Blockchain y ciberseguridad en Auditoría Forense: Un enfoque innovador para la detección de fraudes en empresas de comercio electrónico.

LAURA DANIELA ASCENCIO FRACICA

UNIVERSIDAD SANTO TOMÁS

DIVISIÓNDE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y CONTABLES

ESPECIALIZACIÓN EN AUDITORÍA Y ASEGURAMIENTO DE LA INFORMACIÓN

DIRECTOR: ANDRES LEONARDO ESCOBAR SUAREZ

TUNJA

2024

Resumen

En la era digital, el crecimiento exponencial del comercio electrónico ha traído consigo desafíos significativos en términos de ciberseguridad y la detección de fraudes. La auditoría forense, como herramienta crítica en la identificación de fraudes, ha evolucionado con la incorporación de tecnologías emergentes, entre las que destaca el blockchain. Este artículo reflexiona sobre los resultados de investigaciones recientes que exploran la implementación de blockchain en auditoría forense dentro del ámbito del comercio electrónico, analizando su impacto en la ciberseguridad y la detección de fraudes. Se abordan perspectivas analíticas, interpretativas y críticas sobre cómo esta tecnología puede transformar los procesos de auditoría, fortalecer la integridad de los datos y mejorar la eficiencia en la identificación de actividades fraudulentas.

Palabras clave: Blockchain, Ciberseguridad, Auditoría Forense, Detección de Fraudes, Comercio Electrónico.

Abstract

In the digital age, the exponential growth of e-commerce has brought with it significant challenges in terms of cybersecurity and fraud detection. Forensic auditing, as a critical tool in the identification of fraud, has evolved with the incorporation of emerging technologies, among which blockchain stands out. This article reflects on the results of recent research that explores the implementation of blockchain in forensic auditing within the field of electronic commerce, analyzing its impact on cybersecurity and fraud detection. Analytical, interpretive and critical perspectives are addressed on how this technology can transform audit processes, strengthen data integrity and improve efficiency in identifying fraudulent activities.

Keywords: Blockchain, Cybersecurity, Forensic Audit, Fraud Detection, ECommerce.

Introducción

La rápida expansión del comercio electrónico ha incrementado la necesidad de sistemas robustos de ciberseguridad y mecanismos efectivos para la detección de fraudes. Las auditorías forenses han desempeñado un papel crucial en la investigación de delitos financieros, y la adopción de tecnologías avanzadas, como blockchain, se presenta como una solución innovadora para mejorar estos procesos. Blockchain, una tecnología de registro distribuido, ofrece características únicas como la inmutabilidad y la transparencia de los datos, que pueden ser aprovechadas para fortalecer los procedimientos de auditoría forense (Yli-Huumo et al., 2016).

En la última década, el comercio electrónico ha experimentado un crecimiento exponencial, generando un entorno dinámico pero vulnerable a fraudes y ciberataques. Este panorama ha impulsado a las organizaciones a buscar métodos más avanzados de protección y auditoría. La auditoría forense, un proceso clave en la identificación y análisis de fraudes financieros, ha comenzado a integrar tecnologías emergentes para mejorar su efectividad. Entre estas tecnologías, el blockchain se destaca por su capacidad para proporcionar una mayor transparencia y seguridad en la gestión de datos. Este artículo reflexiona sobre la implementación de blockchain en la auditoría forense aplicada al comercio electrónico, analizando cómo esta tecnología puede transformar la detección de fraudes y fortalecer la ciberseguridad.

El crecimiento acelerado del comercio electrónico ha transformado la manera en que las empresas operan, pero también ha incrementado los riesgos asociados a fraudes y ciberataques. En este contexto, la auditoría forense se ha convertido en una herramienta esencial para investigar y prevenir actividades fraudulentas, garantizando la integridad de cada transacción y la confianza de los consumidores. Sin embargo, los métodos de auditoría tradicionales enfrentan limitaciones importantes, especialmente en un entorno digital en constante cambio. Aquí es donde blockchain emerge como una tecnología prometedora, que ofrece soluciones

innovadoras que pueden revolucionar los procesos de auditoría forense al mejorar la ciberseguridad y proteger los datos.

El objetivo general de este estudio es describir el uso del blockchain y la ciberseguridad en las auditorías forenses como un enfoque innovador para la detección de fraudes en empresas de comercio electrónico. A partir de este objetivo, surge la siguiente pregunta de investigación: ¿Cómo puede la implementación de blockchain en las auditorías forenses mejorar la ciberseguridad y la detección de fraudes en las empresas de comercio electrónico? Esta pregunta guía la exploración de cómo blockchain, con sus características únicas, puede superar las limitaciones de los enfoques tradicionales de auditoría y ofrecer un método más eficaz para identificar y prevenir fraudes en el creciente sector del comercio electrónico.

