

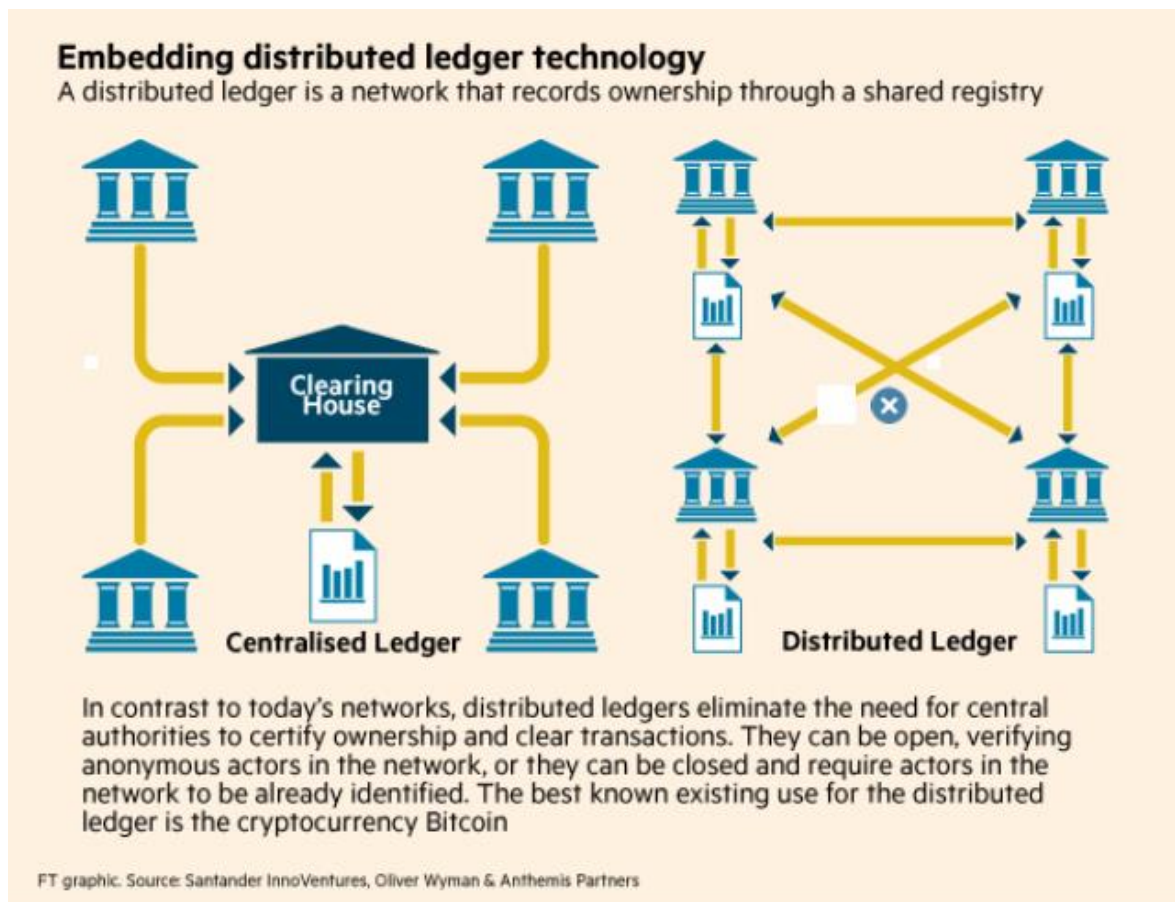
La cadena digital del Bitcoin (blockchain) y los mercados financieros. 1/

23 de julio

Los bancos y las instituciones de intercambio están muy interesados en aplicar la cadena digital (blockchain) que es el registro de propiedad de activos que utiliza Bitcoin. Esto es una mezcla entre Silicon Valley y Wall Street y pudiera representar un relanzamiento radical de las actuales redes financieras que vienen siendo utilizadas desde hace mucho tiempo.

¿Cómo funciona?

Actualmente, cuando un banco envía dinero a otro, no hay dinero físico de por medio. Los Bancos y los sistemas de compensación utilizan un registro central electrónico para rastrear los activos. Sin embargo, los sistemas pueden ser lentos e ineficientes, pues se apoyan en el fax o en alimentación manual, lo que no sólo desperdicia tiempo sino además incrementa las comisiones. Adicionalmente dichos sistemas son vulnerable al “hackeo” y al fraude.



El blockchain funciona ordenando secuencialmente bloques de transacciones en una cadena digital. Las transacciones entre usuarios de bitcoins son reunidas como bloques y retransmitidas a una red de computadoras.

Los que acopian los bloques de transacciones de bitcoins, para su verificación y registro público, son conocidos como mineros de bitcoin (miners) y compiten para verificarlas descriptando los acertijos criptográficos de su contenido.

El ganador transmite los resultados a otras computadoras y recibe un incentivo monetario. Un nuevo bloque es añadido a la cadena digital más o menos cada 10 minutos, conteniendo las transacciones de los últimos diez minutos; entonces las demás computadoras verifican el trabajo. La clave está en el código abierto, que puede ser distribuido y almacenado, y por lo tanto descentralizado. No se puede alterar porque entonces requeriría cambiar cada copia.

