Arquitectura para la verificabilidad criptográfica de eventos basada en blockchain

Jaime Fernando; Lodato Marcos; Hernandez Mario Alejandro

{marcos.lodato; fernando.jaime}@alumnos.uai.edu.ar {alejandromario.hernandez}@uai.edu.ar

Centro de Altos Estudios en Tecnología Informática (CAETI) - Universidad Abierta Interamericana (UAI)

❑ RESÚMEN

Esta investigación se centra en la problemática de la falta de garantías verificables en la ejecución de procesos computacionales dentro de sistemas distribuidos modernos. Su objetivo es proponer una arquitectura que incorpore mecanismos criptográficos y tecnología blockchain como capa de verificación externa, superando las limitaciones de los modelos tradicionales de auditoría. Para ello, se estudian los fundamentos de la Arquitectura Basada en Eventos (EDA) y el patrón Event Sourcing como modelos para representar procesos mediante eventos inmutables. Asimismo, se analizan técnicas criptográficas como funciones hash y estructuras de agregación tipo Merkle Tree, que permiten construir pruebas de integridad verificables sobre conjuntos de eventos.

El objetivo principal es definir una arquitectura que transforma eventos operativos en evidencias criptográficas auditables, habilitando la detección de alteraciones, la verificación independiente y la trazabilidad histórica sin exposición de datos sensibles. Se espera que esta propuesta contribuya al desarrollo de sistemas distribuidos con mayores garantías de integridad, confianza y transparencia.

❑ INTRODUCCIÓN

En la actualidad, los sistemas informáticos distribuidos han evolucionado significativamente gracias a paradigmas como la computación en la nube, los microservicios y las arquitecturas orientadas a eventos. Estos enfoques permiten construir soluciones altamente escalables, desacopladas y resilientes. Sin embargo, esta evolución también ha introducido nuevos desafíos relacionados con la integridad, trazabilidad y verificabilidad de los procesos computacionales.

Los mecanismos tradicionales de auditoría, basados en logs centralizados o bases de datos transaccionales, presentan limitaciones importantes, ya que dependen del mismo dominio que genera y almacena la información. Esto implica riesgos asociados a la manipulación de datos, falta de transparencia y ausencia de garantías independientes sobre la integridad histórica de los eventos.

En este contexto, resulta fundamental incorporar mecanismos que permitan validar la información de forma confiable y descentralizada. La tecnología blockchain, junto con el uso de funciones hash y estructuras criptográficas como los árboles de Merkle, surge como una alternativa capaz de proporcionar inmutabilidad, sellado temporal y verificación independiente

La presente investigación se enfoca en analizar estos conceptos y proponer una arquitectura que permita fortalecer la auditoría de procesos distribuidos, contribuyendo al desarrollo de sistemas más confiables y verificables.

❑ CONTEXTO

Este proyecto pertenece al área Ingeniería de Software una de las tres áreas principales del CAETI "Centro de Altos Estudios en Tecnología Informática". La institución encargada de coordinar y brindar herramientas en nuestra investigación es la Universidad Abierta Interamericana.

❑ LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

La arquitectura propuesta en esta investigación busca resolver las limitaciones de integridad y verificabilidad mediante un desacople radical de confianza entre el dominio operativo y la capa de verificación externa. Se organiza en tres dominios lógicos:

- **Dominio operativo:** tipo de dominio off-chain donde se generan y persisten los eventos completos según patrones EDA y Event Sourcing.
- **Dominio de evidencia:** encargado de transformar cada evento en una huella criptográfica verificable mediante serialización estricta (orden de campos, normalización y codificación).
- **Dominio persistencia inmutable:** almacena los compromisos criptográficos generados en Sepolia a través de un Smart contract.

Para la escalabilidad y optimización de costos de la arquitectura, se implementa modelo de **persistencia dual** y agregación por **Merkle Trees:** los hashes individuales de cada evento de un lote específico se convierten en nodos hoja; se combinan por pares de forma recursiva hasta obtener una única **Merkle Root**, que es anclada en la blockchain junto con un identificador único de lote. Solo esta raíz es la que se encuentra on-chain, preservando la privacidad y reduciendo el costo de las comisiones.

Cualquier auditor externo puede verificar independientemente un evento: serializando los datos de este, calcula su hash, reconstruye el Merkle Tree off-chain y compara el resultado con la registrada en la blockchain.

❑ RESULTADOS ESPERADOS

Se espera que esta investigación ofrezca una arquitectura práctica y las herramientas criptográficas necesarias para reforzar la verificabilidad, integridad y trazabilidad de eventos en sistemas distribuidos, aumentando la confianza y el cumplimiento normativo en procesos computacionales. Se busca aumentar el interés en el uso de la blockchain como capa de auditoría independiente y descentralizada.

❑ FORMACIÓN DE RECURSOS HUMANOS

El equipo de trabajo está compuesto por un profesor y dos estudiantes de quinto año de la carrera de Ingeniería en Sistemas Informáticos de la UAI. El objetivo principal del equipo es aplicar la arquitectura a sistemas que requieran garantías formales de integridad y trazabilidad.