Metodología

Para llevar a cabo este estudio, se realizó una revisión sistemática de la literatura, enfocada en artículos publicados entre 2015 y 2023. Se utilizaron bases de datos académicas como IEEE Xplore, Springer, y Google Scholar, seleccionando estudios que abordaran la aplicación de blockchain en auditoría forense y su impacto en la ciberseguridad dentro del comercio electrónico. Se incluyeron tanto investigaciones empíricas como teóricas para ofrecer una perspectiva integral. La revisión se organizó en tres fases: (1) identificación de estudios relevantes, (2) análisis crítico de los enfoques metodológicos y resultados presentados, y (3) síntesis de hallazgos para evaluar el potencial de blockchain en mejorar los procesos de auditoría forense.

Implementación de Blockchain en Auditoría Forense

La integración de blockchain en auditoría forense se ha posicionado como una innovación que promete mejorar la detección de fraudes en el comercio electrónico. Según Zyskind, Nathan, y Pentland (2015), la naturaleza descentralizada y segura de blockchain proporciona un entorno ideal para almacenar y verificar transacciones de manera confiable. Este enfoque permite a

los auditores forenses acceder a un registro inmutable de todas las transacciones realizadas, lo que reduce la posibilidad de manipulación de datos y facilita la identificación de patrones de fraude.

Investigaciones recientes sugieren que la tecnología blockchain puede transformar las prácticas tradicionales de auditoría forense al proporcionar una capa adicional de seguridad y transparencia (Peters & Panayi, 2016). Esto es especialmente relevante en el contexto del comercio electrónico, donde las transacciones ocurren en tiempo real y a gran escala, lo que dificulta la detección manual de fraudes. Blockchain permite un seguimiento continuo y automático de las transacciones, lo que mejora la eficiencia en la identificación de irregularidades.

Aunque la adopción de blockchain en auditoría forense presenta numerosos beneficios, también es importante considerar las limitaciones y desafíos asociados. Por ejemplo, a pesar de su inmutabilidad, la tecnología blockchain no es completamente infalible. Casos recientes han demostrado que, aunque los datos almacenados en una blockchain son inalterables, la calidad de esos datos depende de la exactitud de la información ingresada en primer lugar (Underwood, 2016). Como, por ejemplo, Provenance, una empresa que utiliza blockchain para rastrear la cadena de suministro de productos alimenticios, ha señalado que la precisión de los datos ingresados es crucial para garantizar la integridad del sistema (Tripoli & Schmidhuber, 2018), lo que puede llevar a problemas graves si en el contexto de una cadena de suministro, un proveedor ingresa datos incorrectos sobre la procedencia o calidad de un producto, como un certificado de origen falso o información errónea sobre las condiciones de almacenamiento, esta información se registrará en la blockchain y se considerará inmutable

O como también puede suceder en el ámbito financiero, si un usuario ingresa información incorrecta al registrar una transacción, como la cantidad de dinero transferido o los datos del receptor, esta información se almacena inmutablemente en la blockchain. Peters & Panay (2016), muestra un claro ejemplo en el uso de blockchain para transferencias internacionales de dinero, donde errores en los datos

ingresados pueden llevar a la pérdida de fondos o a la imposibilidad de rastrear la transacción. Otro ejemplo, que es importante mencionar es, si las criptomonedas o los tokens no fungibles (NFTs), son creados con información incorrecta sobre su origen o autoría, este error se conservará en la cadena, lo que puede generar disputas legales y afectar el valor del activo (Antonopoulos, 2017). Esto plantea la necesidad de mecanismos adicionales para garantizar el flujo de los datos desde el momento en que son ingresados en la cadena.

Además, la implementación de blockchain requiere una infraestructura tecnológica avanzada y personal capacitado, lo que puede representar un obstáculo significativo para las empresas más pequeñas o aquellas que operan en mercados emergentes (Casino, Dasaklis, & Patsakis, 2019). La inversión inicial en tecnología blockchain y la capacitación del personal pueden ser costosos, y la falta de estándares globales puede dificultar la adopción a gran escala.

Enfoques innovadores para la detección de fraudes en empresas de comercio electrónico

La detección de fraudes en el comercio electrónico es un desafío crítico que requiere enfoques avanzados e innovadores. Entre las tecnologías emergentes, el blockchain y sus aplicaciones, como los contratos inteligentes, el Internet de las Cosas (IoT) integrado con blockchain, el monitoreo en tiempo real, la identidad digital descentralizada, la trazabilidad, auditoría, y el análisis predictivo con blockchain, se destacan por su potencial para revolucionar la forma en que se gestionan y previenen los fraudes en este sector.

