17º SIMPOSIO REGIONAL DE INVESTIGACIÓN CONTABLE
Instituto de Investigaciones y Estudio Contables – FCE - UNLP

Tema al que pertenece
AUDITORIA, ASEGURAMIENTO Y COMPLIANCE

Título del trabajo

EL IMPACTO DE LA BLOCKCHAIN Y LOS ACTIVOS DIGITALES EN EL ENFOQUE DE AUDITORIA

ENTREGABLE PERTENECIENTE AL PROYECTO DE INVESTIGACIÓN
“EFECTOS DE LAS NUEVAS TECNOLOGÍAS DE INFORMACIÓN (TI) EN EL EJERCICIO DE LOS
PROFESIONALES EN CIENCIAS ECONÓMICAS - LOS NUEVOS ROLES

Nombre de los autores
Cdor. Carlos Rumitti – Cdora. Gabriela Castiglioni - Becario José Villar

La Plata, Noviembre 14 de 2021

RESUMEN

La Blockchain forma parte de la vida real de las organizaciones y las expectativas a futuro es que su implementación se potencie y deversifique. Una tendencia que ya es irreversible y una de las actividades profesionales que deberá adaptar sus procedimientos a raíz de su existencia es la auditoría. Es una realidad que hay que identificar, analizar, aprovechar sus oportunidades y dar respuesta a los riesgos que trae asociados.

La aparición de la Blockchain plantea en la actualidad variados interrogantes de diversa naturaleza a los auditores, los profesionales de la contabilidad, asesores en finanzas y los liquidadores de impuestos, entre otros.

Desarrollaremos un análisis de las repercusiones que tiene la tecnología blockchain en el enfoque de auditoría a aplicar, dado que, con su utilización, están garantizadas la seguridad, irreversibilidad y transparencia de las transacciones registradas, pero por si mismas, no brindan evidencia suficiente y adecuada de auditoría, requiriendo que el contador aplique procedimientos adicionales para su obtención, así como para la evaluación de los controles que las sustentan.

Palabras clave: blockchain – auditoría – enfoque

ABSTRACT

Blockchain is part of organizations real life and there are future expectations that its implementation will be strengthened and diversified. It is an irreversible trend and Audit is one of the professional activities that must adapt its procedures to the root of its existence. It is a reality that must be identified, analyzed, take profit of its opportunities and give an answer to the associated risks.

The emergence of the Blockchain technology currently raises a number of questions of diverse nature for auditors, accounting professionals, financial advisers and tax officers, among others.

We will develop an analysis of the repercussions that Blockchain technology has on the Audit approach to be applied, since with its use the security, irreversibility and transparency of the registered transactions are guaranteed, but by themselves they do not provide sufficient and adequate audit evidence, requiring to the accountant to apply additional procedures to obtain them, as well as to evaluate the controls that support them.

Keywords: blockchain – audit - audit approach

I. INTRODUCCIÓN

La Blockchain provocó una revolución completa en las transacciones.

La investigación pretende abordar las implicancias que tiene en el enfoque de auditoría a emplear por el auditor de estados contables con fines generales la utilización de Blockchain como parte central de la infraestructura de TI por parte de la organización emisora.

El presente trabajo hace un recorrido desde la consideración de aceptar el encargo, su planificación hasta la ejecución del mismo, centrándose en cómo esta tecnología trae asociados nuevos riesgos, cómo se entrecruza con el control interno, en cuanto al diseño y la implementación.

Por último, pretende ser un disparador para reflexionar sobre las capacidades que deben tener los profesionales en ciencias económicas para cumplir satisfactoriamente con este nuevo rol ante un cambio de paradigma.

II. IMPACTO DE LA BLOCKCHAIN Y LOS ACTIVOS DIGITALES EN LA EVALUACIÓN DE RIESGOS, LA PLANIFICACIÓN Y EJECUCIÓN DE UNA AUDITORIA.

