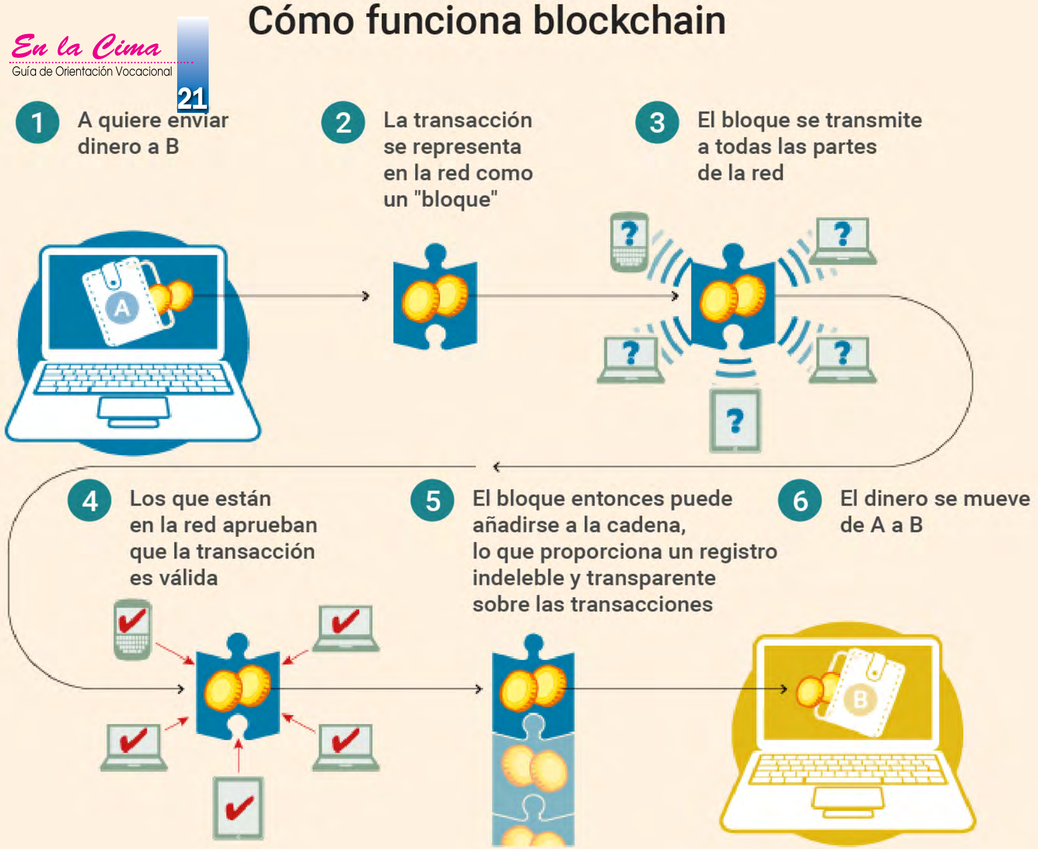

Fuente: FT

Tecnologías digitales distribuidas para la transferencia de valor y la trazabilidad

Imagine que va caminando por la calle y, de repente, un suricato volador con apetito insaciable aterriza en una plaza llena de gente, se come los helados de todos los niños que hay en ella, luego suelta dos chillidos ingentes y se va de la misma forma que ha venido.

Atónitos aún por el inusual hecho y, sin un segundo que perder, se les coloca un detector de mentiras a todos los que han sido testigos del increíble evento y se registra exactamente qué es lo que han visto.

Todos cuentan la misma historia con idénticos detalles. ¡El suricato volador emerge de la nada y consuma el singular hecho!

¿Qué tiene que ver esto con *Blockchain* (*cadenas de bloques*)? Pues bien, vamos a analizar esta analogía para descubrir la verdad detrás de este misterio.