Tabla 1.

Enfoques innovadores para la detección de fraudes en empresas de comercio electrónico

Enfoque Innovador	Descripción	Ventajas	Desafíos	Referencias
Blockchain	Registro inmutable de transacciones en un sistema descentralizado.	- Inmutabilidad de los datos. - Transparencia y trazabilidad. - Automatización de la verificación de transacciones.	- Alta inversión inicial. - Desafíos en la calidad de los datos ingresados. - Complejidad técnica para las PYMEs.	Nakamoto (2008); Peters & Panayi (2016); Casino et al. (2019)
Contratos Inteligentes	Programas que se ejecutan automáticamente cuando se cumplen condiciones predefinidas, basados en blockchain.	- Automatización de auditorías. - Reducción de intervención manual. - Cumplimiento automático de normas.	- Dificultades en la programación de condiciones complejas. - Riesgo de errores en la codificación.	Chen, Shi & Xu (2019); Tapscott & Tapscott (2016)
Internet de las Cosas (IoT) Integrado con Blockchain	Monitorización en tiempo real de activos y transacciones mediante dispositivos conectados y registrados en blockchain.	- Trazabilidad en tiempo real. - Mayor precisión en la detección de fraudes. - Automatización en la recolección de datos.	- Vulnerabilidad a ataques en dispositivos IoT. - Complejidad en la integración de IoT y blockchain.	Liang, Wang & Wu (2019); Kumar, Vealey & Srivastava (2017)
Monitoreo en Tiempo Real	Implementación de sistemas basados en blockchain para la auditoría continua de transacciones.	- Detección temprana de actividades fraudulentas. - Reducción de tiempos en auditorías.	- Requiere infraestructura avanzada. - Alto volumen de datos a procesar en tiempo real.	Zyskind, Nathan & Pentland (2015); Peters & Panayi (2016)
Identidad Digital Descentralizada	Uso de blockchain para la gestión segura de identidades digitales, asegurando la autenticidad de las transacciones.	- Protección contra el robo de identidad. - Verificación segura de usuarios.	- Desafíos regulatorios y de cumplimiento. - Necesidad de adopción a gran escala.	Yermack (2017); Gatteschi et al. (2018)
Trazabilidad y Auditoría de la Cadena de Suministro	Registro de cada paso en la cadena de suministro en blockchain para asegurar la integridad del producto desde su origen hasta la entrega.	- Transparencia total en la cadena de suministro. - Reducción de fraudes en productos y servicios.	- Complejidad en la implementación a nivel global. - Coordinación entre múltiples actores.	Kshetri (2017); Hamida et al. (2017)
Análisis Predictivo con Blockchain	Uso de algoritmos de aprendizaje automático integrados con blockchain para predecir y detectar posibles fraudes.	- Predicción temprana de fraudes. - Mejora continua mediante el aprendizaje de datos históricos.	- Necesidad de grandes cantidades de datos de alta calidad. - Desafíos en la integración de sistemas.	Glaser (2017); McKenna (2018)

Nota: datos extraídos a partir del análisis de cada lectura.

Se puede observar en la tabla, que la detección de fraudes en el comercio electrónico es un desafío cada vez más complejo, y la adopción de tecnologías avanzadas se ha vuelto esencial para mitigar los riesgos asociados. Frente a ello, se ha destacado por su capacidad para proporcionar un registro inmutable y descentralizado de transacciones, lo que es fundamental para asegurar los datos en un proceso de auditoría. Como señalan Tapscott y Tapscott (2016), la inmutabilidad de blockchain asegura que una vez que la información es registrada, no puede ser alterada, lo que reduce significativamente las posibilidades de manipulación fraudulenta. Sin embargo, por sí sola, esta tecnología no es suficiente para abordar todos los aspectos del fraude en el comercio electrónico, lo que lleva a la integración de otras soluciones, como los contratos inteligentes.

En relación con los contratos inteligentes, estos permiten la automatización de procesos específicos dentro de la infraestructura blockchain. Según Szabo (1997), los contratos inteligentes ejecutan automáticamente acciones predefinidas cuando se cumplen ciertas condiciones, eliminando la necesidad de intervención manual, lo que permite reducir el riesgo de errores por factores humanos. No obstante, como advierten Christidis y Devetsikiotis (2016), los contratos inteligentes presentan desafíos, incluyendo la complejidad en su programación y el riesgo en el código que podrían ser explotados por actores malintencionados. Esta realidad subraya la importancia de la implementación cuidadosa y la revisión exhaustiva del código de los contratos inteligentes antes de su despliegue.

