RESUMEN

Este Trabajo de Fin de Máster describe el desarrollo e implementación de una cadena de custodia para pruebas digitales apoyándose en la tecnología blockchain.

El sistema desarrollado tiene tres componentes o subsistemas principales. Por un lado, tenemos una cadena de bloques basada en permisos (distinta de las blockchains públicas como Bitcoin o Ethereum, que no requieren permisos) en la cual se ejecuta un contrato inteligente que permite añadir los hashes de nuevas pruebas digitales a la cadena. De esta forma se puede comprobar en un futuro si las evidencias han sido o no modificadas. Para implementar la blockchain basada en permisos se ha utilizado el framework Hyperledger Fabric y para definir el contrato inteligente la herramienta Hyperledger Composer.

Por otro lado, existe un repositorio de ficheros en el que se almacenan copias de estas pruebas.

Por último, se ha desarrollado una aplicación web en Angular que permite a las distintas entidades involucradas en el proceso de la cadena de custodia intervenir en el mismo. A través de unas credenciales, cada uno de los usuarios de la aplicación web podrá visualizar un listado de casos en los que participa. Cada uno de estos casos tiene una serie de pruebas que las partes implicadas (si tienen los permisos necesarios) se van intercambiando. Todo este proceso de intercambio de evidencias se registra en la blockchain basada en permisos.

Palabras clave

Cadena de custodia, blockchain, prueba, trusted timestamping, permisos, Hyperledger, contrato inteligente, Business Network, repositorio de ficheros, aplicación web, Angular, Firebase.