Evaluación de Riesgos y Planificación

El auditor antes de considerar aceptar un nuevo encargo o continuar uno existente deberá analizar con precaución los riesgos y desafíos únicos que conlleva, en el caso que el ente utilice tecnología blockchain¹ y posea activos digitales.

Si el ente utiliza Blockchain como tecnología subyacente, el auditor principal deberá contemplar que el equipo de auditores y colaboradores sea multidisciplinario y posean la competencia², las habilidades o conocimientos especializados en criptografía, tecnología de contabilidad distribuida, habilidad para aplicar marcos legales y reglamentarios existentes a los criptoactivos, por ejemplo, las disposiciones que afectan al ente sobre conozca a su cliente y contra el lavado de activos.

El Código de Conducta Profesional del AICPA explica el significado de competencia, indicando:

- La competencia se deriva de una síntesis de educación y experiencia.
- La competencia representa el logro y mantenimiento de un nivel de comprensión y conocimiento que permite a un miembro prestar servicios con facilidad y perspicacia.

Otra cuestión importante a considerar antes de aceptar el encargo es si el personal del ente tiene la experiencia para tratar con criptoactivos, porque si no la tiene, aumenta el riesgo de error en el procesamiento y la notificación de las transacciones que involucran criptoactivos. Como menciona el AICPA³ *si la gerencia tiene la integridad y una estrategia comercial sólida, pero no tiene las habilidades y competencias apropiadas, una auditoría puede no ser posible sin que la administración aborde las deficiencias.*

Al evaluar este riesgo (de la competencia y destreza del personal de la entidad) para el período bajo análisis, el auditor deberá comprender cuándo la administración obtuvo estos conocimientos necesarios que le permitan:

1. Identificar los riesgos únicos asociados a la blockchain y activos digitales y diseñar e implementar controles internos para responder a dichos riesgos. Incluirlos en su matriz de riesgos.
2. Comprender que la tecnología se encuentra en constante evolución y que pueden ser necesarios controles y personal adicionales.
3. Disponer procesos y controles para mantener libros y registros apropiados, incluido el mantenimiento de un soporte apropiado para las transacciones y la aplicación del marco de información financiera.
4. Contar con el personal competente, en permanente capacitación.
5. Identificar las leyes y regulaciones aplicables
6. Tener capacidad (decisión y presupuesto) para identificar la necesidad de recurrir a especialistas

Esto es lo que tanto el AICPA como IFAC llaman *evaluar la integridad de la administración*, que además forma parte de lo que el AICPA denomina *ecosistema de activos digitales*.

¹ Blockchain debe ser entendido en este documento como tecnologías de cadenas de bloques y de libro mayor distribuido. *Blockchain y Control Interno: Perspectiva COSO*

² Competencias todavía “escasas” en el mercado.

³ AICPA Accounting for and auditing of digital assets. [accounting-for-and-auditing-of-digital-assets.pdf](#)

Particularmente y de acuerdo al marco normativo de IFAC⁴, los nuevos riesgos requieren adecuar el enfoque al aplicar la **NIA 315** (identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y su entorno), y la **NIA 330** (respuestas del auditor a los riesgos valorados) para la evaluación y respuesta de los nuevos riesgos, así como, los controles diseñados e implementados por los comitentes, incluyendo la prueba de eficiencia operativa de dichos controles y los demás procedimientos sustantivos que se considere necesarios, en la auditoría de Estados Financieros.

El auditor también deberá considerar la magnitud y cantidad de operaciones, definir si son utilizados los activos digitales como medios de pago o son poseídos con carácter especulativo o ambos, lo que podrá incidir en su decisión.

Ponderadas estas cuestiones, que no pretendemos sean exhaustivas, decidirá si se encuentra en condiciones de prestar el servicio, pudiendo ser un encargo de aseguramiento de estados contables.