Por otro lado, el Internet de las Cosas (IoT) integrado con blockchain ofrece un enfoque avanzado para la monitorización continua y en tiempo real de activos y transacciones. Según Gubbi et al. (2013), la integración de IoT con blockchain mejora la precisión y trazabilidad de los datos, registrando de manera segura cada movimiento de un producto. Sin embargo, esta integración también introduce nuevos desafíos. Por ejemplo, como señalaron Weber et al. (2016), la vulnerabilidad a los ciberataques a dispositivos IoT y la complejidad de gestionar grandes

volúmenes de datos son aspectos críticos que se deben temer presente con el fin de garantizar la seguridad y eficiencia del sistema.

Mientras tanto, el monitoreo en tiempo real mediante blockchain, aunque no integra IoT, se centra en la auditoría continua de transacciones financieras. Esto permite la detección inmediata de fraudes, una ventaja significativa en entornos dinámicos de comercio electrónico. Según Tschorsch y Scheuermann (2016), la capacidad de blockchain para proporcionar transparencia y trazabilidad en tiempo real es crucial para mejorar la confianza en las transacciones. Sin embargo, como apuntan Yli-Huumo et al. (2016), este enfoque requiere una infraestructura tecnológica avanzada y un alto nivel de procesamiento de datos, lo que puede representar una barrera para su adopción generalizada.

En el ámbito de la seguridad de la identidad, la identidad digital descentralizada emerge como una solución innovadora que utiliza blockchain para gestionar de manera segura las identidades digitales de los usuarios. Este enfoque es especialmente relevante para prevenir fraudes de identidad en plataformas de comercio electrónico. Según Zyskind, Nathan y Pentland (2015), la gestión descentralizada de identidades permite a los usuarios controlar sus datos personales sin depender de intermediarios centralizados, reduciendo el riesgo de robos de identidad. Sin embargo, como señalan Halpin y Piekarska (2017), este enfoque enfrenta desafíos regulatorios y de privacidad, además de requerir una adopción masiva para ser verdaderamente efectivo.

En contraste, la trazabilidad y auditoría de la cadena de suministro mediante blockchain se centra en garantizar la integridad de los productos. Este enfoque no solo ayuda a detectar fraudes relacionados con productos falsificados o de baja calidad, sino que también mejora la transparencia en el proceso de distribución. Según Kshetri (2018), la trazabilidad proporcionada por blockchain es crucial para asegurar la autenticidad de los productos y proteger tanto a los consumidores como a las empresas. Sin embargo, como destacan Tian (2016) y Abeyratne y Monfared (2016), la implementación de esta tecnología a nivel global es compleja y requiere

la coordinación entre múltiples actores, lo que puede ser un obstáculo significativo para su adopción.

De allí que el análisis predictivo con blockchain representa un enfoque innovador que combina algoritmos de aprendizaje automático con la seguridad y transparencia de blockchain para predecir y detectar posibles fraudes antes de que ocurran. Este enfoque es particularmente valioso en entornos donde la prevención proactiva del fraude es crítica. Según Chen, Chiang y Storey (2012), los modelos predictivos son efectivos para identificar patrones de comportamiento que podrían indicar actividades fraudulentas. Sin embargo, la efectividad de estos sistemas depende en gran medida de la calidad y cantidad de datos disponibles, así como de la capacidad para integrar estos sistemas con la infraestructura existente.

Finalmente, cada uno de estos enfoques ofrece ventajas y desafíos únicos, y su aplicabilidad en el comercio electrónico depende de las necesidades específicas de cada empresa. Mientras que el blockchain proporciona una base segura y transparente para la auditoría, es necesario complementarlo con otras tecnologías como los contratos inteligentes o el IoT para maximizar su efectividad. Asimismo, la identidad digital descentralizada y la trazabilidad en la cadena de suministro abordan problemas específicos, pero requieren una adopción amplia y coordinación global para ser efectivas. Por otro lado, el análisis predictivo con blockchain se perfila como el futuro de la prevención de fraudes, aunque su implementación enfrenta desafíos significativos en términos de datos e integración tecnológica. La elección del enfoque más adecuado dependerá de la capacidad de las empresas para integrar y gestionar estas tecnologías de manera eficiente y segura.

