación Argentina, en mención a las atribuciones del Congreso Nacional, determina en su inciso 11 la facultad de:

"6. Establecer y reglamentar un banco federal con facultad de emitir moneda, así como otros bancos nacionales"[20].

La Constitución por medio de este inciso faculta al Congreso a delegar el poder de emisión de moneda en un banco federal, lo cual, como veremos más adelante se plasmó en el Banco Central de la República Argentina, cuya Carta Orgánica ratifica ese poder delegado.

Además de la facultad de delegar la emisión de moneda en un banco federal (BCRA), el mismo artículo 75 en el inciso 19 establece como atribución del Congreso, proveer lo conducente a la defensa del valor de la moneda:

"19. Proveer lo conducente al desarrollo humano, al progreso económico con justicia social, a la productividad de la economía nacional, a la generación de empleo, a la formación profesional de los trabajadores, ***a la defensa del valor de la moneda****, a la investigación y al desarrollo científico y tecnológico, su difusión y aprovechamiento."[21]*

Este inciso agregado en la reforma constitucional de 1994 refuerza la atribución del Congreso de constituir un banco federal y su conducente emisión de dinero, que mencionamos anteriormente. En este caso, y en sintonía con atribuciones del Congreso orientadas a sustentar políticas de progreso económico y desarrollo humano, promueve la defensa del

[19] BIDART CAMPOS, G. (2000). Manual de la Constitución Reformada, Tomo III, Ediar. Buenos Aires. Capítulo XXIV - LA COMPETENCIA DEL CONGRESO EN EL ARTICULO 75 punto 25

[20] Idem cita anterior. Cita: Capítulo 4 - Atribuciones del Congreso - artículo 75, inc 6

[21] Idem cita anterior. Cita: Capítulo 4 - Atribuciones del Congreso - artículo 75, inc 19 (resaltado por el autor)

valor de la moneda, que como también veremos más adelante, conforma una de las atribuciones delegadas al Banco Central de la República Argentina.[22]

También en referencia a la emisión de moneda, la CNA prohíbe taxativamente el uso de esta atribución por parte de las provincias, en tanto, no pueden hacer uso de esa atribución delegada al gobierno nacional:

"Artículo 126.- Las provincias no ejercen el poder delegado a la Nación. No pueden celebrar tratados parciales de carácter político; ni expedir leyes sobre comercio, o navegación interior o exterior; ni establecer aduanas provinciales; ***ni acuñar moneda****; ni establecer bancos con facultad de emitir billetes, sin autorización del Congreso Federal; ni dictar los Códigos Civil, Comercial, Penal y de Minería, después que el Congreso los haya sancionado; ni dictar especialmente leyes sobre ciudadanía y naturalización, bancarrotas, falsificación de moneda o documentos del Estado; ni establecer derechos de tonelaje; ni armar buques de guerra o levantar ejércitos, salvo el caso de invasión exterior o de un peligro tan inminente que no admita dilación dando luego cuenta al Gobierno federal; ni nombrar o recibir agentes extranjeros".*[23]

Es de destacar que esta prohibición de la CNA tiene una especial relevancia para el trabajo que estamos abordando, en cuanto se refiere a una atribución que las provincias (en nuestro caso la provincia de Santa Fe) han delegado a la Nación, y por lo tanto tienen vedado de poder utilizar. Es una prohibición directa de acuñar moneda. Quedará, como veremos más adelante, determinar si se debe considerar a las criptomonedas, y a los instrumentos derivados del ecosistema Blockchain, como monedas.

BCRA - Banco Central de la República Argentina

Carta Orgánica BCRA - Ley 24.144 / 26.739

Como vimos en los apartados anteriores, el artículo 75, inciso 6 de la CNA permite al Congreso Nacional establecer y reglamentar un banco federal en el cual delegar la emisión de moneda y las medidas conducentes a mantener su valor.

Esta facultad se vé plasmada en la Ley 24.144 - Carta Orgánica del Banco Central de la República Argentina, modificada por la Ley 26.739 de 2012 la cual establece al Banco Central como única autoridad monetaria del país, y como entidad autárquica en referencia al gobierno nacional.

Entre algunas de las funciones delegadas al BCRA podemos mencionar:

1) Promover la estabilidad monetaria y estabilidad financiera

[22] Badeni, G. (2006). Tratado de derecho constitucional. Tomo II. La ley. Capitulo XIII La actividad del Congreso. Punto 528 Moneda y Régimen Bancario

[23] Idem cita anterior. Cita: Título Segundo - Gobiernos de Provincia - artículo 126 (resaltado por el autor)

“ARTICULO 3º — El banco tiene por finalidad promover, en la medida de sus facultades y en el marco de las políticas establecidas por el gobierno nacional, ***la estabilidad monetaria, la estabilidad financiera,*** *el empleo y el desarrollo económico con equidad social.”*[24]

2) Regular la cantidad de dinero circulante

“ARTICULO 4º — Son funciones y facultades del banco:

…

b) ***Regular la cantidad de dinero*** *y las tasas de interés y regular y orientar el crédito;”*[25]

3) Gestionar las reservas que actúan como respaldo del circulante

“ARTICULO 4º — Son funciones y facultades del banco:

…

d) Concentrar y ***administrar sus reservas de oro, divisas y otros activos externos****;”*[26]

4) Regular los sistemas de pago

“ARTICULO 4º — Son funciones y facultades del banco:

…

g) ***Regular, en la medida de sus facultades, los sistemas de pago****, las cámaras liquidadoras y compensadoras, las remesadoras de fondos y las empresas transportadoras de caudales, así como toda otra actividad que guarde relación con la actividad financiera y cambiaria;”*

Podemos destacar, al analizar las atribuciones que mencionamos, que la Carta Orgánica (en especial después de la reforma de Ley 26.739/12), establece para el Banco Central el mandato de alinear sus funciones con políticas de estabilidad monetaria, conducentes al desarrollo económico. En especial considerando la última parte del inciso b) del artículo 4, recién mencionado donde se menciona como una función de la entidad “orientar el crédito”.

[24] Ley 24.144/92 - Carta Orgánica del Banco Central de la República Argentina, con modificatoria de Ley 26.739/12. Artículo 3 (destacado del autor)
[25] Idem cita anterior. Artículo 4 inciso b). (destacado del autor)
[26] Idem cira anterior. Artículo 4 inciso d). (destacado del autor)

Sin perjuicio de todas estas consideraciones relativas a funciones y facultades vinculadas a política monetaria, pondremos foco en esta parte del trabajo, a los aspectos más directamente vinculados a la emisión y gestión de moneda, que se mencionan en la Carta Orgánica de BCRA.

Veamos las definiciones que da la Carta Orgánica en relación a las atribuciones del directorio del BCRA.

Dentro de las atribuciones que podemos mencionar relativas a la emisión y gestión de dinero, podemos mencionar:

1) Intervención sobre el mercado monetario

"ARTICULO 14. — Corresponde al directorio:

a) Intervenir en las decisiones que afecten al mercado monetario y cambiario;"[27]

2) Ejercer facultades poderes asignados al BCRA

"ARTICULO 14. — Corresponde al directorio:

…

i) Ejercer las facultades poderes que asigna al banco esta ley y sus normas concordantes;"[28]

3) Establecer las denominaciones y características de billetes y monedas

"ARTICULO 14. — Corresponde al directorio:

…

k) Establecer las denominaciones y características de los billetes y monedas;"[29]

4) Desmonetización de billetes y monedas en circulación

"ARTICULO 14. — Corresponde al directorio:

…

l) Disponer la desmonetización de los billetes y monedas en circulación y fijar los plazos en que se producirá su canje;"[30]

5) Extender la aplicación de la ley de Entidades Financieras

"ARTICULO 14. — Corresponde al directorio:

---

[27] Ley 24.144/92 - Carta Orgánica del Banco Central de la República Argentina, con modificatoria de Ley 26.739/12. Artículo 14 inciso a)
[28] Idem cita anterior - Artículo 14 inciso i)
[29] Idem cita anterior - Artículo 14 inciso k)
[30] Idem cita anterior - Artículo 14 inciso l)

…

v) Declarar la extensión de la aplicación de la Ley de Entidades Financieras a personas no comprendidas en ella cuando así lo aconsejen el volumen de sus operaciones o razones de política monetaria, cambiaria o crediticia;"[31]

Tal vez el punto más determinante en lo referente a las facultades delegadas por el Congreso al BCRA, para poder emitir y gestionar el circulante de moneda, está plasmado en el artículo 30 y 31 de la Carta Orgánica del mismo, según Ley 24.144 y modificatorias.

"Artículo 30: El banco es el encargado exclusivo de la emisión de billetes y monedas de la Nación Argentina y ningún otro órgano del gobierno nacional, ni los gobiernos provinciales, ni las municipalidades, banco u otras instituciones cualesquiera, podrán emitir billetes ni monedas metálicas ni otros instrumentos que fuesen susceptibles de circular como moneda.Se entenderá que son susceptibles de circular como moneda, cualesquiera fueran las condiciones y características de los instrumentos, cuando:

i) El emisor imponga o induzca en forma directa o indirecta, su aceptación forzosa para la cancelación de cualquier tipo de obligación; o

ii) Se emitan por valores nominales inferiores o iguales a 10 veces el valor del billete de moneda nacional de máxima nominación que se encuentre en circulación."[32]

El artículo 30 refuerza con claridad la competencia exclusiva del BCRA, en base a facultad del Congreso delegada, para la emisión de billetes y monedas, y la expresa prohibición a los gobiernos subnacionales de realizar esto.

El punto clave que entendemos debe tomar relevancia para nuestro análisis a esta altura, es el del alcance reglado por el artículo citado en su última parte. Nos referimos a la mención que realiza acerca de "otros instrumentos que fuesen susceptibles de circular como moneda".

El mismo artículo se encarga de establecer las condiciones en base a las cuales se deberá considerar que los instrumentos son susceptibles de circular como moneda.

La primera es la situación en la cual el emisor imponga en forma directa o indirecta, su aceptación forzosa para la cancelación de cualquier tipo de obligación.

Será clave, para este entendimiento analizar si las criptomonedas, u otros elementos desarrollados bajo la tecnología de Blockchain (tokens), deben ser incluidas en este apartado. En ese contexto, el Código Civil y Comercial viene a reforzar la idea expuesta por la Carta Orgánica del Banco Central:

"*ARTÍCULO 765.- Concepto. La obligación es de dar dinero si el deudor debe cierta cantidad de moneda, determinada o determinable, al momento de constitución de la obligación. Si por el acto por el que se ha constituido la obligación, se estipuló dar moneda que no sea de curso*

[31] Idem cita anterior - Artículo 14 inciso v)
[32] Idem cita anterior - Artículo 30

legal en la República, la obligación debe considerarse como de dar cantidades de cosas y el deudor puede liberarse dando el equivalente en moneda de curso legal."[33]

El código establece con claridad que se considerará obligaciones de dar dinero, a las que se pacten en moneda nacional. A aquellas que corresponden a obligaciones pactadas en moneda que no sea de curso legal en la República Argentina, se las debe considerar como de dar cantidades de cosas.

Y en referencia a la obligatoriedad de su aceptación, podemos ver a que se considera "moneda de curso de legal". Bidart Campos (2006) la define como:

"La moneda de curso legal es aquella moneda —metálica o papel— cuya aceptación es irrehusable y obligatoria, y apareja poder cancelatorio o liberatorio; la moneda de curso forzoso es el papel moneda con curso legal, que además no puede canjearse.

El curso legal, que hace al dinero irrecusable, atiende a la relación "acreedor-deudor", porque el primero no puede rehusar recibir la moneda de curso legal; el curso forzoso apunta a la relación "tenedor del billete- entidad emisora", porque el primero no puede exigir al segundo la conversión del billete. El billete investido de curso legal y curso forzoso suele llamarse "papel moneda"."[34]

En este punto de entendimiento, al no reconocerse en Argentina la aceptación irrehusable y obligatoria, y el poder cancelatorio o liberatorio derivado, no se debería considerar a las criptomonedas como monedas de curso legal. Por lo tanto, los derechos y obligaciones vinculados a las mismas, se deben considerar (según lo establece el CCN) como obligaciones de dar cantidades de cosas.

Un párrafo aparte merece la segunda condición que menciona el artículo 30 de la Carta Orgánica del BCRA, para que se considere la susceptibilidad de circular como moneda:

ii) Se emitan por valores nominales inferiores o iguales a 10 veces el valor del billete de moneda nacional de máxima nominación que se encuentre en circulación.

Un concepto innovador de las criptomonedas, como así también de todos instrumentos generados en el ecosistema de Blockchain, gira en torno a romper con el paradigma de la moneda en papel billete, y consiguientemente su "valor nominal".

Uno de los problemas que se enfrentó al desarrollar la Blockchain de Bitcoin, la primera de todas, fue el de cómo gestionar la cantidad de decimales de la criptomoneda que se intercambiará, como también el redondeo de las cantidades.

La solución que se buscó fue la de fraccionar el Bitcoin en partes atómicas de un valor tan chico que permitiese depreciar el problema de las fracciones en valores transados. De esta manera, cada vez que se realiza una transacción con Bitcoin, en nuestras billeteras digitales veremos la cantidad de Bitcoin y sus valores decimales. En realidad, en la transacción que se envía a la Cadena de Bloques, estará expresada en "Satoshis", que es la mínima unidad

[33] Ley 26.994 - Código Civil y Comercial de la Nación - BO: 08/10/2014 - Capítulo 3 - Clases de Obligaciones - Sección 1a Obligaciones de dar - Artículo 765

[34] Bidart Campos, G. J. (2006). *Manual de la constitución reformada. v. 3*. Ediar.

de medida del Bitcoin. Un Satoshi equivale a 1 / 100.000.000 de Bitcoin. Esta unidad tan atómica, le permite al sistema soslayar cualquier problema de decimales y redondeos.

En base a esta consideración, que deriva de una cuestión tecnológica del desarrollo del protocolo de Bitcoin, se entiende poco razonable la aplicación de la regla establecida en el segundo ápice del artículo 30.

Sin embargo, el problema de aplicabilidad de la norma no termina allí. Supongamos que tomemos como base para determinar el valor nominal de emisión de la criptomoneda, la generación de nuevas criptomonedas, que la Cadena de Bloques, asigna como premio a los mineros. Actualmente 6,25 Bitcoins por cada nuevo Bloque incorporado a la Cadena de Bloques.

De esta forma podríamos caer en la tentación de vincular esos nuevos 6,25 Bitcoins generados por la Blockchain con un nuevo "billete" emitido por la red. Sin embargo, a la primera transacción en que los mismos se transfieran, por ejemplo, dividiéndolos en dos partes de valores arbitrarios, la Blockchain, los marcaría como "usados" y generaría dos nuevos registros de Bitcoins vinculados a cuentas, por el valor en que se separaron. Esta dinámica se efectúa en todas las transacciones que se realizan en la Blockchain, y tal como mencionamos anteriormente, responde a un nuevo paradigma de dinero digital, que no utiliza ni tiene un "valor nominal de emisión", como los billetes del paradigma de dinero papel moneda.

Disposiciones de BCRA sobre Criptomonedas

Si bien, como analizamos previamente, el Banco Central actúa como única autoridad monetaria del país, y por lo tanto tiene a su alcance la regulación de política y cuestiones monetarias, no podríamos encuadrar a las criptomonedas en la categoría de monedas, en cuanto no son emitidas por un gobierno o autoridad, no tienen un valor nominal, y no tienen curso forzoso. Hecho por el cual no estarían bajo la potestad de regulación por parte del BCRA.

Las primeras que podemos destacar, son vinculadas a las restricciones cambiarias. El 01 de setiembre de 2019, el Poder Ejecutivo de la Nación emite el Decreto de Necesidad y Urgencia 609 / 2019, por el cual establece:

"ARTÍCULO 1°.- Establécese que, hasta el 31 de diciembre de 2019, el contravalor de la exportación de bienes y servicios deberá ingresarse al país en divisas y/o negociarse en el mercado de cambios en las condiciones y plazos que establezca el BANCO CENTRAL DE LA REPÚBLICA ARGENTINA.

ARTÍCULO 2º.- El BANCO CENTRAL DE LA REPÚBLICA ARGENTINA, conforme lo previsto en su Carta Orgánica, establecerá los supuestos en los que el acceso al mercado de cambios para la compra de moneda extranjera y metales preciosos amonedados y las transferencias al exterior requerirán autorización previa, con base en pautas objetivas en función de las condiciones vigentes en el mercado cambiario y distinguiendo la situación de las personas humanas de la de las personas jurídicas.

ARTÍCULO 3°.- Facúltese al BANCO CENTRAL DE LA REPÚBLICA ARGENTINA para establecer reglamentaciones que eviten prácticas y operaciones tendientes a eludir, a través de títulos públicos u otros instrumentos, lo dispuesto en esta medida."[35]

En virtud de este DNU, el BCRA emite, el mismo día (01/09/2019) la Comunicación "A" 6770, estableciendo restricciones de acceso al mercado de cambio transitoriamente hasta el 31 de diciembre de 2019[36].

En mismo sentido, el 28 de octubre de 2019, emite la Comunicación "A" 6815[37] endureciendo las restricciones que se habían impuesto por la Comunicación anterior. Y siguiendo ese hilo, el 31 de octubre 2019, se emite la Comunicación "A" 6823, donde por primera vez el BCRA regula el acceso a la compra de "criptoactivos", por medio de compras realizadas con Tarjetas de Débito o Crédito emitidas por instituciones locales:

"Las entidades financieras y otras emisoras de tarjetas locales deberán contar con la conformidad previa del Banco Central para acceder al mercado de cambios para realizar pagos al exterior por el uso de tarjetas de crédito, débito o prepagas emitidas en el país a partir del 01.11.19 inclusive, cuando tales pagos se originen, en forma directa o indirecta a través del uso de redes de pagos internacionales, en las siguientes operaciones:

a) la participación en juegos de azar y apuestas de distinto tipo y/o,

b) la transferencia de fondos a cuentas en Proveedores de Servicios de Pago y/o,

c) la transferencia de fondos a cuentas de inversión en administradores de inversiones

radicados el exterior y/o,

d) la realización de operaciones cambiarias en el exterior y/o,

e) ***la adquisición de criptoactivos en sus distintas modalidades****."*[38]

Dos reflexiones que podemos hacer sobre esta comunicación, es que primero el BCRA no está prohibiendo la compra de criptoactivos (según suponemos usa el término en sentido amplio para abarcar criptomonedas, más todos otros instrumentos generados en el ecosistema de Blockchain). La comunicación establece que el BCRA deberá dar conformidad para que los sistemas de tarjetas de crédito / débito puedan realizar estas operaciones, que se vinculen a redes de pagos internacionales.

La segunda reflexión es que lo que el BCRA está buscando es restringir la salida de moneda extranjera, que se presentaría cuando una persona compre en pesos argentinos, con tarjetas de crédito o débito, criptoactivos, que deban ser pagados por sistemas de pagos al exterior.

---

[35] Decreto 609/2019 - DNU-2019-609-APN-PTE - MERCADO CAMBIARIO - DEUDA PÚBLICA B.O.: 01/09/2019 - Artículos 1 a 3

[36] BCRA - Comunicación "A" 6770 - Circular CAMEX 1 - 805 - Exterior y cambios. Adecuaciones Fecha 01/09/2019

[37] BCRA - Comunicación "A" 6815 - Circular CAMEX 1 - 818 - Exterior y cambios. Adecuaciones Fecha 28/10/2019

[38] BCRA - Comunicación "A" 6823 - Circular CAMEX 1 - 820 - Exterior y cambios. Adecuaciones Fecha 31/10/2019

Se debe considerar la maniobra que esa persona podría hacer, comprando localmente los criptoactivos en pesos argentinos, y liquidarlos en el exterior en moneda extranjera. Lo que se ha dado en llamar actualmente el “dolar cripto”.

La Comunicación “A” 7422 de BCRA, de fecha 16/12/2021, también menciona a los criptoactivos dentro de los activos externos líquidos que deberán declarar ante el BCRA los clientes para los egresos por el mercado de cambios:

“3.16.2. Declaración jurada del cliente respecto a sus tenencias de activos externos líquidos.

La entidad deberá contar con la conformidad previa del BCRA excepto que cuente al momento de acceso al mercado de cambios con una declaración jurada del cliente en la que deje constancia de que:

3.16.2.1. …

Serán considerados activos externos líquidos, entre otros: las tenencias de billetes y monedas en moneda extranjera, disponibilidades en oro amonedado o en barras de buena entrega, depósitos a la vista en entidades financieras del exterior y otras inversiones que permitan obtener disponibilidad inmediata de moneda extranjera (por ejemplo, inversiones en títulos públicos externos con custodia en el país o en el exterior, fondos en cuentas de inversión en administradores de inversiones radicados en el exterior, ***criptoactivos****, fondos en cuentas de proveedores de servicios de pago, etc.).”*[39]

La Comunicación “A” 7506 es la que determina la intervención de regulación de criptoactivos más significativa del BCRA. El 05 de mayo de 2022, ante el anuncio realizado por Banco de Galicia y Brubank de ofrecer a sus clientes la posibilidad de comprar activos digitales, el BCRA emitió la Comunicación citada prohibiendo a las entidades financieras proveer a sus clientes de dichos servicios:

“- Disponer, en el marco de lo previsto por las normas sobre “Servicios complementarios de la actividad financiera y actividades permitidas”, que las entidades financieras no pueden realizar ni facilitar a sus clientes la realización de operaciones con activos digitales –incluidos los criptoactivos y aquellos cuyos rendimientos se determinen en función de las variaciones que ésos registren– que no se encuentren autorizados por una autoridad reguladora nacional competente ni por el Banco Central de la República Argentina.”[40]

La última Comunicación de BCRA que mencionaremos en relación a la regulación de criptoactivos es la “A” 7556 del 26 de julio de 2022. Por dicha comunicación se estableció un regimen especial y transitorio de acceso al mercado cambiario para los productores de granos que vendan soja a partir del 27/07/2022 y hasta el 31/08/2022. En referencia a criptoactivos establece una restricción de noventa días corridos a partir de la emisión de certificaciones,

[39] BCRA - Comunicación “A” 7422 - Circular CAMEX 1 - 904 - Texto ordenado de las normas de "Exterior y cambios". Actualización. Fecha 16/12/2021

[40] BCRA - Comunicación “A” 7506 - Circular RUNOR 1-1730 - Servicios complementarios de la actividad finan-ciera y actividades permitidas. Operaciones con activos digitales. Fecha 05/05/2022

para entregar fondos en moneda local para obtener como prestación activos externos, criptoactivos o títulos valores depositados en el exterior:

"b) emitir las certificaciones para que el productor y/u operador pueda concretar las compras de moneda extranjera y la acreditación de fondos en una "Cuenta especial para titulares con actividad agrícola".

Previamente a la emisión de alguna de dichas certificaciones, la entidad deberá contar con una declaración jurada del cliente en la que se compromete a que desde el momento en que requiere su emisión y por los 90 (noventa) días corridos subsiguientes:

…

vii) no entregará fondos en moneda local ni otros activos locales (excepto fondos en moneda extranjera depositados en entidades financieras locales) a cualquier persona humana o jurídica, residente o no residente, vinculada o no, para recibir como contraprestación previa o posterior, de manera directa o indirecta, por sí misma o a través de una entidad vinculada, controlada o controlante, activos externos, ***criptoactivos*** *o títulos valores depositados en el exterior."* [41]

Algunas consideraciones en referencia a la regulación de criptoactivos por el BCRA

- En el análisis previo observamos que la CNA estipula como potestad del Congreso la emisión de moneda. Esta facultad fue delegada al BCRA por medio de la Ley que establece su Carta Orgánica.
- Pudimos observar también que el BCRA, en función de ese poder delegado se constituyó como el único organismo con la potestad de emisión de moneda en el país, ratificandose la prohibición a los organismos subnacionales y otros bancos de hacer uso de esta atribución.
- Vimos de acuerdo a la definición que se menciona en la Carga Orgánica del BCRA y en la doctrina, que las criptomonedas no cumplen con los requerimientos necesarios para ser consideradas como moneda de curso legal, ya que no se impone la obligatoriedad de su aceptación como medio de pagos, y no son emitidas por un estado.
- En las Comunicaciones emitidas por el BCRA, podemos apreciar una regulación de tipo tangencial sobre los criptoactivos. Las comunicaciones que citamos están claramente orientadas a regular aspectos vinculados a mercado de cambios (evitar la fuga de divisas), prohibir el acceso a la compra de criptoactivos como servicios adicionales brindados por instituciones financieras, y otros; pero no existe una norma compilada y orgánica para regular el mercado de criptoactivos, y los exchanges que participan en el mismo.

Podríamos suponer, en base a lo que vimos, que el BCRA no ha desarrollado una regulación directa sobre criptoactivos, por entenderse que no posee potestad sobre un nuevo mercado

[41] BCRA - Comunicación "A" 7556 - Circular CAMEX 1-926, LISOL 1-986, REMON 1-1066, OPASI 2-663: Exterior y cambios. Depósitos de ahorro, cuenta sueldo y especiales. Efectivo mínimo. Posición global neta de moneda extranjera. Adecuaciones. Fecha 26/07/2022

que no utiliza el dinero en el sentido tradicional, sino que, como también mencionamos se podría considerar a los criptoactivos como obligaciones de dar cosas, y por lo tanto excederían el alcance regulatorio del BCRA.

Otra interpretación puede ser que no se ha desarrollado un cuerpo normativo específico, por ser el ecosistema de Blockchain, una tecnología disruptiva que no se ha consolidado todavía.

Independientemente de cuales sean los motivos de la ausencia de una clara regulación, podemos mencionar que se produce un vacío legal, o como algunos autores mencionan un “limbo” legal en lo que refiere a estos productos de monedas digitales.

Vamos a analizar, en ese sentido, a las leyes impositivas, normativas e interpretaciones referidas a criptoactivos que sustenta la AFIP -Administración Federal de Ingresos Públicos, en referencia a la gravabilidad de estos activos digitales. Siempre considerando la autonomía que se reconoce a las leyes y normativas impositivas.

Normativas Impositivas

En este apartado vamos a analizar la normativa impositiva argentina en referencia a criptoactivos. Vamos a revisar conceptos vinculados a impuestos nacionales como IVA, Impuesto a las Ganancias e Impuestos a los Bienes Personales. El foco de nuestro análisis no estará puesto en la técnica impositiva en sí, sino que más específicamente nuestra atención estará en la conceptualización que las leyes impositivas hacen sobre las criptomonedas y el resto de activos financieros digitales. Haremos una consideración especial, a la interpretación realizada por AFIP por el dictamen 2/2022 de este año, por el cual se define claramente la conceptualización de monedas digitales que sustenta el fisco.

IVA

El artículo 1 de la Ley de Impuesto al Valor Agregado establece con claridad el objeto del impuesto:

"ARTÍCULO 1° — Establécese en todo el territorio de la Nación un impuesto que se aplicará sobre:

a) Las ventas de cosas muebles situadas o colocadas en el territorio del país efectuadas por los sujetos indicados en los incisos a), b), d), e), y f) del artículo 4°, con las previsiones señaladas en el tercer párrafo de dicho artículo.

b) Las obras, locaciones y prestaciones de servicios, incluidas en el artículo 3°, realizadas en el territorio de la Nación. En caso de telecomunicaciones internacionales se las entenderá realizadas en el país en la medida en que su retribución sea atribuible a la empresa ubicada en él.

c) Las importaciones definitivas de cosas muebles"[42]*.*

Claramente se desprende del texto citado, que los criptoactivos, como tales, no se encuentran alcanzados por el impuesto al valor agregado por no encuadrar en ninguna de las enunciaciones del objeto del mismo.

Sin perjuicio de lo mencionado en el párrafo anterior las comisiones que cobran los Exchanges por las operaciones peer-to-peer, estarían gravadas en el IVA. En estas operaciones la plataforma del Exchange acerca compradores y vendedores de criptomonedas, cobrando una comisión por este servicio. Esta comisión encuadraría en lo establecido por el inciso b) del artículo 1 de la Ley del Impuesto al Valor Agregado al ser un servicio brindado en el país.

[42] Decreto 280/97 - texto ordenado de la Ley de Impuesto al Valor Agregado, sustituido por el artículo 1° de la Ley N° 23.349 y sus modificaciones. - BO: 15/04/1997 - Artículo 1 - Objeto

Impuesto sobre los Bienes Personales

Existió una discusión en referencia a si las criptomonedas estaban alcanzadas por el Impuesto sobre los Bienes Personales. A este respecto, dicha discusión se abría entre dos posturas.

Por una parte había quienes sostenían que la tenencia de criptoactivos se encontraba exenta del impuesto, en virtud de lo establecido por el artículo 21 de la Ley del mismo:

"ARTÍCULO 21 — Estarán exentos del impuesto:

a) Los bienes pertenecientes a los miembros de las misiones diplomáticas y consulares extranjeras, así como su personal administrativo y técnico y familiares, en la medida y con las limitaciones que establezcan los convenios internacionales aplicables. En su defecto, la exención será procedente, en la misma medida y limitaciones, sólo a condición de reciprocidad;

b) Las cuentas de capitalización comprendidas en el régimen de capitalización previsto en el título III de la ley 24.241 y las cuentas individuales correspondientes a los planes de seguro de retiro privados administrados por entidades sujetas al control de la Superintendencia de Seguros de la Nación, dependiente de la Subsecretaría de Bancos y Seguros de la Secretaría de Política Económica del Ministerio de Economía y Obras y Servicios Públicos. (Inciso sustituido por inc. b) del art. 7º de la Ley Nº 25.063 B.O. 30/12/1998)

c) La cuotas sociales de las cooperativas;

d) ***Los bienes inmateriales (llaves, marcas, patentes, derechos de concesión y otros bienes similares).***

… "

El inciso d) del artículo 21 de la Ley establece la exención a los bienes inmateriales. Al considerarse los criptoactivos como parte de esta especie de activos "intangibles", se encontrarían encuadrados en la exención mencionada.

La otra postura, contraria a la anterior, abrió la discusión a que los criptoactivos si se encuentren alcanzados por el impuesto, en virtud de la aplicación supletoria del Impuesto a las Ganancias, que se enuncia en artículo 31 del Decreto Reglamentario 127/96 del Impuesto sobre los Bienes Personales.

"ARTÍCULO 31 - En los casos no expresamente previstos en este decreto reglamentario se aplicarán supletoriamente las disposiciones legales y reglamentarias del impuesto a las ganancias."

Al considerarse, según este tipo de interpretación, que los criptoactivos son una nueva especie de activos que no fueron contemplados por la Ley, se debería recurrir

supletoriamente a la Ley del Impuesto a las Ganancias para determinar su gravabilidad. Al estar contemplados, en la Ley del Impuesto a las Ganancias, esto implicaría que serían objeto del Impuesto sobre los Bienes Personales también.

Recientemente, el 16 de junio de 2022, la AFIP salió a determinar postura sobre esta discusión, al emitir interpretación por medio del Dictamen 2/2022 y establecer:

"Se puede caracterizar a las criptomonedas como una nueva clase de activo financiero, no tradicional y basado en la tecnología blockchain el cual versa, en definitiva, acerca de una anotación electrónica que incorpora el derecho a una cantidad de dinero determinada, que puede tipificarse como títulos valores, toda vez que participan de las características principales que poseen estos últimos, es decir, son valores incorporados a un registro de anotaciones en cuenta –la blockchain-; resultan bienes homogéneos y fungibles en los términos del artículo 232 del Código Civil y Comercial; su emisión o agrupación es efectuada en serie –conformada ésta por cada bloque que integra la cadena- y; pueden ser susceptibles de tráfico generalizado e impersonal en los mercados financieros.

Las criptomonedas conforman un activo alcanzado por la ley de Impuesto sobre los Bienes Personales de conformidad con lo prescripto en el citado artículo 19, inciso j) y artículo 22 inciso h) de la ley del gravamen."

A nuestro entender, con este Dictamen la AFIP determina postura en considerar a los criptoactivos como activos financieros gravados, y tipificarlos como títulos valores. No existe dudas, entonces, según esta interpretación que son bienes gravados por el impuesto. Sin embargo, la mención que realiza el dictamen citado, en su último párrafo, equiparandolos a los activos considerados en artículo 19 inciso j) y artículo 22 inciso h), abre algunos interrogantes en referencia a su pertinencia y valuación.

El artículo 19 inciso j) de la Ley de Impuesto sobre los Bienes Personales establece:

"*ARTÍCULO 19 — Se consideran situados en el país:*

…

j) Los títulos, las acciones, cuotas o participaciones sociales y otros títulos valores representativos de capital social o equivalente, ***emitidos por entes públicos o privados, cuando éstos tuvieran domicilio en él****.*

…"

El último párrafo del Dictamen 2/2022 hace referencia a criptomonedas de "conformidad con lo prescripto por el artículo 19 inciso j)". Sin embargo, como destacamos en el inciso j) se hace referencia a entes públicos o privados.

En el caso de criptomonedas públicas, como Bitcoin, Ethereum, y otras, no existe un entidad pública o privada que las emita. Se basan, como hemos ya mencionado en trabajos anteriores, en una red descentralizada, que no posee una entidad que regule su funcionamiento, sino en un protocolo (software) instalado en sus servidores que ejecuta las reglas de funcionamiento de la criptomoneda.

Además, como también está en destacado en nuestra cita del artículo, hace mención a que dichos entes públicos o privados “tuvieran domicilio en él”. En trabajos posteriores, se hará un análisis más detallado sobre la problemática impositiva referida al domicilio o territorialidad de los criptoactivos. Pero por ahora podemos mencionar que, además de la imposibilidad de definir una entidad que emita las criptomonedas, al ser las blockchains públicas redes totalmente descentralizadas, no existe la posibilidad de determinar la territorialidad de donde se emiten nuevas criptomonedas en la misma. Por ejemplo, actualmente Bitcoin, emite 6,25 nuevos Bitcoins. Según su protocolo, el minero que gana la competencia resolviendo el acertijo criptográfico, propone un nuevo bloque a ser incorporado en la red, el cual contendrá los nuevos 6,25 Bitcoins. Para que este bloque sea válido deberá ser aceptado por al menos el 51% de los servidores de la red (mecanismo de consenso). Por lo que la emisión de los nuevos Bitcoins, corresponderán a todos los servidores que acepten el nuevo bloque como válido, haciéndose imposible determinar un único lugar como “domicilio” de esos servidores.

El artículo 22 inciso h), que también se menciona específicamente el Dictamen 2/2022 que estamos analizando, hace referencia a la valuación de títulos públicos y demás títulos valores:

“ARTÍCULO 22 — Los bienes situados en el país se valuarán conforme a:

…

h) Los títulos públicos y demás títulos valores, excepto acciones de sociedades anónimas y en comandita —incluidos los emitidos en moneda extranjera— que se coticen en bolsas y mercados: al último valor de cotización al 31 de diciembre de cada año o último valor de mercado de dicha fecha en el supuesto de cuotas partes de fondos comunes de inversión.

Los que no coticen en bolsa se valuarán por su costo, incrementado de corresponder, en el importe de los intereses, actualizaciones y diferencias de cambio que se hubieran devengado a la fecha indicada.

Cuando se trate de acciones se imputarán al valor patrimonial proporcional que surja del último balance cerrado al 31 de diciembre del ejercicio que se liquida. La reglamentación fijará la forma de computar los aumentos y/o disminuciones de capital que se hubieran producido entre la fecha de cierre de la sociedad emisora y el 31 de diciembre del año respectivo.

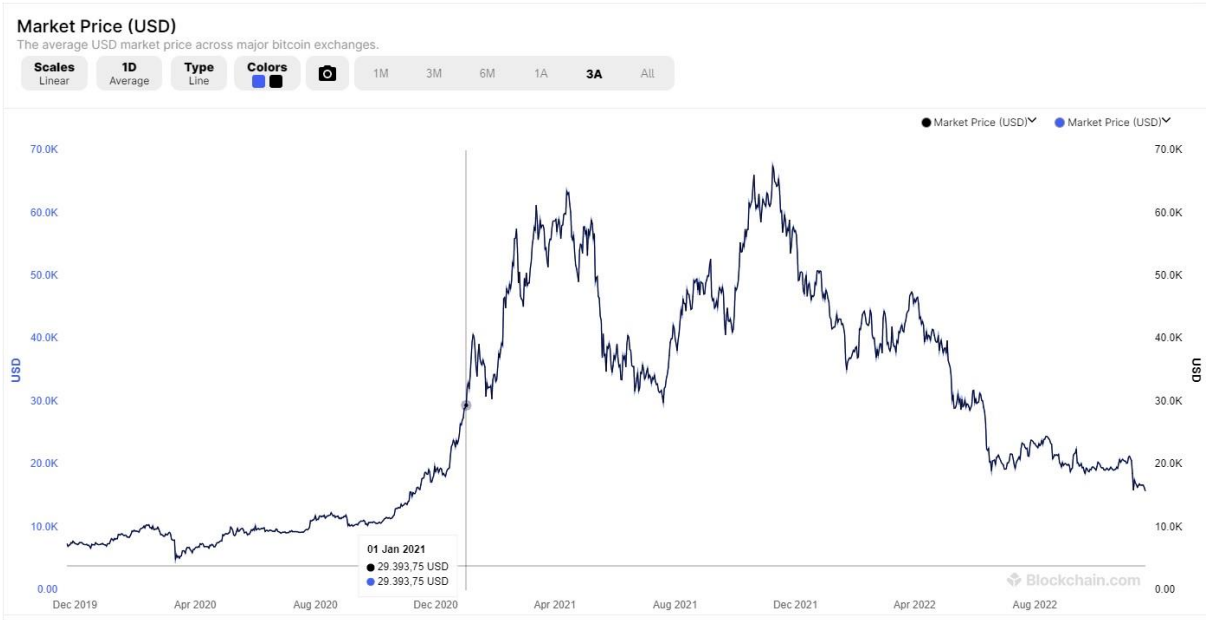
…”

La primera reflexión que podemos hacer es, si las criptomonedas públicas deberían considerarse incluidas en el primer párrafo del inciso h) que define la forma de valuación para títulos públicos y demás títulos valores, que “se coticen en bolsas y mercados”. Las criptomonedas públicas no poseen una bolsa de valores o un mercado regulado en la que cotizen. Los precios que podemos observar en publicaciones periodísticas, plataformas u otros medios de difusión, se corresponden con promedio de precios que se hacen en tiempo real, sobre la negociación que las criptomonedas tienen en los principales Exchanges a nivel mundial. Ese promedio de precios que se nos muestra, inclusive, puede ser muy dispar, en función de cuales son los Exchanges que se consideran, y el peso específico de cada uno de los mismos en el cálculo del promedio.

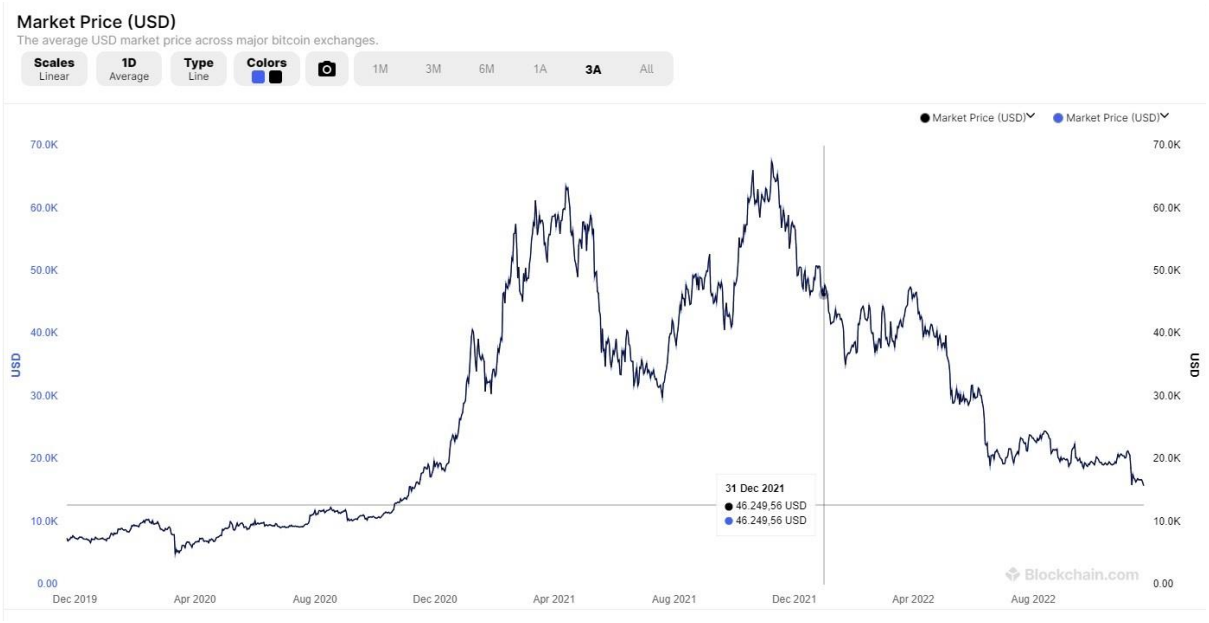
El otro factor a tomar en cuenta, es que no solo no tienen un mercado específico de cotización que refleje un precio “oficial”, sino que el precio que vemos de las criptomonedas no tiene una hora de corte, ni una hora de inicio. Las cripto públicas, por su naturaleza distribuida se negocian las 24 hs del día, en todas partes del mundo.

Siguiendo esta línea de pensamiento, podemos suponer que el criterio de valuación debería ser el establecido en el segundo párrafo del inciso h), “costo, incrementado de corresponder, en el importe de los intereses, actualizaciones y diferencias de cambio”. Pero probablemente la pretensión fiscal se verá enfrentada a la alta volatilidad de precio de las criptomonedas. Sin dudas que la adopción de este criterio (costo), podría significar una considerable diferencia en la liquidación del impuesto. Solo a modo de ejemplo, consideremos que el Bitcoin tenía un valor de 29.394 USD al inicio de 2021, y de 46.250 USD al fin de ese año, pasando por un pico de 67.562 USD el 08 de noviembre de ese año.

Precio del Bitcoin al 01 enero 2021 - Fuente: blockchain.com



Precio del Bitcoin al 31 diciembre 2021 - Fuente: blockchain.com



Precio del Bitcoin al 08 de noviembre 2021 (pico) - Fuente: blockchain.com

Impuesto a las Ganancias

En virtud de la reforma tributaria realizada por medio de la Ley 27.430 B.O.: 29/12/2017, se estableció el alcance en el Impuesto a las Ganancias, de los resultados de la enajenación de monedas digitales

OBJETO DEL IMPUESTO

“ARTÍCULO 2°.- A los efectos de esta ley son ganancias, sin perjuicio de lo dispuesto especialmente en cada categoría y aun cuando no se indiquen en ellas:

…

4) los resultados derivados de la enajenación de acciones, valores representativos y certificados de depósito de acciones y demás valores, cuotas y participaciones sociales —incluidas cuotapartes de fondos comunes de inversión y certificados de participación de fideicomisos financieros y cualquier otro derecho sobre fideicomisos y contratos similares—, ***monedas digitales,*** *Títulos, bonos y demás valores, cualquiera sea el sujeto que las obtenga.*

…"[43]

La modificación del Impuesto a las Ganancias que mencionamos incorpora al objeto del impuesto expresamente las monedas digitales. Tal como mencionamos anteriormente en la interpretación que realizó AFIP por medio del Dictamen 2/2022, el criterio que el organismo aplica es el de equiparar a las monedas digitales con los activos contemplados en artículo 19 inciso j) y artículo 22 inciso h):

"Los títulos, las acciones, cuotas o participaciones sociales y otros títulos valores representativos de capital social o equivalente"

En este caso, para el Impuesto a las Ganancias alinea el mismo criterio, incorporando expresamente a las monedas digitales en el mismo inciso donde contemplaba:

"acciones, valores representativos y certificados de depósito de acciones y demás valores, cuotas y participaciones sociales —incluidas cuotapartes de fondos comunes de inversión y certificados de participación de fideicomisos financieros y cualquier otro derecho sobre fideicomisos y contratos similares—, Títulos, bonos y demás valores, cualquiera sea el sujeto que las obtenga"

FUENTE ARGENTINA

"ARTÍCULO 7°.- Con excepción de lo dispuesto en el párrafo siguiente, las ganancias provenientes de la tenencia y enajenación de acciones, cuotas y participaciones sociales —incluidas cuotapartes de fondos comunes de inversión y certificados de participación de fideicomisos financieros y cualquier otro derecho sobre fideicomisos y contratos similares—, ***monedas digitales****, títulos, bonos y demás valores, se considerarán íntegramente de fuente argentina cuando el emisor se encuentre domiciliado, establecido o radicado en la REPÚBLICA ARGENTINA.*

Los valores representativos o certificados de depósito de acciones y de demás valores, se considerarán de fuente argentina cuando el emisor de las acciones y de los demás valores se encuentre domiciliado, constituido o radicado en la REPÚBLICA ARGENTINA, cualquiera

[43] Ley 27.430 - Modificación de impuestos varios - BO: 29/12/2017 - Capítulo 1 - Ley de Impuesto a las Ganancias - Artículo 2 - Destacado del autor

fuera la entidad emisora de los certificados, el lugar de emisión de estos últimos o el de depósito de tales acciones y demás valores."[44]

En este punto, podemos referenciar el mismo comentario que realizamos en referencia al Impuesto a los Bienes Personales, en lo que respecta a la imposibilidad de determinar el domicilio o territorialidad de una red distribuida como es una Blockchain Pública, tal como Bitcoin, Ethereum, Cardano, y otras.

El problema de la territorialidad de la Blockchain, será abordado con más profundidad en trabajos posteriores, pero creemos conveniente destacar a esta altura, que las Blockchains (tal como se mencionó en trabajos anteriores) se clasifican en "no permisionadas" (o públicas), y "permisionadas" (privadas). Estas últimas, a su vez, se pueden sub-clasificarse en "de consorcio" y "híbridas".

En el caso de las Blockchains permisionadas, generalmente poseen dos tipos de servidores. Los servidores (nodos) administradores, y los servidores (nodos) selladores. Los nodos administradores son los que poseen autoridad para permitir el acceso de usuarios y nodos selladores. Los nodos selladores, son los que realizan las funciones de minería de bloques en la red.

En la mayoría de los desarrollos de Blockchains que se realizan por administraciones públicas, el tipo de Blockchain que se implementa es el de permisionadas o privadas.

En el caso que vamos a analizar de implementación de una Cadena de Bloques para la Provincia de Santa Fe, en el caso que veremos, seguramente será una Blockchain permisionada, por lo cual se podría verificar que al autorizar nodos selladores, estos estén ubicados territorialmente en la República Argentina. De esta manera, si algún token fungible (una nueva moneda digital) se emitiese en la misma, se podría verificar que cumple con lo consignado en la Ley del Impuesto a las Ganancias para considerar a esas monedas digitales como de "fuente argentina".

ALÍCUOTAS

"ARTÍCULO 98.- Operaciones de enajenación de acciones, valores representativos y certificados de depósito de acciones y demás valores, cuotas y participaciones sociales —incluidas cuotapartes de fondos comunes de inversión y certificados de participación en fideicomisos financieros y cualquier otro derecho sobre fideicomisos y contratos similares—, ***monedas digitales****, títulos, bonos y demás valores. La ganancia neta de fuente argentina de las personas humanas y sucesiones indivisas derivada de resultados provenientes de operaciones de enajenación de acciones, valores representativos y certificados de depósito de acciones, cuotas y participaciones sociales —incluidas cuotapartes de fondos comunes de inversión y certificados de participación de fideicomisos financieros y cualquier otro derecho sobre fideicomisos y contratos similares—, monedas digitales, títulos, bonos y demás valores, quedará alcanzada por el impuesto a la alícuota que se detalla a continuación dependiendo del valor de que se trate:*

[44] Idem cita anterior. Artículo 7

a) Títulos públicos, obligaciones negociables, títulos de deuda, cuotapartes de fondos comunes de inversión no comprendidos en el inciso c) siguiente, así como cualquier otra clase de título o bono y demás valores, en todos los casos en moneda nacional sin cláusula de ajuste: CINCO POR CIENTO (5 %).

…

b) Títulos públicos, obligaciones negociables, títulos de deuda, cuotapartes de fondos comunes de inversión no comprendidos en el inciso c) siguiente, ***monedas digitales****, así como cualquier otra clase de título o bono y demás valores, en todos los casos en moneda nacional con cláusula de ajuste o en moneda extranjera: QUINCE POR CIENTO (15 %).*

c) Acciones, valores representativos y certificados de depósitos de acciones y demás valores, certificados de participación de fideicomisos financieros y cualquier otro derecho sobre fideicomisos y contratos similares y cuotapartes de condominio de fondos comunes de inversión a que se refiere el segundo párrafo del artículo 1° de la Ley N° 24.083 y sus modificaciones, que (i) cotizan en bolsas o mercados de valores autorizados por la COMISIÓN NACIONAL DE VALORES que no cumplen los requisitos a que hace referencia el inciso u) del artículo 26 de esta ley, o que (ii) no cotizan en las referidas bolsas o mercados de valores: QUINCE POR CIENTO (15 %).”

Como se puede observar en el articulado el criterio para determinar la tasa de impuesto a aplicar es:

- Si las monedas digitales que se analizan son emitidas en moneda nacional, sin cláusula de ajuste: 5%
- Si son emitidas en moneda extranjera, o moneda nacional con cláusula de ajuste: 15%

Dejamos separado de nuestro análisis si las mismas cotizan en bolsas o mercados regulados por la Comisión Nacional de Valores, ya que hasta el momento, no se ha contemplado esta situación en nuestro país.

El análisis que estamos realizando toma también relevancia, al considerarse en la propuesta que planteamos si los tokens o criptoactivos que se emitan estén “monetizados” o no, y contengan por medio de contratos inteligentes, cláusulas de ajustes.

FORMA DE LIQUIDACIÓN DEL IMPUESTO

“ARTÍCULO 98:

…

La ganancia bruta por la enajenación se determinará con base en las siguientes pautas:

(i) En los casos de los valores comprendidos en los incisos a) y b) del primer párrafo de este artículo, deduciendo del precio de transferencia el costo de adquisición. De tratarse de valores

en moneda nacional con cláusula de ajuste o en moneda extranjera, las actualizaciones y diferencias de cambio no serán consideradas como integrantes de la ganancia bruta.

(ii) En el caso de los valores comprendidos en el inciso c) del primer párrafo de este artículo, deduciendo del precio de transferencia el costo de adquisición actualizado, mediante la aplicación del índice mencionado en el segundo párrafo del artículo 93, desde la fecha de adquisición hasta la fecha de transferencia. Tratándose de acciones liberadas se tomará como costo de adquisición aquél al que se refiere el cuarto párrafo del artículo 49. A tales fines se considerará, sin admitir prueba en contrario, que los valores enajenados corresponden a las adquisiciones más antiguas de su misma especie y calidad."

Debemos destacar que las consideraciones que estamos realizando se refieren a alícuotas y procedimientos a aplicar por personas humanas que liquiden el impuesto. No es la situación de sujetos empresas, o sociedades, en cuyo caso se liquidarán las ganancias correspondientes a la alícuota y con el procedimiento general de tercera categoría del impuesto.

Impuesto sobre los Ingresos Brutos y normativas provinciales

En los últimos años, probablemente impulsados por el auge de compras de criptomonedas que se produjo durante la pandemia covid-19, los gobiernos provinciales de Argentina, comenzaron a incluir dentro de las bases imponibles de impuestos sobre los ingresos brutos, a las actividades vinculadas a la adquisición y venta de monedas digitales.

El presente cuadro muestra un resumen de las provincias que han comenzado a gravar con impuesto a los ingresos brutos a las actividades vinculadas con monedas digitales:

provincia	vigencia	norma legal	características / comentarios
Córdoba	2021	Régimen simplificado - Art. 13: “Fijase en Pesos Cincuenta Mil ($ 50.000,00) mensuales, el monto de ingresos establecido en el inciso j) del artículo 202 del Código Tributario Provincial. Fíjanse en A y B las categorías del Régimen Simplificado Pequeños Contribuyentes a que se refiere el inciso j) del artículo 202 del Código Tributario Provincial, que será aplicable para aquellos sujetos que sólo realicen la actividad de prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente, con operatorias relacionadas con monedas digitales.” Art. 22: Los ingresos derivados de las actividades incluidas en los Códigos de Actividades que se detallan a continuación deben tributar a la alícuota que se establece en la columna “Alícuota” del siguiente cuadro: Código: 620900 La prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente, con operatorias relacionadas con monedas digitales (inciso j) del artículo 202 del Código Tributario).	Se alcanzan por el impuesto: 1. Prestación de servicios vinculados con operatorias relacionadas con monedas digitales; 2. Venta de monedas digitales y su base imponible diferencial; y 3. Los ingresos derivados por la venta de moneda digital cuando éstas provengan del canje por la comercialización de bienes y/o servicios. El reglamento del Código Tributario define qué se entiende por “moneda digital”: A los efectos previstos en el Impuesto sobre los Ingresos Brutos equipárese a

provincia	vigencia	norma legal	características / comentarios
		Alícuota: 4,75% Alícuota reducida: 4,00% Art. 24: Los ingresos provenientes de los servicios financieros, intermediación financiera y otros servicios que se detallan a continuación, efectuados por los sujetos que para cada caso se indica, cuyos Códigos de Actividad se describen en el Anexo I de la presente Ley, deben tributar a la alícuota que se establece en la columna “Alícuota” del siguiente cuadro: 12.- Los servicios destinados a facilitar la gestión y/o intercambio de monedas digitales por monedas fiduciarias de curso legal, otras criptomonedas o cualquier tipo de bienes -y viceversa-, a través de plataformas online, sitios web, aplicaciones tecnológicas, dispositivos y/o plataformas digitales y/o móviles o similares (exchanges de criptomonedas). Alícuota: 4,75% 13.- Compra y venta de monedas digitales conforme inciso b) del artículo 222 del Código Tributario Provincial): Alícuota: 6,50%	“monedas digitales”, los términos “moneda virtual”, “criptomonedas”, “criptoactivos”, “tokens”, “stablecoins” y demás conceptos que por su naturaleza y/o características constituyan y/o impliquen una representación digital de valor que puede ser objeto susceptible de comercio digital y cuyas funciones –directas y/o indirectas- son la de constituir un medio de intercambio y/o una unidad de cuenta y/o una reserva de valor.
Catamarca	2022	ARTÍCULO 11°.- Sustitúyese el Artículo 7 de la Ley 5.022 y sus modificaciones, por el siguiente: «ARTÍCULO 7.- En los actos, operaciones y transacciones que se realicen en especie -incluido los activos digitales- y que configuren el hecho generador de tributos, a los efectos de la determinación de la base imponible se considerará el	También se brinda una definición de activos digitales: Se entiende como activos digitales a aquellos activos intangibles -tales como las

provincia	vigencia	norma legal	características / comentarios
		valor corriente en plaza vigente al momento de producirse el hecho imponible o en su defecto el que surja de procedimiento autorizado por la Dirección General de Rentas. Se entiende como activos digitales a aquellos activos intangibles -tales como las monedas digitales, moneda virtual, criptomonedas, criptoactivos, tokens, stablecoins, etc- que por su naturaleza y/o características constituyan y/o impliquen una representación digital de valor que puede ser objeto susceptible de comercio digital y cuyas funciones – directas y/o indirectas- son la de constituir un medio de intercambio y/o una unidad de cuenta y/o una reserva de valor.» ARTÍCULO 12°.- Incorpórase como inciso j) del Artículo 161 de la Ley 5.022 y sus modificaciones, el siguiente: «j) La prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente con operatorias relacionadas con activos digitales.» ARTÍCULO 13°.- Sustitúyese el Artículo 163 de la Ley 5.022 y sus modificaciones, por el siguiente: «ARTICULO 163.- La persona o entidad que abone sumas de dinero -incluidas las operaciones canceladas con activos digitales- o intervenga en el ejercicio de una actividad gravada, actuará como agente de retención-percepción y/o recaudación en la forma que establezca la Dirección General	monedas digitales, moneda virtual, criptomonedas, criptoactivos, tokens, stablecoins, etc- que por su naturaleza y/o características constituyan y/o impliquen una representación digital de valor que puede ser objeto susceptible de comercio digital y cuyas funciones –directas y/o indirectas- son la de constituir un medio de intercambio y/o una unidad de cuenta y/o una reserva de valor. En la provincia de Catamarca, además de ser alcanzado por ingresos Brutos, los contratos vinculados al comercio de activos digitales, se deberá tributar impuesto de sellos.

provincia	vigencia	norma legal	características / comentarios
		de Rentas.» ARTÍCULO 14°.- Sustitúyese el Artículo 167 de la Ley 5.022 y sus modificaciones, por el siguiente: «ARTICULO 167.- Salvo lo dispuesto para casos especiales, la base imponible estará constituida por el monto total de los ingresos brutos devengados en el período fiscal de las actividades gravadas con independencia de la forma en que se cancelen las operaciones (en efectivo, cheques, en especie, activos digitales, etc.). … » Impuesto de sellos: ARTÍCULO 19°.- Por los actos, contratos y operaciones que a continuación se enumeran deberá pagarse el impuesto que en cada caso se establece: 21.- Contratos vinculados al comercio de activos digitales, criptomonedas, Bitcoin y similares, por la suma total del capital invertido y sus rendimientos Alícuota: 1,50%	
Entre Ríos	2022	ARTICULO 158º.- La base imponible estará constituida por la diferencia entre los precios de compra y venta, en los siguientes casos: … f) En las operaciones de enajenación de acciones, valores representativos y certificados de depósitos de acciones y demás valores, cuotas y participaciones sociales –incluidas	

provincia	vigencia	norma legal	características / comentarios
		cuotas partes de fondos comunes de inversión y certificados de participación de fideicomisos financieros y cualquier otro derecho sobre fideicomisos y contratos similares-, **monedas digitales**, títulos, bonos y demás valores, los ingresos gravados se determinarán deduciendo del precio de transferencia el costo de adquisición que corresponda considerar para la determinación del resultado establecido para este tipo de operaciones en el Impuesto a las Ganancias. A tales fines se considerará, sin admitir prueba en contrario, que los bienes enajenados corresponden a las adquisiciones más antiguas de su misma especie y calidad; …	
La Pampa	2022	Artículo 52.- Incorpórase como inciso l) del artículo 183 del Código Fiscal (t.o. 2018) el siguiente: “l) La prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente con operatorias relacionadas con monedas digitales (monedas virtuales, criptomonedas, criptoactivos, tokens, stablecoins y demás conceptos que por su naturaleza y/o características constituyan y/o impliquen una representación digital de valor que puede ser objeto susceptible de comercio).”. Artículo 53 .- Sustitúyase el inciso c) del artículo 192 del Código Fiscal (t.o. 2018) por el siguiente: “c) las operaciones de compra-venta de divisas o monedas digitales (monedas virtuales, criptomonedas, criptoactivos, tokens, stablecoins y demás conceptos que por su	

provincia	vigencia	norma legal	características / comentarios
		naturaleza y/o características constituyan y/o impliquen una representación digital de valor que puede ser objeto susceptible de comercio).”.	
La Rioja	2022	Ingresos Brutos: ARTÍCULO 125º.- Incorpórese como inciso g) del Artículo 162º del Código Tributario (Ley Nº 6.402 y modificatorias) el siguiente texto: g) La prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente con operatorias relacionadas con monedas digitales”. ARTÍCULO 131º.- Incorpórese como inciso f) del Artículo 171° del Código Tributario Provincial (Ley N° 6.402 y modificatorias) el siguiente texto: “f).- Operaciones de compra y venta de **monedas digitales** realizadas por sujetos que fueran habitualistas en tales operaciones”. Agentes de retención / información ARTÍCULO 128º.- Sustitúyase el Artículo 166º del Código Tributario (Ley Nº 6.402 y modificatorias) por el siguiente texto: “Artículo 166°.- Cuando lo establezca la Dirección General de Ingresos Provinciales, deberán actuar como agentes de retención, percepción o información, las personas humanas, sociedades con o sin personería jurídica, y toda entidad que	Es de destacar que la modificación al código fiscal de la Provincia de La Rioja habilita al gobierno a establecer regímenes de información y percepción de impuestos a los ingresos brutos, en referencia a las actividades vinculadas a monedas digitales

provincia	vigencia	norma legal	características / comentarios
		intervenga en operaciones, o actos – incluidos los cancelados con **monedas digitales** -, con sujetos domiciliados, radicados o constituidos en el país o en el exterior, de los que deriven, o puedan derivar, ingresos alcanzados por el impuesto. Pagos con monedas digitales ARTÍCULO 129º.- Sustitúyase el Artículo 167º del Código Tributario (Ley Nº 6.402 y modificatorias) por el siguiente texto: “Artículo 167°.- Salvo expresa disposición en contrario, el gravamen se determinará sobre la base de los ingresos brutos devengados durante el período fiscal por el ejercicio de la actividad gravada, con independencia de la forma en que se cancelen las operaciones (en efectivo, cheques, en especie, **monedas digitales**, etc.). Valuación Monedas Digitales ARTÍCULO 130º.- Sustitúyase el Artículo 169º del Código Tributario (Ley Nº 6.402 y modificatorias) por el siguiente texto: “Artículo 169°.- Cuando el precio se pacte en especie, - incluidas **monedas digitales** - el ingreso bruto estará constituido por la valuación de la cosa entregada, la locación, el interés, o el servicio prestado, aplicando los precios, la tasa de interés, el valor locativo, etc.; oficiales o corrientes en plaza, a la fecha de generarse el devengamiento.	

provincia	vigencia	norma legal	características / comentarios
		Declaraciones juradas informativas ARTÍCULO 118º.- Sustitúyase el inciso a) del Artículo 25º del Código Tributario (Ley Nº 6.402 y modificatorias) por el siguiente texto: “a).- A presentar en tiempo y forma la declaración jurada de los hechos imponibles atribuidos a ellos por las normas de este Código o Leyes Fiscales Especiales, salvo cuando se disponga expresamente de otra manera. Asimismo, presentar en tiempo y forma la declaración jurada informativa de los regímenes de información propia del contribuyente o responsable o de información de terceros, incluidos los relacionados con operaciones realizadas con **monedas digitales**.” ARTÍCULO 119º.- Sustitúyase el Artículo 27º del Código Tributario (Ley Nº 6.402 y modificatorias) por el siguiente texto: “Artículo 27°.- La Dirección podrá requerir a terceros, y éstos estarán obligados a suministrar, todos los informes (incluidos los relacionados con **monedas digitales**) que se refieren a hechos que, en el ejercicio de sus actividades profesionales, comerciales o de servicios, hayan contribuido a realizar o hayan debido conocer, y que constituyan o modifiquen hechos imponibles según las normas de este Código u otras Leyes Fiscales, salvo el caso en que las normas del Derecho Público o Privado, Nacional o Provincial, establezcan para esas personas el deber del secreto profesional.- ”	

provincia	vigencia	norma legal	características / comentarios
Neuquén	2021	Artículo 182 bis: Se consideran servicios digitales, cualquiera sea el dispositivo utilizado para su descarga, visualización o utilización, aquellos llevados a cabo a través de la red internet o de cualquier adaptación o aplicación de los protocolos, plataformas o de la tecnología utilizada por internet u otra red a través de la que se presten servicios equivalentes que, por su naturaleza, estén básicamente automatizados y requieran una intervención humana mínima, comprendiendo, entre otros, los siguientes: … o) La prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente con operatorias relacionadas con monedas digitales. Se entiende por moneda digital a los fines de la presente ley: moneda virtual, criptomonedas, criptoactivos, tokens, stablecoins y demás conceptos que por su naturaleza y/o características constituyan y/o impliquen una representación digital de valor que puede ser objeto susceptible de comercio digital y cuyas funciones —directas y/o indirectas— son las de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor. (modificado por Ley 33103 B.O.3992 07/01/2022)	En el Código Fiscal 2021 solo se hacía mención muy brevemente en el inciso o) de artículo 182 bis, acerca de monedas digitales. En la nueva modificación del Código Fiscal 2022, se hace un detalle más puntual de a qué se considera monedas digitales.
Tucumán	2021	1. Sustituir el inciso 3. del Artículo 223, por el siguiente: La base imponible estará constituida por diferencia entre los precios de compra y de venta en los siguientes casos:	

provincia	vigencia	norma legal	características / comentarios
		… «3. Operaciones de compra y venta de divisas y títulos públicos. Quedan comprendidos en el presente inciso las operaciones de compra y venta de **monedas digitales**.»	

Tabla 5 Marco normativo algunas provincias respecto a criptomonedas

Todas las provincias, cuyas normativas respecto de criptomonedas se han analizado, coinciden en gravar impositivamente a estas. Es de destacar que en los marcos normativos algunas provincias simplemente se mencionan a las criptomonedas con el fin de gravarlas, mientras que en otros códigos, se hace una conceptualización detallada sobre las mismas, como así también de otros instrumentos que conforman el ecosistema Blockchain.

Normativa de San Luis - Innovación Financiera para la Inversión y el desarrollo socio-económico

Contemporáneamente con la elaboración del presente informe, el Congreso de la provincia de San Luis, sancionó la Ley VIII-1085-2022 de Innovación Financiera para la Inversión y el desarrollo socio-económico. En esta ley, tal vez la primera a nivel de gobiernos subnacionales, se hace mención explícita al uso de la tecnología de Blockchain como instrumento de fomento de la innovación financiera.

La ley, entre otras consideraciones contempla:

"*ARTÍCULO 1°.- La presente Ley tiene por objeto implementar tecnología blockchain para fomentar la Innovación Financiera permitiendo potenciar el desarrollo social, económico, cultural y de inclusión financiera en la Provincia.-*

ARTÍCULO 2°.- A los efectos de la presente Ley se entiende:

Blockchain (cadena de bloques): es una tecnología que permite crear un registro de datos distribuido en una red de ordenadores sin necesidad de contar con un servidor o base de datos central. La actualización y manejo de este registro, solo se puede realizar en consenso con todas las partes que forman la red.

Por esta razón, el poder de cómputo de todos los nodos de la red se usa no solo para introducir información, sino también para protegerla frente a modificaciones no autorizadas. Consecuencia de esto, la blockchain permite alcanzar niveles de seguridad muy altos en comparación con otras tecnologías de bases de datos.-"

Es de destacar, que si bien el artículo 2 parece simplemente enunciativo de lo que es la tecnología de Blockchain, a nuestro parecer, sienta un importante antecedente ante el reconocimiento legal de la infraestructura de la Cadena de Bloque, como soporte de desarrollos, tanto por parte de gobiernos como de particulares.

En esa misma línea, y ya poniendo el foco en el objetivo global de todo nuestro trabajo, que busca evaluar el desarrollo de una plataforma de Blockchain para Santa Fe, creemos que es importante destacar el presente articulado de la Ley promulgada por San Luis;

"ARTÍCULO 4°.- El Poder Ejecutivo establecerá la Autoridad de Aplicación de la presente Ley, que tendrá las siguientes facultades:

a) Elaborar plataformas digitales con tecnología blockchain u otras para integrar servicios y aplicaciones;

b) Seleccionar e instrumentar el protocolo de la cadena de bloques a implementarse, como así también a definir los alcances del mismo y la cantidad de nodos necesarios para su efectiva implementación;

c) Establecer los términos y condiciones para el almacenamiento y disponibilidad de activos digitales;

d) Implementar activos digitales de intercambio, que utilizan criptografía para asegurar las transacciones y establecer el respaldo de los activos virtuales, su resguardo y auditoría;

e) Instrumentar el uso de Contratos Inteligentes y sus alcances;

f) Suscribir convenios con organismos y entidades internacionales, nacionales, provinciales y municipales, públicas y privadas, a fin de adoptar las medidas que resulten necesarias para la organización y desarrollo de estas políticas;

g) Brindar capacitaciones sobre la tecnología blockchain;

h) Implementar toda aquella acción que se considere pertinente o necesaria para la aplicación de la presente Ley.-"

La Ley en cuestión autoriza al poder ejecutivo de San Luis a desarrollar el programa "ACTIVOS DIGITALES SAN LUIS DE AHORRO Y DE ARTE", pero como surge de los artículos anteriores citados, autoriza también al poder ejecutivo de la provincia a actuar como autoridad de aplicación para todo lo vinculado con el desarrollo de uso de la tecnología Blockchain.

También recientemente, se hizo el anuncio periodístico, por parte del gobierno de dicha provincia, sobre la iniciativa de utilizar la tecnología de Blockchain como sustento para la emisión de deuda en moneda extranjera por parte del gobierno de San Luis:[45]

https://www.iproup.com/economia-digital/35910-criptomoneda-provincia-argentina-lanza-patacon-cripto-en-dolares

[45] iProUP | Economía Digital << Llega el "cripto Patacón": el plan de una provincia argentina para emitir deuda en divisa digital atada al dólar >>
https://www.iproup.com/economia-digital/35910-criptomoneda-provincia-argentina-lanza-patacon-cripto-en-dolares
Observado: noviembre 2022

Marco Normativo en otros países

Existe una amplia gama de leyes y reglamentos que regulan la actividad vinculada a criptoactivos, desde las más detalladas y restrictivas, hasta las más abiertas, a nivel regional y mundial.

No es el objetivo del presente trabajo, como también de los posteriores, centrar el foco en un análisis pormenorizado de los marcos normativos de cada país. Pero nos parece oportuno destacar, que tal como expondremos en las conclusiones de este informe, es nuestro entender que en nuestro país no se cuenta con una normativa, orgánica, estructurada y detallada sobre criptoactivos, y en especial, que aborde la problemática de los diferentes desarrollos que se vienen generando en el ecosistema Blockchain.

Atento a esta idea, es que queremos presentar como última parte de este informe, la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos – COM(2020) 593 Final, en fase de aprobación, ya que consideramos que abarca cabalmente la problemática de criptoactivos, desarrollando un ordenamiento minucioso de los principales instrumentos y relaciones jurídicas del ecosistema.

Comenzaremos nuestro análisis, presentando un esquema reducido del ordenamiento propuesto, para poder destacar la diversidad de conceptos que relaciones vinculadas a criptoactivos que abarca.