Una vez decidido a aceptar al cliente, el contador deberá analizar, antes de planificar y definir el enfoque de auditoría a aplicar, si la organización ha adecuado su sistema de control interno, su estructura e implementación, en otras palabras, si ha ampliado el concepto de entorno de control, realizado un análisis de los riesgos, desarrollado actividades de control y supervisión sobre la información financiera asociada a blockchain.

Recordamos que la RT 37 en el capítulo III A Auditoría externa de estados contables con fines generales, apartado i. define qué debe entenderse por Planificación⁵ de la auditoría y qué cuestiones hay que considerar.

Se presenta a continuación un detalle resumen de los aspectos considerados por nosotros como mínimos, que deberá analizar el auditor (previa planificación) relacionados al control interno en la aplicación de esta tecnología, se aborda cada uno a lo largo del documento.

- ✓ Registro
- ✓ Almacenamiento
- ✓ Tipo de cadena
- ✓ Protocolo de consenso
- ✓ Pseudoanonimato de las transacciones
- ✓ Política de riesgo
- ✓ Separación de funciones
- ✓ Responsabilidad y autoridad entorno a esta tecnología y a las transacciones
- ✓ Claves privadas

Al utilizar esta tecnología se ve afectado el componente **entorno de control**, dado que la entidad trabaja de manera colaborativa con diferentes entidades utilizando una **base de datos descentralizada**.⁶

⁴ Aplicable en Argentina por Acta de Tucumán en forma directa o referencial (RT 32 y 37 de FACPE)

⁵ Punto 3.4. Planificar en forma adecuada el trabajo de auditoría, teniendo en cuenta la finalidad del examen, el informe a emitir, las características del ente cuyos estados contables serán objeto de la auditoría (naturaleza, envergadura y otros elementos), las circunstancias particulares del caso y la valoración del riesgo efectuada, con el objetivo de reducir este último a un nivel aceptablemente bajo en las circunstancias. La planificación debe incluir la selección de los procedimientos a aplicar, su alcance, su distribución en el tiempo y la determinación de si han de ser realizados por el contador o por sus colaboradores. Preferentemente, la planificación se debe formalizar por escrito y, dependiendo de la importancia del ente, debe comprender programas de trabajo detallados.

Una distinción que hay que realizar es si blockchain es el **único dispositivo de registro** de los activos digitales. El hecho de ser descentralizada la base, significa que no hay una única parte responsable de los registros sino que todos lo son, ya que todos la validan, logrando una mayor visibilidad de las transacciones y disponibilidad de los datos. Los miembros (nodos) son los responsables de acordar las adiciones a la cadena. Así, antes de que cualquier transacción se introduzca en una cadena de bloques debe ser acordada a través de un **protocolo de consenso por el que se la asegura⁷ en un bloque**. Cada bloque se vincula al bloque anterior con un identificador único, es decir un hash⁸. La cadena de bloques se convierte así en un libro de contabilidad digital, segura, transparente e irreversible que se comparte entre todos los participantes de la cadena.

Deberá el auditor leer, analizar y evaluar ese protocolo de consenso de la cadena de bloques, porque si se encuentra mal diseñado, implementado o es débil, compromete la capacidad de la tecnología para asegurar adecuadamente las transacciones. De ser así, será poco fiable la información registrada en el libro mayor pudiendo ser inválida, por ser inexacta y poco confiable.

Uno de los beneficios de utilizar Blockchain es que mejora el entorno de control al reducir los errores humanos en las registraciones, manteniendo la integridad de los registros y proporcionando un registro irrefutable. ¿Por qué es irrefutable? Porque la organización no puede negar o impugnar su la autorización /envío de un mensaje o registro. También facilita disposición y presentación más oportuna de la información relevante.

