**Tema:** Diseño de un modelo basado en smart contracts para mitigar el riesgo de estafas por compras realizadas en MarketPlaces.

**Introducción**

Cuando se menciona la palabra contrato, lo primero en que se piensa es en un papel escrito donde se establecen ciertas condiciones que, al ser leídas y aceptadas por las partes implicadas, los firman y se comprometen a cumplir con dichas condiciones [1]. Actualmente, aunque este proceso sigue siendo utilizado en aspectos legales en todo el mundo, se ha dado un importante avance en cuanto a la automatización, seguridad y garantías con respecto a los contratos físicos tradicionales debido al surgimiento de los Smart Contracts (SM) o contratos inteligentes [2] que se llevan desarrollando desde 1997 gracias al criptógrafo Nick Szabo quién acuñó el término SM por primera vez, pero debido a las limitaciones tecnológicas de la época no fue factible su idea de desarrollar un sistema de pagos que llevase el concepto de los contratos tradicionales a lo digital [3], pero esta situación se convirtió en viable con la creación del bitcoin en el año 2009 [4].

No obstante, lo interesante radica en lo que está detrás de la creación del bitcoin, la tecnología blockchain, estas hacen posible que la utilización de los SM sea viable, debido a que en el año 2014 con la creación de Ethereum (“plataforma open source, que sirve para programar contratos inteligentes” [5]) los SM funcionan en un sistema descentralizado que no puede ser manipulado por ninguna de las partes implicadas en el contrato ni por organismos externos, el contrato se cumple por condiciones programadas, firmadas por las partes implicadas y enviada a una cadena de bloques donde se asegura inmutabilidad e indelebilidad.

En el campo del ecommerce siendo más específico, en los marketplace donde múltiples negocios ofertan sus productos, han ocurrido problemas de estafas, especialmente en el año 2020 por la aparición del COVID-19 en donde creció la cantidad de microempresas que se volcaron a la venta online y a su vez aumentó la demanda de los clientes y la ciberdelincuencia. A nivel internacional, distintos organismos emitieron alertas a lo largo del 2020 acerca del incremento de estafas en compras online [6] evidenciando claras falencias de los entes reguladores de estos marketplaces que no cuentan con mecanismos confiables y seguro para hacer seguimiento a estos procesos.

Con el blockchain, cualquier gestión de transacciones realizadas bajo esta tecnología se puede certificar su autenticidad debido a que son públicas, seguras e inmutables [7] y al ser aplicada con SM en un sistema ecommerce, éste aportaría a la solución de la problemática mencionada, para este caso particular, mitigar el riesgo de estafas por compras realizadas en marketplaces debido a que una vez realizada una compra, esta información sea procesada en un ambiente descentralizada y abierta donde no exista la intervención de terceros y todo el flujo que implica este proceso de compra-venta se lleve a cabo con normalidad hasta que se cumpla el contrato establecido entre las partes interesadas.

Esta investigación pretende incorporar el concepto de contratos físicos a lo digital, demostrando mejoras como mayor seguridad, confiabilidad, menor coste-tiempo y evitar fraudes o estafas por compras realizadas en marketplaces.

El presente documento se encuentra dividido

**Formulación del problema.**

¿Cómo un modelo basado en smart contracts mitigaría el riesgo de estafas por compras realizadas en MarketPlaces?

**Hipótesis**

Es posible mitigar las estafas por compras realizadas en marketplaces a través de soluciones disruptivas utilizando Smart Contracts apoyados en la tecnología blockchain.

**Objetivo General.**

Diseñar e implementar un modelo que mitigue el riesgo de estafas por compras realizadas en MarketPlaces a través del uso de smarts contracts basados en blockchain.

**Objetivos específicos.**

* Diagnosticar los procesos de compras realizadas por los marketplaces más populares actualmente.
* Evaluar las tecnologías blockchain enfocadas en el diseño de contratos inteligentes.
* Proponer un modelo de solución para mitigar estafas en marketplaces por medio del uso de contratos inteligentes soportado en la tecnología Blockchain seleccionada.

# Bibliografía

|  |  |
| --- | --- |
| [1] | U. M. Stefano DellaVigna, «Contract Design and Self-Control: Theory and Evidence,» *The Quarterly Journal of Economics,* vol. 2, nº 2, p. 353–402, 2004. |
| [2] | L. Hang y D.-H. Kim, «Optimal Blockchain Network Construction Methodology Based on Analysis of Configurable Components for Enhancing Hyperledger Fabric Performance,» *Blockchain: Research and Applications,* 2021. |
| [3] | N. Szabo, «Formalizing and Securing Relationships on Public Networks,» *First Monday. Peer Reviewed Journal on the Internet,* vol. 2, nº 9, 1997. |
| [4] | M. Rahouti, K. Xiong y N. Ghani, «Bitcoin Concepts, Threats, and Machine-Learning Security Solutions,» *IEEE Access,* vol. 6, pp. 67189-67205, 2018. |
| [5] | W. Chen, Z. Zheng, E. C.-H. Ngai, P. Zheng y Y. Zhou, «Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum,» *IEEE Access,* vol. 7, pp. 37575-37586, 2019. |
| [6] | J. M. Harán, «We Live Security - ESET,» 25 11 2020. [En línea]. Available: https://www.welivesecurity.com/la-es/2020/11/25/crece-ecommerce-aumentan-estafas-incidentes-seguridad/. [Último acceso: 03 04 2021]. |
| [7] | S. N. G. Gourisetti, M. Mylrea y H. Patangia, «Evaluation and Demonstration of Blockchain Applicability Framework,» *IEEE Transactions on Engineering Management,* vol. 67, nº 4, pp. 1142-1156, 2020. |