Reglamento del Parlamento Europeo - Criptoactivos

TÍTULO I Objeto, ámbito de aplicación y definiciones		Artículo 1 Objeto
		Artículo 2 Ámbito de aplicación
		Artículo 3 Definiciones
TÍTULO II Criptoactivos distintos de fichas referenciadas a activos o fichas de dinero electrónico		Artículo 4 Ofertas públicas de criptoactivos, distintos de fichas referenciadas a activos o fichas de dinero electrónico, y admisión a negociación de dichos criptoactivos en plataformas de negociación de criptoactivos
		Artículo 5 Contenido y forma del libro blanco de criptoactivos
		Artículo 6 Comunicaciones publicitarias
		Artículo 7 Notificación del libro blanco de criptoactivos y, en su caso, de las comunicaciones publicitarias
		Artículo 8 Publicación del libro blanco de criptoactivos y, en su caso, de las comunicaciones publicitarias
		Artículo 9 Oferta pública de criptoactivos, distintos de fichas referenciadas a activos o fichas de dinero electrónico, de duración limitada
		Artículo 10 Permiso para ofertar al público criptoactivos, distintos de fichas referenciadas a activos o fichas de dinero electrónico, o solicitar su admisión a negociación en plataformas de negociación de criptoactivos
		Artículo 11 Modificación del libro blanco de criptoactivos y, en su caso, de las comunicaciones publicitarias tras su publicación
		Artículo 12 Derecho de desistimiento
		Artículo 13 Obligaciones de los emisores de criptoactivos distintos de fichas referenciadas a activos o fichas de dinero electrónico
		Artículo 14 Responsabilidad de los emisores de criptoactivos, distintos de fichas referenciadas a activos o fichas de dinero electrónico, respecto de la información contenida en el libro blanco de criptoactivos
TÍTULO III Fichas referenciadas a activos	Capítulo 1 Autorización para la oferta pública de fichas referenciadas a activos y	Artículo 15 Autorización
		Artículo 16

		Solicitud de autorización
		Artículo 17 Contenido y forma del libro blanco de criptoactivos relativo a fichas referenciadas a activos
		Artículo 18 Valoración de la solicitud de autorización
		Artículo 19 Concesión o denegación de la autorización
		Artículo 20 Revocación de la autorización
		Artículo 21 Modificación del libro blanco de criptoactivos relativo a fichas referenciadas a activos tras su publicación
		Artículo 22 Responsabilidad de los emisores de fichas referenciadas a activos respecto de la información contenida en el libro blanco de criptoactivos
	Capítulo 2 Obligaciones de los emisores de fichas referenciadas a activos	Artículo 23 Obligación de actuar con honestidad, imparcialidad y profesionalidad, en el mejor interés de los titulares de fichas referenciadas a activos
		Artículo 24 Publicación del libro blanco de criptoactivos y, en su caso, de las comunicaciones publicitarias
		Artículo 25 Comunicaciones publicitarias
		Artículo 26 Información continua a los titulares de fichas referenciadas a activos
		Artículo 27 Procedimiento de tramitación de reclamaciones
		Artículo 28 Prevención, detección, gestión y comunicación de los conflictos de intereses
		Artículo 29 Información a las autoridades competentes
		Artículo 30 Sistema de gobernanza
		Artículo 31 Requisitos de fondos propios
	CAPÍTULO 3 RESERVA DE ACTIVOS	Artículo 32 Obligación de disponer de activos de reserva, y composición y gestión de la reserva de activos

		Artículo 33 Custodia de los activos de reserva
		Artículo 34 Inversión de los activos de reserva
		Artículo 35 Derechos frente a los emisores de fichas referenciadas a activos o sobre los activos de reserva
		Artículo 36 Prohibición del devengo de intereses
	CAPÍTULO 4 ADQUISICIONES DE EMISORES DE FICHAS REFERENCIADAS A ACTIVOS	Artículo 37 Evaluación de las adquisiciones previstas de emisores de fichas referenciadas a activos
		Artículo 38 Contenido de la evaluación de las adquisiciones previstas de emisores de fichas referenciadas a activos
	CAPÍTULO 5 FICHAS SIGNIFICATIVAS REFERENCIADAS A ACTIVOS	Artículo 39 Clasificación de fichas referenciadas a activos como fichas significativas referenciadas a activos
		Artículo 40 Clasificación voluntaria de fichas referenciadas a activos como fichas significativas referenciadas a activos
		Artículo 41 Obligaciones adicionales específicas de los emisores de fichas significativas referenciadas a activos
	Capítulo 6 Liquidación ordenada	Artículo 42 Liquidación ordenada
TÍTULO IV: Fichas de dinero electrónico	Capítulo 1 Requisitos que deben cumplir todos los emisores de fichas de dinero electrónico	Artículo 43 Autorización
		Artículo 44 Emisión y reembolsabilidad de las fichas de dinero electrónico
		Artículo 45 Prohibición del devengo de intereses
		Artículo 46 Contenido y forma del libro blanco de criptoactivos relativo a fichas de dinero electrónico
		Artículo 47 Responsabilidad de los emisores de fichas de dinero electrónico respecto de la información facilitada en el libro blanco de criptoactivos
		Artículo 48 Comunicaciones publicitarias
		Artículo 49 Inversión de los fondos recibidos por los emisores a cambio de las fichas de dinero electrónico

	Capítulo 3: Obligaciones para la prestación de servicios específicos de criptoactivos	Artículo 67 Custodia y administración de criptoactivos por cuenta de terceros
		Artículo 68 Explotación de una plataforma de negociación de criptoactivos
		Artículo 69 Canje de criptoactivos por moneda fiat o canje de criptoactivos por otros criptoactivos
		Artículo 70 Ejecución de órdenes relacionadas con criptoactivos por cuenta de terceros
		Artículo 71 Colocación de criptoactivos
		Artículo 72 Recepción y transmisión de órdenes por cuenta de terceros
		Artículo 73 Asesoramiento sobre criptoactivos
	Capítulo 4: Adquisición de proveedores de servicios de criptoactivos	Artículo 74 Evaluación de las adquisiciones previstas de proveedores de servicios de criptoactivos
		Artículo 75 Contenido de la evaluación de las adquisiciones previstas de proveedores de servicios de criptoactivos
TÍTULO VI: Prevención del abuso de mercado en relación con criptoactivos		Artículo 76 Ámbito de aplicación de las normas sobre abuso de mercado
		Artículo 77 Comunicación de información privilegiada
		Artículo 78 Prohibición de operaciones con información privilegiada
		Artículo 79 Prohibición de comunicación ilícita de información privilegiada
		Artículo 80 Prohibición de manipulación de mercado
Título VII: Autoridades competentes, ABE y AEVM	Capítulo 1: Facultades de las autoridades competentes y cooperación entre las autoridades competentes, la ABE y la AEVM	Artículo 81 Autoridades competentes
		Artículo 82 Facultades de las autoridades competentes
		Artículo 83 Cooperación entre las autoridades competentes
		Artículo 84 Cooperación con la ABE y la AEVM
		Artículo 85

		Cooperación con otras autoridades
		Artículo 86 Obligaciones de notificación
		Artículo 87 Secreto profesional
		Artículo 88 Protección de datos
		Artículo 89 Medidas cautelares
		Artículo 90 Cooperación con terceros países
		Artículo 91 Tramitación de reclamaciones por las autoridades competentes
	Capítulo 2: Medidas y sanciones administrativas de las autoridades competentes	Artículo 92 Sanciones administrativas y otras medidas administrativas
		Artículo 93 Ejercicio de las facultades supervisoras y sancionadoras
		Artículo 94 Derecho de recurso
		Artículo 95 Publicación de decisiones
		Artículo 96 Notificación de sanciones y medidas administrativas a la AEVM y a la ABE
		Artículo 97 Denuncia de infracciones y protección de los denunciantes
	Capítulo 3: Responsabilidades de la ABE en materia de supervisión de emisores de fichas significativas referenciadas a activos y de fichas significativas de dinero electrónico y colegios de supervisores	Artículo 98 Responsabilidades de la ABE en materia de supervisión de emisores de fichas significativas referenciadas a activos y de fichas significativas de dinero electrónico
		Artículo 99 Colegios para los emisores de fichas significativas referenciadas a activos
		Artículo 100 Dictámenes no vinculantes de los colegios para los emisores de fichas significativas referenciadas a activos

		Artículo 101 Colegio para los emisores de fichas significativas de dinero electrónico
		Artículo 102 Dictámenes no vinculantes del colegio para los emisores de fichas significativas de dinero electrónico
	Capítulo 4: Facultades y competencias de la ABE en relación con los emisores de fichas significativas referenciadas a activos y de fichas significativas de dinero electrónico	Artículo 103 Ejercicio de las facultades a que se refieren los artículos 104 a 107
		Artículo 104 Solicitud de información
		Artículo 105 Facultades generales de investigación
		Artículo 106 Inspecciones in situ
		Artículo 107 Intercambio de información
		Artículo 108 Acuerdos administrativos sobre el intercambio de información entre la ABE y terceros países
		Artículo 109 Divulgación de información procedente de terceros países
		Artículo 110 Cooperación con otras autoridades
		Artículo 111 Secreto profesional
		Artículo 112 Medidas de supervisión adoptadas por la ABE
		Artículo 113 Multas
		Artículo 114 Multas coercitivas
		Artículo 115 Divulgación, naturaleza, ejecución y asignación de multas y multas coercitivas
		Artículo 116 Normas de procedimiento para la adopción de medidas de supervisión y la imposición de multas
		Artículo 117 Audiencia de las personas afectadas
		Artículo 118 Control del Tribunal de Justicia

		Artículo 119 Tasas de supervisión
		Artículo 120 Delegación de tareas de la ABE en las autoridades competentes
TÍTULO VIII: Actos delegados y actos de ejecución		Artículo 121 Ejercicio de la delegación de poderes
Título IX: Disposiciones transitorias y finales		Artículo 122 Informe
		Artículo 123 Medidas transitorias
		Artículo 124 Modificación de la Directiva (UE) 2019/1937
		Artículo 125 Transposición de la modificación de la Directiva (UE) 2019/1937
		Artículo 126 Entrada en vigor y aplicación

Tabla 6 Reglamento del Parlamento Europeo - Criptoactivos

Hemos destacado en color diferente en el cuadro, el articulado, que consideramos relevante para poder visualizar las principales directrices de regulación.

Dentro del exhaustivo marco normativo detallado que brinda el Reglamento del Parlamento Europeo, queremos destacar algunos puntos salientes, en especial para reforzar la idea del abordaje integral normativo que se hace en el mismo, de la tecnología de Blockchain, como así de los instrumentos derivados del ecosistema de Cadena de Bloques.

Artículo 3 – Definiciones: se brinda un detalle de 28 definiciones, dentro de las cuales podemos mencionar a actores del ecosistema, como así también aspectos tecnológicos que se deben conceptualizar a los fines de determinar claramente el alcance legal de la regulación que se establece.

Requisitos a cumplir por quienes realicen oferta pública de criptoactivos

“Artículo 4 - Ofertas públicas de criptoactivos, distintos de fichas referenciadas a activos o fichas de dinero electrónico, y admisión a negociación de dichos criptoactivos en plataformas de negociación de criptoactivos

1. Un emisor de criptoactivos, distintos de fichas referenciadas a activos o fichas de dinero electrónico, no podrá, en la Unión, ofertar públicamente dichos criptoactivos ni solicitar su admisión a negociación en una plataforma de negociación de criptoactivos a menos que:

a) sea una persona jurídica;

b) haya elaborado el correspondiente libro blanco de criptoactivos de conformidad con el artículo 5;

c) haya notificado el libro blanco de criptoactivos de conformidad con el artículo 7;

d) haya publicado el libro blanco de criptoactivos de conformidad con el artículo 8;

e) reúna los requisitos del artículo 13.

…
“

Contenido mínimo del white-paper que deben publicar quienes pretendan realizar oferta pública de criptoactivos

“Artículo 5 - Contenido y forma del libro blanco de criptoactivos

1. El libro blanco de criptoactivos a que se refiere el artículo 4, apartado 1, letra b), contendrá toda la información que se indica a continuación:

a) descripción pormenorizada del emisor y presentación de los principales participantes en el diseño y el desarrollo del proyecto;

b) descripción pormenorizada del proyecto del emisor, el tipo de criptoactivo que se ofertará al público o cuya admisión a negociación se solicita, los motivos de la oferta pública del criptoactivo o de la solicitud de su admisión a negociación, y el uso previsto de la moneda fiat o de los otros criptoactivos obtenidos a través de la oferta pública;

c) descripción pormenorizada de las características de la oferta pública, en particular el número de criptoactivos que se emitirá o cuya admisión a negociación se solicita, el precio de emisión de los criptoactivos y las condiciones de suscripción;

d) descripción pormenorizada de los derechos y obligaciones asociados a los criptoactivos, así como de los procedimientos y condiciones para el ejercicio de esos derechos;

e) información sobre la tecnología subyacente y los estándares aplicados por el emisor de los criptoactivos a efectos de su mantenimiento, almacenamiento y transferencia;

f) descripción pormenorizada de los riesgos asociados al emisor de los criptoactivos, los criptoactivos, la oferta pública del criptoactivo y la ejecución del proyecto;

g) elementos de información especificados en el anexo I.”

Obligaciones y Responsabilidades de los emisores de criptoactivos

“Artículo 13 - Obligaciones de los emisores de criptoactivos distintos de fichas referenciadas a activos o fichas de dinero electrónico

1. Los emisores de criptoactivos, distintos de fichas referenciadas a activos o fichas de dinero electrónico:

a) actuarán con honestidad, imparcialidad y profesionalidad;

b) se comunicarán con los titulares de criptoactivos de manera imparcial, clara y no engañosa;

c) prevendrán, detectarán, gestionarán y comunicarán todo conflicto de intereses que pueda surgir;

d) mantendrán todos sus sistemas y protocolos de acceso seguro en conformidad con los estándares pertinentes de la Unión.

A los fines de la letra d), la AEVM, en cooperación con la ABE, elaborará directrices con arreglo al artículo 16 del Reglamento (UE) n.º 1095/2010 para especificar los estándares de la Unión.

2. Los emisores de criptoactivos, distintos de fichas referenciadas a activos o fichas de dinero electrónico, actuarán en el mejor interés de los titulares de los criptoactivos y les brindarán un trato equitativo, salvo que en el libro blanco de criptoactivos y, en su caso, en las comunicaciones publicitarias se haga constar un trato preferencial.

3. Cuando, por cualquier motivo, se cancele una oferta pública de criptoactivos, distintos de fichas referenciadas a activos o fichas de dinero electrónico, los emisores correspondientes se asegurarán de que los fondos obtenidos de los compradores o posibles compradores les sean debidamente reembolsados con la mayor brevedad.

Artículo 14 - Responsabilidad de los emisores de criptoactivos, distintos de fichas referenciadas a activos o fichas de dinero electrónico, respecto de la información contenida en el libro blanco de criptoactivos

1. Cuando un emisor de criptoactivos, distintos de fichas referenciadas a activos o fichas de dinero electrónico, o su órgano de dirección infrinjan el artículo 5 al proporcionar, en el libro blanco de criptoactivos o en la versión modificada de este, información que no sea completa, imparcial o clara, o al proporcionar información engañosa, los titulares de los criptoactivos podrán reclamar una indemnización a dicho emisor o a su órgano de dirección por los perjuicios sufridos a consecuencia de la infracción.

2. Toda exclusión de responsabilidad civil carecerá de efectos jurídicos.

3. Corresponderá a los titulares de los criptoactivos demostrar que el emisor de criptoactivos, distintos de fichas referenciadas a activos o fichas de dinero electrónico, ha

cometido una infracción del artículo 5 que ha afectado a su decisión de compra, venta o canje de los mencionados criptoactivos.

4. Los titulares de criptoactivos no podrán reclamar una indemnización por daños y perjuicios en relación con la información facilitada en el resumen a que se refiere el artículo 5, apartado 7, ni en su traducción, excepto cuando:

a) el resumen sea engañoso, inexacto o incoherente con las demás partes del libro blanco de criptoactivos;

b) el resumen, leído junto con las demás partes del libro blanco de criptoactivos, no proporcione información clave para ayudar a los consumidores y los inversores a tomar una decisión sobre la compra de los criptoactivos.

5. El presente artículo no excluye otras reclamaciones de responsabilidad civil de conformidad con el Derecho nacional."

En este punto el Reglamento indica una serie de obligaciones que deben cumplir quienes realicen la emisión de Fichas referenciadas a activos (tokens fungibles que se sustentados en canasta de monedas u otros activos – oro, plata, soja, etc…), y Fichas de dinero electrónico (tokens fungibles representativos de una moneda fiat). Veamos primero la definición de estos dos conceptos que brinda el Reglamento en artículo 3:

3) «Ficha referenciada a activos»: un tipo de criptoactivo que, a fin de mantener un valor estable, se referencia al valor de varias monedas fiat de curso legal, una o varias materias primas, uno o varios criptoactivos, o una combinación de dichos activos.

4) «Ficha de dinero electrónico»: un tipo de criptoactivo cuya principal finalidad es la de ser usado como medio de intercambio y que, a fin de mantener un valor estable, se referencia al valor de una moneda fiat de curso legal.

Fondos propios que deberán disponer los emisores de fichas referenciadas a activos

"Artículo 31 - Requisitos de fondos propios

1. Los emisores de fichas referenciadas a activos dispondrán, en todo momento, de fondos propios por un importe igual como mínimo al importe más elevado de los siguientes:

a) 350 000 EUR;

b) 2 % del importe medio de los activos de reserva a que se refiere el artículo 32.

A los fines de la letra b), el importe medio de los activos de reserva será el importe medio de los activos de reserva al final de cada día natural, calculado a lo largo de los seis meses anteriores.

Cuando un emisor oferte más de una categoría de fichas referenciadas a activos, el importe de la letra b) será la suma del importe medio de los activos de reserva que respalden cada categoría de fichas referenciadas a activos."

Fondos de activos de reserva a mantener por los emisores

"Artículo 32 - Obligación de disponer de activos de reserva, y composición y gestión de la reserva de activos

1. Los emisores de fichas referenciadas a activos constituirán y mantendrán en todo momento una reserva de activos.

2. Los emisores que oferten al público dos o más categorías de fichas referenciadas a activos constituirán y mantendrán una reserva de activos diferente para cada categoría de fichas referenciadas a activos, y gestionarán cada reserva de forma independiente.

Los emisores de fichas referenciadas a activos que oferten al público una misma categoría de fichas referenciadas a activos constituirán y mantendrán una única reserva de activos para esa categoría.

…

Artículo 33 - Custodia de los activos de reserva

1. Los emisores de fichas referenciadas a activos establecerán, mantendrán y aplicarán políticas, procedimientos y acuerdos contractuales de custodia que garanticen en todo momento que:

a) los activos de reserva se mantengan separados de los activos propios del emisor;

b) los activos de reserva estén libres de cargas y no se pignoren como «acuerdo de garantía financiera», «acuerdo de garantía financiera con cambio de titularidad» ni «acuerdo de garantía financiera prendaria» en el sentido del artículo 2, apartado 1, letras a), b) y c), de la Directiva 2002/47/CE del Parlamento Europeo y del Consejo ;

c) los activos de reserva se mantengan en custodia de conformidad con el apartado 4;

d) los emisores de fichas referenciadas a activos puedan acceder rápidamente a los activos de reserva para atender las solicitudes de reembolso de los titulares de las fichas."

Inversiones que pueden realizar con los activos de reserva

"Artículo 34 - Inversión de los activos de reserva

1. Los emisores de fichas referenciadas a activos que inviertan una parte de los activos de reserva lo harán únicamente en instrumentos financieros de elevada liquidez que

presenten un riesgo mínimo de crédito y de mercado. Las inversiones deberán poderse liquidar rápidamente y con la mínima incidencia negativa en los precios.

…

“

Regulación de la prestación de servicios de custodia de criptoactivos

“ Artículo 67 - Custodia y administración de criptoactivos por cuenta de terceros

1. Los proveedores de servicios de criptoactivos autorizados para prestar el servicio de custodia y administración por cuenta de terceros celebrarán un acuerdo con sus clientes para especificar sus obligaciones y responsabilidades. Este acuerdo incluirá, como mínimo, todos los elementos siguientes:

a) la identidad de las partes en el acuerdo;

b) la naturaleza del servicio prestado y una descripción de dicho servicio;

c) los medios de comunicación entre el proveedor de servicios de criptoactivos y el cliente, incluido el sistema de autenticación del cliente;

d) una descripción de los sistemas de seguridad utilizados por el proveedor de servicios de criptoactivos;

e) las comisiones aplicadas por el proveedor de servicios de criptoactivos;

f) la ley aplicable al acuerdo.

…”

Regulación de servicios de plataforma de negociación de criptoactivos

“Artículo 68 - Explotación de una plataforma de negociación de criptoactivos

1. Los proveedores de servicios de criptoactivos autorizados para explotar una plataforma de negociación de criptoactivos establecerán normas de funcionamiento para la plataforma de negociación. Estas normas de funcionamiento deberán, como mínimo:

a) establecer los requisitos y los procesos de diligencia debida y aprobación que se aplicarán antes de la admisión de criptoactivos en la plataforma de negociación;

b) definir, en su caso, las categorías de exclusión, esto es, los tipos de criptoactivos que no se admitirán a negociación en la plataforma de negociación, si los hubiere.

c) establecer las políticas, los procedimientos y el nivel de las comisiones aplicables, en su caso, para la admisión a negociación de criptoactivos en la plataforma de negociación;

d) establecer criterios objetivos y proporcionados para la participación en las actividades de negociación, que promuevan un acceso equitativo y abierto a la plataforma de negociación para los clientes que deseen negociar;

e) establecer requisitos para garantizar una negociación justa y ordenada;

f) establecer condiciones con el fin de que los criptoactivos permanezcan accesibles para negociación, incluidos umbrales de liquidez y requisitos de información periódica;

g) establecer las condiciones en las que podrá suspenderse la negociación de los criptoactivos;

h) establecer procedimientos para garantizar la liquidación eficiente tanto de las operaciones con criptomonedas como de las operaciones con moneda fiat."

Regulación del canje de criptoactivos por moneda fiat y por otros criptoactivos

"Artículo 69

Canje de criptoactivos por moneda fiat o canje de criptoactivos por otros criptoactivos

1. Los proveedores de criptoactivos autorizados para canjear criptoactivos por moneda fiat u otros criptoactivos establecerán una política comercial no discriminatoria que indique, en particular, el tipo de clientes con los que aceptan realizar operaciones y las condiciones que deberán cumplir los clientes.

2. Los proveedores de servicios de criptoactivos autorizados para canjear criptoactivos por moneda fiat u otros criptoactivos publicarán un precio firme de los criptoactivos o un método para determinar el precio de los criptoactivos que proponen canjear por moneda fiat u otros criptoactivos.

3. Los proveedores de servicios de criptoactivos autorizados para canjear criptoactivos por moneda fiat u otros criptoactivos ejecutarán las órdenes de los clientes a los precios anunciados en el momento de su recepción.

4. Los proveedores de servicios de criptoactivos autorizados para canjear criptoactivos por moneda fiat u otros criptoactivos publicarán los detalles de las órdenes y las operaciones realizadas por ellos, incluidos los volúmenes y precios de las operaciones."

Ordenes de operaciones con criptoactivos por cuenta de terceros

"Artículo 70 - Ejecución de órdenes relacionadas con criptoactivos por cuenta de terceros

1. Los proveedores de servicios de criptoactivos autorizados a ejecutar órdenes relacionadas con criptoactivos por cuenta de terceros tomarán todas las medidas necesarias para obtener, al ejecutar órdenes, el mejor resultado posible para sus clientes, teniendo en cuenta los factores de mejor ejecución, como el precio, los costes, la rapidez, la probabilidad de ejecución y liquidación, el volumen, la naturaleza o cualquier otra consideración pertinente

para la ejecución de la orden, a menos que el proveedor de servicios de criptoactivos ejecute órdenes relacionadas con criptoactivos siguiendo instrucciones específicas dadas por sus clientes.

…"

Colocación de criptoactivos

"Artículo 71 - Colocación de criptoactivos

1. Los proveedores de servicios de criptoactivos autorizados para colocar criptoactivos comunicarán la siguiente información al emisor o a cualquier tercero que actúe en su nombre, antes de celebrar un contrato con ellos:

a) el tipo de colocación considerado, indicando si se garantiza o no un importe mínimo de compra;

b) una indicación del importe de los gastos de transacción asociados al servicio para la operación propuesta;

c) el momento, el proceso y el precio considerados para la operación propuesta;

d) información sobre los compradores destinatarios.

Los proveedores de servicios de criptoactivos autorizados para colocar criptoactivos obtendrán, antes de colocar los criptoactivos de que se trate, el acuerdo de los emisores o de cualquier tercero que actúe en su nombre en lo que respecta a las letras a) a d).

2. Las normas sobre conflictos de intereses a que se refiere el artículo 65 preverán un procedimiento específico y adecuado para prevenir, controlar, gestionar y, en su caso, comunicar cualquier conflicto de intereses derivado de las siguientes situaciones:

a) los proveedores de servicios de criptoactivos colocan los criptoactivos entre sus propios clientes;

b) el precio propuesto para la colocación de criptoactivos se ha sobrestimado o subestimado. "

Asesoramiento sobre criptoactivos

"Artículo 73 - Asesoramiento sobre criptoactivos

1. Los proveedores de servicios de criptoactivos autorizados a prestar asesoramiento sobre criptoactivos evaluarán la compatibilidad de tales criptoactivos con las necesidades de los clientes y los recomendarán únicamente cuando redunde en interés de los clientes.

2. Los proveedores de servicios de criptoactivos autorizados a prestar asesoramiento sobre criptoactivos garantizarán que las personas físicas que faciliten asesoramiento o información sobre criptoactivos o presten un servicio de criptoactivos en su nombre posean los conocimientos y la experiencia necesarios para cumplir sus obligaciones.

3. A efectos de la evaluación a que se refiere el apartado 1, los proveedores de servicios de criptoactivos autorizados a prestar asesoramiento sobre criptoactivos solicitarán

información sobre el conocimiento y la experiencia del cliente o posible cliente en relación con los criptoactivos, sus objetivos, su situación financiera, incluida la capacidad de soportar pérdidas, y su comprensión básica de los riesgos que conlleva la adquisición de criptoactivos.

Los proveedores de servicios de criptoactivos autorizados a prestar asesoramiento sobre criptoactivos advertirán a los clientes de que, debido a su negociabilidad, el valor de los criptoactivos puede fluctuar.

4. Los proveedores de servicios de criptoactivos autorizados a prestar asesoramiento sobre criptoactivos establecerán, mantendrán y aplicarán políticas y procedimientos que les permitan recopilar y evaluar toda la información necesaria a fin de llevar a cabo esta evaluación para cada cliente. Tomarán medidas razonables para garantizar que la información recopilada sobre sus clientes o posibles clientes sea fiable.

5. Cuando los clientes no faciliten la información requerida con arreglo al apartado 4, o cuando los proveedores de servicios de criptoactivos autorizados a prestar asesoramiento sobre criptoactivos consideren, sobre la base de la información recibida con arreglo al apartado 4, que los clientes o posibles clientes no tienen conocimientos suficientes, los proveedores de servicios de criptoactivos autorizados a prestar asesoramiento sobre criptoactivos informarán a dichos clientes o posibles clientes de que los criptoactivos o servicios de criptoactivos pueden ser inadecuados para ellos y les advertirán sobre los riesgos asociados con los criptoactivos. Dicha advertencia de riesgo indicará claramente el riesgo de perder la totalidad del dinero invertido o convertido en criptoactivos. Los clientes deberán reconocer expresamente que han recibido y comprendido la advertencia formulada por el proveedor de servicios de criptoactivos de que se trate.

6. Los proveedores de servicios de criptoactivos autorizados a prestar asesoramiento sobre criptoactivos revisarán, para cada cliente, la evaluación a que se refiere el apartado 1 cada dos años después de la evaluación inicial realizada de conformidad con dicho apartado.

7. Una vez realizada la evaluación a que se refiere el apartado 1, los proveedores de servicios de criptoactivos autorizados a prestar asesoramiento sobre criptoactivos facilitarán a los clientes un informe que resuma el asesoramiento prestado a dichos clientes. Este informe se elaborará y comunicará al cliente en un soporte duradero. Dicho informe deberá, como mínimo:

a) especificar las exigencias y necesidades de los clientes;

b) contener un esbozo del asesoramiento prestado."

Autoridades de aplicación, funciones de la ABE (Autoridad Bancaria Europea) y AEVM (Autoridad Europea de Valores y Mercados), y su regulación (artículo 81 y siguientes)

"Artículo 81 - Autoridades competentes

1. Los Estados miembros designarán a las autoridades competentes responsables de desempeñar las funciones y cometidos previstos en el presente Reglamento e informarán de ello a la ABE y la AEVM.

2. Cuando los Estados miembros designen a más de una autoridad competente de *conformidad con el apartado 1, determinarán sus respectivas funciones y*

designarán a una de ellas como punto de contacto único para la cooperación administrativa transfronteriza entre las autoridades competentes, así como con la ABE y la AEVM.

3. La AEVM publicará en su sitio web una lista de las autoridades competentes designadas de conformidad con el apartado 1.”

Resumen y conclusiones sobre el marco normativo de criptoactivos

Hemos comenzado nuestro informe sobre el marco normativo de criptoactivos, analizando la Constitución Nacional Argentina en lo referente al atributo del Congreso Nacional para emitir moneda de curso legal en el país. Pudimos ver que ese poder fue delegado al Banco Central de la República Argentina, y expresamente denegado a los gobiernos subnacionales por la Carta Orgánica del mismo.

También mencionamos la conceptualización de moneda de curso legal, y vimos que las criptomonedas no pueden encuadrarse dentro de esta categorización. Las operaciones que se realizan con criptomonedas, como mencionamos, deben ser consideradas como obligaciones de entregar cosas.

En función de esta definición podemos suponer que el BCRA no ha emitido un cuerpo normativo específico para criptoactivos, ya que, en la conceptualización de obligaciones de entregar cosas, no estarían los criptoactivos vinculados directamente a la función reguladora de la entidad.

En base a lo planteado en el párrafo anterior, analizamos que el BCRA ha dictado resoluciones vinculadas a la prohibición para bancos de vender criptomonedas, y resoluciones por las cuales interviene en el comercio de criptomonedas, en función de defender los lineamientos de política cambiaria.

Analizamos la normativa impositiva en lo referente a monedas digitales, donde vimos la interpretación realizada por AFIP para considerarlas como activos financieros semejantes a títulos y valores. Vimos también las dudas que abre esta interpretación, en especial por querer categorizar una nueva y diferencial especie de activos, con una categoría de activos financieros altamente regulados, con mercados transparentes y estratificados.

Seguido a esto realizamos un resumen de los marcos normativos emitidos por gobiernos provinciales. Pudimos observar situaciones dispares, como casos en los cuales simplemente se han ocupado de gravar a los criptoactivos por impuestos (Ingresos Brutos), sin dedicarse a conceptualizar a los mismos, y otros casos donde la normativa provincial es más amplia, organizada y puntual.

Por último, en lo referente a la normativa local, analizamos la Ley de Innovación Financiera para la Inversión y el desarrollo socio-económico de la provincia de San Luis.

Realizamos un análisis puntual de esta ley, ya que consideramos, por una parte que expresamente promueve el uso de la tecnología de Blockchain, pero especialmente, porque define un marco normativo específico semejante a la propuesta del trabajo que nos ocupa. Sienta en este aspecto, tal vez, el antecedente más relevante que debería analizar, en la evaluación de nuestra propuesta, el gobierno de la provincia de Santa Fe.

Por último, realizamos un enfoque del marco normativo comparativo a nivel internacional, para lo cual elegimos selectivamente lo que consideramos puede ser el encuadre legal más detallado del ecosistema de Blockchain, el Reglamento del Parlamento Europeo sobre Criptoactivos.

La elección de esta normativa se basa en lo detallada que es cuestión de definiciones de desarrollos del ecosistema Blockchain, y el tratamiento que realiza de temas puntuales como las obligaciones de los emisores, negociadores de tokens, reservas que sustenten tokens (léase Stablecoins) y otros.

Como conclusión podemos pensar, que en el estado en que se encuentra el marco regulatorio de criptomonedas en nuestro país, se puede observar una clara disparidad de criterios, donde por ejemplo, la AFIP sale a dar una interpretación equiparando las monedas digitales a títulos valores, sin existir una clara definición legal. La acción del BCRA donde emite resoluciones que no se orientan a regular los criptoactivos, sino a alinear restricciones vinculadas al mercado de cambios.

Creemos en base a todo esto, que el problema de la normativa no se condice con un vacío legal, sino con lo que podríamos llamar un “limbo” legal, producido por interpretaciones de asemejar legalmente a los criptoactivos, con otros activos reglados legalmente.

De allí, lo importante que sería encarar en nuestro país, un marco normativo estructurado, ampliamente detallado, que brinde una clara conceptualización del tema, y el marco de obligaciones y derechos que generan esta nueva generación de activos digitales.

Territorialidad

Introducción

En el presente apartado ampliaremos el enfoque legal-impositivo de los cripto-activos, pero pondremos especial énfasis en la definición de conceptos vinculados al hecho imponible, fuente del impuesto, objeto y momento del mismo.

Nuestra finalidad será la de plantear las potenciales dificultades, incongruencias y “zonas grises” que se deben tener en cuenta, en el caso que la provincia de Santa Fe realice la gravabilidad de criptomonedas, o activos criptográficos generados (todos los instrumentos del ecosistema Blockchain). En especial, en los aspectos vinculados a territorialidad y residencia, temporalidad y anonimato de los diferentes actores.

Algunos aspectos previos a considerar

Antes de abordar de lleno la discusión sobre materia tributaria, creemos procedente plantear algunos aspectos vinculados a la “Economía del Sector Público” que se deberían considerar al evaluar la gravabilidad de cripto-activos, en general, y en especial si fuesen desarrollados en una plataforma Blockchain, generada por la provincia de Santa Fe.

Estos aspectos, vinculados a la estrategia y planificación estatal, así como también al análisis de ventajas y desventajas, fortalezas y riesgos inherentes a la decisión de impulsar el desarrollo de la plataforma Blockchain, serán abordados con más profundidad en informes posteriores al presente.

Sin embargo, consideramos que es procedente ir perfilando algunos de ellos en este momento, ya que en la definición de las funciones del Estado que veremos, se basará el criterio de gravabilidad o de eximición de sujetos y actividades alcanzados.

Existe una gran cantidad de bibliografía y trabajos elaborados en relación a la intervención del Estado como agente en la economía. Su conveniencia, grado de participación, ventajas y riesgos, son elementos relevantes al estudio en esta materia. Sin perjuicio de la diversidad de material disponible, nos centraremos en este trabajo, en la obra sobre Economía de Sector Público del premio Nobel de economía Josepth Stiglitz. Especialmente por lo abarcativo y contemporáneo de su trabajo.

La crisis financiera del 2008 y el nacimiento de la Blockchain

El 15 de agosto de 2.008, Lehman Brothers, el cuarto banco de inversión más grande de USA y uno de los más relevantes del mundo, se presentó en quiebra, siendo esto el detonante de la última gran crisis financiera mundial.

Para evitar el colapso del sistema financiero de Estados Unidos, el 3 de octubre de 2008, el Senado de dicho país aprobó la ley que permitía la compra de “bonos basura” (sub-prime) a bancos de ese país. El monto de ese rescate de esa ley ascendió a 700.000 millones de dólares. La intervención gubernamental en rescate de bancos, más grande realizada por USA.

Tres meses después, el 3 de enero de 2009, se sellaba el primer bloque de la Blockchain Bitcoin, es decir, comenzaba a funcionar la primera de las criptomonedas y la más utilizada hasta el día de hoy. Allí nace la promesa de las “finanzas descentralizadas”. Un sistema de intercambio de valores, de reservas e inversión, y gestión de pagos, invulnerable a ataques informáticos, totalmente descentralizado, vale decir, sin un dueño o grupo dominante, y sin regulación que se pueda ejercer sobre el mismo.

El correlato de fechas, y el hecho no trivial, de que los creadores del Bitcoin aún se mantengan en el anonimato (solo existe un seudónimo: Satoshi Nakamoto), nos lleva a pensar inexorablemente en una relación de causa-efectos, entre la crisis financiera que se gestaba y el nacimiento de las criptomonedas.

Pero este no será el punto en cuestión, en este momento. Si no, la relevancia del hecho de la intervención del estado para sostener al sistema financiero.

Entendemos, como es obvio, que las decisiones de regulación y participación del gobierno de Santa Fe, en relación a la decisión de crear y gestionar un plataforma de FT/NFT de Blockchain, no tendrán magnitud de comparación con la decisión que citamos referida al Senado de Estados Unidos. Sin embargo, nos llevan a plantear, que antes de considerar los aspectos puntuales impositivos de la decisión, se debe analizar la conveniencia o no de la intervención estatal en ese aspecto.

¿Debe el estado regular al ecosistema de la Blockchain ?

Tal como lo expresa Stiglitz:

“La primera iniciativa en Estados Unidos durante la administración de Carter redujo el papel del estado en la regulación de la economía. Por ejemplo, se dejó de regular los precios de las compañías aéreas y del transporte de larga distancia por carretera. Aunque se reconoce que la regulación tiene un coste, cada vez se es más consciente de que ***el hecho de no regular***

***puede tener incluso mayores costes**. La regulación ha continuado aumentando debido en parte al creciente reconocimiento de los fallos del mercado como los relacionados con el medio ambiente y **la estabilidad del sistema bancario**"*[46]

Como mencionamos previamente, la "promesa" de las finanzas descentralizadas se basaba en una tecnología desarrollada para eliminar la intermediación y la regulación en operaciones financieras. La Blockchain es en sí, un sistema orientado a generar lo que The Economist llamó "la máquina de confianza". Un sistema autónomo que no necesita instituciones de confianza (bancos, instituciones financieras) para poder atesorar o transferir valores. Con un registro único, altamente criptografiado, y redundantemente replicado en miles de servidores que aseguran que ninguno de ellos tengan el dominio del sistema, sino que este sea completamente autónomo, descentralizado y no regulado.

Si esto es contrapuesto a los sistemas de finanzas tradicionales, hará resaltar los altos costos de transacciones, las pesadas cargas burocráticas para acceder al crédito, a la gestión de activos financieros, e incluso el ilógico tiempo de demora y costos de realizar transferencias internacionales, entre otros.

Sin embargo, la gran cantidad de estafas, sistemas piramidales Ponzi, e incluso vulnerabilidades que se han encontrado en los sistemas de finanzas descentralizadas, en especial, en el ecosistema desarrollado por medio de contratos inteligentes, como capa superior en la Cadena de Bloques, ha llevado a nivel mundial, a replantear la necesidad de la intervención regulatoria de los Estados en esta materia.

En esta contraposición disyuntiva entre intervención, o no intervención de los gobiernos en el tema, podemos plantearnos cuáles serían los lineamientos que los diferentes estados deberían observar para poder realizar una eficiente participación regulatoria.

Veamos que plantea este autor, en referencia a las denominadas fallas del Estado:

"Aunque los fallos del mercado impulsaron a los países occidentales a adoptar los grandes programas públicos de los años treinta a los sesenta, en los setenta y en los ochenta las deficiencias de muchos de estos programas indujeron a los economistas y a los politólogos a investigar los fallos del estado ¿en qué condiciones no funciona bien el estado? Pueden extraerse consecuencias para la elaboración de futuros programas.

Son cuatro las causas principales de la incapacidad sistémica del Estado para cumplir los objetivos formulados: su escasa información, su reducido conocimiento de las respuestas

[46] Cortes, L. T., Rabasco, M. E., & Stiglitz, J. E. (2000). *La economía del sector público*. Antoni Bosch.- punto 1.1.5 El nuevo consenso.

privadas a sus intervenciones, su reducido control de la burocracia, y las limitaciones que imponen los procesos políticos.

Información limitada, muchas medidas tienen consecuencias complejas y difíciles de prever.

…

Control limitado de las empresas privadas. El estado no controla totalmente las consecuencias de sus intervenciones.

…

Control limitado de la burocracia. El parlamento aprueba las leyes, pero delega su ejecución en un organismo público. Este puede tardar mucho en redactar los reglamentos correspondientes cuyo contenido es fundamental para determinar las consecuencias de la legislación. En algunos casos los organismos públicos también son responsables de garantizar el cumplimiento de la normativa.

…

Limitaciones impuestas por los procesos políticos. Incluso aunque los Gobiernos estuvieran perfectamente informados de las consecuencias de todas las distintas medidas posibles, el proceso político a través del cual se toman las decisiones plantearía otras dificultades.

…

Los detractores de la intervención del Estado en la economía como el Premio Nobel Milton Friedman, muy conocido por su defensa del libre mercado mientras estaba en la Universidad de Chicago, creen que estas cuatro causas de los fallos del Estado son suficientemente importantes para que este se abstenga de intentar resolver las deficiencias supuestas o demostrables de los mercados. Sin embargo, la mayoría de los países han desarrollado procesos políticos - las normas y las reglamentaciones por las que se rige la democracia - que pueden mejorar los resultados del sector público y que mejoran al menos los problemas que plantean << los fallos del Estado >>".[47]

Entendemos, y por eso quisimos destacar este apartado, que dentro del modelo de evaluación sobre la conveniencia del desarrollo de una Plataforma NFT/FT para Santa Fe, que presentaremos al final de estos trabajos, no solo se deben considerar los factores fiscales y tecnológicos puntuales vinculados al ecosistema Blockchain. También consideramos relevante poseer una visión global, que encuadre el rol que el Estado se plantee dentro del ámbito cripto y su desarrollo.

Como muestran las tendencias a nivel global, y alineado con la lógica que impulsa esta tecnología disruptiva, es deseable que los Estados intervengan en una regulación que garantice, en especial, a pequeños ahorristas, la transparencia en las operaciones del ecosistema Blockchain en que actúen, así como las mínimas garantías de no licuación o pérdida de sus activos.

[47] Cortes, L. T., Rabasco, M. E., & Stiglitz, J. E. (2000). *La economía del sector público*. Antoni Bosch.- punto 8.1.4 los fallos de la intervención del estado.

En este punto, entendemos, y quisimos consignar en este trabajo, la reflexión realizada por Joseph Stiglitz sobre que la intervención del Estado en determinadas cuestiones, puede producir ruidos y distorsiones en los mercados, pero siempre se debe evaluar en forma contrafáctica, con respecto al perjuicio que produce la “no intervención”.

Este es, tal vez, el pilar básico de inicio de evaluación de conveniencia en el desarrollo de la Plataforma NFT/FT para Santa Fe, que pretendemos introducir.

Una vez hechas estas consideraciones en relación a la función del estado y las consecuencias de regulación / gravabilidad de actividades del ecosistema Bockchain, veamos más en detalle algunas consideraciones que se deben tomar en cuenta en referencia a elementos característicos de la tecnología de Cadena de Bloques, y como estos crean aspectos controversiales en materia tributaria.

El concepto de Impuesto

Hector Villegas (1984) citando a Valdés Costa brinda la siguiente definición de impuesto:

“Podemos definir al impuesto como << el tributo exigido por el Estado a quienes se hallan en las situaciones consideradas por la ley como hechos imponibles, siendo estos imponibles ajenos a toda actividad estatal relativa al obligado>>”.

Al decir que el tributo es exigido a quienes << se hallan en las situaciones consideradas por la ley como hechos imponibles >>, queremos significar que el hecho generador de la obligación de tributar está relacionado con la persona o bienes del obligado. La ley toma en consideración alguna circunstancia fáctica relativa a aquel. Este hecho elegido como generador no es un hecho cualquiera de la vida, sino que está caracterizado por su naturaleza reveladora, por lo menos, de la posibilidad de contribuir en alguna medida al sostenimiento del Estado. Si bien la valoración del legislador es discrecional debe ser idealmente en función de la potencialidad económica de cada uno es decir en función de la capacidad contributiva.”[48]

Dos aspectos que podemos destacar de esta definición son la mención de la posibilidad de contribuir al sostenimiento del Estado, y la capacidad contributiva del contribuyente. El primero en referencia al hecho elegido que será generador de la obligación tributaria. El segundo con referencia al límite del impuesto para que no se vuelva abusivo o confiscatorio.

[48] Villegas, H. B. (1984). *Ciencia de las finanzas y actividad financiera*. Ediciones Depalma - 7ma edición

Sin inconveniente con referencia a lo mencionado en el párrafo anterior, un aspecto clave que se deberá tomar en consideración al analizar la posibilidad de gravar los cripto-activos, es la utilización del impuesto como medio de aplicación de política económica. Eximiendo (o no gravando) del impuesto a actividades o activos criptográficos, con el ánimo de fomentar su utilización, o por el contrario, gravandolos para desalentar su desarrollo.

Los elementos básicos del impuesto

Según describe Dino Jarach (2001), los elementos fundamentales de la relación jurídica tributaria están dados por:

"los elementos de la relación jurídica tributaria sustancial son los siguientes: ***el sujeto activo****, titular de la prestación, es decir, del crédito tributario, en otras palabras el acreedor del tributo;* ***el sujeto pasivo*** *principal o deudor principal del tributo, a quién se puede dar el nombre de "contribuyente" y los* ***otros sujetos pasivos codeudores*** *o responsables del tributo por causa originaria (solidaridad, sustitución) o derivada (sucesión en la deuda tributaria);* ***el objeto*** *es decir la prestación pecuniaria, o sea el tributo;* ***el hecho jurídico tributario****, es decir, el presupuesto de hecho al cual la ley vincula el nacimiento de la relación tributaria"*[49]

En ese mismo sentido, el mismo autor, se encarga en destacar las cualidades del sujeto activo, que pueden hacer que el contribuyente quede vinculado con el hecho imponible:

"Domicilio, residencia, nacionalidad, sin embargo, además de ser cualidades personales del contribuyente que pueden ser importantes en la misma definición del hecho imponible, pueden servir también para vincular el hecho imponible al sujeto activo. Así, por ejemplo, el domicilio, residencia, o nacionalidad, son momentos de vinculación en el sentido de que una vez determinado el hecho imponible en su aspecto objetivo y en su atribución subjetiva al contribuyente, el domicilio o la nacionalidad de este indican la existencia de la conexión del hecho imponible con el sujeto activo, de la cual depende finalmente el nacimiento de la concreta pretensión tributaria".[50]

Y profundizando el concepto de momentos de vinculación objetivos o subjetivos del sujeto pasivo con el hecho imponible, Dino Jarach (2001), destaca la diferenciación del mismo con referencia a la territorialidad del impuesto:

"*Pueden ser momentos de vinculación la nacionalidad del contribuyente, su domicilio o residencia, la situación del objeto material del hecho imponible, o de la fuente de que este objeto (rédito, ganancia) procede, el lugar donde el hecho imponible se verifica, o donde*

[49] Dino, J. (2001). *El Hecho Imponible*. Abelado–Perrot, 3ª Edición, reimpresión, Buenos Aires
[50] Dino, J. (2001). Op. citada

produce sus efectos. El domicilio, la residencia, la nacionalidad son momentos de vinculación propios de los tributos personales; los otros son típicos de los tributos reales; sin embargo, como lo hemos dicho recién, los diferentes criterios pueden mezclarse entre ellos. De cualquier manera, hay que sentar el principio de que estos momentos de vinculación, sean subjetivos, sean objetivos, nada tienen que ver con la pretendida regla de la territorialidad de los tributos, a no ser que se conciba el principio de territorialidad de manera muy vaga, comprendiendo en él cualquier vínculo entre el hecho imponible y el sujeto activo."[51]

En resumen, deberíamos considerar en el análisis del impuesto, la nacionalidad, domicilio o residencia del contribuyente (criterio subjetivo), o de los bienes sobre los que el hecho imponible se verifica (criterio objetivo). Adicionalmente a esto, se deberá analizar la regla de territorialidad del tributo.

Veamos, entonces, algunas de las características particulares que imprime la tecnología de Blockchain, y que en este punto se deben tomar en consideración.

Territorialidad - La Blockchain como red distribuida

Uno de los fundamentos de la tecnología de Cadena de Bloques, es la de generar una red distribuida donde todos sus nodos, tienen igual peso.

Esto no es exactamente así. Antonopoulos, A. M. (2017) realizó una clasificación de los diferentes tipos de nodos (servidores) que se integran en una Blockchain, en este caso en la de Bitcoin. La imagen siguiente permite observar esto:

[51] Dino, J. (2001). Op. citada.

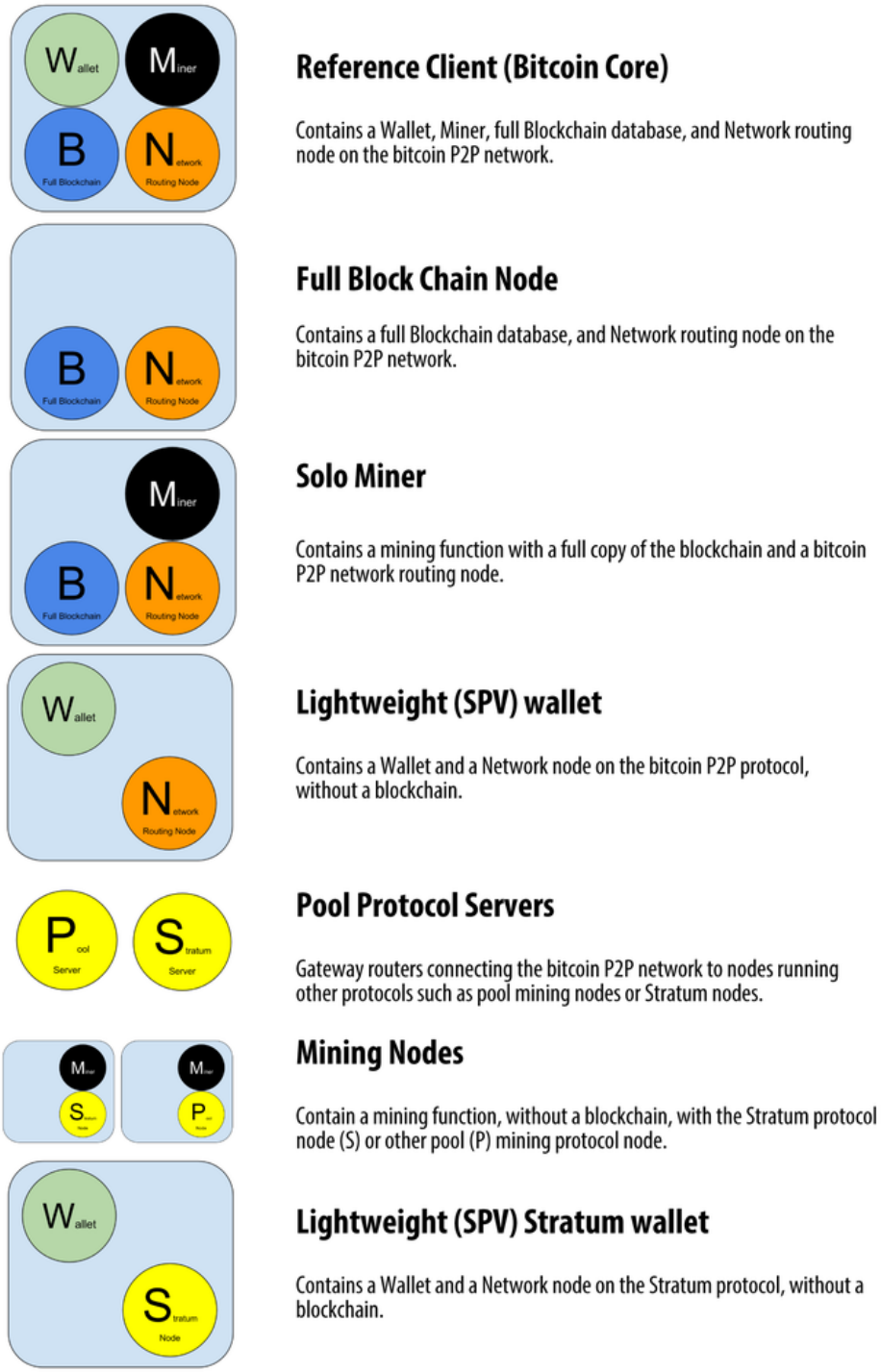


Figura 23 “ diferentes tipos de nodos, interactúan entre sí en la Cadena de Bloques”. Different types of nodes on the extended bitcoin network”. [52]

[52] Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the open blockchain*. " O'Reilly Media, Inc.".

Esos diferentes tipos de nodos, interactúan entre sí en la Cadena de Bloques, y por medio del protocolo propio de cada Blockchain, llegan a un acuerdo sobre la verificación y autenticidad de transacciones, y la sincronización del registro de las mismas por la red. Aún cuando, como menciona Antonopoulos, A. M. (2017), asumen roles dispares en la red.

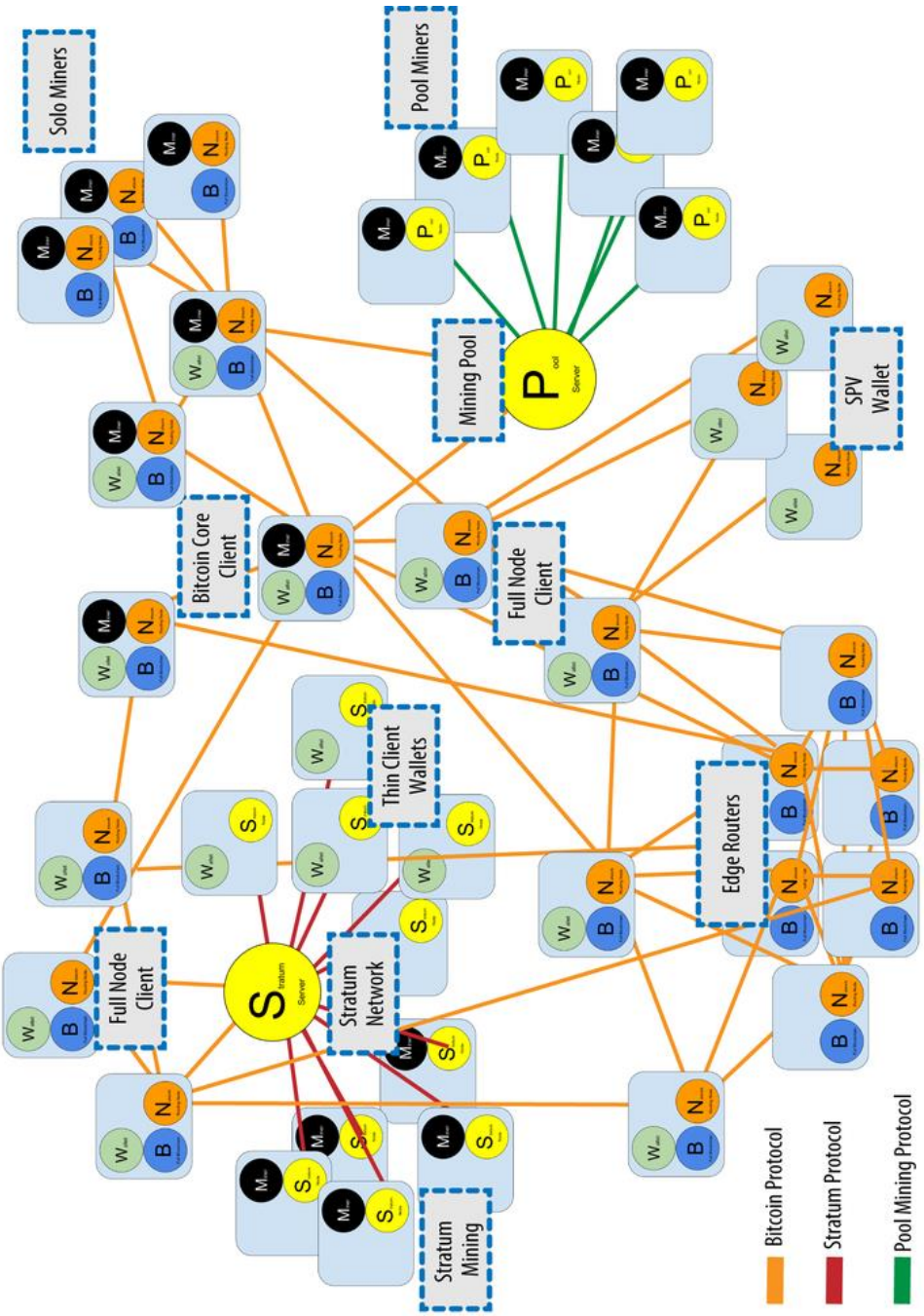


Figura 24 -La red bitcoin extendida que muestra varios tipos de nodos, puertas de enlace y protocolos (*Figure 8-3. The extended bitcoin network showing various node types, gateways, andprotocols*[53]

[53] Antonopoulos, A. M. (2017). *Op. citada*

)

Esta diferenciación, que tiene una finalidad más técnica que funcional, no actúa en detrimento del concepto primordial de la tecnología de Blockchain: una red distribuida de pares.

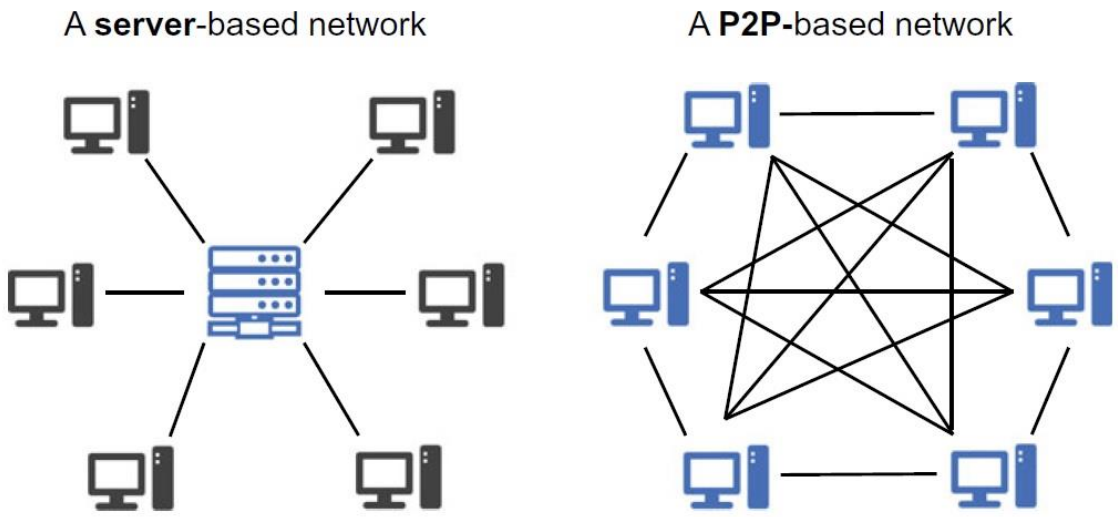


Fig. 1.7 Server-based versus P2P-based network

Figura 25 Diferencias entre una red centralizada (basada en un único servidor) y una red de pares

Hellwig, D., Karlic, G., & Huchzermeier, A. (2020). - diferencias entre una red centralizada (basada en un único servidor) y una red de pares[54]

Si bien, como observamos en la clasificación de nodos de Antonopoulos, A. M. (2017), los diferentes servidores que se conectan a la Blockchain, cumplen diferentes funciones, podemos afirmar que todos realizan las siguientes funciones elementales:

1. recibir transacciones
2. verificar las transacciones
3. registrar las transacciones
4. realizar la divulgación de esas transacciones (las reenvían a otros servidores)
5. realizar este mismo proceso con los bloques generados por los mineros.

Es en el punto 4) de estas actividades, es donde el nodo produce la divulgación de las transacciones, generando un efecto multiplicador en cascada, por el cual en pocos segundos

[54] Hellwig, D., Karlic, G., & Huchzermeier, A. (2020). *Build your own blockchain*. Springer International Publishing.

una transacción validada queda registrada en la Cadena de Bloques, esperando que los mineros la incorporen en forma definitiva por medio de un bloque. Este proceso es conocido en los protocolos de Blockchain como “broadcasting” (la traducción literal sería “radiodifusión” pero hace referencia a la “difusión” de la transacción dentro de la Cadena de Bloques).

¿Cúal es la idea subyacente de la Blockchain, para adoptar esta dinámica y arquitectura de red distribuida de pares ? Elementalmente lo que la Cadena de Bloques busca es la validación y registración redundante de transacciones, de manera que ante un ataque informático, que intente modificar o borrar transacciones, quienes lo busquen, enfrente la imposibilidad de tener que hackear simultáneamente una masiva cantidad de servidores conectados a la red. Junto con el procedimiento criptográfico que posteriormente realizarán los mineros, esta dinámica de la Blockchain le da su principal cualidad como tecnología: la invulnerabilidad.

Analicemos las incidencias de esta dinámica pilar de la Blockchain, en referencia a la territorialidad impositiva.

La territorialidad en una red distribuida de pares.

Mencionamos anteriormente el proceso que se denomina “broadcasting”, dentro del lenguaje propio de la Blockchain. Para realizar este proceso, cada nodo que recibe una transacción la valida, registra y luego envía a 4 o 5 nodos, para que estos realicen lo mismo.

Evidentemente existe un paso previo a esto, y es la generación de la transacción.

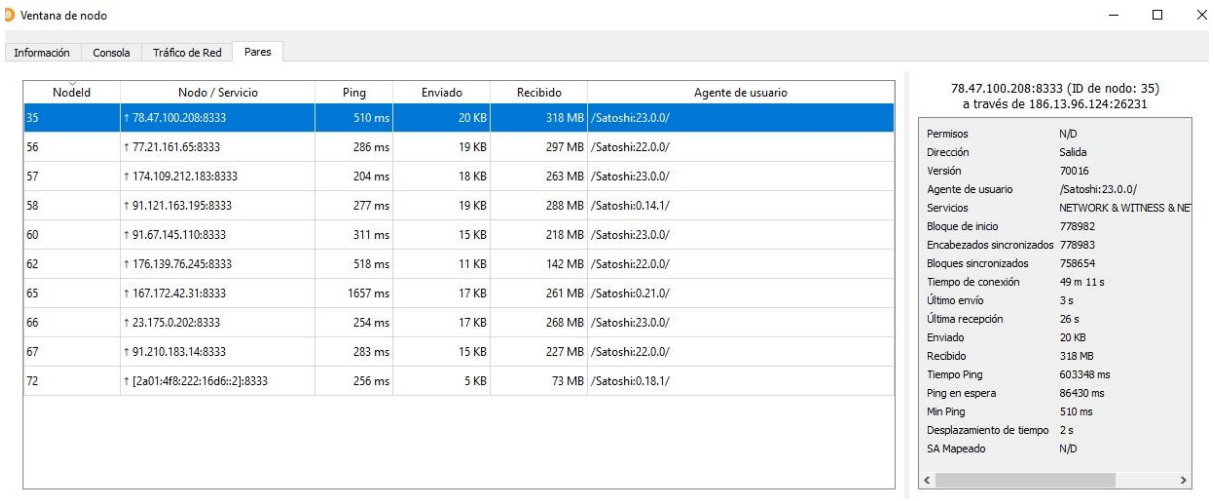
La transacción es algo tan simple como un asiento contable de doble entrada donde se identifica la cuenta/s de origen, la cuenta/s de destino, la cantidad de criptomonedas, y la diferencia entre ambas, que es el fee (comisión) que se le pagará al minero. La billetera se va a encargar de firmar digitalmente esa transacción con la clave privada de la cuenta de origen, y de esta manera permite a los nodos la validación de la misma.

¿ Cómo se genera la transacción ? En la mayoría de los casos, el instrumento que utilizamos para realizar la transacción es una billetera de criptomonedas. Previamente se realizó una descripción de los distintos tipos de billeteras (web, app, de escritorio, papel, hardware).

Pero lo que nos interesa en función de analizar la territorialidad del hecho imponible, es saber cómo envía nuestra billetera la transacción a la Blockchain, para saber si por este medio se puede llegar a identificar la localización geográfica de donde se originó la transacción, o la pertenencia de la misma.

El software que corre la billetera de criptomonedas realiza un proceso semejante al de broadcasting de cada nodo de la Blockchain. El protocolo de la blockchain le permite a la billetera, “descubrir” nodos para poder enviarles las transacciones que prepara. Una vez descubiertos, la billetera suele crear una lista de nodos de confianza, con los cuales va a trabajar. Esa lista es dinámica y de acuerdo al grado de seguridad con que trabaja la billetera suele ir renovándose.

En la imagen siguiente se pueden ver los nodos descubiertos en la blockchain Bitcoin, por la billetera de criptomonedas que instala el software Bitcoin Core (versión original del software de Bitcoin).



Nodeld	Nodo / Servicio	Ping	Enviado	Recibido	Agente de usuario
35	↑ 78.47.100.208:8333	510 ms	20 KB	318 MB	/Satoshi:23.0.0/
56	↑ 77.21.161.65:8333	286 ms	19 KB	297 MB	/Satoshi:22.0.0/
57	↑ 174.109.212.183:8333	204 ms	18 KB	263 MB	/Satoshi:23.0.0/
58	↑ 91.121.163.195:8333	277 ms	19 KB	288 MB	/Satoshi:0.14.1/
60	↑ 91.67.145.110:8333	311 ms	15 KB	218 MB	/Satoshi:23.0.0/
62	↑ 176.139.76.245:8333	518 ms	11 KB	142 MB	/Satoshi:22.0.0/
65	↑ 167.172.42.31:8333	1657 ms	17 KB	261 MB	/Satoshi:0.21.0/
66	↑ 23.175.0.202:8333	254 ms	17 KB	268 MB	/Satoshi:23.0.0/
67	↑ 91.210.183.14:8333	283 ms	15 KB	227 MB	/Satoshi:22.0.0/
72	↑ [2a01:4f8:222:16d6::2]:8333	256 ms	5 KB	73 MB	/Satoshi:0.18.1/

Permisos	N/D
Dirección	Salida
Versión	70016
Agente de usuario	/Satoshi:23.0.0/
Servicios	NETWORK & WITNESS & NE
Bloque de inicio	778982
Encabezados sincronizados	778983
Bloques sincronizados	758654
Tiempo de conexión	49 m 11 s
Último envío	3 s
Última recepción	26 s
Enviado	20 KB
Recibido	318 MB
Tiempo Ping	603348 ms
Ping en espera	86430 ms
Min Ping	510 ms
Desplazamiento de tiempo	2 s
SA Mapeado	N/D

Figura 26 Nodos descubiertos en la blockchain Bitcoin, por la billetera de criptomonedas que instala el software Bitcoin Core

Un procedimiento semejante al mencionado anteriormente realizan los nodos de la Blockchain. Cada nodo posee una lista de nodos de confianza que fue “descubriendo” por medio del protocolo de la Blockchain, a los cuales les va a re-enviar las transacciones que valida y que recibió de una billetera o de otros nodos. Sin embargo, esta lista nunca es fija. Es dinámica y está cambiando constantemente. Entre otras razones, porque muchos de los nodos de la red están disponibles intermitentemente.

Otras de las razones, por las cuales las billeteras de criptomonedas y los nodos de las redes Blockchain, cambian constantemente su lista de nodos de preferencia, es para evitar dos ataques de hackeo: eclipse attack y sybil attack, los cuales se basan en hackear a los nodos de preferencia para que el servidor o la billetera interactúen con la imagen de una blockchain apócrifa.

Para tomar dimensión de la intermitencia y volatilidad de la cantidad de nodos que conforman la Blockchain, tomemos en cuenta que descargando el software Bitcoin core (se muestra imagen), una aplicación de 17 Mb, fácilmente se puede configurar en cualquier computadora

con conexión a Internet, un nuevo nodo de la red. Cada vez que se haga correr ese programa, la computadora pasará a actuar como un nodo más de la red. Consiguientemente, cuando se cierre el programa o se desconecte la computadora, este nodo se apagará[55].

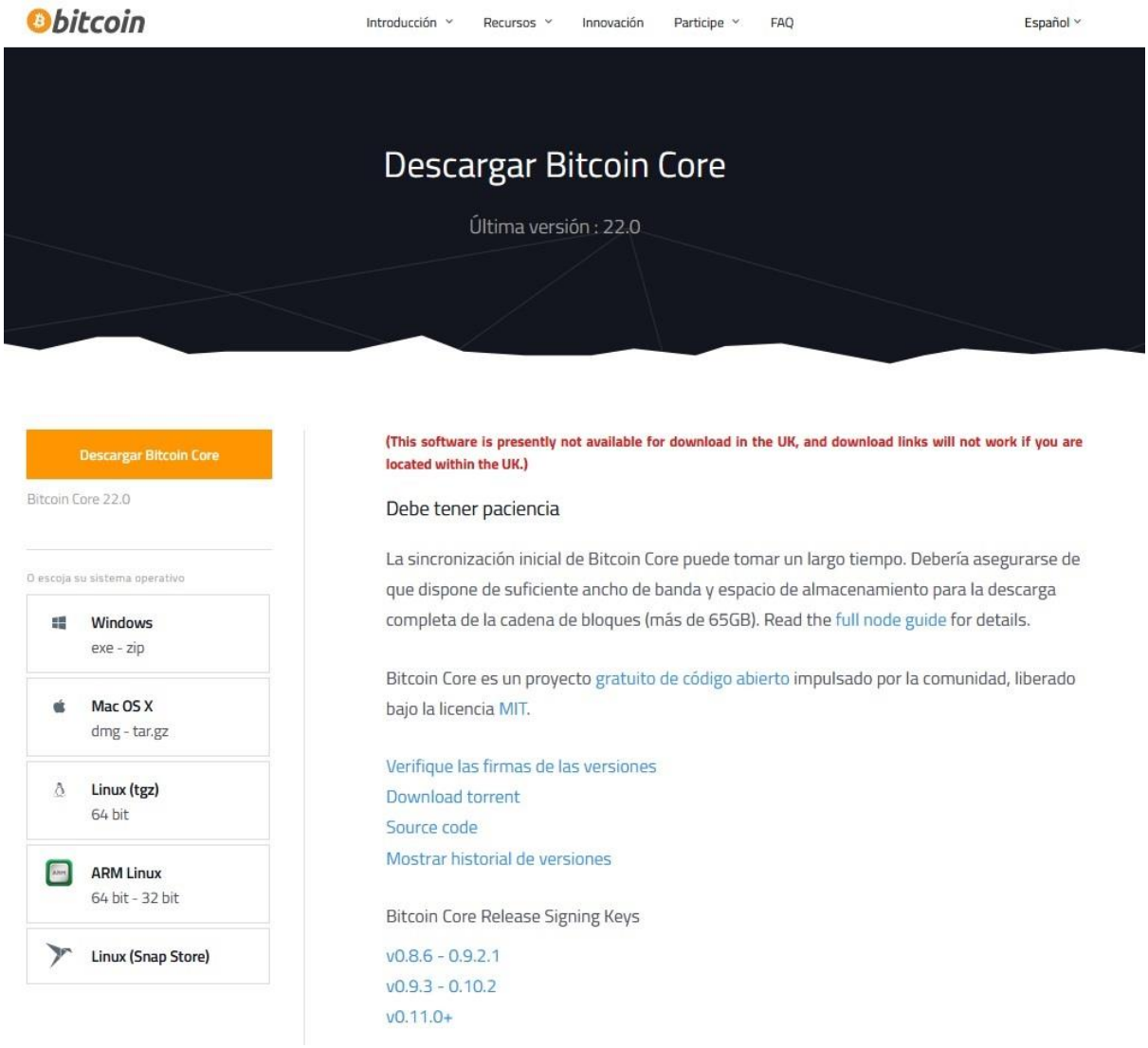


Figura 27 página de descarga de Bitcoin Core - https://bitcoin.org/es/descargar

Lo más importante, en este tema, es que una vez que la billetera de criptos, o el nodo de la red, realizó el broadcasting, no almacena la información de los nodos a los que re-envio la transacción.