Un aspecto importante para el auditor es si la **cadena de bloques** es "**on-chain**" u "**off-chain**", lo cual tiene un efecto en la labor:

- Si la cadena es "on-chain" significa que la información se almacena en la propia blockchain, y el auditor debería realizar pruebas sobre ella.
- Si la cadena es "off-chain" significa que la información no está almacenada en la blockchain pero está conectada directa o indirectamente a la información guardada en la cadena "on-chain". En este caso el auditor evaluará la metodología de conciliación y los controles asociados.

Algunas cadenas de bloques presentan la ventaja de crear y presentar automáticamente un registro electrónico de todas las transacciones lo que se transforma en la **pista de auditoría** pero solo en lo referente a la existencia del registro, es probable que el auditor deba aplicar procedimientos adicionales para determinar la propiedad y derechos sobre ese activo digital, es decir que una transacción este en la cadena valida la existencia, pero no la propiedad y los derechos asociados.

Si el auditor logra validar los controles implementados por el ente relacionados a las tecnologías subyacentes, su trabajo se verá facilitado por la mayor automatización de controles y las interacciones de las tecnologías probadas, reduciendo las pruebas sustantivas.

Clasificación de los controles

Los controles pueden ser:

- ✓ Preventivos: antes que se materialice el riesgo⁹.

⁶ Una base de datos descentralizada es aquella donde los datos están estructurados y organizados para ser fácilmente accesibles, gestionados, actualizados y consultados, con un enfoque de recuperación. *Blockchain y Control Interno: Perspectiva COSO*

⁷ Minado, aceptación para ser registrada en un bloque.

⁸ Algoritmo criptográfico unidireccional para tomar datos de cualquier tamaño y convertirlos en una pieza única de información de tamaño fijo

⁹ posibilidad de que un acontecimiento ocurra y afecte negativamente a la consecución de los objetivos. Informe Coso – Marco Integrado

- ✓ Detectivos: durante o después que se materialice el riesgo.

El efecto de la Blockchain en los controles hace que en los preventivos, las transacciones sean inmutables una vez registradas, es decir, prima el correcto registro. Inmutable hace referencia a la naturaleza de la cadena de bloques sellada criptográficamente, que significa que la información/transacción, una vez escrita en la cadena es muy difícil de alterar (no imposible). Así, como se menciona en *Blockchain y Control Interno: Perspectiva COSO* se promete la integridad de los registros, pero no promete que los propios registros reflejen transacciones legales o debidamente clasificadas. Es decir, proporciona seguridad a las transacciones, pero no proporciona seguridad a la cuenta /cartera, por lo tanto el valor almacenado en cualquier cuenta sigue siendo susceptible de ser tomado, si las claves privadas de una organización son robadas¹⁰.

Con respecto al efecto que posee la Blockchain en los controles detectivos, si se detectan incorrecciones, los ajustes sólo son posibles a futuro en función a la imposibilidad de hacerlos retroactivos o sobre registros históricos.

Riesgos

Los riesgos de control interno se ven fuertemente ampliados por el uso asociado a la Blockchain. A su vez, varían en función de la naturaleza y el tipo de blockchain que se implemente y la cantidad de influencia que ejerza el ente sobre la cadena, la supervisión y el control que la organización imponga.

Los riesgos dependerán del **tipo de cadena** que se implemente, pueden ser:

- Cadena de bloques privada con permisos propios.
- Cadena de bloques privada con permisos uniéndose a la blockchain de otra organización, lo que se llama **consorcio**. Aquí las decisiones se toman de manera coordinada. Deberá el auditor analizar la influencia que tiene cada organización de la cadena para ajustar los registros.
- Cadena de bloques pública sin permisos: lo que implica mayores riesgos porque la toma de decisiones puede ser descentralizada, dejando poco espacio para la influencia individual y poca responsabilidad.

