E

n el documento [*Smart Contracts Vulnerability Auditing With Multi-Semantics*](https://ieeexplore.ieee.org/document/9202747)*,* se expresa que “*Due to the unfamiliarity with the smart contract development and its peculiar operation mechanism, a lot of security risks in capital management and trading continuously come out*”.

Aunque esta problemática de inseguridad en los medios virtuales ha existido desde un largo periodo, esta se ha logrado mitigar a través de sistemas que permiten la protección de los datos personales, logrando que estos sean cada vez más seguros y de difícil acceso a terceros, por medio de su encriptación a través de los *tokens*. Debido a que cada día se puede garantizar un mejor tratamiento de los datos personales se ha normalizado la realización de ciertas actividades por medios digitales, dejando poco a poco las transacciones presenciales.

Por lo tanto y con el fin de seguirle el paso a estos avances de seguridad en la información, en materia de auditoria se ha desarrollado un modelo mejorado llamado *Multi-Sematic gram (MSgram)* programado a través de *Etherum*; este modelo permite apoyar la auditoria de los contratos inteligentes a partir de los estándares de *tokenización*, detectando las vulnerabilidades de la información con un alto índice de precisión del 44%, al analizar este porcentaje es necesario tener en cuenta que este modelo fue aplicable a sistemas de información que manejan un alto flujo de transacciones comerciales a nivel mundial.

La gran diferencia que radica entre este modelo y los demás es que en el modelo *MSgram* se implementan tres secuencias multisemánticas, lo cual permite una mejor captación de la información y de esta manera generar resultados auditados por separado, posteriormente, estos resultados se integran obteniendo un resultado auditado final, el cual es más acertado, debido a que abarca información más detallada y con un menor sesgo.

Es necesario tener en cuenta que la implementación de estos modelos ha permitido mantener la economía digital como la conocemos actualmente. Aunque aún existen varios aspectos de vulnerabilidad en los contratos inteligentes que requieren ser abarcados, estos procesos de infraestructura de confianza y fidelización se han ido desarrollando con el fin de mitigar robo de información, evitar ataques de terceros malintencionados y pérdidas significativas.

De acuerdo con la información expresada anteriormente, se puede afirmar que la implementación de nuevos modelos precisos y detallados son necesarios en esta era digital, debido a que aumentan la confianza y seguridad en las transacciones digitales; sin embargo, estas aún requieren un aumento en su índice de precisión y una mayor implementación en los contratos inteligentes.

*Laura Valentina Triana Gómez*