

“Beneficios de La cadena de bloques o blockchain aplicada a la administración tributaria de la provincia de Santa Fe”

Fundación para los Estudios Internacionales
Mendoza 444 - Rosario, Santa Fe - C.P. 2000

PROVINCIA DE SANTA FE
CONSEJO FEDERAL DE INVERSIONES
“BENEFICIOS DE LA CADENA DE BLOQUES O
BLOCKCHAIN APLICADA A LA ADMINISTRACIÓN
TRIBUTARIA DE LA PROVINCIA DE SANTA FE”
NOVIEMBRE 2021

Autor: “Fundación para los Estudios Internacionales”

Responsable: Pablo Manuel Rossi

Colaborador 1º: Daniel da Silva

Colaborador 2º: Luciano Areste

Colaborador 3º: Juan Guidi

Asistente: Guillermo Mionnet

“Beneficios de La cadena de bloques o blockchain aplicada a la administración tributaria de la provincia de Santa Fe”

Fundación para los Estudios Internacionales
Mendoza 444 - Rosario, Santa Fe - C.P. 2000

ÍNDICE

PRÓLOGO.....	Página 2
CAPÍTULO I: Introducción.....	Página 4
CAPÍTULO II: Casos de Estudio.....	Página 47
CAPÍTULO III: Implementación de tecnología blockchain.....	Página 83
CAPÍTULO IV: Capacitaciones en tecnología blockchain.....	Página 120
CAPÍTULO V: Proyecto BlockchainLAB Santa Fe.....	Página 134
CAPÍTULO VI: Conclusiones finales.....	Página 140
BIBLIOGRAFÍA.....	Página 142

PRÓLOGO

Desde el 2009, año de la creación de Bitcoin y la tecnología detrás de la criptomoneda, la Blockchain, el interés por esta innovación no ha dejado de crecer. Prácticamente todos hemos escuchado hablar acerca de Bitcoin, pero sobre Blockchains o cadenas de bloque el conocimiento, en general, es menor y esta menos difundido. La poca asociación de aplicabilidad a una actividad particular y/o su alto grado de abstracción producen ciertos prejuicios hacía esta herramienta, no tan nueva, como lo fue con internet a principios de los 90s. Pero lo cierto es que estas características (estéticas) hacen a la tecnología blockchain fundamentales para entender el futuro tanto del sector público como el sector privado a nivel mundial.

Si pensamos en el sector público, cada vez más los gobiernos se enfrentan a una encrucijada en donde necesitan entregar servicios públicos, en calidad y cantidad, de manera eficiente y transparente, y a menudo con menos recursos disponibles. Ante esta coyuntura, es esperable que la solución pueda venir de la mano de la aplicación de nuevas tecnologías. Después de todo, las administraciones gubernamentales son muchas veces uno de los últimos refugios del trámite basado en papel, los procesos manuales y los sellos. Si bien es cierto que el uso de nuevas tecnologías puede hacer a las administraciones más eficientes y efectivas, estas no dejan de ser herramientas que deben usarse conociendo muy bien sus potencialidades y limitaciones, y cuya aplicación debe darse siempre acompañada y supeditada a programas de reforma progresiva.

Las potencialidades de la tecnología blockchain extrapolan el universo de las criptomonedas. Varias aplicaciones fueron creadas, están en desarrollo o son evaluadas, incluyendo en el área gubernamental, tales como el registro de bienes y tierras, identidad ciudadana, cadenas de suministro y tributación. Las características centrales de la tecnología Blockchain significan que tiene un potencial significativo para su uso en impuestos:

- Transparencia: blockchain proporciona procedencia, trazabilidad y transparencia de las transacciones.
- Control: el acceso a redes autorizadas está restringido a usuarios identificados
- Seguridad: el libro de contabilidad digital no se puede alterar ni alterar una vez que se ingresan los datos. El fraude es prácticamente imposible y fácilmente detectable
- Información en tiempo real: cuando la información se actualiza, se actualiza para todos en la red en el mismo tiempo.

Estas tecnologías tienden a facilitar la formación de un ecosistema que involucra tanto al gobierno, las empresas, los consumidores, universidades y

diferentes cámaras generando confianza y transparencia entre los participantes. Por ello, el propósito del presente informe es conocer los beneficios potenciales de la aplicación de la tecnología blockchain a la administración tributaria de la provincia de Santa Fe. Al mismo tiempo, ir sentando las bases para desarrollar un ecosistema en donde la aplicación de la tecnología sea transversal al sector público y que involucre a los contribuyentes y el sector privado en general, a través de programas de capacitación en la materia de estudio.

Capítulo I: “INTRODUCCIÓN”

Como creemos que tener ciertos conocimientos básicos acerca de la tecnología resulta sumamente necesario, en esta etapa introductoria, elaboraremos un documento en donde resumiremos y explicaremos de manera sencilla los conceptos básicos a adquirir para ir adentrándose en el entendimiento de las cadenas de bloques. Una vez explicados los conceptos básicos necesarios para entender el funcionamiento de la blockchain, pasaremos a relevar los casos de aplicación a nivel nacional e internacional de la tecnología en el sector público que tengan relación a posibles casos de usos por parte de la provincia de Santa Fe.

1.1. Blockchain o Cadena de Bloques

Las cadenas de bloques o blockchain son registros digitales. En su nivel básico, permiten que una comunidad de usuarios registre transacciones en un libro mayor compartido dentro de esa comunidad, de modo que bajo el funcionamiento normal de la red blockchain no se puede cambiar ninguna transacción una vez publicada. En 2008, la idea de la cadena de bloques se combinó con varias otras tecnologías y conceptos informáticos para crear Criptomonedas: dinero electrónico protegido a través de mecanismos criptográficos en lugar de un repositorio o autoridad central.

Esta tecnología se hizo ampliamente conocida en 2009 con el lanzamiento de Bitcoin, la primera de muchas criptomonedas modernas. En Bitcoin y sistemas similares, la transferencia de datos digitales, la información que representa el dinero electrónico tiene lugar en un sistema distribuido. Los usuarios de Bitcoin pueden firmar digitalmente y transferir sus derechos sobre esa información a otro usuario y la Bitcoin blockchain registra esta transferencia públicamente, lo que permite a todos los participantes de la red verificar de forma independiente la validez de las transacciones. La cadena de bloques de Bitcoin es independiente, mantenido y administrado por un grupo distribuido de participantes. Esto, junto con los mecanismos criptográficos hace que la cadena de bloques sea resistente a los intentos de alterar el libro mayor más tarde (modificando bloques o falsificación de

transacciones). La tecnología blockchain ha permitido el desarrollo de muchos sistemas de criptomonedas como Bitcoin y Ethereum. Debido a esto, la tecnología blockchain a menudo se considera vinculado a Bitcoin o posiblemente a soluciones de criptomonedas en general. Sin embargo, la tecnología está disponible para una variedad más amplia de aplicaciones y está siendo investigada y aplicada por una variedad de sectores.

Los numerosos componentes de la tecnología blockchain junto con su dependencia de la criptografía hacen que los sistemas primitivos puedan dificultar su comprensión. Sin embargo, cada componente se puede describir de manera simple y se puede usar como un bloque de construcción para comprender el sistema complejo. Las cadenas de bloques se pueden definir informalmente como:

Las cadenas de bloques son libros de contabilidad digitales distribuidos de transacciones firmadas criptográficamente que se agrupan en bloques. Cada bloque está criptográficamente vinculado al anterior (lo que lo hace evidente) después de la validación y se somete a una decisión consensuada. A medida que se agregan nuevos bloques, los bloques más antiguos se vuelven más difíciles de modificar (creando resistencia a la manipulación). Los nuevos bloques se replican en copias del libro mayor dentro de la red, y cualquier conflicto se resuelve automáticamente utilizando reglas establecidas.

A grandes rasgos, blockchain se puede pensar como un libro contable, una bitácora o una base de datos donde solo se puede ingresar entradas nuevas y donde todas las existentes no se pueden modificar ni eliminar. Esas entradas, llamadas transacciones, se agrupan en bloques que se van agregando, sucesivamente, al registro en forma de cadena secuencial, cada uno de ellos relacionado necesariamente con el anterior. En ese esquema, si quisiéramos corregir información ya registrada, solo lo podemos hacer mediante el agregado de nueva información. Los datos originales siempre van a permanecer y pueden ser fiscalizados en cualquier momento.

1.2. Un poco de historia

Las ideas centrales detrás de la tecnología blockchain surgieron a fines de la década de 1980 y principios de la de 1990. En 1989, Leslie Lamport desarrolló el protocolo Paxos y en 1990 presentó el documento The Part Time Parliament a ACM TransactionsonComputerSystems. El documento describe un modelo de consenso para llegar a un acuerdo sobre un resultado en una red de computadoras donde las computadoras o la red en sí pueden no ser confiables. En 1991, se utilizó una cadena de información firmada como libro de contabilidad electrónico para firmar documentos digitalmente de una manera que pudiera mostrar fácilmente que

ninguno de los documentos firmados en la colección había sido modificado. Estos conceptos se combinaron y aplicaron al efectivo electrónico en 2008 y se describen en el documento Bitcoin: A Peer to Peer Electronic Cash System, que Satoshi Nakamoto publicó bajo seudónimo, y luego en 2009 con el establecimiento de la criptomoneda Bitcoin. El artículo de Nakamoto contenía el modelo que siguen la mayoría de los esquemas de criptomonedas modernos (aunque con variaciones y modificaciones). Bitcoin fue solo la primera de muchas aplicaciones de blockchain.

Muchos esquemas de efectivo electrónico existían antes de Bitcoin (por ejemplo, eCash y NetCash), pero ninguno de ellos logró un uso generalizado. El uso de una cadena de bloques permitió que Bitcoin se implementara de manera distribuida, de modo que ningún usuario individual controlara el efectivo electrónico y no existiera un único punto que pudiera manejar toda la red; esto promovió su uso. Su principal beneficio era permitir transacciones directas entre usuarios sin la necesidad de un tercero de confianza. También habilitó la emisión de nuevas criptomonedas de manera definida a aquellos usuarios que logren publicar nuevos bloques y mantener copias del libro mayor; estos usuarios se denominan mineros en Bitcoin. El pago automatizado de los mineros permitió la administración distribuida del sistema sin necesidad de organizarse. Mediante el uso de una cadena de bloques y el mantenimiento basado en el consenso, se creó un mecanismo de autocontrol que aseguró que solo se agregaran transacciones y bloques válidos a la cadena de bloques.

En Bitcoin, la cadena de bloques permitió a los usuarios usar seudónimos. Esto significa que los usuarios son anónimos, pero los identificadores de sus cuentas no lo son; además, todas las transacciones son visibles públicamente. Esto ha permitido efectivamente que Bitcoin ofrezca pseudo-anonimato porque las cuentas se pueden crear sin ningún proceso de identificación o autorización. Dado que Bitcoin era seudónimo, era fundamental contar con mecanismos para generar confianza en un entorno en el que los usuarios no podían identificarse fácilmente. Antes del uso de la tecnología blockchain, este fideicomiso generalmente se entregaba a través de intermediarios en los que confiaban ambas partes. Sin intermediarios de confianza, la confianza necesaria dentro de una red de cadenas de bloques está habilitada por cuatro características clave de la tecnología blockchain, que se describen a continuación:

Libro mayor: la tecnología utiliza un libro mayor solo para agregar para proporcionar un historial transaccional completo. A diferencia de las bases de datos tradicionales, las transacciones y los valores en una cadena de bloques no se anulan.

Seguro: las cadenas de bloques son criptográficamente seguras, lo que garantiza que los datos contenidos en el libro mayor no hayan sido manipulados y que los datos dentro del libro mayor sean comprobables.

Compartido: el libro mayor se comparte entre varios participantes. Esto proporciona transparencia entre los participantes del nodo en la red blockchain.

Distribuida: la cadena de bloques se puede distribuir. Esto permite escalar el número de nodos de una red de cadena de bloques para que sea más resistente a los ataques. Al aumentar el número de nodos, la capacidad de un actor para sacar beneficio propio se reduce ya que necesita más poder para corromper la red

Para las redes de blockchain que permiten que cualquier persona cree cuentas y participe de forma anónima (llamadas redes de cadena de bloques sin permiso), estas capacidades brindan un nivel de confianza entre las partes sin conocimiento previo entre sí; esta confianza puede permitir que las personas y las organizaciones realicen transacciones directamente, lo que puede dar como resultado que las transacciones se entreguen más rápido y a costos más bajos. Para una red de cadena de bloques que controla más estrictamente el acceso (llamadas redes de cadena de bloques autorizadas), donde puede haber cierta confianza entre los usuarios, estas capacidades ayudan a reforzar esa confianza.

Hacer una transferencia, pagar con billeteras digitales, Bitcoin, Ethereum y las finanzas descentralizadas, todo esto nos parece cada día más cotidiano, pero realmente sabemos cómo llegamos a este punto. Para entender las criptomonedas o el ecosistema cripto es importante entender el desarrollo del dinero a lo largo de la historia. Si nos ponemos a pensar en perspectiva, ¿la moneda tiene la misma función social que hace más de 5000 años atrás? Aunque la respuesta a esta pregunta es compleja y nos puede parecer a simple vista que no tiene la misma función, el dinero a lo largo de la historia no ha cambiado mucho. Pero arrancamos primero por definir a la moneda y que funciones cumple.

El dinero es todo bien o activo, digital o no, por los agentes económicos para sus intercambios o el comercio. Con esta definición ya tenemos una de las funciones del dinero que el medio de cambio generalmente aceptado. De esta manera solucionamos uno de los principales inconvenientes del trueque. Otra de las funciones del dinero es la unidad de cuenta, debido a que el valor de un bien es utilizado para medir y comparar el valor de otros bienes; y para documentar deudas. La última de las funciones del dinero es la que sirve como reserva de valor, esto nos permite la conservación de riqueza a lo largo del tiempo.

Partiendo de las funciones del dinero podemos entender como fue evolucionando el dinero o la moneda a lo largo de la historia. En la Antigüedad,

como casi toda explicación a los fenómenos que rodeaban y atravesaban a las sociedades, se creía que la escritura y el número provenía de los dioses. Los griegos creían que Prometeo, después de engañar a los dioses y darles el fuego a los mortales, les enseñó la escritura y el número entre otras cosas. En la cultura Sumeria, la diosa Inanna se la había robado a Enki, el dios de la sabiduría. Con el paso del tiempo se dejó de creer que el número y la escritura provenían de los dioses. Fue en esta última cultura, la Sumeria, donde se encontraron las primeras tablas para registrar operaciones de intercambios de bienes, precisamente en los templos de Uruk en el 3.500 AC. No es el objeto de este artículo profundizar sobre las tablas de Uruk pero los sumerios habían desarrollado formas de contratos para diferir pagos en el tiempo. El trueque, que siguió predominando por muchos años más, era la forma de realizar intercambios, pero, como mencionamos anteriormente, presentaba grandes ineficiencias ya que no hay un bien generalmente aceptado ni una unidad de cuenta para cuantificar el valor.

Un salto tecnológico en la evolución del dinero fue la utilización de determinados productos como las semillas, el ganado, especias, etc. para facilitar los intercambios. La utilización de un bien como medio de cambio se conoce como dinero mercancía.

En un contexto donde las sociedades crecían rápidamente, estas se encontraron con la problemática del comercio entre las distintas ciudades dentro de sus fronteras. Por lo que era necesario encontrar un bien de referencia que fuera fácilmente transportable, duradero, divisible y con un valor establecido: los metales preciosos, en particular el oro, se convirtieron en ese valor de referencia. Ya los griegos en las ciudades portuarias como Pireo, comenzaron a sembrar las bases de las actividades bancarias. Los trapezitai daban préstamos y tomaban depósitos en mercancías, siguiendo los principios de la Mesopotamia crearon la idea de valor monetario unificado como activo, commodities, servicio, etc.

Más adelante en el tiempo, las monedas de metales preciosos fueron cambiando y estas fueron hechas con metales menos nobles y más livianos para facilitar su transporte y guarda, pero siempre respaldadas por metales preciosos para conservar su valor. Bueno no siempre. Ya en la última etapa del imperio romano, la moneda era cada vez más devaluada con metales menos nobles y entregada a los ciudadanos a cambio de bienes y servicios produciendo la suba de precios de estos últimos. O el caso del Gran Gengis Kan, que creó uno de los imperios más grande del mundo, precursor de lo que hoy conocemos como papel moneda. Gengis Kan y sus altos funcionarios solían realizar grandes emisiones de dinero para financiar guerras de conquistas. Posteriormente, la economía sufrió una

de las primeras inflaciones en la historia mundial y el imperio se fragmentó; y el dinero papel desapareció de la faz de la tierra por unos cuantos siglos. Esto nos pone en una de las cuestiones fundamentales de Bitcoin y las criptomonedas, la cuestión de la confianza y como saber que la moneda que estoy utilizando está respaldada y/o será aceptada por el resto.

Una de las características que se mantiene desde esa época, fue impuesta por los Romanos, es que la emisión de dinero estaba en mano del estado garantizando el valor de las mismas. A partir del siglo XIX, se institucionaliza a través del patrón oro donde el dinero papel-moneda está respaldado por oro depositado en bancos centrales. Básicamente, el valor del dinero viene dado por el valor intrínseco que tiene el metal precioso. El patrón oro comenzó a abandonarse hace casi un siglo. Desde su final, el valor de una determinada moneda se establece por la confianza que genera. Es lo que se conoce como Dinero Fiduciario: las monedas y billetes fiduciarios no basan su valor en la existencia de una contrapartida en oro, plata o cualquier otro metal noble o valores, ni en su valor intrínseco, sino simplemente en su declaración como dinero por el Estado y también en el crédito y la confianza (la fe en su futura aceptación) que inspira. Sin esta declaración, la moneda no tendría ningún valor. Es importante que los últimos años, a nuestro entender, esta confianza es cada vez menor debido al comportamiento irresponsable de los principales bancos centrales y las restricciones y control por parte de los mismos.

Antes de llegar a bitcoin es importante destacar que, en los últimos años, en conjunto con la digitalización de la sociedad, han irrumpido con fuerza diversos medios de pagos electrónicos. Este tipo de dinero puede utilizarse para el pago de bienes y servicios a través de internet o de otros medios electrónicos.

... Y llegamos a Bitcoin

Desde el 2009, año de la creación de Bitcoin y su tecnología detrás de la criptomoneda, la Blockchain, el interés por esta tecnología no ha dejado de crecer. Una blockchain no es otra cosa que una base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente. Expresado de forma más breve, es una base de datos descentralizada que no puede ser alterada. Acá tenemos una de las cuestiones fundamentales de las criptomonedas que es el consenso. El valor viene determinado por el consenso al que llega la red, no hay una autoridad centralizada que se encarga de garantizar el valor mismo. Este consenso que anteriormente se lograba con una autoridad centralizada significaba altos costos de transacción para los participantes y por ende termina siendo

exclusiva. Costos de transacción más bajos significa que mayor cantidad de gente participa. Esto puede sonar bastante abstracto a simple vista. Las finanzas tradicionales y las nuevas finanzas descentralizadas lo son también. Pero detrás de esto se encuentra un mundo de posibilidades como por ejemplo comprar una milésima parte de un activo o de realizar pagos y cobros transfronterizos a muy bajos costos; o la posibilidad de dolarizar a través de criptomonedas

Bitcoin, Ethereum, etc son solo la punta del iceberg de lo que esta tecnología puede llegar a ser. El cambio que vemos en las finanzas es realmente revolucionario obligando a grandes y tradicionales jugadores adaptándose para ofrecer estos servicios a sus clientes, ya sea como medios de pagos, como inversión, como tecnología para el seguimiento de la trazabilidad de un producto o servicio, etc. Para tomar dimensión de lo que mencionamos, en los próximos meses el PBoC lanzará el Yuan digital; y varios bancos centrales tienen en carpeta el lanzamiento de monedas digitales en los próximos años. Ahora la cuestión a dilucidar es la aceptación de estas últimas ya que el valor de la misma estará determinado por los bancos centrales y no la funcionalidad lograda por la blockchain.

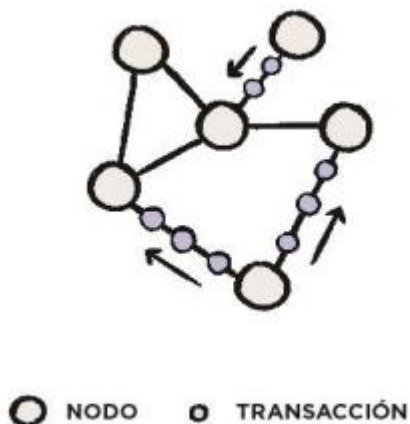
1.3. Funcionamiento de las cadenas de bloques.

El proceso mediante el cual se genera información y se publican nuevos bloques válidos puede describirse en los siguientes 6 pasos. Es conveniente aclarar primero que el significado de la palabra transacción, en este contexto, engloba cualquier tipo de intercambio de información susceptible de ser contenida en un bloque. A saber, información sobre una transacción económica, sobre un contrato inteligente, sobre un cambio en los permisos de un usuario en caso de que la red permita tal posibilidad y un largo etcétera. En general, cualquier información que tenga que ver con la cadena de bloques, ya sea relativa a sus participantes o a la información que comparten entre ellos, queda registrada en un bloque del blockchain en forma de transacción.

Paso 0. Cualquier persona o colectivo de personas que quieran ser parte de la red tienen dos opciones en función del tipo de blockchain que se esté utilizando; descargarse la aplicación correspondiente que les convierte en un nodo con los mismos derechos que todos los demás o acceder vía una interfaz web que los nodos administradores hayan provisto para el resto de usuarios autorizados. La primera opción es generalmente la correspondiente a redes públicas, donde todo aquel que lo desee puede participar; solamente tiene que descargar el software correspondiente y este, de forma automática, se conectará con un número determinado de nodos y les preguntará por la copia más actualizada de la cadena. La opción alternativa corresponde a blockchains federados o privados. En estas

cadena de bloques habrá unos nodos privilegiados administrando la cadena y decidiendo cómo el “usuario promedio” accede a través de una interfaz web que ellos proveerán.

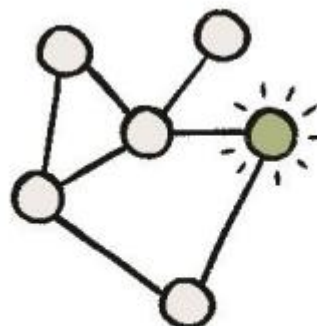
Paso 1. Una vez los participantes están conectados a la cadena, el primer paso consiste en enviar información en forma de transacciones que finalmente acabarán constituyendo los bloques de la misma. Es decir, cuando un nodo quiere realizar una transacción -ya sea una operación económica, un Smart Contract, etc-, le envía la información sobre esa transacción a los nodos con los que está conectado. Un primer protocolo actúa aquí de forma que automáticamente cada nodo



comprueba que las transacciones que “escucha” sean válidas -por ejemplo, que no se esté intentando transferir un dinero que ya haya sido gastado-. En caso de que la transacción sea correcta, cada nodo la añade a su lista de transacciones - que en lo sucesivo llamaremos por su nombre habitual en este contexto: pool- y la reenvía a los nodos a los que cada uno de ellos está conectado. El proceso continúa, pero no por siempre ya que, cuando a un nodo le llega información sobre una transacción que ya tiene en su lista o pool, simplemente la ignora.

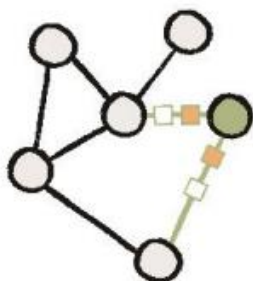
Paso 2. Cada nodo va llenando su lista o pool con las transacciones que va escuchando. En general, los pools de dos nodos diferentes no tienen por qué coincidir puesto que lo normal es que escuchan las transacciones en distinto orden.

Paso 3. En cada ronda -que dependiendo del blockchain tiene lugar tras un tiempo que puede variar, en promedio, desde unos pocos segundos hasta varios minutos-, un nodo es escogido aleatoriamente para proponer un bloque. Este proceso es el más importante, siendo el que hace que blockchain sea un registro en el que los distintos no tienen por qué confiar unas en otros. La forma en la que el nodo es escogido aleatoriamente se conoce como protocolo de consenso. La manera en la que el nodo elegido propone el bloque es tomando la versión actual de la cadena, añadiéndole al final un bloque que contenga las transacciones que había ido registrando en su pool y enviando esta nueva copia de la cadena a los nodos con los que está conectado, que a su vez la replicarán al resto de la red al igual que hacían con las transacciones individuales. Los bloques tienen un tamaño máximo que depende del blockchain, por lo que han de llenarse con un número limitado de transacciones.



○ NODO ● NODO SELECCIONADO

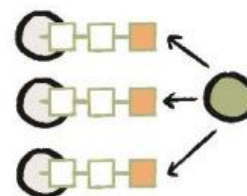
con
del
se
para



○ NODO ■ NUEVO BLOQUE
□ CADENA DE BLOQUES

Paso 4. La persona elegida propone un bloque nuevo con las transacciones que ha ido “escuchando” y registrando en su pool. Antes de ser enviado a los demás nodos, este bloque ha de ser validado un hash -que es el código alfanumérico obtenido a partir de toda la información bloque-. En la sección correspondiente hablaremos en profundidad de cómo encuentra este código, quién lo hace y qué sirve.

Paso 5. El sistema -los protocolos internos del blockchain- solo acepta el bloque si tiene un hash válido. En caso positivo, el resto de nodos verifican que todas las transacciones también sean correctas y actualizan su copia de la cadena con esta nueva versión que contiene el nuevo bloque.



1.3.1. El proceso de encadenamiento.

Para entender el proceso de encadenamiento, es importante conocer el concepto de hasheado. Este



término se usa para describir el uso de funciones llamadas hash, las cuales utilizan un algo- ritmo para convertir cualquier texto, documento o información en una sucesión de caracteres (a la que se denomina hash) siempre de la misma extensión. El algoritmo es tal que, ante cualquier cambio en el texto o documento, se genera una sucesión de caracteres distinta. Por ejemplo, utilizando el algoritmo de la función SHA-256 sobre la primera oración de este párrafo, se genera la siguiente sucesión de caracteres:

```
Hash: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
```

Es importante notar dos cosas con respecto al uso de funciones hash : (i) es computacionalmente imposible cambiar alguna información en el texto original y que se genere el mismo hash ; y (ii) la única forma de llegar a deducir el texto original desde la función hash es a través de prueba y error –fuerza bruta–, lo cual, dependiendo del tipo de función hash y la capacidad computacional que se tenga a disposición, podría llevar mucho tiempo porque implica probar todos los posibles hashes hasta encontrar el válido sin ninguna técnica que permita descartar a algunos de antemano.

SHA256 Hash

Datos: La aplicación blockchain al sector público puede generar avances significativo en la articulación de políticas públicas

Hash: 58bef5fcac2f03d68368d8c7dff1b45ac4632c78ea6ac5145099aead22f6a184

Vemos que si le agregamos un punto al final de la oración vemos que el Hash cambia totalmente

SHA256 Hash

Datos:	La aplicación blockchain al sector público puede generar avances significativo en la articulación de políticas públicas.
Hash:	74c903f6e8587c14a7ca9afb42f7d2d0f2548fc6bd52c03f51bb77c3609e5621

Entonces ¿cómo funciona el encadenamiento en blockchain? Básicamente, en el caso de la blockchain detrás de Bitcoin, cada cierto número de transacciones se crea un nuevo bloque, en el cual se incluye el hash del bloque anterior para crear un nuevo hash que corresponde al nuevo bloque. Es decir, cada nuevo bloque incluye el hash del bloque anterior, lo cual crea en la práctica una cadena de bloques que impide cambiar información contenida en un bloque anterior sin “arrastrar” cambios en los hashes de los bloques siguientes. Entonces, siguiendo el ejemplo de la billetera, todas las entradas y salidas de dinero de la billetera están encadenadas entre ellas de manera que cualquier intento de cambiar una transacción pasada genera un error a la hora de revisar el saldo actual. Ahora bien, si esta cadena de bloques existiera en una sola computadora sería posible alterar la información, ya que al existir solo una copia el único “dueño” de la cadena podría cambiarla toda cuando quisiera. Para evitar esto, entra en juego la segunda característica de blockchain: la distribución del registro.

1.3.2. El registro distribuido.

Esta característica simplemente trata de que el registro, es decir esa cadena de bloques que se va generando con cada nueva agrupación de información y que posee el hash del bloque anterior para garantizar que la información anterior no se ha cambiado, tenga una copia en varias computadoras, de hecho, en la mayor cantidad de computadoras posibles distribuidas en todo el mundo. Cada una de estas computadoras con una copia del registro tiene igual importancia que el resto; es decir: se trata de una red de pares en donde no existe alguien que domine al resto. Ahora bien, para poder cambiar información en un bloque antiguo, habría que cambiar ese bloque y todos los bloques siguientes en todas las copias del registro, haciéndolo mucho más difícil. Más aún, teniendo en cuenta que el proceso agrega nuevos bloques continuamente, la labor de cambiar un bloque antiguo se convierte en casi imposible a medida que aumenta el número de bloques “encima” de aquel

que se quiere cambiar, así como el número de copias del registro distribuidas en todo el mundo.

Lo que tendría que ocurrir para alterar una cadena de bloques es que alguien modificase una transacción en el bloque deseado y volviese a generar los hashes de ese bloque y el de los bloques siguientes coincidiesen con los hashes de la versión anterior de la cadena. Hacer esto es computacionalmente imposible para cada bloque, y ni siquiera se espera que la mecánica cuántica ofrezca una ventaja en este proceso (Allen- de López y Da Silva, 2019).

Sin embargo, esto genera una nueva pregunta: ¿qué pasa con la generación del siguiente bloque en un entorno de registros distribuidos donde todos tienen la misma importancia? ¿Quién se encarga de agregar un bloque adicional al registro y por qué se debe confiar en la veracidad de ese bloque? Es aquí donde cobra importancia el protocolo de consenso.

1.4. Tipos de blockchain

Pueden fácilmente distinguirse al menos tres tipos de redes blockchain: las públicas, las federadas y las privadas. Cabe mencionar asimismo la opción Blockchain as a Service para servicios en la nube.

1.4.1. Blockchain Pública.

Las redes blockchain públicas son aquellas a las que cualquier persona tiene acceso. En general, el procedimiento para participar es descargarse la aplicación correspondiente y conectarse, de forma automática, con un determinado número de nodos a los que se les pregunta por la versión más actualizada de la cadena. Una vez el nodo está actualizado, tiene los mismos derechos y deberes que el resto de participantes a la hora de proponer y validar transacciones, replicar las transacciones que escucha o minar -si desea hacerlo-. También en su mayoría, la seguridad de estas redes está basada en protocolos de consenso y funciones hash, y los usuarios interactúan con la red de forma anónima.

1.4.2. Blockchain Federada.

Los blockchains federados son un concepto de red diferente a los públicos e incluso podrían considerarse una tecnología diferente, puesto que no satisfacen en muchas ocasiones la definición o descripción que hemos abordado en las secciones previas. Estos blockchains han ido surgiendo con la idea de servir como registros descentralizados que permiten generar confianza en entornos complejos con entidades con diferentes intereses. En general no son públicos, sino que un número determinado de organizaciones, entidades o compañías se encargan de administrar la red y mantener copias sincronizadas del blockchain. El acceso generalizado es

en este caso mediante una interfaz web que estos administradores ponen a disposición de los usuarios.

Es por eso de vital importancia, a la hora de diseñar e implementar soluciones de este tipo, acompañar a la herramienta blockchain con un plan estratégico adecuado consistente en definir quiénes son los participantes, quién y cómo se va a administrar la red, quién va a validar las transacciones y qué información se les va a mostrar a los usuarios vía interfaz web.

En muchos casos el usuario que accede vía web puede no tener interés ni conocimiento sobre blockchain, pero sí necesitar de una plataforma que involucre entidades diferentes y requiera confianza y transparencia. Un blockchain federado puede ser entonces una buena opción siempre que las reglas del juego establecidas en la administración y mantenimiento de la cadena sean las

blockchain federado como Hyperledger, Corda, EFW o Multichain donde puedes descargar la aplicación de blockchain y programar la cadena a tu gusto, decidiendo quién quieres que participe, bajo qué reglas se regulan las transacciones, etc. Las redes públicas como Ethereum o Litecoin también ofrecen la oportunidad de hacer un fork para crear entornos federados o privados.

1.4.3. Blockchain Privada.


Los blockchain privados son aquellos en los que el control está reducido a una única entidad que se encarga de mantener la cadena, dar permisos a los usuarios que se desea que participen, proponer transacciones y aceptar los bloques. Son iguales que las federadas, pero con solo una entidad a cargo, de forma que además de todas las diferencias con respecto a las públicas que ya encontrábamos en las federadas, hay que añadir que se pierde la descentralización.

1.4.4. Blockchain As a Service.

“Beneficios de La cadena de bloques o blockchain aplicada a la administración tributaria de la provincia de Santa Fe”

Fundación para los Estudios Internacionales
Mendoza 444 - Rosario, Santa Fe - C.P. 2000

Comparativa entre los tipos de blockchain



	Públicos Bitcoin, Ethereum, Litecoin	Privados Hyperledger, Corda, Quorum	Federados Hyperledger, Corda, Quorum	Blockchain as a Service IBM, Microsoft, Amazon
Cualquiera puede participar	✓	✗	✗	NA
Los participantes actúan, en general, como nodos	✓	✗	✗	NA
Transparencia	✓	≈	≈	NA
Hay un único administrador	✗	✓	✗	NA
Hay más de un administrador	✗	✗	✓	NA
No hay administradores	✓	✗	✗	NA
Ningún participante tiene más derechos que los demás	✓	✗	✗	NA
Se pueden implementar Smart Contracts	✓	✓	✓	NA
Existe recompensa por minado de bloques	≈	✗	✗	NA
Soluciona problema de falta de confianza	✓	✗	≈	NA
Seguridad basada en protocolos de consenso	✓	✗	≈	NA
Seguridad basada en funciones hash	✓	≈	≈	NA
Provee servicios en la nube	NA	NA	NA	✓

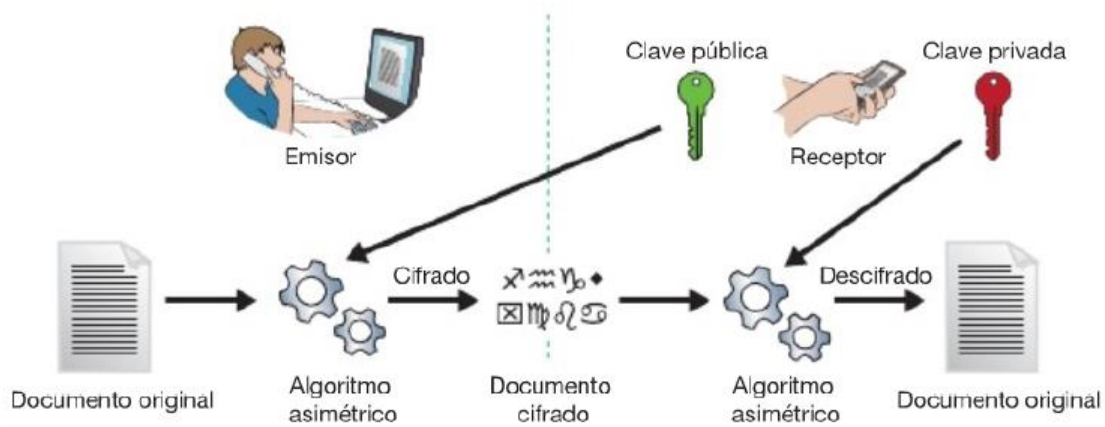
Algunas grandes compañías ofrecen servicios de blockchain en la nube. Algunos ejemplos son IBM especializada en HyperledgerFabric, Amazon colaborando con Digital Currency Group, o Microsoft ofreciendo servicios de R3, HyperledgerFabric o Quorum, entre otras. Estos servicios no solo consisten en almacenamiento de información, en este caso del blockchain, sino que las ventajas de este tipo de servicios son un aumento en la seguridad, la no necesidad de invertir en hardware y la posibilidad de un entorno más amigable con el que trabajar, pudiendo crear tu propio canal de blockchain sin necesidad de programar.

1.5 Criptografía Asimétrica, claves y Wallets

La tecnología Blockchain utiliza criptografía de clave asimétrica (también conocida como criptografía de clave pública). La criptografía de clave asimétrica utiliza un par de claves: una clave pública y una clave privada que están

matemáticamente relacionados entre sí. La clave pública se hace pública sin reducir la seguridad del proceso, pero la clave privada debe permanecer en secreto para que los datos conserven su protección criptográfica. Aunque existe una relación entre las dos claves, la clave privada no puede determinarse de manera eficiente basándose en el conocimiento de la clave pública. Uno puede cifrar con una clave privada y luego descifrar con la clave pública. Alternativamente, uno puede cifrar con una clave pública y luego descifrar con una clave privada.

La criptografía de clave asimétrica permite una relación de confianza entre usuarios que no se conocen ni confían entre sí, al proporcionar un mecanismo para verificar la integridad y la autenticidad de las transacciones y, al mismo tiempo, permitir que las transacciones permanezcan públicas. Para hacer esto, las transacciones son 'firmadas digitalmente'. Esto significa que se utiliza una clave privada para cifrar una transacción de modo que cualquiera que tenga la clave pública pueda descifrarla. Dado que la clave pública está disponible gratuitamente, cifrar la transacción con la clave privada prueba que el firmante de la transacción tiene acceso a la clave privada. Alternativamente, se pueden cifrar los datos con la clave pública de un usuario de modo que solo los usuarios con acceso a la clave privada puedan descifrarlos. Un inconveniente es que la criptografía de clave asimétrica suele ser lenta de calcular.