Volvamos a la analogía. Imaginen a los incrédulos testigos del hecho poniéndose de acuerdo para explicar lo que han visto; no es posible decir otra realidad que la que han presenciado

Así sucede en las cadenas de bloques, cada testigo en ese escenario digital es conocido como un **nodo**; son individuos geográfica y computacionalmente aislados los unos de los otros. Así como era independiente cada testigo que estuvo en la escena del Suricato Volador. Cada nodo ha sido testigo presencial de un evento único del cual con total certeza pueden dar fe.

Al detector de mentiras, le enseñan una "prueba de trabajo" (***proof of work***), que es un proceso criptográfico que demuestra que un miembro de la cadena (**nodo**), y no otro, ha resuelto un problema de forma correcta. ¿Me siguen? Repito, cada nodo fue testigo de que un suricato volador arrasó con todos los helados. ¡No hay duda de que fue ese suricato!

Ahora imaginen que cada estado del evento atestiguado pudiera estar registrado en la memoria de los cientos o miles de personas, a las que llamaremos nodos (*computadoras*), con la seguridad de que nadie puede modificar o borrar, a escondidas, el hecho. Eso sí, si legítimamente se debe alterar algo, en cuestión de segundos, todos los nodos se sincronizan y llegan a la misma verdad inalterable. Una especie de memoria colectiva que certifica un hecho inequívocamente, y en total acuerdo.

Es decir, si algún nodo quisiera alterar la verdad, los demás miembros lo desmentirían, manteniendo íntegro el registro del evento.

Pues bien, esa memoria colectiva es una *Cadena de bloques* (*Blockchain*): un registro inmutable y permanente que mantiene la verdad absoluta a través del consenso de los nodos. Más a fondo, se trata de una base de datos que solo permite escritura por consenso; esto es: nada se puede modificar, ni borrar, a menos que los nodos lleguen consensuadamente a la misma verdad sobre el evento.

Falsificar una entrada en la cadena de bloques, equivaldría a conseguir que más de la mitad de los miembros (nodos) se pusiese de acuerdo en mentir acerca de los detalles del aterrizaje del suricato de la misma manera, todos al mismo tiempo y sin tener la posibilidad de coordinar esa mentira previamente.

Ahora que todos sabemos qué es y de qué se trata *blockchain*, analicemos en qué podemos emplear esta tecnología.

El primer uso que tuvo blockchain (las cadenas de bloques) fue en las **criptomonedas**. La esencia de este uso fue garantizar la inmutabilidad de cada transacción y, principalente, evitar el doble gasto, es decir que alguien pueda gastar dos veces el mismo criptoactivo. A esta disyuntiva se le conoce como el problema de los generales bizantinos (ver https://marvin-soto.medium.com/el-problema-de-los-generales-bizantinos-pgb-e0cb8c4279c2).

Pero este no es el único uso que podemos darle, en realidad hay infinidad de maneras de utilizar las cadenas de bloques.

Una de las aplicaciones más relevantes que han surgido tiene que ver con lo que se conoce como "**contratos inteligentes**". Estos consisten en la capacidad de confiarle a la cadena de bloques el confirmar que un contrato de cualquier tipo ha sido cumplido, sin revelar ningún tipo de información confidencial sobre las partes y(o) la naturaleza de la transacción. Los contratos inteligentes servirían para liberar un pago a un individuo que ha sido subcontratado.

La idea se aplica también para los **contratos de abastecimiento**. Por ejemplo: si en su refrigerador está por agotarse un consumible, mediante un acuerdo previo, el dispositivo y el proveedor liberen por ellos mismos el o los suministros, para reabastecer sin la intervención del dueño de la casa. Nótese las implicaciones que esto tiene respecto de la confianza y la transparencia al realizar transacciones de cualquier tipo.

El **almacenamiento en la nube** también puede ser revolucionado con servicios que permitan que el almacenamiento se haga de forma distribuida utilizando una red basada en Blockchain, a fin de aumentar la seguridad y hacer menos dependiente el servicio, toda vez que sus usuarios puedan alquilar espacio sin que ese mismo bloque de almacenamiento sea utilizado por otros.