En conclusión, por la dinámica con que funciona la Cadena de Bloques, se hace prácticamente imposible identificar la billetera de criptomonedas, y el nodo que primero recibió una transacción. De esto deriva una imposibilidad técnica de identificar, por medio de

[55] Sin perjuicio de estos nodos intermitentes, que se conectan y desconectan de la blockchain, Antonopoulos, estimó que en 2019 la blockchain de Bitcoin poseía un aproximado de 12.000 servidores estables, que se mantienen siempre funcionando.

la información de la Blockchain la territorialidad (localización geográfica) de una transacción determinada. Queda, por lo tanto, para los Estados (nacionales o provinciales) que graven territorialmente a las operaciones que se realizan en determinada Blockchain, solamente la posibilidad de vincular a los sujetos pasivos con el hecho imponible, por medio de la exteriorización de la operación.

En esto juega un rol decisivo, en este caso, la identificación y regulación de los Exchanges de criptomonedas (Casas de Cambio), o el rastreo de transferencias bancarias, o del pago en efectivo de operaciones P2P (persona a persona).

La territorialidad en las Blockchain permisionadas

Previamente ya realizamos una descripción de la clasificación básica de tipos de blockchain actuales. Se suele categorizar a las Cadenas de Bloques en:

- no permisionadas o públicas
- permisionadas o privadas
- de consorcio
- híbridas

La primera Blockchain conocida fue la de Bitcoin, una blockchain no permisionada / abierta que utiliza la mecánica que describimos anteriormente. Como era de esperar, la pretensión lógica que guió a reguladores, corporaciones, y grandes organizaciones, fue la de poder utilizar los beneficios propios de la Blockchain, en aspectos de invulnerabilidad y seguridad, pero combinados con la posibilidad de identificar a los actores que realizan transacciones en la misma.

Esta motivación llevó a adaptar el código fuente de las Blockchain o permisionadas, pero realizando modificaciones al mismo que aseguren una gobernanza de actores y permisos concedidos a diferentes usuarios. Este fue el origen de las Blockchain privadas o permisionadas.

Existen muchos tipos de estas Blockchain, y basándonos en los requerimientos que defina cada organización, la modificación del código fuente original, o la configuración de parámetros que se permita a la Blockchain privada, ha generado un amplio abanico de posibilidades que hace muy difícil de caracterizar en forma única a este tipo de Cadenas de Bloques.

En general, las Blockchain privadas reconocen dos categorías de nodos:

- los nodos “selladores”: que realizan el mismo proceso, de recibir, validar, registrar y difundir transacciones
- los nodos “administradores”: que son los que poseen permisos especiales y permiten la habilitación y funcionamiento de nodos selladores

Por este motivo, y en función de las modificaciones que se realicen al código fuente de la Blockchain original, las Blockchain permisionadas o privadas, permiten identificar a los usuarios que hacen uso de la misma, ya que estos deben acreditarse ante los nodos administradores para poder comenzar a trabajar en la Cadena de Bloques.

Algunas Blockchain privadas, que tomaron el código fuente original de Blockchain públicas, lo modificaron, y generaron nuevas Blockchain configurables, facilitan la tarea de adopción e incorporación de infraestructura BCT a soluciones de requerimientos de uso definidos. En este grupo podemos mencionar, entre otras a Hyperledger (Compose y Fabric, especialmente), que es regenteada por una comunidad en la que participan IBM y Linux Red Hat; o Quorum, una modificación parametrizable de la Blockchain Ethereum, que fue desarrollada originalmente por J.P. Morgan, y actualmente adquirida por la firma Consensys.

Los desarrollos que mencionamos en esta parte, son utilizados en la mayoría de los casos, por empresas, organizaciones y actores que requieren aplicar políticas y procedimientos de KYC - Know Your Client (conozca a su cliente).

Se deriva de esto, que al crearse el “file” del cliente, como requisito para que los nodos administradores admitan a quien va a trabajar sobre la Blockchain, la identidad y domicilio del mismo es detectable en este tipo de Cadenas de Bloques.

Blockchain de consorcio

Tal como lo definió Vitalik Buterin, el principal creador de la Blockchain Ethereum:

“*Una Blockchain de consorcio es una cadena de bloques en la que el proceso de consenso está controlado por un conjunto de nodos preseleccionados; por ejemplo, uno podría imaginar un consorcio de 15 instituciones financieras, cada una de las cuales opera un nodo y de las cuales 10 deben firmar cada bloque para que el bloque sea válido. El derecho a leer la cadena de bloques puede ser público, o restringido a los participantes, y también existen paths híbridas como que los hashes raíces de los bloques sean públicos junto con una API que permite a los miembros del público realizar un número limitado de consultas y recuperar*

pruebas criptográficas de algunas partes del estado de la cadena de bloques. Estas cadenas de bloques pueden considerarse <<parcialmente descentralizadas>> ”.[56]

El ejemplo expuesto por Vitalik, es uno de los más representativos de las Blockchain de Consorcio. Un grupo de bancos podría acordar utilizar una Blockchain de Consorcio, como interfaz común para realizar operaciones, como las transferencias internacionales. En este caso cada banco dispondría de un nodo administrador. A eso se refiere Vitalik cuando las caracteriza como “parcialmente” descentralizadas. Los clientes de cada banco, conseguirían su autorización para acceder la Blockchain, a partir del nodo administrador de su banco. Todos los nodos administradores, y selladores deberán someterse a las reglas previamente definidas en la Blockchain de consorcio, para poder realizar sus operaciones.

Un ejemplo de esto fue la prueba de concepto desarrollada por Bancos brasileños y europeos para realizar transferencias internacionales instantáneas, sobre la Blockchain de Consorcio, configurada como tal, de Corda R3. [57]

Desde el punto de vista del análisis que estamos realizando, en función de la posible detección de localización geográfica de los usuarios de la Blockchain, las Blockchain de Consorcio seguirán la misma lógica que las Blockchain permisionadas, en especial, por ser una variante de estas primeras.

El hecho imponible

Belisario Villegas, H. (2002) define al hecho imponible como "el acto, conjunto de actos, situación actividad o acontecimiento que, una vez sucedido en la realidad, origina el nacimiento de la obligación tributaria y tipifica el tributo que será objeto de la pretensión fiscal"[58].

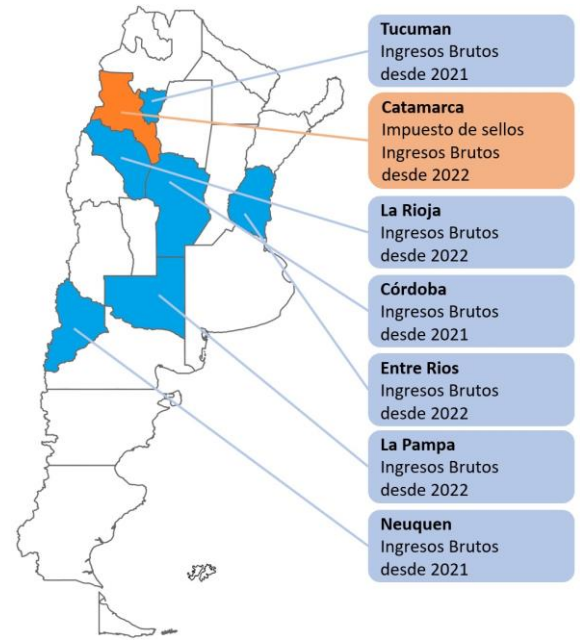
Lo primero que debemos destacar en el análisis que vamos a realizar en referencia al Hecho Imponible es que podemos hablar, de la gravabilidad a nivel provincial, por medio de dos impuestos distintos. Ingresos Brutos e Impuesto de Sellos.

---

[56] Vitalik Buterin - 07 de agosto 2015 - Ethereum Foundation - On Public and Private Blockchains https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains
Observado - febrero 2023

[57] Bnamericas - Cadena de bloques estimularía transferencias de dinero en tiempo real en la región https://www.bnamericas.com/es/noticias/cadena-de-bloques-estimularia-transferencias-de-dinero-en-tiempo-real-en-la-region1
Observado - febrero 2023

[58] Belisario Villegas, H. (2002). Curso de finanzas, derecho financiero y tributario. *Buenos Aires, Argentina: Editorial Astrea*.



En el gráfico siguiente se puede observar las provincias argentinas, que a este momento (febrero 2023) han decidido gravar cripto-activos, con impuesto sobre los Ingresos Brutos, y con impuesto de sellos.

Como se puede observar la única provincia que hasta el momento ha gravado operaciones con cripto-activos con Impuesto de Sellos, es la provincia de Catamarca, la cual también grava la compraventa de monedas digitales, también con el Impuesto sobre los Ingresos Brutos respectivo.

Figura 28 Provincias argentinas, que a febrero 2023 han decidido gravar cripto-activos, con impuesto sobre los Ingresos Brutos, y con impuesto de sellos

El otro aspecto, que se vincula directamente, con la introducción que hacemos en este trabajo en referencia al rol del Estado, es la posibilidad de utilizar la política fiscal para generar incentivos en el uso de cripto-activos por medio de exenciones impositivas, es decir, lo contrario a gravar la actividad vinculada a cripto-activos, en el caso que esta sea la decisión. Este punto en particular será abordado con la profundidad necesaria en los trabajos finales, cuando se plantee las consideraciones sugeridas a realizar para la evaluación final de ventajas y riesgos del desarrollo de una Plataforma NFT/FT para Santa Fe.

En referencia a lo que los códigos fiscales, y leyes impositivas anuales de las provincias, en lo que respecta a la tipificación del Hecho Imponible en cuestión, podemos destacar:

Córdoba:

"Art. 22: Los ingresos derivados de las actividades incluidas en los Códigos de Actividades que se detallan a continuación ….

Código: 620900

La prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente, con operatorias relacionadas con monedas digitales *(inciso j) del artículo 202 del Código Tributario."*

Mera Compra. Frutos del País. Fabricantes en Extraña Jurisdicción.

Artículo 202.- Se considerarán también actividades alcanzadas por este impuesto las siguientes operaciones, realizadas dentro de la Provincia:

…

j) La prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente con operatorias relacionadas con monedas digitales.

"Art. 24: Los ingresos provenientes de los servicios financieros, intermediación financiera y otros servicios que se detallan a continuación, efectuados por los sujetos que para cada caso se indica, cuyos Códigos de Actividad se describen en el Anexo I de la presente Ley, deben tributar …"

*"punto 12.- **Los servicios destinados a facilitar la gestión y/o intercambio de monedas digitales** por monedas fiduciarias de curso legal, otras criptomonedas o cualquier tipo de bienes -y viceversa-, a través de plataformas online, sitios web, **aplicaciones tecnológicas, dispositivos y/o plataformas digitales y/o móviles o similares** (exchanges de criptomonedas).*

Como es observable (véase el destacado en negrita), se está gravando con el impuesto a los "servicios" que se prestan para facilitar la gestión y/o intercambio de monedas digitales. La normativa hace clara referencia a quienes cobran una comisión por juntar a las partes en operaciones "calzadas" de compra-venta de criptomonedas, como también cualquier otro servicio que se brinde en estas situaciones como podría ser la disponibilidad de precio vigente en mercado (recuérdese que las criptomonedas públicas no poseen un "precio oficial" observable, sino que se manejan por un promedio que las plataformas realizan, de los precios que grandes operadores están realizando).

Quisimos destacar la mención a "plataformas digitales y/o móviles o similares", para plantearnos si esto alcanzaría a las operaciones denominadas peer-to-peer, en las que utilice una billetera criptográfica. Si este dispositivo (la billetera) se encuadraría en la mención genérica del artículo cuando establece el término "similares".

En ese aspecto el artículo 222 del CTP hecha luz:

punto 13.- Compra y venta de monedas digitales conforme inciso b) del artículo 222 del Código Tributario Provincial"

*"Código Tributario Provincial - Artículo 222: **La base imponible estará constituida por la diferencia entre los precios de venta y de compra**, excluidos tanto el débito como el crédito fiscal del Impuesto al Valor Agregado facturados, en los siguientes casos:*

…

b) Operaciones de compra y venta de divisas … Asimismo, quedan incluidos en el presente inciso las operaciones de compra y venta de monedas digitales realizada ***por sujetos que fueran habitualistas en tales operaciones****;"*

Agrega a lo normado por el artículo 222 (analizado anteriormente), a las operaciones de quienes, sin utilizar plataformas digitales o aplicativos móviles, hicieran uso habitual de operaciones de compra-venta de monedas digitales.

De esta manera, podemos destacar, que en la normativa de la provincia de Córdoba, no solo se alcanza a la actividad de plataformas digitales, aplicativos móviles, quienes acerquen oferta-demanda (Exchanges), sino que también, se incorpora al impuesto un presupuesto subjetivo, de quienes realicen en forma habitual este tipo de operaciones.

Quedarían excluidos del gravamen, los no habitualistas, que realicen ventas o compras en operaciones peer-to-peer.

Catamarca:

Impuesto de Sellos:

"ARTÍCULO 19°.- Por los actos, contratos y operaciones que a continuación se enumeran deberá pagarse el impuesto que en cada caso se establece:

21.- Contratos vinculados al comercio de activos digitales, criptomonedas, Bitcoin y similares, por la suma total del capital invertido y sus rendimientos."

Al hablar en forma genérica de "contratos vinculados", entendemos que incluiría las operaciones de compra de criptomonedas por medio de Exchanges, o en Plataformas Digitales. Y en ese caso, se aplicarían todas las consideraciones que realizamos previamente acerca de la territorialidad y su dificultad de determinación para cripto-activos públicos.

Otra consideración procedente, es que por lo textual del artículo, en dicha provincia, estarían alcanzadas por este impuesto las operaciones de staking. Las operaciones de staking de criptomonedas alcanzaron un amplio auge reciente, al cambiar la red Ethereum su protocolo de consenso. Al comenzar esta Cadena de Bloques a utilizar el consenso POS - Proof Of Stake (Prueba de participación), se expandió el negocio de las plataformas que por medio de contratos inteligentes, permiten invertir en la composición de un stake (participación), bloqueando una cantidad de Ethers que se transfieren al contrato. Luego de un periodo de

tiempo, pre-pactado, el contrato libera esos Ethers, y paga a quien los depositó un beneficio porcentual sobre la ganancia obtenida en las tareas de mineración, que realizó el stake.

Al mencionar el artículo “capital invertido y sus rendimientos”, entendemos que claramente incluye a este tipo de operaciones, habitual en el mercado cripto, que hemos mencionado.

Impuesto sobre los Ingresos Brutos

“ARTÍCULO 12°.- Incorpórase como inciso j) del Artículo 161 de la Ley 5.022 y sus modificaciones, el siguiente:

«j) La prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente con operatorias relacionadas con activos digitales.»

Y en lo referido en particular a la determinación de la base imponible, amplia diciendo:

“ARTÍCULO 11°.- Sustitúyese el Artículo 7 de la Ley 5.022 y sus modificaciones, por el siguiente:

«ARTÍCULO 7.- En los actos, operaciones y transacciones que se realicen en especie -incluido los activos digitales- y que configuren el hecho generador de tributos, a los efectos de la determinación de la base imponible se considerará el valor corriente en plaza vigente al momento de producirse el hecho imponible o en su defecto el que surja de procedimiento autorizado por la Dirección General de Rentas.

Se entiende como activos digitales a aquellos activos intangibles -tales como las monedas digitales, moneda virtual, criptomonedas, criptoactivos, tokens, stablecoins, etc- que por su naturaleza y/o características constituyan y/o impliquen una representación digital de valor que puede ser objeto susceptible de comercio digital y cuyas funciones – directas y/o indirectas- son la de constituir un medio de intercambio y/o una unidad de cuenta y/o una

reserva de valor.»”

Entendemos que no hace una mención específica, como la normativa de la provincia de Córdoba, a la inclusión de los habitualistas en las operaciones peer-to-peer. Sí, lo hace claramente en la consideración de “servicios de cualquier naturaleza” vinculados a operaciones con activos digitales.

Hace una enunciación más clara y taxativa de lo que se considera “activos digitales”. A nuestro entender, no tiene relevancia la caracterización de “moneda” en orden a su función de representación de valor, unidad de cuenta, y medio de intercambio. En tanto que cualquiera de los instrumentos mencionados previamente, cumple alguna de esas funciones (al conectar sus funciones por medio de “y/o” deja abierta la inclusión, al cumplir cualquiera de las condiciones).

Entre Ríos - Impuesto sobre los Ingresos Brutos

"ARTICULO 158º.- La base imponible estará constituida por la diferencia entre los precios de compra y venta, en los siguientes casos:

…

f) En las operaciones de enajenación de acciones, valores representativos y certificados de depósitos de acciones y demás valores, cuotas y participaciones sociales –incluidas cuotas partes de fondos comunes de inversión y certificados de participación de fideicomisos financieros y cualquier otro derecho sobre fideicomisos y contratos similares-, ***monedas digitales****, títulos, bonos y demás valores, los ingresos gravados se determinarán deduciendo del precio de transferencia el costo de adquisición que corresponda considerar para la determinación del resultado establecido para este tipo de operaciones en el Impuesto a las Ganancias. A tales fines se considerará, sin admitir prueba en contrario, que los bienes enajenados corresponden a las adquisiciones más antiguas de su misma especie y calidad;*

…"

El texto normativo no da un tratamiento especial, ni hace un destacado sobre las monedas digitales que grava, sino que se limita a incluirlas dentro de otra definición de operaciones que se realizan con determinados activos. Incluso la definición de utilización del Impuesto a la Ganancias, como fuente supletoria, para calcular el costo de adquisición de estos activos, sugiere una intención de alinear el cuerpo normativo provincial al nacional.

La Pampa - Impuesto sobre los Ingresos Brutos

"Artículo 52.- Incorpórase como inciso l) del artículo 183 del Código Fiscal (t.o. 2018) el siguiente:

"l) La prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente con operatorias relacionadas con monedas digitales (monedas virtuales, criptomonedas, criptoactivos, tokens, stablecoins y demás conceptos que por su naturaleza y/o características constituyan y/o impliquen una representación digital de valor que puede ser objeto susceptible de comercio).".

Al igual que las normativas previas, hace mención directa y grava a los servicios de "cualquier naturaleza", "directa o indirectamente" con operaciones de monedas digitales. Aquí está incluyendo, como ya mencionamos anteriormente, a los servicios de acercamiento de oferta-demanda y otros servicios brindados por Plataformas y Aplicaciones digitales.

"Artículo 53 .- Sustitúyase el inciso c) del artículo 192 del Código Fiscal (t.o. 2018) por el siguiente:

“c) las operaciones de compra-venta de divisas o monedas digitales (monedas virtuales, criptomonedas, criptoactivos, tokens, stablecoins y demás conceptos que por su naturaleza y/o características constituyan y/o impliquen una representación digital de valor que puede ser objeto susceptible de comercio).””

En este punto se agrega a las operaciones de compra-venta de monedas digitales. No se hace mención de si son realizadas por medio de Plataformas/Aplicativos, ni se considera la habitualidad de quien las realiza, por lo que entendemos que genéricamente es una definición ampliamente abarcativa.

La Rioja - Impuesto sobre los Ingresos Brutos

ARTÍCULO 125º.- Incorpórese como inciso g) del Artículo 162º del Código Tributario (Ley Nº 6.402 y modificatorias) el siguiente texto:

g) La prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente con operatorias relacionadas con monedas digitales”.

ARTÍCULO 131º.- Incorpórese como inciso f) del Artículo 171° del Código Tributario Provincial (Ley N° 6.402 y modificatorias) el siguiente texto:

“f).- Operaciones de compra y venta de ***monedas digitales*** *realizadas por sujetos que fueran habitualistas en tales operaciones”.*

Incluye dentro del impuesto a los servicios de “cualquier naturaleza”, vinculados “directa o indirectamente”con operatorias de monedas digitales. Al igual que en las legislaciones anteriores, grava en forma ampliamente abarcativa a los servicios brindados por Plataformas/ Aplicaciones.

En el caso de las operaciones realizadas por particulares, en forma concordante con lo establecido por la provincia de Córdoba, agrega el supuesto subjetivo de la habitualidad de quien realice las operaciones de compra-venta de monedas digitales.

Neuquén - Impuesto sobre los Ingresos Brutos

“Artículo 182 bis: Se consideran servicios digitales, cualquiera sea el dispositivo utilizado para su descarga, visualización o utilización, aquellos llevados a cabo a través de la red internet o de cualquier adaptación o aplicación de los protocolos, plataformas o de la tecnología utilizada por internet u otra red a través de la que se presten servicios equivalentes que, por su naturaleza, estén básicamente automatizados y requieran una intervención humana mínima, comprendiendo, entre otros, los siguientes:

…

o) La prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente con operatorias relacionadas con monedas digitales. Se entiende por moneda digital a los fines de la presente ley: moneda virtual, criptomonedas, criptoactivos, tokens, stablecoins y demás

conceptos que por su naturaleza y/o características constituyan y/o impliquen una representación digital de valor que puede ser objeto susceptible de comercio digital y cuyas funciones —directas y/o indirectas— son las de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor. (modificado por Ley 33103 B.O.3992 07/01/2022)"

Entendemos que el artículo 182 bis citado, hace una descripción demasiado extensiva, al referenciar a servicios digitales. Menciona la independencia de cual sea el dispositivo, y la generalidad de ser hechos en la red Internet, … "u otra red" (en la actualidad no se conoce ninguna otra red diferente a Internet sobre la que se despliegue una Blockchain. Ni siquiera en el caso de Blockchain privadas, se utilizan, como infraestructura de base, redes diferentes a Internet).

Queremos destacar esta amplitud de definición que dá el artículo, ya que de su lectura estricta, se puede considerar que las billeteras digitales, en el caso de las operaciones de particulares, en característica peer-to-peer y no habitual, quedarían alcanzados por ser un "servicio digital".

Tucumán - Impuesto sobre los Ingresos Brutos

Sustituir el inciso 3. del Artículo 223, por el siguiente:

La base imponible estará constituida por diferencia entre los precios de compra y de venta en los siguientes casos:

…

«3. Operaciones de compra y venta de divisas y títulos públicos. Quedan

comprendidos en el presente inciso las operaciones de compra y venta de monedas digitales.»

Entendemos, que al igual de lo que analizamos en el caso de la provincia de Entre Ríos, se realiza una incorporación de las operaciones de compra-venta de monedas digitales, a una tipificación previa (la de divisas y títulos públicos). Podemos destacar, que no se menciona, como sí lo vimos en otras provincias, a los servicios prestados por plataformas y aplicaciones digitales.

El anonimato en la Blockchain

Tal como analizamos previamente las Blockchain privadas, o de consorcio, pueden ser configuradas para que sus nodos administradores sean los que aprueben el acceso de nuevos usuarios, así como para determinar cuáles operaciones se podrán hacer sobre la misma.

Esto no ocurre en las Blockchain públicas (no permisionadas) como Bitcoin, Ethereum, y otras. Los usuarios en estas redes sólo son reconocidos por las claves públicas de sus billeteras digitales. Esta clave pública se encuentra vinculada por un algoritmo criptográfico con una clave privada, que la billetera guarda en absoluta confidencialidad, ya que esta segunda clave es la que se utiliza para firmar transacciones, y por lo tanto, quien la tiene detenta la propiedad de la totalidad de las criptomonedas vinculadas a la misma.

Podemos hacer una comparación diciendo que las claves públicas de la Blockchain, actuarían como algo similar a una CBU (Clave Bancaria Uniforme) que nos permite identificar la cuenta a la que transferimos criptomonedas, o nuestra clave, para recibir estas.

La diferenciación sustancial, de la Blockchain, con este ejemplo, es que las CBUs son nominadas y permiten la identificación del titular de la cuenta, mientras que en la Blockchain lo único que se va a registrar es la clave pública que va a recibir, o enviar, criptomonedas. Ningún dato identificatorio del usuario queda registrado.

La imagen siguiente muestra una transacción de cuenta a cuenta en la Blockchain de Bitcoin. Se destacó, en la parte inferior la clave pública de la cuenta de origen (a la izquierda) y la clave pública de la cuenta de destino.

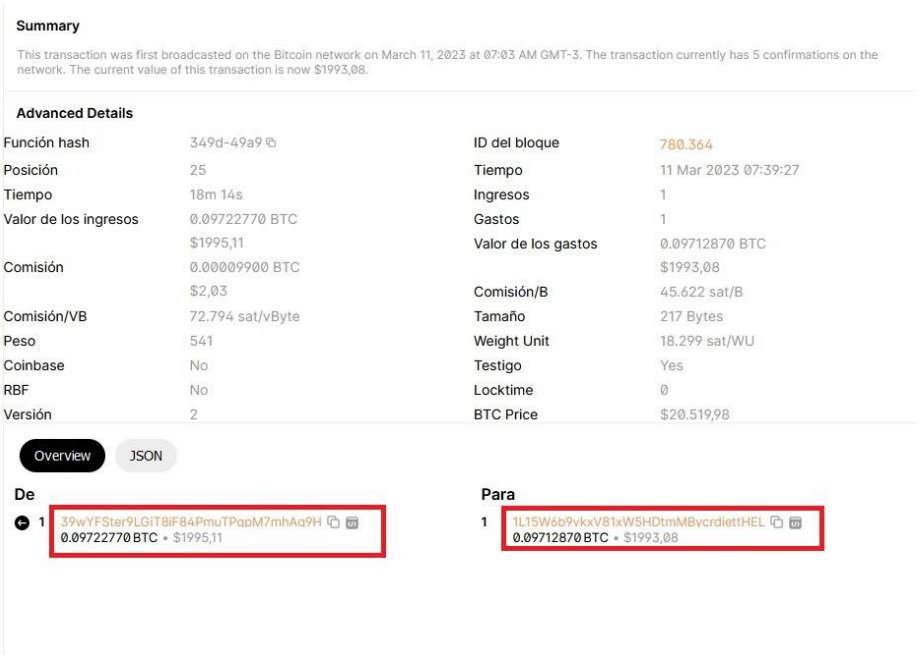


Figura 29 Transacción de cuenta a cuenta en la Blockchain de Bitcoin. Destacado la clave pública de la cuenta de origen y de la cuenta de destino

El punto crucial sobre el cual queremos desarrollar nuestras consideraciones tiene relación con que al tener la Blockchain el registro de todas las transacciones que se realizaron en ella, podemos en cualquier momento realizar la “trazabilidad” de todas las transacciones que realizó y que recibió una clave pública (una cuenta).

La imagen siguiente, muestra la trazabilidad de la cuenta de origen, que se mostró anteriormente. En este caso el “explorador de Blockchain”, nos permite visualizar todas las cuentas que enviaron Bitcoins a esa clave pública, y todas las cuentas, a las que dicha clave pública envió Bitcoins.

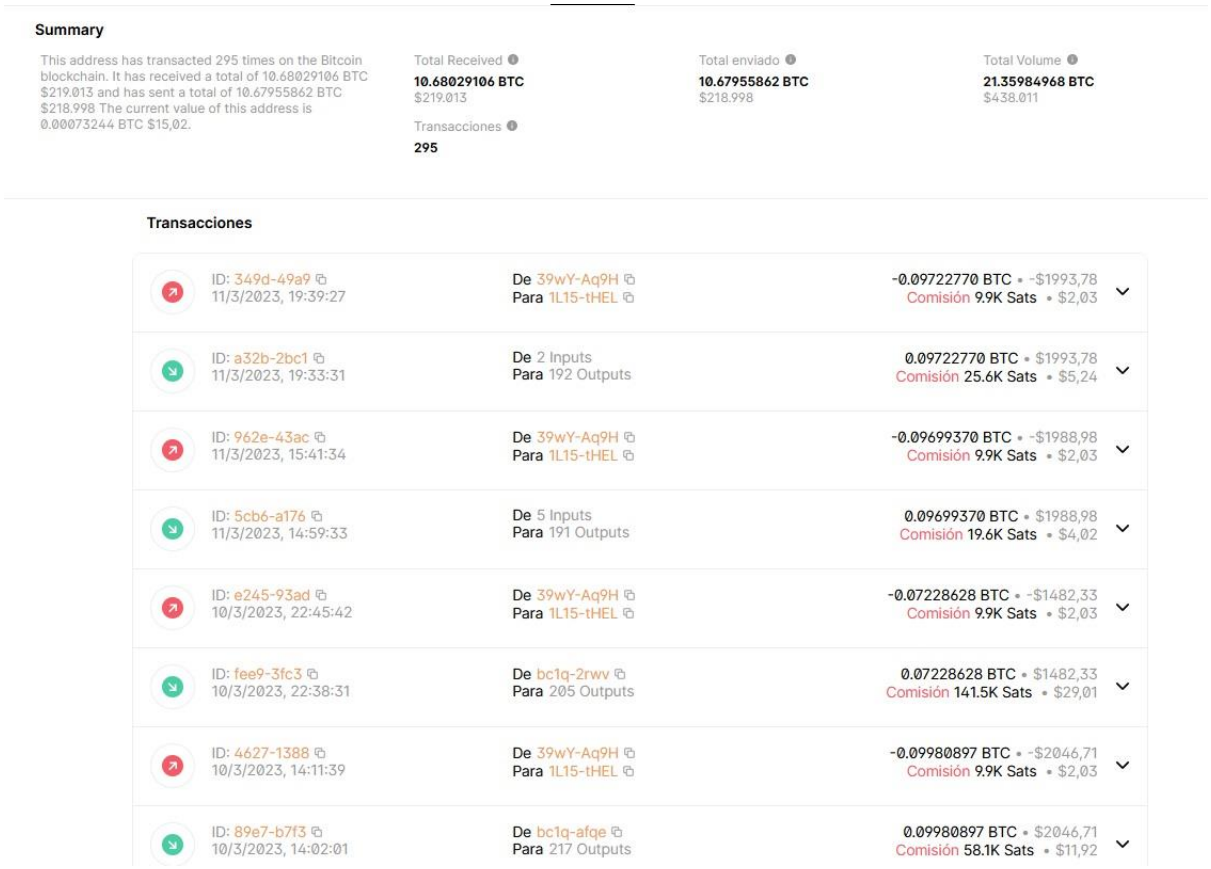


Figura 30 Trazabilidad de la cuenta de origen

Basándose en esto, los reguladores han establecido a los Exchanges la obligación de reportar datos identificativos y las claves públicas con las que sus clientes operan. De este modo, y con esa información capturada desde “out-chain” (ningún dato identificativo queda guardado en la blockchain), se puede vincular a una persona, con determinadas claves públicas de su dominio. Y además realizar la trazabilidad para atrás y para adelante de esa clave pública, para identificar las cadenas de transacciones, y cuentas, que se han ido vinculando.

En este punto, es donde consideramos relevante, analizar brevemente, la problemática que se ha generado en el ambiente Blockchain, en los últimos años con el auge de los denominados “mixers”, en especial con el problema generado por “tornado cash” y la fuerte y decisiva intervención del Tesoro de USA en esta temática.

Nuestro interés en destacar esta temática, no se limita solamente a analizar lo ocurrido, sino también en ver la perspectiva de las denominadas “ZKP - pruebas de conocimiento cero” que tornado cash implementó, y que recientemente Vitalik Buterin identificó como la dirección hacia donde se va a orientar la Blockchain Ethereum (la blockchain líder en desarrollo de contratos inteligentes).

Las Pruebas de Conocimiento Cero y el anonimato de cripto-activos

Veamos brevemente cómo funciona un “mixer”, un Contrato Inteligente que funciona sobre una Blockchain pública y que permite romper la trazabilidad de sus cuentas, y de esta manera convertirlas en anónimas, aún cuando previamente se conociese la identidad del dueño de estas cuentas.

Vamos a suponer que una persona adquirió 3 Ethers por medio de un Exchange registrado, cumplimentando con todos los requisitos de identificarse fehacientemente. Vamos a suponer que su tenencia se encuentra en 3 cuentas, las de color verde en la imagen, donde cada cuenta posee 1 Ether.

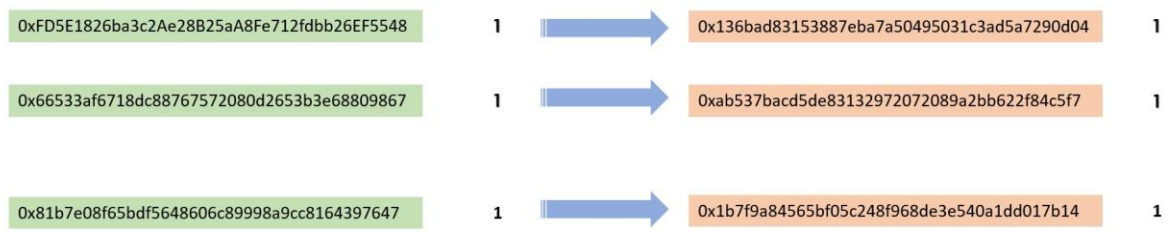


Figura 31 Transferencia de Ethers desde una cuenta a otra”

Esa persona quiere transferir esos Ethers a otras cuentas, que maneje él, pero su objetivo es que se rompa la trazabilidad de la Blockchain. En el ejemplo de la imagen, si realiza la transferencia desde la cuenta que termina en “5548” a la cuenta que finaliza en “0d04”, esa transacción va a quedar registrada at Perpetum en la Blockchain y facilmente se va a poder identificar el destino de sus criptomonedas.

¿Qué es lo que podría hacer para evitar que se puedan relacionar las cuentas de origen con las de destino?

La primera aproximación para resolver el problema, la podemos ver en la siguiente imagen:

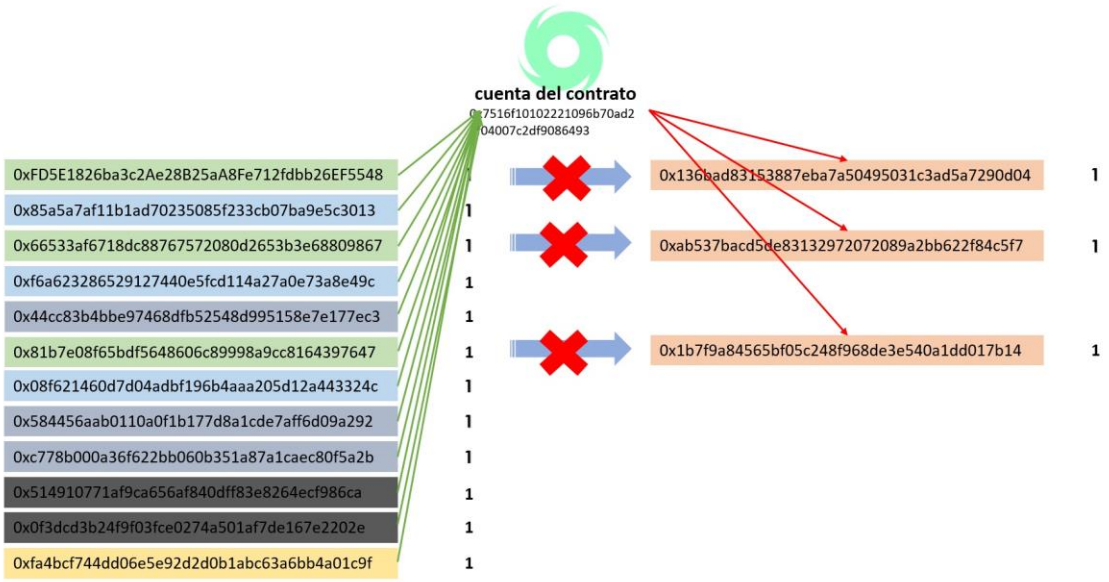


Figura 32 Envio desde distintas cuentas de Ethers a la cuenta de un Contrato Inteligente

Lo que la persona puede hacer, es juntar su cuenta, con una gran cantidad de otras cuentas, todas con el mismo importe. Todas estas cuentas, no realizaran sus transferencias de cuenta a cuenta, sino que enviaran sus Ethers a la cuenta de un Contrato Inteligente (en la imagen la cuenta terminada en “6493”). El Contrato es el que se encargará de transferir, en un segundo momento, los Ethers recibidos a otras cuentas de destino.

Al mezclarse las 3 cuentas de la persona, junto con las cuentas de muchos otros usuarios, y al realizar la transferencia el Contrato Inteligente en un momento posterior, se provocará el efecto denominado “mixer”, es decir, mezclar (hace referencia a la mezcla de cartas en juegos como Black Jack donde se usan varios mazos de cartas) que permite ofuscar la trazabilidad de las transacciones en la Blockchain.

Pero en este punto nos encontramos con otro problema. Como ya mencionamos, los Contratos Inteligentes se registran en la Blockchain con la misma lógica que las transacciones. Es más, el Contrato Inteligente se envía a la Blockchain por medio de una transacción. El código fuente (el programa) del Contrato queda registrado, al igual que toda la información que maneja, y es accesible a todos los usuarios de la Cadena de Bloques.

Es decir, que lo único que logramos fue ralentizar la trazabilidad, ya que quien quiera conocer la relación que existe entre la cuenta “5548” y la “0d04”, solo deberá buscar su conexión en el registro de actividad del Contrato Inteligente, que utilizó su propia cuenta (“6493”) para conectar en forma diferida la cuenta origen y la cuenta destino.

Una segunda aproximación a la solución que se busca, la podemos encontrar en la siguiente imagen:

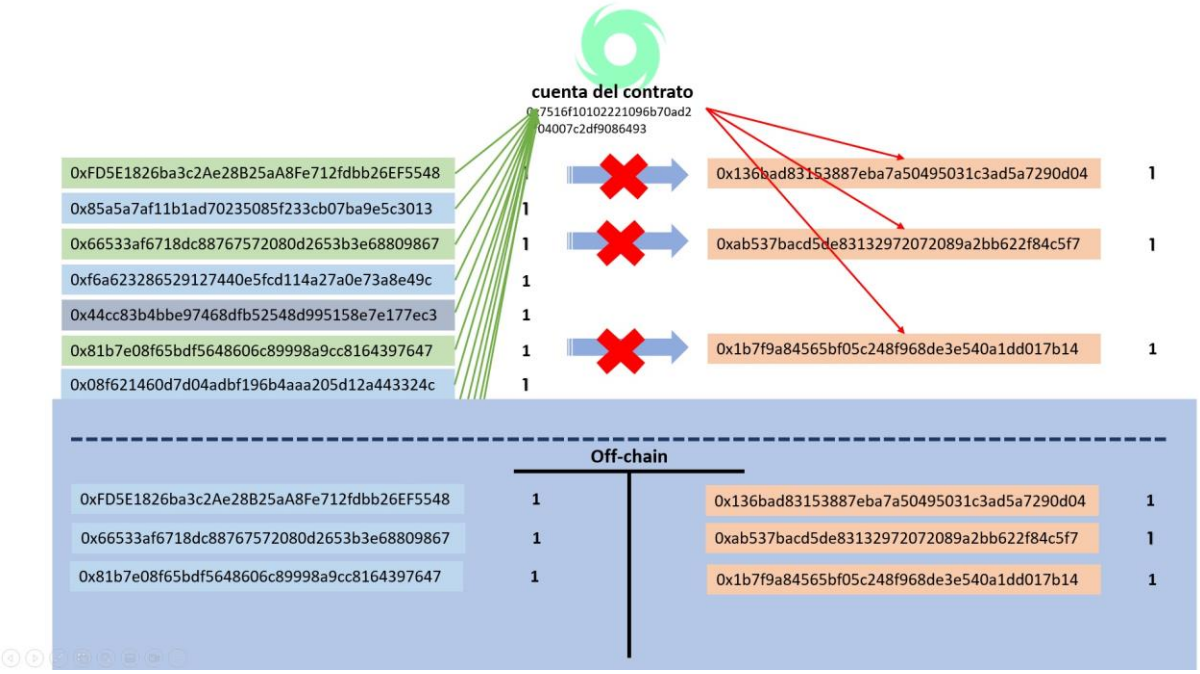


Figura 33 Registro de doble entrada(cuentas origen y destino de cada cliente), de manera que el Contrato Inteligente no almacene dentro de la Blockchain (“on-chain”), la información que vincula las cuentas

En este caso, por afuera de la Blockchain (“off-chain”), vamos a establecer un registro de doble entrada, con las cuentas origen y destino de cada cliente, de manera que el Contrato Inteligente no almacene dentro de la Blockchain (“on-chain”), la información que vincula las cuentas.

En este caso, el Contrato Inteligente, se comunicará con un servidor centralizado fuera de la Blockchain, por medio de un “oráculo” (los puntos de conexión de la Blockchain con el exterior) donde recibirá la orden de pagar, desde el Stock total de Ethers (esta es la función mixer), a la cuenta destino.

Aquí pareciese que resolvimos el tema planteado. Pero existe un inconveniente. La tecnología de la Blockchain se basa en un principio fundacional de la misma, que es la invulnerabilidad de sus registros. Se desarrolló toda esta tecnología con esa finalidad, y es en sí, la razón por la cual la utilizamos en lugar de otros sistemas propietarios ya existentes.

Al guardar un registro “off-chain” de cuales cuentas se vinculan con cuales, nos encontramos, como mínimo con tres problemas:

- Estamos usando un sistema centralizado, por lo cual, estamos creando allí, un punto de vulnerabilidad por hackeo.
- Si algún organismo regulador quisiera conocer la información que vincula las cuentas, podría fácilmente conseguir una orden contra ese servidor, y obtener toda la información necesaria para restablecer la trazabilidad de cuentas.
- Al ser el servidor “off-chain”, un sistema gobernado por una institución, se corre el riesgo de fraude, en especial, que el propietario del Contrato Inteligente dé en un momento orden de transferir la totalidad del stock de Ethers, a una cuenta propia y se robe todos los cripto-activos de los clientes.

Para resolver el problema que analizamos, los denominados “mixer”, en especial el caso que mencionamos de “tornado cash”, comenzaron a implementar las denominadas ZKP - Pruebas de Conocimiento Cero.

¿En qué consiste una Prueba de Conocimiento Cero ? Es un complejo desarrollo matemático y computacional, por el cual yo puedo brindarle a alguien un grado muy alto de certeza, de que poseo determinada información, sin revelar dicha información a esa persona.

La complejidad del algoritmo que sustenta las ZKP, excede el alcance de este trabajo. Nuestro objetivo en este punto es visualizar la dinámica que el método tiene para poder, dentro de la Blockchain pública, romper la trazabilidad de cuentas.

En este caso todas las cuentas de origen transfieren sus fondos al Contrato Inteligente, con la lógica del “mixer”, es decir que el Contrato Inteligente actúe como un fondo acumulativo de Ethers. Por esos Ethers transferidos al Contrato Inteligente se generarán Pruebas de Conocimiento Cero. La segunda etapa se hará cuando el usuario envíe al Contrato Inteligente el “proof”, la validación a ser evaluada por el Contrato. En ese momento, al evaluar la ZKP el Contrato tendrá la certeza de que el solicitante es el dueño de una cantidad determinada de Ethers que ya fueron transferidos al Contrato. Pero, ni el Contrato, ni los terceros podrán acceder a conocer, desde cuales cuentas se realizaron las transferencias (ese sería el “conocimiento cero”).

En ese momento, el Contrato Inteligente aprueba la segunda transacción y envía a las cuentas solicitadas por el usuario, los Ethers correspondientes.

La imagen siguiente, muestra esta dinámica y como las ZKP rompen la trazabilidad de la Blockchain.

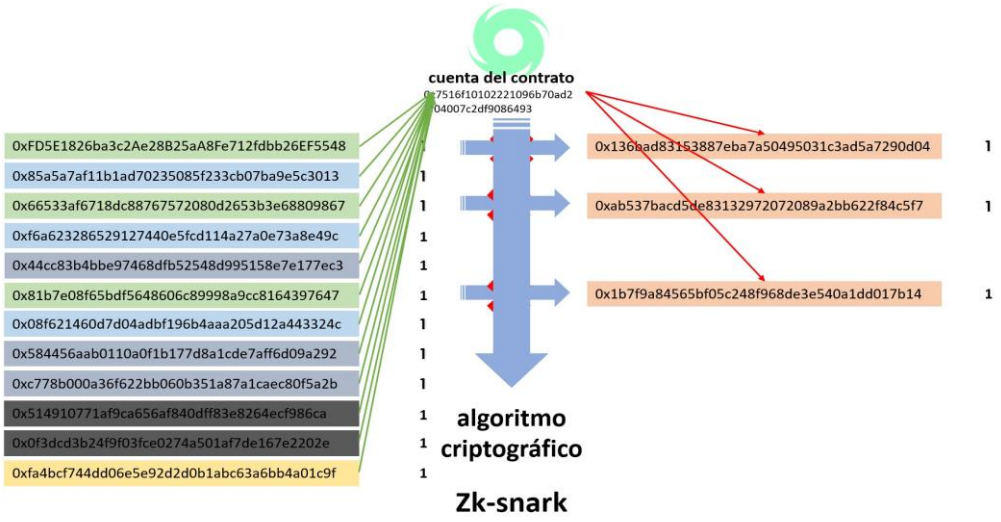


Figura 34 Contrato Inteligente aprueba la segunda transacción y envía a las cuentas solicitadas por el usuario, los Ethers correspondientes, las ZKP rompen la trazabilidad

El caso que mencionamos acerca del uso de mixer con ZKP, Tornado Cash, tuvo especial relevancia en tanto el 08 de agosto de 2022, la OFAC - Treasury's Office of Foreign Assets Control, levantó una denuncia contra los titulares de esa firma, acusándolos de utilizar estos procedimientos para realizar el lavado de operaciones por unos 7.000 millones de dólares[59].

En esta consideración, las ZKP pueden utilizarse para dar anonimato a cuentas de Blockchain públicas, y en consecuencia, para invisibilizar la territorialidad de operaciones que se desplieguen en redes descentralizadas públicas. Un tema que debe ser considerado al momento de diseñar la estrategia de desarrollo de la Plataforma NFT/FT para Santa Fe, como así también para las decisiones de gravabilidad de impuestos.

Una última consideración vinculada con la utilización de las ZKP, es la mención que realizamos previamente sobre las declaraciones de Vitalik Buterin, fundador y alma mater de la red Ethereum, quien manifestó que esa Blockchain se va a ir orientando definitivamente al uso de las Pruebas de Conocimiento Cero. La salvedad que creemos es oportuno realizar, es que en este caso particular, la adopción de las ZKP no tienen como objetivo romper trazabilidad de transacciones, ni utilizarlas para el blanqueo de dinero. Vitalik se refiere al uso de ZKP para lo que se denominan los "roll-ups".

Los "roll-ups", utilizan las Pruebas de Conocimiento Cero, para validar fuera de la Blockchain (off-chain), bloques con grandes cantidades de transacciones. La validación de los bloques se acompañan con ZKP que son evaluadas "on-chain" por la Cadena de Bloques (en principio

[59] Bloomberg - Coinbase Is Helping Sue The US Treasury Over Tornado Cash Sanctions
https://www.bloomberg.com/news/articles/2022-09-08/coinbase-backs-lawsuit-against-us-treasury-for-tornado-sanctions
Observado: febrero 2023

por Contratos Inteligentes, aunque el proyecto en que se trabaja en Ethereum, es que la Blockchain lo haga en forma nativa, dentro de la Ethereum Virtual Machine - el “intérprete” que ejecuta Contratos Inteligentes). De esta manera, al evaluar una ZKP que incluye una gran cantidad de transacciones, se logra un ahorro importante de recursos computacionales y tiempo, haciendo mucho más eficiente el desempeño de la Blockchain.

Conclusiones

Iniciamos esta parte de la evaluación de la conveniencia de desarrollo de una Plataforma NTF/FT viendo la preponderancia que tiene en la actualidad la intervención del Estado en determinadas materias, de la cual no podemos dejar excluida a la tecnología de Blockchain y su respectivo ecosistema.

Planteamos cómo punto de análisis, en línea con lo expuesto por Josepth Stiglitz, la consideración que, en algunas temáticas, la intervención del Estado puede generar distorsiones en el dinamismo propio del sector que se impacta, pero se debe ponderar si la no intervención puede tener resultados finales, más perjudiciales.

En virtud de todo lo que hemos analizado, en especial en el marco jurídico internacional, entendemos que la regulación estatal en los desarrollos del ecosistema Blockchain, no solo es sugerida, sino que estimamos necesaria. Esto toma especial relevancia en el área de DeFi - Finanzas Descentralizadas, dónde el Estado debe velar por el resguardo del capital y patrimonio de ahorristas e inversionistas. Vale destacar, en este punto, la incipiente cantidad de estafas piramidales y licuación de activos provocados por la alta volatilidad de criptomonedas que se han observado en los últimos tiempos.

Analizamos la gravavilidad de hechos económicos en las normativas provinciales que alcanzan cripto-activos, viendo que solamente una provincia, Catamarca, grava a contratos vinculados a monedas digitales con Impuesto de Sellos.

Realizamos también un breve análisis sobre la conceptualización de red descentralizada sobre la que se basa la tecnología de Blockchain, y en función de esto, la complejidad de determinar territorialidad por la cual se pueda verificar el hecho imponible pretendido. Tal vez, por está razón es que no se ha gravado con impuestos de Sellos en otras jurisdicciones a las operaciones vinculadas a cripto-activos.

En referencia al estudio realizado en función de los hechos imponibles identificados en Impuestos sobre los Ingresos Brutos, vimos que en la mayoría de las jurisdicciones se gravan dos situaciones: los servicios vinculados a cripto-activos, y las operaciones realizadas sobre

los mismos. En algunos casos, no sé gravan simultáneamente ambas situaciones, sino sólo una de ellas.

Por último, analizamos la problemática que presenta la tecnología de Blockchain , por su propia dinámica y concepción, en la determinación de identidad de quienes operan con ella. En especial en las Blockchain públicas (no permisionadas), cómo las de las principales criptomonedas.

Este factor se vincula directamente, no solo con la identidad, sino con el domicilio del contribuyente o sujeto impactado por el tributo.

Hicimos una consideración especial vinculada a un tema polémico y de mucha relevancia actual en el mundo cripto, cómo es la función de los "mixers" y las ZKP - Pruebas de Conocimiento Cero. Estás técnicas permiten romper la trazabilidad de transacciones en Blockchain públicas, y de esta manera perder el rastro de transacciones, aún cuando la original haya sido identificada.

En función de todas estas cuestiones creemos, se debe ir perfilando el análisis de factibilidad y conveniencia del desarrollo de una Plataforma NFT/FT y la tentativa gravavilidad impositiva de cripto-activos en la provincia de Santa Fe.

Estás cuestiones se irán integrando al final de este trabajo, para conformar finalmente el modelo de evaluación integral que sugerimos para evaluar la conveniencia del desarrollo de la Plataforma NFT/FT para Santa Fe. Por el momento debemos ir considerando entre otros:

- conveniencia y grado de intervención y regulación estatal, en el ecosistema Blockchain, en función de las decisiones políticas vinculadas
- alcance de gravabilidad de cripto-activos, en el caso que se desee, para la provincia de Santa Fe. Se deberá considerar el hecho imponible en Ingresos Brutos (servicios vinculados a cripto-activos, operaciones con criptomonedas. etc…), y si es procedente gravar también con Impuesto de Sellos, a las operaciones / contratos respaldados o vinculados a criptomonedas.
- definir los puntos críticos de análisis vinculados a la identidad de los actores de la Plataforma NFT/FT, como así también de actores externos a la misma, pero que se vinculen con operaciones de cripto-activos.
- definiciones vinculadas al tipo de Blockchain a utilizar, y su alcance. Este tema en particular se desarrollará en más detalle en trabajos próximos, aunque en el presente se realizó un perfilamiento de la cuestión.
- analizar las variantes que impactan en el ecosistema, tales como las técnicas mixer y ZKP, sus tendencias y probable impacto. En especial con relación a la posibilidad de

quebrar trazabilidad de transacciones y maniobras fraudulentas o de lavado de dinero que se desprendan de esto.

Desarrollos de NFT y FT en el ámbito mundial, nacional y regional

Introducción

Sin intentar restar importancia a los desarrollos en otras áreas, el impacto más fuerte y a su vez más problemático de la tecnología de Blockchain, creemos se evidencia en el campo de las finanzas.

Desde su concepción como la tecnología que diera sustento a las criptomonedas, y considerando la factibilidad de poder eliminar o mitigar la acción de intermediarios en los mercados de dinero, el uso de la Blockchain ha tenido su crecimiento más significativo en el área de finanzas. Por otra parte, en consecuencia a la alta volatilidad de los precios de las criptos, y al "limbo" legal de la rémora de una regulación clara y consistente, es tal vez, el sector más controvertido y provocativo del ecosistema Blockchain, en lo que respecta a la intervención de los Estados.

Vamos, por tanto, a realizar un relevamiento de los principales desarrollos, implementaciones y tendencias que existen actualmente a nivel regional y mundial, en el ecosistema Blockchain, dando preponderancia al mercado innovador y creciente de las DeFi - Finanzas Descentralizadas.

¿Qué son las DeFi - Finanzas Descentralizadas?

Definición

Según definen Lau, D y otros (2020), la definición de DeFi - Finanzas Descentralizadas, gira en torno a:

"Finanzas descentralizadas o DeFi es el movimiento que permite a los usuarios utilizar servicios financieros como cesión u obtención de préstamos, trading, sin la necesidad de depender de entidades centralizadas. Estos servicios financieros se brindan a través de aplicaciones descentralizadas (Dapps), en las que la mayoría de ellas se implementan en la plataforma Ethereum."[60]

[60] Lau, D., Lau, D., Jin, T. S., Kho, K., Azmi, E., Lee, T. M., & Ong, B. (2020). *How to DeFi* (Vol. 1). Coin Geko - Book Starter ID.
Traducción del autor

Vemos que si bien la definición menciona a la Blockchain de Ethereum, como la “plataforma” sobre la que se implementan la mayoría de las Finanzas Descentralizadas, al mismo tiempo se encarga de destacar al inicio, a las DeFi como “el movimiento”, es decir, independizando el concepto de Finanzas Descentralizadas con la tecnología de Blockchain.

Entendemos que en la práctica este desacople entre la idea abstracta de descentralización y la tecnología específica de Blockchain, es casi irrelevante, en tanto la Cadena de Bloques se ha posicionado como la tecnología líder en redes distribuidas. Sin embargo, es bienvenida la definición en su esclarecimiento de que el concepto en que se basan las DeFi es la descentralización, con independencia de la tecnología que la sustente.

Características

Algunas de las características distintivas que podemos destacar de las DeFi son:

- ➢ Si bien en su arquitectura utilizan diferentes interfases y pueden ser desarrolladas en varias capas, todo el “proceso de negocio” de las DeFi ocurre “on-chain”, es decir, en la Blockchain misma. De esta forma todos los datos y procesos vinculados a su ejecución quedan registrados, accesible e inalterablemente en la Cadena de Bloques.
- ➢ El usuario no interactúa con una “entidad” en el aspecto formal. Solo va a hacerlo con un contrato inteligente, donde se puede verificar en cualquier momento las reglas y lógica del mismo, así como el funcionamiento.
- ➢ Son “open source”, vale decir que el código de programa que se ejecuta está plasmado en contratos inteligentes desplegados sobre la Blockchain. Al ser accesibles por todo el mundo, se logra el impulso de que la comunidad de programadores vinculados a la iniciativa puedan ir perfeccionando e innovando el mismo.

DeFi primitivas

La definición de DeFi que citamos nos habla de “cesión de préstamos” (lending), “obtención de préstamos” (borrowing), y trading, esto último no vinculado al comercio propiamente dicho (sería la traducción literal), sino a las técnicas de obtención de ganancias por medio de la compra-venta de divisas y activos financieros.

Es nuestro entender, que los autores nos quieren presentar lo que se denominan las “primitivas” de las DeFi. Este término nos habla, por oposición, de todas las variantes desarrolladas en el universo de productos financieros DeFi, que se derivan de las “primitivas”.

Según sea su apreciación de grado de desarrollos que en el área se destacan, los autores pueden diferir en las “primitivas” que se consideren.

A continuación presentamos una clasificación, con casos de usos, que a nuestro entendimiento son las más relevantes herramientas que se están desarrollando actualmente en el campo de DeFi:

Préstamos:

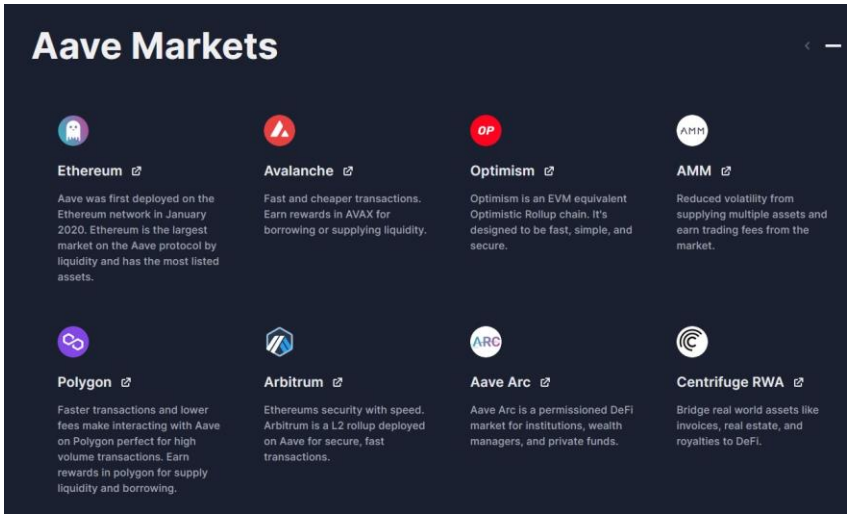
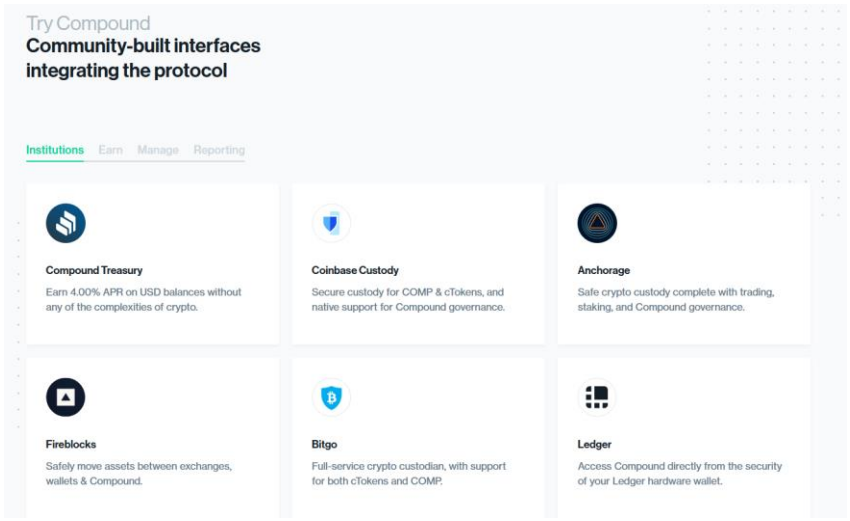
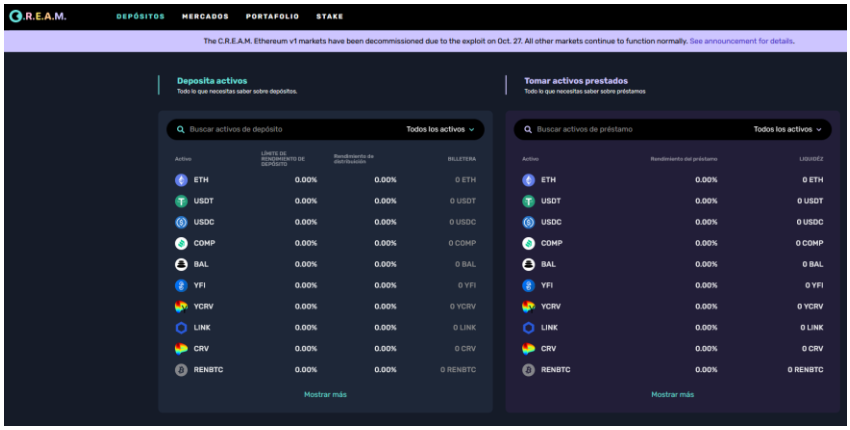
Préstamos colateralizados

La dinámica se basa en depósitos de criptomonedas o tokens específicos que los inversionistas realizan en favor de un Contrato Inteligente. Por esos fondos el Contrato paga un interés previamente pactado. A su vez el contrato “presta” esos tokens a otros usuarios quienes garantizan la operación por medio de una inmovilización de sus activos en favor del Contrato Inteligente.

El monto de inmovilización en garantía, en relación con el préstamo que se otorga está en función del “margen de colateralización” de la operación, el cual está definido en el Contrato Inteligente, y puede variar, entre otras razones, en consideración del token (especie) que se deja en garantía.

El beneficio fundamental de este tipo de préstamos se basa en la liquidez adicional generada por la utilización de activos inactivos (apalancamiento). Por otra parte permite al solicitante recibir activos líquidos de forma inmediata, con los cuales moverse rápidamente en cambio de posiciones que necesite realizar, sin desprenderse de sus activos entregados en garantía al formar el colateral.

Dentro de los desarrollos que proveen préstamos colateralizados en el ambiente DeFi, podemos mencionar

AAVE	
	AAVE - https://aave.com/
Compound	
	Compound - https://compound.finance/
C.R.E.A.M.	
	C.R.E.A.M. - https://app.cream.finance/

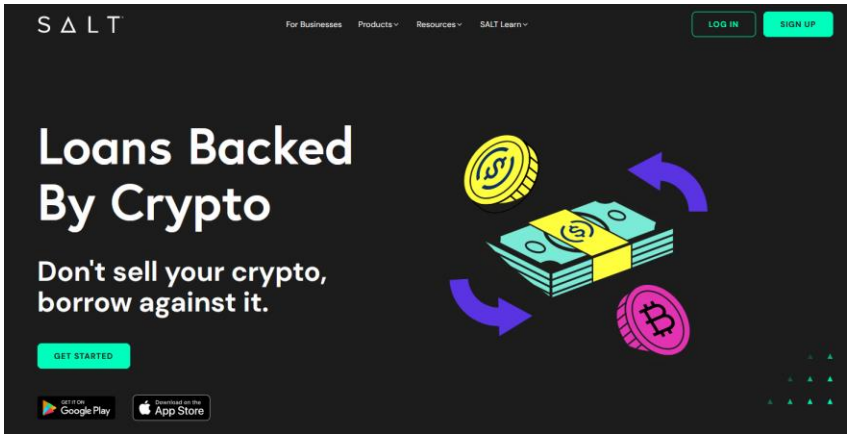
SALT Blockchain-Backed Loans®	
	SALT - https://saltlending.com/

Figura 35 Desarrollos que proveen préstamos colateralizados en el ambiente DeFi

Este tipo de préstamos genera otro tipo de instrumento financiero del sector DeFi, los denominados “Mercados de Liquidación”.

Mercados de Liquidación

Así como en el mundo real, generalmente, las instituciones financieras poseen firmas tercerizadas que se encargan de la ejecución de garantías, existe en el mundo DeFi desarrollos específicos con esa finalidad.

En el caso que analizamos recién, el contrato inteligente que gobierna los préstamos colateralizados, puede transferir activos que fueron bloqueados en garantía, a otro contrato que se encargará de gestionar la liquidación de los mismos, habiendo generando previamente un mercado de liquidación, con actores que se interesen en los márgenes de utilidad con que se realizaran esas operaciones.

Flash Loans - Préstamos instantáneos

Son préstamos sin garantía que se otorgan dentro del sistema DeFi, en especial, sobre la Blockchain de Ethereum.

En una primera mirada parece imposible que algo así exista, ya que nadie daría una cantidad de criptomonedas en préstamos a otra persona, sin ninguna garantía, y en especial en un ámbito de anonimato como el que genera las Blockchain públicas.

La existencia de los préstamos instantáneos se basa en una particularidad del funcionamiento de la Blockchain que se da por el tiempo que transcurre entre la realización de una transacción y el momento en que la misma es incluida en forma definitiva dentro de la Blockchain por medio del proceso de mineración.

En un flash loan, el contrato inteligente, que posee Ethers de liquidez, realiza dos transacciones calzadas, en las cuales, en una realiza el préstamo y en la segunda realiza el cobro del mismo, más los intereses respectivos. Ambas transacciones son programadas para entrar en el mismo bloque de la Blockchain, de modo de quedar registradas como definitivas, juntas.

La cuestión pasa por la disponibilidad que tiene el usuario de la primera transacción, que quedó registrada en la Blockchain como pendiente. Estas transacciones se dice que están en estado “unconscious”. Muchas billeteras digitales (por ejemplo Metamask), no dejan al usuario utilizar esas criptos, hasta que se reciba la confirmación definitiva. Pero no es así, en otros protocolos, especialmente de trading del ámbito DeFi. Estos protocolos lo admiten, ya que una vez que la transacción impactó en la Blockchain, y fue validada por varios nodos, se considera irreversible, independientemente de que todavía no se haya incluido en forma definitiva a un bloque.

Esta brecha de estado inconsciente es lo que le permite al usuario, realizar alguna operación en otro protocolo, obtener ganancias, y volver a saldar su posición. Pensemos que el promedio de mineración de bloques en Ethereum, actualmente está en unos diez segundos, por lo cual, quien hace uso de estos préstamos instantáneos, no realizan una operación dirigida por el ser humano, sino que el pase de fondos y salida del otro protocolo DeFi, en el cual obtendrá la ganancia, está previamente programado, y “acoplado” al préstamo instantáneo. Por este motivo es que generalmente las operaciones que se realizan fondeando con flash loans, son operaciones de arbitrajes puntuales (diferencias de cotización entre mercados que justifican la intervención del tomador de ganancias).

Dentro de los desarrollos que proveen préstamos instantáneos en el ambiente DeFi, podemos mencionar:

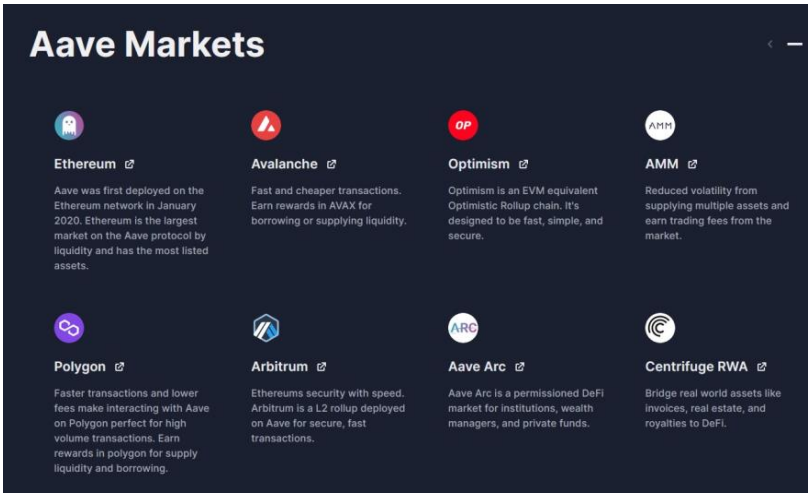
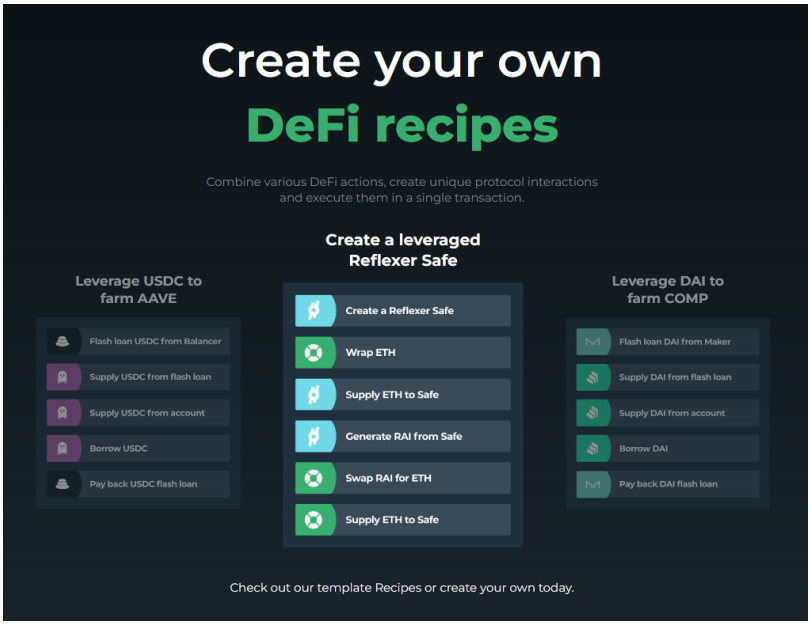
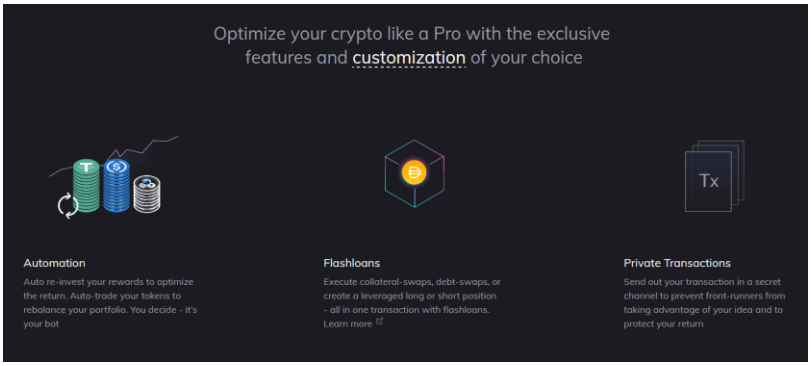
AAVE	
	AAVE - https://aave.com/
DeFi Saver	
	DeFi Saver - https://defisaver.com/
FURUCOMBO	
	FURUCOMBO - https://furucombo.app/

Figura 36 Desarrollos que proveen préstamos instantáneos en el ambiente DeFi

Trading:

Libros de Órdenes descentralizados

Es la implementación básica del trading de cripto-activos, por medio de la cual, clientes "firman criptográficamente" las órdenes que se alojan en el contrato inteligente, bloqueando los tokens respectivos, hasta que calce una orden de compra, en contrapartida. Una vez que el contrato calza ambas órdenes, la liquidación se realiza automáticamente.

La imagen siguiente nos muestra el Libro de Órdenes de Binance corp.