Esto contrasta con la criptografía de clave simétrica en la que se utiliza una sola clave secreta para cifrar y descifrar. Con la criptografía de clave simétrica, los usuarios ya deben tener una relación de confianza establecida entre ellos para intercambiar la clave previamente compartida. En un sistema simétrico, cualquier dato cifrado que se pueda descifrar con la clave previamente compartida confirma que fue enviado por otro usuario con acceso a la clave previamente compartida; ningún usuario sin acceso a la clave pre compartida podrá ver los datos descifrados. En comparación con la criptografía de clave asimétrica, la criptografía de clave

simétrica es muy rápida de calcular. Por eso, cuando uno dice estar encriptando algo que usa criptografía de clave asimétrica, a menudo los datos se encriptan con criptografía de clave simétrica y luego la clave simétrica se encripta usando criptografía de clave asimétrica

Aquí hay un resumen del uso de la criptografía de clave asimétrica en muchas redes de blockchain:

- Las claves privadas se utilizan para firmar transacciones digitalmente.
- Las claves públicas se utilizan para derivar direcciones.
- Las claves públicas se utilizan para verificar firmas generadas con claves privadas.

- La criptografía de clave asimétrica brinda la capacidad de verificar que el usuario que transfiere valor a otro usuario está en posesión de la clave privada capaz de firmar la transacción.

Dentro del ecosistema blockchain hay un elemento que conforma uno de los ejes principales, las billeteras o Wallets, dado que es donde se guardan, almacenan, dispone la información las criptomonedas que poseemos. Podríamos decir que esto es una billetera normal digital, pero en el mundo blockchain esto va un poco más allá. Las billeteras digitales son repositorios personales portables y seguros. Pueden ser por ejemplo aplicaciones móviles que nos permiten administrar nuestros identificadores, autenticadores, datos y credenciales verificables en nuestro teléfono, estando éstos completamente protegidos y bajo nuestro control. De este modo, podemos decidir qué información compartimos con quién, en forma de presentaciones verificables. Básicamente, las billeteras digitales no solo permiten almacenar criptomonedas, las billeteras digitales permiten que la información personal digital sea portable. En ellas se almacenan claves, credenciales y datos.

Es importante tratar de definir las billeteras en el sentido más amplio posible porque nos permitirá más adelante entender conceptos como Non fungible tokens o identidad auto-gestionada.

Al comprar bitcoins o cualquier otra criptomoneda, es necesario cuidarlas para que permanezcan seguras. Por eso es importante conocer los principales tipos de billeteras o wallets existentes. Una billetera criptográfica es una herramienta que permite a los usuarios interactuar con redes blockchain. Son necesarios al enviar y recibir Bitcoin y otras monedas digitales. Las wallets también se pueden utilizar para generar nuevas direcciones de cadena de bloques.

A diferencia de las billeteras tradicionales que usamos en nuestra vida diaria, las wallets de criptomonedas en realidad no almacenan sus fondos. De hecho, sus

monedas (o tokens) son simplemente parte de un sistema de cadena de bloques como piezas de datos, y las billeteras sirven como un medio para acceder a ellas.

Técnicamente hablando, la mayoría de las billeteras criptográficas pueden generar uno o más pares de claves públicas y privadas. La clave pública se usa para generar direcciones de billetera, que son necesarias para recibir pagos. Las claves privadas, por otro lado, se utilizan durante la creación de firmas digitales y la verificación de transacciones (las claves privadas son confidenciales y nunca deben compartirse con nadie).

1.5.1. Tipos de Wallets

Hay tres grupos principales de billeteras de criptomonedas: de software, hardware y de papel. Pero también pueden definirse como billeteras calientes o billeteras frías de acuerdo con la forma en que funcionan. Los hot wallets son los que de alguna manera están conectados a Internet y, por lo tanto, son más susceptibles a los ataques. Las billeteras frías son las que generan claves sin conexión a Internet, lo que las hace altamente resistentes a los ciberataques.

Billeteras de software

Los tipos más comunes de wallets de software incluyen billeteras de web, billeteras de escritorio y aplicaciones móviles.

Billetera web: consiste en una interfaz de navegador que no requiere ninguna descarga ni instalación. Más conveniente pero también más peligroso ya que las claves privadas generalmente son administradas por terceros.

Billetera de escritorio: software que se puede descargar y ejecutar de forma local. Menos convenientes que las carteras web, pero más seguras porque las claves privadas se almacenan localmente y son administradas por los usuarios. Las billeteras de escritorio solo deben usarse en computadoras que estén limpias (sin virus o infecciones de malware).

Aplicaciones móviles: son similares a las de escritorio, pero diseñadas para teléfonos inteligentes. El uso de códigos QR los convierte en una alternativa conveniente para enviar y recibir criptomonedas.

Billeteras de hardware

Las wallets de hardware consisten en dispositivos físicos que generan y almacenan claves sin ninguna conexión a Internet y, como tales, entran en la categoría de billeteras frías. Normalmente, las claves se crean basándose en algoritmos de generación de números aleatorios y se almacenan en el propio dispositivo (y en ningún otro lugar). A pesar de ser menos convenientes debido a la accesibilidad limitada, las billeteras de hardware se consideran una de las alternativas más seguras para "almacenar" y administrar criptomonedas.

Billeteras de papel

Una billetera de papel consiste en una hoja de papel con una dirección blockchain y su correspondiente clave privada. Las claves generalmente se imprimen como largas cadenas de números y letras junto con códigos QR, que se pueden escanear para ejecutar transacciones en criptomonedas. Si se utilizan carteras de papel para generar claves fuera de línea, también se pueden considerar carteras frías. Sin embargo, se desaconseja su uso porque presentan numerosas fallas y un riesgo potencial para los usuarios que carecen de conocimientos técnicos

1.6. Protocolos.

Un aspecto clave de la tecnología blockchain es determinar qué usuario publica el siguiente bloque. Esto se resuelve mediante la implementación de uno de los muchos modelos de consenso o protocolos posibles. Para las redes de cadena de bloques sin permiso, generalmente hay muchos nodos de publicación que compiten al mismo tiempo para publicar el siguiente bloque. Por lo general, hacen esto para ganar criptomonedas y/o tarifas de transacción. Por lo general, son usuarios que desconfían mutuamente y que solo pueden conocerse por sus direcciones públicas. Es probable que cada nodo de publicación esté motivado por un deseo de obtener ganancias financieras, no por el bienestar de los otros nodos de publicación o incluso de la red misma.

En tal situación, ¿por qué un usuario propagaría un bloque que otro usuario está intentando publicar? Además, ¿quién resuelve los conflictos cuando varios nodos publican un bloque aproximadamente al mismo tiempo? Para que esto funcione, las tecnologías de cadena de bloques utilizan modelos de consenso para permitir que un grupo de usuarios que desconfían mutuamente trabajen juntos.

Cuando un usuario se une a una red blockchain, acepta el estado inicial del sistema. Esto se registra en el único bloque preconfigurado, el bloque génesis. Cada red de cadena de bloques tiene un bloque de génesis publicado y cada bloque debe agregarse a la cadena de bloques después de él, según el modelo de consenso acordado. Sin embargo, independientemente del modelo, cada bloque debe ser válido y, por lo tanto, cada usuario de la red blockchain puede validarlo de forma independiente. Al combinar el estado inicial y la capacidad de verificar cada bloque desde entonces, los usuarios pueden acordar de forma independiente el estado actual de la cadena de bloques. Tenga en cuenta que si alguna vez se presentaron dos cadenas válidas a un nodo completo, el mecanismo predeterminado en la mayoría de las redes de cadena de bloques es que la cadena "más larga" se considera la correcta y se adoptará; esto se debe a que ha tenido la mayor cantidad

de trabajo puesto en él. Esto sucede frecuentemente con algunos modelos de consenso y será discutido en detalle.

En resumen, tenemos las siguientes características:

- Se acuerda el estado inicial del sistema (por ejemplo, el bloque génesis).
- Los usuarios aceptan el modelo de consenso por el cual se agregan bloques al sistema.

- Cada bloque está vinculado al bloque anterior al incluir el resumen hash del encabezado del bloque anterior (excepto el primer bloque de 'génesis', que no tiene un bloque anterior y para el cual el hash del encabezado del bloque anterior generalmente se establece en ceros).

- Los usuarios pueden verificar cada bloque de forma independiente.

En la práctica, el software maneja todo y los usuarios no necesitan conocer estos detalles.

Una característica clave de la tecnología blockchain es que no es necesario que un tercero de confianza proporcione el estado del sistema: todos los usuarios dentro del sistema pueden verificar la integridad del sistema. Para agregar un nuevo bloque a la cadena de bloques, todos los nodos deben llegar a un acuerdo común con el tiempo; sin embargo, se permite algún desacuerdo temporal. Para las redes de cadena de bloques sin permiso, el modelo de consenso debe funcionar incluso en presencia de usuarios posiblemente maliciosos, ya que estos usuarios podrían intentar interrumpir o apoderarse de la cadena de bloques. Tenga en cuenta que para las redes de cadena de bloques autorizadas se pueden utilizar recursos legales si un usuario actúa de forma maliciosa.

En algunas redes blockchain, como las autorizadas, puede existir cierto nivel de confianza entre los nodos de publicación. En este caso, puede que no sea necesario un modelo de consenso intensivo en recursos (tiempo de cálculo, inversión, etc.) para determinar qué participante agrega el siguiente bloque a la cadena. Generalmente, a medida que aumenta el nivel de confianza, disminuye la necesidad de uso de recursos como medida para generar confianza. Para algunas implementaciones de blockchain autorizadas, la visión del consenso se extiende más allá de garantizar la validez y la autenticidad de los bloques, sino que abarca todos los sistemas de verificación y validación desde la propuesta de una transacción hasta su inclusión final en un bloque.

En los siguientes párrafos, se analizan varios modelos de consenso, así como el enfoque de resolución de conflictos más común.

1.6.1. Proof of Work (prueba de trabajo).

Proof-of-Work (PoW) corresponde al grupo de protocolos de consenso donde se exige un esfuerzo a los participantes en el sorteo para determinar quién propone el siguiente bloque, y se da una recompensa al ganador. El esfuerzo aquí consiste en emplear capacidad computacional para encontrar el código hash que valide el bloque anterior. En la siguiente sección hablaremos de cómo se obtiene, pero por el momento basta con decir que se necesita tener una computadora que realice intentos aleatorios para encontrarlo. Cuanto mayor es la potencia del ordenador, mayor es el consumo energético y mayor es la probabilidad de obtener el código válido.

Lo que ocurre entonces es que cuando alguien propone un nuevo bloque lo hace sin un código hash, de forma que todos los nodos pueden competir por encontrarlo -solo algunos lo hacen y son conocidos como mineros, ya que al proceso de encontrar el hash se le conoce como minar-

Dado que emplear capacidad computacional para encontrar el hash implica gastar dinero, y que ningún nodo tiene la garantía de ser el primero en encontrarlo, parece poco razonable que un nodo malintencionado gaste energía y dinero en ese propósito. Más aun teniendo en cuenta que, en caso de que ganase el sorteo y propusiese un bloque inválido, el resto de nodos lo rechazarían y se quedaría sin la recompensa.

Para motivar a los mineros no malintencionados a intentar encontrar los hashes válidos, los blockchain que implementan este método ofrecen una recompensa en forma de criptomoneda al primer nodo que lo encuentre. Este método solo se puede usar, por tanto, en blockchains asociados a criptomonedas.

Uno de los argumentos esgrimidos en contra de este protocolo es la gran cantidad de energía empleada -algunos dirían desperdiciada- en validar o minar los bloques. Por un lado, es necesario decir que este proceso no sirve solamente para determinar quién propone el siguiente bloque, sino que también redundante en la seguridad de la cadena. Como veremos, si alguien modifica algo en un bloque tanto ese bloque como todos los posteriores pasaran a tener un hash inválido que necesita ser minado de nuevo.

Por tanto, si alguien consiguiese modificar el blockchain tendría que volver a minar de nuevo no solo ese bloque sino todos los posteriores, y tendría que hacer eso en cada copia del blockchain que está en propiedad de cada nodo. Como es evidente, la dificultad que tendrá dicho hacker que superar sería la misma que tuvieron los mineros iniciales. Cerrando el argumento, aquel que quiera corromper la red va a tener que gastar tanta energía en hacerlo como la que se gastó en

validarla originalmente. Si la dificultad es alta, la energía empleada es mayor, pero también lo es la seguridad.

Por otro lado, también hay que decir que, a partir de un cierto nivel de dificultad en el hash -lo que implica un mayor gasto energético en encontrarlo-, la cadena puede considerarse suficientemente segura y la energía extra empleada para obtener hashes válidos de mayor dificultad puede considerarse desperdiciada. No solo eso, sino que hay otros métodos para aumentar la seguridad como pueden ser aumentar la descentralización -con más nodos manteniendo copias de la cadena-.

La razón por la cual, a pesar de ello, se gasta toda esta energía es que la dificultad del hash no se configura en función de cuánta seguridad se pretende conseguir sino de cuál es el tiempo promedio que se pretende que los mineros tarden en minar. Es decir, como los mineros compiten por encontrar el hash para cada bloque, si se fijase una dificultad de minado que aportase suficiente seguridad para la cadena, entonces cuando los mineros aumentasen en número o incrementasen sus recursos los bloques se minarían cada vez más rápido y por tanto estarían más vacíos -contendrían menos transacciones-. Esto no interesa, de forma que lo que se fija es el tiempo promedio que se desea que tarden los bloques en ser minados -en Bitcoin son 10 minutos y cada 2 semanas aproximadamente se re calcula la dificultad de minado de forma que se satisfaga ese requisito-. Si, por ejemplo, se duplica el número de nodos mineros o los que ya hay duplican su capacidad computacional, entonces disminuirá el tiempo que tardan en minar y, tras el periodo establecido, se re calculará la dificultad de obtener el hash al alza.

1.6.2. Proof of Stake (prueba de participación).

El modelo de Proof of Stake o de participación (PoS) se basa en la idea de que cuanto más participación haya invertido un usuario en el sistema, más probable es que desee que el sistema tenga éxito y menos probable que desee hackearlo. La participación suele ser una cantidad de criptomonedas que el usuario de la red blockchain ha invertido en el sistema (a través de varios medios, como bloquearlo a través de un tipo de transacción especial, enviarlo a una dirección específica o mantenerlo dentro de un software de billetera especial). Una vez depositada, la criptomoneda generalmente ya no se puede gastar. Las redes de blockchain de prueba de participación utilizan la cantidad de participación que tiene un usuario como factor determinante para publicar nuevos bloques. Por lo tanto, la probabilidad de que un usuario de la red blockchain publique un nuevo bloque está ligada a la proporción de su participación en la cantidad total de criptomonedas puestas en la red blockchain.

Con este modelo de consenso, no es necesario realizar cálculos intensivos en recursos (que involucran tiempo, electricidad y potencia de procesamiento) como se encuentra en la prueba de trabajo. Dado que este modelo de consenso utiliza menos recursos, algunas redes de cadenas de bloques han decidido renunciar a una recompensa por creación de bloques; estos sistemas están diseñados para que todas las criptomonedas ya se distribuyan entre los usuarios en lugar de que se generen nuevas criptomonedas a un ritmo constante. En tales sistemas, la recompensa por la publicación en bloque suele ser la obtención de tarifas de transacción proporcionadas por el usuario.

Los métodos de cómo la red blockchain usa la participación pueden variar. Vamos a hablar de cuatro enfoques: selección aleatoria de usuarios apostados, votación de rondas múltiples, sistemas de envejecimiento de monedas y sistemas de delegados. Independientemente del enfoque exacto, es más probable que los usuarios con más participación publiquen nuevos bloques.

Cuando la elección del editor del bloque es una elección aleatoria (a veces denominada prueba de participación basada en cadena), la red de la cadena de bloques observará a todos los usuarios con participación y elegirá entre ellos en función de su proporción de participación con respecto a la cantidad total de criptomonedas apostadas. Entonces, si un usuario tuviera el 42 % de toda la participación en la red blockchain, sería elegido el 42 % de las veces; aquellos con 1 % serían elegidos 1 % de las veces.

Cuando la elección del editor del bloque es un sistema de votación de múltiples rondas, existe una complejidad adicional. La red de la cadena de bloques seleccionará varios usuarios apostados para crear los bloques propuestos. Luego, todos los usuarios apostados emitirán un voto por un bloque propuesto. Pueden ocurrir varias rondas de votación antes de que se decida un nuevo bloque. Este método permite que todos los usuarios apostados tengan voz en el proceso de selección de bloques para cada nuevo bloque.

Cuando la elección del editor del bloque se realiza a través de un sistema de edad de la moneda denominado prueba de participación de la edad de la moneda, la criptomoneda apostada tiene una propiedad de edad. Después de una cierta cantidad de tiempo (como 30 días), la criptomoneda apostada puede contar para que el usuario propietario sea seleccionado para publicar el siguiente bloque. A continuación, se restablece la antigüedad de la criptomoneda apostada y no se puede volver a utilizar hasta que haya transcurrido el tiempo requerido. Este método permite a los usuarios con más participación publicar más bloques, pero no dominar el sistema, ya que tienen un temporizador de enfriamiento adjunto a cada moneda

de criptomoneda contada para la creación de bloques. Las monedas más antiguas y los grupos de monedas más grandes aumentarán la probabilidad de ser elegido para publicar el siguiente bloque. Para evitar que las partes interesadas acumulen criptomonedas antiguas, generalmente hay un máximo incorporado en la probabilidad de ganar.

Cuando la elección del editor de bloques se realiza a través de un sistema delegado, los usuarios votan por nodos para que se conviertan en nodos de publicación y, por lo tanto, crean bloques en su nombre. El poder de voto de los usuarios de la red Blockchain está vinculado a su participación, por lo que cuanto mayor sea la participación, más peso tendrá el voto. Los nodos que reciben la mayor cantidad de votos se convierten en nodos de publicación y pueden validar y publicar bloques. Los usuarios de la red Blockchain también pueden votar en contra de un nodo de publicación establecido, para tratar de eliminarlo del conjunto de nodos de publicación. La votación para los nodos de publicación es continua y permanecer como nodo de publicación puede ser bastante competitivo. La amenaza de perder el estado del nodo de publicación y, por lo tanto, las recompensas y la reputación es constante, por lo que se incentiva a los nodos de publicación para que no actúen maliciosamente. Además, los usuarios de la red blockchain votan por delegados, que participan en la gobernanza de la cadena de bloques. Los delegados propondrán cambios y mejoras, que serán votados por los usuarios de la red blockchain.

Vale la pena señalar que un problema conocido como "nada en juego" puede surgir de algunos algoritmos de prueba de participación. Si existieran varias cadenas de bloques competidoras en algún momento, un usuario en participación podría actuar en cada una de esas cadenas competidoras, ya que es esencialmente libre de hacerlo. El usuario apostado puede hacer esto como una forma de aumentar sus probabilidades de ganar una recompensa. Esto puede hacer que varias ramas de la cadena de bloques sigan creciendo sin reconciliarse en una sola rama durante largos períodos de tiempo.

Bajo los sistemas de prueba de participación, los "ricos" pueden apostar más fácilmente más activos digitales, ganando más activos digitales; sin embargo, obtener la mayoría de los activos digitales dentro de un sistema para "controlarlo" generalmente tiene un costo prohibitivo.

1.6.3. Round Robin.

Round Robin es un modelo de consenso que utilizan algunas redes blockchain autorizadas. Dentro de este modelo de consenso, los nodos se turnan para crear bloques. Round Robin Consensus tiene una larga historia basada en la

arquitectura de sistemas distribuidos. Para manejar situaciones en las que un nodo de publicación no está disponible para publicar un bloque en su turno, estos sistemas pueden incluir un límite de tiempo para permitir que los nodos disponibles publiquen bloques para que los nodos no disponibles no detengan la publicación de bloques. Este modelo garantiza que ningún nodo cree la mayoría de los bloques. Se beneficia de un enfoque sencillo, carece de acertijos criptográficos y tiene bajos requisitos de energía.

Dado que existe la necesidad de confianza entre los nodos, el round robin no funciona bien en las redes de cadena de bloques sin permiso utilizadas por la mayoría de las criptomonedas. Esto se debe a que los nodos maliciosos podrían agregar continuamente nodos adicionales para aumentar sus probabilidades de publicar nuevos bloques. En el peor de los casos, podrían usar esto para subvertir el correcto funcionamiento de la red blockchain.

1.6.4. Prueba de Autoridad.

El modelo de consenso de prueba de autoridad (también conocido como prueba de identidad) se basa en la confianza parcial de los nodos de publicación a través de su vínculo conocido con las identidades del mundo real. Los nodos de publicación deben tener sus identidades probadas y verificables dentro de la red de la cadena de bloques (por ejemplo, documentos de identificación que han sido verificados y notariados e incluidos en la cadena de bloques). La idea es que el nodo de publicación apueste su identidad/reputación para publicar nuevos bloques. Los usuarios de la red Blockchain afectan directamente la reputación de un nodo de publicación en función del comportamiento del nodo de publicación. Los nodos de publicación pueden perder reputación al actuar de una manera con la que los usuarios de la red blockchain no están de acuerdo, al igual que pueden ganar reputación al actuar de una manera con la que los usuarios de la red blockchain están de acuerdo. A menor reputación, menor probabilidad de poder publicar un bloque. Por lo tanto, es de interés de un nodo editorial mantener una alta reputación. Este algoritmo solo se aplica a redes blockchain autorizadas con altos niveles de confianza.

1.6.5. Prueba de tiempo Transcurrido (PoET).

Dentro del modelo de consenso de prueba de tiempo transcurrido (PoET), cada nodo de publicación solicita un tiempo de espera de una fuente de tiempo de hardware segura dentro de su sistema informático. La fuente de tiempo de hardware segura generará un tiempo de espera aleatorio y lo devolverá al software del nodo de publicación. Los nodos de publicación toman el tiempo aleatorio que se les da y quedan inactivos durante ese tiempo. Una vez que un nodo de publicación se

despierta del estado inactivo, crea y publica un bloque en la red blockchain, alertando a los otros nodos del nuevo bloque; cualquier nodo de publicación que aún esté inactivo dejará de esperar y todo el proceso comenzará de nuevo.

Este modelo requiere asegurarse de que se utilizó un tiempo aleatorio, ya que, si el tiempo de espera no se selecciona al azar, un nodo de publicación malicioso solo esperaría la cantidad mínima de tiempo por defecto para dominar el sistema. Este modelo también requiere asegurarse de que el nodo de publicación esperó el tiempo real y no comenzó temprano.

El software verificado y confiable puede ejecutarse en estos entornos de ejecución seguros y no puede ser alterado por programas externos. Un nodo de publicación consultaría al software que se ejecuta en este entorno seguro durante un tiempo aleatorio y luego esperaría a que transcurriera ese tiempo. Después de esperar el tiempo asignado, el nodo de publicación podría solicitar un certificado firmado de que el nodo de publicación esperó el tiempo asignado aleatoriamente. El nodo de publicación luego publica el certificado junto con el bloque.

1.7. Folks

Realizar cambios y actualizar la tecnología puede ser difícil en el mejor de los casos. Para las redes de cadenas de bloques sin permiso que están compuestas por muchos usuarios, distribuidas por todo el mundo y gobernadas por el consenso de los usuarios, se vuelve extremadamente difícil. Los cambios en el protocolo y las estructuras de datos de una red blockchain se denominan bifurcaciones o Folks. Se pueden dividir en dos categorías: Soft Folks y Hard Folks. Para una bifurcación suave, estos cambios son compatibles con versiones anteriores de nodos que no se han actualizado. Para una bifurcación dura, estos cambios no son compatibles con versiones anteriores porque los nodos que no se han actualizado rechazarán los bloques después de los cambios. Esto puede conducir a una división en la red de la cadena de bloques creando múltiples versiones de la misma cadena de bloques. Las redes de cadena de bloques autorizadas, debido a que se conocen los nodos de publicación y los usuarios, pueden mitigar los problemas de bifurcación al requerir actualizaciones de software.

Tenga en cuenta que el término bifurcación también se usa en algunas redes de cadenas de bloques para describir conflictos de contabilidad temporales (por ejemplo, dos o más bloques dentro de la red de cadenas de bloques con el mismo número de bloque). Si bien esto es una bifurcación en el libro mayor, es temporal y no se deriva de un cambio de software.

1.7.1. Soft Folks

Una bifurcación suave es un cambio en una implementación de blockchain que es compatible con versiones anteriores. Los nodos no actualizados pueden continuar realizando transacciones con nodos actualizados.

Si no se actualiza ningún nodo (o muy pocos), no se seguirán las reglas actualizadas. Se produjo un ejemplo de una bifurcación suave en Bitcoin cuando se agregó una nueva regla para respaldar el depósito en garantía y reembolsos con límite de tiempo. En 2014, se hizo una propuesta para reutilizar un código de operación que no realizaba ninguna operación, lo que permite que la salida de una transacción se pueda gastar en un momento en el futuro. Para los nodos que implementen este cambio, el software del nodo realizará esta nueva operación, pero para los nodos que no admitan el cambio, la transacción seguirá siendo válida y la ejecución continuará como si se hubiera ejecutado un NOP 9. Un ejemplo ficticio de una bifurcación blanda sería si una cadena de bloques decidiera reducir el tamaño de los bloques (por ejemplo, de 1,0 MB a 0,5 MB).

Los nodos actualizados ajustarían el tamaño del bloque y continuarían realizando transacciones con normalidad; los nodos no actualizados verían estos bloques como válidos, ya que el cambio realizado no viola sus reglas (es decir, el tamaño del bloque está por debajo del máximo permitido). Sin embargo, si un nodo no actualizado creara un bloque con un tamaño superior a 0,5 MB, los nodos actualizados lo rechazarían como no válido.

1.7.2. Hard Forks

Una bifurcación dura es un cambio en una implementación de blockchain que no es compatible con versiones anteriores. En un momento dado (generalmente en un número de bloque específico), todos los nodos de publicación deberán cambiar para usar el protocolo actualizado. Además, todos los nodos deberán actualizarse al nuevo protocolo para que no rechacen los bloques recién formateados. Los nodos no actualizados no pueden continuar realizando transacciones en la cadena de bloques actualizada porque están programados para rechazar cualquier bloque que no siga su versión de la especificación del bloque.

Los nodos de publicación que no se actualizan seguirán publicando bloques con el formato anterior. Los nodos de usuario que no se hayan actualizado rechazarán los bloques recién formateados y solo aceptarán bloques con el formato anterior. Esto da como resultado dos versiones de la cadena de bloques que existen simultáneamente. Tenga en cuenta que los usuarios de diferentes versiones de hardfork no pueden interactuar entre sí. Es importante tener en cuenta que, si bien la mayoría de las bifurcaciones duras son intencionales, los errores de software pueden producir bifurcaciones duras no intencionales.

Un ejemplo bien conocido de una bifurcación dura es de Ethereum. En 2016, se construyó un contrato inteligente en Ethereum llamado Organización Autónoma Descentralizada (DAO). Debido a fallas en la forma en que se construyó el contrato inteligente, un atacante extrajo Ether, la criptomoneda utilizada por Ethereum, lo que resultó en el robo de USD 50 millones. Los titulares de Ether votaron una propuesta de bifurcación dura, y la gran mayoría de los usuarios acordaron hacer una bifurcación dura y crear una nueva versión de la cadena de bloques, sin la falla, y eso también devolvió los fondos robados. Con las criptomonedas, si hay una bifurcación dura y la cadena de bloques se divide, los usuarios tendrán una moneda independiente en ambas bifurcaciones (con el doble de monedas en total). Si toda la actividad se traslada a la nueva cadena, es posible que la anterior no se utilice ya que las dos cadenas no son compatibles (serán sistemas monetarios independientes). En el caso de la bifurcación dura de Ethereum, la clara mayoría del apoyo se trasladó a la nueva bifurcación, la antigua bifurcación pasó a llamarse Ethereum Classic y siguió funcionando.

1.8. Ethereum

Antes de entrar en temas más específicos como Smart Contract o Tokens es necesario que hagamos una introducción Ethereum. Esto resulta de suma importancia ya que actualmente es donde se corre la mayoría de las aplicaciones mencionadas. Además, como veremos más adelante en Smart Contracts, Ethereum, fue la pionera en permitir este tipo de posibilidades.

Para este fin, recurrimos al fundador de Ethereum, Vitalik Buterin, donde nos da una idea de cuál es el principal objetivo de Ethereum. “El propósito de Ethereum es crear un protocolo alternativo para construir aplicaciones descentralizadas, proporcionando un conjunto diferente de contrapartidas que creemos que serán muy útiles para un amplio abanico de aplicaciones descentralizadas, con especial énfasis en situaciones en las que el rápido tiempo de desarrollo, la seguridad para aplicaciones pequeñas y rara vez usadas y la capacidad de las diferentes aplicaciones para interactuar de manera muy eficiente son importantes. Ethereum lo logra construyendo lo que es esencialmente la capa fundacional abstracta definitiva: una blockchain con un lenguaje de programación Turing completo, que permite a cualquiera escribir contratos y aplicaciones descentralizadas donde pueden crear sus propias reglas arbitrarias de propiedad, formatos de transacción y funciones de transición de estado. Los contratos inteligentes, "cajas" criptográficas que contienen valor y sólo lo desbloquean si se cumplen ciertas condiciones también se pueden desarrollar por encima de la plataforma, con mucho más poder

que el que ofrece el script de Bitcoin gracias a los poderes añadidos de completitud Turing, conocimiento del valor, conocimiento de la blockchain y estado.

1.8.1. ¿Que es Ethereum?

En el universo Ethereum, hay un computador único y canónico (llamado máquina virtual de Ethereum o EVM), cuyo estado han acordado todos los participantes de la red. Cualquiera que participe en la red de Ethereum (cada nodo de Ethereum) mantiene una copia del estado de este ordenador. Adicionalmente, cualquier participante puede emitir una petición para que este ordenador realice un cálculo arbitrario. Cuando se transmite una solicitud de este tipo, los demás participantes de la red verifican, validan y ejecutan el cálculo. Esto causa un cambio de estado en la EVM, que se realiza y propaga a través de toda la red.

Las peticiones de cálculo se llaman solicitudes de transacción; el registro de todas las transacciones, así como el estado actual de la EVM se almacena en la blockchain que, a su vez, almacenan y acuerdan todos los nodos.

Los mecanismos criptográficos garantizan que, una vez que las transacciones se verifican y se añaden a la blockchain, ya no se pueden manipular; los mismos mecanismos garantizan también que todas las transacciones se firman y se ejecutan con los "permisos" apropiados.

1.8.2. Ether.

El propósito de Ether, la criptomoneda, es permitir la existencia de un mercado computacional. Este mercado proporciona un incentivo económico para que los participantes puedan verificar/ejecutar solicitudes de transacción y proporcionar recursos computacionales a la red.

Cualquier participante que emita una petición de transacción debe aportar también cierta cantidad de ether a la red, la recompensa se concederá a quien haga el trabajo completo de verificar la transacción, ejecutarla, incluirla en la blockchain y emitirla a la red.

La cantidad de ether pagada va en función de la duración del cálculo. Esto también previene que los participantes malintencionados congestionen la red solicitando la ejecución de bucles infinitos o scripts que consumen muchos recursos, ya que se les cobrará continuamente.

En la práctica, los participantes no escriben código nuevo cada vez que desean solicitar un cálculo en la EVM. En su lugar, los desarrolladores de aplicaciones cargan programas (fragmentos de código reutilizables) en el almacén de la EVM y, a continuación, los usuarios solicitan la ejecución de estos fragmentos de código con distintos parámetros. Llamamos contratos inteligentes, o "smartcontracts", a los programas cargados y ejecutados por la red.

A nivel muy básico, se puede pensar en un contrato inteligente como una especie de máquina expendedora: un script que, cuando se solicita con ciertos parámetros, realiza algunas acciones o cálculos si se cumplen determinadas condiciones. Por ejemplo, un simple contrato inteligente de proveedor podría crear y asignar la propiedad de un recurso digital si la persona que lo solicita envía ether a un destinatario específico.

Cualquier desarrollador puede crear un contrato inteligente y hacerlo público en la red, usando la blockchain como su capa de datos, a cambio de una tasa/comisión pagada a la red. A continuación, cualquier usuario puede solicitar el uso del contrato inteligente para ejecutar su código, de nuevo, a cambio de una comisión pagada a la red.

Así pues, mediante los contratos inteligentes los desarrolladores pueden construir e implementar arbitrariamente complejas aplicaciones y servicios orientados al usuario: mercados, instrumentos financieros, juegos, etc.

1.9. Smart Contracts o Contratos Inteligentes

El término Smart Contracts puede designar desde contratos o cláusulas contractuales en lenguaje natural trasladados a código informático hasta casos más complejos representados y ejecutados directamente por scripts.

Formular una definición de Smart Contract no resulta una tarea sencilla, y así lo demuestra la variedad de definiciones diferentes que proponen los trabajos sobre la materia, o la total elusión de una definición con la que otros lo abordan. Más aún, su complejidad se agudiza por la diversidad de disciplinas que convergen en el estudio de este fenómeno (p. ej. jurídica, matemática, informática). Por tanto, dependiendo de la disciplina desde la que se trabaje, así como de la función primordial que debe cumplir o que se le atribuye a esta figura, las definiciones y sus características varían.

No obstante, sí es cierto que en todas estas definiciones o aproximaciones a la figura de los Smarts Contracts se observa la concurrencia de algunos rasgos comunes. Por tal motivo, para intentar llegar a una definición que abarque todos los fenómenos posibles y susceptibles de tratamiento bajo esta figura, creemos que lo mejor es exponer las distintas definiciones existentes, buscar sus denominadores comunes y, de esta forma, intentar conformar una definición propia y aclarar algunos conceptos clave.

Una de las primeras definiciones conocidas es la formulada por Nick Szabo, que fue quien acuñó este término, y que definió Smart Contract como a set of promises, specified in digital form, including protocols within which the parties perform on these promises. Este autor se

remonta a las máquinas expendedoras como el antecedente de los Smart Contract. El automatismo de estas máquinas en la ejecución de las prestaciones (entrega de una mercancía) cuando se inserta la moneda y verifica que la misma es legal y en la cuantía acordada, permitiría considerarlo como el contrato inteligente original.

Partiendo de esta definición germinal, las ulteriores definiciones se podrían clasificar en varios grupos. Un primer grupo de definiciones se centran en el automatismo de su ejecución sin intervención humana, pero haciendo referencia a la figura de “contrato”, “acuerdo” o “promesas”. En esta misma línea, otras, aun haciendo referencia a la dimensión contractual, sin embargo, centran la descripción en la función del código informático.

Por otro lado, se encuentran también aquellas otras propuestas que son más neutras y genéricas sin hacer referencia a las palabras “contrato”, “acuerdo” o “promesas”, definiendo Smart Contract como un simple programa informático que ejecuta órdenes predefinidas cuando ciertas condiciones dentro del sistema son reunidas. O la que resulta más común en los distintos foros, que la define como “una herramienta de código computacional programable (scripts) que se almacenan en una red de blockchain y se ejecuta de forma autónoma. Una tecnología que permite que se realicen uno o varios términos contractuales entre varios agentes que responden a una lógica booleana (si esto, entonces esto)”

De todas estas definiciones, aun con sus diversas aproximaciones, podemos extraer una de sus primeras características que representa un importante punto de partida. Los Smart Contracts están escritos o redactados en un lenguaje código o máquina, no en lenguaje humano, con la finalidad de que un dispositivo pueda ejecutar lo establecido en el mismo.

Desde una perspectiva técnica, se califica de Smart Contract tanto un contrato de opción de compra de acciones cuyo ejercicio se ejecuta automáticamente cuando se produce determinado hito (plazo y/o valor de cotización), como simples archivos que gozan de las cualidades de inmutabilidad o integridad del contenido, pero sin valor contractual en un sentido jurídico. En todos ellos suele concurrir un importante elemento de automatismo en la ejecución de instrucciones (o prestaciones) o incluso en la remediación de un incumplimiento de lo programado. Pero, ciertamente, no todas las situaciones que se describen ampliamente con este término responden a un negocio jurídico autoejecutable.

Por tal motivo, y para abarcar con la mayoría de los supuestos, la definición de un Smart Contract tiene que ser neutra, recogiendo sus características principales, sin perjuicio de que, en alguno de los supuestos, los Smart Contract, puedan tener naturaleza contractual cuando reúna los requisitos que establece cada

ordenamiento jurídico. En este trabajo abordamos precisamente los supuestos en los que el Smart Contract tiene naturaleza contractual representando el acuerdo íntegro o incorporándose como parte de un contrato.

Funcionamiento de un contrato inteligente

Son protocolos autoejecutables que trabajan con *blockchain* para hacer cumplir el funcionamiento de un acuerdo entre las partes mediante tres pasos clave:



La tecnología blockchain permitió la existencia de contratos inteligentes ofreciendo la permanencia y las resistencias incorruptibles provistas en el pasado por la tinta, el papel y la autoridad confiable que certificaba el cumplimiento del contrato.

Con la creación de la blockchain Ethereum, se permitió extender las características funcionales de las blockchains agregando mayor lógica de programación. Esta lógica de programación es la que permite crear contratos inteligentes con un amplio conjunto de reglas y condiciones y luego almacenar el código fuente en su blockchain. Permitiendo la posibilidad de crear infinidad de programas que serán ejecutadas en cada computadora de la red y que tendrán todos los beneficios de la tecnología blockchain.

De acuerdo con la historia progresiva de la tecnología blockchain, el desarrollo del contrato inteligente se puede dividir en tres etapas: en blockchain 1.0, la aplicación representativa es Bitcoin, cuyo contrato se utiliza principalmente para lograr una criptomoneda, y su función es relativamente única. Y RSK (rootstock), la plataforma de desarrollo de contratos inteligentes basada en el ecosistema bitcoin, también necesita ser altamente compatible con Ethereum en la actualidad

En blockchain 2.0, con la aparición del contrato inteligente, DApp (aplicación de descentración) se puede construir en blockchain, mejorando la velocidad de

transacción y el rendimiento del sistema, y diversificando las funciones. De acuerdo con la apertura de blockchain, generalmente se puede dividir en blockchain pública y consorcio (tanto la blockchain privada como la blockchain de consorcio pertenecen a la blockchain de licencia, y la blockchain privada es una forma especial de blockchain de consorcio). Entre ellas, las plataformas de desarrollo más representativas son Ethereum e HyperledgerFabric respectivamente. Con la prosperidad y el desarrollo del ecosistema de la cadena de bloques, las nuevas plataformas de desarrollo continúan logrando avances (como la tecnología de cadena lateral/cadena cruzada, etc.) para resolver los problemas actuales y hacer preparativos completos para la llegada de cadena de bloques 3.0.