Los documentos digitales pueden ser sometidos a un proceso criptográfico para crear un digesto imposible de replicar. A esto se le llama un *hash* y funciona como una huella dactilar única. A un documento digital puede asociársele su digesto criptográfico único (*hash*) y guardarlo fuera de la cadena de bloques. Esto puede tener implicaciones para el **registro de patentes** o de otras formas de **propiedad intelectual**. Por ejemplo, una empresa o persona podrá demostrar que ha creado una tecnología en una fecha concreta sin necesidad de hacer una aplicación formal para registrar la patente, pues sería posible vincular sus documentos internos al *hash* de una transacción realizada en un momento certificado y probar así que ella ha sido la primera en desarrollar la invención.

Pensemos ahora en las votaciones. Sí, esos votos que emitimos para decidir por mayoría si algo tiene aprobación o, por el contrario, si la colectividad lo desaprueba. Pensemos en cuánto cuesta un proceso electoral en un país, cuánto papel se consume, la logística y la protección de los formularios. En algunos países, las elecciones pueden ser cuestionadas por la dudosa probidad de algún participante en el proceso. Cuánto cuesta a un país el conteo de los votos, los sistemas informáticos, los delegados y los demás participantes.

Blockchain permite habilitar sistemas de **voto electrónico** en el que las identidades de los votantes se mantienen protegidas. Sería infalsificable, no votarían los difuntos, los indecisos que no salieron de su casa, etc. El costo de esta alternativa tecnológica sería mínimo, al compararlo con el del proceso material usual (con todos sus bemoles); el acceso transparente sería público, tanto a sus resultados como a los resultados inmutables. ¿Recuerdan al suricato volador y a todos los nodos o testigos que lo vieron?

Ni qué decir del **Gobierno Abierto** o del **Gobierno transparente**, donde cualquier empresa pública o entidad gubernamental podría reflejar el estado de sus cuentas de ingreso y gasto en tiempo real, transparentando sus finanzas mediante el registro inmutable en una cadena de bloques.

La tecnología de bloques encadenados podría aplicarse a los **centros de estudios** para el registro de estudiantes, profesores, notas, etc., dando certeza de la historia académica de cada persona que ha estudiado allí. Ahora, que hemos entrado a la educación virtual a pasos agigantados, estos esquemas tecnológicos distribuidos e inviolables ofrecen muchas ventajas.

Podemos pensar incluso más allá, poniendo sobre la mesa **historiales médicos**, **registros de propiedad**, **actas matrimoniales**, **litigios legales**, **estados de cuenta**, **registros financieros y bancarios**, **cadenas de suministro**, **seguimiento de productos agrícolas** y **procesos productivos** para garantizar que sean ecoamigables, sustentables o higiénicos, todos gestionados a través de cadenas de bloques.

Eventualmente, todo conjunto de datos y transacciones digitales podría gestionarse con nuestra "biometría", creando un rastro fácilmente auditable de todo evento digital que tenga lugar en la historia de un individuo, sin comprometer su privacidad.

Les proponemos usar la imaginación y nuestra creatividad para visualizar más actividades en las que puedan ser aplicadas las cadenas de bloques y otras tecnologías digitales distribuidas para la transferencia de valor y la trazabilidad. ¡Vamos!

Agradecimiento

Ing. Marvin Soto Sotelo, Lic., es profesor de Tecnologías de Información y Comunicación en la Universidad Cenfotec. Se desempeña como Arquitecto de Soluciones de Ciberseguridad en Grupo Babel y es Gerente de Cybercom, S.A., empresa especializada en servicios de Ciberseguridad, Diseño y Administración de redes informáticas, Pruebas de penetración para validar seguridad y privacidad y Análisis forense digital.

Ing. Ignacio Trejos Zelaya, M.Sc., es profesor de Informática en el Instituto Tecnológico de Costa Rica y en la Universidad Cenfotec. Su investigación se centra en Lenguajes de programación, Ingeniería del software y Educación en Informática.