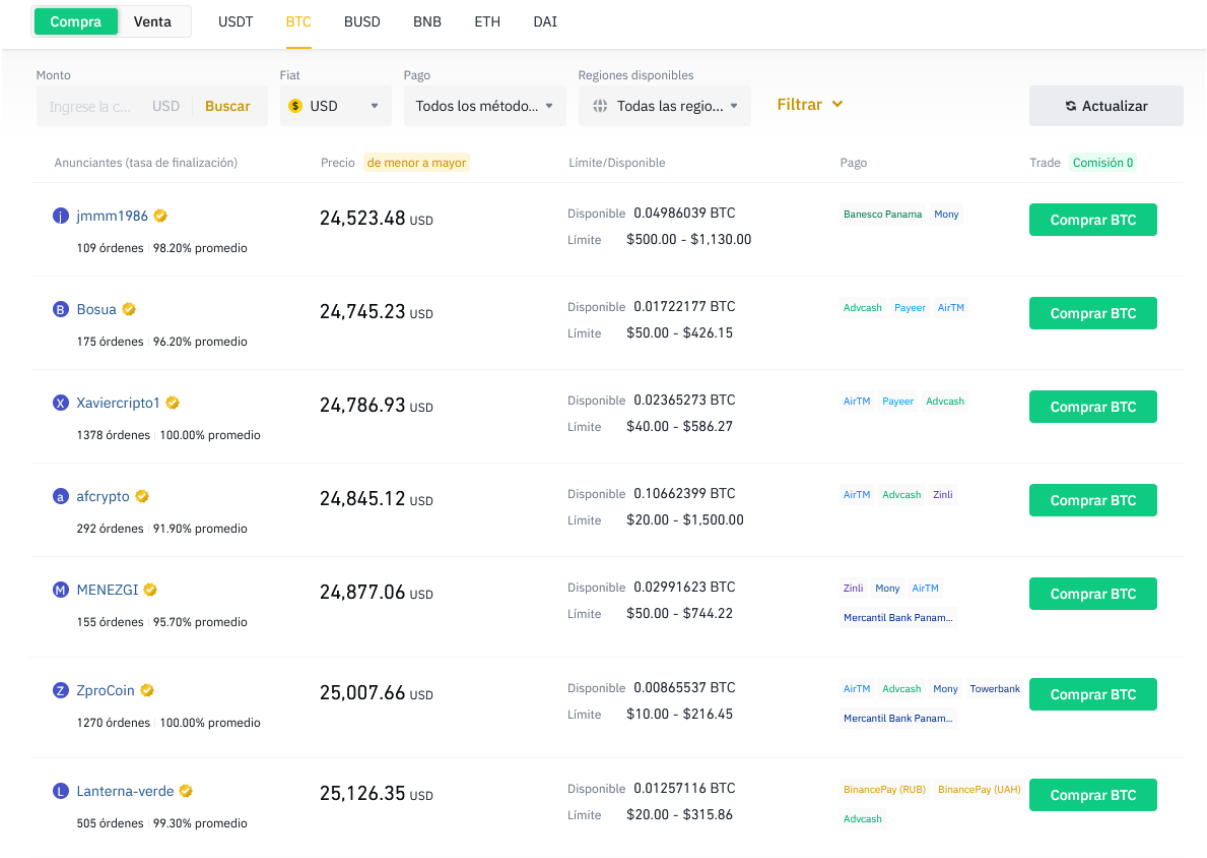
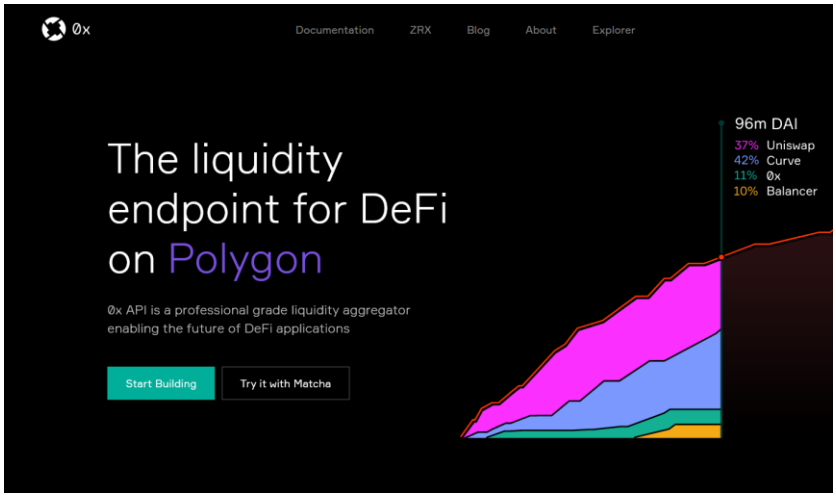
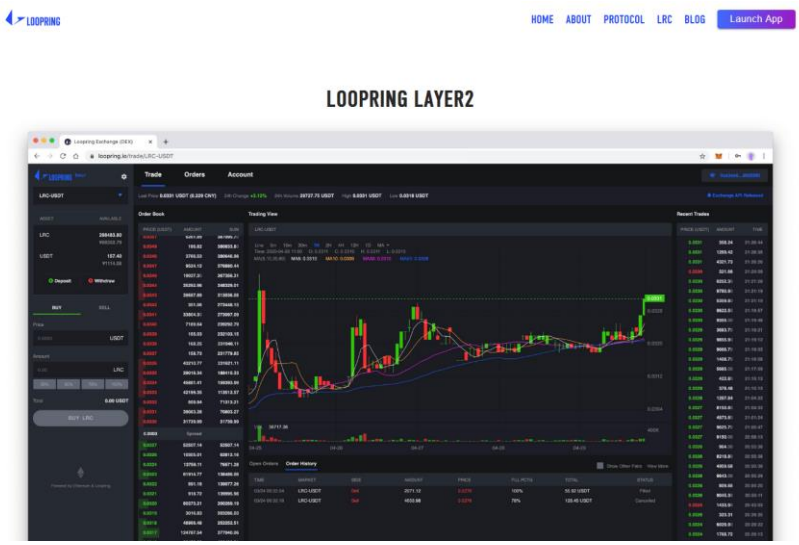


Figura 37 Libro de Órdenes de Binance corp

Dentro de los desarrollos que facilitan Libros de Ordenes, en el ambiente DeFi, podemos mencionar:

0x	
	0x - https://www.0x.org/
LOOPRING	
	Loopring - https://loopring.org

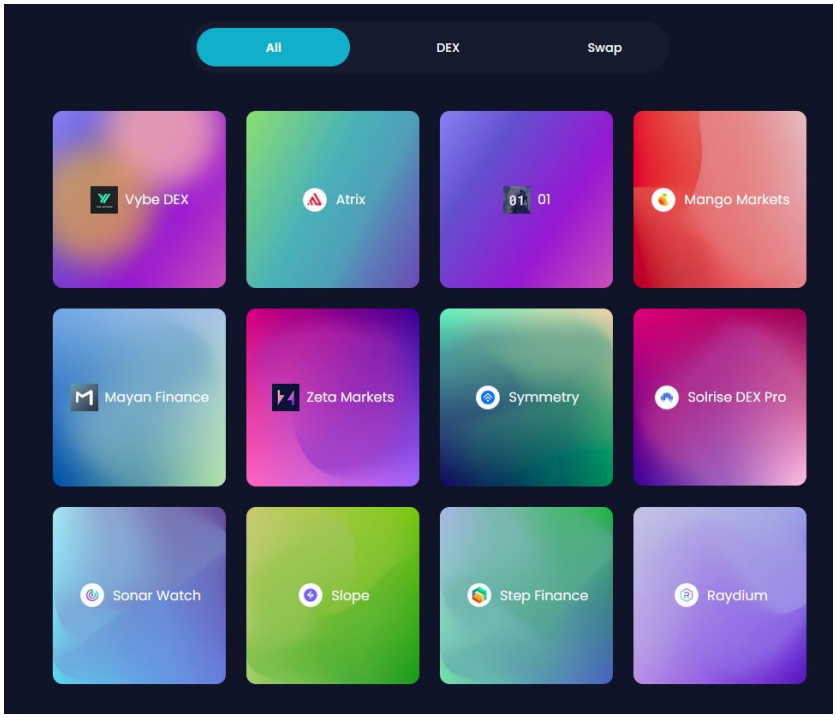
SERUM	
	Serum - https://portal.projectserum.com/

Figura 38 Libros de Ordenes, en el ambiente DeFi

Derivados

Por medio de los derivados, los instrumentos de trading que se desarrollan en el ámbito DeFi, generan un mercado similar al derivados en el mundo real, donde se pueden realizar apalancamientos, coberturas, short selling (especulación a la baja) y otros.

Esto, como es de esperar abre el juego a implementar estrategias e instrumentos más sofisticados, vinculados a opciones, futuros, swaps, e incluso el desarrollo de activos sintéticos digitales, los cuales siguen en forma automatizada el comportamiento de otros activos financieros del mundo real.

Al igual que los otros segmentos que analizamos, su implementación genera más liquidez al mercado particular que se desarrolla, aunque en el caso particular de los derivados, es de destacar su riesgo a exponenciar la volatilidad de los cripto-activos que se manejan en ese ámbito.

Dentro de los desarrollos que generan y negocian Derivados, en el ambiente DeFi, podemos mencionar:

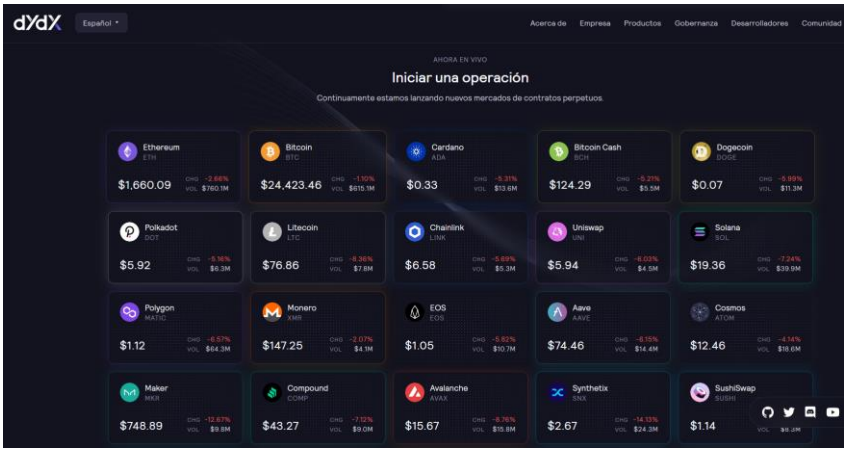
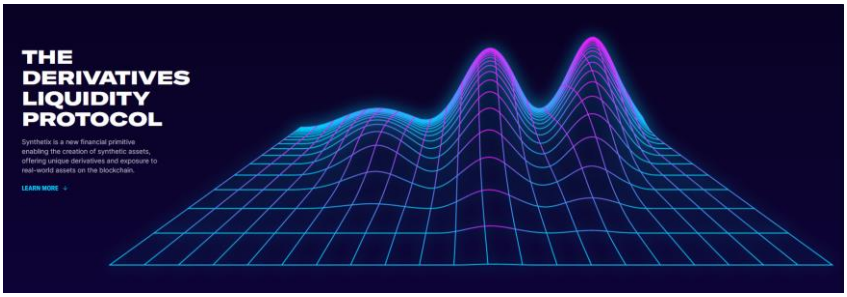
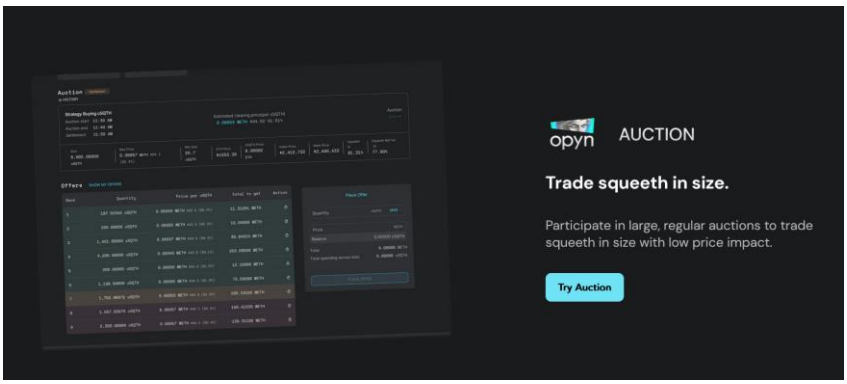
dYdX	
	dydx - https://dydx.exchange/
SYNTHETIX	
	Synthetix - https://synthetix.io/
opyn	
	opyn - https://www.opyn.co/

Figura 39 Desarrollos que generan y negocian Derivados, en el ambiente DeFi

AMM - desarrolladores de mercados automatizados

Son desarrollos basados en Contratos Inteligentes dónde se implementan órdenes de transaccionar entre diferentes tokens. Por ejemplo, una cantidad de ETH que deseo intercambiar por BNB. El Contrato Inteligente se encarga de generar el mercado donde esa operación se perfeccione.

¿Cómo sabe el contrato inteligente, cuál debe ser la relación de cambio entre las dos especies que se van a intercambiar ?

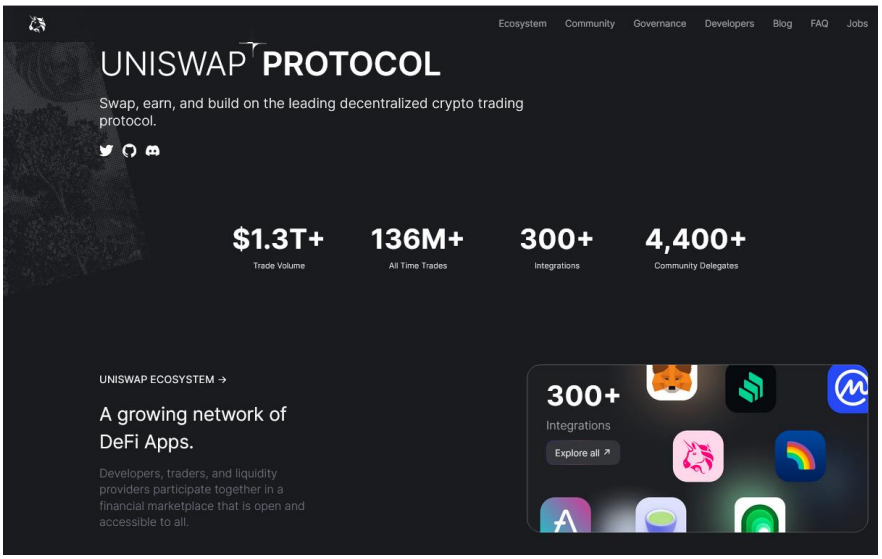
La mayoría de los contratos trabajan con una relación constante predefinida. Por ejemplo, el protocolo UNIWASP utiliza una fórmula matemática basada en la relación:

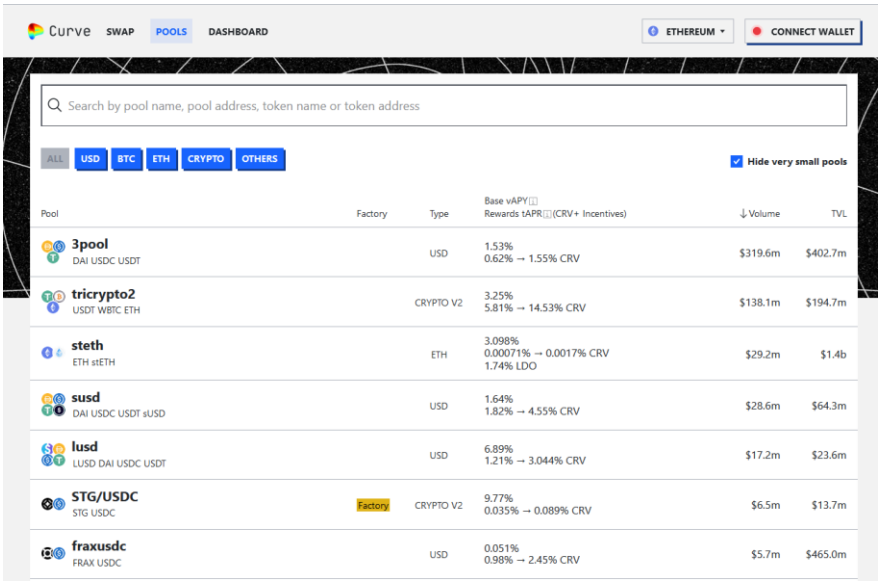
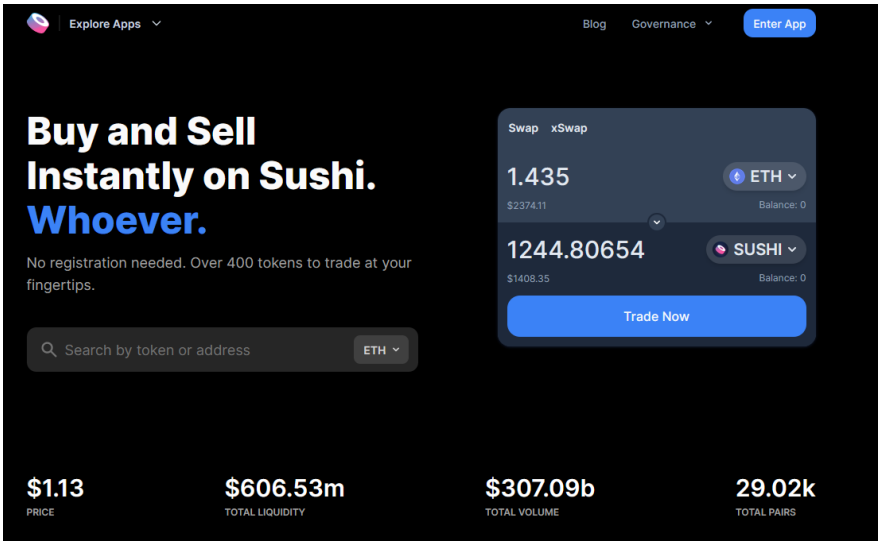
x * y = z

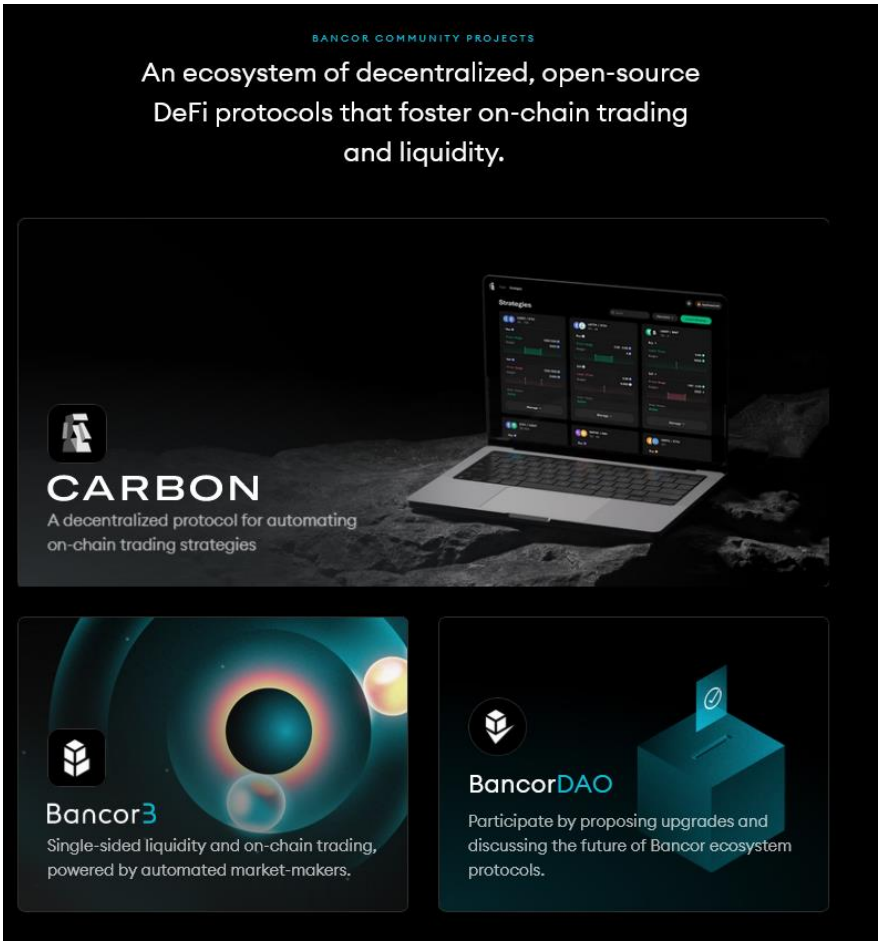
Dónde "x" es la cantidad de tokens de la primera especie a intercambiar que están en dominio del Contrato, y "y" es el stock de tokens de la segunda especie. "z" viene a ser la constante de relación entre ambas especies, que definirá el término de intercambio.

Está fórmula puede variar y complejizarse según sea el protocolo AMM que utilicemos.

Dentro de los desarrollos que generan y gestionan Mercados Automatizados, en el ambiente DeFi, podemos mencionar:

UNISWAP	
	UNIWASP - https://uniswap.org/

Curve	
	Curve - https://curve.fi
SushiSwap	
	Sushi swap - https://www.sushi.com/



Bancor - https://bancor.network/

Figura 40 Desarrollos que generan y gestionan Mercados Automatizados, en el ambiente DeFi,

Pero la pregunta que podemos hacernos es, cómo el Contrato Inteligente se asegura de poseer suficiente stock (liquidez) de tokens para realizar el intercambio. Allí es donde entra a jugar un tipo de desarrollo de DeFi transversal a varios instrumentos. Los denominados "pool de liquidez"

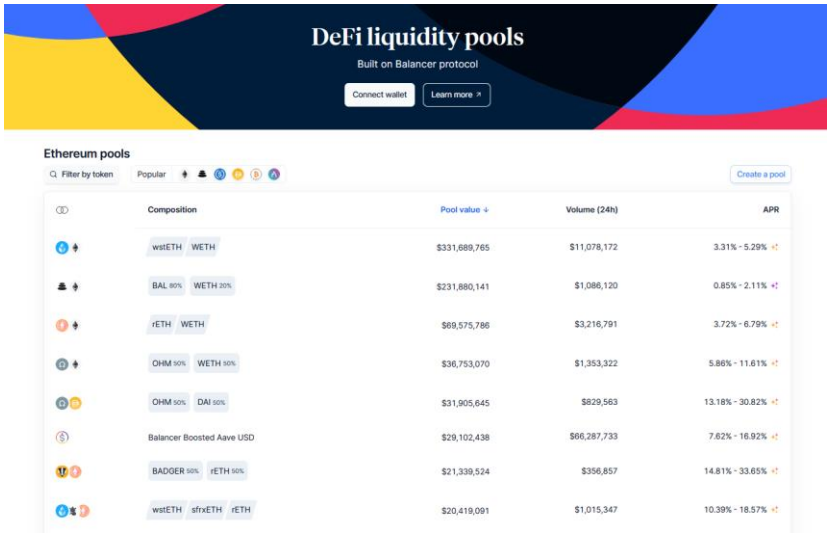
Pool de Liquidez

Un pool de Liquidez es un desarrollo realizado sobre el ambiente DeFi, por medio de Contratos Inteligentes cuyo objetivo es el de generar liquidez necesaria para sustentar determinados desarrollos como los de AMM que acabamos de mencionar, u otros como los de Yield Farming o Activos sintéticos.

Podemos definir a un Pool de Liquidez como, un repositorio de fondos basados en tokens criptográficos, gobernado por un Contrato Inteligente, cuyo principal objetivo es facilitar por medio de la generación de liquidez, que los actores que participan en colocación y obtención de préstamos, trading, y otras actividades de primitivas DeFi, puedan realizar en forma más fluida y eficiente, sus funciones. Quienes aportan sus cripto-activos a la conformación del Pool de Liquidez, reciben una recompensa por esto. Esa recompensa se descuenta de las utilidades de las operaciones que el Pool de Liquidez sustenta.

Los aportantes a la conformación de Pool de Liquidez, suelen denominarse dentro del vocabulario de Blockchain, como **LP - Liquidity Provider**.

Dentro de los desarrollos que gestionan Pooles de Liquidez, en el ambiente DeFi, podemos mencionar:

Balancer	
	Balancer - https://app.balancer.fi

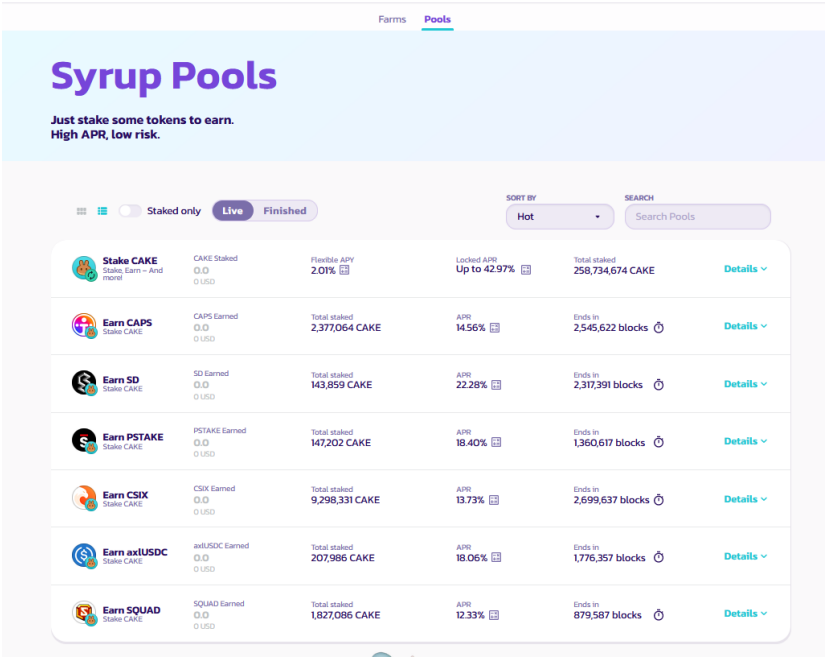
PancakeSwap	
	Pancake swap - https://pancakeswap.finance/

Figura 41 Desarrollos que gestionan Pooles de Liquidez, en el ambiente DeFi

Cultivos de rendimientos (Yield Farming)

Se llama Cultivo de Rendimientos al proceso por el cual un tenedor de cripto-activos, realiza un bloqueo de los mismos en favor de un Contrato Inteligente, por un periodo de tiempo determinado, recibiendo por esto, un interés pagado en criptos.

Las características esenciales de este tipo de práctica que se desarrollan en el ámbito DeFi son:

- puesta a disposición de cripto-activos, que son transferidos a un Contrato Inteligente, por un periodo de tiempo en que permanecen bloqueados, y son utilizados para una actividad generadora de ganancia. Se recibe una recompensa por esta acción de ceder esos cripto-activos.
- en general, los Yield Farming generan rendimientos mayores que otras inversiones DeFi, fundamentalmente por el volumen de cripto-activos que manejan, accediendo a un alto grado liquidez. Sin embargo, es también considerable su exposición a riesgos y volatilidad.
- el rendimiento también se determina en función de las especies de cripto-activos que se aportan al Yield Farming. Los vinculados a Stablecoins, como USDT, USDC, Binance USD, suelen tener mayores rendimientos que los cripto-activos vinculados a Ether, o Bitcoin.

Los rendimientos propuestos por los Yield Farming, suelen medirse con dos índices:

APR - Tasa porcentual anual

APY - Cobertura porcentual anual

La diferencia entre estas medidas se produce porque la APR no tiene en valoración la composición de la inversión que se realiza, mientras que sí lo hace la APY. Por otra parte, la medición de APY incluye la re-inversión de rendimientos obtenidos por la inversión, en función de la cobertura realizada.

Al igual que con muchos otros instrumentos en el mundo cripto, no existen límites taxativos en la terminología, y según sean los autores o fuentes que se accedan, se suele confundir o mimetizar términos. Un caso común de esto, puede ser la difícil distinción de términos que involucren tokens de gobernanza con ICOs y con ADOs. En este punto, no es nuestro interés entrar en una discusión semántica, sino orientar este estudio hacia una clara conceptualización de instrumentos, alternativas y posibilidades.

Hemos hecho esta salvedad, ya que suele confundirse y a veces entremezclar los términos Liquidity Pool y Yield Farming. Esencialmente las diferencias que podemos encontrar entre ambos, son el volumen de cripto-activos que se manejan, siendo los Yield Farming superiores a los Liquidity Pool, y la aplicación de los fondos obtenidos, donde en línea general los LP tienen una finalidad específica (por ejemplo, sustentar un AMM), mientras que los YF suelen sustentar múltiples desarrollos dispares, o incluso apalancar a pooles de liquidez.

Activos Tokenizados

Hablamos previamente sobre la definición de Tokens criptográficos. Mencionamos que Token es la representación digital de un bien o un derecho, dentro de la Cadena de Bloques. Es interesante destacar que al ser el término token, una definición tan amplia de poder comprender cualquier clase de activo a ser digitalizado, puede ser utilizado de forma completamente laxa, como por ejemplo para incluir dentro del mismo a las mismas criptomonedas como el Bitcoin, Ethereum, Litecoin y otras.

Hemos analizado diferentes clasificaciones de Tokens, según su propósito, estatus legal, valor subyacente, visión técnica, propósito. Es decir, una clasificación multidimensional de este complejo abanico de posibilidades.

Sin embargo, una clasificación más intuitiva y funcional en la actualidad, nos lleva a analizarlos como FT - tokens fungibles o, NFT - tokens no fungibles, tomando en cuenta la posibilidad de reemplazo de los mismos, por otro semejante de la misma especie, o no.

De todo esto creemos relevante referenciar un análisis particular sobre los NFT, tokens no fungibles, que han tenido un fuerte desarrollo en los últimos años.

NFT - Tokens no fungibles

Un token no fungible, dentro del universo cripto, se refiere a la representación digital "única" de un bien o derecho del mundo real, para lograr por medio de la tecnología de Blockchain, acceder a una fácil forma de negociación del mismo.

Cuando hablamos de representación digital "única" no estamos haciendo referencia a que el bien no fungible, va a ser representado digitalmente con una sola clave criptográfica. Puede ser que según se desee, se puede fraccionar la representación digital en muchas partes para poder realizar así un fácil acceso a la negociación del bien. Por ejemplo, tokenizar una obra de arte, en 10.000 partes, para poder vender estas cuotas por separado.

Lo que mencionamos con representación digital "única" es que el bien una vez representado digitalmente, no va a poder ser sustituido por otro de igual calidad, sino que solo responderá a la representación digital realizada.

Al bien que se representa digitalmente por medio de un NFT, podemos clasificarlos como bienes reales, que existen fuera de la Cadena de Bloques y, bienes digitales, que pueden ser representados en forma directa en la Blockchain.

Para el primer caso, podemos volver sobre el ejemplo de la representación digital de una obra de arte. En este caso, la tokenización de la misma, permitirá la rápida y fácil negociación de sus tokens sobre la BCT. Pero requerirá, como en todos los casos de bienes "reales", que exista la figura de un "trusted", una organización o persona de confianza, que garantice al adquirente de los tokens respectivos, la entrega del bien real, en caso que lo solicite.

La otra categoría que podemos encontrar es la NFT correspondientes a bienes digitales, como por ejemplo, el denominado "arte digital". En este caso la obra de arte digital, suele quedar almacenada bajo un IPFS, un sistema de registro de archivos digitales, que tiene un funcionamiento semejante al de la Blockchain, en sentido de ser una red distribuida. Esta red solo da acceso al bien digital poseedor de la clave privada con la cual se encriptó ese bien. Esa clave es gestionada por la billetera digital del poseedor, e interactúa con el token criptográfico que se registra en la Blockchain.

La imagen siguiente, presenta a CryptoPunk #5822, figura de arte digital por la que se llegó a pagar 24,2 millones de Euro (conversión del monto de Ethers).

	CryptoPunk #5822, imagen digital firmada digitalmente por su autor, y comercializada por medio de un NFT en la Blockchain de Ethereum. Es una de las obras de arte digital por las que se pagó un monto más alto hasta el momento.

Figura 42 CryptoPunk #5822, figura de arte digital

Otro ejemplo representativo de NFT que se generaron sobre bienes digitales, es la colección de imágenes y videos, que emitió el club de fútbol Manchester United, firmados digitalmente por esa organización para refrendar su carácter de pieza de colección.[61]

Dentro del ámbito particular de DeFi, podemos mencionar como un desarrollo preponderante a los generadores de mercados de NFTs conocidos como “MarketPlaces”.

MarketPlaces

Como vimos los NFT son representaciones digitales de bienes / derechos que, no pueden reemplazarse en forma directa, por uno de la misma especie.

Esto lleva a que los activos representados por estos instrumentos, no tengan tanta facilidad para ser intercambiados, sino que requieran la formulación de mercados específicos.

Siguiendo con el ejemplo que mencionamos, la comercialización en el mundo real de una obra de arte, requerirá de un esfuerzo de acercamiento de las partes interesadas, y todo un proceso de gestión, mucho más complejo que el de un cambio de divisas que hiciéramos en una Casa de Cambios, con mercado transparente. De esta misma manera, los tokens representativos de bienes no fungibles, como la obra de arte que tokenizamos, seguramente

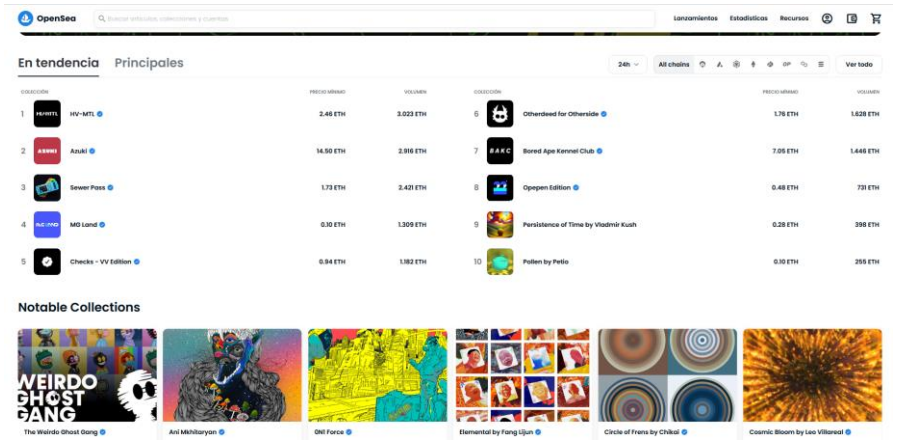
[61] Manchester United - Digital collectibles
https://www.manutd.com/en/digital-collectibles
Observado febrero 2023

necesitará del desarrollo de un mercado específico para juntar las partes que estén interesadas en comprar-vender.

En este punto, es donde, en el ámbito de DeFi, se han creado instrumentos para desarrollar mercados específicos en los cuales se puedan acercar oferta y demanda de tokens digitales representativos de bienes no fungibles.

Estos marketplaces también están configurados para poder realizar la entrega inmediata del bien digital que se representa por tokens criptográficos, como así, agilizar la entrega de bienes físicos, por medio de Trusteds.

Dentro de los desarrollos que gestionan Market Places, en el ambiente DeFi, podemos mencionar:

OpenSea	
	Opensea - https://opensea.io/es

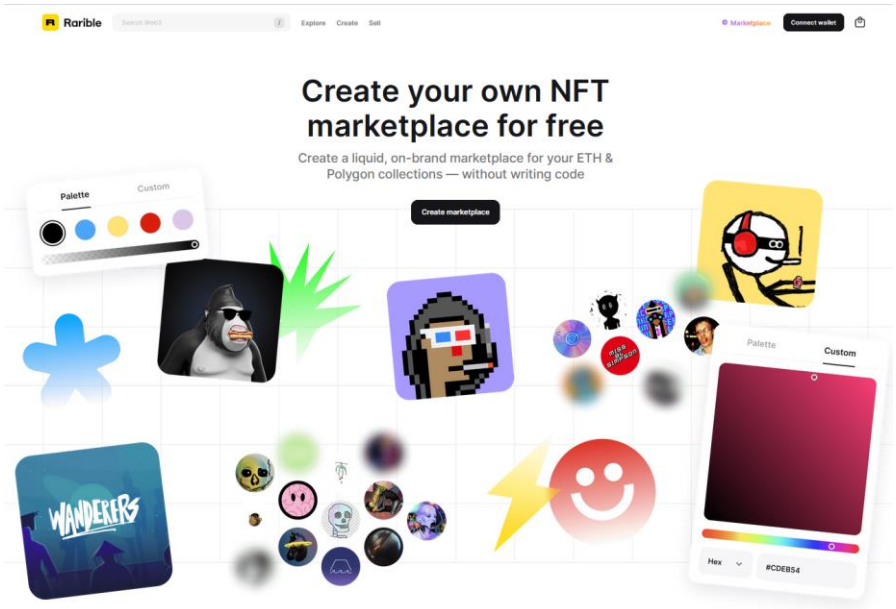
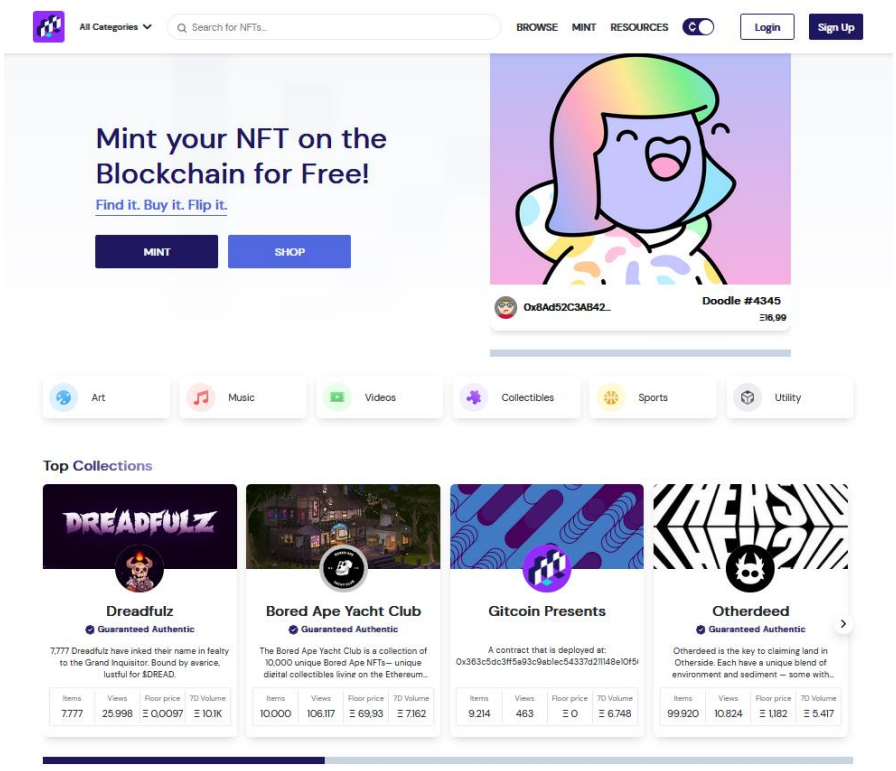
RARIBLE NFT Marketplace	
	Rarible - https://rarible.com/community-marketplace
MINTABLE	
	Mintable - https://mintable.app/

Figura 43 Desarrollos que gestionan Market Places, en el ambiente DeFi

Tokens fungibles

Como mencionamos anteriormente, en una interpretación amplia del término token, cualquier criptomoneda, desde las públicas a las privadas, pueden ser consideradas incluidas dentro de esa definición.

Por esto, dentro de esta enunciación tan amplia, vamos a poner foco específico, en un instrumento muy utilizado dentro del ámbito DeFi, que son las denominadas Stablecoins, o monedas criptográficas estables.

Stablecoins

Una de las características observadas por las criptomonedas públicas, como Bitcoin, Ether, y otras, ha sido su alta volatilidad. Su precio ha variado exponiendo picos y vaivenes de bajas que se producen, en algunos casos en días, y a veces en horas. Esto creó una gran preocupación en la comunidad ya que imposibilita la utilización de estas monedas como medio de pagos, en especial en transacciones internacionales.

Una solución que se busco a esto fue el desarrollo de Contratos Inteligentes que gestionen tokens fungibles, representativos de nuevas criptomonedas, las cuales mantengan paridad con monedas fiat, activos físicos (por ejemplo oro, plata, petróleo) o inclusive otras criptomonedas.

Estas denominadas Stablecoins, o criptomonedas estables, pueden ser clasificadas en:

- **Fiat-collateralized** (con respaldo de monedas fiat): buscan contar con un respaldo que garantice una paridad de 1:1 con el activo subyacente, en este caso una moneda de circulación legal, o una canasta de monedas. Ejemplo de estas Stablecoins son: Tether, Circles y Binance USD
- **Asset-collateralized** (con respaldo de activos): al igual que las anteriores cuentan con un respaldo que garantice paridad, pero en este caso, con algún activo de circulación aceptada, como puede ser oro, plata, soja, petroleo. Ejemplo de estas Stablecoins, podemos mencionar a Paxos.
- **Crypto-collateralized** (respaldadas por otras criptomonedas): fueron desarrolladas para mantener paridad con una canasta de otras criptomonedas. Inicialmente pensado para mitigar el impacto de la caída de precios de una criptomoneda específica, que componen la canasta. La experiencia ha demostrado que no existe un marcado desacople entre criptomonedas, de modo que el conjunto de las mismas suben y bajan sus precios en conjunto. Por ejemplo, la stablecoin Maker de Dai

- **Non-collateralized**, o algorítmicas: en este caso los tokens se emiten con una margen de reserva, administrado por el Contrato Inteligente, para poder hacer operaciones de mint (emitir) como burn (esterilizar) dichos tokens. De esta manera, el Contrato Inteligente “interviene” el mercado de ese token, garantizando su estabilidad en el precio, por medio de oferta y demanda del token. Un ejemplo de Stablecoin algorítima es Ampleforth.

Tokens de Stacking

Un último punto, que consideramos relevante en relación a tokens fungibles, y actualmente está teniendo cada vez más relevancia en la comunidad cripto, es el desarrollo de Tokens de Stacking.

Como ya mencionamos el mecanismo elemental de Blockchain consiste en que cada nodo conectado a la misma, va a validar transacciones, registrarlas y enviarlas a otros nodos para su divulgación. Luego de esto actúan los mineros, quienes se encargan de “diseñar” el próximo bloque que se va a introducir a la Cadena de Bloques conteniendo transacciones.

Para hacer esto, los mineros utilizan un gran poder computacional para asegurar por medio de algoritmos criptográficos la invulnerabilidad de la Blockchain. Pero no es el único fin que tiene la intervención de los mineros. Una de sus funciones, y lo hacen por intermedio de la lógica de la Blockchain, es lograr el mecanismo de “consenso”.

El “consenso” es lo que permite que todos los nodos de la Blockchain vean la misma información al mismo tiempo. Garantiza y resuelve, de este modo, uno de los problemas principales de las redes descentralizadas.

El punto que queremos destacar aquí, es que tanto Bitcoin como Ethereum, iniciaron utilizando el denominado consenso de “Prueba de Trabajo” - POW (Proof of Work). Recientemente Ethereum cambió su mecanismo de consenso, pasando a utilizar la “Prueba de Participación” - POS (Proof of Stake).

El primer mecanismo de consenso que mencionamos, la Prueba de trabajo, hacía competir a los mineros en la resolución de un acertijo criptográfico que les demanda el uso de enormes cantidades de recursos informáticos. De esta manera la Blockchain se aseguraba que el minero que resolvía antes el acertijo, ganase la competencia, incorporando el bloque siguiente a la Blockchain, y gane la recompensa asignada por su trabajo. Este mecanismo es el que sigue sosteniendo la Blockchain de Bitcoin.

En la actualidad, la mayoría de las Blockchain están tratando de migrar sus mecanismos de consenso a algunos diferentes a la Prueba de Trabajo, ya que, entre otras razones, no son eco-sustentables, por la extraordinaria cantidad de energía eléctrica que demanda la tarea de mineración demanda.

En el caso particular de Ethereum se migró recientemente de consenso por Prueba de Trabajo a consenso por Prueba de Participación. ¿En qué consiste el consenso por Prueba de Participación ?

En la POS - Prueba de Participación, se pide a quienes quieran actuar como mineros en la red, que bloqueen una cantidad de criptomonedas (en el caso de Ethereum: Ethers), que servirán para detentar su porcentaje de participación. Cada vez que se debe minerar un nuevo bloque en la Blockchain, se realizará un sorteo aleatorio entre los participantes, a fin de designar cuál será el minero al que le corresponda realizar el trabajo de mineración. Quien mayor participación detente, tendrá un mayor grado de posibilidad de ser elegido. Por supuesto, una vez que el minero realice su trabajo, este deberá ser validado por todos los otros nodos de la red, para que pase a ser incorporado como nuevo bloque en la Blockchain.

Para entender el mecanismo de Prueba de Participación, imaginemos un juego de ruleta de casino, en el cual los jugadores, según un criterio establecido pudiesen “agrupar” números del paño. Supongamos que yo puedo agruparme 18 de los 36 números que participan en cada vez que se tira una bola. El resto de los jugadores que participan, tienen un número asignado de los 18 restantes, cada uno. Matemáticamente yo tendría un 50% de posibilidades de ganar cada vez que se realiza una jugada. ¿ Los otros participantes, quedarían excluidos ? No. Tendrían menos posibilidades, pero en el largo plazo (ley de los grandes números), su número terminaría saliendo. De esta manera, en el mecanismo de Prueba de Participación, quien bloquea la mayor cantidad de criptomonedas, detenta la mayor posibilidad de ser sorteado para realizar la mineración y ganar el premio asignado respectivo por su trabajo. Pero esto no excluye a los otros participantes, que con chances proporcionales a su participación, seguirán beneficiándose cuando sean elegidos por el sorteo.

A este proceso de bloquear una cantidad de criptomonedas para detentar la participación en el trabajo de minería de la Blockchain, se le denomina “stacking”.

Al migrar Ethereum su mecanismo de consenso, de Prueba de Trabajo a Prueba de Participación, abrió el negocio para el desarrollo de aplicaciones que se encargan de agrupar usuarios que están dispuestos a realizar bloqueos de sus tenencias de Ethers, en favor de un Contrato Inteligente, que los va a utilizar para crear grandes pooles de participación (stakes), y de esta forma, ganar chances en los sorteos aleatorios que la Blockchain realiza a fin de determinar mineros. Al finalizar el periodo de bloqueo, el Contrato Inteligente devolverá al aportante, sus Ethers, más una proporción de las ganancias obtenidas por mineración.

Otros instrumentos DeFi auxiliares

Cross-chain Bridges

Los denominados “puentes inter-cadenas” son desarrollos que permiten intercambiar en forma directa valor, representado por diferentes tokens, entre diferentes Blockchains.

En este punto hay que destacar que actualmente se está impulsando fuertemente la utilización de las ZKP - Pruebas de Conocimiento Cero, que mencionamos anteriormente, para perfeccionar la tarea de los Cross-Chain Bridges.

Así como mencionamos anteriormente, que las ZKP se han utilizado para “ofuscar” la trazabilidad entre transacciones en una Blockchain abierta, también se están implementando para permitir la interacción entre Blockchains diferentes, que manejan diferentes tipos de tokens. Si yo deseo interoperar, pasando valores de una Cadena de Bloques a otra, puedo hacer que se emita una Prueba de Conocimiento Cero a ser evaluada por la Blockchain destino. Si el Contrato Inteligente alojado en la Blockchain destino, da por válida la ZKP, puede realizar acciones como reconocerme una “transferencia” de tokens entre Blockchains dispares.

Hoy se está analizando fuertemente este mecanismo, para implementar sistemas de pagos entre CBDCs - Monedas Digitales de Bancos Centrales. Y en este caso, las ZKP pueden ser utilizadas con independencia de que la infraestructura subyacente sea la Blockchain. Se podría estar realizando una transferencia o una operación de compensación entre una CBDC basada en Blockchain, con una CBDC que no posea ese basamento, por ejemplo una CBDC basada en DLT (Registro Contable Distribuido), que no implemente Blockchain.

Perspectivas y conclusiones

En este desarrollo del trabajo hemos querido realizar una mirada a las principales aplicaciones e implementaciones que se han desarrollado últimamente con la tecnología Blockchain.

Como hemos mencionado la tecnología de Blockchain es transversal a todos los tipos de industrias y actividades, encontrando desarrollos en casi todos los ordenes de actividades. Solo para enunciar algunos ámbitos en los que se está utilizando, podemos mencionar, registros médicos, gestión de identidad digital, sistemas de cadena de suministros, votaciones, seguros y otros.

Sin perjuicio de que el desarrollo de una Plataforma NFT/FT para Santa Fe, podría convertirse en el soporte de infraestructura para impulsar implementaciones en todo el abanico de actividades que se pueda imaginar del ámbito provincial, quisimos poner nuestro foco en el

área más sensible, polémica y de efecto multiplicador que tienen esta tecnología, que es el de las DeFi, Finanzas Descentralizadas.

Es relevante destacar que al ser la Blockchain la tecnología desarrollada originariamente para sustentar las criptomonedas, tiene una “concepción nativa” para soportar el modelo de Finanzas Descentralizadas. En el análisis evaluativo de opciones de desarrollo de una Plataforma NFT/FT deberá considerarse preponderantemente el impacto probable que el desenvolvimiento de productos financieros descentralizados podría tener. Tanto desde el punto de vista especulativo, multiplicador o facilitador de acceso fuentes de créditos, de contralor (ya que el gobierno provincial podría auditar los Contratos Inteligentes de la Plataforma), así como también el sigilo de generación de estafas piramidales o de otro tipo que se puedan querer generar.

Desde la óptica de Lending la Plataforma NFT/FT para Santa Fe, podría brindar el soporte para generación de instrumentos que faciliten a pequeñas y medianas empresas, como así también a emprendedores, el acceso al crédito, eliminando la demora, burocracia y costos de la intermediación.

La contrapartida a estos beneficios, entendemos que estará dado por el control necesario que deberá realizarse de la colateralización de préstamos, garantías, e intereses de estos, para evitar que se llegue a situaciones de insolvencia.

En esta intervención deberá considerarse las normas regulatorias que existan (que analizamos previamente). En la actualidad, existe lo que se denomina un “limbo” legal al respecto en nuestro país, aunque existen múltiples iniciativas en estudio de intervención gubernamental.

Otro aspecto destacable, es que los marcos regulatorios que existen a nivel local, regional e internacional, no solo implican la normativa en sí, sino que responden a una cultura y experiencia de años en las gestiones de riesgo, volatilidad, aseguramiento, y otros factores de las Finanzas tradicionales. Si se realizara por medio de la Plataforma NFT/FT una tutela o seguimiento de los Contratos Inteligentes que se desarrollan en la misma para generar instrumentos de Finanzas Descentralizadas, se debería considerar alinear este monitoreo con las mejores prácticas y experiencias de relaciones técnicas (solvencia, liquidez, riesgo y otros), adicionalmente a la regulación directa que se proponga a estos desarrollos.

Otro de los aspectos que analizamos en el presente trabajo, son los denominados “Prestamos instantáneos – Flash Loans”, que tal como mencionamos no tienen colateralización, no requieren de una garantía, y son generados y devueltos dentro del mismo bloque en la Blockchain. Responden fundamentalmente a situaciones puntuales de arbitraje que se presentan en especial por la diversidad de cotizaciones que presentan las criptomonedas.

Estos instrumentos son netamente especulativos, ya que no implican una fuente de financiamiento para actividades productivas, emprendedoras, o ni siquiera de captura de tendencias, alcistas o de baja. Entendemos que será función del Estado evaluar si admitir o no este tipo de prácticas en una futura Plataforma NFT/FT. O tal vez, analizar si gravar impositivamente los rendimientos meramente especulativos que generan estas aplicaciones.

En referencia al Trading de criptomonedas y tokens, la Plataforma NFT/FT puede servir como infraestructura para el desarrollo de aplicaciones locales o regionales que faciliten esto.

De mismo modo, se debería analizar la factibilidad del uso de la Plataforma NFT/FT para desplegar en la misma Contratos Inteligentes vinculados a opciones, futuros, swaps y otros instrumentos derivados para negociar cripto-activos.

El desarrollo de un mercado de derivados, según la experiencia, impulsa a los mercados principales y les provee mayor liquidez. Sin embargo, por las características propias de estos instrumentos financieros, es de esperar que aumente la volatilidad vinculada al mismo. En especial considerando la volatilidad propia y característica de las criptomonedas, y lo que mencionamos previamente, sobre su acople, hasta el momento, con la principal criptomoneda, el Bitcoin.

El desarrollo de mercados automatizados, junto con sus instrumentos subyacentes para crear liquidez (Liquidity Pools, y Yarm Farmings), actuarían en un efecto cascada para el aumento de inversiones en cripto-activos vinculados a la Plataforma NFT/FT.

La característica distintiva de la Blockchain, pensada para mitigar o directamente eliminar la intermediación, juega un rol esencial en los AMM (desarrollo de Mercados Automatizados), ya que los Contratos Inteligentes que los gobiernan calzan operaciones automáticamente, cierran transacciones seguras e incluso, impulsan el desarrollo de mercados.

Sin embargo, consideramos que el riesgo asociado a los AMM, así como a los instrumentos generadores de liquidez, debe ser cuidadosamente analizado, ya que al caer los precios de cripto-activos, como ya ha ocurrido, muchas de las inversiones que se realizan en este tipo de instrumentos financieros DeFi, pueden quedar debajo de la tasa de corte, y hacer que pequeños ahorristas, o público en general, pierda sus posiciones.

En referencia a la Tokenización de activos, en especial a la de obras de arte digital, podemos preguntarnos, haciendo una observación de CryptoPunk #5822 cuya imagen incluimos anteriormente, si intrínsecamente la obra puede tener un valor de 24.2 millones de Euro, como se pagó por ella.

Tal vez la respuesta debe verse por la originalidad de ser una de las primeras obras de arte digital comercializada por medio de la Blockchain. Los coleccionistas, podemos suponer, que valoran a la misma como la primera de una tendencia irreversible, por la cual el arte (primeramente digital, pero el arte del mundo real, también) se comience a negociar desde la tecnología de Blockchain. Hay un marcado crecimiento a nivel mundial de los mercados de NFT.

Esta es una consideración que no debe soslayarse al evaluar la factibilidad y conveniencia del desarrollo de la Plataforma NFT/FT para Santa Fe.

Y por último, dentro del análisis de los instrumentos financieros que se pueden desarrollar en el ámbito DeFi – Finanzas Descentralizadas de la Plataforma NFT/FT, se deberá considerar la tokenización de activos fungibles. En especial, ya que, en la provincia de Santa Fe, y desde el ámbito privado, ya se ha realizado una experiencia exitosa a nivel regional, en la tokenización de cosechas. El desarrollo de Agrotoken, un token criptográfico de fácil

negociación por medio de la Blockchain, que tiene como activo subyacente, los certificados de depósito de cereales.

Relevamiento y análisis de las variantes de plataformas basadas en Blockchain, para el desarrollo, despliegue e implementación de NFT y FT.

Introducción

En el presente apartado vamos a analizar las decisiones de infraestructura de Blockchain que se deberían abordar en el proyecto de desarrollo de la Plataforma BCT para NFT/FT.

Para esto vamos a analizar, primeramente las opciones de diseño de la plataforma Blockchain que sustentará el proyecto, en función de:

- el tipo de Cadena de Bloques (en relación al acceso a la red),
- el anonimato de acceso a la red y realización de transacciones,
- los tipos de mecanismos de consenso.

Luego, volveremos con la enunciación de desarrollos del ecosistema DeFi, pero un abordaje conceptual diferente, el sugerido por el BIS - Bank of International Settlements. Esto nos servirá, en siguientes trabajos, para evaluar si las diferentes tipos de soluciones de infraestructura Blockchain que planteamos, serán eficientes para sustentar el desarrollo de esos productos financieros de carácter digital.

Primera aproximación: tipos de Blockchain según su acceso

Podemos clasificar a las Blockchain, según el acceso y permisos que ofrecen a sus usuarios en:

- Blockchain no-permisionadas (públicas)
- Blockchain permisionadas (privadas)
- Blockchain de consorcio
- Blockchain híbridas.

1. Blockchain no permisionada (pública):

El funcionamiento y acceso a este tipo de Blockchain es transparente y abierto. No tienen restricciones de entrada. Son totalmente descentralizadas y con participación democrática

entre todos los miembros. Cualquier usuario puede acceder a la totalidad de la información registrada en la red. Sin embargo, ningún dato personal o modo de identificar a actores se registra en la red, ya que los usuarios son solo conocidos por las claves criptográficas públicas que utilizan para actuar. Ejemplos de cadenas de bloques públicas son Bitcoin, Ethereum Litecoin, Monero y Zcash.

Uno de los principales problemas vinculados a este tipo de Blockchain es el de la escalabilidad, ya que no son susceptibles de tolerar una gran cantidad de transacciones.

Algunas de las características más destacadas, que nos permiten conceptualizar a este tipo de Cadena de Bloques son:

Participación abierta: Las Blockchain no-permisionadas permiten que cualquier persona pueda unirse a la red, participar en la validación de transacciones y realizar transacciones en la cadena de bloques sin necesidad de una autorización previa. Esto significa que cualquiera puede convertirse en un nodo de la red y contribuir al consenso y la seguridad de la cadena de bloques.

Transparencia y auditabilidad: En una blockchain no permisionada, todas las transacciones y datos registrados en la cadena de bloques son transparentes y públicamente visibles. Cualquier persona puede acceder a la información de la cadena de bloques y verificar la integridad de las transacciones. Vale destacar que el concepto de auditabilidad que mencionamos para las blockchain no-permisionadas, responde al paradigma de auditoría continua, es decir sistemas que realizan paso por paso (en este caso transacción por transacción), la auditoría de identidad y verificación de sus acciones. No existe dentro de las Blockchain no-permisionadas, un servidor con permisos especiales (administrador), que en un segundo momento valide transacciones. Sin embargo, al registrar la Cadena de Bloques, la totalidad de sus transacciones y el encadenamiento de estas, cualquier usuario o interesado, puede auditar, identidad, trazabilidad y verificación de transacciones. Esto brinda mayor transparencia y permite una mayor confianza en la red[62].

Consenso descentralizado: En una blockchain no permisionada, el consenso se logra a través de algoritmos de consenso descentralizados, como la Prueba de Trabajo (Proof of Work) o la Prueba de Participación (Proof of Stake). Estos algoritmos permiten que los nodos de la red lleguen a un acuerdo sobre el estado de la cadena de bloques sin la necesidad de una autoridad centralizada. Como mencionaremos en mayor detalle más adelante (cuando desarrollemos el tema de consensos), es el acuerdo en que se basa la Blockchain para coordinar la información que todos los nodos de la red ven, asegurando de esta manera, la

[62] Furneaux, N. (2018). *Investigating cryptocurrencies: understanding, extracting, and analyzing blockchain evidence*. John Wiley & Sons.

tolerancia de la Blockchain para que se pueda falsificar, modificar o insertar información apócrifa de transacciones[63].

Resistencia a la censura: las blockchain no-permisionadas son resistentes a la censura debido a su naturaleza descentralizada. Como no hay una autoridad centralizada que controle la red, resulta casi imposible censurar transacciones o modificar datos registrados en la cadena de bloques.

Seguridad y robustez: este tipo de Blockchain, están diseñadas para ser seguras y resistentes a ataques maliciosos. La descentralización y el uso de algoritmos de consenso permiten una mayor seguridad, ya que los atacantes tendrían que controlar una mayoría significativa de los nodos para poder alterar la cadena de bloques[64].

Tokenización y criptomonedas: estas redes abiertas suelen permitir la creación y el intercambio de tokens y criptomonedas. Estos activos digitales pueden ser utilizados para representar valor, realizar transacciones y ejecutar contratos inteligentes en la cadena de bloques. Tal es el caso de la Blockchain Ethereum, que es la red que aloja más contratos inteligentes en el mundo[65].

Innovación y desarrollo comunitario: Las Blockchain no-permisionadas fomentan la innovación y el desarrollo comunitario. Cualquier persona puede contribuir al desarrollo de aplicaciones descentralizadas (DApps), contratos inteligentes y mejoras en el protocolo de la cadena de bloques, lo que permite una amplia colaboración y avance tecnológico.

Por todo esto podemos ver que, las Blockchain no-permisionadas permiten: participación abierta, transparencia, consenso descentralizado, resistencia a la censura, seguridad, tokenización, sustentar criptomonedas, y fomento de la innovación y el desarrollo por medio de la comunidad de usuarios y desarrolladores que la impulsan.

---

[63] Norman, A. T. (2017). *Cryptocurrency Investing Bible: The Ultimate Guide About Blockchain, Mining, Trading, ICO, Ethereum Platform, Exchanges, Top Cryptocurrencies for Investing and Perfect Strategies to Make Money*. CreateSpace Independent Publishing Platform.

[64] Mougayar, W. (2016). T*he business blockchain: promise, practice, and application of the next Internet technology.* John Wiley & Sons.

[65] Dannen, C. (2017). *Introducing Ethereum and solidity* (Vol. 1, pp. 159-160). Berkeley: Apress.

2. Blockchain permisionadas (privadas):

La aparición de este tipo de Blockchain se inició en el entorno empresarial, bancos e instituciones que necesitan realizar procesos de estandarización y necesitan control de datos e identidad de los usuarios (identidad soberana de usuario, no solamente la autoria de transacciones).

Las Blockchain permisionadas, en general, surgen de la modificación del código fuente de Blockchain públicas, con el fin de que el acceso sea restringido y administrado con reglas privadas. Las transacciones realizadas en una Blockchain privada se ejecutan entre sus miembros (P2P). Poseen la vinculación de nombre e identidad de los involucrados a las transacciones, lo que permite saber quienes intervienen en la transacción. Las cadenas de bloques privadas tienen la ventaja de tolerar una gran cantidad de transacciones (alta escalabilidad). Sin embargo, en relación a la descentralización, la misma declinan en favor de una mayor centralización, y con ello puede presentarse un mayor grado a fallas de seguridad y ataques que en las Blockchain no-permisionadas. Ejemplos de estas cadenas de bloques son Hyperledger (IBM), TradeLens, Corda (R3);

Sus características más destacadas son:

Acceso restringido: en las Blockchain permisionadas, solo las entidades autorizadas tienen permiso para participar en la validación de transacciones y en la creación de nuevos bloques.

Mayor escalabilidad: al estar diseñadas para un número limitado de nodos, las Blockchain permisionadas pueden manejar un mayor número de transacciones y ofrecer una mayor velocidad de validación.

Mayor eficiencia energética: debido a que se utilizan menos recursos en la validación de transacciones, las Blockchain permisionadas suelen ser más eficientes energéticamente.

Mayor privacidad: como los nodos son controlados por entidades autorizadas, se puede tener un mayor control sobre las transacciones e incluso, establecer niveles de privacidad en la información de la red.

Menor descentralización: como el control está enfocado en una entidad, la descentralización es menor que en las Blockchain no-permisionadas y esto expone puntos de vulnerabilidad que podrían usarse para hackearlas. En especial a los nodos administradores (con permisos especiales) que serían el blanco deseado por los ataques[66].

[66] Baset, S. A., Desrosiers, L., Gaur, N., Novotny, P., O'Dowd, A., Ramakrishna, V., ... & Wu, X. B. (2019). *Blockchain Development with hyperledger: build decentralized applications with hyperledger fabric and composer*. Packt Publishing Ltd.

Aplicaciones empresariales: las Blockchain permisionadas se utilizan con mayor frecuencia en aplicaciones empresariales, como en las DeFi - Finanzas Descentralizadas, la gestión de la cadena de suministro, la gestión de activos y la gestión de identidad.

3. Blockchain Híbrida:

Es una combinación de las características de las Blockchains no-permisionadas y las permisionadas

Mezclan modelos de privacidad fragmentados e incluso pueden usar sus propios tokens, que es la reproducción digital de un activo financiero real en la red, similar a las criptomonedas. Algunas de ellas, como XinFin, permiten configurar operaciones que corran en un ambiente permisionado, mientras que otras operaciones corran en un ambiente no-permisionado, ambos compartiendo la misma Cadena de Bloques raíz. Ejemplos de este tipo de Blockchain son XRP Ledger (Ripple) y XinFin.

Algunas características y elementos de las Blockchain híbridas son:

Control de acceso: Las Blockchain híbridas permiten un control de acceso flexible. Algunas partes de la red pueden ser permisionadas, lo que significa que solo entidades autorizadas tienen acceso y pueden participar en la validación de transacciones. Esto proporciona mayor privacidad y control en áreas donde se requiere confidencialidad o regulaciones específicas.

Zonas públicas: este tipo de redes híbridas pueden tener áreas o zonas públicas en las que cualquier persona puede unirse y participar en la red. Estas zonas públicas pueden ofrecer transparencia y descentralización similares a las Blockchain no-permisionadas.

Consenso: las Cadenas de Bloques híbridas pueden utilizar diferentes algoritmos de consenso según la zona o área de la red. Por ejemplo, en la zona permisionada, se puede utilizar un algoritmo de consenso más eficiente y escalable, como Prueba de Autoridad (Proof of Authority), mientras que en la zona pública se puede utilizar un algoritmo de consenso más descentralizado, como Prueba de Trabajo (Proof of Work) o Prueba de Participación (Proof of Stake).

Flexibilidad: Las Blockchain híbridas ofrecen flexibilidad en términos de configuración y adaptación a diferentes necesidades y requisitos. Pueden ajustar los niveles de permisos, la participación y los algoritmos de consenso según los casos de uso específicos.

Aplicaciones empresariales: Las Blockchain híbridas son particularmente útiles para aplicaciones empresariales que requieren un equilibrio entre privacidad, control y transparencia. Pueden ser utilizadas en casos de uso como la gestión de la cadena de suministro, la gestión de activos digitales y la implementación de soluciones financieras.

4. Blockchain de Consorcio (federada):

Las Blockchain de consorcio, o también llamadas federadas, se caracterizan por ser operadas y mantenidas por un grupo de organizaciones o entidades en lugar de ser administrada por una sola entidad centralizada. Estas organizaciones colaboran para formar una red de blockchain compartida y trabajan juntas para mantener y validar las transacciones en la cadena de bloques.

El modelo surgió por la necesidad de preservar la transparencia, la descentralización y la facilidad de acceso del modelo de Blockchain no permisionada, pero al mismo tiempo continuar con poder de control por medio de varios nodos administradores.

El caso de uso más ejemplificativo de una Blockchain de consorcio, podemos considerar que es el de un sistema de transferencias bancarias. Todos los bancos participantes actúan como servidores con permisos privilegiados, es decir como administradores. De esta manera cada uno de los bancos tiene el dominio y la información de sus cuentas, y puede por medio de la Blockchain de consorcio, recibir, validar y registrar transacciones generadas en cuentas gobernadas por los otros bancos participantes de la red.

Por ejemplo, utilizando una Blockchain de Consorcio, basada en Corda R3, se realizaron pruebas de transferencias internacionales entre algunos bancos brasileros y bancos europeos. De esta manera, cada entidad bancaria poseía un nodo de la red, con permisos de administrador, que gobernaba las cuentas de sus clientes (nodos selladores - sin permisos de administrador).

De esta manera, esos bancos, o en otras situaciones las entidades u organizaciones que controlan el acceso y la privacidad de las transacciones pueden definir, si la visibilidad y las transacciones serán restringidas a usuarios privilegiados, o estarán disponibles públicamente.

Algunos ejemplos de Blockchain de consorcio son Hyperledger Fabric (HF), Quorum y Corda R3.

Las principales características distintivas de este tipo de Blockchain son:

Participación restringida: a diferencia de las Blockchain no-permisionadas, las Blockchain de consorcio tienen una participación restringida. Solo un grupo determinado de organizaciones, previamente consensuadas y con permisos, pueden unirse a la red y operar como nodos administradores, definiendo también los usuarios no administradores a quienes se les habilitará acceso. Esto permite un mayor control y confianza entre las partes participantes.

Mayor escalabilidad y rendimiento: las Blockchain de consorcio suelen tener una mayor escalabilidad y rendimiento en comparación con las Blockchain no-permisionadas. Al limitar la cantidad de nodos y participantes en la red, se reducen los tiempos de confirmación de transacciones y se mejora la eficiencia de la Blockchain.

Eje en privacidad y confidencialidad: una característica clave de las Blockchain de consorcio es la capacidad de implementar mecanismos de privacidad y confidencialidad en la red. Los datos y las transacciones pueden estar restringidos solo a las partes involucradas en la transacción, lo que es especialmente relevante en aplicaciones empresariales donde se requiere confidencialidad de la información. Sobre todo a aquellas aplicaciones vinculadas a métodos de camino crítico, y de protección de datos sensibles.

Governanza y control compartido: en una blockchain de consorcio, las organizaciones participantes colaboran en la toma de decisiones y el gobierno de la red. Establecen reglas y protocolos comunes que rigen el funcionamiento de la cadena de bloques y la resolución de conflictos. Esto permite un mayor nivel de confianza y cooperación entre las organizaciones participantes.

Orientadas a uso empresarial: las Blockchain de consorcio son ampliamente utilizadas en aplicaciones empresariales donde existe la necesidad de compartir datos y llevar a cabo transacciones entre múltiples organizaciones. Esto incluye casos de uso como el que mencionamos previamente para realizar transferencias bancarias, pero también podemos citar casos de uso en la gestión de la cadena de suministro, la trazabilidad de productos, el intercambio de datos confidenciales y la colaboración en industrias específicas.

Estas Blockchain proporcionan mayor escalabilidad, privacidad y confidencialidad en comparación con las Blockchain públicas. Son adecuadas para aplicaciones empresariales donde se busca la colaboración entre organizaciones que tienen intereses comunes, brindando un mayor grado de confianza y control compartido

Comparativa de los tipos de Blockchain según su acceso

Haciendo una comparación de los cuatro tipos de Blockchain que hemos analizado, podemos observar (a modo de resumen):

Características	Blockchain No Permisionada	Blockchain Permisionada	Blockchain de Consorcio	Blockchain Híbrida
Acceso	Público. Participación abierta y descentralizada	Restringido. Control y selección de participantes	Restringido. Control y selección de participantes	Variable según la actividad que realicen. Flexibilidad en la gestión de participantes
Seguridad	Alta seguridad debido a la descentralización y criptografía	Menor que la Blockchain no permisionada. Mayor control y capacidad para implementar medidas de seguridad personalizadas	Diferentes puntos de ataque según sean los nodos administradores que se asignen.	Variable: depende de la configuración y características específicas
Escalabilidad	Limitada debido a la necesidad de validar todas las transacciones	Mejorada en comparación con no permisionada	Mejorada en comparación con no permisionada	Variable: depende de la configuración y características específicas
Velocidad	Variable, generalmente más lenta que las permisionadas	Mejorada en comparación con no permisionada	Mejor en comparación con no permisionada	Variable: depende de la configuración y características específicas de cada

				operación que se realiza
Privacidad	Alta, ya que los datos se comparten de forma anónima y seudónima	Variable, depende de las medidas de privacidad implementadas	Variable, depende de las medidas de privacidad implementadas	Variable: depende de la configuración asignada a las transacciones que se realizan
Transparencia	Alta, ya que todas las transacciones son visibles para todos	Variable, depende de las medidas de privacidad implementadas	Variable, depende de las medidas de privacidad implementadas	Variable: depende de la configuración y características específicas
Participantes	Descentralizados	Controlado	Controlado	Variable
Validación	Consenso descentralizado	Consenso controlado	Consenso controlado	Consensos mixtos, según el área de implementación (pública o privada)
Transparencia	Alta	Variable	Variable	Variable
Ejemplos de Uso	Bitcoin, Ethereum, Litecoin, Monero y Zcash	Hyperledger Fabric, Corda-R3	Corda(R3), Quorum	XRP Ledger (Ripple) y XinFin

Consideraciones a la elección de tipo de Blockchain

A los efectos de analizar y estructurar las decisiones que se deberían afrontar de parte de los gestores del proyecto de desarrollo de Plataforma BCT para NFT/FT de provincia de Santa Fe, en lo que respecta al tipo de Blockchain a adoptar, vamos a separar las mismas en dos opciones: en base a tokens nativos, y en base a tokens generados por Contratos Inteligentes.