En resumen, Ethereum y HyperledgerFabric son representativos en términos de tecnología. Ethereum e HyperledgerFabric son dos plataformas centrales para desarrollar contratos inteligentes en la actualidad, y analizar la arquitectura de su sistema nos ayudará a comprender el principio de desarrollo del contrato inteligente para la cadena de bloques pública y la cadena de consorcios.

En vista de la naturaleza descentralizada de los contratos inteligentes basados en blockchain y la naturaleza de los propios contratos, las aplicaciones de los contratos inteligentes basados en blockchain se pueden dividir en dos categorías desde el nivel técnico:

1.Ethereum. Esta es una plataforma blockchain pública universal y de código abierto con función de contrato inteligente, cuyo contrato punto a punto se procesa a través de su criptomoneda especial Ether (ETH) y Ethereum Virtual Machine (EVM). Se puede utilizar para crear programas descentralizados, organizaciones autónomas y contratos inteligentes, cuyas aplicaciones de objetivos cubren campos como finanzas, IoT, redes inteligentes y cuestionarios deportivos.

2.HyperledgerFabric. Esta es una plataforma modular y de código abierto de clase empresarial con licencia de tecnología de contabilidad distribuida (DLT), que está diseñada para usarse en el entorno empresarial. Proporciona principalmente funciones como la creación de canales y la implementación conectable de diferentes componentes. Fabric tiene una arquitectura altamente modular y configurable, que puede proporcionar innovación, flexibilidad y optimización para las industrias de banca, finanzas, seguros, salud, recursos humanos, cadena de suministro e incluso música digital.

1.10. Tokens

Para comenzar es preciso reseñar que la cadena de bloques no sirve únicamente para generar bitcoin (quizás su uso más conocido, entre otras cosas porque es la plataforma que les da soporte), sino que permite adquirir tokens. Desde

una perspectiva técnica, blockchain se puede utilizar para administrar la transferencia de activos tradicionales tales como acciones, bonos e incluso bienes inmuebles, simplemente al correlacionar los derechos de propiedad con un token respaldado por la cadena de bloques, pudiendo ser intercambiado por cualquier persona con una conexión a Internet en cuestión de segundos.

En el proceso de tokenización, esto es, representar de manera abstracta un valor en correspondencia con el activo real, los empresarios e innovadores han comenzado a darse cuenta del poder disruptivo de la tecnología blockchain y de los tokens. De hecho, en este escenario han cobrado importancia las ICO o Initial Coin Offerings (ofertas iniciales de moneda) como forma de financiación empresarial. Estas venden una serie de tokens a los primeros usuarios a cambio de criptomonedas en una suerte de ronda de financiación alternativa (en tanto en cuanto no es el circuito habitual de los bancos o inversores en capital riesgo), lo que posibilita la captación de fondos para muchas empresas emergentes. Sin embargo, los tokens no son solo una nueva forma de recaudar fondos, sino que suponen una nueva vía de construir ecosistemas.

1.10.1. Definición de token

Un token es “una unidad de valor que una organización crea para gobernar su modelo de negocio y dar más poder a sus usuarios para interactuar con sus productos, al tiempo que facilita la distribución y reparto de beneficios entre todos sus accionistas” (William Mougayar, 2018).

En términos más simples, Se le llama 'token' (en inglés, ficha, como por ejemplo las que se utilizan en las máquinas de juegos) a una unidad de valor basada en criptografía y emitida por una entidad privada en una blockchain, como Bitcoin o Ethereum. Los bitcoins son 'tokens', pero los 'tokens' no solo son criptomonedas, sino que pueden tener muchos más usos.

Los sistemas de tokens en blockchain tienen muchas aplicaciones que van desde submonedas que representan activos como el USD o el oro, hasta acciones de empresas, tokens individuales que representan una propiedad inteligente, cupones seguros infalsificables, e incluso sistemas de tokens sin ningún vínculo con un valor convencional en absoluto, utilizados como sistemas de puntos para incentivos. Los sistemas de token son sorprendentemente fáciles de implementar en Ethereum. El punto clave a entender es que una moneda, o sistema de token, de forma fundamental es una base de datos con una operación: restar X unidades de A y dar X unidades a B, con la disposición de que (1) A tuviera al menos X unidades antes de la transacción y (2) que la transacción sea aprobada por A. Todo

lo que se necesita para implementar un sistema de token es implementar esta lógica en un contrato.

Estas unidades pueden adquirirse a través de blockchain, pero, a diferencia del bitcoin, no nacen de un bloque de la cadena, sino que se crean en la parte superior de la referida cadena, se rigen por un contrato inteligente y sirven para intercambiarse por todo tipo de servicios. Así pues, dentro de una Red privada, un token puede servir para otorgar un derecho, para pagar por un trabajo o por ceder unos datos, como incentivo, como puerta de entrada a unos servicios extra o a una mejor experiencia de usuario.

Actualmente, token y criptomoneda son utilizados como sinónimos. En definitiva, ETH es el token de Ethereum, BTC el de Bitcoin, DAI el de MakerDAO. Podríamos decir que toda criptomoneda es un token, ya que una criptomoneda es una representación de valor. Por el contrario, no todos los tokens son criptomonedas. Podríamos establecer casi un paralelismo con las fichas de un casino.

1.10.2. Clasificación de Tokens

En el campo de las economías y tecnologías digitales, los tokens tienen diversos usos más allá de las criptomonedas:

Como monedas: son los tokens usados para transferir valor entre usuarios de una red. El caso de ETH, el token de Ethereum, es el ejemplo clásico.

Como bienes: cada vez que compramos activos digitales, en realidad compramos un token. Por ejemplo, los CryptoKitties y otros coleccionables.

Como acciones: son los tokens que representan acciones de una empresa tradicional, y que permiten facilitar su trading.

Como recompensas: existen servicios y redes que premian a sus usuarios con tokens. Es el caso de BAT, el token del navegador Brave, browser que bloquea por defecto las publicidades online pero entrega BATs a quienes eligen verlas voluntariamente.

1.10.3. Tipos de Tokens

Currency Token: Mientras que Bitcoin (con mayúscula) refiere a la red, bitcoin (en minúsculas) es la moneda de esa red. Y esos bitcoins ya no tienen un uso restringido a la red Bitcoin: se pueden usar para cualquier transacción cotidiana, como reemplazo del dinero tradicional. Hoy se pueden comprar tickets de avión, zapatillas, o pagar suscripciones a servicios online. En el mundo cripto, a los currency tokens se los llama directamente criptomonedas y en general el concepto de token se usa mayormente para designar a otros tipos.

Utility Token: Son la unidad de cuenta de una red, o sea el símbolo que se usa para medir una cantidad de cierto activo. En el mundo cripto, el utilitario es el tipo más común de tokens usados en ICO. Si bien comparten algunas características con criptomonedas clásicas como las de Bitcoin y Ethereum, también es posible que sólo se puedan usar en la plataforma de la ICO correspondiente. Estos tokens no están diseñados para ser una inversión, más allá de que el auge de su demanda y una limitación de su número puedan disparar su precio.

Security Token: Funcionan como un contrato de inversión, y quienes los compran lo hacen esperando una ganancia actual (en forma de dividendos de una empresa) o futura. Sirven como garantía de propiedad de una porción de la criptomoneda emitida, y ganan y pierden valor acorde a las fluctuaciones de precio de esa moneda. También pueden funcionar como acciones. Son instrumentos diseñados para obtener una ganancia financiera y por eso suelen estar sometidos a regulaciones más estrictas.

Asset Token: Está pensado para representar objetos del mundo real, para facilitar la compra y venta de artículos físicos sin la necesidad de moverlos de un lado al otro. Con un asset token podríamos comprar y vender oro, por ejemplo, sin necesidad de transportarlo. También cabezas de ganado, propiedades, automóviles, juguetes, libros, etc.

Tokens de Gobernanza: A medida que los protocolos descentralizados continúan proliferando y evolucionando, la necesidad de refinar los procesos de toma de decisiones en su entorno es fundamental. Los Gobiernos en la cadena permiten a los interesados, colaborar, debatir y votar sobre cómo administrar un sistema. Los tokens de gobernanza alimentan los sistemas de votación basados en blockchain, debido a que son utilizados a menudo para indicar el apoyo a los cambios propuestos y para votar sobre nuevas propuestas. En el Protocolo Maker, el token de gobernanza es MKR.

Non fungible Tokens (NFT): Arte, videojuegos, música, twits, propiedades, etc. Cada día que pasa se hace más habitual escuchar la cantidad de activos reales llevados a la blockchain para crear NFTs o non fungible tokens. Esta tecnología ha alcanzado su máxima repercusión en los juegos donde los personajes se compran e intercambian por activos que tienen su precio en monedas como ETH. Para entender el fenómeno detrás de los non fungible token es importante que entendamos de qué se trata.

1.10.3.1. NFT

Los NFT (Non-fungible tokens) son artículos digitales únicos, cuya propiedad se gestiona mediante una blockchain. Entre sus ejemplos figuran coleccionables, elementos de videojuegos, arte digital, tickets de eventos, nombres de dominios e incluso registros de propiedad de activos físicos.

Si hay algo claro es que los NFTs no son algo nuevo, dado que existen desde que se creó internet. Pensemos en los dominios de internet o las entradas para eventos que se compran por la web. Ambos casos serían un tipo de NFTs. Lo que si cambio, esto es la esencia de la revolución blockchain es como se conserva el valor de estos activos digitales. A partir de que definimos esto, el activo deja de ser simplemente dato o información y pasa a ser un producto que se negocia en un marketplace.

La mayoría de las discusiones sobre tokens no fungibles comienzan presentando la idea de fungibilidad, que se define como "capaz de reemplazar o ser reemplazado por otro elemento idéntico". Creemos que esto complica demasiado las cosas. Para tener una mejor idea de lo que podría constituir un activo no fungible, solo piense en la mayoría de las cosas que posee. La silla en la que está sentado, su teléfono, su computadora portátil, cualquier cosa que pueda vender en eBay. Todos estos entran en la categoría de cosas no fungibles.

Resulta que los activos fungibles son en realidad los extraños. Una moneda es un ejemplo clásico de un activo fungible. Cien dólares son siempre cien dólares sin importar el número de serie de cada billete específico de cien dólares, o si son cien dólares en su cuenta bancaria. La capacidad de reemplazar un billete de cien dólares por otro billete de cien dólares es lo que hace que la moneda sea fungible.

Volviendo a la discusión sobre la propiedad surge que tenemos toneladas de material digital, pero que simplemente nunca lo hemos poseído. Entonces está claro que ya tenemos toneladas de material digital. ¿Pero hasta qué punto "poseemos" estas cosas digitales? Si la propiedad digital solo significa que un artículo le pertenece a usted y no a otra persona, entonces los posee en algún sentido. Pero si la propiedad digital se parece más a la propiedad en el mundo físico (la libertad de mantener y transferir indefinidamente), este no siempre parece ser el caso con los activos digitales.

Este es el punto principal donde entra la tecnología blockchain. Las cadenas de bloques proporcionan una capa de coordinación para los activos digitales, otorgando a los usuarios la propiedad y el permiso de administración. Las cadenas de bloques agregan varias propiedades únicas a los activos no fungibles que cambian las relaciones de usuario y desarrollador con estos activos. Estas

propiedades son: Estandarización, interoperabilidad, comerciabilidad, liquidez, inmutabilidad y programabilidad.

Estandarización: Los activos digitales tradicionales, desde tickets de eventos hasta nombres de dominio, no tienen una representación unificada en el mundo digital. Es probable que un juego represente sus objetos coleccionables en el juego de una manera completamente diferente que un sistema de venta de entradas para eventos. Al representar tokens no fungibles en blockchains públicas, los desarrolladores pueden crear estándares comunes, reutilizables y heredables, relevantes para todos los tokens no fungibles. Estos incluyen elementos básicos como propiedad, transferencia y control de acceso. Los estándares adicionales (especificaciones sobre cómo mostrar un NFT, por ejemplo) se pueden colocar en capas en la parte superior para enriquecer su visualización dentro de las aplicaciones.

Interoperabilidad: Los estándares de tokens no fungibles permiten que los tokens no fungibles se muevan fácilmente a través de múltiples ecosistemas. Cuando un desarrollador lanza un nuevo proyecto de NFT, estos NFT se pueden ver de inmediato en docenas de proveedores de billeteras diferentes, se pueden comercializar en mercados y, más recientemente, se pueden mostrar en mundos virtuales. Esto es posible porque los estándares abiertos proporcionan una API clara, consistente, confiable y autorizada para leer y escribir datos.

Comerciabilidad: La característica más convincente que permite la interoperabilidad es el libre comercio en los mercados abiertos. Por primera vez, los usuarios pueden mover artículos fuera de sus entornos originales a un mercado donde pueden aprovechar las sofisticadas capacidades comerciales, como subastas, ofertas, paquetes y la capacidad de vender en cualquier moneda, como monedas estables y monedas específicas de la aplicación. Para los desarrolladores de juegos específicamente, la comerciabilidad de los activos representa una transición de una economía cerrada a una economía abierta y de libre mercado. Los desarrolladores de juegos ya no tienen que administrar cada parte de su economía: desde el suministro de recursos, hasta la fijación de precios y los controles de capital. En cambio, ¡pueden dejar que los mercados libres hagan el trabajo pesado!

Liquidez: La intercambiabilidad instantánea de tokens no fungibles conducirá a una mayor liquidez. Los mercados de NFT pueden atender a una variedad de audiencias, desde los más incondicionales hasta jugadores más novatos, lo que permite una mayor exposición de los activos a un grupo más amplio de compradores. De la misma manera que el auge de las ICO de 2017 dio origen a una

nueva clase de activos impulsada por tokens líquidos instantáneamente, las NFT expanden el mercado de activos digitales únicos.

Inmutabilidad y escasez demostrable: Los contratos inteligentes permiten a los desarrolladores colocar límites estrictos en el suministro de tokens no fungibles y aplicar propiedades persistentes que no pueden modificarse después de que se emiten los NFT. Por ejemplo, un desarrollador puede exigir mediante programación que solo se pueda crear un número específico de un elemento específico y escaso, mientras se mantiene infinito el suministro de elementos más comunes. Los desarrolladores también pueden exigir que las propiedades específicas no cambien con el tiempo al codificarlas en la cadena de bloques. Esto es particularmente interesante para el arte, que depende en gran medida de la escasez demostrable de una pieza original.

Programabilidad: Por supuesto, al igual que los activos digitales tradicionales, los NFT son totalmente programables. Los CryptoKitties (de los que hablaremos más adelante) se hornearon en una mecánica de reproducción directamente en el contrato que representa a los gatos digitales. Muchos de los NFT de hoy en día tienen una mecánica más compleja, como forja, elaboración, canje, generación aleatoria, etc. El espacio de diseño está lleno de posibilidades.

1.10.3.2. Estándares para los NFT.

Los estándares son parte de lo que hace que los tokens no fungibles sean poderosos. Brindan a los desarrolladores la garantía de que los activos se comportarán de una manera específica y describen exactamente cómo interactuar con la funcionalidad básica de los activos.

ERC-721

Pionero con los CryptoKitties, ERC721 fue el primer estándar para representar activos digitales no fungibles. ERC721 es un estándar de Smart contract heredable de Solidity, lo que significa que los desarrolladores pueden crear fácilmente nuevos contratos compatibles con ERC721 importándolos de la biblioteca OpenZeppelin. ERC721 también proporciona una forma autorizada de transferir estos activos, utilizando el método transferFrom.

Si lo piensas, estos dos métodos son realmente todo lo que se necesita para representar un NFT: una forma de verificar quién posee qué y una forma de mover las cosas. Hay algunas otras características del estándar (algunas de las cuales resultan ser muy importantes para los mercados de NFT), pero el núcleo de ERC721 es bastante básico.

ERC-1155

ERC-1155, pionero del equipo de Enjin, aporta el concepto de semi-fungibilidad al mundo NFT. Con ERC-1155, los ID no representan activos únicos sino clases de activos. Por ejemplo, una identificación podría representar "espadas", y una billetera podría poseer 1,000 de estas espadas. En este caso, el método `balanceOf` devolvería el número de espadas que posee una billetera, y un usuario puede transferir cualquier número de estas espadas llamando a `transferFrom` con la identificación de "espada".

Una ventaja de este tipo de sistema es la eficiencia: con ERC-721, si un usuario quisiera transferir 1,000 espadas, necesitaría modificar el estado del Smart contract (llamando al método `transferFrom`) para 1,000 tokens únicos. Con ERC-1155, el desarrollador solo necesita llamar a `transferFrom` con una cantidad de 1,000 y realizar una sola operación de transferencia. Esta mayor eficiencia, por supuesto, viene con la pérdida de información: ya no podemos rastrear la historia de cada espada individual.

1.11. ICOs y Airdrops.

1.11.1. ICOs (Initial PublicOffers)

Las ICOs son una forma de financiación de proyectos o de empresas en fases tempranas que presentan una serie de ventajas respecto a la forma tradicional de financiación, ya sea está a través de capital riesgo, de 'businessangels' o incluso haciendo una emisión de acciones.

Las ICOs permiten que una empresa o un proyecto que se va a desarrollar haga una preventa de derechos sobre ese proyecto; esto significa que en el momento en el que se está planeando el proyecto, se propone a aquellas personas que podrían financiarlo, que compren derechos. Estos derechos pueden ser o bien de utilización de la infraestructura que se va a montar, o bien derechos económicos; es decir, que cuando haya beneficios, los inversores obtienen una parte. Esa financiación es la que permite financiar el proyecto.

Con ICOs la empresa hace una emisión. ICO significa 'initial coin offering' en inglés; es decir, una oferta original de monedas. Pero estrictamente lo que se emite no son monedas, sino lo que podríamos considerar como fichas o 'tokens' criptográficos, que son los que dan acceso a la infraestructura que se va a armar con el proyecto. Normalmente esto permite que cualquier inversor en cualquier parte del mundo pueda pagar en bitcoins o en 'ethers', que son criptodivisas públicas, para contribuir al proyecto.

La aparición del ICO como parte de la criptoeconomía, que a veces también se denomina ITO (sustituyendo la C de Coin por la T de Token), está redefiniendo completamente el valor de la empresa tradicional hacia un modelo basado en una

comunidad y un ecosistema. Y eso es posible gracias a la tokenización que podría crear parte de esa nueva economía descentralizada. La gran mayoría de los proyectos que realizan una ICO intentan vender “utility tokens” en lugar de acciones en sus empresas, lo que conlleva a veces un vacío legal. Los organismos reguladores de cada país todavía tienen problemas para clasificar esta nueva clase de activos que no necesariamente genera ganancias. En cualquier caso, es importante hacer las preguntas correctas antes de considerar una inversión en una ICO.

1.11.2. Airdrops

Un airdrop implica la distribución gratuita de tokens nativos por parte de los emisores a usuarios nuevos o existentes de su plataforma, antes o simultáneamente con la oferta de ICO. Es una forma innovadora para que una empresa promueva su producto/servicio a través de participantes activos en lugar del marketing tradicional a través de proveedores de servicios profesionales.

El objetivo principal de los lanzamientos aéreos es impulsar la creación de una comunidad de poseedores de fichas antes o junto con la ICO, o impulsar los efectos de red de las redes ya creadas. Los lanzamientos aéreos se utilizan con fines de marketing; para dar a conocer un nuevo token; atraer a más participantes a la emisión; pero también recompensar a los participantes/poseedores de fichas existentes por su lealtad, su participación activa en la red o por compras al por mayor.

Como la mayoría de los lanzamientos aéreos involucran tokens que aún no se comercializan en mercados secundarios, los titulares de dichos tokens gratuitos no pueden intercambiarlos y retirarlos. Los titulares de tokens pueden beneficiarse del uso del token (acceso a un servicio/producto) o esperar a que el token se vuelva líquido para negociarlo.

En muchos casos, los tokens distribuidos en lanzamientos aéreos se distribuyen aleatoriamente mediante el uso de contratos inteligentes que envían estos tokens gratuitos a billeteras activas. En algunos casos, los airdrops pueden generar consideraciones financieras de protección del consumidor, cuando los utilizan los estafadores que engañan a los usuarios para que revelen sus claves de billetera privadas para recibir tokens gratuitos. La evidencia anecdótica sugiere que los lanzamientos aéreos también pueden usarse como una forma alternativa de proporcionar acceso a tokens en países donde las ICO están prohibidas.

Capítulo II: “CASOS DE USO”

2.1. Introducción

Todo es blockchain. O al menos, todo lo será. Resulta relativamente sencillo llegar a esa conclusión a partir de una sencilla revisión de las noticias: a lo largo de los últimos meses, sin ir más lejos, podemos encontrar menciones sobre el papel fundamental y crucial de esta tecnología en las empresas de generación de energía, en la redefinición de la industria de la música, en la seguridad de la cadena de conservación de alimentos en distribución, en el futuro de la industria aseguradora, en el sector inmobiliario, en la eliminación de la corrupción en la política o, por supuesto, en la banca, entre muchas otras. Blockchain se ha convertido en la tecnología de infinitos usos, en el elemento a incorporar a todos los procesos, y en el cimiento sobre el que se edificará todo nuestro futuro. No importa a qué se dedique, su nivel de responsabilidad o la compañía para la que trabaje: de una manera u otra, puede estar seguro de que muchos de los elementos que manejará en su relación con el mundo estarán contruidos sobre la base de la tecnología blockchain.

Resulta evidente que cada vez son más los avances que se dan en torno a la aplicación de la tecnología blockchain y más las nuevas oportunidades que genera en el ámbito del sector público.

El diseño de una estrategia digital fundamentada en blockchain que permita adoptar de manera sostenible en el tiempo la gestión pública resulta fundamental para lograr un programa de transformación que facilite la identificación de los retos inmediatos en este sector y lograr una mayor eficacia, eficiencia y agilidad de las instituciones. Todo ello, con el fin de poder crear las estructuras y funciones necesarias para dar respuesta a las necesidades de los ciudadanos en una nueva fase de la gestión pública después de la implantación de la administración electrónica.

2.2. Gobierno Abierto

Atendiendo a las propias características de la tecnología blockchain y a la gran diversidad de aplicaciones que puede ofrecer, no resulta extraño que el uso de esta herramienta tenga sus efectos positivos para su utilización en la implantación de un nuevo modelo abierto de gestión pública.

Especial relevancia adquieren las aportaciones de mejora que esta tecnología puede suponer en el diseño e implementación de un programa de Gobierno Abierto. Entendido este como un conjunto de actuaciones puestas en marcha por la Administración tendentes a potenciar la colaboración de los ciudadanos en una mejor prestación de los servicios públicos, con un modelo de gestión que apuesta por la transparencia y la rendición de cuentas en la gestión de los asuntos públicos.

Esta nueva realidad requiere un análisis sistemático y actualizado de las principales cuestiones que se dan en el contexto de esta tecnología que está llamada a convertirse en un elemento central para aplicar un nuevo modelo de gobernanza. La blockchain como tal no puede ser regulada ya que solo se pueden regular aquellas actividades que se sirven de ella. Asimismo, la falta de consolidación de las iniciativas basadas en ella hace que todavía no contemos con una regulación específica de las actividades que se fundamentan en esta herramienta en los distintos ámbitos de aplicación.

En todo caso, a la hora de lograr una adecuada aplicación de la blockchain en el ámbito de un proyecto de Gobierno Abierto se requerirá un sistema que permita construir un modelo de gestión pública que garantice los siguientes aspectos:

Transparencia: el principio de transparencia es uno de los pilares estratégicos en torno al cual se configura un modelo de Gobierno Abierto. La transparencia está directamente relacionada con el deber de los poderes públicos de poner a disposición de los ciudadanos la información y los datos relacionados con su gestión. En este sentido, hay que destacar el interés de los legisladores por incrementar los niveles de transparencia en la actividad pública, incorporando a su marco jurídico nacional una legislación adecuada en materia de transparencia y buen gobierno como ejes fundamentales de toda acción política para mejorar la reputación y credibilidad de la Administración.

La tecnología blockchain permite brindar a todas las operaciones un adecuado sistema de registro que facilita su consulta y su seguimiento a través de la red, favoreciendo un cambio en el ejercicio de la práctica institucional que promueva la aplicación de un sistema efectivo de controles y equilibrios fundamentados en la mayor información facilitada por la Administración Pública. A través de dichos registros, se creará una identidad digital propia de cada elemento u operación que permitirá conocer su historia y realizar su seguimiento en función de los niveles de transparencia que se establezcan y los permisos que se otorguen.

Participación: la participación de los ciudadanos en los asuntos públicos debe ir más allá del ejercicio del derecho al voto cada cuatro años, configurándose un sistema de democracia donde se establezcan espacios participativos y colaborativos. A través de un sistema de acceso sencillo y libre a la información de gobierno se podrá impulsar la participación de los ciudadanos como elemento clave de este modelo de gobernanza basado en la democratización de la información.

El uso del blockchain permitirá aportar modelos innovadores de intercambio de información pública a través de mecanismos que hagan que esta esté disponible

en formatos abiertos y accesibles con el fin de incrementar la participación ciudadana. Precisamente uno de los ámbitos en los que puede desarrollar su efectividad el blockchain es en el ámbito de los procesos electorales mediante el diseño de una metodología electoral automatizada que ofrezca las suficientes garantías de seguridad, inmutabilidad y transparencia que permita a los electores emitir su voto reduciendo costes e incrementando las garantías de fiabilidad.

A diferencia de lo que ocurre con los procesos electorales con votación electrónica que presentan grandes riesgos de vulnerabilidad que afectan a los derechos de seguridad, de privacidad, o de protección de datos, con este procedimiento innovador basado en blockchain, el sufragio de los ciudadanos no se encontrará incorporado en un archivo concreto susceptible de ser intervenido y manipulado, sino que el voto se encontrará replicado en una multitud de nodos que se encargarán de su verificación y validación proporcionando amplias garantías de seguridad y transparencia.

Trazabilidad: directamente relacionado con el principio de transparencia y rendición de cuentas en la Administración, el blockchain permitirá garantizar que la información facilitada no ha sido modificada, que no se ha eliminado ningún documento y que las distintas fases de un procedimiento se han desarrollado correctamente, facilitando, a través de este encadenamiento, mayor control y transparencia en los procesos de gestión.

Seguridad: este nuevo modelo de gestión burocrática ofrece mayores garantías de seguridad ya que asegura que la información incorporada a los registros no haya sido alterada, otorgando integridad a los datos y confianza a las partes al estar distribuida en multitud de nodos. Este sistema con todas las garantías de seguridad se fundamenta en el uso de algoritmos criptográficos y en la descentralización que ofrece el uso del blockchain.

Teniendo en cuenta las iniciativas que están siendo exploradas en el sector público en la región y en función de los atributos de la tecnología, pueden identificarse cuatro grandes categorías en donde podría pensarse que una tecnología como blockchain podría ser de utilidad para el sector público: (i) desintermediación de la información, (ii) tokenización de activos, (iii) automatización de procesos e (iv) interoperabilidad.

1.Desintermediación de la información: En muchas instancias la generación de información en el sector público se basa en una cadena de procesos compuesta por distintas personas o entidades. A través de la tecnología, la información puede registrarse de manera segura y confiable, convirtiendo a la red en una especie de notariada digital de datos y transacciones. Potencialmente, el incluir estos procesos

en una cadena de blockchain permitirá prescindir de algunos de estos intermediarios, aumentar la trazabilidad de cada etapa del proceso de manera confiable y reducir costos tanto en tiempo como en recursos.

2. Tokenización de activos: El uso de la tecnología puede permitir expresar distintos activos como fichas (tokens), de manera que se los pueda representar de manera digital y así contar con un registro confiable de los cambios de propiedad (o de localización, en el caso de cadenas de producción o de distribución). Esta característica también permite la posibilidad de atomizar la propiedad de un solo activo entre muchos propietarios.

3. Automatización de procesos: Una ventaja de la inscripción de contratos inteligentes en un registro distribuido es la posibilidad de automatizar procesos a través del establecimiento de reglas que deberán cumplirse para que se realice cierta acción (ejecución del contrato) de manera automática sin intermediarios de confianza. El pago automático de transferencias condicionadas cuando se cumplen condicionalidades predefinidas, el cobro de bienes y servicios después de haber sido entregados o el hacer cumplir diversas regulaciones pueden traducirse en reglas incluidas en contratos inteligentes.

4. Interoperabilidad: Uno de los principales retos para la prestación integrada de servicios de gobierno es la necesidad de conectar los distintos sistemas de las entidades públicas y privadas de forma segura y confiable. El uso de blockchain para la certificación de información ciudadana puede permitir que sean los mismos ciudadanos los que ayuden a que los distintos sistemas operen entre sí sin la necesidad de que estén integrados, otorgando en tiempo real los permisos necesarios para que su información personal pueda ser accedida por distintas entidades. Este enfoque tiene además la ventaja de permitir una mayor trazabilidad en el acceso de información personal del ciudadano.

2.3. Impacto de las cadenas de bloques en la actividad tributaria

Teniendo en cuenta que el presente documento tiene como destinatario específico a la Secretaria de Finanzas e Ingresos Públicos y Política Fiscal de la Provincia de Santa Fe, en este apartado se va a tratar el impacto que las cadenas de bloques se espera que tengan en materia de tributación.

Como ya mencionamos anteriormente, los beneficios potenciales de la blockchain, tanto para las empresas como para los gobiernos han -y siguen- sido estudiados y tienen movilizadas a ambas partes. También resaltamos que, que las cadenas de bloques están transformando la forma en que intercambiamos valor. Y, siendo el valor intrínseco de las cosas, el objeto de la tributación, es indudable que la nueva tecnología tendrá un fuerte impacto en ella.

Vimos, además, que la blockchain conlleva un cambio paradigmático en la forma de hacer transacciones, al eliminar la necesidad de un intermediario, proporcionando un libro mayor de transacciones seguras y distribuidas en una red. Además de permitir rastrear transacciones y verificar información, la blockchain puede integrar la lógica empresarial en una transacción, mediante el uso de contratos inteligentes. Se han identificado los siguientes atributos de la blockchain que tienen un potencial significativo en el área de impuestos (PricewaterhouseCoopers LLP, 2016):

- Transparencia: la blockchain proporciona procedencia, trazabilidad y transparencia a las transacciones.

- Control: el acceso a redes autorizadas está restringido a usuarios identificados

- Seguridad: el libro de contabilidad digital no se puede modificar ni alterar una vez que se ingresan los datos. El fraude es menos probable y más fácil de detectar.

- Información en tiempo real: cuando la información se actualiza, se actualiza para todos en la red al mismo tiempo. Estos atributos echan luz sobre las áreas de la tributación que se verán afectadas por la nueva tecnología.

Así, es posible afirmar que, además de la incidencia de la blockchain en la materia tributaria propiamente dicha (esto es, en el objeto imponible, en la forma de determinarlo, en cambios ineludibles en los conceptos de territorialidad, residencia, atribución de utilidades, sujeto imponible, etc.) también ocasionará un cambio radical en la forma de liquidar y pagar impuestos (claramente, blockchain jurará un rol fundamental en la implementación, en tiempo real, que permita la automatización de los procesos impositivos para pequeñas y grandes empresas), en los procedimientos, en la lucha contra el fraude impositivo y, muy especialmente, en las administraciones tributarias.

Resultará ineludible una reorganización de la contabilidad y de la forma en que se liquidan y procesan los pagos de los impuestos; y en ambas esferas la forma en que tales cambios se lleven a cabo dependerá de la voluntad de los Estados, fuertemente condicionados por la tecnología y por el resto de los países. También deberán ser rediseñadas las Bases de Datos nacionales (registros de personas, de propiedades, etc.) y los sistemas de red disponibles (interacción entre tales registros y las entidades gubernamentales, y de éstos con el fisco, los organismos de contralor, las entidades financieras, entidades aseguradoras, mercado de valores, consumidores, comunidad en general, profesionales, etc.).

Puede preverse, entonces, también repercusión en el sistema legal, reformando las leyes sobre bases de datos, propiedad intelectual e identidad legal. En esta Sección trataremos de analizar cada una de las áreas tributarias que se verán afectadas por la tecnología, las que, en principio, puede clasificarse en 6 áreas.

2.3.1 Áreas de impacto de blockchain en materia tributaria

Área de Conceptos Legales-Tributarios Básicos: De lo expuesto anteriormente puede deducirse cambios en algunos conceptos conocidos pero cuya definición deberá ser revisada, al menos en materia de tributación. Entre ellos, podemos mencionar:

- “Bien” objeto del impuesto (sólo bienes reales o también los tokens): en un mundo Blockchain, gran parte de lo que se transaccionará serán representaciones digitales de activos reales. La traslación de la cosa, si fuere necesaria, se efectuará con absoluta independencia de la transacción en sí misma, que terminará con la entrega o puesta a disposición del token correspondiente.

- “Transacción” alcanzada por el impuesto: esta definición debería comprender cuando se inicia y finaliza la transacción y el valor del objeto transaccionado, la forma de conversión de cualquiera sea la moneda en que se haya pagado (monedas virtuales o reales) a la moneda de la contabilidad y/o liquidación.

- Residencia: tomando en cuenta la característica de anonimato de la blockchain.

- Territorialidad: puesto que, dependiendo del tipo de blockchain, puede no ser posible determinar el o los lugares donde se obtiene la renta.

- Pago: si es con monedas virtuales o tokens o sólo con monedas fiduciarias

- Persona o sujeto del impuesto: porque los sujetos involucrados no necesariamente serían personas físicas o jurídicas. En los contratos inteligentes, por ejemplo, la transacción se efectuaría de forma automática sin intervención de sujeto -como hoy lo entendemos.

- Renta: ¿comprende la ganancia obtenida en la transacción de tokens únicamente, o también la porción -si la hubiere- de diferencia de valor entre token y bien real?

Área Materia Imponible: En este punto, el autor Seco advierte sobre la posibilidad de ampliar el alcance de los tributos que hoy conocemos como consecuencia del cambio que implicará, en la forma de transaccionar, el desarrollo de la Internet de las Cosas (IoT, Internet of Things) sobre una blockchain. El autor se pregunta si “con billones de dispositivos inteligentes participando de una red

global, desde neveras y cocinas hasta automóviles y barcos, [donde] se antevé un conjunto de aplicaciones maravillosas en distintas áreas... [puede asegurarse que] estos dispositivos pasarán por varios cambios de status desde su fabricación (incluyendo cambio de propietario, upgrades, etc.) y algunos de estos cambios pueden ser de interés tributario” (Seco, 2017). Si bien es probable que la trazabilidad permita reducir las prácticas fraudulentas y minimizar la evasión y, con ello, aumentar la recaudación global, también es cierto que el nuevo paradigma que la economía digital viene mostrando no pone el foco en ese aspecto sino en la posibilidad de ampliar la base imponible y en redistribuir las ganancias obtenidas. Y esto está en línea con lo que Seco anticipa: la simplicidad del modo de transaccionar en el marco de la Economía Digital, traerá como externalidad positiva un aumento de tales transacciones, varias de las cuales podrán ser objeto de materia imponible si pueden ser captadas y alocadas. Una rama de la tributación que se verá fuertemente incida por la nueva tecnología será la de Precios de Transferencia (TP). Hoy en día, las leyes que regulan los TP son diferentes para cada país, y se exige que las transacciones transfronterizas entre partes relacionadas cumplen con el principio Arm's Length. Los Informes de TP son voluminosos, tediosos de hacer y de leer, y muchas veces resulta difícil demostrar que el precio negociado es el de mercado. Al respecto un Informe de Deloitte expone, con claridad, como el régimen de TP podría verse beneficiado si se aplica TB:

TP Tradicional	TP basado en TB
Fuerte dependencia de los documentos internos de la empresa y la correspondencia para definir el papel de cada parte involucrada.	Un libro mayor distribuido de Blockchain que facilita el seguimiento del flujo de transacciones e identidad de todas las partes involucradas.
Los acuerdos intra empresariales se ejecutan manualmente.	Los acuerdos son escritos en un contrato inteligente de ejecución automática.
Alto riesgo de falsificación de documentos de transacción.	Todos los movimientos en Blockchain tienen una marca de tiempo y sellados criptográficamente, eliminando la posibilidad de manipulación.
Todo el sistema depende en gran medida de los documentos en papel y datos almacenados en muchos servidores para rastrear la cadena de suministro.	Cada información se almacena en Blockchain y es visible para las partes que tienen acceso a Blockchain.
El seguimiento de los pagos se basa en ERP.	Los pagos se ejecutan mediante un contrato inteligente si cumplen con las condiciones especificadas.

Fuente: (Deloitte, 2017)

La repercusión de la blockchain en los TP será de tal magnitud, que resulta aún hoy difícil de cuantificar. Si resulta claro que generará una importante reducción de tiempos y costos, más allá de la realocación de renta entre las jurisdicciones.