Condición importante es el **pseudoanonimato de las transacciones**. En las cadenas públicas los activos se intercambian entre las direcciones de la cadena de bloques y las claves privadas se utilizan para la autorización, pero los nombres de las personas y las organizaciones no están explícitamente asociados a esas direcciones y claves. Esto podría llevar a que la organización no sepa con quien realiza transacciones, porque las entidades podrían estar encubiertas, ya que es posible realizar transacciones sin dar ninguna información personal identificable. Esta situación, puede afectar la política de diligencia debida si la tienen establecida. La idea de la contratación entre extraños fue la que impulsó a Nick Szabo en 1995 a concebir los contratos inteligentes sobre plataformas digitales.

El pseudoanonimato junto con la naturaleza abierta y la posible falta de controles¹¹, es una amenaza de que la cadena pueda ser utilizada para realizar operaciones fuera de toda ética e incluso delictivas.

Por estas cuestiones, el auditor deberá proceder a analizar las evaluaciones y conclusiones que haya realizado la dirección y el consejo de evaluación de los riesgos asociados al uso de las cadenas públicas, y si el nivel de riesgo se encuentra dentro de los rangos tolerables de la política de riesgo que tenga aprobada el ente.

¹⁰ La sustracción de claves por parte de los hackers se conoce como "ataque de punto final", común en este tipo de registros.

¹¹ Llamadas Barandillas por *Blockchain y Control Interno: Perspectiva COSO*

Tendrá que poner foco en si la entidad tiene establecido cómo se utilizará la cadena de bloques, y para qué, el nivel de responsabilidad y autoridad en torno a la tecnología blockchain, si existe separación de funciones en cuanto a: los privilegios de nivel de acceso, el acceso a la clave privada, la autorización de las transacciones y los informes financieros asociados.

El auditor deberá analizar la matriz de riesgos si es que la dirección la ha confeccionado, o aplicar algún procedimiento alternativo, para validar si la entidad ha identificado y valorado el efecto del uso de esta tecnología; tendrá que comprender cómo se integra la cadena de bloques con el/los sistemas que tenga la entidad, a su vez los accesos a la blockchain de la empresa y de las empresas que forman parte de la cadena; evaluar la ciberseguridad y ciberataques.

Debe chequear, para validar que se hayan mitigado los riesgos que quienes autoricen las transacciones de la cadena de bloques sean distintos de quien registra en el libro mayor digital, como así también quien autoriza y ejecuta los cambios en la tecnología subyacente.

Concordamos con la Perspectiva COSO que es recomendable utilizar técnicas de multifirma para las autorizaciones (se descentraliza el riesgo y el control al dividir partes de la clave privada).

El auditor debe comprender los controles implementados por el ente relacionados con las transacciones de criptoactivos, abarcando como mínimo:

- ✓ Los controles sobre la generación, gestión, almacenaje y salvaguarda de claves privadas, que son importantes para abordar los riesgos relacionados con la existencia de saldos de criptoactivos¹². Estas claves privadas proporcionan el control (es decir, el código de acceso y la capacidad de disponer) y existe un riesgo inherente de que las claves privadas puedan ser robadas, perdidas o mal utilizadas por personas internas o externas, entonces, comprender como se controlan es primordial
- ✓ Si los controles internos importantes residen en un tercero, determinar si existe un informe sobre controles de la organización de servicios que aborde esos controles, caso contrario esos controles tendrán que ser probados directamente por el auditor del emisor para obtener pruebas de su eficacia, acceso no siempre posible que puede causar una limitación en el alcance de su labor.
- ✓ los controles implantados sobre la fiabilidad de la información de la cadena de bloques que se utilizará como prueba de auditoría (por ejemplo, los controles que abordan las alteraciones de la información almacenada en la cadena de bloques).

En relación a las claves privadas, concordamos con el AICPA, que el auditor debe comprender:

- ✓ La seguridad de la ubicación del medio de resguardo físico de las claves privadas.
- ✓ Los procesos que rodean la gestión del ciclo de vida de las claves y el proceso de generación de estas (hardware, software y algoritmos asociados)
- ✓ La seguridad de los centros de datos de la entidad.
- ✓ Número de usuarios necesarios para procesar una transacción.
- ✓ Segregación de funciones en la autorización de transacciones de los activos digitales.