Decisiones en base a tokens nativos.

Como mencionamos previamente, la tecnología de Blockchain se inició primigeniamente por medio de la Blockchain Bitcoin, que hasta el día de hoy sigue siendo la criptomoneda más utilizada en el mundo.

Con posterioridad a esto, al verse las grandes empresas y organizaciones en la necesidad de restringir y gobernar las operaciones que por medio de esta tecnología se iban a realizar, en sus redes, se pensó en clonar las Blockchain públicas, pero modificando el código fuente de su software, de modo de implementar nuevas Cadenas de Bloques diferenciadas con nodos “selladores”, y nodos “administradores”. Estos últimos con permisos especiales que los habiliten a aceptar usuarios y transacciones en la Blockchain.

De este modo surgieron las Blockchain permisionadas, o también denominadas Blockchain privadas.

Con el devenir y la aceptación de uso de la tecnología, se fueron creando Blockchain de Consorcio, como una variante de las Blockchain permisionadas, facilitando la gobernanza de este tipo de Cadena de Bloques, por medio de varios nodos administradores.

Por último, como vimos, en la actualidad se está impulsando el desarrollo de las Blockchain híbridas, también como variante a las Blockchain permisionadas, pero en este caso, fusionando el ambiente público y privado en una misma Cadena de Bloques, que permita a los usuarios realizar determinadas operaciones al igual que lo hacen en las Blockchain públicas, y otras operaciones en el ambiente privado de la red.

En principio, y basándonos en las premisas básicas del proyecto de desarrollo de una Blockchain para NFT/FT de la provincia de Santa Fe, podemos descartar de lleno la utilización de una Blockchain pública. No referimos en este planteo a la posibilidad de clonar una Blockchain pública, pero sin modificar su código, designando nodos administradores, con permisos especiales.

Podemos descartar esta opción, ya que no tendría sentido clonar exactamente igual a una red pública, de la cual no se pueda tener gobernanza sobre usuarios y transacciones, como así también sobre los Contratos Inteligentes que se desplieguen en la misma.

Sin embargo, veremos en el apartado siguiente a esta cuestión que una variante a esta decisión es la desarrollar tokens generados por Contratos Inteligentes sobre una Blockchain pública.

Al haber descartado la opción 1 (Blockchain no permisionada), de las cuatro que analizamos, nos queda el análisis de las otras 3 opciones.

En estas 3 situaciones podemos volver a bifurcar la decisión en dos opciones.

Consideremos que los 3 últimos modelos, que hasta ahora analizamos, son clonaciones de Blockchain públicas. Para ese fin se procedió a la modificación de los permisos asignados a determinados nodos. A estas variaciones de Blockchain públicas en permisionadas, se debería evaluar si hacerlas en forma directa (clonar una Blockchain pública para convertirla en privada), o utilizar Blockchain privadas ya desarrolladas.

En este último caso estamos hablando de un “framework” de desarrollo de Blockchain, es decir, un proveedor de servicio (puede ser pago o gratuito), que nos brinda la posibilidad de trabajar sobre una Blockchain privada ya desarrollada, pero configurable. Este es el caso de la mayoría de los ejemplos que mencionamos anteriormente en la comparativa de tipo de Blockchain: Hyperledger Fabric, Corda R3, Quorum…

Estos “frameworks” de Blockchain configurables tienen un extraordinario nivel de desarrollo y maduración en términos de software. Solo para mencionar algunas referencias, Quorum es una modificación del software original desarrollado por Ethereum y gestionado originalmente por GP Morgan para implementar soluciones al sector bancario y financiero. Actualmente está gestionada por Consensys, cuyo director fue co-fundador de Ethereum con Vitalik Buterin. Hyperledger es un consorcio de desarrolladores donde, entre otros, trabajan IBM y Linux Red Hat.

Tomando en cuenta el esfuerzo de programación que implica clonar y modificar el código fuente de una Blockchain pública para convertirla en permisionada, la escasez de profesionales en sistemas con capacidad de programar en el dominio de Blockchain, como así también las exhaustivas pruebas de testing que se deben realizar a la Cadena de Bloques antes de ponerla en funcionamiento, creemos que utilizar algunas de las opciones de Blockchain permisionadas ya desarrolladas y configurables (frameworks de BCT), puede ser la opción más ventajosa para el proyecto.

Pero no deberíamos cerrar nuestro análisis de opciones en este punto, sino, que como ya mencionamos otra posibilidad de definición de la infraestructura de BCT es la de utilizar una

Blockchain pública, y desarrollar la Plataforma, por medio de tokens generados por Contratos Inteligentes, es decir, crear nuestro propio ecosistema de Blockchain.

Decisiones en base a tokens generados por Contratos Inteligentes.

Previo al presente trabajo se realizó un relevamiento del ecosistema DeFi, donde pudimos analizar la diversidad de desarrollos hechos en el área de Finanzas Descentralizadas sobre la tecnología de Blockchain.

La mayoría de estos instrumentos financieros digitales, se han desplegado sobre la Blockchain Ethereum, y son gobernados por Contratos Inteligentes que corren sobre esta. También mencionamos en trabajos anteriores, que si bien la Blockchain Ethereum mantiene su criptomoneda, el Ether, y se hacen sobre ella transacciones al igual que en cualquier otro tipo de criptomoneda de BCT pública, su verdadero perfil es el de una red de infraestructura tecnológica basada en Blockchain, donde por medio de contratos inteligentes se pueden crear, divulgar y enriquecer todo tipo de ecosistemas BCT.

Por todo esto, una opción que se debería evaluar para desarrollar la Plataforma BCT para NFT/FT, es la posibilidad de plasmar la misma por medio de una serie de Contratos Inteligentes desplegados sobre la Blockchain Ethereum.

Estos contratos inteligentes podrían establecer las limitaciones y restricciones que se consideren convenientes para que los usuarios actúen con la Plataforma. En otras palabras, crear por medio de una serie de Contratos Inteligentes, los instrumentos financieros digitales que el gobierno de la provincia ofrece. Se estaría de este modo creando un ecosistema, o dominio, donde se permitiría a los usuarios utilizar esos instrumentos financieros digitales, desarrollados por la provincia, en un entorno controlado y sin la necesidad de crear una Blockchain permisionada propia.

Recientemente, en marzo de 2023, la Blockchain Ethereum incorporó una modificación sustancial por medio del denominado ERC-4337, la posibilidad de realizar abstracción de cuentas. De esta forma la red Ethereum, permite gestionar la tenencia de criptomonedas de un usuario por medio de un conjunto de Contratos Inteligentes, predefinidos por el consorcio de Ethereum (Ethereum Foundation), y altamente testeados por la comunidad. Entre otras cosas, estos Contratos Inteligentes configurables, heredables y programables, permiten la recuperación social de claves privadas, multi-sign, creación de listas negras y listas blancas de cuentas, límite de transacciones, y otros.

Contando con este adelanto que ya está funcionando plenamente en la Blockchain Ethereum, el gobierno de la provincia de Santa Fe, en relación al proyecto que estamos analizando,

podría utilizar uno de estos Contratos Inteligentes como “entrypoint” (puerta de acceso), a los desarrollos que el gobierno realice para el funcionamiento de la Plataforma.

Ese punto de acceso al dominio o ecosistema de los instrumentos financieros digitales que desarrolló la provincia de Santa Fe, podría disponer de los primeros requerimientos de usos.

Por ejemplo, si un nuevo usuario quiere acceder a esos instrumentos financieros digitales, debería enviar un file digital a un repositorio descentralizado (IPFS)[67], y esperar el visado de algún funcionario provincial, quien, al brindar acuerdo, aprobaría la cuenta del usuario (la cuenta se gestionaría por medio de un contrato inteligentes ERC-4337). Para brindar esa aprobación el funcionario debería controlar el cumplimiento de los requerimientos de KYC (Conozca a su cliente), que interponga la provincia, tales como DNI/Pasaporte, historial de crédito, constatación de domicilio, y otros.

Blockchain y Frameworks para el desarrollo de la Plataforma

En el análisis anterior realizamos un relevamiento de las diferentes tipologías de Blockchain basados en el análisis del acceso a las mismas, como permisionadas, no-permisionadas, de consorcio e híbridas.

Mencionamos también, dentro de estas categorías algunos ejemplos de Blockchain públicas que se podrían clonar para convertirlas en permisionadas, y de “frameworks”, es decir Blockchain configurables, que facilitan el cumplimiento de requerimientos deseado de una blockchain permisionada, pero sin, o con muy poca modificación de código fuente.

Vamos a ver en esta sección, con un poco más de detalle, las características de las principales Blockchain que enrolan en estas categorías:

Ethereum

En el año 2013, un chico de 23 años llamado Vitalik Buterin propuso una plataforma Blockchain sobre la cual los desarrolladores pudieran implementar Contratos Inteligentes.

Pequeños programas que se registren en la Cadena de Bloques y sean ejecutados por esta. La implementación de esta Blockchain se gestó en 2014, recibiendo el nombre de Ethereum y fue financiada por Crowdfunding en línea (Crowdfunding).

[67] IPFS - Interplanetary File System
https://ipfs.tech/
Observado: mayo 2023

De esta manera Ethereum ascendió un escalón por arriba de las criptomonedas. Es una plataforma descentralizada de código abierto que permite enviar criptomonedas a cualquier usuario al costo de una pequeña tarifa en su criptomoneda nativa, el “Ether”. Pero además, tiene la capacidad de ejecutar Smart Contracts y aplicaciones descentralizadas (Contratos Inteligentes) sobre su plataforma Blockchain, sin restricciones, fraude o intervención de terceros, de manera confiable, es decir, que no puede ser manipulado ni modificado.

En Ethereum, existe lo que se denomina EVM (Ethereum Virtual Machine). Una máquina virtual que forma parte de su Cadena de Bloques y se encarga de ejecutar los contratos inteligentes, previamente desplegados en ella.

Al ser Ethereum una Blockchain pública y descentralizada, cada nodo de la red permite, con el estado de la máquina virtual, guardar una copia de ese estado. De esta manera, cada nuevo bloque insertado en Ethereum Blockchain se incorporará a la copia global de la red existente en todos los nodos de esta, conteniendo las transacciones que se realizan en la misma, como el estado de la máquina virtual.

El almacenamiento de las transacciones que se realizan en la Blockchain Ethereum, se basa en un sistemas de “Saldos” vinculados a las cuentas asociadas, que es un concepto diferente a cómo gestiona esta cuestión la Blockchain de Bitcoin.

En referencia a los Contratos Inteligentes, estos son documentos escritos en un lenguaje de máquina virtual (Bitcode), es decir, se implementan con un lenguaje de programación y se ejecutan en una máquina virtual Ethereum (EVM) con los registros pactados en el contrato a partir de una secuencia de reglas pre-programadas. La ejecución de estos contratos se paga en tarifas que van de acuerdo con el volumen de la transacción en bytes, así como la potencia computacional correspondiente. Estas tarifas se denominan Gas, las cuales se encuentran acordes al desempeño computacional para realizar diversas operaciones en la red.

La medición del esfuerzo computacional en la red Ethereum la realiza por medio de Gas (tarifa en Ethers) para ejecutar diversas operaciones como transacciones con su criptomoneda (Ether) y Smart Contracts.

Por ejemplo, el Gas serán las tarifas que deben pagarse a mineros, para ejecutar una Oferta Inicial de Monedas (ICO), las cuales son tokens (activos virtuales) que simbolizan la coparticipación en las ganancias o servicios de una empresa o emprendimiento. Las ICOs normalmente siguen el estándar ERC-20 y actúan en el ecosistema Ethereum.

Uno de los momentos más traumáticos relacionados con el desenvolvimiento de la Blockchain de Ethereum, fue el ataque a un Contrato Inteligente desplegado sobre su Blockchain, ocurrido en 2016, conocido como "The DAO Hack", en el que los hackers robaron aproximadamente 3,6 millones de Ether, por haber detectado una falla en la que incurrió el programador de dicho Contrato Inteligente.

Otro evento similar a The DAO Hack fue el ataque a Uniswap, que es un Contrato Inteligente desplegado para crear un protocolo para intercambiar tokens en Ethereum. Ante este escenario, los autores advierten sobre la demanda que existe en la comunidad Ethereum de promover e incentivar las auditorías serias y exhaustivas sobre los Contratos Inteligentes que se desarrollan, antes que los mismos sean desplegados en su Cadena de Bloques, ya que luego de esto, no hay forma de modificarlos o corregir sus acciones.

La blockchain Ethereum es conocida por su capacidad para ejecutar contratos inteligentes, que son programas autónomos que se ejecutan automáticamente cuando se cumplen ciertas condiciones predefinidas. Estos contratos inteligentes permiten la creación de aplicaciones descentralizadas y la automatización de acuerdos y transacciones. Son la base sobre la que se ha desarrollado la mayor parte del ecosistema de instrumentos financieros digitales que conocemos, además de otros dominios, como cadena de suministros, registros médicos, IOT (Internet de las cosas), sistemas de identidad digital, y una enorme cantidad de actividades e industrias que utilizan la tecnología de Blockchain.

Dando una mayor profundidad al aspecto técnico, Ethereum utiliza el lenguaje de programación Solidity, que es Turing completo. Esto significa que los desarrolladores tienen una amplia flexibilidad para crear aplicaciones complejas ya que prácticamente no tienen restricciones para poder llevar a cabo la representación digital de cualquier proceso de negocio.

Por medio de estas herramientas, Ethereum facilita la creación de tokens personalizados a través del estándar ERC-20, que permite a los usuarios crear y gestionar sus propios activos digitales en la plataforma. El estándar ERC-20, actúa como un “template” (una plantilla), configurable y heredable, para desarrollar nuestras propias criptomonedas, representadas por tokens fungibles. Esto ha dado lugar a la proliferación de criptomonedas y la realización de ofertas iniciales de monedas (ICO) para financiar proyectos y empresas.

Ethereum ha fomentado la estandarización a través de los estándares ERC. No solamente a través del ERC-20 que mencionamos, sino también por medio ERC-721 (para tokens no fungibles) y ERC-1155 (para tokens híbridos), y muchos otros más. Estos estándares han facilitado la creación, intercambio y gestión de diferentes tipos de activos digitales en la plataforma Ethereum.

En una mirada más amplia al mero funcionamiento técnico, Ethereum se ha convertido en un estándar para la interoperabilidad entre Blockchain. A través de tecnologías como los puentes de cadena (cross-chain bridges) y los contratos de bloqueo (lock-up contracts), Ethereum permite el intercambio de activos y datos entre diferentes Blockchain, lo que fomenta la colaboración y la sinergia entre los ecosistemas blockchain. Incluso, actualmente se está orientando la red, hacia la incorporación nativa (en la EVM - Ethereum Virtual Machine) del procesamiento de ZKPs (pruebas de conocimiento cero), lo cual incrementará sustancialmente la posibilidad de intercambiar criptomonedas y procesos (ejecución de Contratos Inteligentes), con otras Blockchain.

Otro fuerte pilar que se ha observado, en la adopción masiva de Ethereum, es que cuenta con una gran y activa comunidad de desarrolladores y usuarios. La plataforma es de código abierto y fomenta la colaboración y la contribución de la comunidad para mejorar y expandir sus capacidades. Esto ha llevado a un rápido crecimiento de aplicaciones descentralizadas y proyectos basados en Ethereum. Esto, como mencionamos anteriormente, hace que podamos considerar a Ethereum, no solamente como una red de criptomonedas (que lo es), o como una blockchain con capacidad de desplegar Contratos Inteligentes (también lo es), sino considerarla como una red de acceso a toda una gran gama de infraestructura tecnológica.

Uno de los factores críticos y esenciales que se deben considerar al evaluar una Blockchain, son los denominados algoritmos de consenso. Un algoritmo de consenso es el método, incluido en el software de la Blockchain, que le permite a todos los nodos, coordinarse y poder “ver” el mismo registro de transacciones.

Ethereum utilizaba el algoritmo de consenso de Prueba de Trabajo (Proof of Work, PoW) para validar las transacciones y asegurar la red. Sin embargo, Ethereum mudó hacia un algoritmo de consenso de Prueba de Participación (Proof of Stake, PoS) conocido como Ethereum 2.0. También se conoció el proceso de cambio de un protocolo de consenso a otro como “the merge”. La PoS tiene como objetivo aumentar la eficiencia energética y la escalabilidad de la red Ethereum. Fue una necesidad de la red, ya que al pensar en la cantidad de procesos que generan los contratos inteligentes que corren en la Blockchain de Ethereum, se hizo necesario agilizar el proceso de mineración, para poder validar transacciones y estados de estos Smart Contracts.

Como conclusión podemos ver que Ethereum es una Blockchain con características que la hacen distinguirse de las demás. Algunas de estas características son el soporte de Contratos Inteligentes, lenguaje de programación específico, Solidity, de tipo Turing completo, capacidad de tokenización de activos, interoperabilidad con otras redes por medio de estándares predefinidos, una comunidad activa y en crecimiento y la reciente incorporación del protocolo de consenso de Prueba de Participación (POS) que permite una alta escalabilidad de procesamiento de transacciones. Estas características han contribuido a la adopción generalizada de Ethereum y a su posición destacada en el mundo de Blockchain.

Hyperledger

Hyperledger no es en sí una Blockchain, sino que la podemos definir como un proyecto de código abierto que sustenta un framework (marco de trabajo) para desarrollar Blockchain, preferentemente de tipo privadas o permisionadas.

Hyperledger inició como un proyecto de código abierto, con visión comunitaria, impulsado por la Fundación Linux. Actualmente ha sumado a múltiples organizaciones, siendo la más destacada, IBM.

Su objetivo, tal como es definido en su web, es soportar el desarrollo de aplicaciones o soluciones con arquitectura modular destinadas al sector corporativo y recursos de la industria, con un alto nivel de adaptabilidad, invariabilidad, anonimato, confidencialidad, flexibilidad, resiliencia, escalabilidad y diseño.

Aplica protocolo de consenso de tolerancia a fallas bizantinas (BFT - Byzantine Fault Tolerance), pero los desarrollos de Hyperledger Fabric más modernos, permiten configurar el protocolo de consenso con el cual deseamos funcione la Blockchain que desarrollemos. Otra de las ventajas que ofrece es que al ser una plataforma distribuida de nivel empresarial basada en Blockchain, permite ajustar la construcción de soluciones a cualquier ámbito, actividad o industria.

El auge de su viabilidad de desempeño se debe al enfoque único por consenso, garantizando la privacidad. Su arquitectura crea consenso como un módulo configurable llamado Servicio de pedidos, que es un nodo llamado pedido ("nodo de pedidos") que realiza el pedido de la

transacción. Con esto, los participantes pueden decidir utilizar diferentes estrategias, así como implementar un protocolo de consenso escogido. El subsistema de contabilidad de Hyperledger Fabric se compone de dos elementos: el "estado global", que es la representación del estado del libro mayor en un momento definido, y el "registro de transacciones" es la descripción del historial de actualización al en el estado global observado, en donde todos los miembros posee una copia del Ledger (registro) al que pertenece la red Hyperledger Fabric que estamos desarrollando.

En Hyperledger Fabric, los contratos inteligentes se registran por medio de un lenguaje de computación escrito en Go y Node.js llamado “chaincode”[68].

Hyperledger Fabric se encuentra en la versión 2.0 y su planificación ya incorpora estas características de autorización y privacidad consideradas indispensables. En la red transaccional soportada por Hyperledger Fabric, todos los miembros tienen identificación autorizada, es decir, conocida.

El framework de Hyperledger ofrece una serie de sub-plataformas, que permiten desarrollar Blockchain que se adapten más cabalmente a los requerimientos de la empresa u organización que la utilicen.

Hyperledger Fabric:

Hyperledger Fabric es la plataforma más utilizada y difundida de la comunidad Hyperledger. Proporciona un modelo de Cadena de Bloques permisionada que permite a los participantes configurar diferentes niveles de acceso a los datos y las transacciones. Hyperledger Fabric es ampliamente utilizado en aplicaciones empresariales y admite la implementación de contratos inteligentes en lenguajes como Go y JavaScript. Su modularidad y versatilidad es lo que le permite llegar a los más diferentes casos de uso, cubriendo así el abanico de múltiples ramas de actividades[69].

Hyperledger Besu:

Hyperledger Besu es una plataforma de Hyperledger se basada en el protocolo Ethereum. Es compatible con los estándares de la Enterprise Ethereum Alliance (EEA), y tiene plena implementación de la EVM (Ethereum Virtual Machine - el componente básico de Ethereum que se encarga de ejecutar los Contratos Inteligentes). En esta misma dirección es que soporta las testnet (redes de pruebas que permiten testear Contratos Inteligentes antes de desplegarlos) Sepolia y Goerli (las principales de Ethereum).

Besu permite trabajar con diferentes tipos de protocolos de consenso, tales como POS - Prueba de Participación, POW - Prueba de trabajo y POA - Prueba de Autoridad.

---

[68] Zand, M., Wu, X. B., & Morris, M. A. (2021). *Hands-On Smart Contract Development with Hyperledger Fabric V2*. " O'Reilly Media, Inc.".

[69] Shah, N. (2019). *Blockchain for Business with Hyperledger Fabric: A complete guide to enterprise blockchain implementation using Hyperledger Fabric*. BPB Publications.

No es trivial mencionar que las pruebas de concepto (pilotos de pruebas) que BACEN - Banco Central de Brasil para la implementación del Real Digital (proyecto DREX), se están haciendo con Hyperledger Besu como plataforma soporte.

Hyperledger Indy:

Hyperledger Indy se centra en la gestión de identidades digitales descentralizadas y la privacidad. Está diseñado para permitir a las personas tener control sobre su identidad en línea y compartir selectivamente información personal. Hyperledger Indy utiliza una Blockchain permisionada y proporciona herramientas y bibliotecas para la creación de aplicaciones de identidad digital.

Hyperledger Iroha:

Se centra en la simplicidad y la facilidad de uso, ofreciendo una interfaz de programación de aplicaciones (API) simple y una arquitectura modular. Hyperledger Iroha utiliza un modelo de consenso basado en el algoritmo Sumeragi y admite la ejecución de contratos inteligentes en lenguajes como Java.

Hyperledger Sawtooth:

Utiliza un modelo de consenso llamado Prueba de Periodo de Tiempo (PoET) y también de Prueba a Fallos Bizantinos (PBFT) y permite la ejecución de contratos inteligentes en lenguajes como Python y JavaScript. Además su fortaleza se centra en el desdoblamiento del “core” de sistema con el dominio de aplicaciones, de manera que los Contratos Inteligentes que se despliegan en esta sub-plataforma de Hyperledger, son independientes en su ejecución con respecto al núcleo de aplicación de la Cadena de Bloques.

Podemos entonces decir que la elección de la sub-plataforma Hyperledger estará en función de los requisitos específicos y el alcance que se defina para el desarrollo de la Plataforma BCT para NFT / FT de la provincia de Santa Fe.

Al igual de lo que mencionamos anteriormente en referencia a la Blockchain de Ethereum, Hyperledger también cuenta con una amplia y activa comunidad de desarrolladores, implementadores y en general actores interesados, siendo esto un factor crucial en la generación de conocimiento y soporte para desarrollos.

Además, en términos de innovación de su plataforma, cuenta significativamente la participación de grandes actores de desarrollo de software como son Linux Foundation y IBM.

XinFin (Blockchain híbrida - pública y privada)

XinFin es una combinación de Blockchain pública y privada, de alta escalabilidad y seguridad basada en el protocolo XDC-01, una bifurcación de Ethereum y Quorum.

No tiene el protocolo de consenso de POW - Prueba de Trabajo. Su protocolo de consenso se denomina XDC-01, el cual tiene como objetivo generar un esquema de financiamiento efectivo dirigido a transacciones comerciales globales.

XinFin, es compatible con todos los contratos inteligentes, protocolos y transferencias de tokens atómicos entre cadenas compatibles con EVM (Ethereum Virtual Machine).

XinFin Digital Contract (XDC) es la criptomoneda derivada de la Blockchain de XinFin, permite el diseño de nuevos tipos de modelos de token XRC-20 basados en XDC que admitirán Dapps mediante el uso de Smart Contracts. Además, admite "todos los Contratos Inteligentes, protocolos y transferencias de tokens atómicos entre cadenas compatibles con EVM" (Ethereum Virtual Machine).

Los tokens XDC tienen como objetivo aprovechar la ventaja tanto de la cadena de bloques pública como de la cadena de bloques privada, están desarrollados para respaldar la capa de contratos inteligentes e identificar su capa de clientes KYC - Know Your Customer, Conozca a sus Clientes.

Entre sus ventajas podemos mencionar:

XinFin combina características de las Blockchain públicas y privadas para ofrecer una solución híbrida. Esto significa que la red XinFin permite tanto transacciones públicas como privadas, brindando flexibilidad y opciones a las empresas según sus necesidades específicas.

Rendimiento escalable, ya que se ha diseñado para ser altamente escalable y puede manejar un alto volumen de transacciones por segundo. Al implementar un mecanismo semejante al de consenso de Prueba de Autoridad (Proof of Authority, PoA), XinFin puede lograr una mayor velocidad y rendimiento en comparación con otras Blockchain.

Admite la ejecución de contratos inteligentes, lo que permite a las empresas automatizar acuerdos y transacciones basadas en reglas y condiciones predefinidas, en forma independiente de transacciones no-permisionadas en su ambiente público.

XinFin busca lograr la interoperabilidad con otras redes y sistemas. Esto permite la transferencia de activos y datos entre diferentes Blockchain y la integración con infraestructuras y aplicaciones existentes, facilitando la colaboración e impulsando su adopción.

Ecosistema y comunidad activa, cuenta con una comunidad activa de desarrolladores, empresas y colaboradores que trabajan para impulsar la adopción y el desarrollo de la red. También ha establecido asociaciones y colaboraciones estratégicas con diversas organizaciones para promover su ecosistema y expandir su alcance.

XinFin sigue un enfoque de código abierto y promueve la adhesión a estándares y protocolos abiertos. Esto fomenta la transparencia, la colaboración y la innovación, permitiendo que más personas y empresas participen y contribuyan al desarrollo de XinFin.

Quórum

Quorum fue originalmente desarrollada JPMorgan Chase y el socio EthLab, una startup de Ethereum con el objetivo de operar en el área financiera y ofrecer privacidad. Su desarrollo se basó en una derivación de Geth, que es una distribución habilitada por Ethereum Foundation, para interactuar con la red como un nodo en la Blockchain Ethereum.

Por eso, se suele decir que Quorum es la versión empresarial de Ethereum, la que permite a los usuarios operar contratos inteligentes híbridos que pueden ser tanto privados como públicos. Sin embargo, existe una restricción. El Contrato Inteligente que fue configurado como privado no puede hacerse público, al igual que el contrato inteligente público no puede hacerse privado.

La plataforma híbrida híbrida de Quorum se enfoca en reutilizar las diferentes características de la tecnología Ethereum e incorporar funcionalidades de transacciones privadas, asegurando que solo los detalles de la transacción se vuelvan públicos solo. para los participantes de la transacción.

Los recursos de comunicación que utiliza Quorum brindan una reducción en el tiempo de difusión de los mensajes a través de la red. Utiliza dos algoritmos de consenso RAFT y el BFT de Estambul para que los procesos autorizados realicen el mismo curso de solicitudes. El algoritmo RAFT establece que cada nodo en una máquina de estado reproducida ("grupo de servidores") tiene la capacidad de permanecer en cualquiera de los tres estados posibles. Por ejemplo, el nodo podría estar en estado de servidor líder, servidor candidato (al sondear la elección del servidor líder), o servidor seguidor. Utiliza una forma de liderazgo distinta en relación a otros algoritmos.

El consenso bizantino de Estambul-BFT para "Tolerancia a fallas de colisión y Tolerancia a fallas bizantinas" se utiliza para realizar la reproducción de máquinas de estado.

En lo que respecta a privacidad y confidencialidad, Quorum se enfoca en garantizar ambas cualidades de la información utilizando técnicas de cifrado y compartimentación de datos para permitir transacciones confidenciales entre participantes autorizados, lo que la hace adecuada para casos de uso empresariales y en especial financieros donde la privacidad es una preocupación.

Si bien se pueden configurar ambientes públicos, Quórum es una Blockchain permisionada y de acceso controlado. Solo los participantes autorizados pueden unirse a la red y participar en las transacciones. Esto permite un mayor control y seguridad en comparación con las Blockchain públicas, ya que se pueden establecer políticas de acceso y autenticación para garantizar la integridad de la red.

Además, es adecuada para la formación de Blockchain de consorcios y colaboraciones empresariales, ya que proporciona herramientas para establecer estructuras de gobernanza y tomar decisiones conjuntas sobre el funcionamiento de la red. Esto permite la participación de múltiples partes interesadas y promueve la adopción empresarial de blockchain. De allí su preferencia de adopción por bancos o instituciones financieras que necesitan implementar transacciones interbancarias, sobre una Blockchain común, pero cada miembro administrador, conservar sus privilegios sobre permisos y confidencialidad de los clientes que gobierna.

Está diseñada para ser eficiente y escalable, permitiendo un alto rendimiento en términos de procesamiento de transacciones. Utiliza algoritmos de consenso eficientes y técnicas de optimización para minimizar los tiempos de confirmación y mejorar la escalabilidad de la red.

Quorum es compatible con contratos inteligentes y utiliza una versión modificada de la Máquina Virtual Ethereum (EVM), lo que permite a los desarrolladores crear y ejecutar contratos inteligentes en su Cadena de Bloques.

Se puede integrar con sistemas y aplicaciones empresariales existentes, lo que facilita la adopción y la interoperabilidad con la infraestructura tecnológica ya existente en las organizaciones. Esto permite una transición más suave hacia la adopción de blockchain y una mayor facilidad de uso.

Por último deberíamos destacar que originalmente fue desarrollada JPMorgan Chase, pero posteriormente vendida a Consensys, una de las empresas líderes en el área de Blockchain, que cuenta con una comunidad activa de desarrolladores y usuarios. Esto proporciona soporte técnico y recursos adicionales para aquellos que utilizan Quorum y permite la colaboración y el intercambio de conocimientos en el ecosistema.

Corda R3

Corda surgió en el año 2017, cómo un desarrollo de la empresa R3, una empresa especializada el el desarrollo de software BCT.

El objetivo de Corda fue desarrollar una solución para el entorno del mercado financiero global. R3 Corda es una red peer-to-peer validada por nodos que implementan una aplicación de JVM Java Virtual Machine. Además, entre los nodos validadores de DLT (Distributed

Ledger Technologies), la estructura R3 Corda utiliza un protocolo denominado Advanced Message Queuing Protocol over Transport Layer Security (AMQP/TLS).[70]

La plataforma Corda ejecuta la aplicación llamada CorDapps que son Aplicaciones Distribuidas de Corda, las cuales tienen el propósito de permitir que los nodos cumplan con el registro de transacciones en el Ledger de Corda.

Una de las ventajas que ofrece Corda R3, vinculado a su accesibilidad es que se puede programar sobre su Blockchain, con el lenguaje Java, que es el lenguaje de programación más utilizado en el mundo.

Además el entorno de Corda R3 se integra fácilmente con los sistemas que se ejecutan en la mayoría de las empresas, incluidas las bases de datos relacionales, y desarrollos realizados sobre JVM, la máquina virtual de Java.

Posee también una versión denominada Corda Enterprise, está orientado a atender los procesos más complejos y de requerimientos de camino crítico.

Corda R3 opera con dos perspectivas de consenso:

a) Validez de la transacción, los involucrados deben observar si todas las firmas necesarias están incluidas a lo largo del código del contrato o la transacción.

b) Control de la transacción, los involucrados deben asegurarse de que una transacción sea de un solo cliente para todos los datos ingresados, es decir que la transacción en cuestión ya tuvo un consenso.

Corda tiene su propio intérprete de lenguaje de máquina (bytecodes).

El mecanismo de consenso utilizado se denomina “notarios”. Se asigna autoridad a cada elemento de datos. Esta característica asegura la finalización de las transacciones para que se alcance el consenso en toda la red Blockchain.

El propósito del mecanismo de consenso "notario" es asegurarse de que una transacción tenga estados de entrada únicos y específicos. Además, se puede utilizar para validar transacciones, evitar el "doble gasto" y actuar como una autoridad de sellado de tiempo.

Entre las principales características de la plataforma Corda-R3 podemos mencionar:

Confidencialidad y privacidad: Corda se centra en garantizar la confidencialidad de los datos en la red. Utiliza técnicas de compartimentación de datos y cifrado para permitir transacciones confidenciales entre participantes específicos. Esto hace que Corda sea adecuada para casos de uso donde la privacidad y la confidencialidad son críticas, como en el sector financiero.

Arquitectura orientada a transacciones: Corda se basa en una arquitectura orientada a transacciones, donde cada estado y cada transacción son tratados de manera individual. Esto permite un mayor nivel de flexibilidad y granularidad en el modelado y la gestión de acuerdos y contratos complejos.

[70] Travel, T., & Mohanty, D. (2019) *R3 Corda for Architects and Developers*. Apress

Contratos inteligentes legales: Corda se diferencia de otras plataformas blockchain al permitir la creación y ejecución de contratos inteligentes legales. Estos contratos pueden contener lógica jurídica y facilitar la automatización y el cumplimiento de acuerdos en el ámbito legal.

Interoperabilidad: Corda ha sido diseñada para facilitar la interoperabilidad con sistemas y redes existentes en el entorno empresarial. Esto permite la integración con sistemas heredados y otras tecnologías, lo que facilita la adopción y la colaboración entre diferentes actores.

Validación y consenso: Corda utiliza un modelo de validación y consenso basado en la lógica empresarial compartida entre las partes involucradas en una transacción. Esto permite a las partes acordar y validar los términos de la transacción de manera descentralizada, evitando la necesidad de un mecanismo de consenso ampliamente distribuido.

Flexibilidad y modularidad: Corda es altamente flexible y modular, lo que permite a los desarrolladores personalizar y adaptar la plataforma a sus necesidades específicas. Esto incluye la capacidad de elegir los componentes y los servicios que se utilizarán en una implementación de Corda.

Enfoque empresarial: Corda se ha diseñado con un enfoque empresarial desde su concepción. Ha sido desarrollada en colaboración con empresas líderes en diversos sectores, lo que garantiza que las características y funcionalidades de Corda se ajusten a los requisitos y las regulaciones empresariales.

Breve comparativa de las diferentes soluciones de blockchain analizadas:

Características	Ethereum	Corda R3	Hyperledger	Quorum
Tipo de plataforma	Blockchain pública	Blockchain privada	Blockchain permisionada	Blockchain privada
Lenguaje de programación	Solidity	Kotlin, Java, Scala	Go, JavaScript, Java	Solidity, Vyper
Consenso	Prueba de trabajo	Algoritmo propio	Pluggable (puede variar)	Prueba de trabajo o de autoridad
Arquitectura	Smart contracts	Transacciones válidas únicamente entre las partes involucradas	Modular y flexible	Variante de Ethereum con permisos
Gobernanza	Decentralizada	Consorcio	Consorcio	Consorcio
Escalabilidad	Limitada	Escalable	Escalable	Escalable
Privacidad	Pública por defecto	Altamente privado	Configurable	Configurable
Transacciones por segundo	Alrededor de 15	Variable	Variable	Variable
Casos de uso	Contratos inteligentes, tokens, aplicaciones descentralizadas	Mercados financieros, cadena de suministro, servicios financieros	Gestión de identidad, cadena de suministro, seguros	Cadena de suministro, gestión de activos

Protocolos de consenso

Los protocolos de consenso son mecanismos seguros y tolerantes a fallas presentes en Blockchain y que se utilizan para determinar cómo los “nodos” llegan a un acuerdo en relación a una determinada decisión, es decir, para asegurar que los datos de la cadena que se

almacenan se legitimen y no se alteren. . Los protocolos de consenso acuerdan el estado verificable de cada nodo Blockchain. De esta manera, cambiar cualquier dato en la cadena de información invalida todos los bloques subsiguientes. El mecanismo crea un sistema invulnerable para el registro continuo de datos. La destrucción de un nodo Blockchain no afecta su integridad, todos los nodos completos tienen una Blockchain completa. Como no hay un nodo centralizado, los nodos pueden participar colectivamente con un algoritmo de consenso, es decir, la red Blockchain es mantenida por la red. En cuanto a su seguridad y credibilidad, los datos una vez verificados se guardan de forma permanente en la Blockchain, siendo imposible modificarlos. Esto significa que una vez que se registra una transacción en Blockchain, no se puede modificar ni manipular. Es decir, los errores se reparan en transacciones futuras y la transacción pasada (con el error) se registra y es visible para todos los que tienen acceso a la red.

Algunos de los protocolos de consenso, más comunes, utilizados en Blockchain son:

Proof of Work (PoW) o prueba de trabajo:

El "Proof of Work" (PoW), o Prueba de Trabajo en español, es un algoritmo de consenso utilizado en muchas Blockchain, incluyendo Bitcoin y hasta hace poco, Ethereum. Su objetivo principal es asegurar la integridad de la red y validar las transacciones de manera descentralizada a través de la resolución de problemas matemáticos complejos.

En el PoW, los participantes de la red, llamados "mineros", compiten para resolver un problema criptográfico que requiere una gran cantidad de poder computacional. Este problema es conocido como "hash puzzle" o rompecabezas de hash. El primer minero en encontrar la solución correcta puede agregar un nuevo bloque a la cadena de bloques y recibir una recompensa, generalmente en forma de criptomonedas.

El proceso de resolución del rompecabezas de hash implica intentar diferentes combinaciones de datos hasta encontrar un resultado que cumpla con ciertas condiciones predefinidas. Esto requiere una gran cantidad de energía y tiempo de cálculo, lo que hace que sea costoso y difícil de lograr. Sin embargo, una vez que se encuentra la solución, su verificación es sencilla y rápida para el resto de la red.

El PoW proporciona una forma segura y confiable de alcanzar el consenso en una red blockchain descentralizada. Debido a que los mineros compiten entre sí para resolver el problema, se requiere una mayoría significativa del poder computacional total de la red para alterar o falsificar los datos de la cadena de bloques. Esto hace que sea extremadamente difícil para un atacante malintencionado comprometer la integridad de la red.

Una de las principales ventajas del PoW es su resistencia a los ataques de doble gasto y a la manipulación de datos. Dado que cada bloque está enlazado criptográficamente al bloque anterior, cualquier intento de modificar un bloque requeriría recalcular todos los bloques siguientes, lo cual requeriría una cantidad de poder computacional abrumadora y costosa.

Sin embargo, el PoW también presenta algunas limitaciones. El proceso de minería consume una cantidad significativa de energía y requiere una infraestructura especializada, lo que lleva a preocupaciones sobre su impacto ambiental y su centralización en manos de grandes operaciones mineras. Además, a medida que aumenta la dificultad de los problemas de hash, se requieren recursos computacionales cada vez más potentes y costosos.

En respuesta a estas preocupaciones, se han propuesto y desarrollado otros algoritmos de consenso, como el "Proof of Stake" (PoS), que buscan mejorar la eficiencia energética y reducir la dependencia del poder computacional. Estos algoritmos utilizan la tenencia de criptomonedas existentes como factor determinante en la selección del próximo validador de la red, en lugar de depender del poder de cálculo.

Aunque efectivo, el PoW tiene preocupaciones sobre el consumo de energía y la centralización, lo que ha llevado al desarrollo de otros algoritmos de consenso.

Proof of Stake (PoS) o prueba de participación:

El protocolo de consenso Proof of Stake (PoS) es un mecanismo utilizado en Blockchain que difiere del Proof of Work (PoW) en términos de cómo se alcanza el consenso. A continuación, se presentan algunas de las características clave del protocolo de consenso Proof of Stake:

Participación en lugar de poder computacional: A diferencia del PoW, donde los mineros compiten resolviendo problemas computacionales complejos, en PoS los participantes son seleccionados para validar y forjar nuevos bloques basados en la cantidad de criptomonedas que poseen y están dispuestos a "apostar" como garantía.

Selección del validador (minero): En PoS, los validadores se eligen de manera determinística según la cantidad de criptomonedas que hayan caucionado para realizar el trabajo de mineración. Cuanto más alto sea el saldo de criptomonedas en caución, mayor será la probabilidad de ser seleccionado como validador para crear un bloque.

Creación de bloques y recompensas: Los validadores seleccionados tienen la responsabilidad de crear nuevos bloques y validar las transacciones dentro de ellos. A cambio de sus servicios, reciben recompensas en forma de nuevas criptomonedas generadas o comisiones de transacción incluidas en el bloque.

Seguridad a ataques: El protocolo PoS es inherentemente seguro porque para llevar a cabo un ataque malicioso, un atacante debería tener una participación mayoritaria de las criptomonedas en circulación en la red, lo que resultaría en un costo prohibitivo. Además, las sanciones o penalizaciones financieras se pueden imponer a aquellos validadores que intenten comportarse de manera maliciosa o traten de falsificar datos.

Eficiencia energética: A diferencia del PoW, que requiere una gran cantidad de poder computacional y consumo de energía, el PoS es generalmente más eficiente en términos de consumo de energía. Al eliminar la necesidad de resolver problemas matemáticos complejos, se reducen significativamente los requerimientos computacionales y energéticos.

Descentralización y participación: PoS permite una mayor participación de los poseedores de criptomonedas, ya que cualquiera que tenga una cantidad suficiente de la criptomoneda puede convertirse en un validador. Esto promueve una mayor descentralización y evita la concentración de poder en manos de grandes operaciones mineras.

Actualizaciones y cambios de protocolo: PoS permite actualizaciones y cambios de protocolo más flexibles y rápidos en comparación con PoW. Dado que no hay necesidad de coordinar cambios en la dificultad del problema de hash o en el ajuste de la minería, las actualizaciones pueden implementarse de manera más ágil.

Es importante destacar que existen diferentes variaciones del protocolo PoS, como el Delegated Proof of Stake (DPoS) y el Byzantine Fault Tolerance (BFT), que introducen diferentes mecanismos para seleccionar validadores y alcanzar el consenso. Cada variante tiene sus propias características y consideraciones específicas en términos de seguridad, escalabilidad y eficiencia.

Prueba de autoridad (PoA)

Es un algoritmo utilizado como parte de los sistemas Blockchain, principalmente en Consortium Blockchain, para procesar directamente transacciones abiertas para verificar la identidad de los usuarios. Se centra en la identidad y la reputación de los validadores en lugar de depender del poder computacional o de la cantidad de criptomonedas caucionadas. Algunas características del protocolo de consenso Proof of Authority son:

Identidad de los validadores: En PoA, los validadores son entidades preseleccionadas que se consideran confiables y autorizadas para validar las transacciones y crear nuevos bloques en la cadena de bloques. Estos validadores pueden ser individuos o entidades reconocidas en la red, como empresas o instituciones.

Autoridad y reputación: La selección de los validadores se basa en su autoridad y reputación en la red. Generalmente, los validadores son seleccionados por una autoridad centralizada o un grupo de entidades confiables que garantizan su integridad y competencia para mantener la seguridad y el correcto funcionamiento de la red blockchain.

Proceso de validación: Los validadores en PoA tienen la responsabilidad de validar las transacciones y crear nuevos bloques. No necesitan competir o resolver problemas computacionales complejos, ya que su autoridad y reputación ya han sido establecidas. La validación de transacciones se basa en reglas y políticas predefinidas establecidas por el protocolo.

Eficiencia y escalabilidad: PoA es conocido por su alta eficiencia y escalabilidad, ya que no requiere un alto consumo de energía ni recursos computacionales intensivos. Al eliminar la competencia y la necesidad de resolver problemas matemáticos, el proceso de validación se vuelve más rápido y menos costoso.

Centralización controlada: A diferencia de otros protocolos de consenso descentralizados, PoA implica un grado de centralización controlada. La autoridad centralizada o el grupo de entidades confiables que selecciona a los validadores puede tener un control significativo sobre la red. Sin embargo, este enfoque también puede ser útil en casos de uso específicos donde se requiere un mayor grado de confianza y seguridad.

Inmutabilidad y seguridad: Aunque PoA no ofrece el mismo nivel de descentralización y resistencia a ataques como otros protocolos de consenso, sigue garantizando la inmutabilidad y la seguridad de la cadena de bloques. Dado que los validadores son entidades confiables y reconocidas, la red se beneficia de su autoridad y reputación para evitar transacciones fraudulentas y garantizar la integridad de los datos.

El protocolo de consenso Proof of Authority se utiliza comúnmente en casos de uso donde la confianza y la gobernanza son elementos críticos, como Blockchain privadas o consorcios empresariales. Al eliminar la necesidad de competencia y la dependencia del poder computacional, PoA ofrece una solución eficiente y confiable para ciertos escenarios de blockchain donde la centralización controlada es aceptable.

Prueba de Conocimiento Cero (ZKPs)

Es un mecanismo por el cual una parte (el probador) puede probar a la otra parte (el verificador), es decir, que cierta información es auténtica, en oposición al probador, hace dificulte difundir cualquier información adicional más allá de la afirmación de que, de hecho,

la información es auténtica. El protocolo utiliza cuatro funciones distintas: "una función de generador de claves, una función de programa de entrada, una función de prueba y una función de verificación".

Es decir, las ZKPs son utilizadas en Blockchain para verificar la veracidad de una declaración sin revelar la información vinculada. En lugar de validar las transacciones mediante la resolución de problemas computacionales o la posesión de criptomonedas, el ZKP se centra en demostrar que se tiene conocimiento de ciertos datos sin revelarlos.

Las características principales del protocolo de consenso ZKP en blockchain son:

Privacidad: Las ZKPs se basan en el principio de privacidad, permitiendo a los usuarios demostrar que poseen información verificable sin revelar la información misma. Esto implica que una parte puede demostrar que conoce ciertos datos sin tener que exponer los datos reales o revelar información adicional.

Prueba de conocimiento: Las ZKP permiten a una parte probar que posee conocimiento de ciertos datos o información, sin tener que revelar la información en sí misma. Esto se logra mediante la construcción de una prueba matemática que verifica la validez de una declaración sin revelar información adicional.

Verificación eficiente: El proceso de verificación de una prueba de conocimiento cero se puede realizar de manera eficiente en términos computacionales. La verificación no requiere la repetición de cálculos complejos ni el conocimiento de la información subyacente, lo que permite una validación rápida y eficiente.

Confianza y seguridad: Las ZKPs ofrecen un alto nivel de confianza y seguridad al permitir la verificación de declaraciones sin revelar información adicional. Esto es especialmente valioso en situaciones en las que la confidencialidad de los datos es crucial y se busca garantizar la privacidad y la integridad de la información.

El protocolo de consenso ZKP tiene varias aplicaciones en blockchain. Por ejemplo, se puede utilizar para verificar la autenticidad de transacciones sin revelar los detalles específicos de las transacciones, o para demostrar la solvencia de una entidad sin revelar los detalles exactos de sus activos. Sin embargo el uso más destacado que está teniendo esta técnica es la de realizar los denominados “roll-ups”, es decir, poder validar grandes bloques de transacciones, todas juntas por medio de la generación de su correspondiente ZKPs. De esta manera, la intencionalidad de incorporación como metodo de validación en una Blockchain, tiene más que ver con la eficiencia y escalabilidad de la misma, más que con la privacidad de la información subyacente. Este es el plan de trabajo que piensa adoptar la Blockchain de Ethereum, para ir transformando su máquina virtual EVM, en una máquina virtual ZKP, más eficiente y escalable.

Las ZKPs se han desarrollado para ser eficientes y escalables en aplicaciones de blockchain. Aunque el proceso de generación de pruebas de conocimiento cero puede ser computacionalmente costoso, la verificación de estas pruebas se puede realizar de manera eficiente, lo que permite un procesamiento rápido y escalable de las transacciones.

Las ZKPs ofrecen beneficios en términos de privacidad, seguridad y eficiencia en la validación de transacciones y la verificación de información confidencial en la cadena de bloques.

Tolerancia a fallas bizantinas (BFT):

El protocolo de tolerancia a fallas bizantinas (Byzantine Fault Tolerance, BFT) es un mecanismo utilizado en Blockchain para garantizar la seguridad y el consenso en entornos distribuidos, incluso cuando algunos nodos de la red pueden ser maliciosos o fallar de manera arbitraria. El objetivo del protocolo BFT es permitir que los nodos de la red lleguen a un acuerdo sobre el estado de la cadena de bloques a pesar de la presencia de fallas bizantinas, que incluyen nodos que envían información falsa, se comportan de manera impredecible o incluso intentan sabotear la red.

Los ejes del algoritmo de tolerancia a fallas bizantinas en blockchain son:

Consenso descentralizado: El protocolo BFT busca lograr un consenso descentralizado en un entorno distribuido, donde cada nodo puede tener su propia visión de la red y potencialmente ser malicioso. El objetivo es alcanzar un acuerdo en la validez de las transacciones y el estado de la cadena de bloques a través de un proceso de comunicación y votación entre los nodos.

Redundancia y replicación: Para garantizar la tolerancia a fallas, el protocolo BFT utiliza la redundancia y la replicación de nodos. Los nodos en la red se dividen en un grupo de nodos primarios y un conjunto de nodos secundarios o de respaldo. Esto permite que la red continúe funcionando incluso si algunos nodos fallan o actúan de manera maliciosa.

Mensajes firmados y autenticados: En el protocolo BFT, los nodos se comunican entre sí mediante el intercambio de mensajes firmados y autenticados. Esto garantiza que los mensajes provengan de los nodos correctos y que no hayan sido alterados durante la transmisión.

Acuerdo mediante votación: Los nodos en el protocolo BFT llegan a un acuerdo sobre la validez de una transacción o el estado de la cadena de bloques mediante un proceso de

votación. Los nodos intercambian información y votan por un estado propuesto, y se llega a un consenso cuando la mayoría de los nodos está de acuerdo con el mismo estado.

Resistencia a fallas bizantinas: El protocolo BFT es resistente a fallas bizantinas, lo que significa que puede tolerar y superar la presencia de nodos maliciosos o defectuosos en la red. Incluso si algunos nodos intentan sabotear el proceso de consenso, la mayoría de los nodos honestos puede garantizar la integridad de la cadena de bloques.

Eficiencia y escalabilidad: BFT se ha desarrollado para ser eficiente y escalable en entornos de blockchain. Aunque el proceso de votación puede requerir cierta comunicación adicional y tiempo de procesamiento, se han propuesto y desarrollado mejoras para mejorar la eficiencia y la escalabilidad del protocolo.

CONCLUSIONES

En esta etapa de evaluación del proyecto de desarrollo de una Plataforma Blockchain NFT/FT para la provincia de Santa Fe, analizamos los aspectos más destacados vinculados a las decisiones que se deben tomar en relación a la elección de la infraestructura de Cadena de Bloques a utilizar.

Nuestra primera consideración se basó en la clasificación de tipología de Cadenas de Bloques según sea el gobierno de las mismas. En el uso generalizado se suele conocer a esta clasificación como “según su grado de descentralización”. Esta caracterización es bastante representativa de la tecnología de Blockchain, no es del todo acertada, ya que la descentralización de servidores de la red, no necesariamente implica un gobierno totalmente descentralizado. Un ejemplo de esto se puede observar en las Blockchain permisionadas donde los nodos de la misma se distribuyen entre nodos administradores (con permisos especiales), y nodos selladores o validadores, y esto no impide la descentralización de la misma.

Pero no nos vamos a centrar en esta discusión sobre conceptualización en nuestro análisis, sino que vamos a poner foco en el gobierno de las diferentes tipologías de Blockchain.

Blockchain no permisionadas o públicas

Las Blockchain no permisionadas fueron las primeras en haber sido desarrolladas. Su objetivo fue sustentar la criptomonedas públicas y por esto fueron pensadas para tener un gobierno totalmente descentralizado, donde cada servidor de la red tiene igual peso. Al mismo tiempo esos servidores, al igual que todos los actores de la red, se mantienen anónimos. Solamente conocidos por sus claves criptográficas públicas, por lo cual de ellos depende si exponen su identidad o no.

Debido a esta consideración es que no reviste mucho análisis la evaluación de este tipo de Blockchain como solución de infraestructura para nuestro planteo. Ningún gobierno, municipal, provincial o nacional, pensaría en la adopción de una red de tipo no permisionada, como infraestructura básica de la Plataforma Blockchain NFT/FT en cuestión, en tanto la red permita operar libremente y total anonimato, especialmente con las experiencias que se han presentado a nivel global de utilizar estas redes Blockchain para operaciones de lavado de dinero.

Debemos destacar que una excepción a esta consideración sería la posibilidad de realizar el desarrollo completo del sistema deseado como una sobre-estructura de la red, gestionando la totalidad de las funcionalidades del mismo por medio de una arquitectura de Contratos Inteligentes, desplegados en la Blockchain no-permisionada. En este sentido deberíamos considerar no solo la gestión por medio de Contratos Inteligentes de las funciones operativas del sistema, sino también la gestión de cuentas y autenticación de las mismas para firmar transacciones, de modo que estas dejen de ser anónimas. Una solución si se evaluará esta opción sería la de utilizar sobre la red Ethereum el EIP-4337 (una plantilla de Contratos Inteligentes), conocido como “Abstracción de cuentas”.

Blockchain permisionadas o privadas

En la medida que la tecnología de Blockchain fue evolucionando y ganando cada vez más espacio en diferentes industrias y actividades, las organizaciones, grandes empresas y en general el sector corporativo de la sociedad, se vieron enfrentados a la necesidad de romper el esquema de anonimato y gobierno totalmente descentralizado. Es ilógico, por ejemplo, pensar en un banco que desarrollara una Blockchain con estas características, delegando a sus usuarios la total potestad sobre las operaciones, sin control sobre estas, y en especial sin nominalidad de los usuarios.

De esta forma este tipo de instituciones impulsaron clonar el código fuente de las Blockchain no-permisionadas, modificándolo de modo que determinados usuarios (el banco en nuestro ejemplo) se reservaran permisos especiales y privilegios vinculados al gobierno de la red.

El tipo de modificaciones que se realizan sobre el código fuente de las Blockchain no-permisionadas puede variar significativamente en cada tipo de solución que se pretenda desarrollar. Sin embargo, la mayoría de las Blockchain permisionadas responden a un esquema de dos tipos de nodos o servidores de red: los administradores, con permisos especiales, y los selladores, que mantienen el formato de nodos de la Blockchain no-permisionada y tienen como función registrar y validar transacciones.

En el caso de la propuesta de desarrollo de Plataforma Blockchain para NFT/FT para la provincia de Santa Fe que analizamos, deberíamos considerar como primera opción a este tipo de Blockchain, que por una parte permite a usuarios trabajar sobre un ambiente de descentralización, con los beneficios de inalterabilidad e invulnerabilidad de transacciones que brinda la tecnología Blockchain, pero a su vez, preservando los privilegios necesarios que requiere la supervisión por parte del gobierno de la provincia de Santa Fe a operaciones y usuarios admitidos en la red.

Blockchain de consorcio

Una variante de las Blockchain no-permisionadas que analizamos, son las denominadas Blockchain “federadas” o “de consorcio”. En este caso la modificación al código fuente de la Blockchain no-permisionada contempla que la misma tenga no solamente una única autoridad de gobierno con permisos especiales, sino que esa capacidad esté delegada a varios servidores de la red, de manera que haya varios “nodos administradores” de la misma. Tal como se mencionó anteriormente un ejemplo representativo de este tipo de Blockchain son los pilotos que desarrollan bancos para poder realizar transferencias trans-fronterizas, donde cada banco posee permisos de administrador, sobre los usuarios de su dominio (sus clientes).

Este tipo de Blockchain se configura en base a un gobierno compartido de diferentes usuarios con privilegios sobre la red. Por este motivo es que creemos que no es un formato que se pueda vincular como infraestructura para la Plataforma Blockchain que estamos discutiendo.

Blockchain híbridas

Este tipo de Blockchain tienen en la actualidad un surgimiento incipiente, y pretenden juntar lo mejor de las blockchain no-permisionadas y permisionadas, en un único ambiente.

Desde esa perspectiva pareciera ser una opción óptima para aplicar a un desarrollo. Sin embargo, en base a la configuración de requerimientos que pensamos y analizamos para la Plataforma Blockchain NFT/FT para la provincia de Santa Fe resulta por el momento impensable la adopción de un dominio de Blockchain no-permisionada (pública) para algunas operaciones que se fueran a realizar, sin control del gobierno provincial, y con anonimato de los actores.

Por otra parte, al momento de escribir este trabajo no se ha observado un desarrollo significativo de comunidades robustas de desarrolladores y expertos de negocio para estas redes. Por este motivo se debería analizar esto como una desventaja significativa, si se compara la opción de utilizar este tipo de Blockchain con respecto a las comunidades maduras, por ejemplo, de Ethereum en orden de Blockchain no-permisionadas, o de Hyperledger o Corda en el caso de Blockchain permisionadas.

Tokens nativos y generados por Contratos Inteligentes

En el orden de análisis sobre la capa de la Blockchain en que se podría desarrollar la Plataforma BCT NFT/FT para la provincia de Santa Fe, evaluamos las opciones de desarrollo de Tokens nativos o de Tokens desarrollados por Contratos Inteligentes.

En el ámbito específico de la Plataforma BCT NFT/FT para la provincia de Santa Fe, el análisis de este aspecto deberá recaer en la comparación de carga de trabajo y de complejidad de desarrollo entre dos opciones:

1. modificación del código fuente de una Blockchain no-permisionada para que esta genere tokens (criptomoneda) específica, y a su vez incluya en el código de la Blockchain la lógica funcional de la solución deseada.
2. desarrollar un conjunto de Contratos Inteligentes sobre una Blockchain no-permisionada que gestionen la lógica de los diferentes procesos requeridos por la Plataforma.

Un aspecto no menor a tener en cuenta es que en la primera opción, una vez que el software de la Blockchain sea implementado, los cambios que se puedan a llegar a requerir en función de cambios en el contexto se harán mucho más complejos y difíciles de realizar ya que se necesitará realizarlos sobre todos los servidores que estén sustentando la Blockchain, generando lo que se conoce en las Blockchain no-permisionadas como un fork (desvío) fuerte.

Lo mismo podría decirse sobre los cambios que se deberían realizar sobre los Contratos Inteligentes, en la segunda opción. Pero en esta opción existen muchos modelos de los denominados “upgradable smart contracts” que referencian a una arquitectura sobre la que se diseñan los Contratos Inteligentes, para que por medio de parámetros que se informen desde fuera de la Blockchain (off-chain), estos pueden modificar su comportamiento.

Principales Blockchain y Framework de desarrollo

También incluimos un análisis de las principales Blockchain o Frameworks para el desarrollo de Blockchain que existen actualmente en mercado, destacando las soluciones de Blockchain de Ethereum, Hyperledger, XinFin, Quorum y Corda R3.

En este punto, en el cuerpo del presente trabajo se analizó detalladamente las ventajas, desventajas y riesgos que implica la adopción de cada solución específica.

Algoritmos de consenso

Por otra parte, también se analizaron como factor preponderante de la evaluación de infraestructura Blockchain, a los algoritmos de consenso que pueden implementar las diferentes Cadenas de Bloque.

El mecanismo de consenso es el método por el cual la Blockchain valida transacciones, coordinando todos los servidores de red para que todos ellos vean la misma registración. Esto constituye un eje fundamental en la Blockchain ya que es el punto neurálgico del que se deriva la robustez, inalterabilidad e invulnerabilidad de red.

Según sea la definición de la estrategia de desarrollo de la Plataforma Blockchain NFT/FT para la provincia de Santa Fe que se consigne, se deberá evaluar críticamente la el peso específico de los consensos utilizados por cada tipo de Blockchain que se puedan utilizar como infraestructura. A este fin, en la parte respectiva del presente trabajo, se realizó un análisis detallado de funcionamiento, ventajas y desventajas de los principales algoritmos de consenso utilizados por las Blockchain más difundidas.

Informe, a modo de perfil, del proyecto de desarrollo de la Plataforma para generación y gestión de tokens criptográficos, de la Provincia de Santa Fe

Introducción

En el presente tramo nos vamos a centrar en un análisis de metodologías vinculadas a la gestión del proyecto que se propone. Para esto analizaremos las metodologías más comunes utilizadas, y cuando sea relevante vamos a destacar los “diferenciales” que se deberían tomar en cuenta para adaptar algunos aspectos metodológicos a los requerimientos propios del proyecto de desarrollo de la Plataforma BCT NFT/FT.

En búsqueda de un plan de desarrollo o mapa de ruta útil que presente paso a paso las decisiones, actores, riesgos, responsabilidades a tomar en consideración, entendemos como la aproximación más cercana a esto, el CBDC Policy-Maker Toolkit elaborado por el World Economic Forum (Foro de Davos). Si bien el proyecto de desarrollo de una CBDC (Moneda Digital de Banco Central), difiere del proyecto de desarrollo de una Plataforma BCT NFT/FT que nos ocupa, encontramos muchos puntos de discusión y ámbitos similares, especialmente en la consideración de la gestión del proyecto por parte de un gobierno en lugar de particulares, la tecnología subyacente (Blockchain o semejante), los actores involucrados, y más otros aspectos relevantes. A ese fin, fuimos indicando los puntos que consideramos difieren del perfil de un proyecto a otro, como así también los que no serían aplicables.

Posteriormente a esto, identificamos en el presente trabajo a las metodologías de gestión de proyecto más difundidas en el ámbito organizacional, y de igual manera que con el CBDC Policy-Maker Toolkit, fuimos analizando y destacando aspectos que difieren en función de consideraciones especiales que se deberían hacer con respecto a su implementación en el proyecto de la Plataforma BCT NFT/FT. Se hizo un apartado especial para la discusión de utilización de las denominadas “metodologías ágiles”, como también del conocido “manifiesto agile”.

Por último, desglosamos los ejes más relevantes del Project Management Body of Knowledge, conocido como PMBOK Guide, del Project Management Institute, Inc. Esta guia de aspectos relevantes para la gestión de proyectos es la más utilizada y difundida a nivel mundial. Al igual que con los temas previamente mencionados, también fuimos destacando en los casos que fuese menester, las diferencias o consideraciones particulares que deberían tomarse en cuenta en forma diferencial desde el enfoque del desarrollo de la Plataforma BCT NFT/FT.

Central Bank Digital Currency Policy-Maker Toolkit.

En enero de 2020 el Foro Económico Mundial (World Economic Forum, WEF - también conocido como Foro de Dabos) emitió un documento denominado "The World Economic Forum's CBDC Policy-Maker Toolkit" (Kit de herramientas para políticas sobre CBDC - Moedas Digitales de Bancos Centrales - por sus siglas en inglés). El objetivo principal de este documento es proporcionar a los responsables de políticas públicas una guía práctica para comprender, evaluar y diseñar CBDC - Monedas Digitales de Bancos Centrales.

La CBDC es una forma de dinero digital emitida por un banco central y respaldada por la autoridad monetaria de un país.

El kit de herramientas abarca una amplia gama de temas relacionados con las CBDC, incluyendo aspectos técnicos, legales, regulatorios, de gobernanza, privacidad y seguridad. Proporciona una visión general de las CBDC, explorando diferentes modelos y enfoques adoptados por diferentes países. También destaca las consideraciones clave que los responsables de políticas públicas deben tener en cuenta al evaluar la implementación de una CBDC, como la estabilidad financiera, la inclusión financiera, la privacidad y la seguridad cibernética.

De esta forma el kit de herramientas que desarrolló el WEF, busca brindar a los responsables de políticas públicas una comprensión clara de los conceptos, beneficios y riesgos asociados con las CBDC, así como una estructura para la toma de decisiones relacionadas.

En relación a este último aspecto del kit de herramientas CBDC (estructura para la toma de decisiones) y en virtud de haber podido encontrar una metodología propia y específica al desarrollo de una plataforma de implementación NTF/TF que nos ocupa, es que hemos decidido usar como base para el proceso decisorio vinculado al mismo, los lineamientos planteados por el documento de WEF mencionado.

El "The World Economic Forum's CBDC Policy-Maker Toolkit" (Kit de herramientas para políticas sobre CBDC - Moedas Digitales de Bancos Centrales - por sus siglas en inglés), estructura el proceso de análisis y decisiones vinculadas al desarrollo de CBDC, en 5 fases claramente diferenciadas, como muestra la figura siguiente:

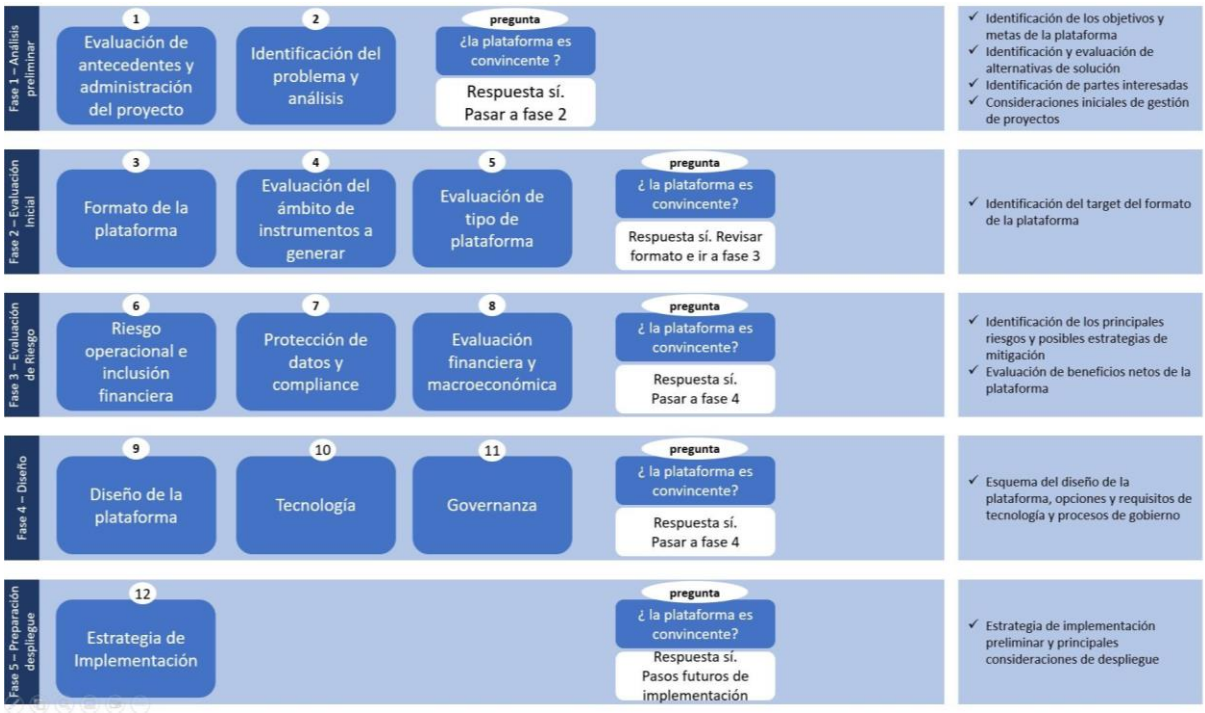


Figura 44

Extraído de "The World Economic Forum's CBDC Policy-Maker Toolkit", con modificaciones para adaptarlo al desarrollo de una plataforma NFT/FT.

WEF - World Economic Forum - https://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf

Observado: abril 2023

Vamos a analizar cada una de las cinco fases que propone el Kit de Herramientas, realizando las adecuaciones y consideraciones correspondientes a lo que sería el proyecto para desarrollar la plataforma Blockchain para NFT y FT para la provincia de Santa Fe.

FASE 1 - Análisis Preliminar

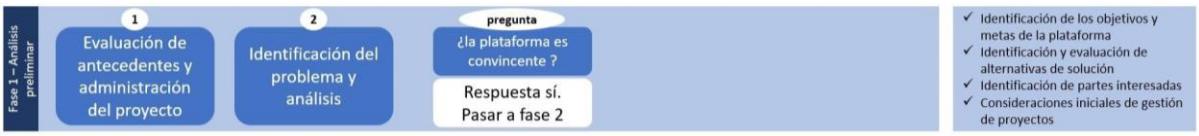


Figura 45 Fase 1: Análisis preliminar

En la "Fase 1: Análisis preliminar", se abordan los siguientes aspectos:

1. Identificación de objetivos y contexto:

El toolkit sugiere que los responsables de la toma de decisiones definan claramente los objetivos y el contexto para la posible implementación de una Plataforma Blockchain para el

desarrollo de NFT/FT. Esto implica comprender los desafíos y oportunidades que la Plataforma podría plantear, así como los posibles beneficios que podría ofrecer.

2. Evaluación de necesidades y beneficios:

Se recomienda realizar un análisis exhaustivo de las necesidades y los beneficios potenciales de una Plataforma BCT para desarrollo de NFT/FT, dentro del contexto económico y financiero del país y particularmente de la provincia de Santa Fe. Esto incluye evaluar cómo una Plataforma BCT para desarrollo de NFT/FT podría enriquecer a los instrumentos financieros existentes, acceso al crédito, formas innovadoras de acceso a financiación empresarial, mejora en la inclusión financiera, facilitar pagos digitales, formas de inversión y promover la innovación tecnológica en general.

Este análisis se espera brinde una visión más definida del contexto y motivación para el proceso de análisis crítico vinculado al desarrollo de la Plataforma BCT para el desarrollo de NFT/FT.

Los responsables de la formulación de políticas deberían considerar las siguientes

preguntas estratégicas de alto nivel:

– ¿Cuáles son las principales prioridades actuales y los objetivos estratégicos de la Provincia de Santa Fe, en relación con los medios de financiación empresarial, como de colocación de inversiones innovadoras, especialmente las vinculadas a la tokenización económica por medio de una Plataforma BCT NFT/FT?

– ¿Cuáles son las limitaciones del gobierno que podrían influir en la investigación y el desarrollo de la Plataforma?

– ¿Existe una agenda de investigación o estudio relacionada con Plataformas BCT?

– ¿Cuál es el conocimiento, la experiencia y la pericia de los recursos humanos internos relacionados con BCT?

– ¿Se exploró o consideró implementaciones de Blockchain de alguna forma en el pasado?

– ¿Cuáles son las creencias positivas o negativas actuales relacionadas con la tecnología de Blockchain, y especialmente con la economía de tokenización?

– ¿Existe demanda e interés en una Plataforma BCT para desarrollo de NFT/FT entre otras partes interesadas en la economía?

3. Evaluación legal e institucional

Se deberá llevar a cabo una evaluación detallada de las implicaciones legales de la implementación de una Plataforma BCT para el desarrollo de NFT/FT. Esto probablemente implicará realizar una revisión de la legislación existente en relación con medios innovadores de acceso a financiación, inversiones en activos financieros criptográficos, evaluación de los diferentes instrumentos y artefactos vinculados a finanzas descentralizadas (DeFi) que en experiencias internacionales se vienen desarrollando en el ecosistema cripto y otros aspectos relevantes. También se deben abordar consideraciones legales tangenciales, pero

relevantes, como las relacionadas con la privacidad, la protección de datos y el cumplimiento normativo.