Área Recaudación y liquidación de Tributos: Entre los usos que se prevén de la blockchain, se incluyen varias en el área gubernamental, tales como el registro de bienes, identidad ciudadana, cadenas de suministro, registros médicos, etc. Todos estas implementaciones tendrán impacto en la forma en que los sujetos liquiden y paguen sus impuestos: algunos permitirán liquidaciones automáticas - como la de los bienes registrables-; otros permitirán de forma automática determinar los responsables sustitutos y complementarios en materia impositiva; la integración e interconexión con otras bases de datos confiables a través de blockchain dará lugar poder deducir automáticamente gastos computables; también será posible integrar las contribuciones a la Seguridad Social con todo el esquema impositivo, y los sistemas de salud y previsional, cuyos beneficios podrán direccionarse mediante contratos inteligentes una vez que las condiciones predefinidas se hayan cumplido. La característica de blockchain de prescindir de intermediarios para dar certeza a

las transacciones llevará, también, a un cambio en la forma de pago de los impuestos y a una reducción de los costos involucrados en el proceso de pago (certificaciones, garantías, seguros, etc.). Otro aspecto de seguro impacto será el del pago de los tributos. Especialistas de tecnología y estudiosos prevén que los gobiernos iniciarán, en promedio, la cobranza de tributos utilizando blockchain para el 2023; esto es, dentro de 1 año. Pagar y cobrar impuestos disminuirá los costos de transacción, agilizará los tiempos y reducirá, inevitablemente, los montos de intereses. Todo el proceso de devoluciones de impuestos debería ser inmediato, gestionado por contratos inteligentes. Así se habla, por ejemplo, de que “la responsabilidad por cobrar impuestos sobre ventas o ingresos puede, posiblemente, cambiar completamente desde las autoridades tributarias hacia los mismos participantes de la economía compartida” (Seco, 2017). Con relación a las Contribuciones a la Seguridad Social, la implementación de una blockchain basada en una situación donde los empleadores no necesitarán actuar como intermediarios, responsables del cálculo y transferencia de tales recursos, permitirá no sólo digitalizar el proceso sino también evitar duplicaciones de registros, con el consiguiente ahorro de costos, detección de duplicaciones, inconsistencias, etc., facilitando auditorías permanentes tanto de la parte impositiva como de salud y previsional, y no sólo a nivel de empleados sino también de empleadores, de organismos públicos y de entidades de salud. En otro orden, merece destacarse el énfasis que se ha puesto a la utilidad que la blockchain puede tener para ayudar a racionalizar y automatizar los impuestos indirectos, al establecer de forma segura el qué, el dónde y el cuándo de las transacciones. Incluso se está evaluando si los libros de contabilidad distribuidos pueden eliminar la necesidad de facturas; si es posible utilizar a las criptomonedas para pagar y cobrar reembolsos de IVA; y si las declaraciones de aduanas pueden ser presentadas automáticamente no por agentes de aduanas sino por portacontenedores (EY, 2018). El motivo se debe a que la definición de una cadena de bloques a menudo recuerda los impuestos indirectos. Estos impuestos incluyen impuestos generales sobre el consumo, como el IVA, el impuesto sobre bienes y servicios y los impuestos a las ventas, pero también los aranceles aduaneros, los impuestos especiales a la energía y los impuestos ambientales. Estos impuestos a menudo siguen cadenas de transacciones y su hecho imponible, y la obligación tributaria consiguiente, a menudo son "activadas" por eventos clave que deben documentarse y registrarse de forma segura. Estos eventos incluyen la prestación de un servicio o la entrega de bienes, la celebración de un contrato, la fabricación de un producto y por un acto de importación o exportación de bienes y servicios. Cómo, dónde, cuándo y qué

impuesto se aplica a menudo depende de decisiones complejas que deben aplicarse correctamente para cada transacción. La recaudación de la cantidad correcta de impuestos depende de la presentación honesta de información precisa, a menudo en "tiempo real". Los errores de los contribuyentes, la contabilidad negligente, la falta de datos y la actividad fraudulenta pueden tener un impacto significativo. Vemos entonces que la blockchain parece haber sido diseñada para servir de soporte y hacer más fácil y eficiente a los impuestos indirectos. El Informe EY resalta, que la factura es el documento de IVA más crítico. Y se sugiere que, en un régimen basado en Blockchain, es probable que para que una factura con IVA sea válida, se requerirá una huella digital, derivada del proceso de consenso de Blockchain con IVA. La huella dactilar confirmaría de inmediato que el bloque bajo escrutinio está permanentemente vinculado a los bloques anteriores y posteriores. Toda la historia de la cadena comercial (hacia adelante y hacia atrás desde esta transacción) podría ser seguida y analizada por un funcionario de impuestos en una oficina, por un robot o por un oficial de aduanas en una frontera. Cualquier persona conectada a un programa de auditoría fiscal aprobado podría detener inmediatamente toda la cadena comercial de un artículo de una factura válida (EY, 2018). Con respecto a las Declaraciones de aduanas y los controles de exportación, que dependen de información detallada y precisa para probar el origen y el destino de las mercancías, su uso final y su composición o clasificación, no solo para garantizar el pago correcto de los aranceles, sino también para cumplir con las regulaciones que prohíben el comercio ilegal o sustancias peligrosas, el Informe EY destaca que la veracidad y confiabilidad de esta información es vital, pero la certeza puede ser difícil de lograr ya que los detalles necesarios a menudo son proporcionados por terceros, y pueden extraerse de una variedad de sistemas dentro de una organización. Los errores pueden conducir a sanciones, oportunidades perdidas y demoras costosas en la transferencia de mercancías a través de las fronteras. Además, a menudo es difícil para los comerciantes y agentes de aduanas proporcionar información suficiente o pruebas documentales para beneficiarse de posibles reducciones o reducciones (como las disponibles a través de un acuerdo de libre comercio, por ejemplo). Sin embargo, si los artículos se comercializaran en una cadena de bloques y las autoridades aduaneras tuvieran acceso a la cadena, podrían verificar con total precisión el origen y la naturaleza de los productos en cada etapa de la cadena. Y esto no solo se aplicaría a los productos terminados, sino también a las materias primas, componentes y productos semi acabados. Las autoridades aduaneras podrían, por ejemplo, cobrar derechos automáticamente a medida que las mercancías transitan a través de las fronteras,

eliminando las declaraciones de terceros. Y como esta tecnología les permitiría verificar cada aspecto de 80 un envío con certeza, podrían mantener la seguridad de la cadena de suministro con menos oficiales que pudieran enfocar sus inspecciones con mayor precisión (EY, 2018). El avance logrado en materia de factura electrónica se traduce en un primer paso hacia la digitalización del proceso.

Área Procedimientos Tributarios: Una de las características de blockchain es el de la de inmutabilidad, que implica que toda la información que se vuelca no solo no se puede modificar sino tampoco eliminar; es decir, nada puede revertirse y por tanto proporciona prueba irrefutable del estado de cualquier información volcada en la red en un momento en el tiempo. Con la característica de inmutabilidad de los datos que surjan de transacciones en blockchain, estos datos se prueban por sí mismos, por lo que es de esperarse que la etapa de prueba en los procedimientos administrativos y contenciosos tiendan a simplificarse enormemente. Ya no sólo no será necesario acompañar prueba documental apropiada (basta con informar los “enlaces” o ubicación en la red de tales datos) sino que, si en la medida en que a través de la propia red blockchain sea posible -con las medidas de seguridad y permisos del caso- acceder a otras bases de datos (de fiscos, las entidades bancarias, las entidades aseguradoras, las entidades de contralor de las sociedades, los datos personales de las personas, el registro de sus propiedades, etc.) pruebas como acreditación de personería, Certificación de Balances Contables, Liquidaciones de Impuestos presentadas, Toneladas exportadas, fecha de adquisición o realización de propiedades, movimiento de fondos, etc., todo podrá ser consultado en la red Blockchain bastando su sólo existencia en la red para que el dato quede probado. También mencionamos que la descentralización, junto a la inmutabilidad nos permite realizar una trazabilidad de todas las transacciones que se producen en la red. Esta, en lo que aquí interesa, viene a facilitar enormemente el trabajo de los organismos de revisión, sin contar con la reducción de costos e incremento en la velocidad y cantidad de respuestas que ello conllevaría. La característica de descentralización puede repercutir en materia tributaria en aspectos tales como la confidencialidad y el blanqueo de capitales, al punto que se están observando iniciativas legales que buscan proteger al ciudadano en general y al contribuyente en particular de los datos que, en cumplimiento de obligaciones legales, los llevan a informar datos personales que deben ser protegidos de ser divulgados a terceros, nacionales o internacionales. Y en este contexto, se comienza a hablar de nuevos conceptos jurídicos como son los de Responsable de Tratamiento de Datos Personales (RTDP), Encargado de Tratamiento de Datos Personales (ETDP, que actúan por cuenta de terceros responsables de tratamiento)

y Transferencias internacionales de Datos Personales. Estos dos sujetos -que, como vimos, pueden ser personas físicas y/o jurídicas- jugarán un rol esencial en materia de procedimiento tributario por cuanto serán ellos la puerta de entrada a ciertos datos que necesitará la autoridad de revisión y que no estarán disponibles para el público en general en la red. A su vez, el concepto de Transferencia Internacional de Datos Personales además de su sentido jurídico tiene una clara arista económica que, más allá de estar regulada de forma adecuada para que no sea objeto de comercio, es probable que esté alcanzada impositivamente en un esquema de sanciones y multas. Por último, respecto de los Contratos Inteligentes, cualquier procedimiento tributario que involucre lidiar con tales instrumentos deberá tener la capacidad técnica para poder comprender su código y las variables detonadoras de sus cláusulas.

Área Administración Tributaria: La blockchain, por sus características intrínsecas, tiene conquistada a las Administraciones Tributarias tanto como al sector privado; aunque por distintos motivos. La blockchain será de valor para las autoridades fiscales y para los reguladores porque proporciona información precisa que puede ser utilizada para la autoliquidación de los impuestos y para facilitar la recaudación y la supervisión anticipada de los impuestos relacionados con las transacciones. Por ello, las administraciones -y los gobiernos- tienen tanto interés de entender, manejar, y facilitar el desarrollo y crecimiento de la tecnología en áreas hasta hoy no previstas. Seco advierte que se puede pensar en aplicaciones que requieran la coordinación de acciones entre administraciones tributarias, entre administraciones tributarias y contribuyentes y entre órganos internos de una Administración Tributaria (Seco, 2017). Y esto, con blockchain de los tipos privados o federadas puede ser realizado en forma segura (respetando el principio de confidencialidad y el secreto fiscal), rápida y sin intermediarios ni necesidad de pruebas de veracidad. Los expertos también anticipan el advenimiento de las llamadas Auditorías inteligentes, en las que, utilizando plataformas con blockchain las administraciones de impuestos indirectos podrían llevar a cabo análisis de riesgo independientes facilitados por inteligencia artificial. Debido a que el régimen de blockchain de impuestos indirectos probablemente estaría vinculado a otras fuentes gubernamentales, los auditores podrían tener acceso inmediato a grandes cantidades de bases de datos públicas y privadas y grandes cantidades de contribuyentes y datos comparativos. Las anomalías estadísticas podrían identificarse en tiempo real y las autoridades pertinentes (incluidas las de otros países) podrían recibir alertas (EY, 2018).

El Secreto Fiscal y la blockchain, uno de los aspectos normativos que necesitarán adaptarse es aquel vinculado al acceso a la información impositiva y aduanera, en tanto que la blockchain implica un uso compartido de la información entre múltiples usuarios, de modo ilimitado y en tiempo real. En Argentina, por ejemplo, las declaraciones juradas, manifestaciones e informes que los responsables o terceros presenten a la AFIP son secretos y excluidos del derecho al acceso a la información pública conforme lo dispone el art. 101 de la ley 11.683. Al respecto la Corte Suprema estableció que “el secreto de las declaraciones juradas no ha sido establecido... en beneficio del Fisco, sino de los contribuyentes o terceros que podrían ser afectados o perjudicados por la divulgación de aquellas circunstancias sobre la cual incumbe pronunciarse a los tribunales”. Ello conduce a pensar que, en caso de utilización de blockchain, en el futuro, las únicas limitaciones al acceso o a la obligación de no divulgación deberían focalizarse en aquellos datos que pudieran generar perjuicio o desmedro a los propios operadores y no simplemente – en términos generales- a cualquier información “fiscal o aduanera digital”. En el caso de Blockchain, los datos se enviarían no sólo a los entes fiscales, sino también a otros sujetos públicos y privados (humanos y empresas). Por otra parte, cualquier intento de restricción, sería absolutamente impensable, dado que la atomización de los datos entre los diversos operadores de la cadena (nodos) ubicados en múltiples puntos del planeta impediría cualquier regulación vinculada al secreto del contenido recibido. Claramente, el tema del Secreto Fiscal -al igual que la Protección de Datos Personales debe ser evaluado y resuelto antes de cualquier implementación de blockchain en las Administraciones Tributarias.

Área Lucha contra el fraude: Se ha dicho en varias oportunidades que la blockchain es a prueba de manipulaciones. Si bien la inviolabilidad es una característica intrínseca de la blockchain, esto no impide que, desde un inicio, no ingrese información falsa a Blockchain (PwC, 2019). Por tanto, es ahí donde habrá de ponerse mayor énfasis en lo que a control se refiere, entendiendo que, en definitiva, ningún sistema puede prevenir el comportamiento fraudulento por completo. Sin embargo, la blockchain hace que el fraude y los errores sean mucho más fáciles de detectar porque el sistema proporciona información transparente sobre transacciones y nodos en la red. Por ejemplo, se podría rastrear si se ha pagado el IVA y dónde se ha pagado y, al hacerlo, reducir el fraude del IVA. Blockchain también podría ayudar a impulsar el cambio de comportamiento debido a los riesgos y las consecuencias del incumplimiento. Es más probable que lo atrapen y lo excluyan para siempre de la red Blockchain (PwC, 2019). Otra externalidad positiva que traería aparejada el uso de la TB es que, al tratarse de

nodos y transacciones sin importar la envergadura de los primeros ni el monto de los segundos, facilitará a las micro y pequeñas empresas el cumplimiento de sus obligaciones tributarias, a la vez que les dará mayor visibilidad ante las autoridades fiscales, pudiendo ayudar así a reducir la brecha fiscal. Por último, el Informe de EY destaca que el uso de información verificable y disponible de forma inmediata podría permitir a los contribuyentes respaldar los reclamos por deducciones de IVA, impuestos a los bienes y servicios y descuentos y exenciones aduaneras. Los reclamos fraudulentos e incorrectos para deducciones de impuestos al ingreso representan una grave amenaza para muchos sistemas de IVA e Impuestos a los Bienes y Servicios. Estas demandas pueden crear obligaciones de cumplimiento significativas para los contribuyentes y los comerciantes transfronterizos. La velocidad, la precisión y la transparencia de las cadenas de bloques podrían ayudar a aliviar estas cargas para los contribuyentes al disminuir el riesgo de fraude.

2.4. Aplicaciones.

En el apartado 2.4. se presenta una visión general de las posibles aplicaciones de blockchain, haciendo énfasis en casos de estudio específicos asociados a diversos sectores del Estado.

El sector gobierno puede verse beneficiado con el uso de Blockchain porque con su uso se pueden obtener múltiples ventajas como ahorros de tiempo en trámites, uso de cero papeles, trazabilidad en la gestión contractual, seguimiento de la entrega de los subsidios, lucha contra el fraude como ya mencionamos con anterioridad.

A continuación, se describe casos específicos de uso en el sector gobierno.

2.4.1. Aplicaciones – Sistemas de Votación.

La tecnología blockchain se puede utilizar para realizar procesos de votación transparentes. Con un sistema de votación sobre blockchain se puede eliminar muchos intermediarios; actualmente se selecciona a personas naturales para que ejerzan como jurados, sin verificar un perfil y sin comprobar una capacidad específica para ejercer el cargo, y son seleccionados aleatoriamente miles de jurados. Usando Blockchain cada ciudadano puede enviar su voto anónimo a la cadena de bloques, además, los resultados de las votaciones al quedar registrados no se pueden modificar. Esto elimina la sobrecarga considerable del entorno de votación, desde la preparación hasta la tecnología, el personal y los recuentos (Kakavand, Kost De Sevres, & Chilton, 2017).

2.4.2. Aplicaciones – Contratos Inteligentes.

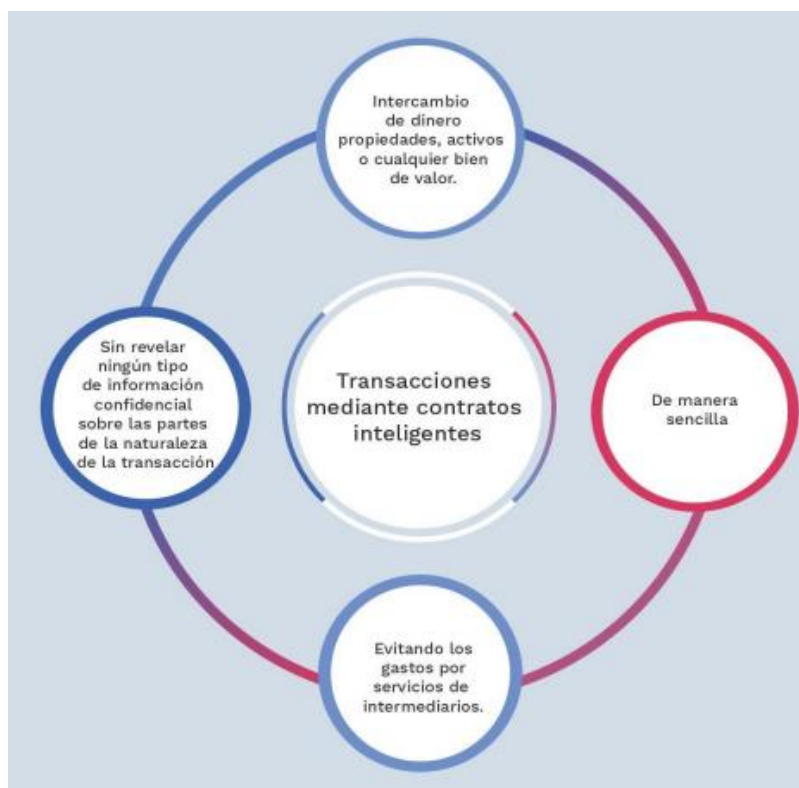
Contratos Inteligentes Una de las aplicaciones de la tecnología blockchain, que ha aumentado en su auge en los últimos años son los contratos inteligentes;

los términos que conforman un contrato inteligente se codifican y se cargan en los registros, generando un contrato descentralizado donde no se necesita de un tercero para el registro o la ejecución del mismo. Datos importantes para tener en cuenta en contratos inteligentes:

- Las cláusulas contractuales implícitas en el contrato se ejecutan de manera automática, cuando se cumplen las condiciones estipuladas, eliminando la ambigüedad que se pueda presentar en los términos estipulados en los acuerdos y los conflictos respecto a dependencias externas.

- Los contratos inteligentes son protocolos informáticos que facilitan, verifican o imponen la negociación o ejecución de un contrato, o que hacen que una cláusula contractual sea innecesaria; generalmente también tienen una interfaz de usuario y, a menudo, emulan la lógica de las cláusulas contractuales. Bajo el diseño de contratos inteligentes, muchos tipos de cláusulas contractuales pueden, por lo tanto, hacerse parcial o totalmente auto-ejecutables. Los contratos inteligentes tienen como objetivo proporcionar seguridad superior al derecho contractual tradicional y reducir otros costos de transacción asociados con la contratación.

La funcionalidad de firma múltiple se puede incorporar en contratos inteligentes donde se requiere la aprobación de dos o más partes antes de que se pueda ejecutar algún aspecto del contrato. Cuando las condiciones de un contrato inteligente dependen de datos del mundo real, se pueden desarrollar sistemas externos acordados llamados "oráculos" para monitorear y verificar precios, desempeño u otros eventos del mundo real.



¿Qué son las transacciones financieras para los contratos inteligentes? Los contratos inteligentes se pueden codificar de manera tal que el pago, la compensación y la liquidación se realicen automáticamente de manera descentralizada sin la necesidad de un intermediario externo (Houman, 2014). Por ejemplo, un contrato de derivados inteligentes podría reprogramarse con todos los términos contractuales (es decir, calidad, cantidad, entrega), excepto el precio, que podría determinarse algorítmicamente a partir de los datos del mercado suministrados a través de un oráculo. El margen podría transferirse automáticamente en llamadas de margen y el contrato podría rescindirse en caso de incumplimiento de la contraparte.

¿Qué permiten los contratos inteligentes? El intercambio de dinero, propiedades, activos o cualquier bien de valor de una manera sencilla, evitando los gastos por el servicio de intermediarios y sin revelar ningún tipo de información confidencial sobre las partes la naturaleza de la transacción. Para ilustrar mejor el desarrollo de un contrato inteligente, consideremos la venta o el alquiler de un vehículo, implementando la tecnología Blockchain a través del pago con monedas digitales; la persona que desea adquirir el vehículo obtiene un recibo, que en este caso se considera un contrato inteligente y la llave digital que llega a este en la fecha

especificada; en caso de que la llave no llega a tiempo, se le reembolsa el dinero al cliente, si llega, ambas partes reciben lo acordado a tiempo.

2.4.3. Aplicaciones – Educación.

Actualmente los títulos académicos formales (pregrados, especializaciones, maestrías y doctorados) no permiten determinar la capacidad y conocimiento de las personas al presentar su curriculum vitae; el aprendizaje no formal adquirido también es necesario y apreciado en las diferentes empresas en los procesos de contratación, los cuales se validan por medio de mecanismos internos en los procesos de selección.

Al momento de las compañías solicitar un currículum vitae a una persona en un proceso de selección, este es elaborado por el propio aspirante, donde dicho documento no acredita la veracidad de los títulos y conocimientos que expone el aspirante; por otro lado, el proceso de recolección de los certificados que garantizan los títulos obtenidos por el aspirante y la comprobación por parte de la empresa se convierte en un proceso complejo.



Para dar solución a la veracidad de la información presentada por un aspirante en un proceso de selección, se debería establecer una entidad central que garantice la información expuesta. En la actualidad se pueden encontrar identificadores institucionales que garantizan la información como el sistema GREC de la universidad de Barcelona, este permite verificar de forma correcta los títulos, pero deja abierta la posibilidad para que se verifiquen las competencias adquiridas por los aspirantes y los conocimientos desarrollados en programas de educación no formal (Bartolomé, Bellver, Castañeda, & Adell, 2017). En materia del ámbito de investigación: Se pueden encontrar sistemas que garantizan la producción científica de un investigador como Google Scholar, OrcID, el Researcher ID, o redes como Research Gate, Academia.edu o Mendeley, para citar algunos, los cuales han permitido automatizar la recolección de dicha información científica. La adecuada implementación de Blockchain permitiría acreditar la información suministrada por los aspirantes en un curriculum vitae, de tal forma que se pueda contrarrestar la manipulación de la información suministrada, convirtiendo este sistema en una especie de “moneda intelectual”. Un uso educativo obvio es almacenar registros de

logros y créditos, como certificados de grado. Los datos del certificado serían agregados al Blockchain por la institución que los otorga, a la que el estudiante puede acceder, compartir con los empleadores o generar un enlace desde un curriculum vitae en línea. Se abren oportunidades para la concesión directa de certificados y distintivos por parte de expertos y maestros de confianza (Sharples & Domingue, 2016).

2.4.4. Aplicaciones – Salud.

Existen múltiples aplicaciones de la tecnología Blockchain para la industria de la salud, incluida la distribución de productos y servicios. Un caso específico es el suministro de medicamentos desde la planta hasta el usuario final, por lo que los paquetes de medicamentos se autentican y se sellan en el tiempo en cada punto de entrega intermedio. Por ejemplo: para un lote de medicamentos que se envían desde el piso de la fábrica, el registro de lote se autentica, se marca con la hora, se coloca en Blockchain, se autentica y se marca de nuevo en cada punto de entrega intermedio.

¿Beneficios en el sector salud? El seguimiento del medicamento a medida que se abre paso a través del proceso de entrega. Esto simplifica y agiliza en gran medida la gestión de la distribución de medicamentos que puede evitar que caigan en las manos equivocadas, autenticando el medicamento para el consumidor final, lo que reduce en gran medida la posibilidad de falsificación, la manipulación de precios y la entrega de medicamentos vencidos.

2.4.5. Aplicaciones – Sistemas de registro de propiedad.

Las aplicaciones de la tecnología Blockchain en el sector inmobiliario pueden aplicarse tanto al sector público como al privado. En el sector público, el registro de la propiedad y catastro pueden colocar en una plataforma bajo tecnología Blockchain, lo que permite a las partes interesadas y agencias relevantes acceder en tiempo real a los registros de la propiedad; esto reduce considerablemente las disputas de propiedad y la necesidad de intermediarios para autenticar documentos y adjudicar disputas, lo que en última instancia ahorra costos y tiempo para el consumidor final.

2.4.6. Aplicaciones – Gestión de Identidad.

La gestión de identidad es muy importante en el proceso de verificación sobre el poseedor de documentos de identificación como el pasaporte o la cedula de ciudadanía, y en general sobre todo registros públicos que se asocie a un ciudadano. Las soluciones para la gestión de identidades en Blockchain son aún emergentes, sin embargo, se están realizando una cantidad considerable de trabajos sobre este tema, en especial sobre pasaportes y licencias de conducir.

2.4.7. Aplicaciones – Cadenas de suministros.

Es una realidad que afrontamos en la actualidad la gran cantidad de productos falsificados que se encuentran en el mercado, especialmente en Latinoamérica. Con más productos falsificados en el mercado, los consumidores tienen una necesidad aún mayor de encontrar proveedores confiables e información de calidad, ya que existen muchos peligros en el uso de productos falsificados. La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) advierte a los consumidores que la compra de productos falsificados puede costarles más que solo pérdidas financieras; el uso de productos falsificados puede causar enfermedades, discapacidades o incluso la muerte.

La comida es un área donde la confianza es primordial. Muchas marcas importantes han hecho grandes esfuerzos en generar confianza al hacer que el proceso de creación y envío de sus productos sea más transparente. Se ha intentado probar el valor, la frescura y la autenticidad de los productos cotidianos que utilizan algún software de seguimiento hasta hoy, pero la entrega de esos datos o la confiabilidad de ese sistema de entrega simplemente no ha sido lo suficientemente buena. Los consumidores todavía tienen que confiar en cualquiera de los datos ingresados en el sistema, y podrían haber sido editados después del hecho también.

Existen al menos una docena de sistemas de seguimiento de software heredados que pueden seguir un artículo del productor a la tienda, y contarnos algo al respecto en línea, pero desde el punto de vista del consumidor, ¿por qué debemos confiar en sus datos? Los productores crean y controlan toda esa información, no los consumidores, ni siquiera el gobierno, por lo que si hay alguna duda sobre dónde el origen de algún producto, sería ingenuo no preguntar por qué no podrían simplemente informar erróneamente o falsifique completamente los datos cuando sea en su beneficio hacerlo. Provenance es la primera empresa en intensificar y crear estas cadenas de suministro transparentes para todo tipo de productos basados en tecnología Blockchain. Si bien algunos servicios especializados como Everledger y Ascribe utilizan la Blockchain para rastrear tipos de productos individuales, en sus casos de diamantes y arte digital, respectivamente, Provenance se diseñó para rastrear cualquier tipo de producto, a lo largo de cada parte de su ciclo de vida. Los tres utilizan la inmutabilidad de Blockchain para registrar información sobre el viaje de sus productos, pero Provenance es el primero en crear un sistema en el que todo el historial de un producto puede rastrearse completamente desde el productor hasta el consumidor,

brindando actualizaciones en cada paso, dónde está, quién lo tiene y por cuánto tiempo.

2.5. Relevamientos.

En el presente apartado se presenta un análisis de casos de aplicaciones blockchain relevadas, que a nuestro parecer pueden resultar de interés a la provincia de Santa Fe, especialmente a la Secretaria de Finanzas e Ingresos Públicos y Política Fiscal. Los presentes proyectos pueden ser considerados como factibles de realizar por la provincia, generando los beneficios que en cada caso se describen. En el capítulo III del presente documento, se brindará una guía base de implementación de proyectos Blockchain y emisión de Tokens que complementada con los siguientes casos de interés permitirían a la provincia de Santa Fe comenzar con algunos proyectos pilotos de implementación de la tecnología.

2.5.1. Relevamientos- El caso de Estonia.

El diseño de una estrategia digital fundamentada en blockchain que permita adoptar de manera sostenible en el tiempo la gestión pública resulta fundamental para lograr un programa de transformación que facilite la identificación de los retos inmediatos en este sector y lograr una mayor eficacia, eficiencia y agilidad de las instituciones. Todo ello, con el fin de poder crear las estructuras y funciones necesarias para dar respuesta a las necesidades de los ciudadanos en una nueva fase de la gestión pública después de la implantación de la administración electrónica.

En la actualidad, existen a nivel mundial diferentes proyectos desarrollados por distintas administraciones públicas para poner en marcha el uso blockchain en la gestión pública. Entre los países pioneros en la puesta en práctica de la tecnología blockchain destaca, por encima de todos, Estonia que, desde 2008 su administración está poniendo en práctica un programa de servicios públicos digitalizados a través de un ecosistema eficiente, seguro y transparente a los que acceden los ciudadanos que disponen de identidades digitales seguras y que la convierte en la sociedad digital más avanzada del mundo.

El e-Estonia es un proyecto de acción de gobierno que pretende acercar y facilitar la relación entre el ciudadano y el Estado a través de una administración pública totalmente digitalizada que carece de registros en papel y que simplifica a través de su portal gubernamental, la gestión pública mejorando claramente la calidad de los servicios públicos.

Nacimientos, historiales médicos, pago de impuestos, registro de empresa, el voto en las elecciones, renovación de cédulas de identidad o permisos de conducir, todo ello se gestiona a través de un proceso digital en el que los

ciudadanos son los únicos propietarios de sus datos, todas las operaciones dejan un rastro digital y en el que todo acceso indebido lleva aparejado su correspondiente responsabilidad.

Para ello, utiliza el protocolo X-Road. Este protocolo permite que los distintos sistemas de información digital tanto del sector público como del privado de la



- 1 Aumenta el número de contribuyentes.
- 2 Se reduce el costo administrativo para la el Consejo de Impuestos y Aduanas.
- 3 Las declaraciones de impuestos pueden presentarse en 3 a 5 minutos.
- 4 Los contribuyentes reciben sus reembolsos en 5 días.
- 5 La recaudación de impuestos es transparente y eficiente.

nación estén conectados y funcionen en armonía. Puede operar en múltiples sistemas de información, transmitir gran cantidad de datos de diversa naturaleza y realizar búsquedas en varios sistemas de información de manera simultánea, lo que, en definitiva, garantiza la independencia de la plataforma y de su estructura, gran disponibilidad de servicios a través de protocolos con estándares internacionales y, sobre todo, seguridad en las operaciones. En definitiva, la apuesta de Estonia por la sociedad digital, que le ha

llevado a considerar la conexión a internet como un “derecho humano básico”, le otorga en la actualidad los más altos niveles de sociedad digital y de gobierno abierto.

En 2002, se introdujeron en el sistema los formularios automáticos de declaración de impuestos, lo que supuso un importante logro del desarrollo. El contribuyente utiliza una ID segura para acceder al sistema, puede revisar sus datos en los formularios que rellenó antes, hacer las modificaciones necesarias y, finalmente, aprobar el documento con su firma digital. El proceso suele durar de tres a cinco minutos y, gracias a ello, el 99% de las personas presentan sus declaraciones de impuestos por medios electrónicos en Estonia.

A demás de las declaraciones de impuestos individuales, el sistema también permite presentar:

- Aumenta el número de contribuyentes.

- Se reduce el costo administrativo para la el Consejo de Impuestos y Aduanas.
- Las declaraciones de impuestos pueden presentarse en 3 a 5 minutos.
- Los contribuyentes reciben sus reembolsos en 5 días.
- Declaraciones de aduanas

2.5.2. Relevamientos- El caso de Bahía Blanca.

El municipio de Bahía Blanca, perteneciente a la provincia de Buenos Aires en Argentina, ha creado en el año 2007 el Fondo Municipal de las Artes, el cual otorga subsidios a artistas locales. El monto del fondo y la cantidad de subsidios varían de manera anual y su otorgamiento no tiene un criterio único, aunque intenta mantener un balance en la asignación de acuerdo con las distintas disciplinas artísticas. Un consejo consultivo conformado por el director del Instituto Cultural de Bahía Blanca, representantes de los sectores de las artes y un representante de los empleados del instituto realiza la selección de los proyectos.

El caso de Bahía Blanca ha sido uno de los primeros pilotos a nivel local y fue desarrollado con la finalidad de experimentar la tecnología blockchain en el sector público, aprender de las particularidades de la tecnología y demostrar que puede utilizarse como un “notariado digital” de información pública. El problema central que buscó resolver el piloto es incrementar la transparencia en la asignación de subsidios públicos del Fondo de las Artes del Instituto Cultural de Bahía Blanca, y de este modo aumentar la confianza de la ciudadanía en el proceso. A través del atributo de inmutabilidad de los registros que otorga la tecnología blockchain, la información sobre el otorgamiento de subsidios (por ejemplo, destinatarios, montos, fecha de adjudicación, entre otros) no podrá ser alterada por funcionarios sin dejar un registro de la acción. (Serale, Redl, 2019)

Descripción de la solución

La solución ha sido desarrollada en una red pública (Ethereum) y se ha diseñado una interfaz para que cualquier usuario con acceso a la red pueda corroborar que la información sobre el proceso de asignación no ha sido alterada por ningún funcionario público municipal. La implementación ha sido desarrollada por técnicos no pertenecientes al municipio y tuvo una duración de tres meses; el lanzamiento oficial se realizó en noviembre de 2017. Como paso previo al piloto se digitalizó toda la información vinculada al otorgamiento de subsidios del mencionado fondo. El piloto emite tres certificados de confianza bajo la tecnología blockchain. El primero de ellos está vinculado a la asignación del subsidio al artista local con todos

sus datos, el segundo se realiza al momento del otorgamiento del subsidio, con base en la información de gastos que realiza el artista y de acuerdo con la regulación del fondo. Finalmente, un tercer certificado se emite con base en la información analizada por el Instituto Cultural, el cual verifica si la información emitida por el adjudicatario cumple con las condicionalidades del subsidio y certifica la finalización de la obra. (Serale, Redl, 2019)

Condiciones para implementar esta solución con tecnología blockchain

Este caso demuestra que la implementación de un piloto basado en la tecnología blockchain necesita de ciertas condiciones tecnológicas para ser implementado, y de hecho puede servir como incentivo para comenzar con procesos de modernización en el sector público. La evaluación del piloto resalta que blockchain requiere de una estrategia de gobierno digital que implique la digitalización de los procesos, la existencia de firma electrónica y la infraestructura adecuada (por ejemplo, conectividad, servidores).

Otra condición para la implementación de un piloto de este tipo es el diseño de una interfaz de usuario amigable. Delo contrario, se corre el riesgo de incumplir el objetivo de mayor transparencia y auditoría ciudadana de las transacciones.

Reflexiones finales del caso

Este caso evidencia que bajo ciertas condiciones blockchain otorga seguridad y transparencia a la asignación de subsidios y puede ser escalable a otros procesos públicos que requieran notorizar transacciones, como compras o licitaciones públicas. El piloto ha permitido que bajo un correcto uso de la tecnología y el establecimiento de contratos inteligentes no sea posible otorgar más de un subsidio a una misma persona. También ha posibilitado la auditoría ciudadana del proceso burocrático en tiempo real. El informe de evaluación del piloto ha identificado varias lecciones aprendidas del caso que vale la pena resaltar de cara a la implementación de pilotos a nivel local, a saber: (i) la necesidad de una voluntad política para emprender procesos de apertura de información; (ii) la existencia de un proceso estandarizado, con pasos y actores claramente identificables; y (iii) el diseño de un piloto simple, con claros potenciales de ser escalable, en un municipio de tamaño razonable. (Serale, Redl, 2019)

2.5.3. Relevamientos- El caso de Georgia.

Desde 2004 la Agencia Nacional de Registro Público (NAPR, por sus siglas en inglés) de la República de Georgia ha realizado varios procesos de reestructuración organizacional, numerosos cambios legales y la digitalización de los archivos, los cuales han mejorado su eficiencia y efectividad significativamente. Sin embargo, la NAPR estaba buscando formas de modernizar sus servicios al

ciudadano, manteniendo la seguridad de los datos del registro de la propiedad, pero permitiendo la transferencia de títulos de propiedad de forma electrónica con mínima interacción personal. En este contexto se ha evaluado la viabilidad de utilizar la tecnología blockchain para enfrentar estos desafíos.

Descripción de la solución.

En abril de 2016, la NAPR de la República de Georgia decidió diseñar una solución basada en blockchain para la gestión de sus registros de propiedad. En una primera fase, se utilizó una blockchain privada autorizada para mantener registros críticos, y una blockchain pública de Bitcoin para permitir a los ciudadanos verificar el registro de transacciones de transferencia de títulos de propiedad.

Uno de los elementos centrales de la solución es la publicación de hashes de documentos de transferencia de títulos de propiedad en la blockchain pública de Bitcoin. Al hashear un documento y publicar el hash en una cadena de bloques pública se pueden conseguir los beneficios de un notariado (es decir, la verificación/garantía/certificación de la integridad del documento) sin la necesidad de un intermediario. Teniendo en cuenta la dificultad de cambiar información de la cadena (especialmente si es pública), una vez que se publican los hashes, el documento tiene una marca de tiempo. Esto permite a los ciudadanos verificar si una transacción de transferencia de títulos de propiedad ha sido registrada (concretamente en la cadena de bloques) de acuerdo con el certificado de registro que ellos han obtenido al final del proceso. También sea segura la integridad de los datos almacenados, previniendo su falsificación y facilitando la auditoría de la información histórica casi en tiempo real. (Serale, Redl, 2019)

Sin embargo, debido a que los documentos y las transacciones asociadas que se almacenan se colocan en una base de datos de back-end de la NAPR en la primera fase del piloto, los ciudadanos aún necesitan visitar las oficinas de la NAPR para completar las transacciones. Es por ello que en febrero de 2017 la NAPR consideró que el programa era viable y que podía aplicarse más ampliamente la tecnología blockchain a las transacciones de propiedades, introduciendo contratos inteligentes para simplificar y automatizar las operaciones comerciales, incluida la venta de propiedades y la transferencia, entre otras.

Actualmente, cuando la NAPR recibe la aplicación para registrar un cambio de propiedad en el proceso tradicional, comprueba que la propiedad le pertenece al vendedor y que no hay gravámenes impagos en ella antes de transferir la propiedad. Mientras la NAPR está realizando el proceso, tanto el vendedor como el comprador pueden cambiar de opinión (antes o después de efectuarse el pago), con lo que pueden generarse conflictos que luego podrían llevar mucho tiempo de

resolución en la justicia. Los ciudadanos usualmente protegen sus intereses contratando a escribanos, bancos como intermediarios; sin embargo, esto es costoso.

