¿Qué es la tecnología blockchain?

La tecnología blockchain es una tecnología mayormente empleada en el ámbito de la criptografía, y más específicamente en las criptomonedas. Sin embargo, esta tecnología tiene un gran potencial como medida de seguridad, debido a sus funciones intrínsecas.

Primero que nada, la tecnología blockchain se basa en un conocimiento público de todas las transacciones que por ella ocurren. Debido a que cada transacción debe ser validada por la mayoría (51%) de los operadores de la red, está dotada de una característica de inmutabilidad o resistencia a la manipulación. Esto quiere decir que cualquier persona que intente modificar los registros de la red, no será capaz de hacerlo, debido a que una sola persona no puede obtener la mayoría del consenso en una red compuesta por miles o millones de ordenadores.

No solo eso, sino que el concepto básico de bloque (block) en esta tecnología, se basa en que para resolver cada operación matemática en la red (o algoritmo), se debe utilizar el resultado de la operación inmediatamente anterior. Por ende, modificar el resultado de un bloque anterior generaría una caída en cadena, rompiendo así todas las funciones siguientes. Esta es otra razón por la cual la cadena rechazaría los bloques modificados.

Finalmente, esta tecnología muchas veces se utiliza para asegurar la anonimidad de los que operan, debido a que todos los datos que se envíen por esta cadena están relacionados solamente a una dirección criptográfica (mayormente usadas en criptomonedas), y no a una identidad real. Esto es, obviamente, un arma de doble filo, pues también asegura la anonimidad de los delincuentes.

Sin embargo, estas tres características hacen de la tecnología blockchain una tecnología robusta para ser utilizada como método de seguridad, a pesar de sus fallas o de su inmadurez todavía.

El mayor uso que se le da, hoy en día, es la transferencia de activos, más conocidos como criptomonedas. Debido a la forma en la que los datos no pueden modificarse, la gente envía criptomonedas sin miedo a perderlas, y debido también a la rápida velocidad de estas redes, puede recibir sus activos al instante. Hoy en día, debido a la aceptación cada vez creciente de las criptomonedas como activos financieros, incluso los bancos están empezando a adoptar tecnologías blockchain, para hacerse transferencias entre ellos de manera segura, puesto que pueden generar sus propias redes blockchain por las cuales enviarse sus activos, sin intervenir en las redes principales (aunque nada les impide hacerlo mediante las redes principales tampoco).

Además, la tecnología DLT (Distributed Ledger Technology) que permite que todos los participantes de la red tengan acceso a los mismos datos, en este caso el ledger, o libro contable de las transacciones, y que cada persona tenga su propia copia (ergo todos funcionan como un backup de todos), le da una gran transparencia a las transacciones y a los movimientos del dinero o activos, asegurando así que nada se pierda, y que si hay movimientos sospechosos, o ilegales, puedan ser detectados rápidamente por todos los participantes de la red, no solo por la persona que sea dueña de la cuenta, algo que en el pasado ha demostrado ser una efectiva medida de seguridad.