Estrategias de implementación de blockchain en las auditorías forenses

La implementación de blockchain en las auditorías forenses ofrece un enfoque transformador para mejorar la ciberseguridad y la detección de fraudes en las empresas de comercio electrónico. Al proporcionar un registro inmutable y descentralizado de todas las transacciones, blockchain reduce significativamente

las oportunidades de manipulación de datos, uno de los principales factores que facilitan el fraude. Según Tapscott y Tapscott (2016), la naturaleza inmutable de blockchain asegura que cualquier intento de alteración sea fácilmente detectable, lo que fortalece los datos almacenados y aumenta la confianza en las auditorías. Esta capacidad es particularmente útil en entornos de comercio electrónico, donde la transacción de grandes volúmenes de datos financieros y personales está expuesta a riesgos continuos de fraude y ciberataques.

Además, la transparencia inherente a blockchain permite un monitoreo en tiempo real de las transacciones, lo que facilita la detección temprana de actividades sospechosas. Como señalan Christidis y Devetsikiotis (2016), la capacidad de blockchain para registrar cada transacción de manera visible y accesible para todas las partes involucradas reduce la posibilidad de que los fraudes pasen desapercibidos. Esta característica es clave en la auditoría forense, ya que permite a los auditores identificar patrones inusuales de comportamiento que podrían indicar fraude. Adicionalmente, la utilización de contratos inteligentes dentro del ecosistema blockchain permite automatizar ciertos aspectos de la auditoría, como la verificación de cumplimiento normativo, lo que minimiza los errores humanos y aumenta la eficiencia del proceso de detección de fraudes (Szabo, 1997).

No obstante, para maximizar el impacto de blockchain en la mejora de la ciberseguridad y la detección de fraudes, es crucial que las empresas de comercio electrónico adopten estrategias complementarias. En primer lugar, deben garantizar la calidad de los datos que se ingresan en la cadena de bloques, ya que, como advierte Underwood (2016), la inmutabilidad de blockchain solo es efectiva si los datos son precisos desde el inicio. Implementar mecanismos de validación robustos antes de registrar la información es una estrategia esencial para preservar los datos.

Otra estrategia clave es la integración de blockchain con tecnologías como el Internet de las Cosas (IoT) y el análisis predictivo. La combinación de IoT con blockchain puede proporcionar una visibilidad sin precedentes, ayudando a detectar anomalías en tiempo real (Gubbi et al., 2013). Asimismo, el uso de análisis predictivo

con datos seguros de blockchain permite identificar patrones que podrían predecir fraudes antes de que ocurran, lo que proporciona una ventaja significativa en la prevención proactiva (Chen et al., 2012).

El análisis permite concluir que la implementación de blockchain en las auditorías forenses puede revolucionar la ciberseguridad y la detección de fraudes en las empresas de comercio electrónico, siempre que se complemente con estrategias que aseguren la calidad de los datos y aprovechen el poder de tecnologías adicionales. Estas medidas, junto con la educación continua y la actualización de las prácticas de auditoría, garantizarán que las empresas no solo reaccionen ante fraudes, sino que también desarrollen una capacidad robusta para prevenirlos.

Análisis de resultados

Los estudios revisados indican que la integración de blockchain en la auditoría forense puede ofrecer una solución eficaz para mejorar la ciberseguridad y la detección de fraudes en el comercio electrónico. La capacidad de esta tecnología para garantizar la integridad y transparencia de las transacciones la convierte en una herramienta valiosa para las empresas que buscan protegerse contra el fraude. Sin embargo, su implementación exitosa depende de una evaluación cuidadosa de los costos y beneficios, así como de la preparación de las organizaciones para adaptarse a esta nueva tecnología.

En el contexto del comercio electrónico, donde las transacciones son frecuentemente objeto de intentos de fraude, blockchain puede actuar como un fuerte disuasivo. Su naturaleza inmutable y la posibilidad de realizar auditorías en tiempo real facilitan la detección temprana de actividades sospechosas, permitiendo una respuesta rápida y efectiva (Kshetri, 2017). Sin embargo, la dependencia exclusiva de blockchain para la seguridad y la detección de fraudes podría ser insuficiente si no se complementa con otros métodos de ciberseguridad.

La revisión de la literatura muestra que la implementación de blockchain en auditoría forense ofrece beneficios significativos en la detección de fraudes. Según Zyskind, Nathan y Pentland (2015), la tecnología blockchain permite almacenar y verificar transacciones de manera descentralizada, lo que garantiza la inmutabilidad de los datos y reduce el riesgo de manipulación. Esto es especialmente relevante en el contexto del comercio electrónico, donde la integridad de las transacciones es fundamental para la confianza del consumidor.

