Ing. Carlos Ormella Meyer y Asoc.
Gestión y Auditoría de Riesgos y Seguridad de la Información
Tel: +54-11-3979-7220 – Cel: (+54-911) 6513-2751
E-mail: ingcomyasoc@gmail.com

BLOCKCHAIN MAS ALLA DE LAS CRIPTOMONEDAS

Una Introducción

© *Ing. Carlos Ormella Meyer* (*).

Blockchain es un sistema digitalizado y descentralizado bajo la forma de una cadena ordenada de bloques de todos los *Mensajes* que se intercambien, y que puede asimilarse a un **Registro Maestro** que se copia y actualiza en todas las entidades intervinientes, eliminando así un punto único de falla.

Dos son los sistemas más usuales de **Blockchain**: Público, que es el sistema típico que maneja criptomonedas, y Privado que típicamente incorpora una persona responsable a cargo del sistema

Una variante de un Blockchain Privado es el Blockchain de Consorcio que es propio de asociaciones de empresas o instituciones con intereses comunes.

El análisis del funcionamiento del Blockchain puede considerarse en dos partes. La primera se refiere al tratamiento por el cual cada mensaje emitido se firma digitalmente, mientras que la segunda concierne a la estructura y formación de bloques.

La **Firma Digital** usa el sistema de dos claves, una Privada para encriptar y otra Pública para desencriptar, lo que permite establecer en destino la **autenticidad** del remitente.

Además, se aplica una función ***hash*** que produce un ***extracto*** o **Hash** del mensaje que, de nuevo en destino, se usa para verificar la **integridad** del mensaje, con lo que el **Blockchain** adquiere la característica de ***inmutabilidad*****,** es decir que un bloque no puede ser ni modificado ni eliminado.

La Clave Pública de un usuario está respaldada por un **Certificado Digital** emitido por una **CA** (***Autoridad de Certificación***) previa recolección y verificación de datos. La **CA** es parte del **PKI** (***Infraestructura de Claves Públicas***) que maneja los servicios propios de los Certificados Digitales.

Cada bloque se identifica por un **Hash** con el cual se encadenará el bloque siguiente. Además, incorpora la fecha y hora del mensaje de modo que el ordenamiento de los bloques permite la ***trazabilidad*** de las operaciones.

Hay varias soluciones para Blockchain Privados como las que siguen:
- Un Sistema básico asocia un Certificado con la máquina correspondiente.
- Otro enfoque responde a un Sistema de PKI Interno que emula un sistema PKI clásico.
- Y finalmente un Sistema Integrado con PKI estándar puede trabajar con certificados emitidos por las CAs tradicionales y también con las CAs creadas internamente en el Blockchain.

Blockchain permite establecer **Contratos Inteligentes** (Smart Contracts) en una aplicación, de modo tal que al cumplirse una condición pre-programada, se ejecuta la cláusula contractual correspondiente

Las aplicaciones actuales de Blockchain son múltiples. Incluso, la característica inherente del Blockchain en cuanto a **Privacidad y Seguridad** lo hace adecuado para aplicaciones de **Ciberseguridad**.

* Ing. Carlos Ormella Meyer. Cursos y Soporte Digital - Asesoramiento - @meyerormella

Hecho el depósito en custodia bajo la Ley Nro. 11.723