Una cuestión no menor al trabajar sobre el riesgo de fraude es contemplar el riesgo de anulación por parte de la dirección de los controles sobre las claves privadas, que puede dar lugar a un uso

¹² En caso de realizar transacciones mediante Exchange, las claves privadas permanecen en su poder.

indebido o a la apropiación indebida de las tenencias de criptoactivos por parte de quienes controlan las claves.

El auditor deberá comprender cómo la entidad auditada evaluó o consensuó las tolerancias al riesgo entre los miembros de la cadena de bloques, dado que no todos los componentes asumirán el mismo umbral. Es posible que lo encuentre en el protocolo, si no es así, deberá obtener la información necesaria requiriéndola a los aditores de los componentes si se trata del auditor del grupo.

La tabla que sigue contiene un resumen de principios claves a considerar sobre controles de una cadena de bloques.

Tabla sobre Controles de aspectos clave de Blockchain

Aspecto de la Cadena de Bloques	Consideraciones sobre la actividad de control
Nodos	<ul style="list-style-type: none"> - Cada ordenador de una red blockchain se conoce como "nodo". Será importante que las empresas hayan establecido controles que regulen las actividades de los nodos que almacenan copias de la base de datos, realizan la validación de las transacciones, trabajan para preparar los datos que se añadirán a la cadena o realizan otros servicios. - Asegurarse de que hay suficientes nodos trabajando para minimizar la oportunidad de que algunos colaboren para atacar el sistema. - Probar la disponibilidad de los datos de la cadena de bloques desde diferentes nodos de la red - Verificar la coherencia de los datos obtenidos de los diferentes nodos. - Comprobar que los nodos realizan las validaciones pertinentes antes de aceptar añadir datos a la cadena. - Seguimiento y provisión de incentivos para las validaciones correctas y sanciones para las validaciones incorrectas.
Protocolos de consenso	<p>Los protocolos de consenso deben ser evaluados periódicamente para determinar si:</p> <ul style="list-style-type: none"> - Los nodos adecuados están autorizados a participar en el consenso. - Los protocolos se han diseñado adecuadamente y funcionan con eficacia. - Los incentivos para el cumplimiento de los protocolos y las sanciones por incumplimiento se han diseñado adecuadamente para mitigar el fraude. - Las principales categorías de consenso incluyen la prueba de trabajo, la prueba de participación o el voto mayoritario.
Claves Privadas	<p>Los entes deben tomar medidas para gestionar el acceso a sus claves privadas. Pueden contratar un custodio externo, quien puede requerir que se divida el acceso a la clave privada entre varias partes, requiriendo así la aprobación de las transacciones por varias partes (multifirma).</p>
	<p>Para mitigar los riesgos asociados a su uso los entes pueden:</p> <ul style="list-style-type: none"> - Implantar controles para validar la idoneidad del diseño y la

Contrato inteligente¹³	<p>eficacia de la implementación de los contratos inteligentes, realizar seguimiento de los cambios y actualizaciones de forma controlada, y garantizar que existe una documentación adecuada y un registro histórico para establecer la responsabilidad.</p> <ul style="list-style-type: none"> - Implementar controles sobre las entradas
--	--

Fuente: Tabla 5 *Blockchain y Control Interno. Perspectiva COSO*

El auditor deberá obtener evidencias acerca de cómo supervisa la administración las transacciones registradas mediante esta tecnología blockchain, particularmente deben estar identificadas las personas responsables de ejecutar los controles de supervisión y establecer las políticas y procedimientos acordados para el monitoreo, detección y comunicación de las deficiencias y posibilitar a la dirección tomar medidas correctivas en caso de ser necesarias.