Otro estudio realizado por Peters y Panayi (2016) destaca cómo blockchain puede mejorar la eficiencia de las auditorías forenses al permitir el monitoreo continuo de aquellas transacciones en tiempo real, lo que facilita la detección temprana de patrones sospechosos, lo que a su vez permite una respuesta más rápida y efectiva ante posibles fraudes. Además, Casino, Dasaklis y Patsakis (2019) señalan que blockchain puede reducir los costos asociados con la auditoría forense al automatizar ciertos procesos, como la verificación de datos y la creación de registros contables seguros.

Bajo este contexto, los resultados de la investigación sobre la implementación de blockchain y ciberseguridad en auditorías forenses para la detección de fraudes en empresas de comercio electrónico pueden desglosarse en varios hallazgos clave, basados en el análisis y comparación de tecnologías emergentes y su impacto en la detección y prevención del fraude.

Primero, se confirma que la implementación de blockchain en auditorías forenses mejora significativamente la integridad de los datos y la transparencia en las transacciones. Debido a su característica de inmutabilidad, blockchain ofrece un registro inviolable que reduce drásticamente las oportunidades de manipulación de datos, lo que refuerza la confianza en los procesos de auditoría. Este resultado es consistente con investigaciones anteriores que destacan la capacidad de blockchain para asegurar la integridad de las transacciones en entornos digitales (Tapscott & Tapscott, 2016).

Segundo, se identifica que la automatización mediante contratos inteligentes facilita la auditoría en tiempo real y reduce los errores humanos. Los contratos inteligentes permiten la ejecución automática de verificaciones y acciones predeterminadas, lo que optimiza la eficiencia de las auditorías forenses y minimiza los riesgos asociados a la intervención manual. Sin embargo, también se destaca la necesidad de implementar revisiones exhaustivas del código de los contratos inteligentes para evitar vulnerabilidades, como se menciona en la literatura existente (Christidis & Devetsikiotis, 2016).

Otro resultado clave es que la integración de IoT con blockchain ofrece un enfoque avanzado para la monitorización continua y la trazabilidad en tiempo real, lo que permite detectar anomalías en etapas tempranas, mejorando la capacidad de las empresas para responder rápidamente a posibles fraudes. No obstante, se señala que la implementación exitosa de esta tecnología depende de superar desafíos relacionados con la seguridad de los dispositivos IoT y la gestión de grandes volúmenes de datos (Gubbi et al., 2013; Weber et al., 2016).

En cuanto a la identidad digital descentralizada, se encuentra que esta tecnología ofrece una solución efectiva para prevenir fraudes de identidad, un problema común en el comercio electrónico, en este caso, proporcionar a los usuarios controles más fuertes sobre sus datos personales, lo que se denomina identidad digital descentralizada, la cual minimiza el riesgo de robo de identidad. Sin embargo, se identifican desafíos regulatorios y la necesidad de una adopción masiva para que esta tecnología sea realmente efectiva (Zyskind, Nathan & Pentland, 2015).

Por último, la utilización del análisis predictivo en conjunto con blockchain demuestra ser una estrategia prometedora para la prevención proactiva del fraude. El análisis predictivo, al identificar patrones sospechosos antes de que ocurra el fraude, proporciona a las empresas una ventaja significativa en la protección contra actividades fraudulentas. Este hallazgo subraya la importancia de la calidad de los

datos y la integración de tecnologías avanzadas para maximizar la efectividad de las estrategias de prevención (Chen, Chiang & Storey, 2012).

En conjunto, estos resultados sugieren que la implementación de blockchain en auditorías forenses, complementada con tecnologías como los contratos inteligentes, IoT y análisis predictivo, puede transformar la capacidad de las empresas de comercio electrónico para detectar y prevenir fraudes, siempre que se aborden adecuadamente los desafíos técnicos y regulatorios asociados.

Sin embargo, la revisión también revela desafíos significativos. Underwood (2016) advierte que, aunque los datos en una blockchain son inalterables, la precisión de estos depende de la calidad de la información ingresada originalmente. Esto sugiere que, aunque blockchain puede mejorar la seguridad de los datos, no elimina la necesidad de controles rigurosos en la etapa de entrada de datos. Además, la adopción de blockchain requiere una inversión considerable en infraestructura tecnológica y capacitación, lo que podría ser una barrera para su implementación en pequeñas y medianas empresas.