Al introducir contratos inteligentes a la solución, los ciudadanos que quieren vender una propiedad pueden iniciar una sesión en el sitio web de la NAPR, acceder a los datos relativos a su propiedad y ponerla a la venta. Los interesados pueden realizar ofertas y si alguna resulta atractiva, los vendedores pueden aceptarla. La disponibilidad de fondos por parte del comprador y la confirmación de la propiedad por parte del vendedor pueden hacerse automáticamente, y entonces la transacción se cierra. La información de compra estará disponible en la cadena de bloques pública. Cabe destacar que el piloto se diseñó de forma tal que, si la cadena de bloques no funcionaba correctamente, se volvería al esquema anterior automáticamente.

Si todas las transacciones vinculadas a la transferencia de títulos de propiedad están registradas en la cadena de bloques (el registro de propiedad y las transacciones financieras que corresponden a su transferencia), y todas las partes involucradas (vendedor, comprador, bancos, gobierno) confían en la integridad de los datos, una transferencia de propiedad podría realizarse electrónicamente, sin intermediarios y en tiempo casi real (dependiendo del mecanismo de consenso usado). Mediante el uso de contratos inteligentes, en el futuro la agencia podría beneficiarse del potencial de automatizar pasos del proceso de registración de títulos de propiedad que hasta ahora han necesitado la intervención manual de funcionarios del gobierno. (Serale, Redl, 2019)

Consideraciones de diseño para aprovechar el potencial de la tecnología

Como se observa en este caso, blockchain puede ayudar a resolver problemas relacionados con la confiabilidad e integridad de los registros públicos. Sin embargo, la tecnología es un sistema basura dentro, basura fuera; es decir, si la información que se carga en el sistema es falsa (ya sea por descuido o engaño), la información escrita en la cadena será falsa también es importante definir roles y permisos de los distintos actores que utilizarán y/o editarán estos registros en el caso de la blockchain privada. Para garantizarla consistencia de los datos entre los nodos, es importante definir cómo, cuántos y bajo qué autoridad estarán distribuidos los nodos de la red. Si existe solo un nodo, los datos no son más seguros que en bases de datos tradicionales no replicadas (incluso se podría cuestionar si el término blockchain es aplicable en este caso). Además, la replicación de los datos a múltiples nodos podría impedir la pérdida de información si uno (o un número insignificante) de los nodos falla. (Serale, Redl, 2019)

Reflexiones finales del caso

El principal valor añadido por el uso de blockchain en este caso es un aumento en la seguridad y confiabilidad de los certificados. La solución tecnológica ha permitido una mayor transparencia en el proceso de registro de los títulos de propiedad, aunque los ciudadanos solamente tienen medios limitados para verificar los datos debido al uso de una blockchain privada autorizada para el manejo de la información relacionada a la registración de títulos de propiedad, lo cual los excluye del proceso de auditoría. Por último, el piloto trae mejoras significativas en términos de eficiencia y efectividad de la registración y verificación de los títulos de propiedad: el tiempo de entrega del servicio de registración se ha reducido de entre uno y tres días hábiles a varios minutos; el tiempo de verificación de certificados se ha reducido de unos pocos días a unos segundos; los costos operativos del servicio de registro se han reducido en un 90%. (Serale, Redl, 2019)

2.5.4. Relevamientos- El caso de Bahamas.

En la actualidad se está analizando el potencial de la tecnología blockchain para generar un mercado laboral más transparente y adecuado a las necesidades del mercado a nivel global. A través de los blockcerts, un estándar abierto para credenciales digitales

creado por el laboratorio del Instituto Tecnológico de Massachusetts en 2016, pueden emitir y eventualmente verificar certificados de formación laboral de una persona. De esta manera, un trabajador que se ha formado en línea y ha obtenido certificados de diversas instituciones a nivel global puede portar los registros de sus habilidades y experiencia de manera segura y digital. El gobierno de Malta fue el primero en experimentar con blockcerts en el sector educativo. En Latinoamérica el gobierno de Bahamas emitió en 2018 los primeros 78 certificados digitales a través de la Agencia Nacional

de Capacitación (NTA, por sus siglas en inglés) en blockchain. Bahamas Blockcerts ha implementado un piloto con los certificados de capacitación de esta entidad, pero está explorando la manera de incluir nuevos sectores para verificar otros certificados (tributarios, licencias comerciales, etcétera.) (Serale, Redl, 2019)

Descripción de la solución

El proyecto Bahamas Blockcert permite la emisión de certificados digitales validados a nivel nacional con un formato abierto e interoperable, por lo que pueden alojarse en diversas plataformas. En este caso se utiliza una billetera digital, a la que se accede a través de una aplicación móvil. Además de poder alojar y portar sus blockcerts, las personas tendrán la posibilidad de agregar su currículum vitae y otros atributos de identidad (ID, tarjeta de seguro social, licencia de conducir).

Adicionalmente, podrán enviar estas certificaciones a potenciales empleadores, los cuales pueden verificar la autenticidad de la información. Como consecuencia, se intenta remover barreras al acceso de información y hacer más eficiente la búsqueda laboral. La tecnología blockchain brinda seguridad y certeza a los blockcerts, pero además elimina intermediarios que anteriormente debían certificar la validez de los títulos académicos, cursos de capacitación y certificaciones. Debido a que la verificación de esta información se puede automatizar, pueden ahorrarse tiempos y costos de transacción vinculados al reclutamiento. Dado el éxito del piloto, en la actualidad se está evaluando la posibilidad de emitir blockcerts para obtener licencias de negocio, las cuales requieren de la verificación de varios documentos. Como primer paso, se espera poder emitir estos certificados como blockcerts para luego emitir certificados digitales de todos los documentos requeridos para el trámite, automatizando el proceso. (Serale, Redl, 2019)

Condiciones necesarias de implementación

Tal como se menciona en la primera parte, el éxito en la implementación y escalamiento de un proyecto de estas características depende en gran medida de la generación de un ecosistema digital que emita y utilice estos certificados. Pero también requiere la generación de habilidades digitales tanto para los usuarios como para quienes deben gestionar esta información

Reflexiones del caso

El principal valor añadido por el uso de blockchain en este caso es un aumento en la seguridad y certeza de los certificados digitales. Además, la tecnología facilita la eliminación de intermediarios que anteriormente debían certificar la validez de los títulos académicos, cursos de capacitación y certificaciones, da a los ciudadanos mayor control sobre sus credenciales (auto soberanía, protección de privacidad) y habilita la automatización de la verificación de esta información a través de un estándar abierto, ahorrando tiempos y costos de transacción vinculados al trámite de validación y a los procesos que dependen de estos certificados (por ejemplo, reclutamiento de personal).

2.6. Relevamiento de buenas prácticas blockchain.

En el mundo Los gobiernos pueden aprovechar la tecnología blockchain para ofrecer ciberseguridad, optimización de procesos, integrar servicios de forma híper conectada al mismo tiempo de estar robusteciendo la confianza y la responsabilidad. Además, plataformas de registros distribuidos pueden aprovecharse para soportar una serie de aplicaciones en el sector público, incluyendo dinero digital, pagos, registro de tierras, gestión de identidad,

trazabilidad de cadena de abastecimiento, salud, registro de transacciones, impuestos, votación, y gestión de entes legales.

A continuación, se muestran algunas buenas prácticas internacionales sobre el uso de blockchain en el gobierno, ejecutados entre los años 2014 a 2021 divididas por regiones:

Norte América

Canadá

- El Consejo Nacional de Investigación de Canadá (NRC) anunció que había construido un explorador de blockchain de Ethereum para experimentar con la administración transparente de los contratos gubernamentales y compartir datos de manera confiable con el público.

- El Gobierno de Canadá (GC) está utilizando la tecnología blockchain para emitir a los empleados, un currículum o hoja de vida digital, que proporciona "un registro permanente, propio y seguro de sus habilidades y experiencias".

México

- El gobierno mexicano planea realizar un procedimiento de contratación pública en una red blockchain

- La Unidad de Gobierno Digital - Secretaría de la Función Pública de México lanzó HACKMX, un proyecto que aprovecha la tecnología blockchain para rastrear y validar licitaciones de contratos públicos.

Estados Unidos

- La Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) está creando un escudo de ciberseguridad blockchain, una plataforma basada en blockchain para transmitir mensajes seguros o procesar transacciones que se pueden rastrear a través de numerosos canales. La aplicación se utilizará de diferentes maneras para facilitar la comunicación entre las unidades y el cuartel general para transmitir información entre los oficiales de inteligencia y el Pentágono.

- La Fuerza Aérea de los Estados Unidos implementó el proyecto Blockchain Approach for Supply Chain Additive Manufacturing Parts (BASECAMP) para asegurar largas cadenas de valor con tecnología de contabilidad distribuida.

- El Servicio Postal de los Estados Unidos (USPS) presentó una patente para incorporar tecnología blockchain y certificados digitales para autenticar la información del usuario y más recientemente propuso facilitar la jornada.

- La Administración de Alimentos y Medicamentos (FDA) lanzó un proyecto piloto que explora la utilidad de blockchain en el seguimiento seguro y la verificación de prescripciones médicas.

- En 2014, el Servicio de Impuestos Internos de los Estados Unidos clasificó la moneda digital como propiedad.

Europa

Alemania

- La Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH estableció un 'Blockchain Lab' para aprovechar el potencial de blockchain y tecnologías relacionadas en los esfuerzos por alcanzar los Objetivos de Desarrollo Sostenible de las Naciones Unidas.

Austria

- El gobierno austriaco inauguró el nuevo Instituto de Investigación de Criptoconomía, que apoyará proyectos de investigación de blockchain a través de un fondo de € 8 millones.

Lituania

- El Banco Central de Lituania lanzó un sandbox para desarrollar productos y soluciones basados en blockchain.

Luxemburgo

- El proyecto Infracchain crea un marco de gobernanza que permite que las aplicaciones blockchain se vuelvan operativas en el entorno regulatorio actual.

Malta

- El registro de empresas de Malta adoptará la tecnología blockchain con el objetivo de aumentar la eficiencia y modernizar los procesos de negocios.

- El gobierno de Malta puso a prueba un programa de credenciales basado en blockchain que verifica instantáneamente las credenciales académicas.

Países Bajos

- La ciudad de Groningen lanzó una prueba de concepto para ayudar a los ciudadanos a recuperar el control financiero sobre sus deudas a través de una variedad de servicios, que incluyen asistencia para deudas, prevención de deudas y administración de ingresos. El proyecto almacena los cambios de estado financiero de los clientes de GKB en un blockchain privado, junto con facturas e información de pago de ingresos de socios externos.

Eslovaquia

- Cuenta con un portal de licitaciones públicas basado en tecnología blockchain.

España

- El Ministerio de Energía, Turismo y Agenda Digital cofinancia el proyecto TrustForWills, una plataforma de Smart contracts para la gestión de activos digitales usando blockchain.

- El gobierno de Cataluña puso en marcha un proyecto de identidad autónoma, denominado IdentiCAT. El "IdentiCAT" puede ser gestionado de forma privada por los ciudadanos.

Suecia

- El registro de la propiedad sueco (Lantmäteriet) está probando transferencias de bienes raíces y otras transacciones de “multipartita” sobre blockchain.

Suiza

- En asociación con el uPort de ConsenSys, el municipio de Zug probó una identidad soberana emitida por el gobierno en el blockchain de Ethereum. La referencia al caso de uso completo en inglés se encuentra en este link: <https://consensys.net/Blockchain-use-cases/government-and-the-publicsector/zug/>

Ucrania

- El Ministerio de Finanzas de Ucrania puso a prueba subastas de prueba utilizando tecnología blockchain. Reino Unido

- La Agencia de Normas Alimentarias (FSA) del Reino Unido completó un piloto para rastrear la distribución de carne en un matadero de ganado utilizando blockchain. Esta prueba marcó la primera vez que la tecnología blockchain de trazabilidad, se ha utilizado como una herramienta reguladora para garantizar el cumplimiento en la industria alimentaria.

África

Ghana

- El gobierno de Ghana, en asociación con Bitland, lanzó un proyecto piloto para registrar tierras en un blockchain. Más del 78% de la tierra de Ghana no está registrada. El proyecto se había probado ahora en 20 comunidades de Kumasi en el año 2018.

Mauricio

- El gobierno de la isla de Mauricio ha creado una Licencia Regulatory Sandbox (RSL), que permite a los inversionistas externos desarrollar soluciones basadas en blockchain bajo la supervisión de la Junta de Inversiones de Mauricio.

Sierra Leona

- El gobierno de Sierra Leona, en cooperación con la organización sin fines de lucro Kiva, lanzó una plataforma blockchain para el historial crediticio.

Sudáfrica

- El gobierno sudafricano ha establecido un grupo de trabajo regulador de criptoactivos para investigar conceptos relacionados con blockchain.

- La Alianza Nacional de Blockchain de Sudáfrica (SANBA) se formó para establecer una asociación entre el gobierno, las empresas, la academia y la sociedad civil para apoyar el uso de las tecnologías de blockchain en el contexto sudafricano.

Tanzania - El gobierno de Tanzania eliminó a 10,000 trabajadores fantasmas del sector público utilizando tecnología blockchain para auditar la nómina pública.

Asia

China

- Xiong'an lanzó un proyecto de forestación de 6.667 hectáreas. Una plataforma en línea basada en blockchain, big data y otros rastros de alta tecnología y gestiona el ciclo de vida de los árboles.

- El Centro de Información del Estado, Union Pay, China Mobile y otras tres organizaciones lanzaron Blockchain Services Network (BSN), un proyecto de infraestructura de blockchain a nivel nacional que se concibió como el "sistema IOS de Android o Apple" para blockchain.

RAE de Hong Kong

- El departamento financiero de Hong Kong publicó nuevas reglas para que los intercambios de criptoactivos obtengan licencias. Una regla estipula que los intercambios de cifrado no necesitan una licencia de la Comisión de Valores y Futuros (SFC) para operar si no comercializan ningún producto definido como valor.

India
- El Ministro de Estado de Electrónica y Tecnología de la Información ha identificado la tecnología Blockchain como un área de investigación esencial en dominios como gobernanza, banca y finanzas, y ciberseguridad en un borrador de documento de enfoque. El documento también presenta un marco blockchain a nivel nacional, que analiza el potencial de la tecnología de contabilidad distribuida y la necesidad de una infraestructura compartida para diferentes casos de uso.

- El gobierno de Maharashtra y el Departamento de Ingresos se asociaron con una plataforma de cadena de bloques híbrida de código abierto para completar una prueba de concepto para los registros de tierras en la cadena de bloques.

Malasia

- La Corporación de Economía Digital de Malasia (MDEC) anunció que está poniendo a prueba un programa de visas de trabajo para que los autónomos tecnológicos trabajen en Malasia a corto plazo, a fin de satisfacer la demanda de talentos con capacidad de inteligencia artificial, blockchain y ciberseguridad.

Corea del Sur

- El servicio de Aduanas de Corea del Sur lanzó un sistema de compensación basado en blockchain para la gestión de envíos de importación y exportación.

Tailandia

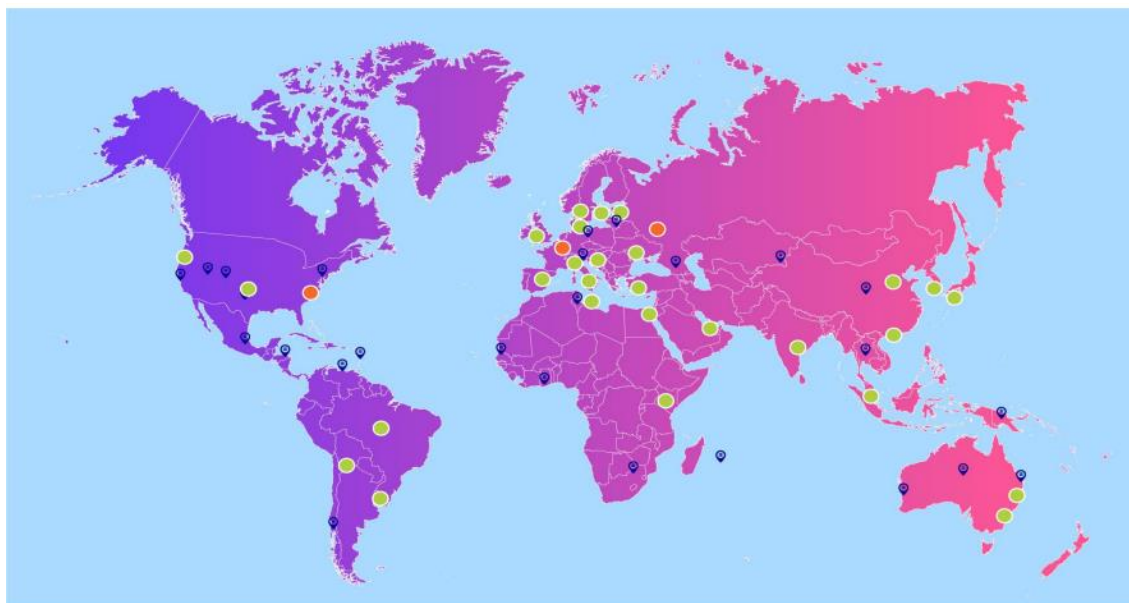
- El Ferrocarril Estatal de Tailandia y el Correo de Tailandia desarrollarán y aplicarán la tecnología de Internet de las cosas (IoT) para rastrear las llegadas y salidas de trenes y la tecnología blockchain para rastrear paquetes de alto valor.

Australia

- El Commonwealth Bank de Australia emitió un bono criptográfico para Queensland Treasury Corporation.

- La Comisión Australiana de Valores e Inversiones (ASIC) publicó una hoja de información regulatoria INFO 219 para empresas que consideren operar la infraestructura del mercado o que brinden servicios financieros o de crédito al consumidor, utilizando tecnología de contabilidad distribuida.

Por su parte, el Foro y Observatorio de la Comisión Europea EUBlockchain, tiene un mapa de iniciativas públicas muy interesante que se puede consultar en línea.



Se deja el enlace para mapa interactivo aquí:

<https://www.euBlockchainforum.eu/initiative-map>

Situación en Argentina:

En el ámbito del sector público argentino, desde julio de 2017 por ejemplo, las ediciones electrónicas del Boletín Oficial se certifican mediante la utilización de

blockchain, para que los usuarios puedan verificar la autenticidad y obtener prueba de la existencia de la edición electrónica.

Un año más tarde, en julio de 2018, se lanzó el proyecto “Blockchain Federal Argentina” que, con auspicio de NIC Argentina, la Cámara Argentina de Internet (CABASE) y la Asociación de Redes de Interconexión Universitaria (ARIU), busca conformar la infraestructura sobre la que correrá la primera plataforma nacional multiservicios de uso público, que busca mejorar los procesos públicos.

Por último, en abril de 2019, Argentina se convierte en un miembro del Blockchain Research Institute (BRI), siendo el segundo gobierno nacional en convertirse en miembro del BRI, como la primera etapa del proceso de creación de un "Centro de Excelencia del Instituto de Investigaciones Blockchain" en Argentina; acuerdo que le brinda al gobierno federal acceso a más de 100 proyectos de investigación, seminarios en línea y otros productos exclusivos, así como acceso a varios programas y eventos junto a grandes corporaciones, gobiernos, organizaciones sin fines de lucro y miembros de la comunidad de startups.

La iniciativa Blockchain Federal Argentina (BFA). Blockchain Federal Argentina es una plataforma multiservicios abierta y participativa pensada para integrar servicios y aplicaciones sobre blockchain en Argentina. Se trata de una iniciativa confiable y completamente auditable que permita optimizar procesos y funcione como herramienta de empoderamiento para toda la comunidad. Siguiendo el modelo de Múltiples Partes Interesadas, BFA mantiene un modelo de gobernanza que asegura la representación de todos los sectores en la toma de decisiones. Pero al ser una plataforma pública, su uso no estará restringido a las organizaciones que participen del consorcio, sino que está abierta a toda la comunidad. Se caracteriza por:

- Sin criptomoneda: está diseñada específicamente para no poseer criptomoneda asociada, siendo el incentivo para participar el de favorecer al desarrollo de servicios e iniciativas basadas en la innovación tecnológica y en un trabajo horizontal entre diversos actores.

- Ser un modelo liviano (al no depender del minado de criptomonedas y del esfuerzo por obtener una recompensa), es decir, no se requiere contar con gran cantidad de computadoras a disposición de la resolución de algoritmos complejos, con el gasto de energía que eso conlleva.

- Es una red permissionada, que funciona bajo un consenso basado en Prueba de Autoridad: la red se estructura en base a un conjunto confiable, una determinada cantidad de nodos selladores a partir del consenso de las partes que integran BFA y respaldados por la infraestructura de las instituciones, empresas u

organismos responsables de cada uno de ellos. Así, el procesamiento no se basa en un conjunto de mineros anónimos compitiendo por la creación de un bloque, sino en la cooperación entre aquellos que representan a distintos sectores.

– Las transacciones son gratuitas: el “combustible” necesario para realizarlas será provisto, sin ningún costo asociado, por BFA.

– Almacenamiento Off-Chain: en BFA no se almacenan documentos o archivos dentro de la blockchain, solo se guardan los hashes de esos documentos, siendo los usuarios, los servicios, los responsables de resguardarlos de la manera que consideren más adecuada. Y, al tener los digestos criptográficos sellados en la blockchain encuentran la forma de demostrar que esos documentos no fueron modificados luego de que ese hash se obtuvo.

– Software libre: el software de BFA se basa en una implementación abierta y robusta. Todos los desarrollos y modificaciones que se realicen serán igualmente abiertos, de modo que puedan ser públicamente auditados por cualquier interesado, más allá de los participantes del consorcio. La transparencia inherente en el modelo queda también garantizada desde el código.

2.7. Relevamientos – Emisión de Tokens.

2.7.1 El Caso del municipio de Marcos Paz.

En el nuevo paradigma de la Internet del Valor, las ciudades inteligentes pueden avanzar un paso más, utilizando las blockchains como una herramienta de registro de conductas ciudadanas deseables, que permiten también registrar ciertos beneficios y premios en favor de aquellos ciudadanos comprometidos con fines socialmente beneficiosos. En este sentido, quizás uno de los primeros casos de Latinoamérica es el desarrollado en 2019 por el municipio de Marcos Paz (provincia de Buenos Aires) junto con la empresa Koibanx: un innovador programa conocido como Activos Marcos Paz.

Su funcionamiento requiere de la descarga y autenticación del vecino (o del comercio que adhiera al programa) mediante una billetera criptográfica que registra información en la blockchain de RSK. Las billeteras pueden escanear códigos QR, que se utilizan para transaccionar tokens criptográficos que representan beneficios y descuentos en comercios adheridos y ante el municipio.

Ciertas conductas comunitarias deseables realizadas por los residentes empadronados en Marcos Paz (como por ejemplo asistir a talleres culturales, utilizar el transporte municipal, el pago puntual de tasas municipales, reciclar residuos domiciliarios, entre otros) se premian y se incentivan con tokens criptográficos (llamados Activos Marcos Paz) que se acreditan en sus billeteras criptográficas.

Estos tokens criptográficos generan beneficios reconocidos por los comercios adheridos al programa y, una vez recibidos por ellos, estos tokens criptográficos pueden ser utilizados por los mismos comercios para el pago de tasas municipales.

2.7.2. Proyecto caso Madrid.

El Ministerio de Asuntos Económicos y Transformación Digital dio luz verde a la financiación de empresas mediante la emisión de tokens digitales en Ethereum. El proyecto promovido por Bolsas y Mercados (BME) facilitará la captación de fondos a través de la emisión de préstamos participativos y notas convertibles representados como activos digitales en la blockchain.

Marketplace, (nombre del proyecto) es una plataforma alternativa de financiación que pretende ser un punto de encuentro entre las pequeñas y medianas empresas que buscan captar recursos y los inversores interesados en este tipo de compañías. Se plantea con un modelo abierto e integrador que contrasta con el sistema de silos en el que se lleva a cabo ahora esta financiación alternativa. Una nueva forma de obtener fondos, pero que también es disruptiva en la manera en la que se articula. Y es que la plataforma, que está basada en tecnología blockchain, emite tokens en Ethereum para facilitar la captación de recursos a través de préstamos participativos.

2.7.3. El caso de la provincia de Misiones.

La provincia de Misiones lanzó en 2019, su proyecto en conjunto con la empresa privada green bond meter (GBM) para la emisión de su propio Token (GBM Coin), cuya propuesta consiste en la conservación y recuperación del patrimonio natural de la selva misionera argentina. La compañía GreenBond Meter hizo su primera emisión de tokens cuyo valor está respaldado en un metro cuadrado de un terreno de 24.500 hectáreas en la provincia de Misiones, destinado a la recuperación de la biosfera nativa y su conservación por un período de 100 años, para luego ser donado al Estado y crear un parque protegido. La tenencia de cada GBM Coin no da derecho real de dominio, posesión o uso sobre la porción de la tierra preservada, sino un derecho de exigencia de cumplimiento de preservación y no explotación. Adicionalmente, este cripto activo generará un bono GBM (un bono de carbono), con el que no solo se puede hacer un aporte a la conservación de este espacio natural sino también vender y obtener un rédito económico.

Capítulo III: “Implementación de tecnología blockchain”

3.1. Hoja de ruta para implementar proyectos blockchain

Basados en “Technology Roadmapping in Canada: A development Guide”, y adaptando los conceptos, no a una industria, sino a una tecnología (específicamente Blockchain), se procede a realizar una propuesta metodológica para el diseño de una hoja de ruta, que primero que todo, debe ser entendida como un proceso y no como una actividad; es decir que la hoja de ruta no consiste en una lista de chequeo o en una fórmula a seguir para obtener un resultado específico, sino que está definida como un proceso iterativo que permite identificar los principales aspectos que deben ser tenidos en cuenta para maximizar las probabilidades de apropiar adecuadamente la tecnología. Partiendo de este hecho se procede entonces a utilizar los elementos enunciados en “Technology Roadmapping in Canada: A development Guide” y a adaptarlos al caso de la provincia de Santa Fe para obtener una primera aproximación a una hoja de ruta para la adopción de la tecnología Blockchain en la provincia.

3.1.1. Misión

Generar escenarios sociales y productos tecnológicos que promuevan y utilicen las tecnologías Blockchain en la gestión pública.

3.1.2. Visión

Ser una provincia líder y reconocida en el contexto nacional, por el uso de tecnologías Blockchain en la gestión pública, generando así confianza en la interacción gobierno ciudadanía.

3.1.3. Objetivo del proyecto, metas y resultados esperados

Generar aplicaciones tecnológicas basadas en Blockchain con el fin de facilitar el intercambio ciudadano de recursos que posean valor social o económico en un entorno confiable.

3.1.4. Alcance de las condiciones del mapa de ruta

- Ser una provincia líder en la implementación de Blockchain en el sector público en un lapso de 5 años, en aras de mejorar la transparencia, confianza y optimizar procesos en los sectores gubernamentales.
- Adaptar y desarrollar aplicaciones informáticas haciendo uso de la tecnología Blockchain en el sector público que permita optimizar los procesos al interior de los diferentes entes gubernamentales.

3.1.5. La industria actual

Teniendo en cuenta que se ha restringido el mapa de ruta al sector público, es importante entonces entender el ecosistema de Blockchain para este sector específico y una fuente relevante de información al respecto es el documento desarrollado por Deloitte University Press, “Will Blockchain Transform the Public Sector?”, donde muestra por ejemplo los recientes desarrollos oficiales de parte de

gobiernos alrededor del mundo en el uso de la tecnología Blockchain específicamente.

3.1.6. Ecosistema Blockchain.

- Entidades públicas: Ministros de las unidades de sistemas, planeación, estadística o interesados en implementar la tecnología blockchain en sus secretarías.

- Entidades privadas: sociedades, ONGs, cooperativas, Bancos, Bolsa de Valores, emprendedores.

- Congreso de la provincia: Encargado de generar la legislación necesaria para el correcto funcionamiento de la tecnología blockchain en Santa Fe.

- Ciudadanos: desarrolladores

- Sector académico.

Productos que ofrece blockchain

Una de las principales aplicaciones de la tecnología blockchain son los contratos inteligentes (smart contracts) que se pueden construir sobre plataformas como Ethereum.

3.1.7. Impactos de DLT/Blockchain.

- En el sector financiero, la tecnología DLT/Blockchain permite agilizar las transacciones, estas se pueden realizar a cualquier hora y en cuestión de minutos, reduciendo los costos de las mismas al eliminar intermediarios.

- En el sector salud, el desarrollo de sistemas de información desarrollados sobre plataformas DLT/Blockchain optimiza los tiempos de respuesta del ecosistema.

- En procesos de administración pública, vuelve más transparentes los procesos y la administración pública.

- En proyectos sociales, la transparencia permite verificar el buen uso de los recursos utilizados por empresas sociales, lo que da mayor confianza a los donantes. Tendencias del mercado y proyecciones Los nuevos desarrollos y tendencias del mercado están enfocados en desarrollar aplicaciones que permitan:

- Nuevos flujos de ingresos y modelos de negocio basados en registros de datos de salud del paciente.

- Acceso y verificación de datos en tiempo real.

- Uso de contratos inteligentes para desarrollar automáticamente el cumplimiento legal y regulatorio.

- Reducción del fraude en transacciones gubernamentales.

- Reducir los costos de transacción a través de la desintermediación.

- Permitir que los pacientes conserven el control sobre los datos individuales.

- Importancia para la protección de la propiedad intelectual y el registro de datos de las cadenas de suministro.
- Mejorar la eficiencia de la distribución de medicamentos. Reducir la falsificación.
- Conectar directamente a los productores de contenido (incluidos los artistas) y los consumidores, y alinear el consumo de medios con el precio pagado.
- Simplificación de los pagos de regalías, mejor protección de datos y costos reducidos para la protección de la propiedad intelectual.

3.1.8. Limitaciones relevantes.

- La principal limitación para implementar la tecnología blockchain en Santa Fe es la falta de conocimiento; bajo la cual los procesos de apropiación y aplicación del conocimiento se hacen mucho más extensos y no se cuenta con la capacidad instalada para llevar los procesos a gran escala.
- Desde el punto de vista técnico, la escalabilidad y la convergencia son limitantes a la hora de implementar la tecnología blockchain.
- Desde el punto de vista legal, Santa Fe no cuenta con una legislación que permite la incorporación de la tecnología en el sector público.

3.1.9 Necesidades técnicas y capacidades

3.1.9.1. Barreras y brechas.

En la implantación de la tecnología blockchain existen barreras y brechas de tipo conceptual-cultural y tecnológicas la cuales describiremos a continuación. Barreras de tipo Conceptual-Cultural. Desconocimiento de las posibilidades de uso en el sector público.

- Para identificar un activo digital se requiere reconocer dónde radica el valor social o económico para establecer “el activo” y cómo generar confianza en que este valor puede residir en un formato digital. Se considera una barrera conceptual porque identifica que el valor no es un asunto trivial y se considera cultural porque para un ciudadano es más confiable un documento que puede guardar en su escritorio.
- Al momento de plantear una arquitectura blockchain puede requerirse de los nodos mineros, los cuales realizan su trabajo por un incentivo, en el caso de Bitcoin el incentivo está claro y son criptomonedas en otras aplicaciones como un banco de tiempo o en una cadena logística la recompensa de los nodos mineros ¿tendrá que ser siempre dinero?, o ¿cómo puedo motivar este esfuerzo computacional?
- Generación de usuarios, generar confianza e incrementar la usabilidad de una plataforma DLT siempre es una barrera cultural.

3.1.9.2. Barreras tecnológicas.

- Pocos profesionales capacitados en la implantación de aplicativos blockchain.
- Los tiempos de respuesta en una transacción.
- La escalabilidad de la solución. Brecha Conceptual-Cultural
- El nivel de apropiación de la tecnología en el país es bajo. Brecha Tecnológica
- Existen diferencias entre las posibilidades de implementación de la tecnología entre grandes ciudades y pequeños municipios.

3.1.10. Recomendaciones de mejoras de programas para las habilidades necesarias para implementar Blockchain

Ante la falta de la existencia de una masa crítica con las capacidades para realizar los desarrollos necesarios lo más sensato es promover programas de transferencia de conocimiento basados en la tecnología Blockchain, que permita a los actores del ecosistema adquirir las capacidades relevantes para desarrollar sistemas de información basados en Blockchain contribuyendo a la solución de problemas del sector público.

3.1.11. Puntos de decisión y cronograma.

Para el desarrollo de un cronograma tentativo que permita la implementación de la tecnología DLT/Blockchain en el sector público y que permita a Santa Fe ser una provincia líder en la región en la implementación y desarrollo de aplicaciones sobre esta tecnología se proponen las siguientes actividades:

Actividad #1: Capacitación al ecosistema blockchain Al ser una tecnología emergente, se requiere capacitar a desarrolladores, emprendedores de las TIC y empleados del sector público respecto a la tecnología y su implementación.

Actividad #2: Levantamiento de requerimientos funcionales Levantamiento de requerimientos que permitan la eficaz implementación de la tecnología blockchain en el sector público.

Actividad #3: Publicación de requerimientos Al ser una tecnología emergente se requiere que todos los actores relacionados con el ecosistema conozcan los requerimientos bajo los cuales se implementará la tecnología blockchain, de tal manera que se desarrolle un trabajo colaborativo.

Actividad #4: Análisis y diseño Diseño de los casos de uso necesarios para la implementación de la tecnología blockchain en el sector público.

Actividad #5: Desarrollar la aplicación DLT Implementación de un sistema de información, basado en la tecnología blockchain en el sector público.

Actividad #6: Validación A partir de los resultados obtenidos, se desarrolla un proceso de mejoramiento que permita optimizar la aplicación.

Actividad #7: Evaluación de impacto Los actores del ecosistema Blockchain desarrollaran actividades de evaluación e impacto, que permita a los ciudadanos y entes gubernamentales conocer e implementar la tecnología Blockchain en el sector público.

3.1.12. Conclusiones.

- La tecnología blockchain elimina los intermediarios y permite trabajar solo con activos digitales.
- Los contratos inteligentes emulan la lógica de las cláusulas contractuales.
- Los contratos inteligentes permiten efectuar transacciones “sin confianza”, monitorear y ejecutar bilateralmente a través de una red digital sin necesidad de un intermediario externo de confianza.
- Los procesos de cadenas de suministros garantizan un eficaz seguimiento a los productos, minimizando la falsificación y asegurando que el cliente obtenga sus productos en óptimas condiciones.

3.1.13. Recomendaciones.

- Generar un marco normativo, para que la tecnología blockchain pueda ser implementada en el sector público.
- Desarrollar procesos de transferencia de conocimiento que permitan al ecosistema blockchain interiorizar la tecnología y desarrollar aplicaciones en el sector público.
- Las personas que participan en un proyecto de blockchain deben comprender la tecnología o al menos sus implicaciones.
- Con blockchain no puede desarrollar procesos de almacenamiento de altos volúmenes de información.
- Si la solución propuesta no busca o no requiere administrar de manera cuidadosa el intercambio de valor de un activo digital, entonces quizá una tecnología diferente a blockchain pueda ser una mejor solución.

3.2. Principios y buenas prácticas sobre tecnología blockchain.

El Foro Económico Mundial ha publicado los Principios bajo los cuáles se busca que los organismos se basen en el desarrollo de aplicaciones bajo tecnología blockchain. ¿Qué es lo que está en juego? Las organizaciones enfrentan algunos de los siguientes retos al desarrollar tecnologías como blockchain:

- Riesgos para los usuarios: uno de los aspectos que debe tenerse en cuenta es la protección de los derechos de los usuarios, en especial la protección de sus datos personales. Las propiedades de blockchain como tecnología fundamental

hacen que estas consideraciones sean particularmente importantes, dado el potencial daño y los efectos posteriores que pueden prevenir en la verificación de posibles riesgos en la implementación del proyecto.

▪ Ampliación de las brechas existentes: Es posible que el uso de tecnologías pueda ampliar brechas existentes, por ejemplo, a pesar de que se habla del potencial de la inclusión financiera, si no se diseña con cuidado, blockchain puede conducir a una mayor exclusión y explotación de poblaciones vulnerables. ¿Qué se puede hacer? Al igual que con cualquier tecnología, las promesas y los peligros finales de la tecnología blockchain se reducirán a las decisiones individuales tomadas en su estrategia, desarrollo e implementación. Es imposible controlar todas estas opciones de diseño, pero hay espacio para asegurar la alineación entre los actores clave, entre estos definir cuáles deberían ser los estándares mínimos para la tecnología.

El Consejo Global de Blockchain del Foro Económico Mundial ha creado una "Declaración de Derechos Blockchain: Principios de Diseño para un Futuro Descentralizado", cuyo objetivo es alinear a los líderes del sector privado, los formuladores de políticas y los consumidores en una visión fundamental de cómo los usuarios pueden y deben ser protegidos a medida que se desarrolla la tecnología blockchain, particularmente en torno a los siguientes pilares:

- Agencia e interoperabilidad: el derecho a poseer y administrar datos.
- Privacidad y seguridad: el derecho a la protección de datos.
- Transparencia y accesibilidad: El derecho a la información sobre el sistema.
- Rendición de cuentas y gobernanza: el derecho a comprender los recursos disponibles.

Los 16 principios: Las aplicaciones creadas sobre sistemas basados en blockchain deben conservar los siguientes derechos de participante. Un participante debe tener acceso a información que le permita:

I. Comprender cómo se opera un servicio, incluidos los riesgos potenciales del servicio, la disponibilidad del código fuente y las reglas y estándares en los que se basa.

II. Comprender los riesgos y beneficios potenciales del uso de la tecnología blockchain de un servicio.

III. Comprender las expectativas de rendimiento del sistema y dónde reside la responsabilidad de la prestación del servicio dado.

IV. Comprender los derechos y obligaciones de los diferentes participantes del sistema. Un participante debe poder:

V. Crear, administrar y almacenar de forma independiente claves criptográficas.

VI. Gestionar el consentimiento de los datos almacenados en sistemas de terceros.

VII. Transferir datos entre sistemas interoperables o partes de un sistema.

VIII. Revocar el consentimiento para la recopilación de datos en el futuro.

IX. Tener acceso a información suficiente para facilitar la interoperabilidad del sistema.

X. Evaluar si sus datos están en riesgo mediante los procedimientos de divulgación adecuados, que pueden incluir, entre otros, un examen de los resultados de la auditoría, las certificaciones o el código fuente.