El auditor, utilizando la evaluación continua mediante el uso de técnicas de auditoría de TI, identificará los cambios y actualizaciones de la tecnología, evaluará los protocolos de consenso, los contratos inteligentes y las claves privadas.

Lo mencionado es crítico para la identificación y evaluación eficaz del riesgo y es la base para planificar y realizar una respuesta de auditoría adecuada.

Ejecución

Para poder concluir con su labor, el auditor deberá realizar pruebas y procedimientos de auditoría suficientes y adecuados para obtener evidencias¹⁴ para respaldar su opinión. Estas comprenden tanto la información que respalda y corrobora las afirmaciones de la dirección, como la información que puede contradecir dichas afirmaciones.

Dados los desafíos descritos en los párrafos previos, encontramos apropiado como auditores incrementar nuestros procedimientos habituales, por ejemplo realizar consultas adicionales a la gerencia para comprender su propósito comercial relacionado con la participación actual y futura con los activos digitales, sobre la naturaleza de los activos digitales mantenidos y su importancia para el negocio; las políticas y procedimientos para incorporar nuevos clientes o entablar relaciones con actores; cuáles son los procesos y procedimientos para monitorear las transacciones en busca de actividades ilegales, entre otros.

Se presenta a continuación como la blockchain afecta a la **evidencia de auditoría**:

Concepto	Explicación
Valoración	La mayor parte del uso de la cadena de bloques es para rastrear una cantidad de algo (como el saldo de un activo digital), pero el valor del elemento rastreado no se mantiene necesariamente en la cadena de bloques.
Existencia	A menudo, la existencia de activos digitales depende únicamente de las pruebas que pueden obtenerse de una cadena de bloques. La fiabilidad de la información obtenida de la cadena depende de la eficacia de la tecnología y de los controles implementados en apoyo del sistema. Por lo tanto, el mero hecho de

¹³ programas informáticos almacenados que se auto ejecutan y el resultado de su ejecución queda registrado en la blockchain, no están limitados ni diseñados para actuar como un contrato legal, pero pueden impulsar el registro de una transacción o el intercambio de un activo digital de manera automática si se dan las condiciones

¹⁴ NIA 500 3.c IFAC: información utilizada por el auditor para alcanzar las conclusiones en las que basa su opinión.

	proporcionar información puede no considerarse una prueba adecuada suficiente para validar la existencia de un activo. En muchos casos, se justifican procedimientos adicionales (por ejemplo, la prueba de los controles internos relacionados con la cadena y la seguridad de las claves privadas).
Asignación	La información de la cadena de bloques -como el seguimiento de las acciones, los derechos de voto u otras relaciones basado en la cadena de bloques- puede utilizarse para respaldar los cálculos de asignación.
Ocurrencia	Al igual que en el caso de la existencia, la información obtenida de la cadena de bloques puede no respaldar por sí sola la afirmación de ocurrencia. Pueden ser necesarios procedimientos adicionales para demostrar la fiabilidad de la información almacenada en la cadena y, por tanto, la ocurrencia de una transacción. Además, la naturaleza pseudoanónima de las transacciones en la cadena podría ofrecer a los usuarios la oportunidad de realizar transacciones ficticias o transacciones con partes relacionadas que no tienen sustancia económica, inflando así los ingresos.
Complejidad	Cuando una cadena de bloques es el único registro de transacciones, puede servir como un registro completo; sin embargo, la integridad de las transacciones almacenadas en la cadena dependerá de la fiabilidad de la tecnología, así como de los controles implementados por la entidad para garantizarla. Además, cuando la información se registra total o parcialmente en otro sistema, la cadena de bloques no admite la integridad. Habría que establecer controles para garantizar que toda la actividad, dentro o fuera de la cadena, y todos los detalles, dentro o fuera de la cadena, estén disponibles y se registren por completo. Y que sus libros y registros capturan adecuadamente todas las transacciones.
Precisión	Al servir de registro para los activos digitales, la cadena almacena el historial de todas las transacciones y saldos. Esto no significa que la información sea exacta, sólo que los registros mantienen integridad.