¿Qué utilidad pudiera haber para mercados financieros?

Los que apoyan el sistema mencionan que se pueden generar ahorros millonarios en colaterales y costos de liquidación, así como automatizar los caros sistemas de “back-office”. *Santander Innoventures, Anthemis* y *Oliver Wyman* estiman reducciones de costos de \$15 a \$20 miles de millones en costos bancarios para pagos internacionales, compraventa de títulos y cumplimiento regulatorio para el año 2022.

También se están explorando programaciones de “contratos inteligentes” que puedan ejecutar acuerdos comerciales.

¿Dónde está la desventaja?

La cadena digital nunca se pensó para transformar el sistema financiero, por lo que se le critica de tener varios defectos. El proceso computacional requiere de electricidad lo que es un costo real. La minería bitcoin ya es controlada por varios grupos pequeños que utilizan enormes granjas de servidores. Eso crea problemas potenciales. Si el incentivo monetario para hacer minería no es mayor al costo de hacer trabajar tantos servidores, tal vez no permita la existencia de suficientes mineros.

La cadena digital más larga –la que tiene incorporado más trabajo hecho- es aceptada como el registro. Para que alguien pueda modificarlo tendría que tener el control, aunque sea temporal de la red, si ello no ocurre es difícil distinguir, legalmente, a quién le pertenece.

El sistema puede mostrar falibilidad. Recientemente *Bitcoin.org*, un sitio de esta industria vigilado estrechamente, advirtió que varias computadoras generaban bloques inválidos. En efecto las computadoras fueron más incentivadas a ganar nuevos bitcoins y no validaron las transacciones existentes. (Dado que los bloques inválidos cuestan dinero a los mineros ellos asumieron que la cadena era correcta).

Otros se preocupan por que la cadena digital está creciendo demasiado volviéndose ineficiente para tratar con un número creciente de transacciones. Cuando se encontraron los bloques inválidos la empresa Bitcoin sugirió a los clientes esperar 30 confirmaciones o 50 minutos antes de aceptar las transacciones.

¿Qué pasaría si estos problemas se resolvieran?

El Banco de Inglaterra mencionó el año pasado que cada transacción financiera es registrada al menos por dos partes. Sin la certeza del cumplimiento legal de los contratos, y preocupaciones de seguridad, otros aceptan la necesidad de una autoridad central. Los bienes reales (mercancías) pueden ser pactadas pero aun así se requiere la evidencia de la entrega. La cadena digital es un protocolo y no tiene la habilidad de identificar a las partes. Los bancos han señalado que eso es necesario para cumplir con las duras regulaciones en el tema de la prevención de lavado de dinero.

Además está el problema de la liquidación. Una cámara de compensación, puede “netear” intercambios cortos o largos de títulos de brokers que se compensan. Si las posiciones se cancelan unas a otras, el miembro tiene que poner un pequeño margen a la cámara. Un registro distribuido como el de Bitcoin, necesitaría que la cámara liquide posiciones cortas y largas por cliente, lo cual es una carga operativa inmensa. Las compraventas tendrían que ser profundeadas lo que constituiría un dren de liquidez tal que países como Rusia han dejado la liquidación mismo día.

En la liquidación de derivados se trata de saber manejar márgenes en contratos vigentes. “En el mundo de los derivados tengo todo el incentivo de conseguir un margen (pagado) cuando mis contratos están “en el dinero” (in the money) además del incentivo de dejar que las cosas fluyan por sí solas cuando mis contratos están en rojo” dice un especialista. Cuando un banco está tratando con alguien poco sofisticado entonces la otra parte podría no saber que tiene derecho a cobrar el pago de un margen.

¿Entonces que hay con la liquidación?

Al igual que cualquier tecnología la experimentación abunda. El término cadena digital (blockchain) está siendo difícil de definir. Por ejemplo hay un creciente debate sobre si la cadena digital eventualmente necesita un “token” digital como el bitcoin.

Algunos negocios nuevos están volteando al permissionado de la distribución de registros donde el permiso es otorgado para aprobar a los participantes a acceder a la red y rápidamente registrar las transacciones y descubrir la propiedad del activo.

Compañías como Hyperledger no usan “blocks” sino un algoritmo más tradicionalmente aceptado que puede representar transacciones que podrían ser liquidadas en menos de 400 milisegundos. Si esto es una cadena digital es otro asunto. Algunos críticos señalan, en este punto, que la tecnología para distribuir registros se convierte menos en una herramienta revolucionaria y simplemente en el siguiente paso del back office de la infraestructura IT.

1/ Traducción y resumen del documento original: Explainer, Financial Times. Phillip Stafford.

Este documento es propiedad de la Unión de Instituciones Financieras Mexicanas A.C., su uso es exclusivo de sus asociados y debe ser tratado como información confidencial. Queda prohibida la copia parcial o total de este documento.