XI. Tener sus datos protegidos de acuerdo con estándares técnicos de seguridad reconocidos internacionalmente.

XII. Limitar la recopilación de datos a lo que sea necesario y el uso de datos para el propósito para el que se proporcionaron.

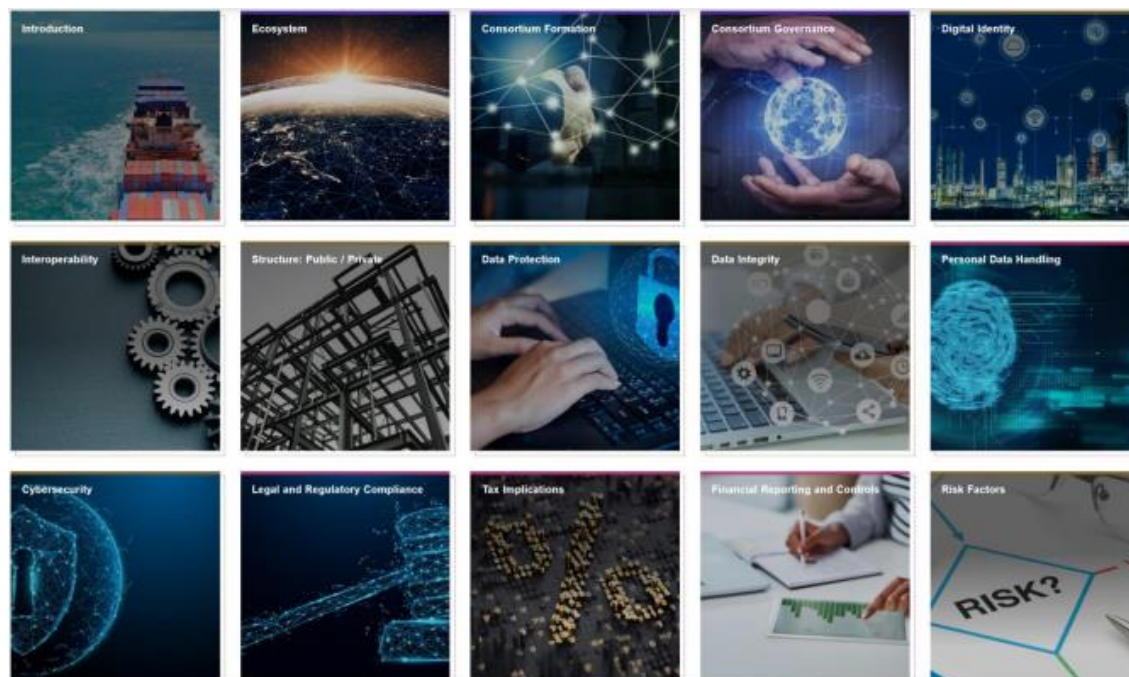
XIII. Verifique, a través de herramientas de terceros o creadas por usted mismo, que las operaciones se hayan completado y confirmado de acuerdo con las reglas del sistema.

XIV. Acceder a la información necesaria para: (a) comprender la gobernanza y las reglas del sistema y (b) buscar mecanismos de recurso eficaces.

XV. Desactive el uso de aplicaciones que no tratan los datos de acuerdo con los estándares de protección de datos y gobierno reconocidos internacionalmente.

XV. Rectifique los datos que demuestren ser falsos, inexactos o incompletos cuando sea necesario.

3.2. kit de herramientas blockchain del Foro Económico Mundial



Fuente: Foro Económico Mundial Blockchain Toolkit

Blockchain tiene el potencial de revolucionar la forma en que las empresas compiten y las partes interesadas colaboran en el mundo de las cadenas de suministro. Dado que la tecnología es incipiente, el Foro Económico Mundial ha publicado este conjunto de herramientas para proporcionar orientación para el desarrollo y la implementación de nuevas soluciones blockchain. La figura anterior, muestra los elementos constitutivos de ese kit de herramientas, diseñado para una organización que quiera integrar una solución de las características de blockchain. En esta guía se presentarán de manera resumida algunos aspectos de los módulos del kit elaborado por el Foro Económico Mundial, se recomienda hacer una consulta de cada módulo y obtener un mejor entendimiento de todos los conceptos.

3.2.1. Ecosistema.

Blockchain es más efectivo cuando se usa para automatizar flujos de trabajo entre las organizaciones lo que permite impulsar los procesos de negocio y el intercambio de datos. Sin embargo, hacerlo de manera eficaz requiere un ecosistema con una estructura de gobernanza acordada que defina los roles y comportamientos de los participantes, cómo y qué información se compartirá entre los participantes, la propiedad de los datos, los criterios de entrada y salida y la también la financiación. Un Registro Distribuido conlleva algunas ventajas notables, que incluyen descentralización, mayor flexibilidad, mayor transparencia, seguimiento de auditoría, independencia y más. Pero, como cualquier nueva tecnología implementada en la operación diaria de una organización, blockchain

también conlleva consideraciones adicionales, como administrar qué información es apropiada para poner en la red y quién puede escribir esa información en la cadena compartida.

3.2.2. Formación de alianzas.

Uno de los aspectos que pueden ser claves en la exploración y adopción de blockchain es la de formar una alianza entre múltiples partes interesadas con la intención de crear, implementar, acelerar y escalar soluciones de blockchain para un sector específico. El modelo de alianza permite a los participantes aprovechar la tecnología blockchain al equilibrar los beneficios, que a menudo incluyen permitir que los competidores colaboren para crear soluciones descentralizadas en red para resolver problemas compartidos, al tiempo que protege su ventaja competitiva individualmente, manteniendo la confidencialidad de los datos sensibles. A medida que esta tecnología continúa emergiendo, el enfoque de consorcio puede llevar la investigación y el desarrollo (I + D) al siguiente nivel más allá de lo que una empresa puede lograr por sí sola para desarrollar nuevas soluciones de blockchain que aborden casos de uso específicos de la cadena de suministro. Esta alianza puede evolucionar a medida que se implementan las soluciones para fomentar la adopción, crear estándares e interoperar con otras organizaciones comerciales y alianzas adicionales. Por ejemplo, una prueba de concepto (PoC) puede comenzar internamente en una sola empresa o con un pequeño grupo de participantes dentro de una industria, luego crecer con el tiempo en términos de participación vertical y horizontal, sofisticación técnica o ambos, en la que la participación del gobierno puede ser importante para que se aprenda más de esta tecnología y sus ventajas.

3.2.3. Gobernanza de la alianza.

La buena gobernanza es un indicador clave del buen funcionamiento de una alianza. Crear el marco para que las entidades trabajen juntas de manera efectiva es tan importante como construir la solución tecnológica relacionada. Inevitablemente, los miembros de una alianza tendrán diferentes prioridades e intereses que deben conciliarse. Por lo tanto, antes de formar una alianza, es importante planificar de antemano cómo se tomarán las decisiones y cómo se resolverán las diferencias de opinión. Si bien no existe una solución única que permita dar cabida a todos los intereses dispares, establecer reglas de tránsito desde el principio puede ayudar en gran medida a suavizar los desacuerdos, o incluso a prevenirlos por completo. Decidir sobre un modelo de gobernanza es importante en la misma formación de una alianza, ya que el modelo de gobernanza es clave para todas las demás tomas de decisiones. Las decisiones iniciales

importantes incluyen quién financiará las operaciones, quién será responsable del desarrollo de nueva tecnología y quién será el propietario de esta tecnología. Sin embargo, tenga en cuenta que también es posible, e incluso probable, que el modelo de gobernanza de una alianza cambie con el tiempo a medida que la solución blockchain se vuelve más sofisticada, agregando nuevos participantes y funcionalidades.

3.2.4. Identidad Digital en cadenas de abastecimiento.

Con la creciente complejidad de las cadenas de suministro, las identidades confiables de los pares en la red de suministro son fundamentales para operaciones eficientes. Una identidad confiable puede abarcar diferentes contextos, tanto físicos como digitales. Este módulo del Kit de Herramientas se centra en la última forma de identidad: una presencia en línea que representa y actúa en nombre de un actor externo. Este módulo cubre consideraciones y preguntas para guiar el diseño de un sistema de identidad digital responsable. La información de este módulo asume que blockchain es la capacidad clave que permite la transformación en un caso de uso en la cadena de suministro. Este módulo debe ser aprovechado por los diseñadores, propietarios y operadores de la red blockchain para enfocar la identidad digital como uno de los componentes clave de la capacidad blockchain. Contiene consideraciones generales sobre el diseño de un sistema de identidad digital, incluidos quiénes son los actores, decisiones tecnológicas, modelos comerciales, protección de datos de identidad, procesos y gobernanza. También incluye un área de enfoque específica destinada a informar el diseño de un sistema de identidad descentralizado.

3.2.5. Interoperabilidad.

Uno de los aspectos más mencionados a lo largo de esta guía ha sido la interoperabilidad. Sin lugar a dudas constituye un aspecto fundamental para el desarrollo de infraestructuras blockchain intragubernamentales, interinstitucionales e incluso internacionales. La tecnología blockchain, por su propia naturaleza, se basa en interacciones entre pares en torno a Registros Distribuidos que son compartidos. Esto hace que la transformación de un enfoque aislado y fragmentado a la integración de la cadena de valor de un extremo a otro sea más alcanzable, pero también significa que la importancia de la interoperabilidad es imperativa. En los términos más simples, la interoperabilidad exitosa permite al usuario confiar en “sé que lo que veo, es lo que tú ves”. Este módulo del Kit de Herramientas proporciona herramientas para analizar el desafío de hacer que las soluciones blockchain funcionen a la perfección en ese sentido y para elegir el enfoque de interoperabilidad correcto.

3.2.6. Estructura.

Pública / Privada Una de las consideraciones que debe gestionarse es qué modelos de permisos se requieren para el proyecto. Un blockchain pública, como la de Bitcoin, permite a cualquier persona en Internet leer o escribir en el Registro Compartido, mientras que una cadena de bloques administrada por un consorcio o alianza, por ejemplo, podría restringir el acceso a organizaciones asociadas. En última instancia, la decisión de "público versus privado" afectará la funcionalidad, la seguridad, la compatibilidad con los sistemas de otros socios y, quizás lo más importante, el posicionamiento competitivo de las organizaciones en sus proyectos de cadena de suministro. Sin duda, no hay una única respuesta "correcta". Es vital comprender primero los beneficios y los inconvenientes únicos de cada tipo de cadena y luego elegir la que mejor se adapte a los requisitos de su proyecto en particular.

3.2.7. Protección de los Datos.

La pérdida de control percibida sobre los datos es uno de los mayores obstáculos para la adopción de blockchain que enfrentan muchas organizaciones de cadenas de suministro. Sin embargo, con una buena planificación y comunicación del proyecto, este problema se puede mitigar en gran medida. La tecnología blockchain nunca requiere que una organización revele más datos de los que se siente cómoda. Los datos en cadena también se pueden cifrar para que solo puedan utilizarlos las partes autorizadas. Por lo tanto, en el curso de la selección e implementación de una solución blockchain, una organización de cadena de suministro tiene una flexibilidad real para garantizar que aborda tanto sus preocupaciones de protección de datos y privacidad como las de otros socios de la cadena de suministro.

3.2.8. Integridad de los datos.

La integridad de los datos es la propiedad de que los datos utilizados en una solución sean correctos, confiables y útiles para todos los participantes. El término "integridad de los datos" se utiliza aquí en el sentido más amplio y ubicuo en el mundo de la cadena de suministro, refiriéndose no solo a la resistencia a la modificación de datos no intencionada, sino también a la integridad, puntualidad y precisión de los datos durante toda su vida útil. Este módulo cubre las consideraciones típicas para garantizar que los datos utilizados en una solución blockchain sean correctos, confiables, oportunos para todos los participantes y se conserven desde el punto de creación de datos hasta el punto de uso en blockchain. Este módulo enfatiza que la tecnología blockchain no necesariamente garantiza la precisión de los datos ingresados en la cadena. Destaca que, de hecho, existen

múltiples etapas y pasos en los que la integridad de los datos puede verse comprometida.

3.2.9. Tratamiento de datos personales

El tratamiento en materia de datos personales, es un aspecto que debe conllevar al análisis de la normativa vigente de cada país. Por ejemplo, el Reglamento General de Protección de Datos de la Unión Europea, impone obligaciones sobre lo que denomina controladores y procesadores de datos; sin embargo, cuando no hay un proveedor de servicios centralizado como en una red blockchain, ¿quién es responsable de supervisar el tratamiento de los datos personales? Y si una cadena registra datos de manera inmutable, ¿qué significa eso para las obligaciones de borrado si esos datos no se pueden eliminar? Si bien estas consideraciones no tienen por qué ser prohibitivas para comenzar un nuevo proyecto de blockchain, deben abordarse desde el principio, incluso, en algunas circunstancias, por organizaciones de la cadena de suministro que no se encuentran en la jurisdicción donde aplique a la cadena de blockchain. Además, todos los aspectos relacionados con el tratamiento de datos personales, deben ser resueltos teniendo en cuenta las buenas prácticas internacionales, pero asegurando el cumplimiento de la normativa en Santa Fe.

3.2.10. La seguridad cibernética

Cualquier implementación de nueva tecnología debe incluir salvaguardas adecuadas contra estos escenarios de incidentes de seguridad digital o de la información. Aunque la tecnología blockchain está evolucionando rápidamente, existen algunos conceptos de seguridad fundamentales que se pueden aplicar al espacio blockchain de manera efectiva. Después de cubrir estas áreas de enfoque, este módulo del Kit ofrece un marco de gestión de riesgos y un plan de implementación segura de 10 pasos que debería ser útil en una amplia gama de proyectos de la cadena de suministro.

3.2.11. Cumplimiento legal y regulatorio.

Existen algunas consideraciones comunes que los proyectos de blockchain deben abordar desde un punto de vista legal y regulatorio. En el módulo del kit se exponen, algunas recomendaciones para que los proyectos consideren las leyes y reglamentaciones específicas de la jurisdicción y de la industria.

Este Punto lo vamos a desarrollar en detalle por considerar ser de mucha importancia para el presente documento.

La transición a tecnologías de vanguardia a menudo ha implicado un obstáculo importante y la transición a blockchain no es diferente: las leyes escritas

hace décadas no se redactaron teniendo en cuenta el intercambio de datos distribuidos o los contratos de ejecución automática. Esto puede generar incertidumbre sobre los requisitos de cumplimiento de la nueva tecnología dentro de las organizaciones, a veces exacerbada por las diferencias entre los reguladores en diferentes jurisdicciones.

Dicho esto, hay algunas consideraciones comunes que los proyectos de blockchain deben abordar desde un punto de vista legal y regulatorio. A continuación, se presenta una discusión de ellos, con la advertencia de que los proyectos también deben considerar la jurisdicción y las leyes y regulaciones específicas de la industria, y siempre se debe tomar el consejo de los abogados locales donde operan las organizaciones.

3.2.11.1. Cuestiones legales y reglamentarias comunes con el uso de blockchain

¿Cuáles son los problemas legales y regulatorios más comunes que surgen al usar la tecnología blockchain?

Las tecnologías de cadena de bloques pueden exponer al operador de la red de cadena de bloques y/o a los participantes en la red a la incertidumbre legal y regulatoria porque muchos gobiernos y reguladores todavía están trabajando para comprender la cadena de bloques y si ciertas leyes deben actualizarse para abordar adecuadamente la descentralización.

Si bien algunos gobiernos están encabezando la adopción de blockchain, muchos reguladores nacionales y regionales están adoptando un enfoque de esperar y ver, prefiriendo explorar y comprender las implicaciones de blockchain antes de avanzar con requisitos u orientación legales y regulatorios adicionales. La falta de certeza regulatoria y la posición legal y regulatoria en evolución es un desafío para los participantes del mercado, y es necesario que evalúen continuamente su participación en las redes de blockchain.

En esencia, el doble desafío de los participantes de la red blockchain por ahora es garantizar que cumplan con las regulaciones actuales y, al mismo tiempo, mitigar en la medida de lo posible los riesgos comerciales asociados con posibles cambios en el entorno regulatorio.

Los siguientes son algunos de los problemas más comunes relacionados con el cumplimiento que surgen con el uso de la tecnología blockchain, aunque, por supuesto, esto estaría sujeto al caso de uso específico y la jurisdicción y las reglas y regulaciones específicas de la industria.

Jurisdicción:

Blockchain tiene la capacidad de cruzar fronteras jurisdiccionales ya que los nodos en una cadena de bloques pueden ubicarse en cualquier parte del mundo. Esto puede plantear una serie de problemas jurisdiccionales complejos que requieren una cuidadosa consideración en relación con las actividades relevantes de la plataforma y sus participantes, así como las relaciones contractuales entre ellos. Para abordar estos problemas, existe cada vez más una serie de regímenes legales y regulatorios que tienen un efecto extraterritorial, como el RGPD de la Unión Europea o las leyes fiscales. Como resultado, incluso si los usuarios y los nodos de blockchain están ubicados en todo el mundo, las leyes locales aún pueden aplicarse cuando se considere que existe un nexo suficiente con esa jurisdicción.

Régimen regulatorio tecnológicamente neutral:

Los regímenes de licencias y cumplimiento reglamentarios normalmente no se redactan con la intención de regular tecnologías específicas. Más bien, la intención habitual es regular las actividades que la tecnología ayuda a facilitar. Sin embargo, una redacción neutral puede dificultar la interpretación de cómo se debe aplicar la regulación y qué participantes deben ser atrapados. Por lo tanto, es necesario evaluar cuidadosamente la naturaleza y las actividades de una red blockchain y sus participantes y determinar dónde deben ubicarse esa plataforma y sus participantes dentro del panorama regulatorio.

Gobernanza y documentación legal

La naturaleza de utilidad de una plataforma blockchain significa que es necesario documentar adecuadamente la relación entre la red blockchain, el operador de la red (si lo hay) y sus participantes a través de contratos legalmente exigibles. Es importante establecer un modelo de gobernanza claro y sólido con respecto a las interacciones entre los participantes en la red. El modelo también debe establecer claramente los términos y condiciones aplicables a la plataforma blockchain, por ejemplo, los mecanismos mediante los cuales el operador de la red puede implementar cambios en la red o los requisitos en torno a su participación. Deben establecerse criterios objetivos y justos para regir el acceso a la red y la suspensión o terminación de los participantes de la red.

Responsabilidad

Blockchain plantea riesgos nuevos y diferentes como consecuencia de la naturaleza de la tecnología y la forma de operar, incluidos los riesgos relacionados con la seguridad, la confidencialidad, la regulación, la fiscalidad, la protección de datos, la inmutabilidad, la automatización y la descentralización, entre otros riesgos. Por lo tanto, la asignación y atribución de riesgos y responsabilidades en relación con la red blockchain y las transacciones procesadas en la red (incluidos los errores, fallas o mal funcionamiento) deben evaluarse y documentarse cuidadosamente dentro de cada nivel de participación en la red.

Propiedad intelectual (PI)

Para desbloquear verdaderamente el potencial de la cadena de bloques, la tecnología subyacente, incluido su software, deberá compartirse para que se obtenga valor. La naturaleza de tal 'intercambio' depende completamente de la naturaleza específica de la cadena de bloques en cuestión, incluidos sus propósitos, el tema y la relación entre los participantes de la cadena de bloques. Por lo tanto, es importante considerar preguntas sobre la naturaleza de la PI subyacente, la propiedad de la PI y el acuerdo de licencia como parte de la estructuración de la cadena de bloques.

Las consideraciones centrales y las posibles opciones de PI (p. ej., con respecto a la propiedad y licencia de PI) no son, en gran medida, diferentes a las de cualquier otro régimen tradicional de PI o acuerdo de desarrollo de software y, dependiendo de las disposiciones de licencia acordadas, es probable que dependan de si esos requisitos específicos podrían dar a un cliente una ventaja competitiva y/o pueden ser utilizados por el proveedor de la cadena de bloques (es decir, si existe alguna exclusividad, cuál es la naturaleza y el alcance de la disposición de licencia). Los desarrolladores y propietarios de IP tendrán que determinar su estrategia de IP, incluido quién posee qué y la protección en todos los niveles. Es probable que los proveedores deseen capitalizar cualquier otro beneficio comercial que se genere a partir de la cadena de bloques, incluida la comercialización del conjunto de datos subyacente mediante la concesión de licencias de propiedad intelectual subyacente. Especialmente en cadenas de bloques públicas basadas en software de código abierto, esto puede ser un desafío, pero se debe considerar la creación de mecanismos para identificar quién creó y quién posee qué (por ejemplo, sellos de tiempo). Además de las consideraciones sobre la propiedad de la PI en la cadena de bloques subyacente, otra cuestión importante se relaciona con si la

cadena de bloques se puede utilizar para registrar la propiedad, el uso y la remuneración de las licencias/transacciones de PI.

Privacidad de datos personales

Uno de los puntos de venta únicos clave de un sistema de cadena de bloques es que una vez que se almacenan los datos, no se pueden modificar fácilmente, en todo caso. Esto claramente tiene implicaciones para la privacidad de los datos, particularmente cuando los datos relevantes son datos personales o metadatos suficientes para revelar los detalles personales de alguien. La regulación de protección de datos puede exigir que los datos personales se mantengan actualizados y precisos o que se eliminen a discreción del individuo, y la inmutabilidad de un sistema de cadena de bloques puede no ser coherente con dichos requisitos.

Organizaciones autónomas descentralizadas (DAO)

Las DAO son esencialmente entidades u organizaciones digitales en línea que operan a través de la implementación de reglas precodificadas mantenidas en una plataforma blockchain. La naturaleza descentralizada de las DAO presenta preguntas únicas que no necesitaban ser abordadas previamente ya que las entidades tradicionales estaban centralizadas y tenían una estructura y forma legal reconocible. ¿Qué estatus legal o responsabilidad se adjuntará a una DAO? ¿Son corporaciones simples, sociedades, personas jurídicas, contratos legales o algo más? Esto dependerá de cómo esté estructurado cada DAO y la jurisdicción en la que se incorpore el DAO (si corresponde).

Contratos inteligentes

Los contratos inteligentes no siempre o necesariamente son contratos legales en el sentido tradicional, a pesar de la palabra "contrato". Si los contratos inteligentes se consideran contratos legales es una cuestión de si los elementos de un contrato legal están presentes. En esencia, los contratos inteligentes son códigos informáticos autoejecutables y, como resultado, su uso puede presentar dudas sobre su cumplimiento si se intenta analizarlos dentro de la definición tradicional de "contrato legal". Para mayor aclaración, un contrato inteligente no es una cadena de bloques per se, sino una aplicación de la cadena de bloques, es decir, un posible uso de la cadena de bloques. Muchos contratos inteligentes están

estructurados para automatizaciones, instrucciones o cláusulas de contratos legales separados pero no constituyen contratos legales en sí mismos y estos contratos no legales presentan menos riesgos legales.

Sin embargo, algunos contratos inteligentes en sí mismos se están estructurando como contratos legales y, por lo tanto, tienen toda la fuerza de la ley. En tales casos, será necesario comprender cómo cumplen las condiciones previas para la formación de contratos en diferentes jurisdicciones, así como también cómo serán interpretados por un tribunal u organismo arbitral en caso de disputa.

Salir de la cadena de bloques

La necesidad de asistencia de salida estará determinada en gran parte por la solución específica y la medida en que el proveedor de la cadena de bloques conserva los datos del cliente y cómo se almacenan los datos en la cadena de bloques. Si el cliente no tiene su propia copia de los datos, necesitará asistencia de migración de datos para garantizar que el proveedor esté obligado a entregar todos esos datos al vencimiento o terminación.

Los problemas descritos en esta área de enfoque no son una lista exhaustiva de todas las posibles consideraciones legales y reglamentarias. Las leyes de localización de datos y las leyes específicas de la industria deben tenerse en cuenta cuando sea pertinente.

3.2.11.2. Cuestiones legales al establecer una red blockchain

¿Cuáles son las preocupaciones legales al construir y establecer una red blockchain?

Es importante que los participantes de la red blockchain consideren una serie de cuestiones, incluida la estructura legal, la responsabilidad y el modelo de gobernanza de una red blockchain y que establezcan claramente todas las reglas, derechos y obligaciones en la documentación legal. La documentación legal clara es fundamental para garantizar que los participantes tengan claridad sobre el funcionamiento de la red blockchain.

La documentación legal clara es fundamental para garantizar que los participantes tengan claridad sobre el funcionamiento de la red blockchain.

A continuación se presentan algunas consideraciones que los participantes de la red blockchain deben tener desde el principio antes de embarcarse en su proyecto blockchain:

Estructura legal

- ¿Cómo se estructurará la red blockchain desde una perspectiva legal?
- ¿La red se ubicará dentro de una entidad legal, como una empresa o sociedad?
- ¿Habrá uno o más operadores de red?
- ¿Quién posee y controla la red y cómo se estructura su propiedad?
- ¿Cómo se unirán los participantes a la red? ¿Tomarán una participación de propiedad?

Documentación legal

Por ejemplo, se debe establecer documentación legal para la gobernanza y los términos de uso de la red blockchain, la relación entre los participantes de la red blockchain, el operador de la red y los usuarios, la limitación de responsabilidades y la propiedad y el uso de la PI.

Como se mencionó anteriormente, la documentación legal clara sobre todos los aspectos de la red blockchain, por ejemplo, la estructura legal, la responsabilidad y la gobernanza, es esencial para la claridad. Además, es importante asegurarse de que lo siguiente se considere y se cubra dentro del alcance de la documentación legal de cualquier red de blockchain.

- ¿La red blockchain tendrá un libro de reglas/términos de uso legalmente exigibles que los participantes deban suscribir? ¿Existen sanciones de derecho civil por incumplimiento de las normas?
- Alternativamente, ¿cada participante firmará un contrato por separado con el operador de la red y/o los propietarios de la red? ¿Se negociará este contrato por separado de manera que cada participante esté sujeto a términos separados y distintos?
- ¿Cuáles son los derechos y obligaciones de los participantes? ¿Habrá diferentes clases de participantes con diferentes derechos y obligaciones? De ser así, ¿cómo garantiza la red/el operador de la red un trato justo a las diferentes clases de participantes?
- ¿Hay una tarifa para que los participantes se unan a la red y cómo está estructurada?
- ¿Se beneficiarán los participantes de los ingresos de la red y, de ser así, cómo se estructurarán los pagos?

- ¿Existen consideraciones antimonopolio y existen medidas contractuales (y de otro tipo) que se pueden tomar para mitigarlas?
- ¿La red utiliza contratos inteligentes y estos son legalmente exigibles?
- ¿Existen limitaciones de responsabilidad e indemnizaciones? Si es así, ¿quién se beneficia? ¿Son exigibles en todas las jurisdicciones pertinentes?
- ¿Cómo se tratará la propiedad/licencia y/u otros derechos de propiedad intelectual?
- ¿Cómo deben estructurarse los derechos de rescisión/salida? ¿Qué datos deben permanecer dentro de la red en la terminación?
- ¿Cómo protege la red la confidencialidad de sus miembros y qué disposiciones de confidencialidad deben incluirse en la documentación?

Responsabilidad legal

- ¿Cómo se determinará la responsabilidad de los participantes de la red? Idealmente, esto debería determinarse desde el principio y anotarse en el contrato (si lo hay) firmado por los participantes de la red.
- ¿Cuáles serán los criterios para los factores que se considerarán al evaluar la distribución de la responsabilidad?

Gobernanza

- ¿Cuál es el modelo de gobernanza de la red blockchain? Por ejemplo, ¿está gobernado por el operador de red, gobernado por un comité de participantes o gobernado por un mecanismo de participación/votación?
- ¿Quién es responsable de hacer cumplir las reglas de la red?
- ¿Quién es responsable de la diligencia debida sobre los participantes?
- ¿Cuáles son los arreglos necesarios para la recuperación ante desastres, la continuidad del negocio y la planificación de contingencias y quién es responsable de ejecutarlos?

Requisitos de subcontratación

Si se contemplan acuerdos de subcontratación, los participantes deben preguntarse:

- ¿Constituyen los arreglos una subcontratación y es necesario celebrar un acuerdo de servicio?

- Si se aplica un acuerdo de servicio, ¿se celebra con el operador de la plataforma o con cada nodo/usuario de forma consecutiva?
- ¿Existen requisitos reglamentarios que se aplican a la subcontratación?

Violación de la ley antimonopolio

Puede haber riesgos antimonopolio derivados de los modelos de colaboración de blockchain (por ejemplo, consorcios) que se consideran como:

- Abuso de posición dominante: atraer una parte significativa del mercado a un ecosistema cerrado que genera una desventaja para los competidores y los consumidores.
- Desfavorecer a los competidores, por ejemplo, excluyéndolos, ofreciendo descuentos a socios seleccionados, castigando a los competidores utilizando monedas privadas alternativas.
- Conducta colusoria: fijación o manipulación de precios para obtener una ventaja competitiva.
- Entrar en colusión entre miembros importantes dentro de un consorcio de blockchain que conduce a la manipulación de los servicios ofrecidos a entidades más pequeñas, confirmación preferencial de transacciones, etc.

Antilavado de dinero, KYC y sanciones

Los participantes de la red Blockchain, en particular los operadores de red, deben considerar los siguientes riesgos e implementar sistemas y controles apropiados para mitigarlos:

- Incumplimiento de las normas AML/KYC aplicables o requisitos de sanciones.
- Anonimato de transacciones e identidades en la cadena de bloques.
- Falta de rigor en la realización de controles “Conozca a su proveedor”.
- Pago a/desde partidos o países en la lista de sanciones o con estatus de “persona políticamente expuesta”.
- Implementación de aplicaciones distribuidas que aceptan o transmiten valor sin los controles y programas de cumplimiento necesarios.

- Falta de actividades de vigilancia y monitoreo para detectar y prevenir actividades inapropiadas'; o realizar análisis de tendencias de patrones que informan el uso.

Los participantes de la red Blockchain también deben considerar quién debe asumir la responsabilidad general de las funciones AML/KYC.

Protección de datos y ciberseguridad

Hay una serie de leyes vigentes que rigen la ciberseguridad, en particular la Directiva de la UE sobre seguridad de redes y sistemas de información (Directiva NIS). Esto proporciona medidas legales para impulsar el nivel general de ciberseguridad en la UE al garantizar, entre otras cosas, que los "operadores de servicios esenciales" en sectores que son vitales para la economía y la sociedad (por ejemplo, banca, infraestructuras del mercado financiero e infraestructura digital) deberá tomar las medidas de seguridad adecuadas y notificar los incidentes graves de ciberseguridad a la autoridad nacional competente.

La protección de datos y la ciberseguridad deben considerarse cuidadosamente al diseñar una solución de cadena de bloques. Las preguntas importantes que debe hacerse en esta área incluyen:

Aunque, estrictamente hablando, la ciberseguridad y la protección de datos son áreas legales separadas, a menudo se agrupan porque ambas tienen como objetivo salvaguardar los datos (personales). En consecuencia, algunos de sus principios clave en torno a la implementación y el mantenimiento de un cierto nivel de seguridad, o el tratamiento de las filtraciones de datos, se superponen.

- ¿Cómo se diseña una solución blockchain para cumplir con las leyes de protección de datos?
- ¿Se puede convertir la protección de datos en una parte esencial de la funcionalidad central de la cadena de suministro y cómo se puede construir un marco sólido de cumplimiento de la protección de datos?
- ¿Se tratarán datos personales? En caso afirmativo, ¿qué categorías de datos personales se procesarán?
- ¿La red blockchain entrará en el ámbito territorial de una regulación de privacidad de datos en particular, como el RGPD o la CCPA?
- ¿Qué tipos de tecnologías se pueden utilizar para cumplir con los requisitos de la normativa de protección de datos?

- ¿Cómo se mantiene la precisión de los datos? ¿Se pueden satisfacer los derechos de los interesados, como el acceso, la corrección y la eliminación de datos, cuando un interesado ejerce uno de esos derechos?
- ¿Qué tipo de vulnerabilidades potenciales hay en la solución? ¿Qué tipo de estructura de cadena de bloques (pública/privada, sin permiso/autorizada) ofrece el nivel de seguridad necesario? ¿Debe el gobierno de la seguridad estar completamente descentralizado o controlado por un grupo selecto?

Propiedad intelectual

Las consideraciones de PI en una red de cadena de bloques dependerán de la naturaleza de la cadena de bloques específica en cuestión, incluidos sus propósitos, la relación entre los participantes de la cadena de bloques, el software subyacente (por ejemplo, de código abierto) y si la PI subyacente está destinada a ser comercializada. La importancia de proteger la PI viene como una extensión de abordar los secretos comerciales, la información confidencial y otros derechos de propiedad potencialmente contenidos en los datos compartidos o vinculados a una cadena de bloques. Las siguientes son preocupaciones y preguntas legales fundamentales para las consideraciones y preguntas de los participantes de la red blockchain sobre la propiedad intelectual en las cadenas de bloques:

- Cada tipo de propiedad intelectual (p. ej., patentes, marcas registradas, derechos de autor, secretos comerciales) tiene sus propias reglas de propiedad (p. ej., la doctrina del trabajo por contrato en derechos de autor que se aplica a ciertas jurisdicciones). Las partes deberán considerar cada tipo de derecho de PI que se crearía con respecto a una red blockchain de cadena de suministro. Los derechos de PI varían en cada jurisdicción. Por lo tanto, los detalles jurisdiccionales deben considerarse junto con la ley que rige el acuerdo de blockchain (es decir, el acuerdo para acceder y utilizar la infraestructura de blockchain).
 - ¿Será clave determinar quién posee la IP en la cadena de bloques?
 - Dependiendo de la estructura de la cadena de bloques, la PI en la cadena de bloques puede ser propiedad de una o varias partes (por ejemplo, la propiedad conjunta, a través de esto no siempre es sencillo y debe considerarse cuidadosamente dentro del contexto de la cadena de bloques específica en cuestión). Por ejemplo, la PI en la cadena de bloques podría ser propiedad de la empresa detrás de la plataforma (o su accionista/inversor), el desarrollador, los miembros fundadores del consorcio, el operador del nodo o los participantes que

aportan conocimientos y datos para desarrollar la plataforma. Esta evaluación puede volverse más compleja cuando se utiliza software de código abierto creado por comunidades de desarrolladores.

- Cuando un consorcio participe en el desarrollo de una plataforma de cadena de bloques, se debe cubrir la propiedad de los derechos de propiedad intelectual (incluida la propiedad intelectual de primer plano y de fondo), así como los derechos de licencia asociados (y los parámetros que acompañan a dicha licencia, por ejemplo, limitada, mundial, etc.). como parte del acuerdo de preconsorcio o consorcio, en su caso.

- Es necesario considerar cómo los acuerdos de membresía asignarán los derechos de propiedad intelectual y la licencia de propiedad intelectual a los participantes de la red blockchain, o si existe una licencia implícita para los usuarios de blockchain. Como parte de esto, se deben considerar: los términos de la concesión de licencias de PI a los participantes de la red, incluido qué PI se licencia, si las licencias se otorgan de forma exclusiva/no exclusiva, o si se otorgan en forma justa, razonable y no discriminatorios?

- ¿Cuál es el valor de la IP en la red blockchain y alguna de las IP está destinada a la comercialización?

- ¿Cómo se otorga acceso a las partes previstas? ¿Es un acuerdo de depósito en garantía un medio apropiado para mantener cualquier código fuente en el software, por ejemplo? Es importante entender la relación contractual y las implicaciones relevantes (precios de transferencia, diseño del modelo).

- Riesgos relacionados con la PI
 - Falta de claridad sobre el modelo de gestión de PI más óptimo para un consorcio de cadena de bloques, si corresponde (p. ej., propiedad de los principales participantes, propiedad del desarrollador, uso de fuente abierta, etc.)
 - Riesgo de monetización subóptima de la propiedad intelectual creada en la cadena de bloques
 - Riesgo de infracción de PI dentro de un consorcio o por otros consorcios ya que algunas organizaciones forman parte de múltiples consorcios
 - Riesgo de falta de control sobre cómo los miembros y terceros pueden contribuir/mejorar una IP actual debido a la responsabilidad compartida en blockchain
 - Riesgo relacionado con el incumplimiento de los términos de licencia de código abierto subyacentes de las cadenas de bloques que se basan, por ejemplo, en los libros de contabilidad de Ethereum o Bitcoin por parte de los desarrolladores de software

- Riesgo en torno a la mejora potencial del software de código abierto, incluidas las posibles críticas cuando se realiza un "lavado abierto" (cuando el software propietario se presenta como de código abierto pero en realidad, la contribución del código clave se retiene de los repositorios públicos)
- Complejidades e incertidumbres involucradas en el cumplimiento de las leyes de protección de la PI cuando la cadena de bloques se extiende a través de múltiples jurisdicciones
- Riesgo relacionado con la falta de apoyo de los miembros en el ciclo de vida de desarrollo o mantenimiento de IP
- Incertidumbre sobre el intercambio de IP en caso de insolvencia (por ejemplo, cuenta de depósito en garantía para mantener la IP)
 - Considere implicaciones adicionales de PI en estructuras de cadena de bloques más complicadas que se ocupan de los derechos de PI de terceros para ciertos casos de uso (por ejemplo, lucha contra la falsificación, gestión de marcas, aplicación de los derechos de PI).
 - Otra pregunta importante se relaciona con si la cadena de bloques se puede utilizar para registrar la propiedad, el uso y la remuneración de las licencias/transacciones de PI.

3.2.11.3. ¿Formando una red?

Además de diseñar la gobernanza del consorcio de una manera que sea útil para el éxito de un proyecto, también hay algunos aspectos de la gobernanza que es útil considerar para evitar disputas legales.

- Punto de partida para identificar asuntos legales y regulatorios
- Esta lista de verificación pretende ser un punto de partida útil de las consideraciones legales y reglamentarias clave para cualquier proyecto de blockchain en el área de las cadenas de suministro. Cualquiera que esté considerando un nuevo proyecto de cadena de bloques en esta área debería ayudar a comprender rápidamente algunos de los obstáculos legales y regulatorios comunes que deberán abordarse.
 - La lista de verificación no pretende ser una lista exhaustiva de cuestiones legales y reglamentarias y no reemplaza el asesoramiento legal específico. Este último deberá buscarse caso por caso para cada proyecto, ya que los requisitos legales y reglamentarios siempre serán específicos del proyecto. Sin embargo, esta lista de verificación está destinada a ayudar a enmarcar los problemas clave y debería ser útil como punto de partida en el proceso de

participación con asesores legales para cualquier proyecto de blockchain en el área de las cadenas de suministro.