Los responsables de la formulación de políticas públicas deben analizar cómo la implementación de la Plataforma afectará a las instituciones existentes, como los bancos mayoristas y minoristas, tanto privados como públicos, y otros actores y canales del sistema financiero. Se deben considerar aspectos externos vinculados a la Plataforma, que puedan ser impactados localmente, como la estabilidad financiera global, la gobernanza, la supervisión y la gestión de riesgos.

Algunas de las preguntas guías de carácter estratégicas vinculada a este análisis pueden ser:

– ¿Cuál es el papel del estado provincial en el fomento de formas innovadoras de acceso a financiamiento empresarial, y a colocación de inversiones por medio de tokenización? ¿cuál en la facilitación de acceso a la tecnología de Blockchain

– ¿Está la facilitación de emisión de tokens criptográficos dentro de las atribuciones del gobierno provincial, considerando las operaciones y la supervisión del ecosistema que sobre la plataforma se puedan generar? ¿Es legalmente permisible? Si es relevante, ¿son posibles los cambios que permitirían generar la Plataforma

– ¿Qué requisitos con respecto a las leyes y la supervisión legal existen que limitan o informan a la Plataforma que facilite el desarrollo de NFT/FT, incluido el cumplimiento de normativas vinculadas como LAFT (Lavado de Activos y Financiación del Terrorismo)?

– ¿Qué posibles obstáculos legales o restricciones reglamentarias existen ?

– ¿Los requisitos legales y reglamentarios existentes son compatibles con la implementación de la Plataforma o será necesario desarrollar diferentes estándares antes de la implementación?

4. Aporte de múltiples partes interesadas

El toolkit del WEF también destaca la importancia de involucrar a diversos actores relevantes en la evaluación, tanto legal e institucional, como en medición de impacto, de la implementación de la Plataforma. Algunos de estos actores / interesados a considerar pueden ser: legisladores, reguladores, BCRA y CNV, instituciones financieras y grupos de defensa del consumidor, entre otros.

La participación activa de múltiples partes interesadas ayuda a abordar los aspectos relevantes de la Plataforma a desarrollar, identificar desafíos potenciales y garantizar la legitimidad y aceptación de la Plataforma en sí. Además, el Toolkit del WEF destaca la importancia de establecer mecanismos transparentes y efectivos de colaboración con las

partes interesadas en todas las fases del proyecto, no solo en la fase de análisis preliminar que estamos analizando en este momento.

Algunos aspectos claves de la identificación de múltiples partes interesadas que propone el Toolkit pueden ser:

Identificar partes interesadas clave: Se debe identificar a las partes interesadas clave que tienen un interés directo en la implementación de la Plataforma BCT para el desarrollo de NFT/FT. Esto puede incluir a bancos, instituciones financieras, proveedores de servicios de pago, reguladores, legisladores, grupos de defensa del consumidor y la sociedad civil en general.

Establecer un diálogo estructurado: Se sugiere fomentar un diálogo estructurado y colaborativo con las partes interesadas identificadas. Esto implica organizar reuniones, talleres o mesas redondas en las que se puedan discutir abiertamente los aspectos relacionados con la Plataforma, su alcance, impacto, y disparadores de innovación tecnológica que puede generar. El objetivo es obtener diferentes perspectivas y conocimientos para gestionar el proceso de toma de decisiones.

Recopilación de aportes y retroalimentación: Se deberá permitir que las partes interesadas compartan sus conocimientos, preocupaciones y recomendaciones sobre la Plataforma. Esto se puede lograr mediante la recopilación de aportes escritos, presentaciones orales, encuestas o cualquier otro medio adecuado para recopilar información valiosa. Incluso, recurrir a la gestión de publicaciones en redes sociales o comunidades virtuales, que puedan apalancarse como medios de comunicación efectiva.

Análisis y consideración de los aportes: Es fundamental analizar y considerar los aportes de las partes interesadas de manera imparcial y objetiva. Los formuladores de políticas públicas vinculados al desarrollo de la Plataforma, deben evaluar los diferentes puntos de vista y utilizarlos para enriquecer su análisis preliminar y la toma de decisiones posteriores.

Algunas de las preguntas estratégicas y guías que se pueden formular en esta etapa serían:

– ¿ Qué partes del sector público o privado están obligadas a proporcionar información o consultas sobre una posible Plataforma BCT para desarrollo de NFT/FT ?

– ¿ De qué instituciones o partes interesadas sería beneficioso solicitar aportes ?

– ¿ Qué partes interesadas adicionales deberían estar representadas e involucradas en la toma de decisiones ?

– ¿ Cómo se gestionará la coordinación entre las distintas partes interesadas ?

5. Inicio, gestión y toma de decisiones del proyecto

Los aspectos relevantes al proceso de toma de decisiones para el diseño y la implementación de la Plataforma BCT para desarrollo de NFT/FT debe determinarse en las primeras etapas del ciclo de vida de la gestión del proyecto.

Las preguntas y consideraciones que se deberían incluir son:

– ¿ Cómo se identificará el grupo de trabajo base que gestione y diseñe el proceso de desarrollo de la Plataforma ? ¿ Podrán los representantes de departamentos y áreas específicas del gobierno conformar el grupo de trabajo ? ¿ Cómo se manejará la coordinación sobre el proyecto dentro del gobierno provincial ?

– ¿ Cuál es la estrategia y el conjunto de reglas que rigen la toma de decisiones relacionadas con la Plataforma ?

– ¿ Cuál será el grado de autonomía que tendrá el gobierno provincial en el diseño, desarrollo y despliegue de la Plataforma ?

FASE 2 - Evaluación Inicial

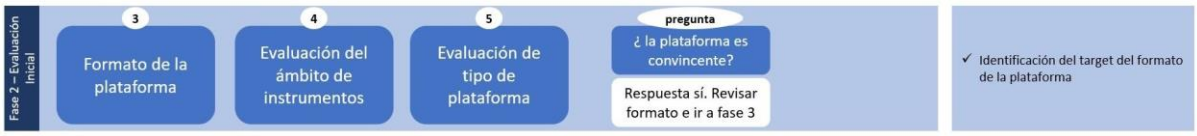


Figura 46 Fase 2: Evaluación inicial

La "Fase 2: Evaluación inicial" del "Central Bank Digital Currency Policy-Maker Toolkit" del Foro Económico Mundial se centra en aspectos técnicos, funcionales y económicos / financieros relacionados con la implementación de la Plataforma BCT para el desarrollo de NFT/FT. Proporciona orientación sobre la evaluación técnica, el diseño y forma de la Plataforma, impacto y fundamentalmente la alineación de la selección de opciones de forma de la Plataforma, con los objetivos que se persigue.

En el Toolkit de CBDC de WEF, en este punto se sugiere analizar detenidamente los formatos de CBDC que se quieran desarrollar tomando en consideración si la Moneda Digital de Banco Central se piensa desarrollar como CBDC mayorista o minorista, y si va a ser de uso doméstico o para pagos internacional, tomando en cuenta la combinación de estas clasificaciones. Un apartado adicional se realiza con respecto a las “Hybrid CBDC” definidas originalmente por el trabajo de julio 2019 del Fondo Monetario Internacional “The rise of Digital Money”.[71]

La configuración de la Plataforma y las diferentes opciones de desarrollo vinculadas a la misma, fue un tema desarrollado con mayor detenimiento en la Tarea 5: “Confeccionar un relevamiento y análisis de las variantes de plataformas basadas en Blockchain, para el desarrollo, despliegue e implementación de NFT y FT. Se considerarán, diferentes plataformas de Blockchain de código abierto para implementar Contratos Inteligentes, Tokens, NFT, FT, estrategias de desarrollo, gobernanza, y otros.”

Sin perjuicio de esto, el toolkit realiza una revisión de experiencias y actores vinculados directa e indirectamente a los formatos entre los cuales se debería optar de desarrollar la Moneda Digital de Banco Central en cuestión. Esta enumeración la realiza con la finalidad de que los decisores de políticas, puedan encontrar un relevamiento inicial del ecosistema y casos de uso.

[71] Adrian, T., & Mancini-Griffoli, T. (2021). The rise of digital money. *Annual Review of Financial Economics*, *13*, 57-77.
https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097
Observado: mayo 2023

En el caso que estamos desarrollando, el ecosistema de DeFi - Finanzas descentralizadas con el que se podría vincular la Plataforma BCT para desarrollo de NFT/FT, fue desarrollado en la Tarea 4. En la descripción de cada tipo de herramienta de finanzas descentralizadas de la tarea, se pueden encontrar diferentes casos de uso y desarrollos en marcha dentro del mundo cripto.

Most relevant for retail CBDC
– Domestic or overseas payment service providers (PSPs)
– Examples: Alipay and WeChat in China, Swish in Sweden, Paytm in India, M-Pesa in Kenya, Venmo in the US
– Fast retail payment systems
– Examples: BiR in Sweden, FPS in the UK, FAST in Singapore, CD/ATM system in South Korea, IBPS in China, IMPS in India, TIPS and RT1 in Europe, FedNow Service in the US (under development)
– Globally available cryptocurrencies
– Examples: bitcoin (BTC), ether (ETH)
– Stablecoins
– Examples: CENTRE Foundation's USDC, Tether, Libra token, MakerDAO's Dai, Paxos Standard, Gemini Dollar
Most relevant for wholesale CBDC
– Innovations in existing/legacy market infrastructures
– Examples: SWIFT gpi initiative
– Crypto-assets designed for inter- or intrabank payments and settlements
– Examples: JPM Coin, XRP
– Collaboratively developed DLT-driven interbank payment systems
– Example: Utility Settlement Coin (USC)
Relevant for wholesale or retail CBDC
– Foreign-country CBDC
– Examples: China (DC/EP, under development) and others

Figura 47 diferentes casos de uso que el toolkit de CBDC del WEF

Imagen ilustrativa de los diferentes casos de uso que el toolkit de CBDC del WEF, presenta para las diferentes clasificaciones de formatos de Monedas Digitales de Bancos Centrales.

FASE 3 - Evaluación de Riesgos

Figura 48 Fase 3: Evaluación de riesgos

La "Fase 3: Evaluación de riesgos" del "Central Bank Digital Currency Policy-Maker Toolkit" del Foro Económico Mundial se enfoca en la identificación y evaluación de riesgos asociados con la implementación de una Plataforma BCT de desarrollo de NFT/FT. Proporciona directrices para evaluar los riesgos técnicos, legales, regulatorios, financieros y operativos, y sugiere medidas de mitigación adecuadas para abordarlos.

Riesgo operativo

Algunas de las consideraciones que el toolkit de CBDC realiza en relación al riesgo operativo de emisión de CBDC son:

- *"Falla de la red y riesgos operativos: para todas las formas de CBDC, dado que los pagos son parte integral de la economía, el banco central y los responsables de la formulación de políticas deben buscar habilitar el mayor grado posible de disponibilidad del sistema, implementando salvaguardas y planes de contingencia que reduzcan los riesgos de interrupción del sistema.*

La disponibilidad del sistema CBDC y el acceso continuo las 24 horas del día, los 7 días de la semana deben diseñarse para considerar a las personas que viven fuera del alcance de Internet o que no tienen acceso regular a Internet; esto es esencial para los refugiados y las personas que viven en entornos remotos.

- *El sistema también debe proteger la disponibilidad de CBDC de la interrupción física de los sistemas o la infraestructura (por ejemplo, interrupciones de electricidad a gran escala por tormentas).*

- *Riesgos de ciberseguridad: los bancos centrales deben crear precauciones y políticas sólidas de resiliencia cibernética para reducir los riesgos de los ataques cibernéticos. Deben operar bajo el supuesto de que un ciberatacante tiene recursos ilimitados, ya que no es impensable que el atacante pueda ser un gobierno extranjero."*

Algunas consideraciones de lo expuesto, en referencia a su adaptabilidad con referencia a la Plataforma BCT para desarrollo de NFT/FT:

Falla en la red:

En referencia a lo establecido con respecto al primer riesgo asociado al proyecto, el de falla de la red y riesgos operativos, podemos realizar las siguientes consideraciones.

Las CBDC - Monedas Digitales de Bancos Centrales, no necesariamente son desarrolladas con tecnología Blockchain. En la mayoría de los casos se respeta que sean DLT - Tecnología de Registro Distribuido, pero no necesariamente utilizan la tecnología de Blockchain para sustentarla.

Asimismo, en el caso que se decida en una CBDC utilizar la tecnología de Blockchain, las autoridades monetarias de los diferentes países, no van a ceder el control de la red a una red totalmente descentralizada como son las Blockchains públicas (o no permisionadas). De allí que implementen Blockchain privadas (permisionadas), o Blockchain de consorcio, las cuales son una variante de las anteriores.

Todos estos aspectos se deben evaluar en función que, al no utilizarse la tecnología de Blockchain, o usando la misma en forma permisionada, se está disminuyendo el grado de invulnerabilidad que la misma posee al registrar redundantemente la información y organizarla criptografiada en bloques.

Probablemente las decisiones vinculadas al tipo de Blockchain que se adoptará para el desarrollo de la Plataforma BCT para desarrollo de NFT/FT, se vuelquen hacia el uso de una Blockchain permisionada también, en tanto el gobierno de Santa Fe, querrá mantener el control de la misma por medio de determinados servidores con permisos especiales. Sin embargo, también se podría llegar a evaluar para el proyecto de la Plataforma BCT NFT/FT, la adopción de una red pública como Ethereum o una clonada de esta. Esta posibilidad es casi impensada para una Moneda Digital de Banco Central.

Protección de datos y compliance

Algunos de los aspectos que el toolkit CBDC de WEF destaca en vinculación con la protección de datos personales son:

- equilibrar los objetivos de privacidad de los datos de los usuarios con los requisitos de AML/CFT (acciones contra el lavado de dinero y combate contra la financiación del terrorismo, por sus siglas en íngles).

- proteger el acceso público a las transacciones realizadas por los usuarios, por medio de las cuales se pueda realizar un seguimiento de hábitos de gastos e identificación de datos personales confidenciales.
- implementar estrictas políticas y protecciones de privacidad, para evitar entre otros tratamientos discriminatorios de los usuarios en virtud de sus preferencias/habitos de gastos y pertenencia a sub-poblaciones o grupos culturales.
- la privacidad de datos personales de los usuarios no solo debe considerarse en el ámbito interno del país, sino también en la factibilidad de ataques externos por parte de otros países que maliciosamente pretendan utilizar esa información sensible.

Acerca del tema de protección de datos personales, y en relación a las tentativas adecuaciones del objeto del toolkit CBDC de WEB con respecto a la Plataforma para el desarrollo de NFT/FT, debemos destacar que el objeto, funcionalidad y alcance de una CBDC es mucho más amplio que los instrumentos digitales que se puedan generar por medio de la Plataforma. No pudiendo ser obviada la condición de obligatoriedad de una moneda de curso legal que reviste una CBDC. Por todo esto, es lógico asumir que la privacidad y protección de datos de una Moneda Digital de Banco Central debe ser observada más rigurosamente que en el caso que nos comprende (en la Plataforma BCT para desarrollo de NFT/FT).

Hecha esta salvedad, es de destacar, que una de las consideraciones más relevantes que deberíamos realizar sobre el desarrollo de la Plataforma BCT para NFT/FT, es que la misma encuentra como fundamento la posibilidad cierta que el gobierno de la provincia de Santa Fe pueda tener un control más cercano sobre los instrumentos financieros digitales que se desarrollen en su ecosistema Blockchain. De esta forma se estaría facilitando a los usuarios el despliegue de sus desarrollos en un ambiente similar al de una Blockchain pública, pero con única salvedad de poseer un control de identidad y de acciones de sus usuarios.

Esto no necesariamente es opuesto a la protección de datos personales, ya que el gobierno de la Provincia de Santa Fe, debería garantizar la imposibilidad de acceso de terceros a esa información sensible.

A este respecto es procedente lo que el toolkit WEF sugiere en referencia a los datos privados de usuarios, y a su gobernanza:

“Podría ser prudente desarrollar una política de datos de usuarios que articule claramente las reglas para la gestión, el acceso, la privacidad y la custodia de los datos. Debe reducir cualquier conflicto de interés aplicable y estar claramente conectado a los procesos de gobierno con requisitos estrictos y sanciones por violaciones.”

Evaluación Financiera y Macroeconómica

Algunas de las preguntas guías y estratégicas que el toolkit sugiere deberían realizarse los responsables de formulación de políticas a cargo del proyecto son (adaptadas para el desarrollo de Plataforma BCT para NFT/FT):

– ¿Qué objetivos macroeconómicos y financieros u oportunidades, y el grado de impacto, podría permitir el desarrollo de la Plataforma en la economía local ?

– ¿Qué riesgos macroeconómicos y financieros, en relevancia de su impacto, es importante considerar? ¿Qué soluciones o estrategias pueden mitigar los riesgos?

– ¿Quiénes tendrán acceso al uso de la Plataforma, en términos de ciudadanos e instituciones financieras nacionales y extranjeras?

– ¿Cuál es el efecto previsto en el sector financiero impactado? ¿Cómo se espera que cambien las funciones y los modelos comerciales de financiamiento empresarial y colocación de inversiones en ambientes digitales, después de que se implemente la Plataforma?

– ¿Qué tipos adicionales de empresas se verían afectadas positiva o negativamente por la Plataforma a desarrollar?

– ¿Cuáles serían las implicaciones de la Plataforma para el entorno político provincial, las instituciones gubernamentales y la geopolítica?

– ¿Qué decisiones de política macroeconómica se deben tomar con respecto a la Plataforma?

– ¿Habrá actividad crediticia asociada con el desarrollo de “DeFi Lending” (sistemas de préstamos descentralizados) en la Plataforma? ¿Por qué o por qué no?

….

FASE 4 - Diseño

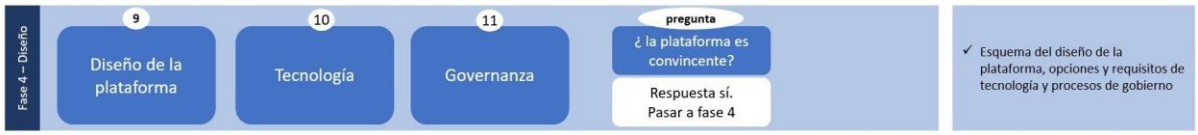


Figura 49 FASE 4 - Diseño

En esta fase, los responsable de la formulación de políticas públicas deben considerar cómo debe diseñarse la Plataforma para lograr los resultados previstos y mitigar los riesgos identificados en las secciones anteriores de este conjunto de herramientas.

Diseño de la Plataforma

Algunos de los lineamientos que el toolkit define para el diseño de la CBDC, y con las adecuaciones que consideramos deberían ser considerara para el diseño de la Plataforma son:

Disponibilidad/acceso: ¿Para qué entidades / organizaciones debería estar disponible la Plataforma BCT para desarrollo NFT/FT? ¿Debería haber restricciones o regulaciones especiales para las empresas/organizaciones que deseen participar en la Plataforma como desarrolladoras de sistemas de financiación, o de como colocadoras de inversiones en activos digitales?

¿deberían existir restricciones para el acceso y uso de la Plataforma por parte de organizaciones o empresas extranjeras?

¿Cuáles serían las restricciones o regulaciones que tendrían en el acceso a la Plataforma, los bancos comerciales o de inversión extranjeros, las empresas no bancarias, los fondos de inversión, y demás instituciones financieras de importancia sistémica?

Custodia y almacenamiento: ¿Dónde se implementará la Blockchain que sustente a la Plataforma, en el caso que sea una Blockchain permisionada (privada)? Esto en relación a la ubicación de nodos servidores (con permisos especiales)

Anonimato: ¿hasta qué punto los usuarios, el saldo de la cuenta y la información de la transacción son privados o seudónimos? ¿en ese sentido, qué ocurre con los Contratos Inteligentes que se despliegan en la Plataforma?

¿Qué políticas regulatorias, legales o de cumplimiento limitarán el anonimato? ¿Cuáles son los objetivos de la Plataforma con respecto al rastreo, monitoreo o anonimato de

transacciones y de Contratos Inteligentes? ¿El grado de anonimato se debería corresponder con el tamaño de las transacciones / operaciones de los Contratos Inteligentes?

Límites de cuentas y transacciones: ¿debería haber límites o restricciones sobre el tamaño de las transacciones o el saldo total de la cuenta / monto de operaciones por medio de Contratos Inteligentes?

Pago de intereses: No aplica → Debería analizarse la implementación de beneficios directos / indirectos a los usuarios, en el caso que se desee incentivar el desarrollo de mercados de activos digitales por medio de la Plataforma

Tasas de conversión y redención: No aplica

Plazos y finalidad de la liquidación: No aplica

Funciones de programabilidad: ¿ además de Contratos Inteligentes que se desplieguen por parte de usuarios en la Plataforma para gestionar activos financieros digitales, debería el gobierno desarrollar propios? ¿con qué alcance?

Elecciones de Tecnología. Consideraciones y riesgos

Los aspectos relevantes a las elecciones de infraestructura que se deberían realizar al abordar el proyecto de desarrollo de una Plataforma BCT para NFT/FT, fueron planteados en la tarea 05 - “Confeccionar un relevamiento y análisis de las variantes de plataformas basadas en Blockchain, para el desarrollo, despliegue e implementación de NFT y FT. Se considerarán, diferentes plataformas de Blockchain de código abierto para implementar Contratos Inteligentes, Tokens, NFT, FT, estrategias de desarrollo, gobernanza, y otros.”

Sin perjuicio de esto, creemos conducente, al igual que en puntos anteriores, recalcar algunos de los puntos esenciales para el análisis de esta fase, y relevar las preguntas-guías que presenta el toolkit, realizando la obvia adecuación de un proyecto de desarrollo de CBDC, con respecto a un proyecto de desarrollo de una Plataforma BCT para NFT/FT.

Los aspectos ineludibles que se deberían abordar en la evaluación de elecciones de tecnología son:

1. **Seguridad cibernética**: Evaluar los riesgos de seguridad y las vulnerabilidades asociadas con la infraestructura tecnológica utilizada para el desarrollo de la Plataforma, incluyendo la protección de datos, la prevención del fraude y la protección

contra ataques cibernéticos, tanto a nivel de transacciones, como de implementación de Contratos Inteligentes.

2. **Escalabilidad y rendimiento**: Considerar la capacidad de la infraestructura tecnológica para manejar grandes volúmenes de transacciones como así también poder ejecutar, por medio de máquina virtual, los eventos y acciones de los Contratos Inteligentes implementados, asegurando un rendimiento eficiente en tiempo real.
3. **Interoperabilidad:** Evaluar la capacidad de la tecnología para facilitar la interoperabilidad de la Plataforma, con otras Plataformas, sistemas de pago/cobros, billeteras digitales, Exchanges, y en general otros activos criptográficos. Tanto a nivel nacional como internacional. En este punto toma relevancia los desarrollos que se vienen realizando en interoperabilidad de Blockchains por medio de plantillas de Contratos Inteligentes (como por ejemplo ERC-20), como también interfaces con ZKP (Pruebas de Conocimientos Cero).
4. **Privacidad y anonimato:** Diseñar mecanismos tecnológicos que garanticen la privacidad y protección de datos de los usuarios de la Plataforma al tiempo que se cumplen los requisitos regulatorios, tal como se planteó en el punto anterior de análisis, referido a diseño de elementos.
5. **Actualizaciones y mantenimiento:** Considerar cómo se realizarán las actualizaciones y el mantenimiento de la infraestructura tecnológica subyacente de la Plataforma, asegurando la continuidad y la adaptabilidad a los cambios tecnológicos futuros, y evaluando las actualizaciones de la Blockchain subyacente que se haya elegido.

Dentro de las preguntas-guías que deberían plantearse los responsables del proyecto, mencionadas por el toolkit de CBDC, y con las adecuaciones a un proyecto de Plataforma BCT para NFT/FT, podemos enumerar:

Funcionalidades principales

¿Qué características son prioritarias?

– Escalabilidad y rendimiento de transacciones

– Privacidad y confidencialidad de la información de la transacción

– Inalterabilidad de las transacciones

– Interoperabilidad con los sistemas e infraestructuras de pago existentes, billeteras digitales, Exchanges y otras Plataformas BCT.

Evaluación de tecnología

– ¿Cuáles son las compensaciones, ventajas y desventajas asociadas con varias opciones tecnológicas?

– Al basarse la Plataforma en tecnología Blockchain, ¿quiénes servirían como nodos de validación? ¿Qué plataforma y algoritmo de consenso puede ser relevante emplear y por qué?

– ¿Qué proveedores de tecnología, servicios o expertos pueden apoyar la implementación?

– ¿Qué tecnologías pueden ser las más adecuadas y por qué?

Evaluación de costos

– ¿Qué restricciones de costos existen para la implementación de la Plataforma?

– ¿Cuánto costará implementar esta tecnología objetivo?

– ¿Cuánto mantenimiento se necesitará con esta tecnología y cuáles son los costos asociados?

Debería tomarse en cuenta en este punto el concepto TCO (Total Cost of Ownership - Costo Total de Apropiación), es decir, consideración de Hardware, Software, Capacitación, Consultoría, Mantenimiento, y todos aquellos costos vinculados directa e indirectamente a que el proyecto se implemente en forma óptima.

Ciberseguridad y resiliencia

– ¿Cuáles son las vulnerabilidades de ciberseguridad que podrían tener la Plataforma ?

– ¿Cuáles son los requisitos apropiados de resiliencia cibernética?

¿Cómo se puede estudiar la ciberresiliencia del sistema?

– ¿Qué estándares y técnicas de ciberseguridad deben ser

identificados para reducir los riesgos cibernéticos?

– ¿Cuáles son los requisitos continuos de monitoreo de ciberseguridad para la implementación de esta tecnología? ¿Cómo se llevarán a cabo el monitoreo y las actualizaciones para que sean mínimamente perjudiciales?

Consideraciones adicionales

– ¿Cuánto se ha desplegado y probado esta tecnología en el mundo? ¿Hay suficiente disponibilidad y experiencia del desarrollador de software para respaldar la plataforma?

– ¿Cuáles son los requisitos de monitoreo continuo de esta tecnología?

Interoperabilidad e integración

No aplica directamente para el desarrollo de la Plataforma BCT para NFT/FT.

Gobernanza

La gobernanza implica las reglas y prácticas que rigen el ciclo de vida de la Plataforma BCT para NFT/FT.

El buen gobierno es un elemento crucial para una implementación exitosa y no debe pasarse por alto. El toolkit CBDC de WEF, sugiere atender a la siguiente lista para definir una clara gobernanza con las partes interesadas (al igual que en los casos anteriores, hemos modificado los puntos en cuestión en función del proyecto Plataforma BCT para NFT/FT).

Evaluación jurídica

– ¿Qué requisitos existen con respecto a las leyes y la supervisión legal?

– ¿Sería políticamente factible el desarrollo de la Plataforma? ¿Cómo podrían las limitaciones políticas afectar el diseño de la Plataforma ? (Por ejemplo, ¿sería políticamente sostenible una competencia entre sistemas de financiación empresarial tradicionales y sistemas digitales como el que se podría desarrollar en la Plataforma?)

– ¿Cómo se determinará el interés público en la Plataforma?

– ¿Debería haber alguna consideración especial si hay un

próximo ciclo electoral?

– ¿La Plataforma es compatible con la infraestructura del mercado financiero existente y qué validación legal debe realizarse para garantizar que las operaciones financieras basadas en la Plataforma, sean legalmente exigibles?

Compromiso del usuario

– La participación y la consulta de los usuarios son fundamentales para un diseño efectivo de la Plataforma; los usuarios deben participar tan pronto como sea posible en el proceso de desarrollo de la Plataforma.

– ¿Cómo se puede consultar a los usuarios finales (el público, tomadores de créditos, inversores, etc.) sobre la Plataforma y proporcionar información para el proceso de diseño y prueba?

– ¿Qué requisitos de solución existen para la usabilidad, las interfaces de usuario, la gestión de identidades y claves, la privacidad y la seguridad?

– Podría ser valioso proporcionar una guía de usuario o preguntas frecuentes para varias clasificaciones de participantes, con recursos educativos e información básica sobre cómo participar con éxito en la Plataforma.

Gestión financiera

– ¿Cómo se llevará a cabo la gestión financiera y el seguimiento del proyecto?

– ¿Cuáles costos, si es que los hay, podrían tener los usuarios de la Plataforma, para desarrollar productos financieros digitales, o hacer uso de estos, y quién es responsable de administrar esos costos?

Identificación de criterios de desempeño

Los criterios de desempeño deben identificarse antes del lanzamiento de la Plataforma para:

1) establecer objetivos y metas relevantes;

2) medir el éxito e identificar áreas de mejora;

3) inculcar responsabilidad en el programa; y

4) garantizar el éxito en el cumplimiento de los requisitos de gestión de riesgos y seguridad.

Debe determinarse una frecuencia de evaluación específica (p. ej., semanal o mensual).

Terminación de la Plataforma

Se podría identificar un plan de terminación antes de la implementación del proyecto. El plan puede incluir las siguientes consideraciones:

– ¿Qué condiciones indicarían que el proyecto de desarrollo de la Plataforma debería terminarse?

– ¿Qué obligaciones deberían cumplirse antes de la rescisión para reducir las interrupciones y los riesgos para los usuarios?

– ¿Cómo se puede garantizar la seguridad de los ahorros públicos de la Plataforma?

– ¿Cómo se destruirían los tokens que se hubiesen generado en la Plataforma (en el caso que se haya llegado a emitirlos)?

Consideraciones adicionales

– ¿Cómo se monitoreará, evaluará y controlará el impacto ambiental y la huella de la Plataforma ? (especialmente el consumo de energía eléctrica, si se decide utilizar protocolos de consenso como el POW - Prueba de Trabajo).

– ¿Puede un tercero, como una institución encargada de hacer cumplir la ley, congelar los activos de una cuenta de la Plataforma y en qué circunstancias?

– ¿Qué otros riesgos de implementación y consecuencias no deseadas se deben considerar?

FASE 5 - Implementación

Figura 50 FASE 5 - Implementación

El toolkit en esta sección propone informar consideraciones y requisitos vitales antes de implementar el desarrollo de la Plataforma prevista.

Los formuladores de políticas deben considerar los siguientes temas, entre otros, como parte de una estrategia de implementación de la Plataforma:

Experimentos y prototipos

El ambiente de desarrollo y prueba de la Plataforma adquiere una importancia relevante sobre otros tipos de proyectos tecnológicos en función de la dinámica esencial de la tecnología de Blockchain.

Desde su concepción, la Blockchain se generó como infraestructura tecnológica para poder brindar confianza entre partes, sin que intervengan terceros. De allí que una vez que la Cadena de Bloques es lanzada, por su propia concepción, sus operaciones no pueden modificarse, borrarse, y en el caso de los Contratos Inteligentes que gobiernan los instrumentos financieros digitales, no puede evitarse su ejecución, ni modificarse sus acciones programadas.

De allí, que sería sugerido a los desarrolladores de políticas públicas vinculadas al proyecto, además de las prácticas habituales a todo proyecto, como las pruebas de concepto, pilotos, y otros, la consideración de ambientes de prueba totalmente funcionales, como son las denominadas “testnet” de la Blockchain. Estas testnet son redes clonadas a la “mainnet” (red principal), donde en forma libre y gratuita, se permite el acceso a los desarrolladores con contratos inteligentes, para que realicen exhaustivas pruebas de los mismos, antes de su despliegue en la red principal.

Tanto para la experimentación como para la implementación, el gobierno provincial debe trabajar en colaboración con las partes interesadas identificadas, incluidas las partes relevantes del sector público, regulador, sector privado, sociedad civil y tecnología.

Metodología

Además, los procesos de diseño y desarrollo de Plataforma deben adoptar un enfoque ágil y flexible, ajustándose de acuerdo con las pruebas, los comentarios y las nuevas

investigaciones. Para los componentes orientados al usuario, debe involucrar la entrada del usuario, pruebas y entrevistas para informar una interfaz de usuario (IU) efectiva y

experiencia del usuario (UX), adoptando un enfoque "centrado en el usuario" cuando sea posible. Esta metodología fortalecerá la adopción y la usabilidad.

Compromiso público para CBDC minorista

No Aplica -

Experimentación e implementación colaborativa

Los formuladores de políticas podrían considerar si cooperar con otros proyectos de Blockchain, comunidades vinculadas a la tecnología, organizaciones internacionales, bancos comerciales u otras instituciones gubernamentales o financieras en el desarrollo de la Plataforma.

Plano de introducción

Por último, el gobierno de la provincia debe desarrollar un plan de introducción de la Plataforma que considere factores vitales como:

– El alcance, la naturaleza y la estrategia de implementación específica para un PoC (Prueba de Concepto), piloto o implementación completa.

– La línea de tiempo de la introducción de la Plataforma.

– Una estrategia para introducir y monitorear el lanzamiento de la Plataforma

Metodologías de gestión de proyectos. Su relación con la Plataforma NFT/FT

Como hemos mencionado anteriormente, el toolkit para CBDC desarrollado por el World Economic Forum, constituye una herramienta de suma importancia para los decisores y formuladores de políticas a cargo de un proyecto de desarrollo de una Moneda Digital de Banco Central.

El toolkit no fue concebido como una metodología de gestión propiamente dicha, sino como una guía de carácter estratégico, que permite a quienes encaren el análisis y definición de un proyecto CBDC, acceder un ordenamiento de cuestiones claves que, en experiencia de quienes han desarrollado proyectos de este tipo, son fundamentales para poder adquirir la visión detallada del emprendimiento.

Por este motivo, y habiendo hecho las salvedades vinculadas a las diferencias que puedan tener un proyecto específico de CBDC, con respecto al de desarrollo de una Plataforma BCT que nos atañe, es que decidimos exponer la adecuación del mismo a nuestro propósito.

Habiendo hecho estas consideraciones, resta adentrarnos en forma más sistemática en los conocimientos y herramientas específicos vinculados a la gestión de proyecto, y analizar en los mismos, las particularidades específicas de un proyecto de desarrollo de Plataforma BCT para NFT/FT, para la provincia de Santa Fe.

Antes de adentrarnos en procesos, acciones y buenas prácticas generalmente aceptadas en la gestión de proyectos, veamos algunas de las metodologías que sustentan a estos.

Vamos a realizar una breve descripción y análisis de las principales metodologías y compendios de buenas prácticas reconocidas a nivel mundial, y que poseen un grado de madurez que garantiza la sustentabilidad de la gestión de proyectos.

Con la única finalidad de sistematizar nuestro análisis vamos a separar las metodologías en dos grupos. Un primer grupo cuyo enfoque tiene como objetivo compilar conocimientos y buenas prácticas de gestión, y un segundo grupo al que denominamos “metodologías ágiles”. Debemos aclarar, por lo expuesto, que estos grupos de clasificación no son excluyentes el uno del otro, ya que las prácticas y recomendaciones del primer grupo se pueden vincular a gestión tradicional de proyectos, como así también a la gestión “ágil” de proyectos (metodologías incluidas en el segundo grupo clasificatorio).

Por último, vamos a destacar, que incluimos al final del análisis de cada uno de los grupos, las consideraciones que entendemos relevantes con referencia a los conocimientos y buenas prácticas, y a los enfoques metodológicos, para el caso particular del desarrollo de la Plataforma BCT para desarrollo de NFT/FT para la provincia de Santa Fe.

Conocimientos y buenas prácticas en la Gestión de Proyectos

1) Project Management Body of Knowlegde (PMBOK).

Es reconocido internacionalmente y se aplica en diversidad de sectores. Ofrece una guía con una serie de buenas prácticas que pueden adaptarse a las necesidades de cada proyecto.

Es un conjunto de estándares y mejores prácticas ampliamente reconocido para la gestión de proyectos. Consiste en un conjunto de procesos, áreas de conocimiento y buenas prácticas que abarcan todas las etapas de un proyecto, desde la iniciación hasta el cierre. Fue desarrollado por el Project Management Institute (PMI) y se utiliza como referencia por profesionales a cargo de la gestión efectiva de proyectos.

El PMBOK Guide está estructurado en cinco grupos de procesos y diez áreas de conocimiento:

Grupos de procesos / actividades:

1. Iniciación: Se enfoca en definir y autorizar formalmente un proyecto o una fase del mismo.
2. Planificación: Implica la elaboración de un plan detallado que guiará la ejecución y el control del proyecto.
3. Ejecución: Consiste en coordinar y dirigir los recursos para llevar a cabo las actividades del proyecto.
4. Seguimiento y control: Se refiere al monitoreo del progreso del proyecto, el control de cambios y la gestión de los riesgos.
5. Cierre: Involucra la finalización y el cierre formal del proyecto, incluyendo la documentación de lecciones aprendidas.

Áreas de conocimiento:

1. Gestión de la Integración del Proyecto.
2. Gestión del Alcance del Proyecto.
3. Gestión del Tiempo del Proyecto.
4. Gestión de los Costos del Proyecto.

5. Gestión de la Calidad del Proyecto.
6. Gestión de los Recursos Humanos del Proyecto.
7. Gestión de las Comunicaciones del Proyecto.
8. Gestión de los Riesgos del Proyecto.
9. Gestión de las Adquisiciones del Proyecto.
10. Gestión de los Interesados del Proyecto.

Cada área de conocimiento incluye procesos, actividades y prácticas específicas que se aplican durante el ciclo de vida del proyecto.

El PMBOK Guide es una referencia valiosa para los profesionales de la gestión de proyectos, ya que proporciona un marco estructurado y comúnmente aceptado para abordar los desafíos y las responsabilidades de la gestión de proyectos. Sin embargo, es importante destacar que el PMBOK no es una metodología específica, sino una guía que puede adaptarse y complementarse con otras metodologías y enfoques según las necesidades de cada proyecto.

2) ISO 21500 (Norma UNE-ISO 21500:2012)

La norma UNE-ISO 21500:2012, también conocida como ISO 21500, es una norma internacional que establece las directrices para la gestión de proyectos. Fue desarrollada por la Organización Internacional de Normalización (ISO) con el objetivo de proporcionar un marco de trabajo común y genérico para la gestión de proyectos, aplicable a diferentes tipos de organizaciones y proyectos en todo el mundo.

La norma ISO 21500 se basa en los principios fundamentales de la gestión de proyectos y proporciona una guía para los procesos, las actividades y las tareas que se deben llevar a cabo en cada etapa del ciclo de vida de un proyecto. La ISO 21500 define los términos y conceptos fundamentales utilizados en la gestión de proyectos, lo que facilita la comunicación y el entendimiento común entre los diferentes actores involucrados en un proyecto.

A su vez, establece los principios básicos que deben guiar la gestión de proyectos, como el enfoque en los objetivos, la responsabilidad, la transparencia, la adaptabilidad, entre otros.

Describe las fases y etapas típicas que se encuentran en el ciclo de vida de un proyecto, desde la concepción hasta el cierre proporcionando de esta manera orientación sobre las actividades y tareas que se deben realizar en cada etapa.

Algunas de las consignas básicas que define la SO 21500 son la identificación y descripción de los procesos de gestión de proyectos clave, incluyendo la planificación, la ejecución, el control, el cierre, entre otros. Cada proceso se divide en subprocesos y se detallan las

actividades recomendadas y dentro de ese contexto se establece los roles y las responsabilidades típicas de los actores involucrados en un proyecto, como el director de proyecto, el equipo de proyecto, los patrocinadores y los interesados. Además, la ISO 21500 describe la importancia de la comunicación y la colaboración efectiva entre los miembros del equipo.

Es importante tener en cuenta que la ISO 21500 es una norma de orientación y no está destinada a ser utilizada para fines de certificación. Su objetivo principal es proporcionar un marco de referencia común y genérico para la gestión de proyectos que pueda ser adaptado y aplicado según las necesidades y características de cada proyecto y organización.

3) PRojects IN Controlled Environments 2 (PRINCE2).

PRINCE2 (Projects IN Controlled Environments 2) es una metodología de gestión de proyectos

generalizada en el Reino Unido. Nació asociado a la gestión de proyectos públicos. Se estructura en un conjunto de ocho procesos y no cubre aspectos asociados a la gestión de proyecto como la calidad, ya que considera que están cubiertos por otras metodologías. Los ocho procesos que identifica son:

Enfoque basado en procesos: enfoque estructurado y basado en procesos para la gestión de proyectos. Proporciona un marco de trabajo detallado que define los procesos, las actividades y los roles requeridos en cada etapa del proyecto.

Enfoque orientado a productos: se centra en los productos o resultados del proyecto. Define claramente los productos esperados en cada etapa y proporciona directrices sobre su desarrollo, calidad y revisión.

Enfoque por fases: se propone dividir el proyecto en etapas gestionables y controladas. Cada etapa tiene un inicio y un final definidos, y se evalúa y revisa antes de pasar a la siguiente etapa. Esto permite un control y una toma de decisiones efectiva a lo largo del proyecto.

Roles y responsabilidades definidos: se debe buscar establecer roles y responsabilidades claramente definidos para los participantes del proyecto. Algunos roles clave incluyen el Director de Proyecto, el Patrocinador, el Comité de Dirección del Proyecto y los Usuarios Finales. Cada rol tiene responsabilidades específicas y contribuye al éxito del proyecto.

Gestión de riesgos: PRINCE2 pone un fuerte énfasis en la gestión de riesgos. Proporciona un enfoque estructurado para identificar, evaluar y mitigar los riesgos en todas las etapas del proyecto. También incluye un registro de riesgos y estrategias para su control.

Enfoque orientado a excepciones: se deben establecer límites claros para la toma de decisiones y el control del proyecto. Se definen tolerancias y niveles de autoridad para permitir una gestión ágil y efectiva de las desviaciones del plan.

Enfoque de aprendizaje continuo: fomentar el aprendizaje continuo y la mejora del proyecto. Incluye la revisión regular del proyecto, la identificación de lecciones aprendidas y la implementación de cambios para futuros proyectos.

Adaptabilidad: PRINCE2 es una metodología flexible y adaptable que puede adaptarse a diferentes tipos y tamaños de proyectos. Puede ser utilizado tanto en proyectos tradicionales como en proyectos ágiles o híbridos.

4) Goal Directed Project Management (GDPM).

La metodología Goal Directed Project Management (GDPM) es un enfoque de gestión de proyectos desarrollado por el Dr. Eliyahu Goldratt, conocido por sus contribuciones al campo de la teoría de restricciones. GDPM se basa en el principio de que el objetivo principal de un proyecto es alcanzar un resultado deseado o una meta específica, centrada en el lado humano de los proyectos —las personas— y la necesidad de tener un objetivo y enfoque del trabajo común. Se basa en dos herramientas básicas —el plan de hitos y la matriz de responsabilidades— que pueden ser complementadas con herramientas que ofrecen otras metodologías.

A diferencia de otras metodologías de gestión de proyectos que se centran en la planificación detallada y el control de actividades, GDPM se enfoca en la definición y el logro de los objetivos del proyecto. Se centra en responder a la pregunta: "¿Cuál es el objetivo final que queremos lograr con este proyecto?".

Algunos aspectos fundamentales de GDPM son los siguientes:

Definición clara de objetivos: pone un énfasis especial en la definición clara y precisa de los objetivos del proyecto. Esto implica establecer metas específicas, medibles, alcanzables, relevantes y con un tiempo definido (objetivos SMART).

GDPM identifica y aborda las restricciones o limitaciones clave que pueden afectar la consecución de los objetivos del proyecto. Estas restricciones pueden ser recursos, tecnología, tiempo, presupuesto, entre otros. La metodología se enfoca en gestionar y superar estas restricciones para lograr los resultados deseados.

En GDPM se debe procurar utilizar un enfoque de diseño basado en objetivos. Esto significa que se establece un camino de acción que se enfoca directamente en alcanzar los objetivos del proyecto, sin perder tiempo y recursos en actividades que no contribuyen directamente a esos objetivos.

Otra característica de GDPM es que también utiliza el concepto de la cadena crítica, que identifica las actividades con más aspectos críticos, o que tienen mayor impacto en el logro de los objetivos del proyecto. Se busca gestionar y proteger estas actividades críticas para asegurar el cumplimiento de los plazos y la entrega exitosa del proyecto.

La metodología GDPM se centra en la definición clara de objetivos, el manejo de las restricciones y la gestión eficiente de los recursos y el tiempo. Busca asegurar que los proyectos se enfoquen directamente en el logro de los resultados deseados y se adapten continuamente para maximizar el valor entregado.

Comparativa de los principales aspectos de cada guía de conocimientos y buenas prácticas

A modo de resumen podemos observar en siguiente cuadro los aspectos más significativos en comparación, de los cuerpos de conocimientos y buenas prácticas para la gestión de proyectos, que fuimos mencionando:

Aspecto	PMBOK	UNE-ISO 21500:2012	PRINCE2	GDPM
Marco general	Marco de conocimientos y mejores prácticas para la gestión de proyectos	Norma internacional para la gestión de proyectos	Metodología estructurada y basada en procesos	Enfoque basado en objetivos y resultados
Estructura	Procesos de gestión de proyectos divididos en 10 áreas de conocimiento	Estructura de alto nivel que abarca conceptos clave y procesos de gestión de proyectos	Metodología dividida en principios, temas y procesos	Marco de fases y pasos para la gestión de proyectos

Enfoque de Proceso	Enfocado en procesos y grupos de procesos para la gestión del proyecto	Enfatiza los procesos de dirección y gestión del proyecto	Se centra en principios, temas y procesos definidos	Enfocado en fases y pasos claramente definidos
Roles y Responsabilidades	Define roles y responsabilidades generales en cada área de conocimiento	No define roles específicos, pero enfatiza la responsabilidad de la dirección del proyecto	Define roles específicos para los diferentes roles del proyecto	Define roles y responsabilidades en cada fase del proyecto
Gestión de Alcance	Incluye la planificación, recolección de requisitos, definición del alcance y control del alcance	Enfoca la definición y control del alcance del proyecto	Incluye la planificación del producto y la gestión del cambio	Define los objetivos y resultados esperados del proyecto
Gestión del Tiempo	Incluye la planificación, programación, estimación y control del tiempo del proyecto	Enfoca la programación, control y seguimiento del tiempo del proyecto	Incluye la planificación y control de tiempo, pero con mayor énfasis en la dirección	Establece fases y pasos para cumplir con los objetivos en el tiempo establecido
Gestión de Costos	Incluye la estimación, presupuestación y control de costos del proyecto	Enfoca la estimación, presupuestación y control de costos del proyecto	Incluye la planificación, control y seguimiento de costos	Establece presupuestos y recursos para lograr los objetivos del proyecto
Gestión de Calidad	Incluye la planificación, aseguramiento y control de la calidad del proyecto	Enfoca la gestión de la calidad en el proyecto	Incluye la planificación y control de calidad del producto y el proyecto	Define estándares y resultados de calidad esperados

Comunicación	Incluye la planificación, gestión y distribución de información del proyecto	Enfoca la comunicación y la información en el proyecto	Enfoca la comunicación y la gestión de interesados	Enfoca la comunicación para lograr los objetivos del proyecto
Riesgos	Incluye la identificación, análisis, planificación y control de riesgos del proyecto	Enfoca la gestión de riesgos en el proyecto	Incluye la identificación, evaluación y gestión de riesgos	Enfoca la gestión de riesgos para lograr los objetivos del proyecto

Tabla 7- aspectos más significativos en comparación

Como podemos ver, los aspectos más destacados y esenciales para guiar la gestión de proyectos, son abordados satisfactoriamente por las cuatro Guías. En tanto, son las más reconocidas y utilizadas internacionalmente en su temática específica, todas tienen un grado de maduración que demuestra su habilitación para ser utilizadas en cualquier proyecto.

Consideraciones sobre guías de gestión de proyectos en referencia a la Plataforma BCT NFT/FT.

Solo como un análisis de sintonía fina, podemos mencionar que GDPM, fue desarrollada originalmente por Eliyahu Goldratt. Eliyahu es un reconocido autor y científico de métodos de producción, reconocido entre otras obras por “La Meta”. Esto deriva en que el GDPM revista un enfoque más profundo a la estructuración de la dirección de proyectos por medio de metas, objetivos y desvíos, y refuerza la idea de evaluación crítica y la constante revisión de las restricciones que se puedan presentar en el desarrollo del proyecto.

Por parte de la UNE-ISO 21500:2012, al estructurarse como norma ISO conlleva un mayor énfasis en claras definiciones de conceptos, así como en prácticas robustas para estructurar los procesos de gestión de proyectos. Lo mismo podemos observar en PRINCE2, que como mencionamos su primigenia fue vinculada a guiar procesos vinculados con la administración pública, y por lo tanto, converge con métodos estructurados del buró de gestión gubernamental.

Habiendo hecho estas salvedades, es nuestro entender, que cualesquiera de estas opciones de Guías puede aplicarse sin ningún inconveniente a la gestión del proyecto de desarrollo la Plataforma BCT para NFT/FT de la provincia de Santa Fe.

Los responsables de políticas públicas referidas al proyecto, como sus gestores, podrían volcarse a una guía más estructurada, o a un cuerpo de conocimientos y buenas prácticas más flexible, como el PMBOK. En el primer caso, podría prevalecer la convergencia a normativas legales específicas de procesos de gobierno y administración pública, mientras que en el segundo caso (PMBOK), la decisión de utilizar la guía, tendría como impulsores la adopción masiva a nivel mundial que hay de este compendio de conocimientos, como la cantidad de bibliografía, y experiencias de uso que existen al respecto.

Metodologías ágiles para la Gestión de Proyectos

Metodologías ágiles de gestión

Una de las modalidades más utilizadas en la gestión de proyectos, son las metodologías ágiles, que nacieron en 2001 en el sector del desarrollo de software. Sus promotores consensuaron un marco de principios que se refleja en el Manifiesto por el Desarrollo Ágil de Software:

“Estamos descubriendo formas mejores de desarrollar software tanto por nuestra propia experiencia como ayudando a terceros. A través de este trabajo hemos aprendido a valorar más:

- Individuos e interacciones - sobre procesos y herramientas
- Software funcionando - sobre documentación extensiva
- Colaboración con el cliente - sobre negociación contractual
- Respuesta ante el cambio - sobre seguir un plan

Esto es, aunque valoramos los elementos de la derecha, valoramos más los de la izquierda”.

Las metodologías ágiles se caracterizan por un ciclo de vida iterativo o adaptativo que se

estructura en ciclos fijos. Durante el proyecto, el alcance del mismo se mantiene abierto y se van entregando los productos —o entregables— de forma continuada. Estas metodologías priorizan el valor al cliente integrándolo como parte del equipo de trabajo. Describimos brevemente las principales metodologías:

Scrum

Es la principal metodología ágil en la actualidad y apareció en Japón aplicada al desarrollo de nuevos productos.

Scrum es una metodología ágil de gestión de proyectos que se utiliza comúnmente en el desarrollo de software, aunque también puede aplicarse a otros tipos de proyectos. Se basa

en un enfoque iterativo e incremental, que promueve la colaboración y la entrega continua de valor.

La metodología ágil que desarrolla Scrum permite diferenciar roles como la figura del"scrum master", que es quien será responsable de facilitar y asegurar que se sigan las prácticas y los principios de Scrum. Ayuda a eliminar obstáculos y promueve la colaboración y la mejora continua.

También se identifica al "product owner" que es el representante del cliente o del usuario final. Define y prioriza los requisitos del producto, y se asegura de que el equipo de desarrollo entregue un producto de alto valor.

El otro rol que define y precisa identificar la metodología SCRUM es el del "equipo de desarrollo": los profesionales que realizan el trabajo real del proyecto. Son multidisciplinarios y auto-organizados, y se encargan de desarrollar, probar y entregar las funcionalidades del producto.

Además de los roles mencionados SCRUM define los siguientes elementos esenciales a su proceso:

Backlog del producto: Es una lista priorizada de todas las características, funcionalidades y requisitos del producto que se desea desarrollar. Es responsabilidad del Product Owner definir y mantener el backlog del producto, asegurándose de que esté alineado con las necesidades del cliente.

Sprints: Los sprints son períodos de tiempo fijos y cortos (generalmente de 1 a 4 semanas) durante los cuales se desarrolla, prueba y entrega un incremento potencialmente utilizable del producto. Al inicio de cada sprint, el equipo selecciona una cantidad de elementos del backlog del producto que se compromete a completar durante ese sprint.

Reuniones diarias (Daily Stand-up): Son reuniones diarias de corta duración (generalmente de 15 minutos) en las que el equipo de desarrollo actualiza sobre su progreso, comparte cualquier impedimento y coordina las actividades del día.

Revisión del sprint (Sprint Review): Al final de cada sprint, se realiza una reunión de revisión en la que el equipo de desarrollo muestra el trabajo completado al Product Owner y a otros interesados. Se recopila su retroalimentación y se realiza una actualización del backlog del producto en función de lo aprendido durante el sprint.

Retrospectiva del sprint (Sprint Retrospective): Es una reunión al final de cada sprint en la que el equipo de desarrollo reflexiona sobre el proceso y las prácticas utilizadas, y busca oportunidades de mejora. Se identifican acciones para implementar en el próximo sprint y se fomenta la mejora continua.

SCRUM se caracteriza por su enfoque en la adaptabilidad, dinamismo, transparencia y la colaboración constante entre los miembros del equipo. El objetivo es maximizar el valor entregado al cliente en cada iteración y responder rápidamente a los cambios y requisitos cambiantes. Scrum no proporciona una guía detallada sobre la planificación y el seguimiento

del proyecto, por lo que es común combinar Scrum con otras prácticas y técnicas ágiles para abordar estos aspectos.

Lean Software Development

Consiste en la aplicación de los principios de lean manufacturing al desarrollo de software. Se basa principalmente en eliminar aquello que no aporta valor al cliente, retrasar las decisiones hasta poder basarlas en evidencias, entregar lo más rápido posible y potenciar al equipo reduciendo las jerarquías.

Los principales conceptos y principios de la metodología Lean Software Development son:

Eliminación de desperdicio: se busca identificar y eliminar cualquier actividad, proceso o recurso que no agregue valor al cliente. Además minimizar el tiempo y los recursos dedicados a actividades no esenciales, como el exceso de documentación, la espera, la duplicación de esfuerzos, entre otros.

Entrega continua de valor: el enfoque que se sugiere es la entrega frecuente y continua de incrementos de valor al cliente. En lugar de esperar a tener un producto completamente terminado, se priorizan y desarrollan características esenciales primero, permitiendo una entrega temprana y la posibilidad de recibir retroalimentación y adaptarse a las necesidades del cliente de manera oportuna.

Amplitud de visión: La LSD considera el proyecto en su totalidad y busca optimizar el sistema completo en lugar de optimizar partes individuales. Se busca un equilibrio entre la eficiencia y la eficacia, asegurándose de que el proyecto en su conjunto sea exitoso y cumpla con las expectativas del cliente.

Desarrollo iterativo e incremental: Al igual que en otras metodologías ágiles, la LSD se basa en ciclos iterativos y entregas incrementales. Se divide el proyecto en partes más pequeñas y manejables, se desarrollan y se entregan en iteraciones, permitiendo la adaptación y la mejora continua a medida que se obtiene retroalimentación.

Aprendizaje y experimentación: se promueve un enfoque experimental y de aprendizaje continuo. Se fomenta la colaboración, la retroalimentación y la mejora basada en el aprendizaje obtenido de cada entrega y ciclo. Se valora el aprendizaje a través de la experimentación y la adaptación constante del enfoque y las prácticas utilizadas.

Colaboración y empoderamiento del equipo: es importante enfatizar la colaboración y la participación activa de todos los miembros del equipo. Se fomenta la toma de decisiones

descentralizada y se confía en el equipo para definir cómo se llevará a cabo el trabajo y cómo se lograrán los objetivos.

Calidad integrada: se debe buscar la integración de la calidad en todos los aspectos del proyecto. Se fomenta la colaboración temprana entre los equipos de desarrollo y de control de calidad, y se promueve la prueba continua y la detección temprana de errores.

Kanban

La metodología Kanban es un enfoque visual y flexible para la gestión de proyectos que se originó en la industria manufacturera, pero que también se utiliza ampliamente en el desarrollo de software y otros ámbitos. Se basa en la visualización del flujo de trabajo, la limitación del trabajo en curso y la mejora continua.

Los principales elementos y conceptos de la metodología Kanban son:

Dentro de la metodología que propone Kanban, un aspecto destacable es el de Tablero Kanban. El Tablero Kanban es la representación visual del flujo de trabajo del proyecto. El flujo de trabajo se representa mediante las columnas en el tablero Kanban. Cada tarea se mueve de una columna a otra a medida que avanza en el proceso. Esto permite tener una vista clara y actualizada del estado de cada tarea y del proyecto en su conjunto.

El tablero, en sí, consiste en una pizarra o un software en el que se dividen las tareas en columnas, que representan las diferentes etapas del proceso (por ejemplo, "Pendiente", "En progreso" y "Completado"). Cada tarea se representa como una tarjeta o un elemento visual.

Vinculado con esto, la metodología cuenta con Tarjetas Kanban. Son elementos visuales que representan las tareas o los elementos de trabajo. Cada tarjeta contiene información relevante, como una descripción de la tarea, el responsable y cualquier otro detalle necesario para llevar a cabo la tarea.

En la dinámica de su metodología, Kanban promueve la limitación de la cantidad de trabajo en curso (WIP, por sus siglas en inglés) en cada etapa del proceso. Esto significa establecer un límite máximo de tareas que se pueden trabajar simultáneamente en una columna determinada. Esta limitación ayuda a evitar la sobrecarga del equipo y a mantener un flujo de trabajo constante y equilibrado. Otro aspecto de Kanban, es que el trabajo se "tira" en lugar de "empujarse". Esto significa que se inicia una nueva tarea solo cuando hay capacidad disponible en la siguiente etapa del flujo de trabajo. Se basa en la demanda real y evita la sobrecarga de trabajo innecesaria.

Por último, y también enfocando Kanban fomenta la recopilación de métricas y el análisis de datos para identificar áreas de mejora. Se busca medir el tiempo de ciclo, el tiempo de

respuesta y otros indicadores clave para identificar cuellos de botella, ineficiencias y oportunidades de mejora. Estas métricas ayudan a impulsar la mejora continua en el proceso y a optimizar el flujo de trabajo.

Comparativa de los principales aspectos de las metodologías ágiles

Al igual que en el análisis de Guías de conocimiento y buenas prácticas, vamos a conceptualizar y diferenciar las metodologías ágiles que mencionamos anteriormente, por medio de un cuadro comparativo de algunos de los aspectos más relevantes.

Aspectos	Scrum	Lean Software Development	Kanban
Filosofía	Enfoque de desarrollo iterativo e incremental centrado en equipos auto-organizados y entregas frecuentes	Enfoque de mejora continua y eliminación de desperdicio, centrado en la entrega de valor al cliente	Enfoque visual y de flujo de trabajo que busca maximizar la eficiencia y la capacidad de respuesta
Roles clave	Scrum Master, Product Owner y Equipo de Desarrollo	No se definen roles específicos, pero se enfatiza la colaboración y la responsabilidad compartida	No se definen roles específicos, pero se enfatiza la colaboración y el trabajo en equipo
Artefactos	Product Backlog, Sprint Backlog y Incremento	No se definen artefactos específicos, pero se enfatiza la entrega de valor y la reducción de desperdicio	Tablero Kanban con columnas y tarjetas que representan las tareas y el flujo de trabajo

Ceremonias	Sprint Planning, Daily Scrum, Sprint Review y Sprint Retrospective	No se definen ceremonias específicas, pero se enfatiza la colaboración continua y la mejora continua	No se definen ceremonias específicas, pero se enfatiza la revisión y la mejora del flujo de trabajo
Principios clave	Transparencia, inspección y adaptación	Eliminación de desperdicio, entrega temprana y aprendizaje rápido	Visualización del flujo de trabajo, limitación del trabajo en progreso y mejora continua
Enfoque de planificación	Planificación basada en Sprints (iteraciones) con objetivos claros y backlog priorizado	Planificación basada en la entrega de valor y reducción de desperdicio	Planificación basada en el flujo de trabajo continuo y la mejora continua
Control de calidad	Pruebas continuas, revisión y adaptación durante cada Sprint	Enfocado en la mejora continua de la calidad y la entrega de valor al cliente	Enfocado en la mejora continua de la calidad y la eficiencia del flujo de trabajo
Flexibilidad	Flexible y adaptable a cambios en los requisitos del cliente	Flexible y adaptable a cambios en las necesidades del cliente y a la mejora continua	Flexible y adaptable a cambios en el flujo de trabajo y la demanda del cliente

Tabla 8 principales aspectos de las metodologías ágiles

Consideraciones en relación a metodologías ágiles en referencia al proyecto de Plataforma NFT/FT - Provincia de Santa Fe.

Las denominadas metodologías ágiles surgen al principio de este siglo, más representativamente en el año 2001 cuando se emite el Manifiesto Ágile.

Este tipo de metodologías surgen en oposición a las metodologías tradicionales, las cuales tenían una carga excesiva en la estructuración de actividades, procesos y documentación. En especial la metodología de desarrollo de software UML (Unified Modeling Language), iniciada en 1994 por James Rumbaugh, Ivar Jacobson y Grady Booch, y establecida con posterioridad como estándar sugerido por el OMG (Object Management Group).

Algunas de las razones que impulsaron el Manifiesto agile y el desarrollo de este tipo de nuevas metodologías, tiene que ver con un nuevo paradigma de desarrollo de software que se viene observando desde el cambio de la década del 90 al 2000. En el plano social y económico, el proceso denominado “globalización”, imprimió nuevos modelos de negocios, alianzas e impulsó el comercio global, lo que se denominó “la aldea global”. Los cambios del contexto comercial, financiero e incluso social, comenzaron a acelerarse desde ese momento.

Desde el punto de vista de desarrollo de software, el advenimiento de Internet en la década del 90 y la maduración de sistemas de comercio electrónico vía web, llevó a un cambio en las modalidades de desarrollo, en el cuál el modelo de aplicaciones “stand-alone” (instalables en el computadora), cambiaron por las aplicaciones web. El lema que se acuñó fue “la aplicación es el navegador”. Esto con un objetivo claro. Al alojar las aplicaciones en un servidor web, y permitir a los usuarios trabajar en esas aplicaciones desde una interfaz web, en su navegador, cualquier cambio o actualización se podía realizar con mucha rapidez, ya que al actualizar la aplicación web, todos los usuarios pueden instantáneamente acceder a los cambios.

Podríamos resumir todo esto en una idea: rápida respuesta a cambios constantes de contexto.

¿Cúal sería el vínculo de estas consideraciones con respecto al análisis de las metodologías agiles, con relación al desarrollo del proyecto de desarrollo de Plataforma BCT para NFT/FT?

Entendemos que la concepción de las metodologías ágiles que detallamos anteriormente, se vincula a múltiples interacciones cortas que logren rápidamente productos entregables, acorde a los requerimientos de los proyectos en que se utilicen. Esto permite que, ante cambios en el contexto o en los requerimientos del sistema (tanto legales, normativos, sociales o tecnológicos), la metodología permite que el proyecto se adapte rápidamente para poder resolver estas cuestiones.

De esta manera, probablemente el proyecto sustente durante toda su duración sus objetivos, pero por debajo de estos, los procesos, actividades, productos, e interacciones necesarias vayan cambiando frecuentemente, para adaptarse a nuevos requerimientos.

En este punto, creemos que se debería poner el foco, para decidir si adoptar una metodología ágil para el proyecto de desarrollo de la Plataforma. En función de esto, se debería analizar

si el entorno del proyecto se espera sea muy volátil en relación a cambios tecnológicos, normativos, y de compliance.

¿Qué posibilidades hay de que se produzcan cambios relevantes en las tecnologías que utilizará la Plataforma, como en el marco regulatorio que la impacta ? Veamos algunas consideraciones.

ZKP - Pruebas de Conocimiento Cero.

Este año se realizó el anuncio de que la principal Blockchain en implementar contratos inteligentes en el mundo, Ethereum, iba a comenzar a utilizar algoritmos de Pruebas de Conocimiento Cero (ZKP). Las Pruebas de Conocimiento Cero, son algoritmos criptográficos que permiten a alguien dar certeza de que una persona tiene determinada información, pero permiten lograr esa certeza, sin que esa persona revele la información mencionada.

En el caso de Ethereum, estas Pruebas de Conocimiento Cero, no buscan la finalidad de la anonimidad de transacciones (como se busco en otros desarrollos como el famoso caso de Tornado-Cash), sino que lo que se pretende es escalar la potencia de red, hasta más de 300.000 validaciones por segundo. Además de este proceso conocido como Roll-Up en BCT, las ZKP permiten la interoperabilidad de diferentes Blockchains entre sí.

Destaquemos también que cuando hablamos de Ethereum, no solo hablamos de esa Blockchain específica, sino que al ser esta Cadena de Bloques la líder en implementación de Contratos Inteligentes, arrastra a todas las demás, a innovar tecnológicamente con la misma orientación que ella.

EPI-4337 - Abstracción de Cuentas

A partir de marzo de 2023, la Blockchain de Ethereum, comenzó también a implementar una serie de Contratos Inteligentes, que permiten desarrollar las denominadas “billeteras inteligentes”. Hasta el momento, la tenencia y potestad sobre las criptomonedas eran ejercidas por la clave privada que nuestras billeteras digitales guardaban en secreto y custodiaban celosamente.

Con la modificación adoptada recientemente, los usuarios podrán transferir a un Contrato Inteligente, sus tenencias de criptomonedas, y el Contrato gestionará las mismas, permitiendo entre otras posibilidades, la recuperación de claves por medio de preguntas o biométrica, sistemas de listas blancas o listas negras, límites de transacciones, múltiple signatura, entre otras.

De esta forma, se rompe la lógica de “la perdida de la clave privada, implica la pérdida de las criptomonedas”.

Marco Normativo actual y cambios esperados

En el corto plazo (se piensa que es casi inminente), los tribunales de NYC se pronunciarán sobre la disputa legal que Rippio Lab (XRP) mantiene con la S.E.C. (Securities and Exchange Commision) de USA[72]. Este no se considera un caso menor, ya que puede sentar precedentes sobre la consideración legal que se deba realizar sobre la emisión de tokens de gobernanza sobre la Blockchain, para saber si deben ser considerados legalmente como “securities” (acciones).

Si bien, es una disputa que se realiza en el ámbito de Estados Unidos, puede convertirse en un leader case para la regulación de ese país, y en arrastre para la consideración regulatoria y normativa de otros países.

En el ámbito local, solamente para mencionar las últimas novedades que se presentan en el ámbito normativo de cripto-activos, podemos mencionar que la CNV - Comisión Nacional de Valores, ha emitido una resolución para la autorización del reglamento de contratos de futuros sobre el Índice Bitcoin Matba Rofex, con negociación y liquidación en pesos argentinos y sin entrega del activo subyacente[73].

Existen también, varios proyectos de Ley en análisis sobre la regulación de cripto-activos, y en especial sobre el rol que debería asumir la CNV en este aspecto.

Beneficios de una metodología ágile

En relación a los cambios tecnológicos inminentes (algunos de los que mencionamos ya están en marcha), como así también los cambios esperados que en el corto plazo se vayan a realizar en referencia al marco regulatorio de los cripto-activos, creemos que la adopción de una metodología de desarrollo, basada en métodos ágiles, puede ser de suma importancia para el proyecto que analizamos.

---

[72] Femi Olude (2023) - What Are the Stakes in the SEC vs. Ripple Case? - CoinDesk
https://www.coindesk.com/consensus-magazine/2023/05/18/what-are-the-stakes-in-the-sec-vs-ripple/
Observado mayo 2023

[73] miArgentina - La CNV aprobó futuros basados en índice Bitcoin
https://www.argentina.gob.ar/noticias/la-cnv-aprobo-futuros-basados-en-indice-bitcoin
Observado: mayo 2023

La dinámica en que se basan las metodologías ágiles, facilitan la adaptación a cambios inesperados, como también a cambios esperados, pero de un impacto rápido sobre los procesos del proyecto. Las interacciones y revisiones que se potencian por estas metodologías podrían acolchar el efecto de cambios de reglas, normativas o adecuaciones a tecnologías innovadoras que se deben considerar en el ciclo de vida del proyecto.

Líneas directrices de PMBOK

En esta sección vamos a describir los aspectos fundamentales que establece el PMBOK, reconocido a nivel global como el cuerpo de conocimientos y guía más utilizado para la dirección de proyectos.

Vamos a identificar, en este contexto, las características particulares y diferenciales de estos aspectos fundamentales del PMBOK, en lo que respecta al proyecto que estamos analizando de una Plataforma BCT NFT/FT para la provincia de Santa Fe.

1. Gestión de la integración del proyecto

Según define el PMBOK la Gestión de Integración del Proyecto consiste en:

"La Gestión de la Integración del Proyecto incluye los procesos y actividades necesarios para identificar, definir, combinar, unificar y coordinar los diversos procesos y actividades de dirección del proyecto dentro de los Grupos de Procesos de la Dirección de Proyectos.

En el contexto de la dirección de proyectos, la integración incluye características de unificación, consolidación, comunicación y acciones integradoras cruciales para que el proyecto se lleve a cabo de manera controlada, de modo que se complete, que se manejen con éxito las expectativas de los interesados y se cumpla con los requisitos.

La Gestión de la Integración del Proyecto implica tomar decisiones en cuanto a la asignación de recursos, equilibrar objetivos y alternativas contrapuestas y manejar las interdependencias entre las Áreas de Conocimiento de la dirección de proyectos. Los procesos de la dirección de proyectos se presentan normalmente como procesos diferenciados con interfaces definidas, aunque en la práctica se superponen e interactúan entre ellos de formas que no pueden detallarse en su totalidad dentro de la Guía del PMBOK®."[74]

[74] Guía de los Fundamentos Para la Dirección de Proyectos (Guía del PMBOK®)–Quinta Edición [A Guide to the Project Management Body of Knowledge (PMBOK® Guide)-Fifth Edition](Spanish Edition) - 2013 - Project Management Institute, Inc.