Conclusiones

La investigación sobre la implementación de blockchain en la auditoría forense dentro del comercio electrónico muestra un potencial significativo para mejorar la detección de fraudes y fortalecer la ciberseguridad. Si bien los beneficios de esta tecnología son evidentes, también es necesario considerar sus limitaciones y los desafíos que representa su adopción. Para que blockchain se convierta en una herramienta estándar en la auditoría forense, las empresas deben evaluar su capacidad para integrarla de manera efectiva, tomando en consideración los costos y la infraestructura requerida. A medida que la tecnología continúa evolucionando, es probable que veamos un aumento en su adopción, lo que podría transformar radicalmente la manera en que se realizan las auditorías forenses en el comercio electrónico.

…

La implementación de blockchain en auditoría forense dentro del comercio electrónico presenta un potencial considerable para mejorar la detección de fraudes y fortalecer la ciberseguridad. Los estudios revisados sugieren que esta tecnología puede ofrecer una solución robusta y eficiente para almacenar y verificar transacciones, garantizando la estabilidad de los datos. Sin embargo, para que blockchain sea efectivamente adoptado en la auditoría forense, es crucial que las organizaciones evalúen cuidadosamente los costos y beneficios, así como la preparación de su infraestructura y personal.

A pesar de los desafíos identificados, la tendencia hacia la digitalización y la creciente amenaza de fraudes en el comercio electrónico hacen que la integración de blockchain sea una opción atractiva. Es probable que, con el tiempo, esta tecnología evolucione y se adapte a las necesidades específicas del comercio electrónico, lo que podría llevar a una adopción más amplia y efectiva en el campo de la auditoría forense.

Referencias

Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, *5*(9), 1-10. https://ijret.org/volumes/2016v05/i09/IJRET20160509001.pdf

Amengual, J. (). Fundamentos del Blockchain. To the Moon. https://www.studocu.com/co/document/universidad-externado-de-colombia/economia-colombiana/libro-fundamentos-blockchain-joan-amengual/21975084

Batres, M.; Sánchez, C.; Santana, J. (2022). Procedimientos de auditoría forense aplicables a la investigación de fraudes electrónicos enfocado en cuentas bancarias e inversiones. Trabajo de grado de Especialización en: Auditoría Forense. https://ri.ues.edu.sv/id/eprint/30442/1/PROCEDIMIENTOS%20DE%20AUDITOR%C3%8DA%20FORENSE%20APLICABLES%20A%20LA%20INVESTIGACI%C3%93N%20DE%20FRAUDES%20ELECTR%C3%93NICOS%20ENFOCADO%20EN%20CUENTAS%20BANCARIAS%20E%20I.pdf

Caamaño Fernández, E.E., y Gil Herrera, R.J. (2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional, NOVUM, 1(10), 61 - 80. Recuperado de: file:///C:/Users/elifa/Downloads/dirnovum,+4_Cybersecurity+risk+prevention.pdf

Carballo, I.; Garnero, P.; Chomczyk, A.; Henao, J. (2021). Expansión de Herramientas Financieras digitales para impulsar el Comercio Electrónico de las MiPyMEs de América Latina. Banco Interamericano de Desarrollo.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55-81. https://doi.org/10.1016/j.tele.2018.11.006

Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly*, *36*(4), 1165-1188. https://www.jstor.org/stable/i40080007

Chen, Y., Shi, Y., & Xu, H. (2019). A Blockchain-Based Framework for Auditing Internet of Things Data. *International Journal of Information Management*, 49, 200-209. https://doi.org/10.1016/j.ijinfomgt.2019.03.005

Chin, K. (2024). El papel de la ciberseguridad en la tecnología Blockchain. UpGuard,Inc.https://www.upguard.com/blog/the-role-of-cybersecurity-in-blockchain-technology

Chomczyk, A. (2020). Regulación de blockchain e identidad digital en América Latina. El futuro de la identidad digital. Banco Interamericano de Desarrollo.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292-2303 Doi: 10.1109/ACCESS.2016.2566339

Finck, M. (2018). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? *European Law Journal*, 24(1), 1-21. https://doi.org/10.1111/eulj.12272

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet, 10*(2), 20. https://doi.org/10.3390/fi10020020

Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis. *50th Hawaii International Conference on System Sciences (HICSS)*, 1543-1552. https://doi.org/10.24251/HICSS.2017.186

González, S. (2021). *Creación y despliegue de arquitecturas híbridas para la mejora de la ciberseguridad en sistemas de control industrial en infraestructuras críticas*. Programa Doctorado en Ingeniería de Sistemas y Control. Escuela Internacional de Doctorado. http://e-spacio.uned.es/fez/eserv/tesisuned:ED-Pg-IngSisCon-Sgonzalez/GONZALEZ_GONZALEZ_Santiago_Tesis.pdf