Fuente: Apéndice 3. Blockchain, información financiera, afirmaciones y pruebas de auditoría. *Blockchain y Control Interno: Perspectiva COSO*

Algunas posibles incorrecciones que el auditor puede encontrar:

- Incorrecciones asociadas a los saldos de criptoactivos, que podrían depender de si los criptoactivos se almacenan en la propia cartera digital del emisor o por un tercero.
- La probabilidad y la magnitud de las posibles incorrecciones asociadas a las transacciones con criptoactivos podrían depender del número de tipos de criptoactivos, el número de clientes, el volumen de transacciones y la naturaleza del mantenimiento de registros (por ejemplo, si son off-chain las transacciones de los clientes se registran fuera de la cadena de bloques).
- Incorrecciones relacionadas con la validación de la transacción, lo que podría implicar que el auditor deba examinar la estructura de validación del emisor, y cualquier participación de terceros en el suministro.

III. TENDENCIAS: VENTAJAS Y DESVENTAJAS.

Desde enero de 2018 la IAASB ha emitido documentos, entre ellos una declaración de retroalimentación llamada "Explorando el uso de la tecnología en la auditoría, con un enfoque en el

análisis de datos”, donde aclaran que las ISAs (NIAs) deben seguir basándose en principios, y reflejar la era digital en el material de aplicación. Estos principios deben reconocer la evolución de la tecnología.

En relación a las pruebas de auditoría el IAASB enfatizó en la necesidad de que los auditores ejerzan escepticismo profesional en el uso de análisis de datos para ser utilizados como evidencias y destacó la importancia de la fuente y la calidad de los datos internos y externos utilizados.

IV. CONCLUSIÓN

Consideramos que el enfoque de auditoría que el auditor de estados contables deberá intentar aplicar será fundamentalmente de control en contraposición al enfoque basado en pruebas sustantivas; dado que si el auditor logra validar el entorno tecnológico del ente como no repudiable, es decir que logra validar los controles implementados relacionados a la utilización de Blockchain como tecnología base, todas las transacciones que se registren allí serán válidas; logrando así que su trabajo se vea facilitado por la mayor automatización de controles y las interacciones de las tecnologías probadas reduciendo las pruebas sustantivas.

No obstante, lograr que esta pista de auditoría sea confiable es el comienzo de la auditoría y no el final. La tecnología blockchain garantiza la seguridad, la irreversibilidad y transparencia de las transacciones registradas, sin embargo no brinda evidencia suficiente y adecuada de auditoría para poder emitir una opinión, debiendo el profesional aplicar los procedimientos adicionales específicos desarrollados a lo largo del documento para su obtención. Aplicando a lo largo de la auditoría escepticismo y criterio profesional.

REFERENCIAS BIBLIOGRÁFICAS

Auditoría de las criptomonedas. Audinet. Septiembre 2021

Auditoría para activos digitales. Aicpa.accounting-for-and-auditing-of-digital-assets.pdf

Blockchain y control interno: PERSPECTIVA COSO. COSO

Blockchain oportunidad desafío o riesgo para la auditoría interna. IAIA.

Guía de aplicación contable del bitcoin en El Salvador. Consejo de vigilancia de la profesión de contaduría pública y auditoría (CVPCPA).

NIA 300: Planificación de la auditoría de estados financieros

NIA 315 (Revisada): Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y de su entorno

Resolución Técnica 37: Normas de auditoría, revisión, otros encargos de aseguramiento, certificación y servicios relacionados . FACPCE

Revisión de la ISA-NIA 500, evidencia de auditoría. Septiembre de 2020. [iaasb-isa-500-project-update-september-2020 \(1\).pdf](#)