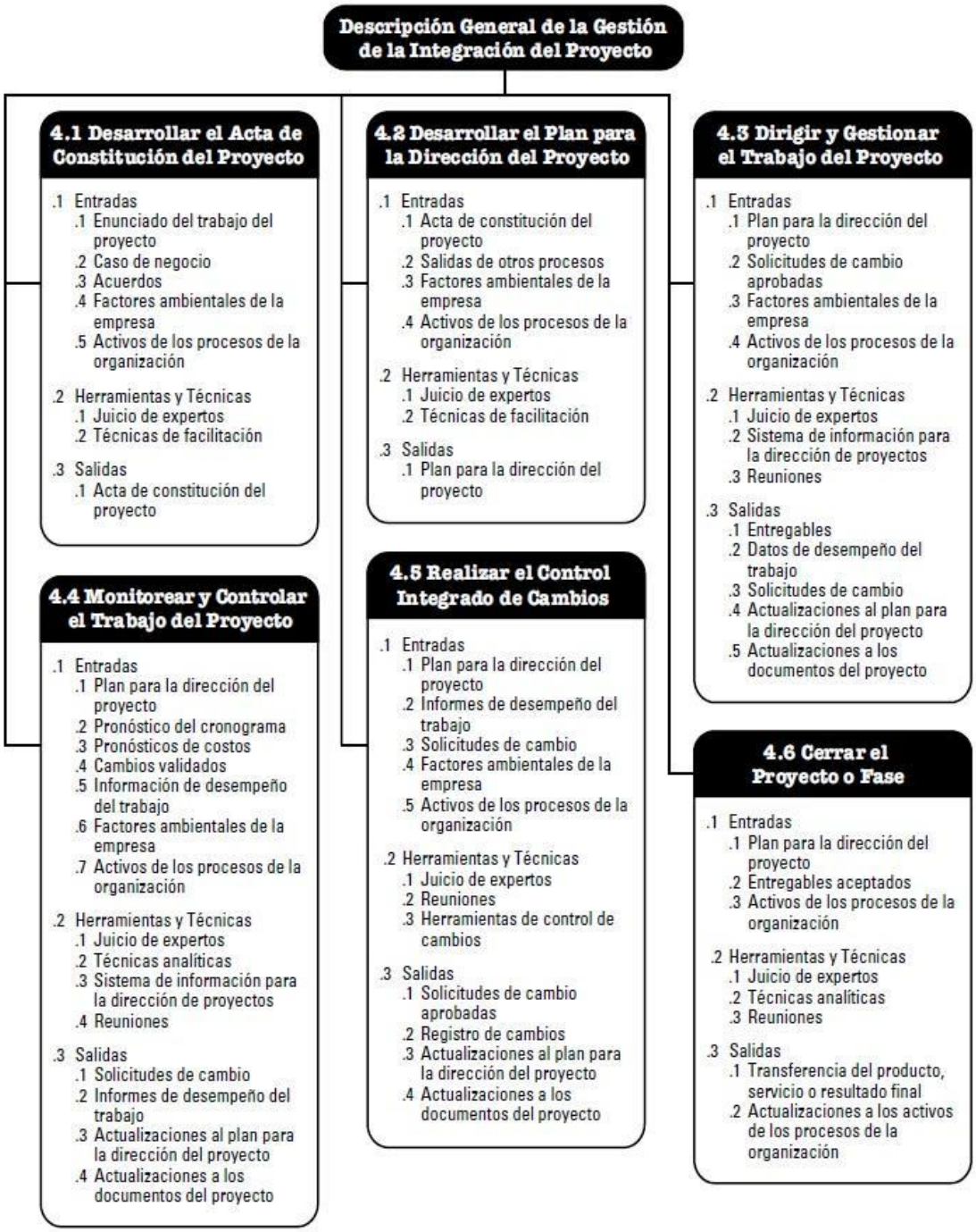


Figura 51 Gestión de Integración del Proyecto. Extraído de PMBOK quinta edición. Op cit.

El PMBOK define varios procesos relacionados con la integración del proyecto. Los más relevantes (no son limitativos) son:

Desarrollar el acta de constitución del proyecto: Este proceso consiste en la elaboración del documento formal que autoriza el inicio del proyecto. El acta de constitución del proyecto establece la justificación del proyecto, sus objetivos, los interesados involucrados y los criterios iniciales de éxito.

Desarrollar el plan para la dirección del proyecto: En este proceso se crea el plan de gestión del proyecto, que incluye la descripción detallada de cómo se llevará a cabo el proyecto, los objetivos específicos, los cronogramas, los costos, los recursos necesarios, los riesgos, entre otros aspectos.

Dirigir y gestionar la ejecución del proyecto: Este proceso implica llevar a cabo el plan establecido, coordinando las actividades del equipo, gestionando los recursos, realizando el seguimiento del progreso y tomando las acciones necesarias para cumplir con los objetivos del proyecto.

Monitorear y controlar el trabajo del proyecto: Se trata de vigilar el avance del proyecto, comparándolo con el plan establecido y tomando medidas correctivas cuando sea necesario. Este proceso implica el seguimiento de los plazos, el presupuesto, la calidad, los riesgos y otros aspectos relevantes.

Realizar el control integrado de cambios: Aquí se gestiona cualquier cambio que surja durante la ejecución del proyecto. Se evalúa el impacto del cambio en el alcance, el tiempo, los costos y otros aspectos del proyecto, y se toman decisiones sobre si se aprueba o se rechaza el cambio.

Cerrar el proyecto o la fase: Al finalizar el proyecto o una fase del mismo, se realiza el cierre formal. Esto implica la entrega del producto o servicio final, la documentación de lecciones aprendidas, la liberación de recursos y la finalización de las obligaciones contractuales.

La integración del proyecto, según el PMBOK, abarca la coordinación de estos procesos y la gestión de las interacciones entre ellos. Se busca garantizar que el proyecto se ejecute de manera coherente y eficiente, asegurando que los resultados cumplan con los requisitos y expectativas del cliente y de los interesados.

Gestión de la integración del proyecto. Consideraciones para Plataforma BCT NFT/FT

La integración del proyecto, implica en sí la coordinación de diversos procesos que se entramen en prosecución del objetivo deseado. Un factor preponderante para cualquier desarrollo que se busque utilizar como infraestructura base, la tecnología de Blockchain es la implementación de un robusto proceso de testing de los Contratos Inteligentes a utilizar.

La característica distintiva de la tecnología de Blockchain radica en el registro coordinado, redundante y criptografiado de transacciones, lo que posibilita su invulnerabilidad, pero en especial su inalterabilidad. Esta inalterabilidad de registro de transacciones. se extiende a los Contratos Inteligentes, que se utilizaran para sustentar la Plataforma BCT NFT/FT. De allí, que una vez desplegados estos, no podrán ser modificados, ni evitarse su ejecución.

Por esto el proceso clave, especialmente distinguible y diferencial de un proyecto basado en la tecnología de Blockchain, es el de testing de sus artefactos, es decir, de sus Contratos Inteligentes.

Viendo esto desde la perspectiva de la integración del Proyecto, veremos que todos los procesos claves que definamos en este ámbito, deben buscar identificarse, definirse, combinarse, unificarse y coordinarse con respecto a los resultados satisfactorios del testeo de Contratos Inteligentes.

2. Gestión del alcance del proyecto

El PMBOK define a la Gestión del Alcance del Proyecto como:

“La Gestión del Alcance del Proyecto incluye los procesos necesarios para garantizar que el proyecto incluya todo el trabajo requerido y únicamente el trabajo para completar el proyecto con éxito. Gestionar el alcance del proyecto se enfoca primordialmente en definir y controlar qué se incluye y qué no se incluye en el proyecto”.

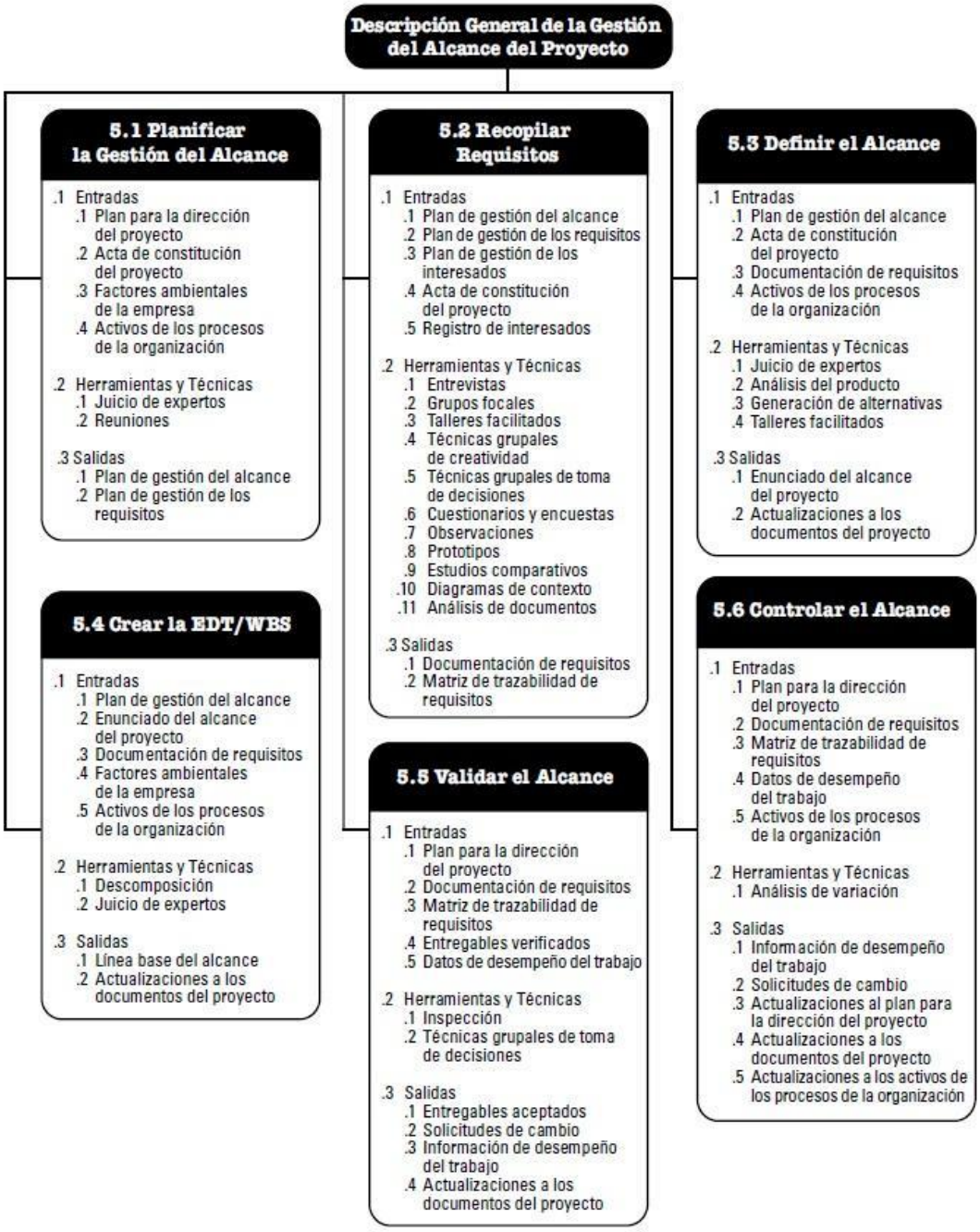


Figura 52 Gestión de Alcance del Proyecto. Extraído de PMBOK quinta edición. Op cit.

El PMBOK establece que el alcance del proyecto se refiere a la totalidad de los trabajos necesarios para completar el proyecto de manera exitosa. Define los límites del proyecto, es decir, lo que está incluido y lo que está excluido. El alcance del proyecto se desarrolla a través del proceso de gestión del alcance y se documenta en el plan de gestión del alcance.

El PMBOK proporciona una estructura para la gestión del alcance del proyecto, que consta de las siguientes actividades:

1. Planificar la gestión del alcance: Se establece cómo se definirá, documentará y gestionará el alcance del proyecto, incluyendo los procesos y las herramientas que se utilizarán.

2. Recopilar los requisitos: Se identifican, documentan y validan los requisitos del proyecto. Se involucran a los interesados relevantes para asegurarse de capturar todos los requisitos necesarios.

3. Definir el alcance: Se desarrolla una descripción detallada de los resultados del proyecto y los criterios de aceptación asociados. Esto implica la elaboración de una declaración del alcance del proyecto y la creación de la estructura de desglose del trabajo (EDT o WBS, por sus siglas en inglés).

4. Crear la EDT (Estructura de Desglose del Trabajo): Se descompone el alcance del proyecto en componentes más pequeños y manejables, utilizando una estructura jerárquica.

5. Verificar el alcance: Se lleva a cabo una revisión formal de los resultados del proyecto para asegurar que se han cumplido los requisitos establecidos y obtener la aceptación del cliente o del patrocinador del proyecto.

6. Controlar el alcance: Se monitorea y controla el alcance del proyecto a lo largo de su ejecución. Se gestionan los cambios que puedan surgir y se asegura que el proyecto se mantenga dentro de los límites establecidos.

Gestión de alcance del proyecto. Consideraciones para Plataforma BCT NFT/FT

En este aspecto del PMBOK no encontramos diferencias relevantes con lo que se enuncia respecto de otros proyectos que no aplican la tecnología de Blockchain como basamento.

Simplemente destacar, que si se desea habilitar la posibilidad de que los usuarios de la Plataforma, puedan desplegar y desarrollar en ella sus propios Contratos Inteligentes, es decir, incrementar el ecosistema Blockchain de la Plataforma, se deberá definir con claridad el alcance que proyecto deberá valorar para la extensión que se puedan realizar de esta forma.

3. Gestión del tiempo del proyecto

"La Gestión del Tiempo del Proyecto incluye los procesos requeridos para gestionar la terminación en plazo del proyecto."

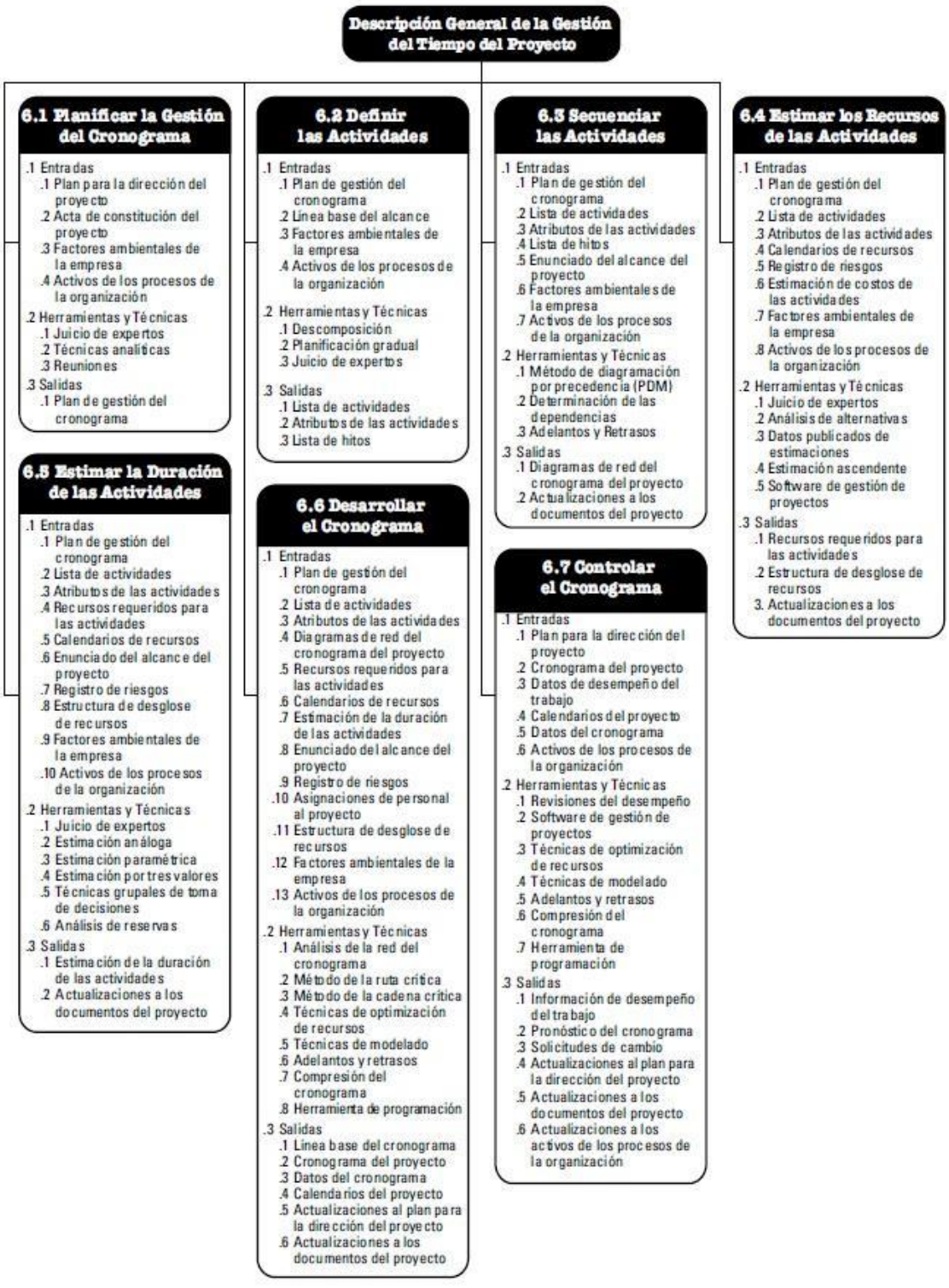


Figura 53 Gestión del tiempo del Proyecto. Extraído de PMBOK quinta edición. Op cit.

El PMBOK establece directrices y buenas prácticas para la gestión del tiempo del proyecto en el área de conocimiento de Gestión del Cronograma del Proyecto. Estas directrices sugeridas ayudan a los profesionales de gestión de proyectos a planificar, secuenciar, estimar y controlar las actividades del proyecto para cumplir con los objetivos de tiempo establecidos. Un resumen de estas actividades es:

1. Planificar la gestión del cronograma: Se desarrolla un plan de gestión del cronograma que establece cómo se gestionará, controlará y comunicará el cronograma del proyecto. Este plan define los enfoques, herramientas y técnicas que se utilizarán para desarrollar el cronograma.

2. Definir las actividades: Se identifican y documentan las actividades específicas necesarias para completar el proyecto. Las actividades son tareas discretas y mensurables que consumen tiempo y recursos.

3. Secuenciar las actividades: Se establece la relación lógica entre las actividades, determinando el orden en que deben llevarse a cabo. Esto implica identificar las dependencias entre las actividades y establecer la secuencia adecuada.

4. Estimar la duración de las actividades: Se determina la cantidad de tiempo necesaria para completar cada actividad. Se pueden utilizar técnicas como la estimación basada en expertos, la estimación análoga (comparación con proyectos anteriores similares) o la estimación paramétrica (uso de modelos matemáticos).

5. Desarrollar el cronograma: Se crea el cronograma del proyecto utilizando la información obtenida en los pasos anteriores. Se utilizan técnicas como el diagrama de red del proyecto (como el método del camino crítico) y el análisis de la cadena crítica para determinar la duración total del proyecto y las fechas de inicio y fin de las actividades.

6. Controlar el cronograma: Se monitorea y controla el cronograma del proyecto durante su ejecución. Se comparan las fechas reales de inicio y finalización de las actividades con las planificadas, y se toman acciones correctivas en caso de desviaciones. También se gestionan los cambios que puedan afectar al cronograma y se actualiza en consecuencia.

Todas estas directrices, buenas prácticas y sugerencias del PMBOK facilitan un marco de trabajo integral para los profesionales de gestión de proyectos facilitandoles planificar, ejecutar y controlar eficazmente las actividades del proyecto en función de los plazos establecidos.

Gestión del tiempo del proyecto. Consideraciones para Plataforma BCT NFT/FT

No encontramos diferencias relevantes en lo específico al desarrollo de la Plataforma BCT NFT/FT.

4. Gestión de los costos del proyecto

"La Gestión de los Costos del Proyecto incluye los procesos relacionados con planificar, estimar, presupuestar, financiar, obtener financiamiento, gestionar y controlar los costos de modo que se complete el proyecto dentro del presupuesto aprobado".

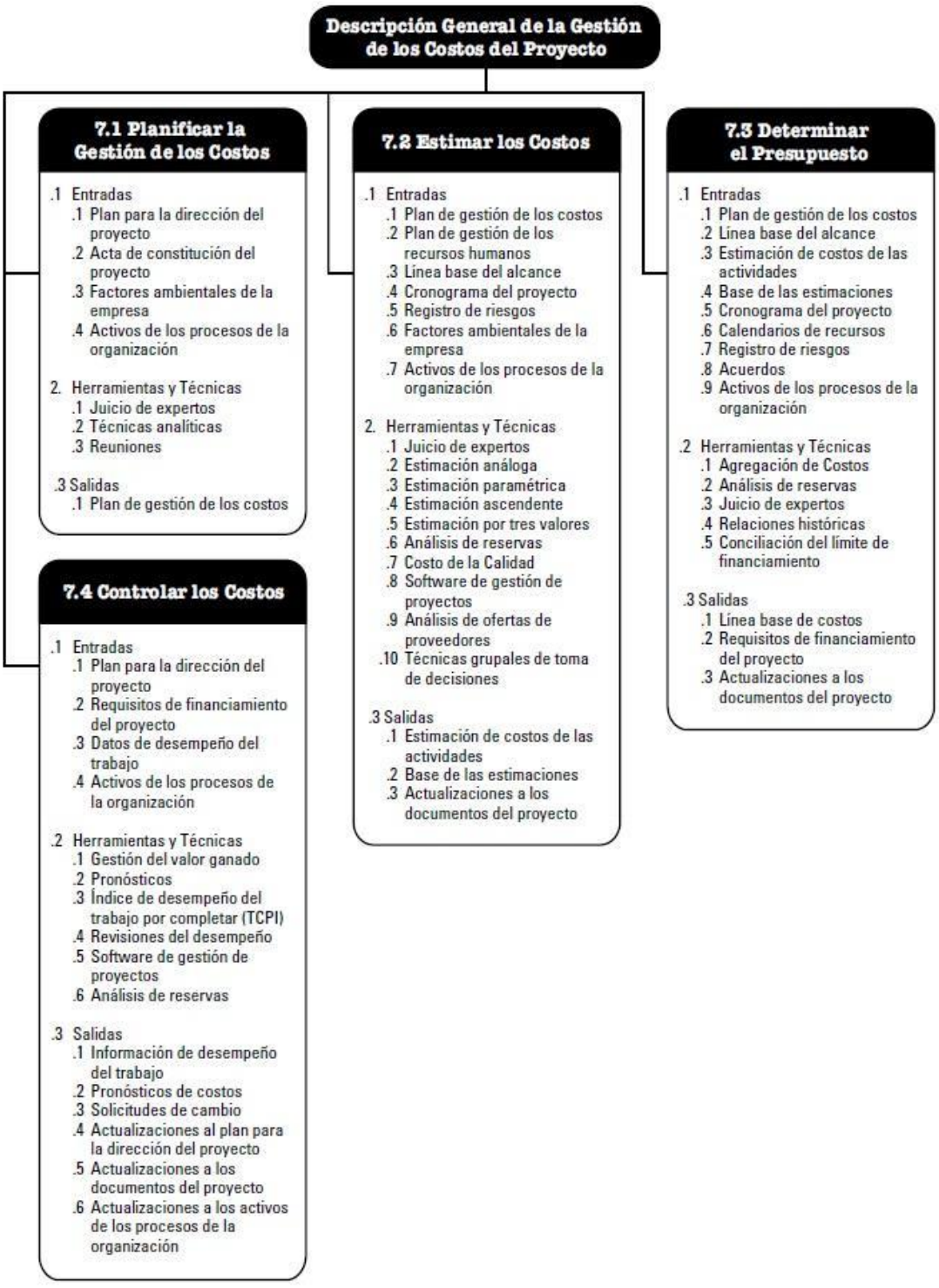


Figura 54 Gestión de Costos del Proyecto. Extraído de PMBOK quinta edición. Op cit.

Algunas de las acciones sugeridas por el PMBOK en relación a la gestión de costos del proyecto son:

1. Planificar la gestión de costos: Se desarrolla un plan de gestión de costos que define cómo se gestionarán, controlarán y comunicarán los costos del proyecto. Este plan establece los enfoques, herramientas y técnicas que se utilizarán para estimar y controlar los costos.

2. Estimar los costos: Se determina el monto de los recursos financieros necesarios para completar las actividades del proyecto. Se utilizan técnicas como la estimación análoga (basada en proyectos anteriores similares), la estimación paramétrica (basada en relaciones matemáticas) y la estimación basada en tres puntos (utilizando valores optimistas, pesimistas y más probables).

3. Desarrollar el presupuesto: Se calcula el costo total del proyecto en base a las estimaciones de costos de las actividades individuales. Se establece un presupuesto que asigna los recursos financieros necesarios para ejecutar el proyecto.

4. Controlar los costos: Se monitorean y controlan los costos del proyecto durante su ejecución. Se comparan los costos reales con los costos planificados, y se toman acciones correctivas si hay desviaciones significativas. Se registra y analiza el rendimiento financiero del proyecto a través de herramientas como el Valor Ganado (Earned Value Management) para evaluar la eficiencia y el cumplimiento del presupuesto.

5. Controlar los cambios en el proyecto: Se gestionan los cambios que pueden afectar a los costos del proyecto. Se evalúan los impactos financieros de los cambios propuestos, y se toman decisiones informadas sobre la aprobación o rechazo de los cambios.

6. Controlar los compromisos de gastos: Se supervisan y controlan los desembolsos de fondos del proyecto para asegurarse de que se adhieran al presupuesto y a los compromisos financieros establecidos.

El PMBOK proporciona un marco de trabajo detallado para la gestión de costos del proyecto, que ayuda a los profesionales de gestión de proyectos a planificar, controlar y tomar decisiones informadas sobre los recursos financieros necesarios para el éxito del proyecto.

Gestión de costos del proyecto. Consideraciones para Plataforma BCT NFT/FT

Si bien en este aspecto no existen diferencias relevantes que tengan relación con el desarrollo de la Plataforma BCT NFT/FT, es destacable, que uno de los costos más significativos que se deberá gestionar, es el de la auditoría funcional, de negocio y técnica de los Contratos Inteligentes que se vayan a implementar.

Algunas de las firmas a nivel internacional con mayor prestigio en la auditoría de Contratos Inteligentes, que se deberían relevar son:

Open Zeppelin

https://www.openzeppelin.com/security-audits

Consensys

https://consensys.io/diligence/

Hacken

https://hacken.io/

BlockSec

https://blocksec.com/

PeckShield

https://peckshield.com/

QuillAudits

https://www.quillaudits.com/smart-contract-audit

5. Gestión de la calidad del proyecto

"La Gestión de la Calidad del Proyecto incluye los procesos y actividades de la organización ejecutora que establecen las políticas de calidad, los objetivos y las responsabilidades de calidad para que el proyecto satisfaga las necesidades para las que fue acometido. La Gestión de la Calidad del Proyecto utiliza políticas y procedimientos para implementar el sistema de gestión de la calidad de la organización en el contexto del proyecto, y, en la forma que resulte adecuada, apoya las actividades de mejora continua del proceso, tal y como las lleva a cabo la organización ejecutora. La Gestión de la Calidad del Proyecto trabaja para asegurar que se alcancen y se validen los requisitos del proyecto, incluidos los del producto".

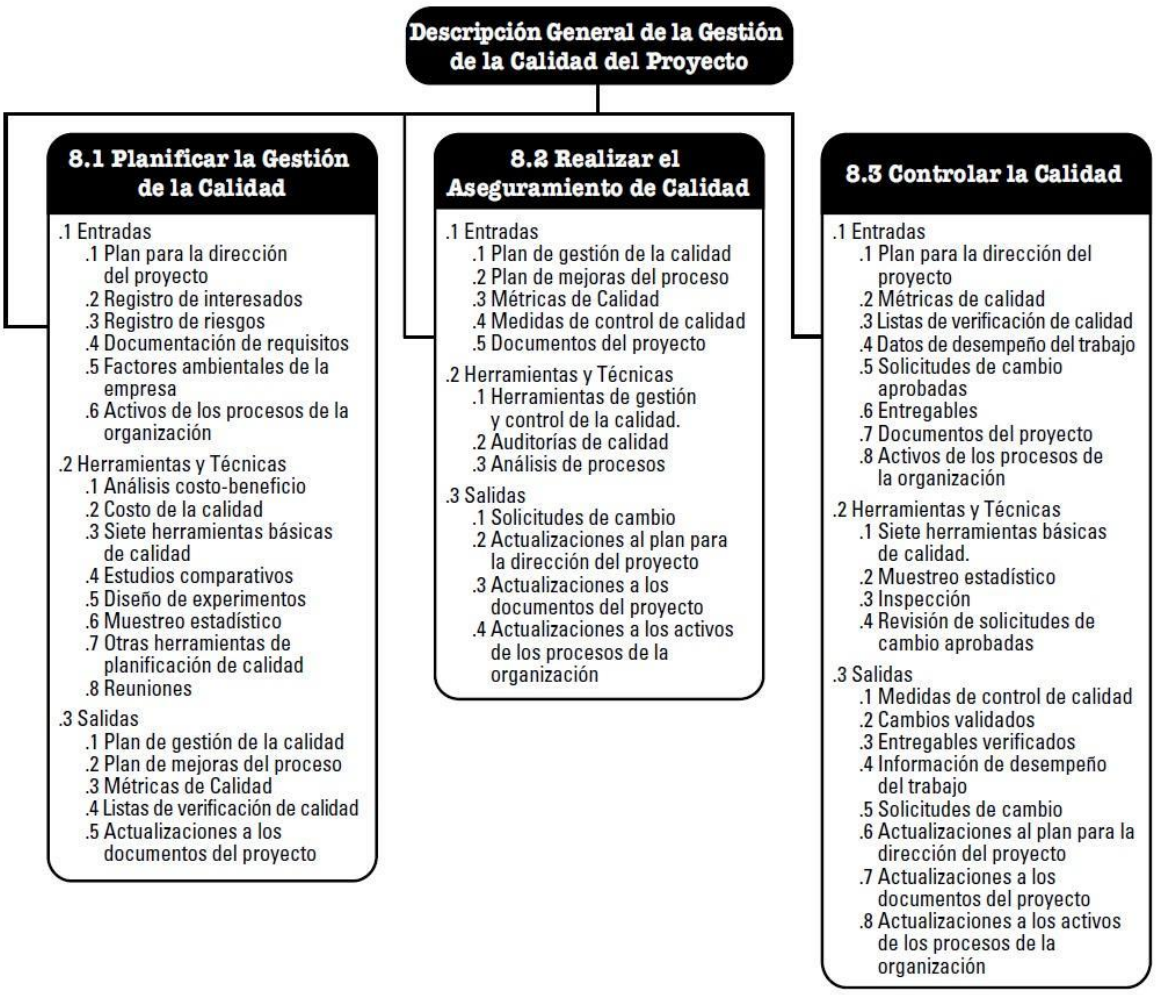


Figura 55 - Gestión de Calidad del Proyecto. Extraído de PMBOK quinta edición. Op cit

.

Las directrices que establece el PMBOK en relación a la calidad del proyecto, ayudan a los profesionales de gestión de proyectos a planificar, asegurar y controlar la calidad de los entregables y los procesos del proyecto. A continuación, se resumen los principales elementos sugeridos por el PMBOK en este aspecto:

1. Planificar la gestión de la calidad: Se desarrolla un plan de gestión de la calidad que establece cómo se gestionará y asegurará la calidad del proyecto. Este plan define los enfoques, estándares, herramientas y técnicas que se utilizarán para cumplir con los requisitos de calidad.

2. Realizar el aseguramiento de la calidad: Se ejecutan las actividades planificadas para asegurar que los entregables y los procesos del proyecto cumplan con los requisitos de calidad establecidos. Esto puede incluir la realización de revisiones y auditorías de calidad, así como la implementación de medidas de control de calidad.

3. Controlar la calidad: Se monitorea y controla la calidad a lo largo de la ejecución del proyecto. Se comparan los resultados reales con los estándares de calidad establecidos, y se toman acciones correctivas si se detectan desviaciones. Se utilizan herramientas y técnicas como el muestreo de control, las inspecciones y las pruebas para evaluar y verificar la calidad de los entregables y los procesos.

4. Mejorar la calidad: Se busca continuamente mejorar la calidad del proyecto. Se recopilan datos y se analizan para identificar oportunidades de mejora. Se implementan acciones correctivas y preventivas para abordar las deficiencias y evitar problemas futuros.

5. Asegurar la calidad de los proveedores: Se establecen criterios de calidad para los proveedores y se realizan actividades de aseguramiento de calidad en relación con los productos y servicios proporcionados por los proveedores externos al proyecto.

El enfoque principal de la gestión de calidad del proyecto según el PMBOK es asegurarse de que los productos y procesos cumplan con los requisitos establecidos y las expectativas de los interesados. Esto se logra a través de la planificación, ejecución y control de actividades relacionadas con la calidad, con el objetivo de garantizar la satisfacción del cliente y el éxito general del proyecto.

6. Gestión de los recursos humanos del proyecto

"*La Gestión de los Recursos Humanos del Proyecto incluye los procesos que organizan, gestionan y conducen al equipo del proyecto. El equipo del proyecto está compuesto por las personas a las que se han asignado roles y responsabilidades para completar el proyecto. Los miembros del equipo del proyecto pueden tener diferentes conjuntos de habilidades, pueden estar asignados a tiempo completo o a tiempo parcial y se pueden incorporar o retirar del equipo conforme avanza el proyecto. También se puede referir a los miembros del equipo del proyecto como personal del proyecto. Si bien se asignan roles y responsabilidades específicos a cada miembro del equipo del proyecto, la participación de todos los miembros en la toma de decisiones y en la planificación del proyecto es beneficiosa. La participación de los miembros del equipo en la planificación aporta su experiencia al proceso y fortalece su compromiso con el proyecto*".

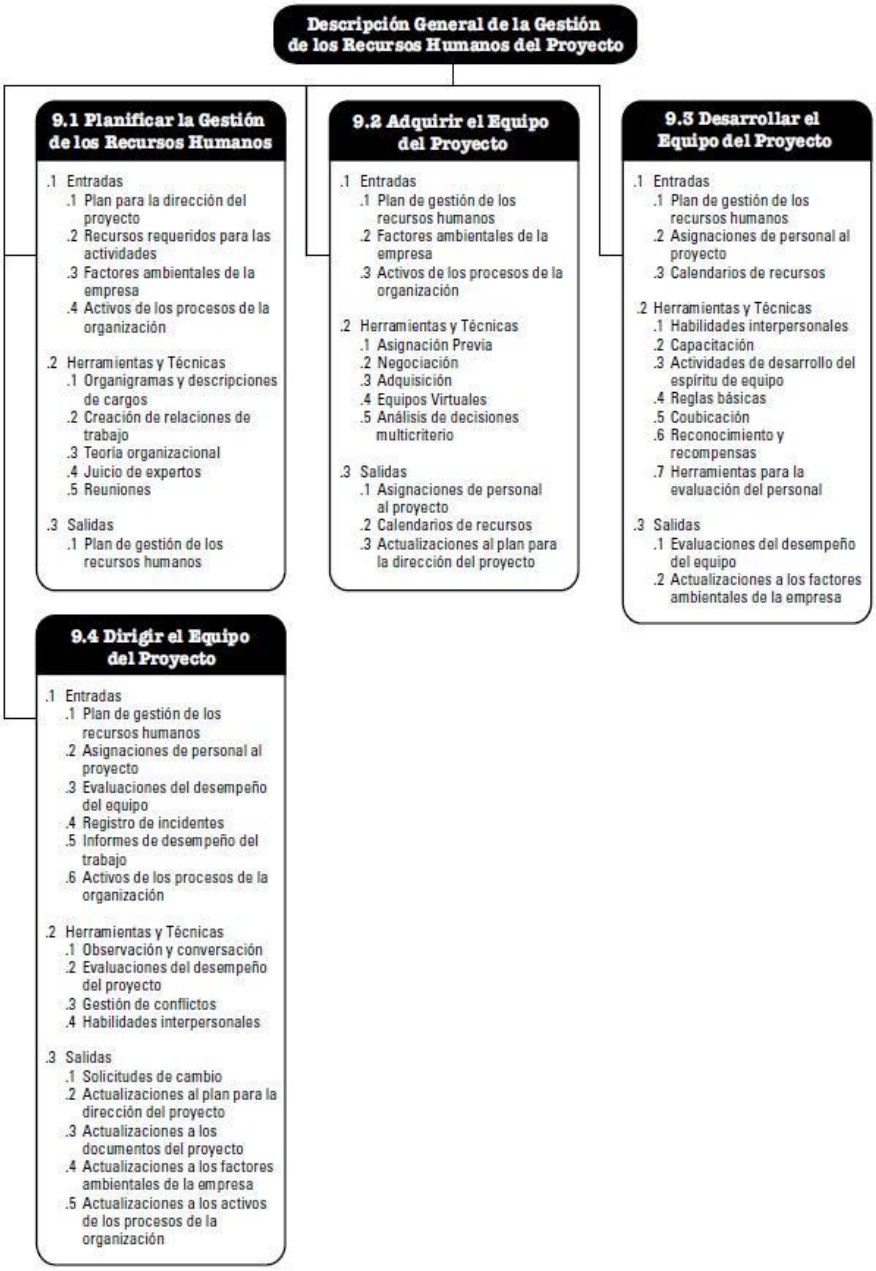


Figura 56 Gestión de Recursos Humanos del Proyecto. Extraído de PMBOK quinta edición. Op cit.

El PMBOK (Project Management Body of Knowledge) proporciona directrices y mejores prácticas para la gestión de recursos humanos del proyecto en el área de conocimiento de Gestión de Recursos Humanos del Proyecto. Estas directrices ayudan a los profesionales de gestión de proyectos a identificar, adquirir, desarrollar y gestionar eficazmente el equipo de proyecto. Actividades y procesos sugeridos en este ámbito son:

1. Planificar la gestión de recursos humanos: Se desarrolla un plan de gestión de recursos humanos que establece cómo se gestionarán, organizarán y gestionarán los recursos humanos del proyecto. Este plan define los roles y responsabilidades del equipo, las

necesidades de capacitación, el enfoque de comunicación y otras consideraciones relacionadas con el personal.

2. Adquirir al equipo del proyecto: Se identifican y se asignan los recursos humanos necesarios para el proyecto. Esto incluye la contratación de personal interno o externo, la asignación de miembros del equipo ya disponibles en la organización o la contratación de recursos externos.

3. Desarrollar al equipo del proyecto: Se proporciona capacitación, orientación y desarrollo profesional para mejorar las habilidades y competencias del equipo del proyecto. Esto implica identificar las necesidades de capacitación, proporcionar oportunidades de desarrollo y fomentar la colaboración y el trabajo en equipo.

4. Gestionar el equipo del proyecto: Se trabaja para mantener un ambiente de trabajo colaborativo y motivador para el equipo del proyecto. Esto incluye la comunicación efectiva, la resolución de conflictos, el reconocimiento y la gestión del desempeño. Se establecen canales de comunicación abiertos y se fomenta la colaboración y el compromiso del equipo.

5. Dirigir al equipo del proyecto: El líder del proyecto proporciona dirección y liderazgo al equipo del proyecto. Esto implica establecer una visión clara, establecer metas y objetivos, motivar al equipo y tomar decisiones efectivas. Se fomenta la participación activa del equipo y se busca maximizar el rendimiento y la productividad.

6. Gestionar las partes interesadas del proyecto: Se trabaja para comprender, gestionar y satisfacer las necesidades de las partes interesadas del proyecto. Esto implica identificar las partes interesadas clave, establecer una estrategia de gestión de partes interesadas y gestionar las expectativas y los requerimientos de las partes interesadas a lo largo del proyecto.

El PMBOK destaca la importancia de la gestión eficaz de los recursos humanos en el éxito del proyecto. Al proporcionar orientación en áreas como adquisición de personal, desarrollo de habilidades, gestión del equipo y liderazgo, el PMBOK ayuda a los profesionales de gestión de proyectos a optimizar el rendimiento del equipo y mejorar la colaboración y la comunicación en el entorno del proyecto.

Gestión de recursos humanos del proyecto. Consideraciones para Plataforma BCT NFT/FT

En relación a la gestión de recursos humanos del proyecto, un factor esencial a considerar para el desarrollo de la Plataforma BCT NFT/FT es la combinación de dos ejes de

organización de los recursos humanos: el equipo de expertos de negocio, y el de expertos en IT.

El equipo de IT deberá contar mínimamente con profesionales con destacadas habilidades en programación de Contratos Inteligentes, en lenguajes de programación acordes con la Blockchain elegida, preferentemente lenguaje Solidity. También se deberá contar con profesionales que trabajen a nivel de interfase de la Blockchain con aplicaciones móviles o de camino crítico. En este caso con conocimientos de JASON-RPC, Python, entre otros.

Por el lado de la arquitectura de la Plataforma, se requerirá conocimientos sólidos en la estructura de Blockchain, especialmente en la configuración e interacción de las diferentes capas (tiers) de la Cadena de Bloques.

Por parte de los recursos humanos que pertenecen al eje de expertos de negocio, será recomendable conocimiento amplios en gestión financiera, análisis y proyecciones de mercado, y la dinámica propias de activos digitales, estudiados actualmente por la denominada token-economic.

Por último y en consideración a lo que ya se mencionó acerca de la necesidad de reforzar fuertemente los procesos de verificación y testing vinculados a la dinámica propia de desarrollos basados en Blockchain, debemos mencionar la preponderancia de un robusto equipo de testing del proyecto. Independientemente de que se contrate como consultoría externa los procesos de auditoría de Contratos Inteligentes, es fundamental el trabajo del equipo se testing en la definición de requerimientos a probar, cómo así también del set de pruebas, y el grado de stress a someter el sistema.

7. Gestión de las comunicaciones del proyecto

"La Gestión de las Comunicaciones del Proyecto incluye los procesos requeridos para asegurar que la planificación, recopilación, creación, distribución, almacenamiento, recuperación, gestión, control, monitoreo y disposición final de la información del proyecto sean oportunos y adecuados. Los directores de proyecto emplean la mayor parte de su tiempo comunicándose con los miembros del equipo y otros interesados en el proyecto, tanto si son internos (en todos los niveles de la organización) como externos a la misma. Una comunicación eficaz crea un puente entre diferentes interesados que pueden tener diferentes antecedentes culturales y organizacionales, diferentes niveles de experiencia, y diferentes perspectivas e intereses, lo cual impacta o influye en la ejecución o resultado del proyecto".

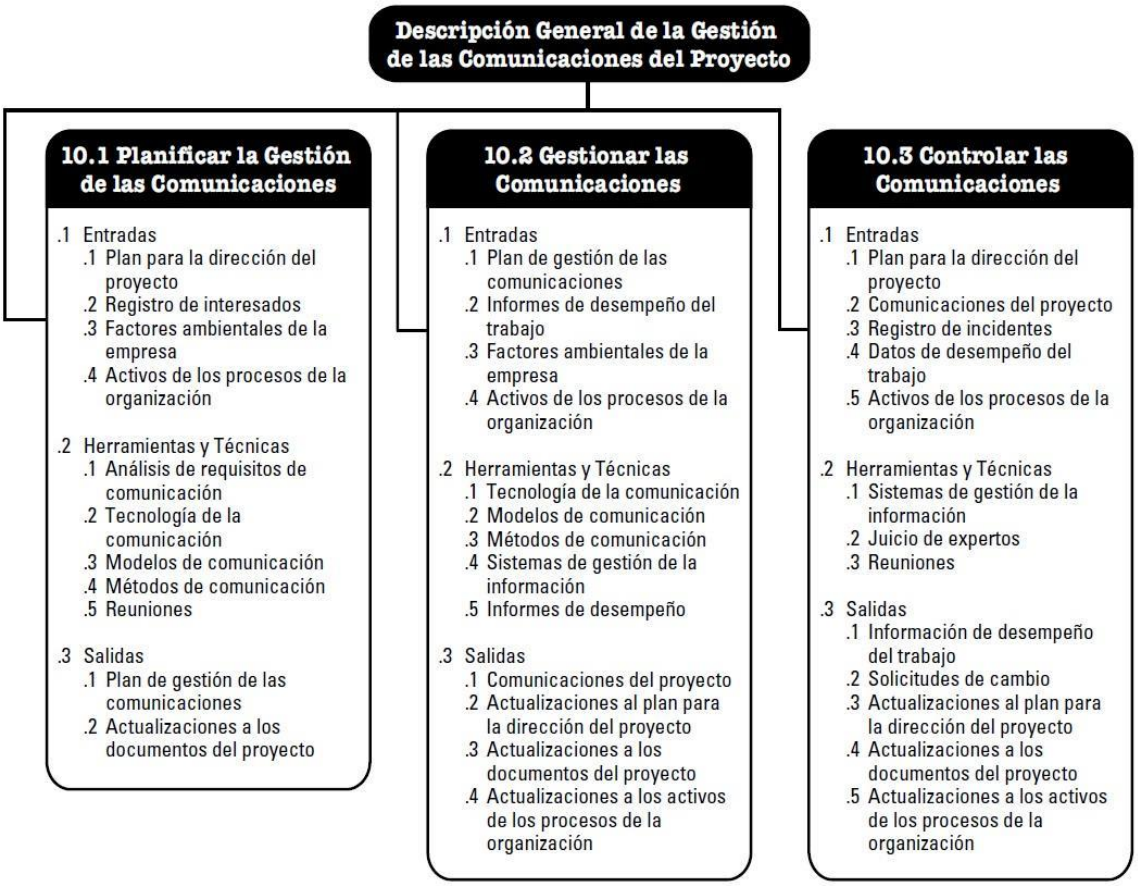


Figura 57 Gestión de Comunicaciones del Proyecto. Extraído de PMBOK quinta edición. Op cit.

El PMBOK (Project Management Body of Knowledge) proporciona pautas y mejores prácticas para la gestión de comunicaciones del proyecto en el área de Gestión de las Comunicaciones del Proyecto. Estas directrices ayudan a los profesionales de gestión de proyectos a planificar, gestionar y controlar las comunicaciones dentro del proyecto y con las partes interesadas. Los principales elementos que el PMBOK establece en relación con la gestión de comunicaciones del proyecto son:

1. Planificar la gestión de las comunicaciones: Se desarrolla un plan de gestión de las comunicaciones que establece cómo se gestionarán y controlarán las comunicaciones del proyecto. Este plan identifica a las partes interesadas, define los objetivos de comunicación, establece los requisitos de información y establece los canales y métodos de comunicación que se utilizarán.

2. Gestionar las comunicaciones del proyecto: Se implementa el plan de gestión de las comunicaciones. Esto implica recopilar, generar, distribuir, almacenar y recuperar la información del proyecto de manera oportuna y efectiva. Se establecen canales de comunicación adecuados y se garantiza la disponibilidad de la información relevante para las partes interesadas.

3. Gestionar las partes interesadas: Se gestiona de manera efectiva la comunicación con las partes interesadas del proyecto. Esto incluye identificar las necesidades de información de las partes interesadas, establecer una estrategia de comunicación con ellas, gestionar las expectativas y resolver los problemas de comunicación que puedan surgir.

4. Controlar las comunicaciones del proyecto: Se monitorean y controlan las comunicaciones a lo largo del proyecto. Esto implica asegurar que la información esté siendo transmitida correctamente, identificar y resolver problemas de comunicación, y gestionar cualquier cambio en los requisitos de información o en los canales de comunicación.

5. Gestionar el registro de la documentación del proyecto: Se mantiene un registro actualizado de toda la documentación y la información relevante del proyecto. Esto incluye la gestión de versiones, la organización y el almacenamiento adecuados, y la disposición de la documentación según las políticas y requisitos establecidos.

Gestión de comunicaciones del proyecto. Consideraciones para Plataforma BCT NFT/FT

La mención que podemos hacer, cómo diferencial con respecto a la gestión de comunicaciones, en el caso de la Plataforma BCT NFT/FT, se en encuentra vinculada a la necesidad de interoperabilidad entre los ámbitos de expertos de negocio, con los expertos de IT. Se hace necesario el poder expresar con claridad, y sin lenguaje técnico o críptico los enfoques de desarrollos que se esperan.

En un plano más específico, y vinculado con la comunicación, se debería considerar las subculturas propias de cada área de multidisciplinariedad, para poder integrar profundamente una comunicación efectiva.

8. Gestión de los riesgos del proyecto

“La Gestión de los Riesgos del Proyecto incluye los procesos para llevar a cabo la planificación de la gestión de riesgos, así como la identificación, análisis, planificación de respuesta y control de los riesgos de un proyecto.

Los objetivos de la gestión de los riesgos del proyecto consisten en aumentar la probabilidad y el impacto de los eventos positivos, y disminuir la probabilidad y el impacto de los eventos negativos en el proyecto”.

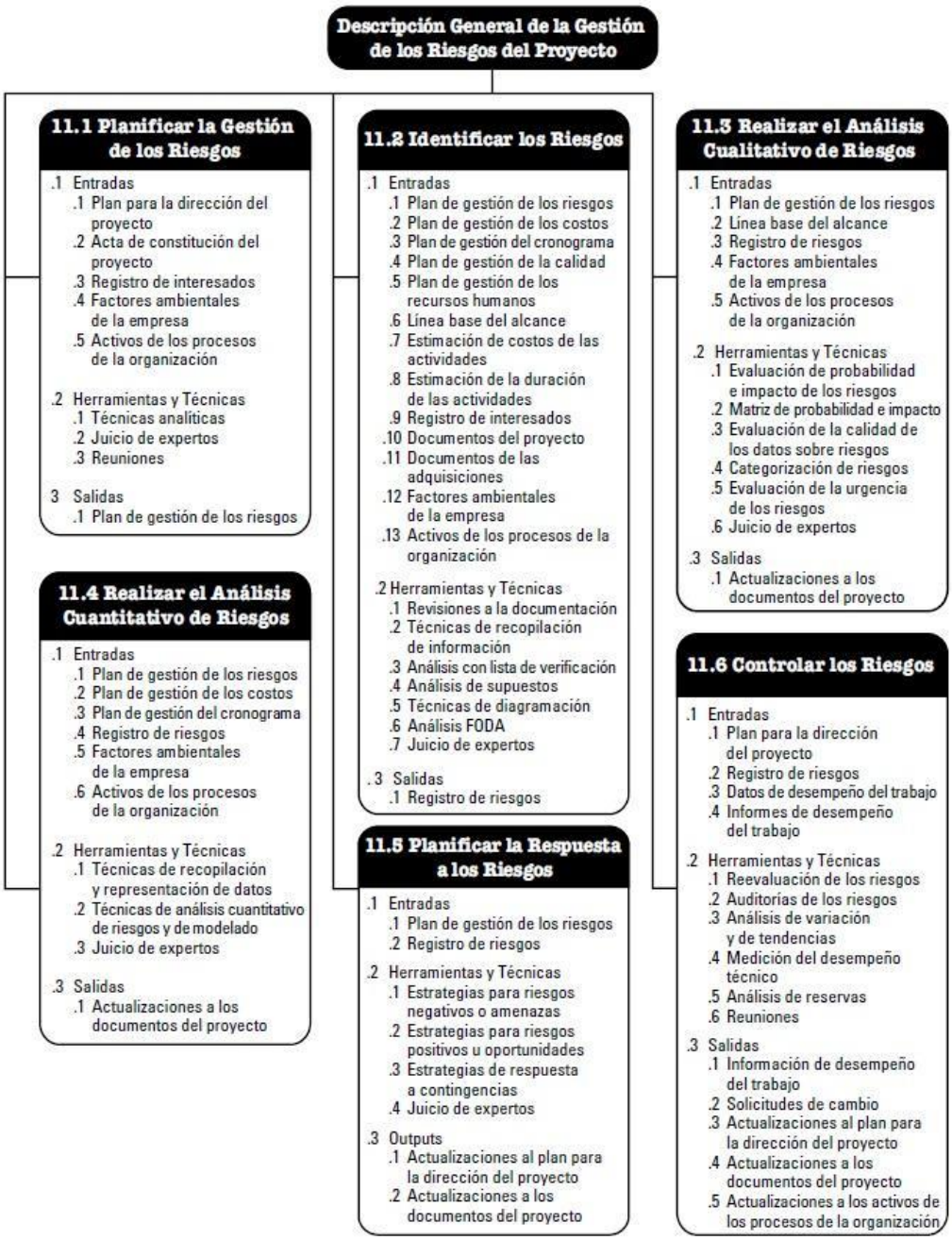


Figura 58 Gestión de Riesgos del Proyecto. Extraído de PMBOK quinta edición. Op cit.

El aseguramiento de riesgos del proyecto es una de las áreas de conocimiento clave establecidas por el PMBOK (Project Management Body of Knowledge).

Se centra en identificar, analizar, evaluar y responder a los riesgos potenciales que podrían afectar al proyecto. Entre los principales elementos que el PMBOK establece en relación con la gestión de riesgos del proyecto podemos encontrar:

1. Planificar la gestión de riesgos: Se desarrolla un plan de gestión de riesgos que establece cómo se gestionarán y abordarán los riesgos del proyecto. Este plan incluye la metodología a utilizar, los roles y responsabilidades, el enfoque de identificación de riesgos y las herramientas y técnicas a emplear.

2. Identificar los riesgos: Se identifican los riesgos específicos que podrían afectar al proyecto. Esto implica la identificación de eventos inciertos o situaciones que podrían tener un impacto negativo o positivo en los objetivos del proyecto. Se utilizan técnicas como la lluvia de ideas, la revisión de documentos y la consulta a expertos para identificar los riesgos potenciales.

3. Realizar el análisis cualitativo de riesgos: Se evalúa la probabilidad y el impacto de cada riesgo identificado. Se asigna una calificación a cada riesgo según su gravedad y se priorizan para determinar los riesgos más significativos. Esto ayuda a enfocar los esfuerzos de gestión de riesgos en los aspectos críticos del proyecto.

4. Realizar el análisis cuantitativo de riesgos: Se cuantifican los efectos de los riesgos en los objetivos del proyecto, como el costo, el cronograma o la calidad. Se utilizan técnicas estadísticas y modelos para evaluar la probabilidad de ocurrencia de los riesgos y sus impactos potenciales. Esto proporciona una evaluación más precisa y cuantitativa de los riesgos y permite tomar decisiones informadas.

5. Planificar las respuestas a los riesgos: Se desarrollan planes de respuesta para abordar los riesgos identificados. Esto implica determinar estrategias de mitigación, transferencia, aceptación o evitación de los riesgos. Se establecen acciones específicas y se asignan responsabilidades para implementar estas respuestas.

6. Controlar los riesgos: Se monitorean y controlan los riesgos a lo largo del proyecto. Se supervisan los riesgos identificados, se evalúa su efectividad y se toman medidas adicionales según sea necesario. También se gestionan los nuevos riesgos que puedan surgir durante la ejecución del proyecto.

La gestión de riesgos del proyecto según el PMBOK es esencial para anticipar y abordar los eventos inciertos que podrían afectar al éxito del proyecto. Al seguir las directrices establecidas, los profesionales a cargo del proyecto pueden identificar y gestionar los riesgos de manera proactiva, lo que reduce la probabilidad de problemas graves y ayuda a garantizar el logro de los objetivos del proyecto.

Gestión de riesgos del proyecto. Consideraciones para Plataforma BCT NFT/FT

Cómo ya se expresó en este trabajo el riesgo intrínseco más destacado de proyectos basados en la tecnología de Blockchain, se vincula a la inalterabilidad y autoejecución de los Contratos Inteligentes en que se sustenta.

Sin embargo, y como se detalló más puntualmente cuando se analizaron en este trabajo las metodologías ágiles, un riesgo inherente a la tecnología de Blockchain es su carácter permanente de tipo innovador y disruptivo.

Los ecosistemas Blockchain se encuentran sujetos a cambios tecnológicos constantes, en especial los vinculados a la Blockchain Ethereum, por su sustentación en una comunidad de desarrolladores y actores altamente activos. Aún cuando se conciba el carácter dinámico del proyecto de desarrollo de la Plataforma que estamos analizando, la capacidad de nuevas tecnologías vinculadas a la Blockchain, de solaparse unas con otras, lleva a la necesidad de planes de contingencia más elaborados a fin de poder mitigar los riesgos que ese devenir tecnológico implica.

9. Gestión de las adquisiciones del proyecto

"La Gestión de las Adquisiciones del Proyecto incluye los procesos necesarios para comprar o adquirir productos, servicios o resultados que es preciso obtener fuera del equipo del proyecto. La organización puede ser la compradora o vendedora de los productos, servicios o resultados de un proyecto".

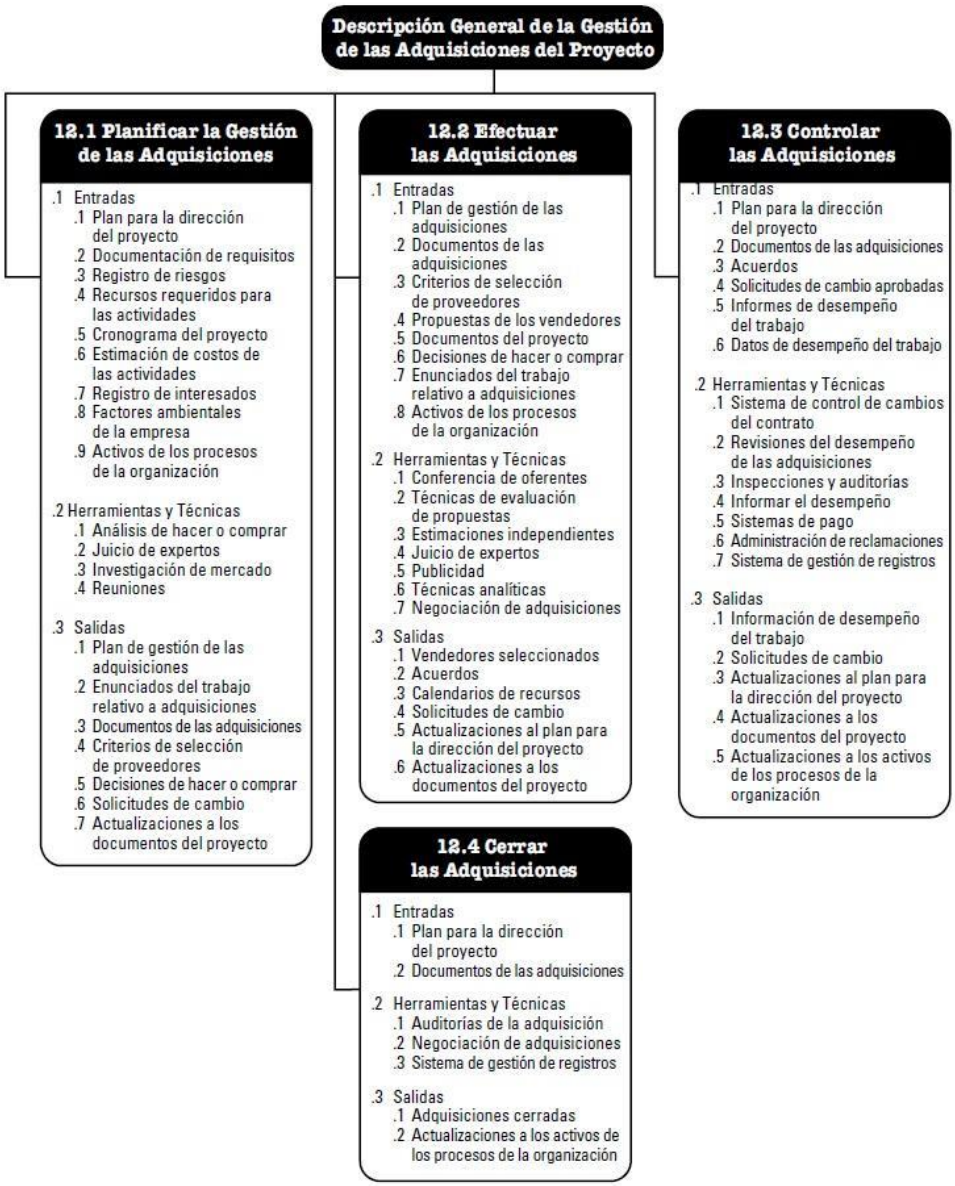


Figura 59 Gestión de adquisiciones del Proyecto. Extraído de PMBOK quinta edición. Op cit.

Las directrices que establece el PMBOK en referencia a adquisiciones del proyecto, ayudan a planificar, ejecutar y controlar las actividades relacionadas con la adquisición de bienes y servicios necesarios para el proyecto. Entre las acciones, procesos y elementos sugeridos, podemos mencionar:

1. Planificar la gestión de las adquisiciones: Se desarrolla un plan de gestión de adquisiciones que establece cómo se gestionarán las adquisiciones necesarias para el proyecto. Este plan incluye la identificación de los bienes y servicios a adquirir, la definición de los criterios de selección de proveedores, el enfoque de contratación y los procedimientos de gestión de contratos.

2. Efectuar las adquisiciones: Se lleva a cabo el proceso de adquisición según lo establecido en el plan. Esto incluye la identificación y la selección de proveedores, la solicitud de propuestas o cotizaciones, la negociación de contratos y la adjudicación de los contratos correspondientes.

3. Administrar las adquisiciones: Se gestiona el desempeño de los proveedores y los contratos durante la ejecución del proyecto. Esto implica asegurar que los proveedores cumplan con los términos y condiciones acordados, supervisar el progreso de las adquisiciones, gestionar los cambios en los contratos y resolver cualquier problema o disputa que pueda surgir.

4. Cerrar las adquisiciones: Se finalizan las adquisiciones una vez que se han cumplido los requisitos del proyecto y se han completado los contratos correspondientes. Esto incluye la verificación de la entrega y aceptación de los bienes o servicios, la resolución de cualquier problema pendiente y la liquidación de los contratos.

El PMBOK también destaca la importancia de la ética y la responsabilidad en la gestión de adquisiciones. Se alienta a los decisores de gestión de proyectos a actuar de manera justa y transparente en todas las actividades relacionadas con las adquisiciones, y a seguir los estándares éticos y legales aplicables.

Gestión de adquisiciones del proyecto. Consideraciones para Plataforma BCT NFT/FT

En términos de un análisis diferencial, es decir, en relación a aspectos de adquisiciones que sean propios y distintivos de la implementación de la tecnología de Blockchain sobre un proyecto, no vemos que existan de este tipos de aspectos que sean relevantes o significativos para destacar, en diferenciación de los ya mencionados para cualquier otro tipo de proyecto.

10. Gestión de los interesados del proyecto

“La Gestión de los Interesados del Proyecto incluye los procesos necesarios para identificar a las personas, grupos u organizaciones que pueden afectar o ser afectados por el proyecto, para analizar las expectativas de los interesados y su impacto en el proyecto, y para desarrollar estrategias de gestión adecuadas a fin de lograr la participación eficaz de los interesados en las decisiones y en la ejecución del proyecto. La gestión de los interesados también se centra en la comunicación continua con los interesados para comprender sus necesidades y expectativas, abordando los incidentes en el momento en que ocurren, gestionando conflictos de intereses y fomentando una adecuada participación de los interesados en las decisiones y actividades del

proyecto. La satisfacción de los interesados debe gestionarse como uno de los objetivos clave del proyecto”.

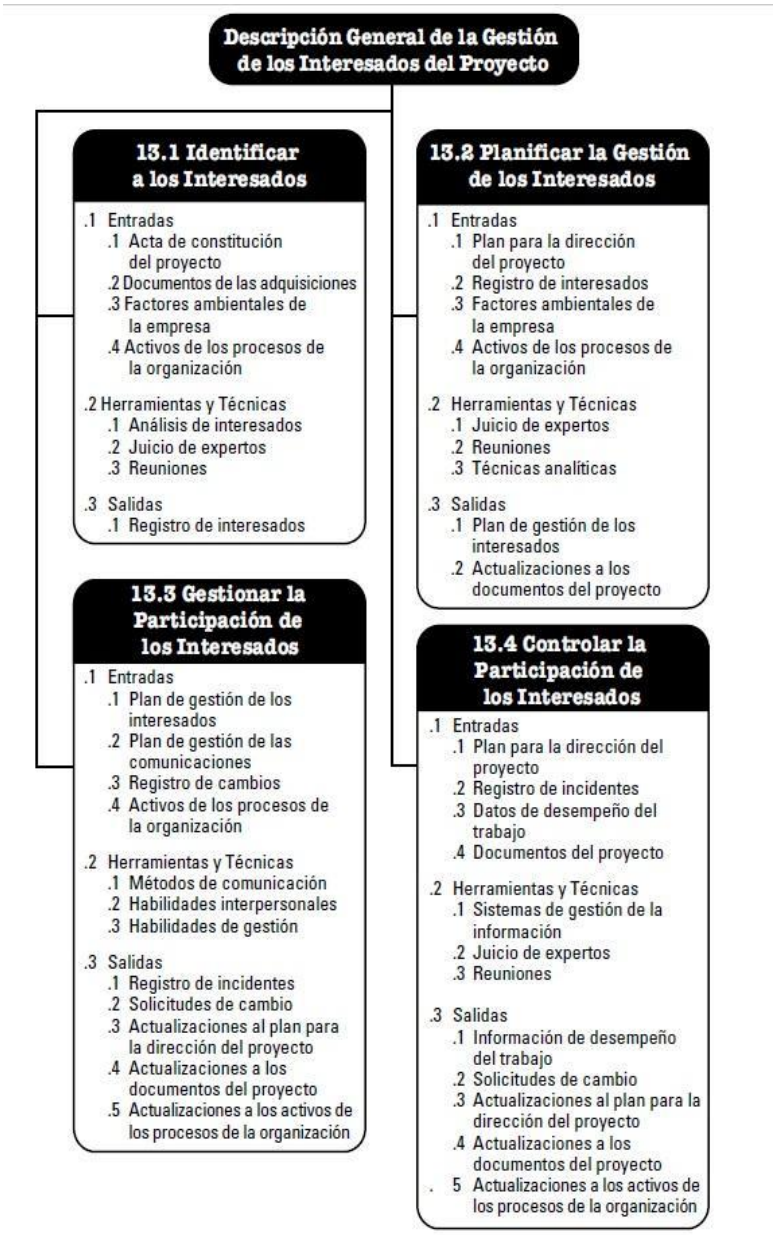


Figura 60 Gestión de Interesados (stakeholders) del Proyecto. Extraído de PMBOK quinta edición. Op cit

.

En el ámbito de Gestión de Interesados del proyecto se busca identificar, analizar, involucrar y gestionar a las partes interesadas del proyecto. A ese fin podemos señalar las siguientes actividades y procesos sugeridos:

1. Identificar a las partes interesadas: Se identifican todas las personas, grupos u organizaciones que pueden afectar o ser afectados por el proyecto. Esto incluye a los patrocinadores, los clientes, los usuarios finales, los miembros del equipo del proyecto, los proveedores, los reguladores y cualquier otra parte interesada relevante.

2. Planificar la gestión de los interesados: Se desarrolla un plan de gestión de los interesados que establece cómo se gestionarán y se involucrarán las partes interesadas a lo largo del proyecto. Este plan define las estrategias de comunicación, los niveles de participación, las expectativas de las partes interesadas y las acciones para gestionar los riesgos y los problemas relacionados con las partes interesadas.

3. Gestionar la participación de los interesados: Se involucra a las partes interesadas de manera activa y continua a lo largo del proyecto. Esto implica la comunicación regular y efectiva con las partes interesadas, la recopilación de sus necesidades y expectativas, y la integración de sus comentarios en la toma de decisiones del proyecto. También se busca su apoyo y compromiso para el éxito del proyecto.

4. Controlar la participación de los interesados: Se supervisa y se controla la participación de las partes interesadas durante todo el proyecto. Esto incluye la evaluación de la efectividad de las estrategias de gestión de los interesados, el seguimiento de los cambios en las necesidades y expectativas de las partes interesadas, y la gestión de los problemas y conflictos que puedan surgir.

5. Gestionar los conflictos de los interesados: Se identifican y se resuelven los conflictos entre las partes interesadas. Esto implica la negociación, la mediación y la facilitación para llegar a soluciones aceptables para todas las partes. Se busca encontrar un equilibrio entre las necesidades y expectativas de las partes interesadas y los objetivos y restricciones del proyecto.

Podemos ver que se enfatiza la importancia de la gestión efectiva de las partes interesadas en el éxito del proyecto. Por tanto, se espera comprender mejor las necesidades y expectativas de las partes interesadas, involucrarlas de manera adecuada y gestionar los riesgos y los conflictos asociados con estas partes. Esto ayuda a establecer relaciones positivas con las partes interesadas y a mantener su apoyo y compromiso a lo largo del proyecto.

Gestión de interesados del proyecto. Consideraciones para Plataforma BCT NFT/FT

El único aspecto vinculado a la gestión de interesados que consideramos, puede mostrar perfiles diferenciales o propios de la Plataforma BCT NFT/FT con relación a otros proyectos, es la vinculación a las comunidades o partes interesadas en utilizar el soporte de la Plataforma para desplegar Contratos Inteligentes propios, o en desarrollar interfaces o aplicaciones externas a la Plataforma misma.

En este caso se deberá valorar la influencia o impacto que puedan tener estos actores externos, involucrados en el proyecto, en función de extender las funcionalidades del mismo. Esta interacción deberá ser considerada en sus alcances directos, e indirectos. Es decir, se deberá valorar, no solamente el impacto en el proyecto de Plataforma BCT NFT/FT de los desarrollos que se desplieguen por parte de terceros en la misma, sino también, los mercados secundarios que estos potencialmente puedan generar, completando así el alcance propio del ecosistema BCT generado.

Conclusiones

En el presente trabajo realizamos un abordaje sobre la metodología de gestión de proyecto de la Plataforma BCT NFT/FT para la provincia de Santa Fe que estamos analizando.

En términos de definir una hoja de ruta, o guía sistemática de acciones, decidimos utilizar el CBDC Policy-Maker Toolkit del The World Economic Forum (conocido como el Foro de Davos). Esta herramienta no es la óptima para identificar las acciones que se deberían llevar a cabo en el desarrollo de la Plataforma BCT NFT/FT, ya que se vincula directamente con el desarrollo de Monedas Digitales de Bancos Centrales. Sin embargo, creemos que el Toolkit puede ser utilizado como base para delinear una tentativa Hoja de Ruta para nuestro análisis particular de una Plataforma BCT NFT/FT.

De esta forma es que analizamos paso a paso, las fases y actividades propuestas por el Toolkit, y en los casos en que consideramos se deberían hacer salvedades, modificaciones o inclusiones vinculadas con alinear las especificaciones al ámbito particular de una Plataforma BCT NFT/FT.

En segundo lugar, se analizó las características propias de las principales metodologías, conocimientos y buenas prácticas de gestión de proyectos que se utilizan actualmente. De esta manera fueron analizadas, características del PMBOK (Project Management Body of Knowledge), ISO 21500, PRINCE2 (PRojects IN Controlled Environments 2), GDPM (Goal Directed Project Management).

Consideramos necesario, realizar también un análisis detallado de las denominadas “metodologías ágiles” por sus características disruptivas en términos de presentar un nuevo paradigma en el desarrollo de proyectos, especialmente vinculado a proyectos de desarrollo de software. De esta forma se analizaron los métodos SCRUM, Lean Software Development, Kanban. Realizamos una comparativa de características esenciales de cada una de estas metodologías, y una evaluación de consideraciones específicas que al respecto se deberían considerar con relación a la Plataforma BCT NFT/FT.

Por último, fuimos analizando cada uno de los aspectos relevantes del PMBOK, ya que es a nivel global la guía/metodología más utilizada en la gestión efectiva de desarrollo de proyectos.