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

Halpin, H., & Piekarska, M. (2017). Introduction to Security and Privacy on the Blockchain. *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 1-3. https://inria.hal.science/hal-01673293/document

Hamida, E. B., Brousmiche, K. L., Levard, H., & Thea, E. (2017). Blockchain for enterprise: Overview, opportunities and challenges. *In IEEE International Conference on Collaboration and Internet Computing (CIC)* (pp. 9-15). IEEE. https://doi.org/10.1109/CIC.2017.00009

Hermann, J. (2024). IoT powered by Blockchain. How Blockchains facilitate the application of digital twins in IoT. Deloitte. Disponible en: https://www2.deloitte.com/de/de/pages/innovation/contents/iot-powered-by-blockchain.html

Jehl, L. (2018) Blockchain Security: A Primer: Disponible en: https://www.law.berkeley.edu/wp-content/uploads/2018/08/Blockchain-Primer-Bloomberg-Law.pdf

Kshetri, N. (2017). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

KPMG Advisory Services Ltda.(2011). Encuesta de Fraude en Colombia 2011. Recuperado de: http://www.kpmg.com/co/es/issuesandinsights/articlespublications/paginas/encuestadefraudeencolombia2011.aspx

Kumar, N., Vealey, T., & Srivastava, H. (2017). Security in internet of things: Challenges, solutions, and future directions. *Proceedings of the 49th Annual Southeast Regional Conference*, 42-47. https://doi.org/10.1145/3077286.3077294

Liang, X., Wang, J., & Wu, G. (2019). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. *Future Generation Computer Systems, 99*, 617-624. https://doi.org/10.1016/j.future.2019.04.034

Marín Hernández, G. y Gómez Lara, I. (2022). La ciberseguridad: Un estudio comparado. Centro de Estudios de Derecho e Investigaciones Parlamentarias-(CEDIP).https://www.nodal.am/wp-content/uploads/2023/06/cibersegu.pdf

Meegan, X. (2020). *Identifying Key Non-Financial Risks in Decentralised Finance on Ethereum Blockchain*. MIP Politecnico di Milano

McKenna, B. (2018). The blockchain disruption: Financial institutions and the search for new business models. *Journal of Digital Banking, 3*(2), 101-111.

Pervez, H.; Muneeb, M.; Irfan, M.; Haq, I. (2018). A Comparative Analysis of DAG-Based Blockchain Architectures. *12th International Conference on Open Source Systems and Technologies (ICOSST)*. Lahore, Pakistan, 2018, pp. 27-34, doi: 10.1109/ICOSST.2018.8632193

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. *Banking Beyond Banks and Money* (pp. 239-278). Springer. https://doi.org/10.1007/978-3-319-42448-4_13

Preukschat, A.; Kuchkovsky, C.; Gómez, G.; Díez, D.; Molero, I. (2017). *Blockchain: la revolución industrial de internet*. Centro Libros PAPF, S.L.U. España.

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin Random House.

Tian, F. (2016). Un sistema de trazabilidad de la cadena de suministro agroalimentario para China basado en tecnología RFID y blockchain. *13th International Conference on Service Systems and Service Management (ICSSSM)*, 1-6. doi: 10.1109/ICSSSM.2016.7538424

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin y más allá: una encuesta técnica sobre monedas digitales descentralizadas. *IEEE Communications Surveys & Tutorials*, *18*(3), 2084-2123. https://doi.org/10.1109/COMST.2016.2535718

Tripoli, M., & Schmidhuber, J. (2018). Oportunidades emergentes para la aplicación de Blockchain en la industria agroalimentaria. *Food and Agriculture Organization of the United Nations (FAO)*. Recuperado de: https://openknowledge.fao.org/handle/20.500.14283/ca9934en

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, 59(11), 15-17. https://doi.org/10.1145/2994581

Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., & Mendling, J. (2016). Untrusted Business Process Monitoring and Execution Using Blockchain. *International Conference on Business Process Management (BPM 2016)*, 329-347.

http://www.imweber.de/downloads/UntrustedBusinessProcessMonitoringAndExecutionUsingBlockchain--BPM2016--authors_copy.pdf

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance, 21*(1), 7-31. https://doi.org/10.1093/rof/rfw074

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. *PloS one*, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Zyskind, G., Nathan, O., & Pentland, A. (2015). Descentralizar la privacidad: usar blockchain para proteger los datos personales. *IEEE Security and Privacy Workshops* (pp. 180-184). IEEE. https://doi.org/10.1109/SPW.2015.27