- Preocupaciones generales
- Esta lista de verificación cubre consideraciones de cumplimiento de alto nivel relacionadas con el uso de blockchain:
 - casillas de verificación
 - ¿Cuáles son los regímenes legales y reglamentarios aplicables a las transacciones previstas en la red blockchain?
 - ¿Cómo monitoreará y hará cumplir las normas?
 - ¿Cómo abordar y mitigar los riesgos relacionados con los requisitos antimonopolio, antilavado de dinero (AML) y "conozca a su cliente" (KYC), protección de datos y ciberseguridad?
 - ¿Cómo actualizar la gobernanza cuando se identifican nuevas regulaciones o se agregan nuevos miembros a un consorcio?
 - ¿Cómo se hará cumplir el modelo de gobernanza de la red blockchain?
 - ¿Cómo garantizar la exigibilidad de los contratos inteligentes?
 - ¿Cuáles son los regímenes legales y regulatorios aplicables a las transacciones previstas en la plataforma/red de blockchain?
 - ¿Cuáles son los derechos de auditoría de los participantes?
 - ¿Quién hará cumplir los modelos de gobernanza?
 - ¿Quién participará en la creación del modelo de gobierno, estatutos, etcétera?
 - ¿Cómo se pagarán las sanciones y se realizarán las evaluaciones?
 - ¿Qué estándares de auditoría se han definido para la solución blockchain y sus participantes?
- Riesgos de la industria/producto
- Esta lista de verificación cubre consideraciones de cumplimiento normativo y legal de alto nivel relacionadas con los riesgos de la industria/producto cuando se usa blockchain.
 - casillas de verificación
 - ¿Existen requisitos regulatorios de licencia y/o cumplimiento que se aplican a la industria relevante y/o al producto relevante que se va a comercializar?
 - ¿Existen requisitos reglamentarios de divulgación que deben cumplir los participantes en esa industria, o requisitos de divulgación específicos del producto que se aplican?

- ¿Existen normas o reglamentos que cubran la infraestructura del mercado relacionada con la industria y/o los productos relevantes?
- ¿Los diferentes aspectos de la plataforma se tratan de manera diferente desde una perspectiva regulatoria? Por ejemplo, ¿algunas actividades en la plataforma están reguladas mientras que otras no lo estarían?
- Riesgos de jurisdicción
- Esta lista de verificación cubre las consideraciones de cumplimiento normativo y legal de alto nivel relacionadas con los riesgos de jurisdicción cuando se usa blockchain.
- casillas de verificación
- ¿Cuáles son las jurisdicciones del operador de la red blockchain (si corresponde), los participantes de la red y los mercados objetivo de los participantes de la red?
- ¿Cómo caracterizarían los reguladores locales en esas jurisdicciones las actividades de la red/operador de red, los participantes y las transacciones que tienen lugar en la red?
- ¿Se aplican diferentes estándares regulatorios y de licencias en diferentes jurisdicciones y se pueden cumplir caso por caso o es necesario adoptar un enfoque de máximo común denominador?
- ¿La plataforma implica la transferencia de criptomonedas o criptoactivos? Existe una amplia divergencia sobre el estado regulatorio de las criptomonedas y los criptoactivos entre jurisdicciones y, por lo tanto, será importante evaluar las obligaciones regulatorias de una plataforma transfronteriza que implique la transferencia de este tipo de activos.
- ¿La transacción implica firmas electrónicas? Existe un enfoque divergente sobre la aplicabilidad de los documentos ejecutados mediante firmas electrónicas, y será importante evaluar y determinar que las firmas electrónicas son válidas en las jurisdicciones relevantes en las que opera la plataforma.
- ¿La plataforma busca digitalizar los tipos existentes de contratos legales en papel que tienen requisitos de formalidad especiales? En algunas jurisdicciones, puede que no sea posible replicar digitalmente ciertos tipos de contratos legales en papel.

3.2.11.4. Marco regulatorio de las criptomonedas en Argentina

UIF-GAFI La primera y (hasta el momento) la única definición normativa en Argentina del concepto “moneda virtual” fue dado por la Unidad de Información Financiera (UIF) mediante la Resolución 300/2014 (B.O. 10/07/2014). Siguiendo lo estipulado por el Grupo de Acción Financiera Internacional (GAFI, 2014), la UIF las

definió (art. 2 de la Res. 300) como: “...la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción. En este sentido las monedas virtuales se diferencian del dinero electrónico, que es un mecanismo para transferir digitalmente monedas fiduciarias, es decir, mediante el cual se transfieren electrónicamente monedas que tienen curso legal en algún país o jurisdicción”. Mediante la Resolución 300, la UIF también modifica el artículo 15-ter de la Resolución-UIF 70/2011, el cual, desde entonces, exige a los Sujetos Obligados enumerados en los incisos 1, 2, 3, 4, 5, 7, 8, 9, 11, 12, 13, 18, 19, 20, 21, 22 y 23 del art. 20 de la Ley N° 25.246 (entidades financieras, empresas autorizadas por la CNV, etc) a informar, a través del sitio www.uif.gov.ar de la UIF, todas las operaciones efectuadas con monedas virtuales. Estos reportes deben efectuarse mensualmente, hasta el día 15 de cada mes, y contener la información correspondiente a las operaciones realizadas en el mes calendario inmediato anterior. Como se aprecia, la definición de la UIF abarca sólo a las “monedas virtuales” y no a las “monedas digitales” o “criptomonedas”.

Por su parte, el organismo internacional GAFI sí sostiene que por “monedas digitales” debe entenderse “...una representación digital de cualquier moneda virtual (no dinero fiduciario) o de dinero electrónico (dinero fiduciario)...” (GAFI, 2014). A su vez, el GAFI advierte sobre los riesgos frente al lavado de activos y financiación del terrorismo que estos activos representan (pueden ser canjeadas por dinero fiduciario y/o por otras monedas virtuales y ser utilizadas para transferencias internacionales bajo un casi completo anonimato). Esta misma preocupación es compartida por muchos países.

Además de la expuesta en la Resolución 300, ni UIF ni ningún otro organismo local ha brindado una nueva definición de qué se debe entender por “monedas virtuales”. Y, como se verá más adelante, recién con la reforma tributaria de fines de 2017 se ha incorporado la expresión “moneda digital” al cuerpo normativo argentino. Cabe señalar que la Resolución 300 indica que las monedas virtuales “...ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción”, sin embargo, en la actualidad existen países que ya han emitido en forma oficial su “criptomoneda” (como Venezuela y su petro).

En conclusión, lamentablemente no se cuenta hasta hoy con una clara, completa y actualizada definición de los conceptos “moneda virtual”, “moneda digital”, “criptomonedas” y “criptoactivo”.

El 04/12/2017 la Comisión Nacional de Valores (CNV) emitió un comunicado alertando a los inversores sobre los potenciales peligros de las ofertas iniciales (ICO) de monedas virtuales o tokens. Es dable señalar que aquí se habla de las ICO y no de la normal operatoria de compra y venta de monedas virtuales. En el comunicado la CNV sostiene que se denomina ICOs “a la forma digital de recaudar fondos del público a través de la oferta inicial de monedas virtuales o tokens, implementada sobre una cadena de bloques o blockchain”. Y agrega que son inversiones especulativas de alto riesgo debido a la: “(a) falta de regulación específica, (b) volatilidad de precios y falta 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”. Y concluye que “solo debería invertir en ICOs un inversor experto, que está capacitado para analizar el proyecto financiado por la ICO y está preparado para perder, eventualmente, toda su inversión”. Lamentablemente, esta alerta fue la única declaración de la CNV sobre el tema, al menos hasta la fecha de hoy. De este texto, que ni siquiera es una norma, no se pueden extraer muchas conclusiones más allá de lo peligroso que pueden llegar a ser las ICO.

Por su parte, el Banco Central de la República Argentina (BCRA), en mayo de 2014 emitió un comunicado afirmando que las monedas virtuales "no son emitidas por este Banco Central ni por otras autoridades monetarias internacionales, por ende, no tienen curso legal ni poseen respaldo alguno". A su vez, alertó por la volatilidad de su precio y los riesgos de operar con estos activos. Este comunicado no fue acompañado de una nueva definición oficial del término moneda virtual.

Posteriormente, el BCRA ha dictado algunas normas que mencionan, tímidamente, las expresiones monedas virtuales y criptoactivos. Por ejemplo, la Comunicación “A”6823 del 31/10/2019, impide la utilización de tarjetas de crédito (emitidas por entidades locales) para la “adquisición de criptoactivos en sus distintas modalidades” en casas de cambio de criptomonedas del exterior. Con esta norma el BCRA buscó reducir la salida de dólares de sus reservas; fue sólo una medida cambiaria que también imposibilita el uso de tarjetas para otros consumos en el exterior (como, por ejemplo, juegos de azar), pero no fue una prohibición de la operatoria con monedas virtuales.

Luego, la Comunicación “A”7030 del 28/05/2020 (modificada por la “A”7042 del 11/06/2020) estableció que aquellos sujetos que deban acceder al mercado único y libre de cambios (MULC) para adquirir divisas, por ejemplo, con el objetivo de saldar obligaciones internacionales (como pago a proveedores del exterior), y a

su vez sean titulares de activos externos por un monto superior a los USD100.000, deberán disponer de ellos (al menos hasta encontrarse por debajo de dicho límite) para pagar sus obligaciones internacionales antes de acudir al MULC. Entre estos activos externos se incluye (además de, por ejemplo, billetes de divisas extranjeras) a los criptoactivos, pero sin dar una explicación del concepto. Nuevamente, aquí se está sólo frente a una medida cambiaria y no a una regulación específica sobre las criptomonedas.

Cabe destacar que, al menos hasta la fecha, la compraventa de estos activos no está sujeta al “cepo cambiario” ni a las demás restricciones establecidas por el BCRA y la CNV sobre los denominados “dólar bolsa (MEP)” y “contado con liquidación (CCL)”. Por tal motivo, se ha incrementado sustancialmente la operatoria con criptomonedas en los últimos meses, cuyo principal objetivo es la adquisición indirecta de dólares, evitando los límites establecidos en el MULC (pero a un tipo de cambio implícito más alto que el oficial y conocido popularmente como “dólar crypto”):

3.2.12. Implicaciones fiscales

Si bien las implicaciones fiscales rara vez se incluyen con el diseño y desarrollo temprano, este conjunto de herramientas fomenta un enfoque de base amplia para que ninguna parte del negocio sea una ocurrencia tardía. Las implicaciones fiscales se deben considerar desde la fase inicial de alcance y estrategia de una implementación de blockchain. El propósito de este módulo del Kit es educar a los gerentes de implementación y a las organizaciones e identificar detalles y abordar las características para aplicar adecuadamente las diversas implicaciones fiscales del uso de blockchain. Para cálculos específicos de responsabilidad tributaria y requisitos de informes de cumplimiento, quien aplique la guía debe consultar con especialistas tributarios locales en la jurisdicción, ya que las leyes tributarias pueden variar según los hechos y jurisdicciones específicos. La planificación adecuada y la investigación fiscal pueden reducir la incertidumbre fiscal, cumplir con los requisitos reglamentarios, generar eficiencias con respecto a las operaciones y reducir la carga fiscal general.

3.2.13. Informes y controles financieros.

Cualquier solución de blockchain diseñada e implementada para una cadena de suministro debe considerar los requisitos de los informes financieros de los participantes, los controles internos y sus partes interesadas, para que cualquier caso se aborde con éxito. Cuando se combina con formas más tradicionales de contabilidad empresarial, la información blockchain puede ayudar a las empresas a respaldar la preparación de estados financieros oportunos y confiables. Es

importante abordar los muchos desafíos que pueden existir cuando una organización se basa en la información obtenida de una cadena de bloques y la tecnología subyacente como parte de su proceso de información financiera y sistema de control interno.

3.2.14. Factores de riesgo.

Las nuevas tecnologías tienen posibles inconvenientes que deben identificarse y gestionarse. Esto es especialmente cierto, cuando esa tecnología no es simplemente una aplicación superpuesta, sino es parte central de la infraestructura de TI subyacente de la organización, como suele ser el caso de blockchain. La lista de verificación incluida en este módulo del Kit cubre algunos posibles riesgos y errores comunes asociados con el despliegue de tecnologías blockchain. Sin embargo, hay que tener en cuenta que esta lista no pretende ser exhaustiva. Teniendo esto en cuenta, los gerentes de proyectos deben ver la información como una guía genérica y trabajar con las partes interesadas internas relevantes, como los equipos de seguridad cibernética, auditoría interna, finanzas, cumplimiento, legal, operaciones y tecnología de la información para identificar y priorizar los riesgos que son importantes para sus despliegue y desarrollo de mecanismos para gestionar los riesgos de forma proactiva.

3.3. Guía técnica para emisión de tokens.

Al crear una nueva criptomoneda, puedes optar por hacer una moneda o un token. Una moneda tiene su propia blockchain, mientras que un token se basa en una red preexistente. Las criptomonedas dependen de las blockchains por su seguridad y naturaleza descentralizada.

Crear un token requiere menos experiencia y esfuerzo que hacer una criptomoneda. Una moneda por lo general necesita un equipo de desarrolladores y expertos para crearla. Para un token también se necesita de conocimientos técnicos, pero es posible crearlo en minutos mediante el uso de otras blockchains, como Ethereum, Binance Smart Chain, Solana y Polygon.

la elección de token o moneda cambiará según la personalización y la utilidad que se desee. En general, los costos involucrados dependen del trabajo necesario, como el uso de desarrolladores externos y el tiempo invertido.

Ethereum y Binance Smart Chain son blockchains populares para crear monedas digitales. Se puede usar el código establecido para crear tokens o pagar para usar un servicio de creación de monedas. Las sidechains son otra opción popular, ya que brindan más personalización con los principales beneficios de la blockchain.

Antes de crear una criptomoneda propia, se deberá considerar su utilidad, tokenomía y estado legal. Después de esto, tu elección de blockchain, mecanismo de consenso y arquitectura son todos necesarios para la etapa de desarrollo. Luego, se podría considerar una auditoría del proyecto y una verificación legal final. Si bien casi cualquier persona puede crear una criptomoneda, desarrollar un proyecto sólido requiere un trabajo serio y dedicación.

3.3.1. Introducción.

Hay muchas formas de crear monedas y tokens. Los costos y el conocimiento también varían según la complejidad del proyecto.

Diferencia entre criptomonedas y tokens: Las criptomonedas se pueden dividir aproximadamente en dos categorías: monedas y tokens. La diferencia entre ellas es simple. Las monedas tienen su propia blockchain nativa, como Bitcoin, por ejemplo. Ether (ETH) tiene la blockchain Ethereum. Crear un token es mucho más simple que crear una moneda. Una moneda requiere que se desarrolle y mantenga con éxito una blockchain. Esta es una descripción general básica de las dos opciones:

Moneda	Token
Se ejecuta en su propia red blockchain	Se puede construir en blockchains existentes con una base de usuarios establecida
Requiere conocimientos avanzados de blockchain y habilidades de programación	Bastante simple de crear con herramientas preexistentes y código de fuente abierto
El desarrollo de blockchain es más costoso y lleva tiempo	El desarrollo de tokens es más rápido, más simple y relativamente barato

3.3.2. Crear un Token.

Crear un token en una blockchain existente puede mejorar su reputación y seguridad. Si bien no se tendrá un control completo sobre todos los aspectos del token, se tendrá mucha capacidad de personalización disponible. Hay una variedad de sitios web y herramientas disponibles para crear tu propio token, especialmente en BSC y Ethereum.

Algunas de las soluciones más populares para crear criptomonedas son BSC, Ethereum y Solana. Estas redes proporcionan formas de crear una variedad de tokens basados en estándares preexistentes. Los estándares de token BEP-

20 y ERC-20 son ejemplos destacados y compatibles con casi cualquier proveedor de billetera de criptomonedas.

ERC-20 pertenece a la blockchain Ethereum, mientras que BEP-20 es parte de Binance Smart Chain (BSC). Ambas redes permiten la creación y personalización de contratos inteligentes con los que puedes crear tus propios tokens y aplicaciones descentralizadas (DApps). Con las DApps, puedes crear un ecosistema que proporcione más casos de uso y funcionalidad a tu token.

También se puede optar por sidechains que utilizan la seguridad de una cadena más grande como Ethereum o Polkadot, pero que también proporcionan cierta capacidad de personalización. La red Polygon está conectada a Ethereum y proporciona una experiencia parecida, pero es más barata y rápida de utilizar.

Después de elegir una blockchain, se necesitará un método para crear el token. Con BSC y otras blockchains que se basan en Ethereum Virtual Machine, el proceso es relativamente simple. También se pueden encontrar herramientas listas para usar que crean tokens según los parámetros y las reglas que se proporcione. Por lo general, estas herramientas tienen un costo, pero son una opción más práctica para los usuarios que no están familiarizados con los contratos inteligentes.

Si se desea hacer una propia blockchain y moneda, es probable que se necesite un equipo de desarrolladores de blockchain y expertos de la industria. Incluso si se busca hacerle fork a una blockchain como Ethereum o Bitcoin, todavía se requiere una gran cantidad de trabajo para configurar la red. Esto incluiría alentar a los usuarios a actuar como validadores y ejecutar nodos para mantener la blockchain en funcionamiento.

3.3.3. Define la utilidad de tu criptomoneda.

Las criptomonedas pueden desempeñar muchos roles. Algunas actúan como claves para acceder a los servicios. Otras incluso son para representar acciones u otros activos financieros. A fin de comprender y trazar el proceso de creación de tu cripto, se deberán definir sus características desde el inicio.

3.3.4. Diseñar la tokenomía (economía del token)

La tokenomía (tokenomics) es la economía que rige a la criptomoneda, como el suministro total, el método de distribución y el precio inicial. Una buena idea puede fallar si la tokenomía no es correcta y los usuarios no están incentivados a comprar la criptomoneda.

3.3.5. Verificar cumplimiento legal

Países de todo el mundo tienen sus propias leyes y reglas con respecto a las criptomonedas. Algunas jurisdicciones incluso pueden prohibir el uso de criptomonedas. Considerar completamente las obligaciones legales y cualquier problema de cumplimiento que se pueda enfrentar.

3.4. Factibilidad Normativa para emisión de Tokens.

A la fecha de la preparación del presente informe no existe en el país un marco normativo claro para la emisión de activos digitales. Hay dudas respecto de si una provincia puede emitir un cryptoactivo. El Artículo 126 de la Constitución Nacional establece que no son facultades de las provincias acuñar moneda o imprimir billetes y la ley argentina establece que una entidad federal debe estar a cargo de emitir una moneda nacional, acción que recae en el Banco Central de la República Argentina. Sin embargo, los tokens, especialmente los utility tokens, no son considerados moneda por lo cual ante la no prohibición expresa por parte de la ley de su emisión, se podría considerar que su emisión se encuentra permitida y hasta el momento, esos activos no se encontrarían bajo el contralor de ningún ente nacional.

3.5. Propuestas de implementación de blockchain a la provincia de Santa Fe.

A continuación presentamos propuestas para implementación de la tecnología blockchain aplicables a la administración tributaria de la provincia de Santa Fe, que sirvan como para empezar a pensar el uso de la tecnología a nivel provincial.

3.5.1. Licitaciones

Las compras públicas representan la principal vía de relación directa entre el Estado y el sector privado. También, la Sociedad Civil interviene como parte interesada en los mecanismos de auditoría.

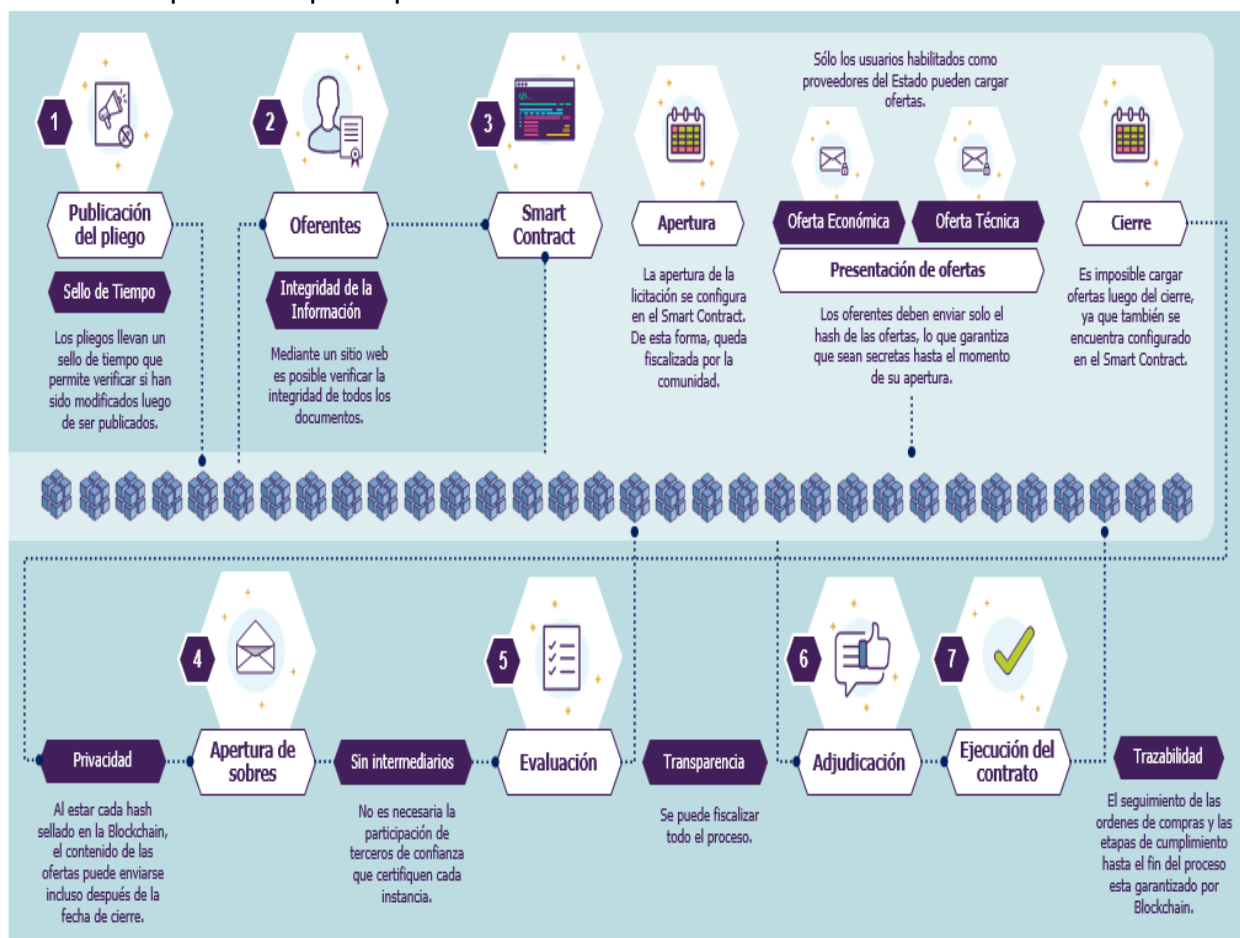
Las licitaciones públicas, la mayor fuente de afectación de los recursos públicos, se han ido modernizando en los últimos años pero el seguimiento de las etapas y los procesos de control administrativos resultan ajenos a la mayoría de los ciudadanos. Por este motivo resulta indispensable que las contrataciones se

“Beneficios de La cadena de bloques o blockchain aplicada a la administración tributaria de la provincia de Santa Fe”

Fundación para los Estudios Internacionales
Mendoza 444 - Rosario, Santa Fe - C.P. 2000

desarrollen dentro de un marco que no solo contribuya a favorecer las buenas prácticas, sino que también las visibilice.

Al incorporar Blockchain a un proceso de licitación, encontramos nuevas formas de facilitar el proceso de auditoría, tanto a los oferentes como a la sociedad en general. Esta tecnología posibilita el desarrollo de una plataforma para la compra de bienes y la contratación de servicios por parte del Estado que garantice transparencia e impida cualquier tipo de fraude.



Ventajas:

- Al estar públicos en la blockchain, y llevar un sello de tiempo, todos los documentos que deben presentar los interesados acordes a los términos de la convocatoria son públicos e inalterables.
- Blockchain ofrece las herramientas para que las ofertas digitales sean efectivamente privadas hasta la apertura de los sobres. Esto optimiza los tiempos de presentación y a su vez, mitiga la desconfianza de los oferentes en relación a

irregularidades durante el proceso, lo que muchas veces se traducía en ofertas tardías o falta de las mismas.

- La utilización de smart contract permite establecer parámetros facilitando la automatización del proceso, de manera transparente, permitiendo entre otras cosas aceptar propuestas o rechazar aquellas que no cumplan con los requerimientos, notificar automáticamente al ganador o ejecutar los procesos administrativos vinculados.

- La evaluación se realiza de forma virtual de acuerdo a las condiciones de la convocatoria, pero es completamente pública y transparente.

- Se pueden fiscalizar las órdenes de compras y las etapas de cumplimiento hasta el fin del proceso, incluyendo la ejecución del contrato

3.5.2. Emisión de Tokens.

Como hemos visto en los puntos anteriores, cualquier activo de la economía real puede a través de un proceso de digitalización “tokenizarse”. Dentro de este marco teórico y sin entrar en detalles técnicos y normativos que fueron detallados con anterioridad al presente punto, se podría pensar en digitalizar a través de criptoactivos la recaudación futura de la provincia de Santa Fe, creando esos tokens para diversos fines como por ejemplo el pago de subsidios. Los receptores de los subsidios podrían recibir los Tokens en vez de dinero, volcarlos a la actividad real, a través del diseño de planes y acciones que generen beneficios en las transacciones en los que intervengan los activos digitales. Se pueden crear incentivos especiales para abonar impuestos provinciales, servicios públicos u cualquier otro tipo de obligación provincial. De esta manera, los tokens que representan digitalmente la futura recaudación tributaria de la provincia y se encuentran plasmados en una blockchain, podrán pasar de los beneficiarios iniciales de los subsidios a la economía real, y posteriormente volver al emisor original. Al encontrarse asentados en la cadena de bloques permite correr "contratos inteligentes" o Smart contracts. Es decir, pueden programarse transacciones y definir el destino o usos posibles de los tokens, sujetándolos a ciertas condiciones futuras que se fijan de antemano. De esta forma, si la provincia quisiera incentivar el pago de impuestos a través de los tokens, sólo necesitaría poner a disposición de los usuarios un contrato inteligente que les permitiera pagar impuestos con tokens de manera automatizable. Otra ventaja es la posibilidad de aplicar la Analítica de Datos para extraer información sobre patrones de uso y consumo a partir de las transacciones realizadas con tokens, lo que permitiría a la provincia

conocer con precisión ciertos datos, como rangos de precios o tipos de productos y servicios. Esta información, generada por el uso de los tokens, se registraría en la blockchain de la provincia y esto le permitiría nutrirse de datos para realizar análisis, generar información y mejorar el proceso de toma de decisiones de gobierno y gestión.

La propiedad del token sería de la provincia de Santa Fe, quien tendría el control total de su forma de uso y condiciones, así como también todas las cuestiones relativas a su tokenomía.

Al momento de emitir el presente informe, la provincia de Santa Fe tiene implementado el programa billetera Santa Fe que es de gran masividad. De ser posible, sería conveniente por cuestiones de desarrollo, practicidad y economía permitir que dentro de la App Billetera Santa Fe, se obtenga un visor o apartado para alojar los Tokens, permitir ver el saldo, las transacciones y transferencia de los mismos mediante lector de QR.

Capítulo IV: “Capacitaciones en tecnología blockchain”

4.1. Detalle de las capacitaciones.

En el presente apartado procederemos a detallar las capacitaciones brindadas a las personas seleccionadas por la Secretaría de Finanzas e Ingresos Públicos y Política Fiscal de Santa Fe.

Módulo 1: Fundamentos de la tecnología Blockchain: Bitcoin y origen de Blockchain. Consensos, estructuras y tipos de Blockchain. Conceptos y tipos de criptografía. Función Hash, clave pública y privada. Tipos de Billeteras. El presente módulo se dictó el miércoles 30 de Marzo de 2022 a las 19 Hs.

Módulo 2: Cadena de bloque en funcionamientos: Transacciones en Bitcoin. Ethereum como un agregado de valor exponencial en internet. Transacciones en Ethereum. Smart contract. Características de los Smart contract. Dinero digital. Seguridad en Blockchain. El presente módulo se dictó el jueves 31 de Marzo de 2022 a las 19 Hs.

Módulo 3: Aplicaciones concretas: Finanzas descentralizadas. Firma digital. Blockchain y los impuestos. Microcréditos. Denominación de origen y trazabilidad. DAOs. El presente módulo se dictó el viernes 01 de Abril de 2022 a las 19 Hs.

Las 3 clases tomaron una hora y media cada una. Al finalizar las charlas se entregó un material en formato PDF, de lo dictado en las capacitaciones compuesto por las diapositivas utilizadas en las clases, como así también los capítulos I,II y III del presente Documento.

El equipo encargado de realizar las capacitaciones quedó a disposición de los interesados para responder dudas y consultas a través de la casilla de correo electrónico institucional de la fundación para los estudios internacionales, la cual fue informada en las clases y se encuentra insertadas en las diapositivas que componen el material entregado. Al momento de la redacción del presente informe, no se ha recibido ninguna consulta o duda.

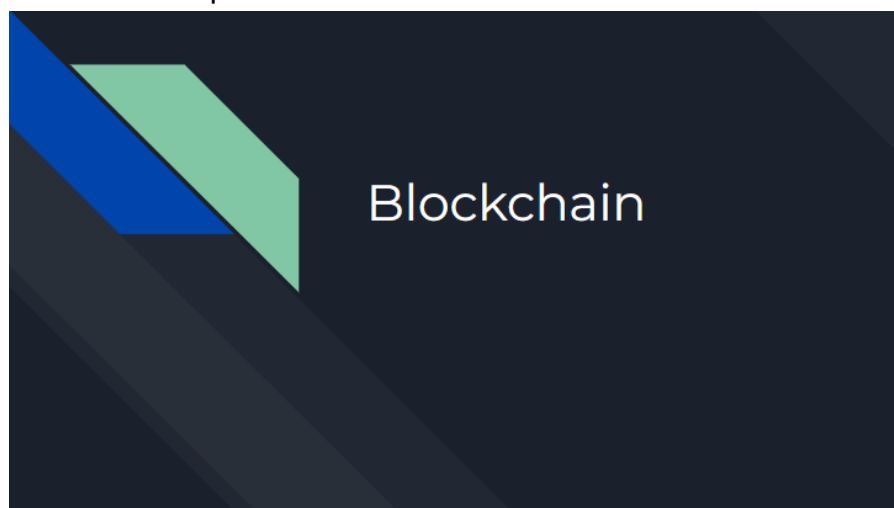
Al finalizar las capacitaciones se realizó una charla con los asistentes para así obtener información para sacar conclusiones y emitir un documento en donde se detalle en que sectores se pueden lograr grandes beneficios de aplicación y en cuales se encuentra cierta resistencia a la nueva tecnología.

Equipo de Trabajo: Capacitador Areste Luciano; Capacitador Cont. da Silva Daniel; Moderador Cont. Rossi Pablo Manuel.

Asistentes: Completaron una asistencia del 100% de la capacitación los señores Lic. Gomez Sepliarsky Lautaro, CUIL 20-30948505-0; Prado Natalia, CUIL 27-29671652-4; Tedesca Juan Pablo, CUIL 20-31136610-7; Andino Plechuk Miguel Orlando, CUIL 20-28509695-3; Morales Marcela Liliana, CUIT 27-21768569-4

4.2. Material y Detalle de las capacitaciones.

En el presente capítulo dejaremos imágenes de las diapositivas utilizadas para la ronda de capacitaciones dictadas a través de Zoom a los asistentes mencionados en el apartado anterior.



Módulo 1: Fundamentos de la tecnología blockchain

Resumen

- Bitcoin y el origen de blockchain
- Tipos de consensos y estructuras
- Tipos de blockchain
- Conceptos y tipos de criptografías
- Función Hash
- Clave Públicas y privadas
- Tipos de Billeteras.
- Folks

Bitcoin y el origen de blockchain

Que es Blockchain?

Las cadenas de bloques o blockchain son registros digitales. En su nivel básico, permiten que una comunidad de usuarios registre transacciones en un libro mayor compartido dentro de esa comunidad, de modo que bajo el funcionamiento normal de la red blockchain no se puede cambiar ninguna transacción una vez publicada.

Las cadenas de bloques son libros de contabilidad digitales distribuidos de transacciones firmadas criptográficamente que se agrupan en bloques. Cada bloque está criptográficamente vinculado al anterior (lo que lo hace evidente) después de la validación y se somete a una decisión consensuada.

Cuando hacemos hincapié en estas definiciones nos encontramos con tres cuestiones fundamentales: Transparencia, seguridad y control

Un poco de historia...

- El origen del dinero y su evolución.
- las funciones del dinero.
- Cyberpunk y Blockchain
- Satoshi y Bitcoin
- Ethereum y DEFI

Funcionamiento de la cadena de bloques

- Proceso de encadenamiento: cada cierto número de transacciones se crea un nuevo bloque, en el cual se incluye el hash del bloque anterior para crear un nuevo hash que corresponde al nuevo bloque. Es decir, cada nuevo bloque incluye el hash del bloque anterior, lo de bloques que impide cambiar información contenida en un bloque anterior sin “arrastrar” cambios en los hashes de los bloques siguientes.
- Registro distribuido: Cada uno de los nodos con una copia del registro tiene igual importancia que el resto; es decir: se trata de una red de pares en donde no existe alguien que domine al resto

Tipos de Blockchain

- Blockchains públicas: Las redes blockchain públicas son aquellas a las que cualquier persona tiene acceso.
- Blockchain federadas: los usuarios comunes o corrientes tendrán acceso a tanta información como se les decida mostrar a través de la misma. Se tendrán entonces alternativas que varíen desde un gran nivel de transparencia hasta una transparencia mínima.
- Blockchain Privadas: Los blockchain privados son aquellos en los que el control está reducido a una única entidad que se encarga de mantener la cadena, dar permisos a los usuarios que se desea que participen, proponer transacciones y aceptar los bloques.
- Blockchain as a service: Servicios de blockchain en la nube.

Criptografías y claves

- La tecnología Blockchain utiliza criptografía de clave asimétrica (conocida como criptografía de clave pública). La criptografía de clave asimétrica utiliza un par de claves: una clave pública y una clave privada matemáticamente relacionados entre sí.
- Criptografía simétrica: Es la que utiliza una sola clave secreta para cifrar y descifrar, los usuarios ya deben tener una clave de confianza entre sí.
- Las claves privadas se utilizan para firmar transacciones digitalmente.
- Las claves públicas se utilizan para derivar direcciones.
- Las claves públicas se utilizan para verificar firmas generadas con claves privadas.
- La criptografía de clave asimétrica brinda la capacidad de verificar que el usuario que transfiere valor a otro usuario está en posesión de la clave privada capaz de firmar la transacción

Tipos de Wallets

Dentro del ecosistema blockchain hay un elemento que conforma uno de los ejes principales, las billeteras o Wallets, dado que es donde se guardan, almacenan, dispone la información las criptomonedas que poseemos. Podríamos decir que esto es una billetera normal digital, pero en el mundo blockchain esto va un poco más allá. Las billeteras digitales son repositorios personales portables y seguros.

- Billeteras de software.
- Billeteras de hardware.
- Billeteras de papel.

Modelos de consenso

Un aspecto clave de la tecnología blockchain es determinar qué usuario publica el siguiente bloque. Esto se resuelve mediante la implementación de uno de los muchos modelos de consenso o protocolos posibles.

- Proof of work (Prueba de trabajo).
- Proof of stake (Prueba de participación)
- Round Robin.
- Prueba de autoridad.
- Prueba de tiempo transcurrido.

Folks

Los cambios en el protocolo y las estructuras de datos de una red blockchain se denominan bifurcaciones o Folks. Se pueden dividir en dos categorías: Soft Folks y Hard Folks.

- **Soft Folks:** Una bifurcación suave es un cambio en una implementación de blockchain que es compatible con versiones anteriores. Los nodos no actualizados pueden continuar realizando transacciones con nodos actualizados.
- **Hard Folks:** Una bifurcación dura es un cambio en una implementación de blockchain que no es compatible con versiones anteriores. En un momento dado (generalmente en un número de bloque específico), todos los nodos de publicación deberán cambiar para usar el protocolo actualizado.

Módulo 2: Blockchain en funcionamiento

Resumen.

- Transacciones en Bitcoin.
- Elementos claves de las Transacciones
- Ethereum.
- Transacciones en Ether.
- Smart Contract.
- Dinero digital.
- Seguridad en Blockchain.
- Tipos de ataques

Transacciones en Bitcoin.

- Una transacción es una transferencia de valores entre monederos Bitcoin que será incluida en la cadena de bloques. Los monederos Bitcoin disponen de un fragmento secreto llamado clave privada, utilizada para firmar las operaciones, proporcionando una prueba matemática de que la transacción está hecha por el propietario del monedero. La firma también evita que la transacción no sea alterada por alguien una vez ésta ha sido emitida. Todas las transacciones son difundidas entre los usuarios y por lo general empiezan a ser confirmadas por la red en los 10 minutos siguientes a través de un proceso llamado minería.
- La minería es un sistema de consenso distribuido que se utiliza para confirmar las transacciones pendientes a ser incluidas en la cadena de bloques. Hace cumplir un orden cronológico en la cadena de bloques, protege la neutralidad de la red y permite un acuerdo entre todos los equipos sobre el estado del sistema. Para confirmar las transacciones, deberán ser empacadas en un bloque que se ajuste a estrictas normas de cifrado y que será verificado por la red. Estas normas impiden que cualquier bloque anterior se modifique, ya que hacerlo invalidaría todos los bloques siguientes. La minería también crea el equivalente a una lotería competitiva que impide que cualquier persona pueda fácilmente añadir nuevos bloques consecutivamente en la cadena de bloques. De esta manera, ninguna persona puede controlar lo que está incluido en la cadena de bloques o reemplazar partes de la cadena de bloques para revertir sus propios gastos.