Los aspectos relevados fueron, Gestión de la Integración del Proyecto, Gestión del Alcance del Proyecto, Gestión del Tiempo del Proyecto, Gestión de los Costos del Proyecto, Gestión de la Calidad del Proyecto, Gestión de los Recursos Humanos del Proyecto, Gestión de las Comunicaciones del Proyecto, Gestión de los Riesgos del Proyecto, Gestión de las Adquisiciones del Proyecto, y Gestión de los Interesados del Proyecto.

Al igual que en todos los pasos previos, fuimos evaluando las características propias a considerar con relación al proyecto específico de desarrollo de la Plataforma BCT NFT/FT, en cada uno de los aspectos citados.

Sería redundar, repetir en este punto los análisis puntuales que fuimos desarrollando en cada tema analizado. Por dicho motivo, sólo mencionaremos en este apartado de conclusiones dos aspectos, ya analizados, pero que consideramos esenciales, en virtud de la naturaleza que imprime la tecnología de Blockchain sobre proyectos basados en la misma:

- el impacto de nuevas tecnologías, o desarrollos implementados sobre la Blockchain, tales como EIP-4337 Account Abstraction, ZKP - Pruebas de conocimiento cero, las cuales ya se encuentran en utilización en las Cadenas de Bloques. Esta valoración es fundamental para el análisis y evaluación de adopción de metodologías ágiles, que puedan sopesar el impacto de nuevas tecnologías disruptivas sobre la gestión de proyecto.
- la necesidad de considerar como eje central de la planificación de desarrollo de la Plataforma BCT NFT/FT para la provincia de Santa Fe, los procesos y actividades vinculadas al desarrollo de testing de Contratos Inteligentes que se implementarán, como así también las auditorias funcionales y técnicas sobre los mismos. Este factor es esencial en la tecnología de Blockchain, en relación a la imposibilidad de modificar o evitar la ejecución de los Contratos Inteligentes que sustentan sus desarrollos.

Análisis de ventajas, desventajas, fortalezas, debilidades y oportunidades del desarrollo de la Plataforma para la generación y gestión de Tokens criptográficos de la Provincia de Santa Fe

Introducción

En el primer informe que realizamos al abordar la evaluación de desarrollo de una Plataforma Blockchain de NFT/FT para Santa Fe, hicimos un relevamiento de los principales componentes de la tecnología de Cadena de Bloques, analizando billeteras digitales, transacciones, mineros, minería de bloques, mecanismos de consensos. También evaluamos los aspectos distintivos de los Contratos Inteligentes, base fundacional del ecosistema de Blockchain. Finalmente realizamos una descripción de los artefactos generalmente utilizados para desarrollar sistemas basados en a Blockchain, como Tokens, Tokens no Fungibles y Fungibles, ERC-20, ICOs, DAOs y otros.

En el segundo nos centramos en analizar el marco normativo argentino e internacional en referencia a criptomonedas y otros activos financieros digitales. Se relevó la normativa en relación al marco de Constitución Nacional Argentina, Leyes impositivas nacionales y subnacionales. En el ámbito internacional se estudió el marco regulatorio del Parlamento Europeo referido a Criptoactivos por ser considerado el de mayor detallamiento y alcance en el tema.

En el tercer reporte se desarrollaron las cuestiones vinculadas a definiciones difusas que se pueden apreciar en referencia a la territorialidad de impuestos, en especial considerando la disrupción de la tecnología de Blockchain, en lo que concierne a red descentralizada.

En el cuarto informe se realizó un relevamiento y análisis de los principales instrumentos financieros digitales, desarrollados sobre plataformas Blockchain, es decir, un mapeo de lo que se denomina el ecosistema de las DeFi - Finanzas Descentralizadas.

Siguiendo con el plan de actividades propuesto, en el quinto informe se realizó una evaluación de las diferentes plataformas de Blockchain disponibles en mercado, analizando los proyectos y comunidades que las sustentan, como así también los mecanismos, o protocolos, de consenso en las que se basan. Es central en la tecnología de Blockchain, la cuestión vinculada al protocolo de consenso, ya que es el mecanismo por el cual la tecnología alcanza, factores críticos como su escalabilidad, seguridad, invulnerabilidad y transparencia.

Por último, en el sexto reporte abordamos las principales cuestiones vinculadas con la gestión de proyecto, para el desarrollo de la Plataforma BCT NFT/FT para la provincia de Santa Fe. En este trabajo se analizaron las líneas directrices a la gestión de proyectos propuestas por al PMBOK, el recurso más utilizado a nivel mundial en ese ámbito. Sin perjuicio de esto se evaluaron también metodologías ágiles. Al no existir un plan de actividades propias para el desarrollo de una Plataforma BCT NFT/FT, se relevó detalladamente el “Central Bank Digital Currency Policy-Maker Toolkit” sugerido por el WebForum, realizando las salvedades vinculadas a las diferencias encontradas entre la tipología de desarrollo de una CBDC (Central Bank Digital Currency) y la Plataforma objeto de nuestro análisis.

En el presente documento vamos a abordar un análisis de ventajas, desventajas, fortalezas, debilidades y oportunidades del desarrollo de la Plataforma. Para esto vamos a utilizar la metodología de análisis estratégico conocida como FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) desarrollada originalmente por Albert Humphrey.

Vamos también a realizar una evaluación crítica de posibles rumbos vinculados al desarrollo de la Plataforma.

Primero veamos en forma global las ventajas y desventajas que se deben tener en cuenta al evaluar la Plataforma BCT NFT/FT para Santa Fe.

Ventajas:

1. Descentralización y seguridad:

La descentralización es el pilar fundamental sobre el cual se sustenta la blockchain. En una red blockchain, la información y los datos se almacenan en una cadena de bloques distribuida entre múltiples nodos o participantes en la red. Esto contrasta marcadamente con los modelos tradicionales, donde la información suele concentrarse en servidores centralizados. La plataforma blockchain proporciona un enfoque descentralizado que aumenta la seguridad y reduce la vulnerabilidad a ataques cibernéticos, ya que la información se distribuye en múltiples nodos de la red.

La descentralización ofrece ventajas fundamentales para la tecnología de Blockchain:

1.1. Imposibilidad de eliminar o modificar información

La ausencia de un único punto de control centralizado hace que sea casi imposible censurar o bloquear la información en una blockchain, lo que garantiza una imposibilidad directa para que una autoridad gubernamental pueda restringir el uso del sistema que se basa en tecnología Blockchain.

1.2. Mayor seguridad

Al descentralizar los datos y las transacciones, se minimiza la vulnerabilidad a ataques y fallos. Incluso si uno o varios nodos fallan, la red continúa operando. Solo colapsaría si una cantidad masiva de los mismos caen al mismo tiempo.

La seguridad en la blockchain es un componente esencial que trabaja en conjunto con la descentralización para lograr un sistema robusto y confiable. La seguridad se logra principalmente a través de dos mecanismos clave:

- **Criptografía:** la criptografía asegura que los datos almacenados en la blockchain sean inmutables y resistentes a la manipulación. Los algoritmos criptográficos protegen la integridad de los registros, lo que garantiza que una vez que la información se almacena en un bloque, no pueda ser alterada sin ser detectada.

- **Consenso distribuido:** si bien existen una gran cantidad de protocolos de consenso, los más utilizados, el de Prueba de Trabajo (PoW) y el Prueba de Participación (PoS), garantizan que solamente las transacciones legítimas sean validadas y añadidas a la cadena de bloques. Esto impide la falsificación y el doble gasto.

1.3. Transparencia y confianza

La información almacenada en la blockchain es pública y verificable por cualquier participante. Esto aumenta la confianza en las transacciones y la integridad de los datos.

1.4. Programabilidad - Contratos Inteligentes

La combinación de descentralización y seguridad permite la ejecución confiable de contratos inteligentes, pequeños programas que van a ser registrados en la Blockchain, y esta se encargará de ejecutarlos. Esto abre la puerta a la modelización de procesos legales y financieros sin necesidad de intermediarios que centralizan el gobierno de la red.

Es esencial destacar en este punto, que la base de los Contratos Inteligentes es su capacidad de auto-ejecución descentralizada. Todos los nodos de la Blockchain se encargan de ejecutarlos y al haber sido registrados en la Blockchain en forma similar a las transacciones, se garantiza que el código del Contrato Inteligente no se pueda modificar y sea inexorablemente ejecutado.

2. Transparencia

La transparencia es uno de los valores fundamentales que sustentan la tecnología blockchain. A diferencia de los sistemas centralizados, donde la información puede estar oculta o manipulada, la blockchain ofrece un grado sin precedentes de visibilidad y verificabilidad. Todos los nodos de la Blockchain conservan y gestionan una copia “sincronizada” (por medio del protocolo de consenso) de todas las transacciones que se realizaron en la red, desde el inicio de esta. El mecanismo de consenso de la Blockchain es el que permite que todos los nodos acepten como válido un registro único de las transacciones.

Todo esto asegura que la información de la Blockchain se encuentre disponible en forma permanente en todos los nodos de esta, y esa información esté sincronizada de modo que no haya inconsistencias. En conclusión, estos factores garantizan la transparencia de la red.

Dos factores adicionales a las consideraciones realizadas sobre transparencia son:

2.1. Trazabilidad

Al quedar registradas todas las transacciones, desde la primera (“bloque genesis”) se puede realizar una trazabilidad de cada cuenta criptográfica que ha actuado en la Blockchain.

2.1. Auditabilidad

La información almacenada en la blockchain es inmutable y no se puede alterar una vez que se confirma. Esto facilita las auditorías y garantiza que las transacciones no se puedan manipular.

Es de destacar, en relación a ambos factores mencionados anteriormente, se encuentran vinculados pero, que a su vez, en las Blockchain públicas - no permisionadas, las cuentas criptográficas son anónimas ya que no se registran ningunos datos identificativos de sus titulares, como tampoco se necesita una autorización de alguno de los nodos de la red para poder actuar en esta.

En el caso concreto que nos ocupa, la Plataforma Blockchain NFT/FT para Santa Fe, debemos considerar como opción casi indiscutible el desarrollo de una Blockchain privada o permisionada, pero esto no afecta las consideraciones que realizamos sobre trazabilidad y auditabilidad.

3. Eliminación de Intermediarios:

La blockchain permite transacciones peer-to-peer sin intermediarios. Esto reduce la posibilidad de fraude y reduce los costos asociados con intermediarios financieros.

La afirmación de que la tecnología blockchain elimina a los intermediarios se basa en las características fundamentales de esta tecnología, que cambia la forma en que se realizan y registran las transacciones. Entre las razones claves por las que podemos afirmar que la tecnología de blockchain puede eliminar a los intermediarios, podemos mencionar:

3.1. Transacciones peer-to-peer

En una red blockchain, los usuarios pueden realizar transacciones directamente entre sí, sin necesidad de un intermediario central, como un banco, una entidad financiera o una empresa de sistemas de pagos. Esto se aplica a la transferencia de activos digitales, como criptomonedas, pero también a otros tipos de transacciones, como la venta de bienes y servicios, previamente tokenizados.

3.2. Contratos inteligentes

Como ya mencionamos, la tecnología blockchain permite la creación e implementación de contratos inteligentes, que son pequeños programas informáticos auto-ejecutables que automatizan acuerdos y transacciones cuando se cumplen ciertas condiciones. Estos contratos pueden reemplazar a intermediarios en situaciones como la compra de una activo financiero digital, un pago de interés o premio por colocar en staking una cantidad determinada de criptoactivos.

En el caso de la Plataforma BCT NFT/FT que estamos analizando, la posibilidad de que terceros puedan desplegar Contratos Inteligentes sobre la misma, será una decisión política y estratégica a tomar por parte del gobierno de la Santa Fe. En el caso que sea así, se deberá ponderar el beneficio de facilitar el desarrollo de un ecosistema Blockchain propio de la Plataforma, en el cual por medio de los Smart Contracts se regulen y programen relaciones directas entre usuarios, y contraponer esto a que el gobierno ceda un control directo sobre ese ecosistema.

3.3. Reducción de costos

Al eliminar intermediarios, las transacciones en blockchain a menudo resultan en menores costos para los usuarios. En las Blockchain públicas - no permisionadas, todas las transacciones pagan una tarifa. En principio, como recompensa a los mineros que realizan el trabajo de mineración de bloques para lograr el consenso, factor fundamental para asegurar la inalterabilidad e invulnerabilidad de la Cadena de Bloques. Pero también el pago de una tarifa por cada transacción tiene como objetivo invitar ataques de DOS (denied of services), es decir que se intente hacer caer la red enviando una cantidad exageradamente masiva de transacciones simultáneas. Al tener que pagar una tarifa, aunque sea baja, por cada transacción, se imposibilita que un hacker pueda realizar este tipo de ataque masivo contra la red.

En la Plataforma BCT NFT/FT que estamos analizando, es de esperar que se procure que los usuarios paguen una tarifa lo más baja posible por transacciones, o por la ejecución de

Contratos Inteligentes, incluso, que no se pague por cada transacción (en el caso que la Blockchain sea privada - permisionada). Todo esto para alentar el uso de la misma.

Si bien la blockchain ofrece estas ventajas en términos de eliminación de intermediarios, también es importante destacar que no todas las aplicaciones y casos de uso pueden prescindir por completo de intermediarios. En algunos casos, los intermediarios pueden seguir siendo necesarios para proporcionar servicios adicionales, como la conversión de activos digitales en moneda fiduciaria o la gestión de disputas. Sin embargo, la blockchain ha allanado el camino para una mayor autonomía y control de los usuarios sobre sus activos y transacciones, lo que ha llevado a una reducción significativa de la dependencia de intermediarios en muchos escenarios.

4. Acceso global:

La naturaleza digital de los tokens y la tecnología blockchain permiten un acceso global sin restricciones geográficas, ni de horarios o identidad de usuarios.

La blockchain tiene un acceso global y proporciona información siempre disponible debido a sus características técnicas fundamentales y su arquitectura descentralizada. Algunas de las características propias de esta ventaja de la tecnología Blockchain, ya han sido descriptas previamente en este trabajo. Sin perjuicio de esto, mencionaremos algunas de las más relevantes.

4.1. Descentralización

Como ya se mencionó, la descentralización es uno de los aspectos centrales de la tecnología de Blockchain. En una Blockchain, la información y los datos se almacenan en múltiples nodos distribuidos en diferentes localizaciones geográficas. Estos nodos trabajan juntos para mantener la integridad de la cadena de bloques y validar las transacciones. De este modo, y en relación con la capacidad de acceso global de la Blockchain, la información no reside en un solo lugar o servidor centralizado, lo que la hace accesible desde cualquier parte del mundo y la protege contra fallos locales.

4.2. Consistencia de datos

La información en una Blockchain es replicada y sincronizada entre todos los nodos de la red. Esto garantiza que, en cualquier momento, todos los participantes tengan una copia actualizada y consistente de la cadena de bloques. No importa dónde se encuentre un usuario, siempre verá la misma información en la Blockchain, lo que garantiza la disponibilidad permanente de datos.

4.3. Inmutabilidad de datos

Una vez que la información se registra en una blockchain, se vuelve inmutable y no puede ser modificada ni eliminada sin el consenso de la mayoría de la red. Esto asegura que la información esté siempre disponible y sea confiable, ya que no puede ser alterada por actores maliciosos.

La blockchain ofrece acceso global y disponibilidad constante de información gracias a su estructura descentralizada, su distribución global de nodos, su capacidad de mantener la consistencia de datos, y su inmutabilidad. Estas características la hacen adecuada para una variedad de aplicaciones, como las criptomonedas y todas las variedades de instrumentos financieros digitales que hemos mencionado al describir el ecosistema DeFi.

5. Programabilidad de cripto-activos

Los tokens pueden ser programables mediante contratos inteligentes, lo que facilita la automatización de procesos y la creación de aplicaciones descentralizadas.

La programabilidad de los contratos inteligentes en la blockchain, hace referencia, como ya se mencionó, a la capacidad de estos contratos para llevar a cabo acciones y ejecutar lógica de determinados procesos de negocio de manera autónoma y automatizada cuando se cumplen ciertas condiciones predefinidas.

La lógica de un contrato inteligente es visible y transparente en la cadena de bloques, lo que significa que todos los participantes pueden verificar cómo está programado el contrato y cómo se comportará en diferentes situaciones.

Una vez que se despliega un contrato inteligente en una cadena de bloques, su código es inmutable y no se puede cambiar sin el consenso de la red. Esto garantiza la previsibilidad y la confiabilidad de los contratos.

Los contratos inteligentes se ejecutan en nodos de la cadena de bloques distribuidos en toda la red. Esto significa que la ejecución de un contrato no depende de un solo servidor o entidad central, lo que aumenta la resistencia a la censura y la confiabilidad.

Amplio rango de aplicaciones: Los contratos inteligentes se pueden utilizar en una amplia variedad de aplicaciones, desde las criptomonedas hasta la gestión de la cadena de

suministro, la votación electrónica, los juegos en línea y mucho más. Su programabilidad permite que se adapten a diversas necesidades y casos de uso.

La programabilidad de los contratos inteligentes ha revolucionado la forma en que se realizan las transacciones y se gestionan los activos digitales, al permitir la automatización de procesos y la creación de aplicaciones descentralizadas (dApps), como así también ser el sustento de todo el ecosistema DeFi (Finanzas Descentralizadas), factor esencial a considerar en el desarrollo de la Plataforma BCT NFT/FT para la provincia de Santa Fe.

Desventajas

1. Escalabilidad:

La falta de escalabilidad en la blockchain se refiere a la limitación en la capacidad de una red blockchain para manejar un número creciente de transacciones de manera eficiente y rápida a medida que la red crece. La tecnología de Blockchain como mencionamos reiteradamente, gana su invulnerabilidad e inmutabilidad por medio del registro descentralizado de sus operaciones y por la fuerte encriptación que utiliza. Todo esto, evidentemente, tiene un costo en performance y velocidad de la red.

La escalabilidad es un desafío técnico importante que ha sido objeto de atención y desarrollo continuo desde los primeros días de las blockchain. La falta de escalabilidad puede manifestarse de varias maneras:

1.1. Ralentización de las transacciones:

A medida que más usuarios realizan transacciones en una cadena de bloques, la velocidad de procesamiento de estas transacciones puede disminuir. Esto significa que las transacciones pueden tardar más tiempo en confirmarse, lo que afecta la eficiencia de la red.

En este aspecto, las Blockchain, como el caso de Ethereum, han decidido cambiar de protocolos de consenso, por ejemplo, desde el POW (Prueba de Trabajo) al del POS (Prueba de Participación).

Para abordar estos desafíos, se han propuesto y desarrollado soluciones como el aumento del tamaño de los bloques, la implementación de algoritmos de consenso más eficientes (como Prueba de Participación delegada o Sharding), y la búsqueda de capas de escalabilidad como las soluciones de capa 2 (por ejemplo, Lightning Network para Bitcoin o canales de estado para Ethereum).

1.2. Costos de transacción elevados:

Vinculado con el punto anterior, la competencia por la inclusión en un bloque puede llevar a tarifas de transacción más altas. Los usuarios pueden verse obligados a pagar tarifas más elevadas para que sus transacciones se procesen más rápidamente.

1.3. Congestión de la red:

En momentos de alta demanda, como durante un pico de actividad en una cadena de bloques, la red puede congestionarse, lo que lleva a demoras significativas en las transacciones y aumenta la competencia por la inclusión en los bloques.

1.4. Tamaño de la cadena de bloques:

A medida que se agregan más transacciones a una cadena de bloques, su tamaño crece constantemente. Esto puede hacer que la descarga y la sincronización de la cadena de bloques sean un proceso lento y exigente en recursos para nuevos nodos que se unen a la red.

Por otra parte, el tamaño máximo de los bloques en una cadena de bloques puede limitar la cantidad de transacciones que se pueden incluir en cada bloque. En Bitcoin, por ejemplo, el tamaño del bloque es de 1 MB, lo que establece un límite en la cantidad de transacciones que se pueden procesar por bloque.

1.5. Latencia de la red:

Además de la demora en el minado de cada bloque, por consecuencia de una gran cantidad de transacciones a procesar, la latencia de la red puede causar también retrasos significativos. En especial, en la propagación de las transacciones entre los nodos de la red, lo que puede afectar la velocidad y la eficiencia global de la cadena de bloques.

La falta de escalabilidad es un problema continuo en el desarrollo de blockchain, ya que el equilibrio entre la descentralización, la seguridad y la escalabilidad es un desafío técnico complejo. Diversos proyectos están trabajando en soluciones para abordar este problema y permitir que las blockchain manejen un mayor volumen de transacciones de manera más eficiente.

2. Consumo energético:

El alto consumo energético es uno de los principales inconvenientes asociados con muchas blockchain, especialmente aquellas que utilizan el algoritmo de consenso de Prueba de Trabajo (PoW), como Bitcoin. En relación al alto consumo energético en las blockchain podemos destacar:

2.1. Impacto ambiental:

El alto consumo de energía de las blockchain, en especial las basadas en PoW (Prueba de Trabajo) tiene un impacto significativo en el medio ambiente. La minería de criptomonedas, que utiliza PoW, requiere una cantidad sustancial de energía, y gran parte de esta energía proviene de fuentes no renovables, como los combustibles fósiles. Esto contribuye al aumento de las emisiones de gases de efecto invernadero y al cambio climático.

2.2. Costos económicos:

La minería de PoW es costosa en términos de energía eléctrica. Esto puede hacer que la operación de nodos de minería sea costosa y limitar la participación en la red a aquellos que pueden pagar los costos de energía.

Blockchain como Bitcoin, tienen un sistema de autorregulación del minado, que lleva a gestionar la facilidad o dificultad de la tarea de los mineros. Esto sirve para permitir el acceso de más mineros cuando la dificultad es baja y de esta manera aumentar la competencia, o por el contrario, aumentar la dificultad para que los mineros desistan de continuar en esa tarea. Pero, existe un impacto directo en este esquema, de los costos fijos y la inversión inicial que deben hacer los mineros, que no encaja con la facilidad de acceso y expulsión de los mismos en el negocio de minado.

2.3. Centralización:

En algunas blockchain que utilizan protocolo PoW, la centralización de la minería es un problema debido a los altos costos y la necesidad de infraestructura especializada. Esto puede llevar a la formación de pools de minería, donde varios mineros se unen para aumentar sus posibilidades de recompensa, lo que potencialmente amenaza la descentralización.

Para abordar estos inconvenientes relacionados con el alto consumo energético, se han propuesto y desarrollado alternativas al algoritmo PoW. Una de las alternativas más notables es la Prueba de Participación (PoS), que requiere que los validadores bloqueen una cantidad de criptomonedas como garantía en lugar de gastar energía resolviendo problemas computacionales complejos. PoS se considera más eficiente energéticamente y menos dañino para el medio ambiente. Otras soluciones incluyen algoritmos de consenso como Prueba de Autoridad (PoA) y Prueba de Historial (PoH).

Una nota aparte que se considera relevante realizar, es que la Blockchain Ethereum, que lidera tecnológicamente en la comunidad Blockchain, se está orientando al uso de mineria

por medio de ZKP - Pruebas de Conocimiento Zero. La idea tras esta iniciativa es que la minería de grandes cantidades de transacciones se haga “off-chain” (fuera de la Blockchain), pero su validación al ingresar dichas transacciones a la Cadena de Bloques se realice por medio una prueba de conocimiento cero, es decir, validar una cantidad importante de transacciones, en un solo paso. Esta tecnica denominada Roll-Up en la Blockchain es lo que aseguraría a Ethereum poder procesar una gran cantidad de transacciones en pocos segundos, sin perder su seguridad, ni perder potencial escalabilidad.

Análisis FODA

El análisis SWOT (Strengths, Weaknesses, Opportunities, Threats), también conocido como análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) por sus siglas en español, tiene sus raíces en la década de 1960. Fue desarrollado por Albert Humphrey y su equipo en el Stanford Research Institute durante un proyecto de investigación encargado por Fortune 500 para identificar por qué las empresas tenían problemas de planificación estratégica[75].

La idea tras el proyecto que lideró Albert Humphrey tenía como objetivo principal desarrollar una herramienta que ayudara a las empresas a evaluar su situación estratégica de manera más efectiva. Albert Humphrey y su equipo crearon lo que entonces se llamó el "Método SOFT", que más tarde se popularizó como el análisis SWOT. La idea era proporcionar un esquema sistemático para que las organizaciones evalúen sus factores estratégicos internos y externos más relevantes[76].

A medida que empresas y organizaciones fueron adoptando, el análisis SWOT se convirtió en una herramienta ampliamente utilizada en la toma de decisiones estratégicas y en la planificación estratégica en general. En la actualidad es una técnica altamente difundida, y considerada central en la gestión empresarial y en la planificación estratégica.

La idea base del análisis FODA es evaluar la situación actual de una organización, proyecto o situación, con el objetivo de identificar sus Fortalezas (F), Debilidades (D), Oportunidades (O) y Amenazas (A). Estas cuatro categorías representan aspectos internos y externos que pueden afectar el desempeño y la viabilidad de la entidad o proyecto en cuestión.

Metodología del análisis FODA

Los pasos para realizar un análisis FODA consisten en[77]:

Recopilación de información: antes de realizar el análisis FODA, se debe recopilar información relevante sobre la organización/empresa, proyecto o situación bajo análisis. Esto puede incluir datos financieros, estadísticas de mercado, información sobre competidores, comentarios de clientes, y cualquier otro dato pertinente.

---

[75] Fine, L. G. (2009). *The SWOT analysis: Using your strength to overcome weaknesses, using opportunities to overcome threats*. Kick It LLC.
[76] Humphrey, A. (2005). SWOT analysis for management consulting. *SRI alumni Newsletter*, *1*, 7-8.
[77] Dealtry, T. R. (1992). *'Dynamic SWOT Analysis': Developer's Guide*. Intellectual Partnerships.

En lo referente al aspecto en análisis que estamos realizando para el desarrollo de una plataforma Blockchain para desarrollo de NFT/FT, la recopilación de información se realizará en referencia al ecosistema de Blockchain, grupos de interés, comunidades de desarrolladores, especialmente de las denominadas DeFi (Finanzas Descentralizadas).

Creación de la matriz FODA: Se deben organizar las fortalezas, debilidades, oportunidades y amenazas en una matriz de cuatro cuadrantes. Esto te ayudará a visualizar la información de manera clara y concisa.

Análisis y estrategia: Una vez que se haya desarrollado la matriz FODA, se debe analizar las relaciones entre las diferentes categorías.

Las estrategias más comunes son:

Estrategias FO (potenciar Fortalezas para aprovechar Oportunidades): Consiste en vincular las fortalezas internas con oportunidades externas, con la finalidad de aprovechar las mismas.

Estrategias FA (utilizar Fortalezas para mitigar Amenazas): consiste en planificar cómo utilizar las fortalezas internas para defenderse de las amenazas externas.

Estrategias DO (mejorar Debilidades para aprovechar Oportunidades): se debe trabajar en las corregir debilidades internas para aprovechar las oportunidades externas.

Estrategias DA (superar Debilidades para mitigar Amenazas): se basa en abordar las debilidades internas para defenderse de las amenazas externas.

Desarrollo de un plan de acción: basándose en el análisis FODA y las estrategias identificadas, se debe crear un plan de acción que establezca los procesos específicos que la entidad o proyecto debe tomar para capitalizar sus fortalezas, abordar sus debilidades, aprovechar oportunidades y mitigar amenazas.

Implementación y seguimiento: se debe llevar a cabo las acciones planificadas y realizar un seguimiento constante para evaluar su efectividad, logro de metas y objetivos, y hacer ajustes que fuesen necesarios.

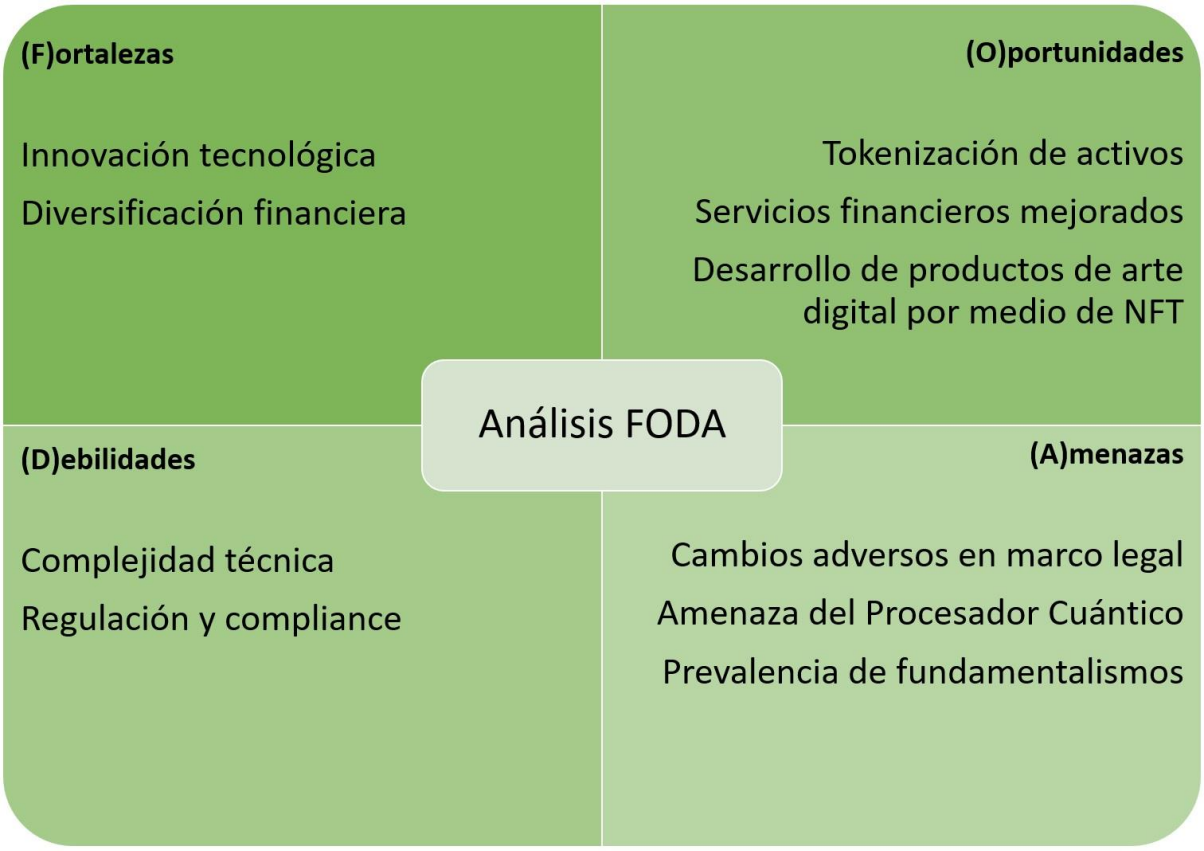
En el análisis particular que estamos realizando, en relación a la Plataforma Blockchain NFT/FT para la provincia de Santa Fe, vamos a obviar los aspectos vinculados al desarrollo de plan de acción, implementación y seguimiento, ya que estos deberán ser desarrollados

por los responsables políticos del proyecto, tal como se expuso detalladamente en la Tarea 06 - *“Confeccionar un Informe, a modo de perfil, del proyecto de desarrollo de la Plataforma para generación y gestión de tokens criptográficos, de la Provincia de Santa Fe analizando entre otros factores relevantes, la contratación de RRHH, conformación de equipos de trabajo, líneas de tiempo, adquisiciones, riesgos”*.

Análisis FODA plataforma Blockchain NFT/FT para la provincia de Santa Fe

La tecnología blockchain ha revolucionado la forma en que se gestionan los activos digitales y las transacciones en línea. Una plataforma de blockchain para tokens criptográficos NFT/FT para la provincia de Santa Fe tiene como objetivo crear un ecosistema donde los usuarios puedan emitir, intercambiar y gestionar tokens digitales de manera descentralizada.

En este punto vamos a analizar, fortalezas, debilidades, oportunidades y amenazas asociadas con el desarrollo de dicha plataforma.



Fortalezas

1. Innovación tecnológica:

El desarrollo de una plataforma de blockchain para tokens criptográficos impulsa la innovación en el campo de las finanzas, la tecnología y la seguridad cibernética.

2. Diversificación financiera:

Permite la creación de diversos tipos de tokens, como tokens de utilidad, tokens de seguridad y stablecoins, que brindan opciones de inversión más amplias.

Existen varios tipos de tokens que se pueden desarrollar y operar en blockchain, y su funcionalidad puede variar significativamente según sus propósitos. Aquí tienes algunos de los tipos más comunes de tokens:

2.1. Tokens de Utilidad:

Estos tokens se utilizan dentro de una red o plataforma blockchain específica para acceder a servicios o productos. Por ejemplo, los tokens de utilidad pueden usarse para pagar tarifas de transacción, obtener acceso a características adicionales en una aplicación o plataforma, o canjear bienes y servicios dentro de un ecosistema particular.

2.2. Tokens de Seguridad:

Estos son tokens que representan la propiedad de un activo subyacente, como acciones en una empresa, deuda o participación en un fondo de inversión. Los tokens de seguridad suelen estar sujetos a regulaciones financieras y pueden ofrecer derechos de voto o dividendos.

2.3. Stablecoins - Criptomonedas estables:

Los tokens de stablecoins están diseñados para mantener un valor constante o seguir una paridad con un activo real, generalmente, como una moneda fiduciaria (por ejemplo, USD, EUR, etc.). También pueden estar atados al precio de algún commodity como plata u oro, o incluso tener un Contrato Inteligente que lea la cotización del token y realice operaciones de minting (acuñamiento) o de burning (destrucción) de tokens, para mantener el precio estable del token. Estos tokens se utilizan para reducir la volatilidad y facilitar las transacciones y la adopción de criptomonedas.

2.4. Tokens de Gobierno (Governance Tokens):

Estos tokens se utilizan para participar en la toma de decisiones y la gobernanza de una red blockchain o plataforma. Los titulares de estos tokens pueden votar en propuestas de cambios en el protocolo o en otras decisiones importantes dentro del ecosistema.

2.5. NFT Tokens no Fungibles o Coleccionables:

Estos tokens representan activos digitales únicos o escasos, como arte digital, tarjetas coleccionables, objetos de juego, etc. Cada token de coleccionable tiene un valor único y puede ser intercambiado o vendido en mercados especializados.

2.6. Tokens de Acceso:

Estos tokens se utilizan para otorgar acceso a contenido o servicios específicos, como eventos en vivo, cursos en línea o contenido premium en una plataforma.

2.7. Tokens de Fidelidad (Loyalty Tokens):

Se utilizan en programas de fidelización para recompensar a los usuarios por su lealtad o uso continuo de un servicio o plataforma. Los usuarios pueden ganar y canjear estos tokens por beneficios adicionales o descuentos.

2.8. Tokens de Identidad:

Estos tokens se utilizan para gestionar y verificar la identidad en línea de manera segura. Pueden utilizarse en aplicaciones de gestión de identidad y autenticación.

2.9. Tokens de Pagos (Payment Tokens):

Estos tokens se utilizan principalmente como monedas digitales para realizar transacciones y pagos en la red blockchain. Ejemplos incluyen Bitcoin (BTC) y Ethereum (ETH), es decir lo que conocemos como criptomonedas clásicas, que en realidad al ser una representación digital de un derecho o valor, entran en esta categoría de Tokens.

2.10. Tokens de Deuda (Debt Tokens):

Representan acuerdos de préstamo o deuda y pueden utilizarse para financiar proyectos o empresas a través de contratos inteligentes.

Dentro de esta categoría de tokens criptográficos, podemos encontrar a las ICO (Oferta Inicial de Criptomonedas), que como ya hemos mencionado en trabajos anteriores, tienen una amplia difusión en sistema de crowdfunding, especialmente utilizados para financiar emprendimientos start-up.

2.11. Tokens de Participación -Acciones (Equity Tokens):

Son similares a los tokens de seguridad y representan una inversión en una empresa o proyecto. Los titulares de estos tokens pueden recibir dividendos o participar en las ganancias y pérdidas del proyecto.

Estos son solo algunos ejemplos de los diversos tipos de tokens que se pueden desarrollar y utilizar en blockchain. La elección del tipo de token dependerá de los objetivos y la funcionalidad específica que se busque en una aplicación o plataforma blockchain.

Debilidades:

(D)ebilidades

Complejidad técnica

Usuarios finales

Desarrolladores de aplicaciones blockchain

Ingenieros de blockchain

Expertos en seguridad blockchain

Expertos en gobernanza y regulación blockchain

Arquitectos de redes blockchain

Regulación y compliance

Falta de estandarización

Jurisdicciones múltiples

Contratos inteligentes complejos

Interoperabilidad

1. Complejidad técnica:

Tanto el desarrollo como la operación de una plataforma blockchain son técnicamente complejos y requieren conocimientos especializados.

La complejidad técnica de la tecnología blockchain puede variar significativamente según el contexto y el propósito de su implementación.

Por otra parte también puede analizarse la complejidad técnica de la blockchain desde las funciones de los diferentes interesados que intervienen en su ecosistema:

1.1. Usuarios finales:

Para los usuarios finales que simplemente desean utilizar aplicaciones o servicios basados en blockchain, la complejidad técnica es generalmente baja. Pueden descargar una billetera de criptomonedas, comprar tokens, realizar transacciones y participar en proyectos blockchain sin necesidad de conocimientos técnicos avanzados.

1.2. Desarrolladores de aplicaciones blockchain:

Los desarrolladores que desean crear aplicaciones, contratos inteligentes o protocolos blockchain necesitarán un nivel moderado a alto de conocimientos técnicos. Deben estar familiarizados con lenguajes de programación específicos de blockchain (como Solidity para Ethereum), entender los conceptos de la tecnología blockchain y ser capaces de diseñar, implementar y probar soluciones blockchain.

1.3. Ingenieros de blockchain:

Los ingenieros de blockchain son profesionales altamente especializados que trabajan en el diseño y desarrollo de blockchain desde cero o en la mejora de blockchain existentes. Requieren un conocimiento profundo de criptografía, algoritmos de consenso, arquitectura de red, seguridad y optimización de rendimiento.

1.4. Expertos en seguridad blockchain:

Dado que la seguridad es fundamental en blockchain, los expertos en seguridad de blockchain se especializan en la identificación y mitigación de vulnerabilidades en contratos inteligentes y protocolos blockchain. Esto implica un alto nivel de conocimiento de criptografía y hacking ético.

1.5. Expertos en gobernanza y regulación blockchain:

Aquellos que trabajan en la gobernanza y regulación de blockchain deben tener un profundo conocimiento de la tecnología blockchain, así como de los aspectos legales y regulatorios que la rodean. La complejidad varía según las jurisdicciones y las regulaciones específicas.

En el caso de la Plataforma BCT NFT/FT que estamos analizando, podríamos decir que las regulaciones específicas se vinculan casi en forma directa a un “limbo” legal vigente actualmente, no existe una clara y específica normativa, sino normativas diversas a las cuales equiparar las cuestiones propias del ecosistema blockchain.

1.6. Arquitectos de redes blockchain:

Los arquitectos de redes blockchain se centran en el diseño de la infraestructura de una red blockchain, incluyendo la configuración de nodos, la gestión de la escalabilidad y la elección de algoritmos de consenso. Esto requiere un conocimiento profundo de redes y sistemas distribuidos.

2. Regulación y compliance:

El entorno legal y regulatorio en torno a las criptomonedas y los tokens es aún incierto en Argentina, lo que puede dificultar la adopción y el desarrollo.

En el momento de escribir el presente trabajo la CNV - Comisión Nacional de Valores se encuentra analizando la posibilidad de regular cripto-activos.

La regulación de la tecnología blockchain presenta una serie de desafíos y problemas debido a la naturaleza única y disruptiva de esta tecnología.

Algunas de las discusiones que se deberían abordar en torno a la regulación de blockchain son:

2.1. Falta de estandarización:

La tecnología blockchain, y en especial el ecosistema derivado de la utilización de Contratos Inteligentes, es relativamente nueva y está en constante evolución. Existen marcos normativos amplios y detallados a nivel mundial, como el desarrollado por la SEC - Securities and Exchange Commission de USA, y el marco regulatorio de cripto-activos de la Comunidad Económica Europea, sin embargo se dificulta la creación de un marco regulatorio coherente y consistente a nivel global, en especial por la cantidad, diversidad y la constante aparición de nuevos instrumento financieros digitales.

2.2. Jurisdicciones múltiples:

La naturaleza global de la tecnología blockchain significa que las transacciones pueden cruzar fácilmente las fronteras, lo que crea desafíos para la regulación, ya que cada jurisdicción puede tener sus propias leyes y regulaciones.

En este aspecto hicimos un análisis pormenorizado de las dificultades de la gravabilidad de cripto-activos, en base a la complejidad de determinar territorialidad de los mismos.

La misma consideración se debería aplicar en torno a la regulación de los mismos.

2.3. Contratos inteligentes complejos:

La regulación de contratos inteligentes que, como ya mencionamoes, son programas auto-ejecutables en blockchain, puede ser complicada. Estos contratos pueden tener implicaciones legales significativas, y la falta de claridad legal puede llevar a disputas y desafíos.

Los Contratos Inteligentes, al llevar la misma lógica de registración en la Blockchain que las transacciones, son inalterables. De allí que al expresar en su lógica de proceso de negocios acciones que vinculan asignaciones de valores, o generación de obligaciones y derechos, estas pasan a ser inmutables e imposible de evitar su ejecución. De allí la complejidad adicional que conlleva su regulación.

2.4. Interoperabilidad:

Las blockchain a menudo operan de manera independiente, lo que dificulta la interoperabilidad entre diferentes blockchain y la transferencia de activos entre ellas. La regulación debe abordar estos problemas para facilitar la adopción y el uso de la tecnología blockchain en múltiples casos de uso. En especial en la adopción o generación de estándares que garanticen el mismo marco de seguridad “on-chain” (intra-red) que “off-chain” (extra-red).

Esto toma relevancia dentro del ámbito de la Plataforma BCT NFT/FT que estamos analizando, en cuanto múltiples gobiernos, provinciales y estado nacional están planificando desarrollar sistemas basados en Blockchain, para diferentes casos de uso.

Oportunidades

1. Tokenización de activos:

La Plataforma BCT NF/FT para Santa Fe, puede facilitar la tokenización de activos del mundo real, como bienes raíces o acciones, además de valores criptográficos regulares, lo que puede aumentar la liquidez y la accesibilidad a ambos tipos de activos.

Esta tokenización ofrece varias ventajas significativas. Algunas que deberíamos considerar son:

1.1. Fraccionamiento de activos:

La tokenización permite dividir activos en unidades más pequeñas y fraccionables. Esto facilita la inversión, ya que los inversores pueden comprar fracciones de activos de alto valor, como bienes raíces o obras de arte, en lugar de tener que adquirir el activo completo.

Este proceso de “atomización” de inversiones repercute directamente en facilidad de accesibilidad, y diversificación de cartera de quienes quieran participar en los productos financieros digitales que se ofrezcan por medio de la Plataforma BCT NFT/FT para Santa Fe.

1.2. Accesibilidad:

La tokenización democratiza el acceso a inversiones que anteriormente estaban limitadas a inversores institucionales o personas con alto patrimonio neto. Cualquier persona con acceso a una plataforma por medio de la tokenización puede invertir en una amplia variedad de activos, incluso formando sus propias carteras.

1.3. Liquidez mejorada:

Los activos tokenizados suelen ser más líquidos que sus contrapartes tradicionales. Los inversores pueden comprar, vender o intercambiar tokens más fácilmente, lo que facilita la entrada y salida de inversiones, dando un dinamismo relevante a las inversiones que impulsan la liquidez inherente.

1. 4. Reducción de costos:

La tokenización puede reducir los costos asociados con la intermediación financiera y la administración de activos. Esto se debe a la eliminación de intermediarios y a la automatización de procesos, como la liquidación y la gestión de registros.

1.5. Transparencia:

Con independencia de la gestión de identidades que se puede realizar en Blockchain privadas - permisionadas, como ya desarrollamos previamente, las transacciones y la propiedad de activos tokenizados se registran en la cadena de bloques de manera transparente y son accesibles para cualquiera que quiera verificarlas. Esto reduce el riesgo de fraudes y aumenta la confianza de los inversores.

1.6. Plantillas de contratos inteligentes para el proceso de tokenización:

Los contratos inteligentes pueden programarse para ejecutarse automáticamente cuando se cumplen ciertas condiciones predefinidas. Pero como ya se mencionó en documentos anteriores, existen en la comunidad de Blockchain (especialmente en Ehtereum), plantillas prediseñadas para desenvolver los Contratos Inteligentes de tokenización de activos. Esto simplifica la gestión de acuerdos y pagos, eliminando la necesidad de intermediarios.

1.7. Mayor seguridad:

La criptografía y la inmutabilidad de la blockchain hacen que los activos tokenizados sean resistentes a la falsificación y a la alteración de registros. Los activos están protegidos de manera más efectiva contra el fraude.

1.8. Facilitación de la inversión global y acceso a mercados:

La tokenización puede abrir oportunidades de inversión a nivel global, ya que los inversores de todo el mundo pueden participar en proyectos y activos sin obstáculos geográficos. Esto se vincula al desarrollo local de fuertes comunidades de usuario que se encarguen de difundir información relevante de inversiones tentativas.

1.9. Gobernanza transparente:

Algunos tokens de seguridad pueden incluir derechos de voto en decisiones relacionadas con la gestión de activos o proyectos, lo que permite a los inversores tener un papel activo en la toma de decisiones.

La variedad de instrumentos financieros digitales que se han desarrollado en el ecosistema Blockchain, en especial en el campo de las DeFi (Finanzas Descentralizadas), nos lleva a poner especial énfasis en la necesidad de monitorear, gestionar y regular los tokens de gobernanza que se vinculen a desarrollos de la Plataforma BCT NFT/FT para Santa Fe.

1.10. Diversificación de cartera:

Los inversores pueden diversificar su cartera de inversión más fácilmente al tener acceso a una variedad más amplia de activos tokenizados, lo que reduce el riesgo asociado con una sola clase de activo.

2. Servicios financieros mejorados:

El mundo financiero actual se encuentra interpelado por el impacto de las denominadas DeFi (Finanzas Descentralizadas). De hecho se ha generado el término “TradFin” para englobar a las Finanzas Tradicionales, y contrastarlas a las DeFi - Finanzas descentralizadas, que principalmente surgen de las tecnologías innovadoras que impactan diariamente en los negocios bancarios y financieros.

Dentro de este contexto, podemos analizar a una serie de factores, dentro del ámbito de instrumentos financieros que pueden enriquecerse por medio de implementación de desarrollos similares pero basados en la tecnología de Blockchain

2.1. Mayor eficiencia:

La blockchain permite la liquidación de transacciones financieras de manera más rápida y eficiente, eliminando intermediarios y simplificando los procesos de reconciliación. Esto abre la posibilidad de que los usuarios de la Plataforma BCT NFT/FT para Santa Fe puedan realizar en forma casi instantánea complejas transacciones financieras, seguras. En forma práctica la única latencia que tendrían estas operaciones es la de la red Blockchain que las soporta.

2.2. Reducción de costos:

Al eliminar intermediarios y automatizar procesos, la blockchain ayuda a reducir los costos operativos asociados con la gestión de transacciones financieras, lo que puede traducirse en tarifas más bajas para los usuarios finales. Este factor ya lo analizamos reiteradamente. Desde la óptica de las oportunidades que se abren en el desarrollo de la Plataforma BCT NFT/FT para Santa Fe, se debería considerar la oportunidad de integrar o hacer interoperables los desarrollos realizados en la Plataforma con los de algunos mercados locales significativos como el sistema de tokenización de AgroToken (desarrollado en la pcia. de Santa Fe), y el mercado de futuros de ROFEX (sito en Rosario, y con el agregado que es el primer mercado con autorización para negociar futuros de criptomonedas como Bitcoin).

2.3. Gestión de identidad descentralizada:

Una de las cuestiones más discutidas en la actualidad es la del empoderamiento de la ciudadanía por medio de la gestión de identidad soberana. Que el individuo sea dueño y pueda administrar libremente los datos referidos a su persona, gustos, actividades, comportamientos, es una cuestión fundamental para reorientar la soberanía sobre los derechos personalísimos como el del sigilo de nuestra vida privada.

Un ejemplo de esto lo podemos ver en el sistema denominado open finance (previamente conocido como open banking), desarrollado e implementado por el Banco Central de Brasil[78]. Por medio de este sistema cada usuario del sistema financiero puede habilitar a que una institución financiera diferente a la que es cliente, tenga acceso directo a los datos de su comportamiento financiero (consumos de tarjetas de crédito, ingresos, transferencias …). De esta manera, la nueva institución financiera que recibe los datos personales, puede realizar una oferta que mejore en términos competitivos la del banco en la que usuario tiene cuenta.

La iniciativa se basa, por lo tanto, en la idea directriz de “consumidor en el centro”. Los datos relacionados a mi comportamiento financiero son míos, y por lo tanto, yo puedo decidir libremente con quien compartirlos.

Los sistemas basados en Blockchain vienen desarrollando lo que se llama DID (Identidad descentralizada), permitiendo por medio de una segunda capa de encriptación proteger los datos personales, y dando oportunidad al usuario final a disponibilizar libremente los mismos.

Esto abre una oportunidad clara de empoderamiento, a la Plataforma BCT NFT/FT para Santa Fe, para incorporar como una de sus consignas, la gestión descentralizada y soberana de la identidad digital de sus usuarios. Empoderando en forma directa a los beneficiarios de uso.

2.4. Transferencias internacionales más rápidas y económicas:

Ya se analizó previamente la capacidad de la tecnología de Blockchain para poder realizar transacciones peer-to-peer, entre pares, sin la necesidad de intermediarios. Esto permite la realización de transferencias transfronterizas, prácticamente instantáneas.

El desarrollo de la Plataforma BCT NFT/FT para Santa Fe abre la oportunidad de enriquecer el acceso a portfolios variados de inversiones en activos digitales por parte de inversores externos, sin dejar de tener en cuenta el tentativo impacto en generación de liquidez para impulsar iniciativas regionales, por medio de este sistema.

[78] Open Finance - BACEN Banco Central de Brasil
https://www.bcb.gov.br/estabilidadefinanceira/openfinance
Observado octubre 2023

2.5. Mayor inclusión financiera:

La blockchain puede brindar servicios financieros a poblaciones que anteriormente no tenían acceso a sistemas bancarios tradicionales, lo que promueve la inclusión financiera global.

Dentro de esto podemos mencionar la oportunidad que se abre para poder desarrollar en la Plataforma BCT NFT/FT para Santa Fe, instrumentos financieros digitales, basados en crowdfunding, donde pequeños inversionistas atomizados, puedan colocar fondos de ahorros en iniciativas productivas locales.

Otra experiencia vinculada a oportunidades de inclusión financiera que se abre por medio la Plataforma, es la de generar sistemas de lending (prestamos) basados en Contratos Inteligentes, que direccionen fondos en favor de personas que se encuentren excluidas o tengan dificultades de acceso al sistema financiero tradicional.

3. Desarrollo de productos de arte digital por medio de NFT

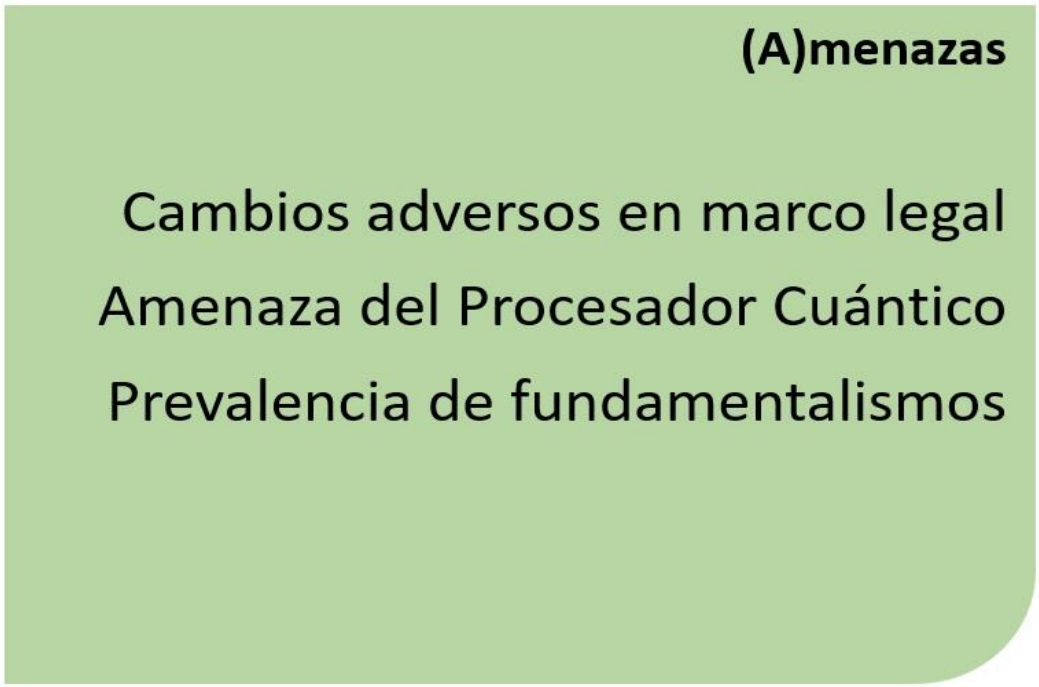
También previamente mencionamos el impacto que se está observando en la actualidad en la promoción del arte, tradicional o digital, por medio de los denominados NFT.

NFT - Tokens No Fungibles, pueden ser representados en formato digital para ser gestionados por medio de una Plataforma BCT. Por medio de la Plataforma se cuenta con la posibilidad de gestionar y negociar, activos de arte, que de otra manera, tendrían que transitar por una serie de engorrosos canales burocráticos para lograr su difusión.

Esto facilita la inclusión artística y consecuentemente financiera de los creadores de arte. Por otra parte, el fraccionamiento y atomización de valores que facilita la tokenización, promueve el acceso y disfrute de esos activos de arte, para el público en general.

Por último, y tal como se ha visto en experiencias en este campo en el mundo entero, al no poder ser los activos de arte, negociados en mercados fungibles tradicionales, sino que requieren de mercados específicos que garanticen su correcta información y difusión, la Plataforma BCT NFT/FT para Santa Fe, tiene la oportunidad de actuar como puente de generación para estos mercados o sitios de negociación específicos.

Amenazas



1. Cambios adversos en el marco legal

Como ya se ha mencionado anteriormente, Argentina no tiene todavía un marco legal claro y definido para cripto-activos como para los productos financieros digitales desarrollados sobre el ecosistema Blockchain.

Einstein a nivel mundial lo que se ha denominado el proceso de “convergencia” hacia activos digitales. Los principales países y bloques están cambiando su enfoque en lo que respecta a regulación de cripto-activos, cambiando la tendencia de prohibirlos por la de regularlos.

Sin embargo esta tendencia observada puede verse afectada por decisiones políticas según sean las circunstancias económicas y financieras del país.

2. Amenaza del Procesador Cuántico

Previamente también se analizó la cuestión vinculada a la denominada “amenaza del procesador cuántico”.

No existe un horizonte preciso, pero se estima que en un plazos cercano entre 5 a 15 años se va a poder contar con procesadores cuánticos de uso comercial, no como los experimentales que actualmente se están desarrollando. Al trabajar con partículas sub-atómicas, el procesador cuántico puede representar múltiples estados simultáneamente haciendo crecer exponencialmente el poder de cómputos de las computadoras que lo utilizan.

Como la Blockchain es una tecnología fuertemente basada en encriptación, se ve como una amenaza la posibilidad que en un futuro no muy lejano, este tipo de procesadores pueda quebrar los algoritmos que sustentan esa encriptación.

Con las computadoras actuales, la fortaleza de algoritmos de encriptación de grado militar, como los que se utilizan en la Blockchain brindan un grado de invulnerabilidad segura. Sin embargo, y en conocimiento del advenimiento de la amenaza de procesador cuántico, algunas Blockchain, como Ehtereum han comenzado a planificar la mudanza a algoritmos de encriptación pos-cuánticos, como los basados en ZKP - Pruebas de Conocimiento Cero, o los desarrollados en base a rendillas.

3. Prevalencia de fundamentalismos

La primera criptomoneda y la más vendida hasta el momento, el Bitcoin, nació bajo la idea de generar un sistema absolutamente autónomo que terminase con la intervención de terceros intermediarios como bancos o instituciones financieras.

Esa idea sigue vigente dentro de muchas comunidades de criptomonedas. Los usuarios, programadores, arquitectos, evaluadores y divulgadores de cripto-activos que mantienen la idea fundamentalista de la nula intervención o regulación, suelen negar y rechazar los desarrollos de Blockchain privadas o permisionadas, como así también cualquier regulación que se pretenda realizar sobre Cadena de Bloques.

Si bien este pensamiento no es mayoritario no puede obviarse su posible impacto negativo al intentar realizar la difusión del desarrollo de la Plataforma BCT NFT /FT para Santa Fe.

Conclusiones finales, factibilidad y rumbos futuros

Conclusiones de tipos generales sobre la propuesta Plataforma BCT NFT/FT Santa Fe

Hemos podido analizar a lo largo de todo este trabajo el impacto disruptivo que la tecnología de Blockchain está provocando transversalmente en casi todas las ramas de diferentes actividades económicas. Nuestro foco, en este amplio espectro fue puesto con especial énfasis en el campo de las DeFi - Finanzas Descentralizadas, término acuñado para identificar a las actividades bancarias y financieras basadas en la tecnología BCT.

Pudimos analizar los fundamentos de la tecnología, para comprender con mucha mayor claridad sus potencialidades. Realizamos también un análisis del marco legal argentino e internacional, para comprender con claridad las deudas que la regulación de cripto-activos presenta en nuestro país. Estudiamos los problemas e inconvenientes de la gravabilidad impositiva sobre desarrollos basados en Blockchain, en especial los aspectos vinculados a la territorialidad de sus actividades, realizando también un relevamiento de los principales productos financieros digitales que existen en el ecosistema Blockchain. Se detallaron soluciones de plataforma que existen en el mercado como opciones que permitan la implementación de la Plataforma BCT NFT/FT para Santa Fe. Luego de esto, y entrando ya en el plano metodológico, pusimos foco en los aspectos vinculados a la gestión del proyecto que brinde sustento a la Plataforma. Por último hicimos un análisis crítico sobre ventajas, desventajas, fortalezas, debilidades, oportunidades y amenazas de la iniciativa basándonos en la metodología de análisis FODA.

Entre las conclusiones más relevantes a la propuesta de desarrollo de la Plataforma podemos mencionar:

- ✓ La propuesta de desarrollo de una Plataforma Blockchain de tokens NFT/FT presenta una oportunidad clara de inserción de la provincia de Santa Fe dentro del ámbito de la que muchos autores consideran la tecnología más innovadora y disruptiva de la actualidad,
- ✓ La propuesta puede actuar como un impulso para liberar a las fuerzas productivas en la industria del conocimiento, en tanto convoca a profesionales de negocio con amplios conocimientos en instrumentos y mercados financieros innovadores, programadores capacitados en lenguajes de programación de última generación, arquitectos de sistemas, y expertos en redes.
- ✓ Vinculado con el punto anterior, la propuesta de desarrollo de la Plataforma, se espera que empuje a que jueguen un rol preponderante en el aspecto de conocimientos necesarios, las universidades, consejos profesionales, organizaciones intermedias y el resto de las entidades civiles vinculadas.
- ✓ No debemos descartar, como ha ocurrido en desarrollos semejantes a nivel mundial, la incorporación por los actores vinculados o beneficiados por el proyecto, de otras tecnologías lindantes a la de Blockchain, tales como ciencia de datos, analitica predictiva, aprendizaje de maquina. En este caso la iniciativa puede actuar como un apalancamiento de la incorporación en el medio local de estas tecnologías.

- ✓ Es de esperar que la generación de un ecosistema Blockchain de productos financieros digitales, redundará en un empoderamiento ciudadano, propio de las tecnologías descentralizadas, en las cuales la participación de terceros intermediarios de confianza se ve reducida en términos de preponderancia
- ✓ El proyecto propuesto se espera, también en función de lo observado en experiencias de desarrollos internacionales, que aliente a la inclusión financiera, permitiendo el acceso de la ciudadanía excluida por sistemas de finanzas tradicionales a productos financieros digitales que permitan la financiación y sustento de emprendimientos locales.
- ✓ En particular, y como ya se mencionó previamente, el dominio de NFTs - Tokens No Fungibles, se ha volcado a nivel mundial al desarrollo de instrumentos digitales que permiten divulgar y comercializar en forma innovadora activos de arte y productos culturales. Es esperable por esto, que la Plataforma actúe como un impulsor para este tipo de aspecto social, redundando en un beneficio multiplicador en la comunidad.
- ✓ Un factor que no podemos obviar en considerar, es el de la sustentabilidad de la propuesta. Como desarrollamos previamente, la Blockchain más avanzada tecnológicamente en la actualidad, y que actúa como impulsor de la mayoría de las que existen en mercado, la Blockchain Ethereum, ha cambiado recientemente su protocolo de consenso, pasando del tradicional POW - Prueba de Trabajo al de POS - Prueba de Participación. El ahorro energético entre uno y el otro se estimó en superior al 97%, por lo que el problema típico del consumo eléctrico alocado que conllevan Cadenas de Bloques como Bitcoin, se está corrigiendo actualmente y deja una perspectiva clara de sustentabilidad para la Plataforma que estamos estudiando.

Aspectos controversiales a tomar en cuenta en la factibilidad y conveniencia de gravar o eximir de tributos a NFT/FT y demás tokens criptográficos de la provincia de Santa Fe

En el apartado “Impuesto sobre los Ingresos Brutos y normativas provinciales” realizamos un estudio comparativo de los diferentes enfoques normativos y consiguientes imposiciones de gravabilidad / exención sobre cripto-activos que se han definido hasta la actualidad en provincias argentinas.

Los aspectos más relevantes de las definiciones observadas en los respectivos códigos fiscales fueron:

Córdoba: Se alcanzan por el impuesto 1. Prestación de servicios vinculados con operatorias relacionadas con monedas digitales; 2. Venta de monedas digitales y su base imponible diferencial; y 3. Los ingresos derivados por la venta de moneda digital cuando éstas provengan del canje por la comercialización de bienes y/o servicios

Catamarca: En la provincia de Catamarca, además de ser alcanzado por ingresos Brutos, los contratos vinculados al comercio de activos digitales, se deberá tributar impuesto de sellos.

Entre Ríos: La base imponible estará constituida por la diferencia entre los precios de compra y venta, en los siguientes casos:… f) En las operaciones de enajenación de acciones, … , monedas digitales, ….

La Pampa: Estarán alcanzadas por el impuesto "*l) La prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente con operatorias relacionadas con monedas digitales (monedas virtuales, criptomonedas, criptoactivos, tokens, stablecoins y demás conceptos que por su naturaleza y/o características constituyan y/o impliquen una representación digital de valor que puede ser objeto susceptible de comercio)*."

La Rioja: "*g) La prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente con operatorias relacionadas con monedas digitales*".

Neuquén: "*o) La prestación de servicios de cualquier naturaleza, vinculados directa o indirectamente con operatorias relacionadas con monedas digitales."*

Tucumán: *"La base imponible estará constituida por diferencia entre los precios de compra y de venta en los siguientes casos:… 3. Operaciones de compra y venta de divisas y títulos públicos. Quedan comprendidos en el presente inciso las operaciones de compra y venta de monedas digitales."*

Del relevamiento de las normativas provinciales se puede concluir que se pueden observar situaciones dispares, como casos en los cuales simplemente se han ocupado de gravar a los criptoactivos por impuestos (Ingresos Brutos), sin dedicarse a conceptualizar a los mismos, y otros casos donde la normativa provincial es más amplia, organizada y puntual.

Si comparamos estos marcos normativos de gobiernos subnacionales con la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de cripto-activos – COM(2020) 593 Final (que desarrollamos en el apartado "Reglamento del Parlamento Europeo – Criptoactivos"), podemos observar una clara diferenciación entre un conjunto normativo maduro, de amplio alcance, y minuciosamente descriptivo de derechos, obligaciones y situaciones de regulación, con respecto a enunciaciones puntuales que simplemente buscan incluir a criptomonedas en el alcance del impuesto a los ingresos brutos, probablemente guiadas por la voracidad fiscal.

Es de esperar que en el corto plazo se desarrolle una normativa robusta, a nivel nacional, que englobe todos los aspectos dinámicos del denominado "mundo cripto", y que sirva de marco de referencia y armonización para las normativas impositivas provinciales. Sin perjuicio de esta deuda legal pendiente, podemos considerar algunos aspectos controversiales, que ya enumeramos en los apartados "Territorialidad" y "El anonimato en la Blockchain" y que los encargados de gestionar el proyecto de desarrollo de la Plataforma BCT NFT/FT para la Provincia de Santa Fe, deberán considerar.

Anonimato y territorialidad:

Como ya se mencionó y desarrolló en el presente trabajo, existen dos grandes grupos de Blockchain: las no permisionadas (o públicas) y las permisionadas (o privadas), esto en función a si los actores de estas pueden comenzar a operar directamente, o necesitan identificarse para conseguir "permiso" para poder hacerlo. También mencionamos a las Blockchain de consorcio e híbridas, pero en función del punto que estamos desarrollando, vamos a obviarlas por considerarlas como una variante de las Blockchain permisionadas.

Este es un factor básico para tomar en consideración si se piensa gravar o eximir de impuesto a los desarrollos que se realicen sobre la Plataforma BCT NFT/FT para la provincia de Santa Fe, ya que al identificarse el actor que va a actuar, podremos aplicar los supuestos de principios impositivos rectores como el de "sujeto alcanzado", o "territorialidad" que definirá el alcance de la exención o gravamen del hecho económico.

Visto desde este enfoque, la decisión más coherente sería la de adoptar el supuesto de una Blockchain permisionada, tanto para alcanzar con el impuesto a las operaciones identificables del contribuyente, como para brindarles exenciones. Sin embargo se deberá considerar que culturalmente existe una gran aprehensión al uso Blockchain permisionadas por parte de quienes comparten la filosofía de redes descentralizadas autogobernadas, como originalmente fueron las primeras criptomonedas (que siguen en la actualidad liderando mercado).

Otros aspectos controversiales a analizar

Otras cuestiones que deberán considerarse al momento de definir los supuestos de gravabilidad o exención de cripto-activos desarrollados por medio de la Plataforma BCT NFT/FT de la Provincia de Santa Fe son:

- ✓ conveniencia y grado de intervención y regulación estatal, en el ecosistema Blockchain, en función de las decisiones políticas vinculadas.
- ✓ alcance de gravabilidad de cripto-activos, en el caso que se desee, para la provincia de Santa Fe. Se deberá considerar el hecho imponible en Ingresos Brutos (servicios vinculados a cripto-activos, operaciones con criptomonedas. etc…), y si es procedente gravar también con Impuesto de Sellos, a las operaciones / contratos respaldados o vinculados a criptomonedas.
- ✓ definir los puntos críticos de análisis vinculados a la identidad de los actores de la Plataforma NFT/FT, como así también de actores externos a la misma, pero que se vinculen con operaciones de cripto-activos.
- ✓ definiciones vinculadas al tipo de Blockchain a utilizar, y su alcance.
- ✓ analizar las variantes que impactan en el ecosistema, tales como las técnicas mixer y ZKP, sus tendencias y probable impacto. En especial con relación a la posibilidad de quebrar trazabilidad de transacciones y maniobras fraudulentas o de lavado de dinero que se desprendan de esto.

Rumbos futuros

Hemos mencionado y destacado el efecto multiplicador que genera la incorporación al medio de determinadas tecnologías innovadoras y disruptivas como es la de Cadena de Bloques.

Dentro de este contexto, es preponderante la elección de la Cadena de Bloques sobre la cual desarrollar la Plataforma BCT NFT/FT para Santa Fe.

Se analizaron las diferentes opciones prevalecientes en mercado, relevando las diferentes opciones de posibilidades categorizadas por Blockchain públicas, privadas, de consorcio, híbridas. De este análisis se desprende que la Blockchain que viene aunando los desarrollos más innovadores desde el punto de vista tecnológico es Ethereum.

Algoritmos de encriptación pos-cuánticos

De hecho, hemos visto que dentro del plan constante de actualización de la red, Ethereum, ya está considerando la migración de sus algoritmos de encriptación, a algoritmos pos-cuánticos, es decir, que soporten la amenaza del procesador cuántico.

Si bien este no es un factor determinante actual, no puede ser soslayado, ya que su impacto sobre la tecnología de Blockchain pasaría en los próximos años a ser crucial.

Desde el punto de vista de la Plataforma que estamos analizando, contar con un aseguramiento de invulnerabilidad sobre la misma, es un factor constituyente. La pérdida de confianza de los usuarios y de la comunidad que la sustente, puede tener un efecto devastador para la Plataforma, por lo que un alineamiento y seguimiento de la evolución del desarrollo de la computación cuántica pasa a ser un factor esencial.

Escalabilidad

También en el ámbito de análisis de la eficiencia de la red, Ethereum, viene impulsando a nivel mundial, el desarrollo de los denominados Roll-ups. Sistemas que validan en bloque grandes cantidades de transacciones fuera de la Blockchain (off-chain), pero que generan una ZKP - Prueba de Conocimiento Cero, que permite verificar, también en bloques, todas las transacciones, al ser incorporadas a la red.

Esto permite que la red aumente su eficiencia, sin perder su grado de invulnerabilidad. Según manifestó Vitalik Buterin, el objetivo de este cambio es llegar a poder validar 300.000 transacciones por segundo, logrando llevar la Blockchain Ethereum a un nivel competitivo con, por ejemplo, los sistemas de tradicionales de tarjetas de crédito como Visa o American Express.

Al ser la eficiencia de la red y su capacidad de sobrellevar congestionamientos, un factor preponderante en su adopción, la Plataforma BCT NFT/FT debería realizar un monitoreo constante de su eficiencia, y alinear a las mejoras constantes que tecnológicamente se proponen dentro de la comunidad Blockchain

Desarrollo de un ecosistema blockchain público

Es innegable el efecto multiplicador que la tecnología Blockchain viene desencadenando. Por lo que no deberíamos perder de vista, que a la adopción primera de la misma por parte de la Plataforma BCT NFT/FT para Santa Fe, sigan otros desarrollos similares en el ámbito gubernamental. Algunos de los que se puede pensar apalanquen desde la Plataforma, pueden ser:

- ✓ Sistema Blockchain, con Contratos Inteligentes, que permita gestionar licitaciones y compras directas del gobierno provincial, como así también que la ciudadanía acceda a trazabilidad de la información correspondiente. Factor esencial para el mejoramiento de la transparencia en la gestión pública.
- ✓ Sistema Blockchain para la gestión de registro médicos, especialmente basado en la confidencialidad de los datos personales que deben permanecer encriptados, para que quien detente la identidad soberana de los mismos, pueda consultar o compartir.
- ✓ Sistemas de pagos, proveedores de servicios de pagos, o billeteras digitales, descentralizados y gobernados por Contratos Inteligentes, los cuales enriquezcan a los sistemas TradFin actuales, centralizados.