Elementos que conforman las transacciones.

- Entradas (inputs). Las entradas son las referencias a una salida de una transacción pasada que no ha sido empleada en ninguna otra transacción. Estas nos permiten confirmar la procedencia de los activos que se utilizarán en una transacción. Y son las que contienen la dirección donde originalmente se recibieron los bitcoins.
- Salidas (outputs). Estas contienen la dirección a la cual se realiza la transferencia y la cantidad enviada. Además contienen las direcciones de cambio o de retorno donde son enviadas las vueltas de las transacciones. Por lo que en una transacción puede contener más de una salida.
- Identificador (TXid). Cada transacción realizada tendrá su propio hash. Este hash se genera a partir de las entradas y las salidas. Este valor es el que permite identificar una transacción de forma única e irrepetible dentro de una blockchain.
- Tarifa de comisión (fee). La fee es el pequeño pago que reciben los mineros por procesar una transacción. Así, el minero que genere un nuevo bloque, recibirá una fee por cada transacción procesada dentro de dicho bloque. La comisión no viene de forma explícita en el contenido de una transacción, es decir no se asocia a ninguna salida, ya que no se sabe el minero que recibirá esa fee. Para ello lo que se hace es dejar una determinada cantidad sin asociar a ninguna salida, y esta será entendida como comisión para los mineros.

Tipos de Transacciones

- Una transacción coinbase es la que le permite a los mineros generar o activar nuevas criptomonedas. Con las que pueden recibir las recompensas de la minería. En el caso de Bitcoin, la primera transacción realizada se denominó coinbase. Y no fue efectuada de una persona a otra, sino más bien que fue realizada por la misma red como una transacción generadora. Mediante la cual se dio vida a todo el sistema Bitcoin. Los nodos mineros pueden añadir sólo una transacción coinbase por cada nuevo bloque generado. Así, el sistema se asegura de que el minero reciba sólo la recompensa que le corresponde y que entren en circulación nuevas monedas que nunca han estado dentro de la blockchain.
- Las UTXOs son las monedas no gastadas. En el protocolo Bitcoin, las entradas de transacciones (inputs) también son llamadas UTXOs de una transacción anterior. Es decir, salidas de una transacción no gastadas o utilizadas. Y contienen básicamente, el cambio o vueltas producto de una transacción. Por ejemplo, si tienes 1 BTC en tu monedero, es probable que estos provengan de varias UTXOs. Que pueden ser 4 de 0.25 BTC cada uno. Si deseas gastar en algún producto una cantidad total de 0.30 BTC, verás que no posees ningún UTXO con esa cantidad específica. Aunque tu monedero mostrará un balance de 1 BTC como total para simplificar las cosas.

Ethereum y su historia.

- 2009-Bitcoin, Ethereum y su relación con la crisis sub-prime.
- 2013- Propuesta de desarrollo de Ethereum.
- 2014- Preventa de Ether para el desarrollo de Ethereum.
- 2015- Se mina el primer bloque
- 2016- Homestead y el incidente DAO.
- 2019-constantinople
- 2021- Serenity y Ethereum 2.0

Ethereum y la EVM.

- “El propósito de Ethereum es crear un protocolo alternativo para construir aplicaciones descentralizadas, proporcionando un conjunto diferente de contrapartidas que creemos que serán muy útiles para un amplio abanico de aplicaciones descentralizadas, con especial énfasis en situaciones en las que el rápido tiempo de desarrollo, la seguridad para aplicaciones pequeñas y rara vez usadas y la capacidad de las diferentes aplicaciones para interactuar de manera muy eficiente son importantes. Ethereum lo logra construyendo lo que es esencialmente la capa fundacional abstracta definitiva: una blockchain con un lenguaje de programación Turing completo, que permite a cualquiera escribir contratos y aplicaciones descentralizadas donde pueden crear sus propias reglas arbitrarias de propiedad, formatos de transacción y funciones de transición de estado” Buterin, Vitalik.
- En el universo Ethereum, hay un computador único y canónico (llamado máquina virtual de Ethereum o EVM), cuyo estado han acordado todos los participantes de la red. Cualquiera que participe en la red de Ethereum (cada nodo de Ethereum) mantiene una copia del estado de este ordenador. Adicionalmente, cualquier participante puede emitir una petición para que este ordenador realice un cálculo arbitrario. Cuando se transmite una solicitud de este tipo, los demás participantes de la red verifican, validan y ejecutan el cálculo. Esto causa un cambio de estado en la EVM, que se realiza y propaga a través de toda la red.

Ether y Transacciones en Ethereum

- El propósito de Ether, la criptomoneda, es permitir la existencia de un mercado computacional. Este mercado proporciona un incentivo económico para que los participantes puedan verificar/ejecutar solicitudes de transacción y proporcionar recursos computacionales a la red.
- Una transacción de Ethereum hace referencia a una acción iniciada por una cuenta de propiedad externa, en otras palabras, una cuenta controlada por un humano, no un contrato. Por ejemplo, si Bob le envía 1 ETH a Alice, este debe debitarse de la cuenta de Bob y acreditarse en la cuenta de Alice. Esta acción modificadora del estado de la red tiene lugar en una transacción.
- Las transacciones necesitan una comisión y deben minarse para convertirse en transacciones válidas.
- El gas hace referencia a la unidad que mide la cantidad de esfuerzo computacional requerida para ejecutar operaciones específicas en la red de Ethereum. Como cada transacción de Ethereum requiere recursos computacionales para ejecutarse, cada transacción requiere una comisión. El gas hace referencia a la comisión necesaria para llevar a cabo una transacción en Ethereum con éxito.

Smart Contract

- En el ámbito de las criptomonedas, podemos definir los smart contract como aplicaciones o programas que se ejecutan en una blockchain. Normalmente, actúan como acuerdos digitales que son obligados a cumplir por una serie específica de reglas. Dichas reglas son predefinidas por un código informático, que será replicado y ejecutado por toda la red de nodos
- La tecnología blockchain permitió la existencia de contratos inteligentes ofreciendo la permanencia y las resistencias incorruptibles provistas en el pasado por la tinta, el papel y la autoridad confiable que certificaba el cumplimiento del contrato.
- De forma resumida, un smart contract funciona como un programa determinístico: el mismo ejecuta una tarea particular cuando ciertas condiciones se cumplen, si es que se cumplen. De esta forma, los sistemas smart contract a menudo siguen sentencias condicionales del tipo “if... then...”. Pero a pesar de la terminología popular, los smart contracts ni son contratos legales, ni son inteligentes. Simplemente son pedazos de código ejecutados en un sistema distribuido (blockchain).

Características Claves de los Smart Contracts

- Distribuidos. Los smart contracts son replicados y distribuidos por todos los nodos de la red Ethereum. Esta es una de las principales diferencias respecto a otras soluciones basadas en servidores centralizados.
- Determinísticos. Los smart contracts solamente realizan las acciones para las que fueron diseñados, siempre y cuando las condiciones se cumplan. Además, el resultado será siempre el mismo, sin importar quién sea el que los ejecute.
- Autónomos. Los smart contracts pueden automatizar todo tipo de tareas, funcionando como programas autoejecutables. En la mayoría de casos, sin embargo, si un smart contract no es activado, permanecerá “latente” y no ejecutará ninguna acción.
- Inmutables. Los smart contracts no pueden ser modificados una vez desplegados. Solamente pueden ser eliminados, si una función particular ha sido previamente implementada. Por lo tanto, podríamos afirmar que los smart contracts pueden proporcionar código a prueba de manipulaciones (tamper-proof code).
- Customizables. Antes de ser desplegados, los smart contracts pueden ser codificados de muchas maneras distintas. Así que, pueden ser empleados para crear múltiples tipos de aplicaciones descentralizadas. Esta característica está directamente vinculada al hecho de que Ethereum sea una blockchain Turing Completa.

Seguridad en Blockchain

- La seguridad de blockchain es un sistema integral de gestión de riesgos para una red de blockchain, que utiliza estructuras de ciberseguridad, servicios de garantía y mejores prácticas para reducir los riesgos contra ataques y fraudes. La tecnología blockchain produce una estructura de datos con cualidades de seguridad inherentes. Se basa en principios de criptografía, descentralización y consenso, que garantizan la confianza en las transacciones.
- Si bien la tecnología blockchain produce un libro mayor de transacciones a prueba de manipulaciones, las redes blockchain no son inmunes a los ciberataques y al fraude. Aquellos con malas intenciones pueden manipular vulnerabilidades conocidas en la infraestructura de blockchain y han tenido éxito en varios ataques y fraudes a lo largo de los años.

Tipos de ataques en Blockchain

- Phishing. Phishing es un intento de estafa para obtener las credenciales de un usuario. Los estafadores envían e-mails a los propietarios de claves de billetera diseñados para que parezca que provienen de una fuente legítima. Los e-mails solicitan a los usuarios sus credenciales mediante hipervínculos falsos. Tener acceso a las credenciales de un usuario y otra información confidencial puede resultar en pérdidas para el usuario y la red blockchain.
- Ataque de enrutamiento. Los blockchains se basan en grandes transferencias de datos en tiempo real. Los hackers pueden interceptar datos mientras se transfieren a proveedores de servicios de Internet. En un ataque de enrutamiento, los participantes de blockchain generalmente no pueden ver la amenaza, por lo que todo parece normal. Sin embargo, entre bastidores, los estafadores han extraído datos confidenciales o monedas.
- Ataque de Sybil. En un ataque de Sybil, los hackers crean y utilizan muchas identidades de red falsas para inundar la red y bloquear el sistema. Sybil se refiere a un famoso personaje de libro diagnosticado con un trastorno de identidad múltiple.
- Ataque del 51%. La minería requiere una gran cantidad de potencia informática, especialmente para los blockchains públicos a gran escala. Pero si un minero, o un grupo de mineros, pudiera reunir suficientes recursos, podrían alcanzar más del 50 % de la potencia minera de una red blockchain. Tener más del 50 % del poder significa tener control sobre el libro mayor y la capacidad de manipularlo.

Módulo 3: Aplicaciones concretas

Resumen.

- Finanzas Descentralizadas.
- Firma Digital.
- Educación.
- Sistemas de votación.
- Blockchain y los impuestos.
- Microcréditos e identidad digital.
- Cadenas de suministros.
- Salud.
- DAOs.

Finanzas Descentralizadas (DeFi).

Concepto: El término Decentralized Finance (Finanzas Descentralizadas) puede emplearse para aludir a un movimiento que pretende crear un ecosistema de servicios financieros de código abierto, no permissionado y transparente, que sea accesible para todo el mundo y opere sin ninguna autoridad central. Los usuarios mantendrían un control total sobre sus activos e interactúan con dicho ecosistema a través de aplicaciones descentralizadas (Dapps) de tipo peer-to-peer (P2P).

Principales casos de uso.

- **Préstamos:** La toma y concesión de préstamos de forma abierta y descentralizada otorga las ventajas de liquidación (settlement) instantánea de las transacciones, la capacidad de colateralizar activos digitales, la ausencia de controles de crédito y una potencial estandarización en el futuro.
- **Servicios Bancarios:** Entre estos se incluyen la emisión de stablecoins (monedas estables digitales), hipotecas y seguros.
- **Marketplace descentralizados:** Estas plataformas permiten a los usuarios tradear activos digitales sin la necesidad de un intermediario confiable para mantener tus fondos.

Firma Digital.

Concepto: Una firma digital es un mecanismo criptográfico empleado para verificar la autenticidad e integridad de datos digitales. Podemos considerarla una versión digital de las firmas escritas a mano ordinarias, pero con un nivel más elevado de complejidad y seguridad.

Importancia de las firmas digitales:

- **Integridad de los datos.** Bob puede verificar que el mensaje de Alice no haya cambiado en el camino. Cualquier modificación en el mensaje produciría una firma completamente diferente.
- **Autenticidad.** Mientras la clave privada de Alice se mantenga en secreto, Bob puede usar su clave pública para confirmar que las firmas digitales fueron creadas por Alice y nadie más.
- **No repudio.** Una vez que se haya generado la firma, Alice no podrá negar haberla firmado en el futuro, a menos que su clave privada se vea comprometida de alguna manera.

Casos de Uso en Blockchain:

- Los esquemas de firma digital aseguran que solo los propietarios legítimos de las criptomonedas puedan firmar una transacción para mover los fondos (siempre que sus claves privadas no se vean comprometidas).

Educación.

- La adecuada implementación de Blockchain permitiría acreditar la información suministrada por los aspirantes en un curriculum vitae, de tal forma que se pueda contrarrestar la manipulación de la información suministrada, convirtiendo este sistema en una especie de “moneda intelectual”. Un uso educativo obvio es almacenar registros de logros y créditos, como certificados de grado. Los datos del certificado serían agregados al Blockchain por la institución que los otorga, a la que el estudiante puede acceder, compartir con los empleadores o generar un enlace desde un curriculum vitae en línea.
- A través de la implementación de la tecnología Blockchain es posible una mayor rigurosidad en el control de los derechos de propiedad y otorgamiento de permisos de uso de obras académicas por parte de sus autores.

Sistemas de Votación.

- La tecnología blockchain se puede utilizar para realizar procesos de votación transparentes. Con un sistema de votación sobre blockchain se puede eliminar muchos intermediarios; actualmente se selecciona a personas naturales para que ejerzan como jurados, sin verificar un perfil y sin comprobar una capacidad específica para ejercer el cargo, y son seleccionados aleatoriamente miles de jurados. Usando Blockchain cada ciudadano puede enviar su voto anónimo a la cadena de bloques, además, los resultados de las votaciones al quedar registrados no se pueden modificar. Esto elimina la sobrecarga considerable del entorno de votación, desde la preparación hasta la tecnología, el personal y los recuentos.

Blockchain y los impuestos.

Atributos de blockchain con potencial significativo en el área impuestos:

- **Transparencia:** la blockchain proporciona procedencia, trazabilidad y transparencia a las transacciones.
- **Control:** el acceso a redes autorizadas está restringido a usuarios identificados
- **Seguridad:** el libro de contabilidad digital no se puede modificar ni alterar una vez que se ingresan los datos. El fraude es menos probable y más fácil de detectar.
- **Información en tiempo real:** cuando la información se actualiza, se actualiza para todos en la red al mismo tiempo. Estos atributos echan luz sobre las áreas de la tributación que se verán afectadas por la nueva tecnología.

Áreas de impacto de la tecnología blockchain en materia tributaria:

- Área de Conceptos Legales-Tributarios Básicos
- Área Materia Imponible
- Área Recaudación y liquidación de Tributos
- Área Procedimientos Tributarios
- Área Administración Tributaria
- Área Lucha contra el fraude

Microcréditos e Identidad Digital.

- Un microcrédito se refiere a la extensión de préstamos pequeños o muy pequeños a prestatarios de bajos recursos, típicamente microempresas o personas humanas en economías emergentes, que normalmente no serían elegibles para un crédito bancario porque carecen de garantías y documentación que los identifique. Además, la mayoría de los bancos no estarían interesados en conceder préstamos tan pequeños, ya que no sería rentable para dichas instituciones.
- La gestión de identidad es muy importante en el proceso de verificación de antecedentes crediticios de un ciudadano. Las soluciones para la gestión de identidades en Blockchain son aún emergentes, sin embargo, se están realizando una cantidad considerable de trabajos sobre este tema, en especial sobre pasaportes, licencias de conducir e historiales crediticios.

Cadenas de Suministros.

Actualmente, el sistema de gestión de las cadenas de suministro se ve afectado por una falta de eficiencia y transparencia, y la mayoría de redes se enfrentan a dificultades cuando intentan integrar todas las partes involucradas. Idealmente, tanto los productos y los materiales, como el dinero y los datos, necesitan moverse sin dificultades a través de las distintas etapas de la cadena. Dado que las blockchains están diseñadas como sistemas distribuidos, son altamente resistentes a modificaciones y pueden resultar muy adecuadas para redes de cadenas de suministro.

Beneficios:

- Registros Transparentes e inmutables.
- Reducción de costos.
- Creación de datos interoperables.
- Acuerdos digitales.
- Compartición de datos.

Salud.

Existen múltiples aplicaciones de la tecnología Blockchain para la industria de la salud, incluida la distribución de productos y servicios. Un caso específico es el suministro de medicamentos desde la planta hasta el usuario final, por lo que los paquetes de medicamentos se autentican y se sellan en el tiempo en cada punto de entrega intermedio.

Beneficios:

El seguimiento del medicamento a medida que se abre paso a través del proceso de entrega. Esto simplifica y agiliza en gran medida la gestión de la distribución de medicamentos que puede evitar que caigan en las manos equivocadas, autenticando el medicamento para el consumidor final, lo que reduce en gran medida la posibilidad de falsificación, la manipulación de precios y la entrega de medicamentos vencidos.

DAOs.

¿Qué es una DAO y cómo funciona?

El acrónimo DAO alude a Decentralized Autonomous Organization (Organización Autónoma Descentralizada). En términos simples, una DAO es una organización gobernada por código y programas informáticos. De esta forma, tiene la capacidad de funcionar de manera autónoma, sin necesidad de una autoridad central. Mediante el uso de smart contracts, una DAO puede trabajar con información externa y ejecutar órdenes basadas en ella, todo ello sin ninguna intervención humana. Las DAOs son habitualmente operadas por una comunidad de partes interesadas, incentivados a través de algún tipo de mecanismo ligado a tokens. Las reglas y los registros de las transacciones de una DAO se almacenan de forma transparente en la blockchain.

“Beneficios de La cadena de bloques o blockchain aplicada a la administración tributaria de la provincia de Santa Fe”

Fundación para los Estudios Internacionales
Mendoza 444 - Rosario, Santa Fe - C.P. 2000



4.3. Conclusiones obtenidas.

Como bien estaba planteado en el proyecto, al concluir las capacitaciones se preveía una charla con los asistentes para así obtener información para sacar conclusiones y emitir un documento en donde se detalle en que sectores se pueden lograr grandes beneficios de aplicación y en cuales se encuentra cierta resistencia a la nueva tecnología de acuerdo al conocimiento, área y experiencia de los capacitados. Copiamos debajo una gráfica de elaboración propia, para sintetizar de forma visual los sectores de la Provincia de Santa Fe en donde es más factible la aplicación de la tecnología blockchain y los sectores en los que se encuentra mayor resistencia.

Areas	Muy Factible	Factible	Poco Factible
Licitaciones	X		
Educación	X		
Salud		X	
Administración tributaria		X	
Servicios Públicos			X
Registro de propiedad	X		
Defensa			X
Administración general		X	
Aduana	X		
Seguridad			X
Licencias y títulos	X		
Producción y Economía	X		
Identidad		X	

Capítulo V: “Proyecto BlockchainLAB Santa Fe”

5.1. Introducción

El objetivo de esta etapa es brindar un marco teórico para el desarrollo de un Laboratorio Blockchain (BlockchainLAB) con un enfoque regional amplio, es decir, un lab que abarque tanto al sector tributario, el resto del sector público de la provincia de Santa Fe, como así también al sector privado y académico de la provincia.

La creación de un Blockchain LAB tiene como objetivo principal generar un entorno en el que se incentive el uso de la tecnología blockchain. El desafío es poner a disposición de los diferentes ecosistemas productivos un entorno en el que puedan encontrar infraestructuras comunes, colectivas, abiertas e inclusivas para sus soluciones. Este espacio está pensado en facilitar la posibilidad de acceder a información y capacitación como así también la infraestructura blockchain (red) en donde se podrá correr, testear y desarrollar las diferentes iniciativas.

Para la presente etapa, se relevaron proyectos tanto del ámbito privado (Blockchain communityLab de España) como del ámbito público (UTN Blockchain Lab de La Plata.) que sirvieron como base para la preparación del presente proyecto.

5.2. Misión y Visión

Misión: Impulsar la adopción de la tecnología blockchain en la provincia de Santa Fe para fomentar la innovación.

Visión: Brindar conocimiento a los santafesinos, mejorar la seguridad digital, generar confianza en el estado, economía y sociedad digital, fomentando el uso eficiente de la energía, apoyando así el crecimiento inclusivo y el bienestar de los habitantes de la provincia.

5.3. Características

BlockchainLAB Santa Fe, a nuestro entender tendría que organizarse como un consorcio para la gestión y administración de una infraestructura que se cataloga como público permissionada. Es por tanto una red abierta a cualquier participante que esté de acuerdo con un conjunto de reglas a establecer, que se podrían reducir a estar identificado y cumplir con la regulación.

La infraestructura tiene que ser de propósito general, abierta a cualquier tipo de uso que cada participante decida siempre y cuando no se haga un uso ilícito u ofensivo. A diferencia de otras redes muy orientadas a usos especializados, como los pagos, la trazabilidad de alimentos, la transparencia en procesos públicos; o muy focalizadas en los criptoactivos, tendría que promoverse un uso inclusivo y mixto de cualquier caso de uso. Esto permitirá la diversidad de participantes, la creación de un verdadero espacio digital único.

Una red blockchain implica la existencia de registros compartidos con múltiples actores que afectan a múltiples interesados. Por tanto, la regulación común, el uso de un mismo lenguaje y de unos estándares sobre sus procesos y componentes se hace imprescindible. En este sentido, habría que desarrollar una estrategia activa para su normalización y estandarización que sea reconocida globalmente a través de alguna institución especializada en la materia.

Propuesta de Valor: El LAB es un elemento articulador de Comunidades que necesitan una infraestructura que apoye sus iniciativas comunes o los proyectos individuales de sus miembros. Es una oportunidad para el desarrollo del emprendimiento y de los negocios al ofrecer un espacio digital completamente único, seguro, confiable y comprensible para los reguladores. Buscamos decididamente generar un entorno viable para que puedan ofrecerse soluciones y servicios válidos para ciudadanos y consumidores para los que les resulta indiferente la tecnología que subyace a los mismos.

El objetivo de la iniciativa es construir un espacio digital a nivel regional. Una infraestructura principal que no conozca de fronteras, que permita que las soluciones y los servicios que la utilicen puedan estar a disposición de cualquier persona u organización de la provincia y zonas aledañas.

Testnet: El LAB tendría que contar con redes testnet robustas que pueden utilizarse gratuitamente, sobre las que las entidades interesadas puedan desplegar

sus aplicaciones y casos de uso. Para el desarrollo de la testnet o asociación a una blockchain externa, se podría realizar un convenio con la BFA (Blockchain Federal Argentina).

La blockchain del LAB está pensada para un uso masivo y en la vida real de la tecnología. Quiere ser la infraestructura de soluciones y servicios pensados para usuarios finales que tengan la condición de ciudadanos en el uso, por ejemplo, de servicios públicos o consumidores en un ámbito comercial. La gestión de la responsabilidad es un elemento esencial para que esta tecnología pueda ser usable con plena garantía legal. Por tanto, el establecimiento de marcos tecno-legales robustos y confiables se convierten en una de las necesidades esenciales. Sin ellos no sería posible un uso masivo y escalable de este espacio digital.

Localización: Creemos que la localización más conveniente para el emplazamiento del LAB sería la ciudad de Santa Fe, debido a que allí se encuentra ubicada toda la administración central de la provincia, la universidad del litoral y cuenta con el aprovisionamiento de todos los servicios necesarios para llevar a cabo el proyecto.

5.4. Administración

Pensamos que una adecuada organización del LAB podría estar integrada de la siguiente manera:

Consejo de Administración: Constituido por cinco miembros titulares y cinco suplentes, representando a cada uno de los sectores: 2 representantes del Gobierno de la Provincia de Santa Fe, 1 representante de una Institución académica, 1 representante del Sector Privado, y 1 representante de la Sociedad Civil. La responsabilidad del Consejo sería administrar el LAB de acuerdo a las instrucciones del contrato de creación del mismo.

Reunión de Sectores: Constituido por los sectores representados, cuya función sería elegir a los representantes, elaborar y/o modificar el contrato de creación del LAB.

Comité Técnico: Conformado por expertos en Blockchain e IT. Cuya responsabilidad sería la de brindar asesoramiento al Consejo de Administración.

Grupos de Trabajo: Son espacios de debate con participación abierta para las partes e interesados. Proponemos la organización de los grupos de trabajo de la siguiente manera: Tecnología – Comunicación – Casos de uso – Legal y Finanzas–

El Grupo de tecnología es responsable de la implantación, mantenimiento y mejora de la infraestructura, y las diferentes herramientas de monitorización y análisis de datos. También es responsable del apoyo en diseño e integración de soluciones digitales y aplicativos sobre la red, apps, dapps y proyectos que utilizan la red. El apoyo consiste en el asesoramiento en el diseño de la solución y el soporte técnico para su correcto despliegue sobre la red. Dentro de lo que es infraestructura específicamente, este grupo de trabajo tendrá a su cargo mejorar todas las herramientas tecnológicas ofrecidas por el LAB para hacerlas cada día más escalables y robustas, mantener y mejorar la capa de red, idear, diseñar, y desarrollar herramientas de monitorización sobre la red, mejorar todo lo relacionado con la seguridad de la red y el despliegue de soluciones sobre la misma, así como realizar pruebas de estrés que permitan mapearlos límites funcionales y operativos.

Comunicación: La comunicación es clave para que todos los aliados estén enterados de lo que ocurre dentro del proyecto. Y se podría dividir en 2 vertientes:

Externa.

- **Página web:** La página web busca resolver con inmediatez cualquier posible duda que puedan tener los futuros interesados en todos los niveles y líneas de actuación, al mismo tiempo que ofrecer un lugar de encuentro y exposición para todos los que estén explorando o usando blockchain en la región.

- **Redes sociales:** Actualización de contenidos que se generan desde el LAB, desde participación en eventos, lanzamiento de aplicaciones, desarrollo de soluciones, talleres, colaboraciones, etc.

- **Eventos:** Eventos únicos y disruptivos que generen repercusión, visualización y divulgación. Los eventos serán talleres, hackatones, retos, meet ups, webinars, entre otros.

- **Prensa:** Se busca crear repercusión y divulgación de eventos y acontecimientos de relevancia en los medios de comunicación de la provincia.

- **Comunidad:** Presencia activa en grupos de mensajería instantánea donde ya hay una fuerte presencia de la comunidad blockchain.

Interna.

- **Junta directiva:** Reuniones de seguimiento mensual con el objetivo de mantener informados a los participantes sobre los avances que se han producido durante el mes, acordar enfoques y definir siguientes pasos.

- Newsletters: Actualización de actividades, eventos y noticias con periodicidad mensual para los participantes.

Legal y Finanzas: La idea del LAB es de promover infraestructuras blockchain para la vida real. Que puedan soportar aplicaciones y servicios que tengan como usuarios finales todo tipo de organizaciones y personas, en su condición de ciudadanos -usuarios de servicios públicos- y consumidores normalmente protegidos por regulaciones especializadas.

Por ello, las aplicaciones que utilicen las infraestructuras, lo harán en un entorno seguro, en el que la gestión del ciclo de vida de la red (su establecimiento, operación y, en su caso, terminación) tenga un marco regulatorio preciso.

Dentro de esta área se trabajará la elaboración de un marco normativo y regulatorio acorde a las normas legales del país y de la provincia. Por su parte el área de finanzas será la responsable del destino de los fondos recibidos por parte de los participantes, cumplimiento de las metas presupuestarias y consideramos sería oportuno que esta área cuenta con un fondo que actúe como incubadora o aceleradora de proyectos innovadores que sean de utilidad para la provincia de Santa Fe.

Finalmente, otro grupo de trabajo que se propone es de casos de uso. En esta categoría se concentrará la información sobre los proyectos que están participando del LAB. El objetivo es que cada proyecto pueda proveer información sobre demos, código, videos, documentos, enlaces y entidades o personas involucradas.

5.5. Ecosistemas

Los servicios del LAB están destinados a todo tipo de personas y organizaciones que consideren que la tecnología blockchain puede ser un elemento de utilidad. Podría denominarse ecosistema al colectivo de personas y organizaciones que directa o indirectamente participan y se benefician de las infraestructuras y servicios del BlockchainLAB Santa Fe. Estas comunidades pueden estar configuradas a nivel de una localidad o región. También la comunidad puede corresponderse con un sector de actividad económica, o tratarse de un ámbito de estudio. Confiamos igualmente que sectores de la sociedad, como las universidades o las administraciones públicas, o de la actividad empresarial, desde los servicios financieros a la actividad agropecuaria vayan organizando sus propios grupos de trabajo aprovechando una infraestructura ya existente que evita un importante esfuerzo en tiempo e inversiones necesarias.

5.6. Emprendimientos

Una idea clave del proyecto es que se logre establecer un soporte para el emprendimiento de la región. Los Proyectos se lanzarían sobre bases estándar ya desarrolladas que configuran sus infraestructuras principales (tecnología, identidad, dinero tokenizado), ofreciendo de manera nativa elementos que, en un entorno tradicional, habría que construir cada vez y para cada emprendimiento. El esfuerzo de inversión en cada proyecto empieza a ser en cierto punto marginal, el time-to-market se acelera, los riesgos tecnológicos, operacionales y regulatorios se minimizan. También incluso los riesgos de mercado se mitigan, dado que facilitará la creación de un marketplace especializado que permitirá el acceso de estos nuevos emprendimientos a los grandes clientes que participan en la iniciativa, aportándoles por tanto tracción y verdaderas oportunidades de negocio. Además, sería conveniente que se desarrolle un conjunto de plataformas de apoyo al emprendimiento (como por ejemplo servicios de incubadora, aceleradora o contacto), incluyendo no solo la puesta a disposición de la infraestructura, sino también la asesoría tecnológica, la financiación de nuevos prototipos de aplicaciones y la inversión en los emprendimientos con mayor potencial de negocio y propósito de impacto.

5.7. Enseñanza

Por último y como uno de los pilares del proyecto, se recomienda crear un plan estratégico de formación académica en blockchain para fortalecer los conocimientos de los interesados e incentivarlos a descubrir los beneficios de la tecnología. Como hemos visto en capítulos anteriores el desconocimiento general en la materia es una de las principales barreras para su adopción. Desarrollar un programa de capacitación que incluya publicaciones, videos y cursos certificables sería de vital importancia para el futuro del proyecto en general.

Capítulo VI: “Conclusiones Finales”

El mundo que conocemos está cambiando; y lo hace a una velocidad tal que no hay proceso de adaptación conocido que pueda igualarlo. Eso, en sí mismo, no parecería una desventaja sino hasta que se toma conciencia de todo lo que está en riesgo si no se acompaña ese cambio tecnológico, diseñando un marco normativo a nivel nacional que lo contenga, que lo acote, que evite pueda descontrolarse.

La tecnología Blockchain y las criptomonedas llegaron para quedarse. Es un hecho, tanto como que habrá fuertes repercusiones en todas las esferas de la vida:

social, económica, legal, ambiental, institucional, técnica. Y esta tecnología está en su "etapa embrionaria", lo que significa que estamos a tiempo de aprovechar una rápida adopción por parte de la Administración Tributaria de la provincia de Santa Fe.

Una de las características distintivas de estas nuevas tecnologías es la naturaleza distribuida de la información, que mantiene una pista de auditoría completa en toda la cadena. Cualquier persona con los derechos de acceso apropiados puede acceder a una copia de ese libro mayor y verificar transacciones pasadas sin tener que confiar en los participantes en la transacción original. Esta cualidad intrínseca de Blockchain, la de brindar confianza sin depender de intermediarios, viene a romper el paradigma transaccional que nos acompañó desde el origen del hombre e implica, desde un punto de vista económico, empoderar al sujeto, individuo, y desempoderar a los intermediarios (bancos, gobierno, organismos supranacionales, registros, consejos profesionales, empresas de seguros). Esto deviene en menores costos de transacción, menores tiempos de transacción, mayor certidumbre de todo el proceso, mayor seguridad, mayor transparencia, más fácil de ejercer control por parte de cualquier nodo de la red. Tales cualidades facilitarán enormemente las tareas de liquidación y pago de tributos respecto de los contribuyentes, y las de contralor y fiscalización de las Administraciones Tributarias.

Los retos jurídicos que plantea el uso de contratos inteligentes, en el marco de las tecnologías de registro distribuido, son actualmente inabarcables. Se requiere una investigación por sectores del ordenamiento capaz de dar respuesta al posible acoplamiento a las normas existentes de las respuestas a los retos que plantean, en la práctica, las cadenas de bloques, tanto públicas como privadas.

En muchas ocasiones, el derecho vigente no puede acoger los supuestos fácticos presentados en la aplicación de estas tecnologías, por lo que es preciso un nuevo abordaje, tanto doctrinal como normativo, de la diversidad de cuestiones presentadas. Y para llevar el proceso de automatización un paso más allá, se pueden utilizar productos y dispositivos "inteligentes". Estos tienen la capacidad de comunicarse entre sí y de informar su estado y posición a través de Internet. Esto les permite confirmar cuándo se han cumplido ciertas condiciones en un contrato, lo que desencadena el pago y la creación del siguiente bloque.

La incertidumbre parece estar en la raíz del conflicto, la incertidumbre provocada por cambios continuos a un ritmo sin precedentes. Esta incertidumbre necesita ser abordada si se quiere superar el conflicto. Con este fin, construyendo un marco para las nuevas tecnologías y sus aplicaciones y potencialmente para el cambio continuo es un paso clave.

Para ese fin, en esta etapa, el enfoque debe estar en los errores del pasado que deben ser explotados para formulación de las preguntas a responder para establecer el contexto. En cualquier caso, establecer el contexto reglamentario no será suficiente. La sociedad necesita estar preparada para comprender las reglas del juego para jugar por ellos. Se necesita una cultura de cambio que nos permita vivir en el mundo de la revolución digital y de cada nueva revolución por venir.

Es la comunicación, el diálogo y la participación transparentes y sustanciales lo que necesitará la sociedad, así como un método para controlar la riqueza de la información, para que sea utilizada con un buen propósito.

Se ha dicho que Blockchain tiene el potencial de desestabilizar el monopolio estatal sobre los ciudadanos y aumentar la libertad a través de la web. Usar esta tecnología es como tomar un paso hacia la independencia. Y, como todo proceso hacia la independencia requiere de la valentía, esfuerzo y sacrificio de algunos para que todos podamos disfrutar de ella. También conlleva costos, no necesariamente soportado por todos o al menos no en igual medida. Pero una cosa es cierta en todo proceso de independencia: el que va a la vanguardia tiene más probabilidad de quedarse con las mejores oportunidades.

Por todo lo expresado en los párrafos anteriores, creemos resulta indispensable por parte de la AT de la Provincia de Santa Fe, embarcarse en el conocimiento, uso y perfeccionamiento de las cadenas de bloques, para así comprender los beneficios que esta tecnología le aportaría a la eficiencia de su estructura y funciones.

Capítulo VII: “Bibliografía”

Satoshi Nakamoto (2008). Bitcoin: A Peer to Peer Electronic Cash System.
Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. By Vitalik Buterin (2014).

Nick Szabo (1996) Smart Contracts: Building Blocks for Digital Markets.

Fabian Vogelsteller, Vitalik Buterin, "EIP-20: Token Standard," *Ethereum Improvement Proposals*, no. 20, November 2015. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-20>.

William Entriken, Dieter Shirley, Jacob Evans, Nastassia Sachs, "EIP-721: Non-Fungible Token Standard," *Ethereum Improvement Proposals*, no. 721, January 2018. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-721>.

Witek Radomski, Andrew Cooke, Philippe Castonguay, James Therien, Eric Binet, Ronan Sandford, "EIP-1155: Multi Token Standard," *Ethereum Improvement*

“Beneficios de La cadena de bloques o blockchain aplicada a la administración tributaria de la provincia de Santa Fe”

Fundación para los Estudios Internacionales
Mendoza 444 - Rosario, Santa Fe - C.P. 2000

Proposals, no. 1155, June 2018. [Online serial]. Available:
<https://eips.ethereum.org/EIPS/eip-1155>.

Kakavand, Kost De Sevres, & Chilton, 2017 *The Blockchain Revolution*.

Bartolomé, Bellver, Castañeda, & Adell, 2017. *Blockchain en Educación*.

Sharples & Domingue, 2016. *The Blockchain and Kudos: A Distributed System por Education Record, Reputation and Reward*.

“Technology Roadmapping in Canada: A development Guide” 2011

Deloitte University Press (2017). “Will Blockchain Transform the Public Sector?”

Foro Económico Mundial (2020). *Kit de herramientas blockchain del Foro Económico Mundial*.

Unidad de Información Financiera (UIF) mediante la Resolución 300/2014 (B.O. 10/07/2014)

BCRAComunicación “A”6823 del 31/10/2019.

BCRA Comunicación “A”7030 del 28/05/2020 (modificada por la “A”7042 del 11/06/2020).

Leslie Lamport (1990) *Part Time Parliament a ACM Transactions on Computer Systems*

PricewaterhouseCoopers LLP. (2016, December). *How blockchain technology could improve the tax system*. PWC.

Deloitte. (2017, December). *Blockchain technology*. (D. Poland, Ed.) Deloitte

EY. (2018, April 25). *How blockchain could transform the world of indirect tax*. (EY, Ed.) Ernst & Young Global Limited.

PwC. (2019). *Establishing blockchain policy. Strategies for the governance of distributed ledger*. Future Blockchain Summit. Dubai: Dubai World Trade Centre.

Secco, A. (2017b, Julio 19). *Blockchain: Conceptos y aplicaciones potenciales en el Área Tributaria (2/3)*. (CIAT, Ed.) Centro Interamericano de Administraciones Tributarias.

Seco, A. (2017a, Julio 17). *Blockchain: Conceptos y aplicaciones potenciales en el área tributaria (1/3)*. (CIAT, Ed.) Centro de Interamericano de Administraciones Tributarias. Retrieved from <https://www.ciat.org/blockchainconcepts-and-potentialapplications-in-the-tax-area-13/?lang=en>

Tapscott, D., & Tapscott, A. (2017). *La revolución blockchain. Descubre cómo esta nueva tecnología transformará la economía global*.



Dr. JOSÉ ANIBAL ROMERO
PRESIDENTE