Recorrido histórico de todos los avances que nos han llevado a este punto supuestamente revolucionario de las criptomonedas y la cadena de bloques, y ayude a entender cuáles son las promesas y los retos que conllevan estas plataformas basadas en contratos inteligentes

Uno de los atractivos, a la par que dificultades, de todo lo relacionado con criptomonedas y cadenas de bloques lo resumió el cómico John Oliver en un tuit: “Las criptomonedas combinan todo aquello que no entendemos del dinero con todo aquello que no se entiende de los ordenadores.»

Se trata esta de una temática donde es muy fácil perderse en tecnicismos sofisticados, pero si mantenemos una perspectiva global, es relativamente sencilla de entender y promete tener un impacto tan relevante que los profetas hablan poco menos que de la venida de una nueva internet.

Esperamos que este artículo sirva como un recorrido histórico de todos los avances que nos han llevado a este punto supuestamente revolucionario y ayude a entender cuáles son las promesas y los retos que conllevan estas plataformas basadas en contratos inteligentes.

La criptografía es el estudio de todas aquellas técnicas que sirven para ocultar la información ante accesos no autorizados, mediante la ofuscación de los datos empleando contraseñas secretas a las que sólo los destinatarios legítimos tienen acceso. Estas técnicas tienen siglos de antigüedad y cobraron especial relevancia durante la II Guerra Mundial, donde ya existían dispositivos capaces de cifrar la información usando técnicas resistentes al ataque mediante la fuerza bruta.

> John Oliver, cómico: Las criptomonedas combinan todo aquello que no entendemos del dinero con todo aquello que no se entiende de los ordenadores.

Pero todas estas técnicas, por muy avanzadas que sean, asumen una simetría en la propia esencia de las contraseñas: tanto el remitente como el destinatario de la información cifrada deben ponerse de acuerdo para compartir un secreto de antemano, proceso durante el cual un atacante pondrá todo su esfuerzo en conseguir esa contraseña.

¿Es posible cifrar la información sin tener que compartir estos secretos a través de un canal no seguro? Resulta que sí.

A mediados de los 70 se comienzan a popularizar las técnicas de cifrado asimétrico donde, mediante relaciones matemáticas tales como la factorización de números primos, estas contraseñas se descomponen en dos: una parte pública, que se puede comunicar a cualquiera e incluso publicar en internet y otra parte

privada, que sólo conoce el usuario en cuestión. De esta forma, cualquier usuario que disponga de mi clave pública puede enviarme un mensaje que sólo yo podré leer, y por otro lado yo puedo publicar un mensaje (en principio visible para todo el mundo) con una firma que haga que cualquier usuario que disponga de mi clave pública puede verificar que he sido yo el autor.

Así, la criptografía moderna desdobla su propia utilidad: no sólo tiene la capacidad de cifrar mensajes, sino que sirve también para firmarlos. La firma de un mensaje y su relación unívoca con un autor implica la no renuncia: yo no me puedo desdecir de aquellos mensajes que se encuentren firmados por mi clave privada.

Este uso de criptografía asimétrica no es nuevo: se trata del estándar utilizado a nivel mundial tanto para accesos a equipos remotos como para asegurar las comunicaciones entre usuarios y sitios web mostrando tráfico SSL.

Con esto llegamos a una de las ideas fundacionales y el motivo del prefijo cripto- en las criptomonedas como bitcóin: no trata tanto de camuflar cuáles son los movimientos y transacciones que suceden en una red de pagos, sino de garantizar que los actores que intervienen en dicha red son quienes dicen ser.

Bitcóin, criptomoneda y cadenas de bloques

Si bien bitcóin no es el primer intento del uso de criptografía para trazar la transferencia de valor entre actores de una red económica, sí que es la primera criptomoneda en conseguirlo sin un agente central que actúe como registro del estado de las cuentas tras cada transacción. En palabras más técnicas, bitcóin permite resolver el problema del consenso distribuido en su aplicación a los movimientos de una moneda digital.

Así, si hay múltiples agentes operando entre sí, ¿quién determina el estado real de ese libro de anotaciones contables que todos deben compartir y asumir como cierto? La propuesta de bitcóin es engañosamente sencilla: uno de los participantes de la red, aleatoriamente, determinará la actualización de ese estado contable compartido entre todos.

La aleatoriedad no reside en un sorteo del estilo de la lotería, sino más bien en la resolución de un problema matemático que sólo es posible acometer probando soluciones de forma aleatoria con un consumo de CPU extremadamente alto.

Esto hace que deba haber un incentivo para que existan agentes que se presten a determinar el consenso distribuido en la red de bitcóin. En el caso de bitcóin, el incentivo es recibir una recompensa en forma de bitcóin que, de la nada, pasan a estar a disposición del agente que logra resolver este problema y determinar el nuevo estado global del gran libro contable de bitcóin. Estos agentes son los conocidos como mineros y son los actores encargados de generar masa monetaria en la red bitcóin: no hay otra forma de conseguir bitcóin que no sea generando bloques válidos en la cadena.

Hay un incentivo para que existan agentes que se presten a determinar el consenso distribuido en la red de

bitcóin. En el caso de bitcóin, el incentivo es recibir una recompensa en forma de bitcóin

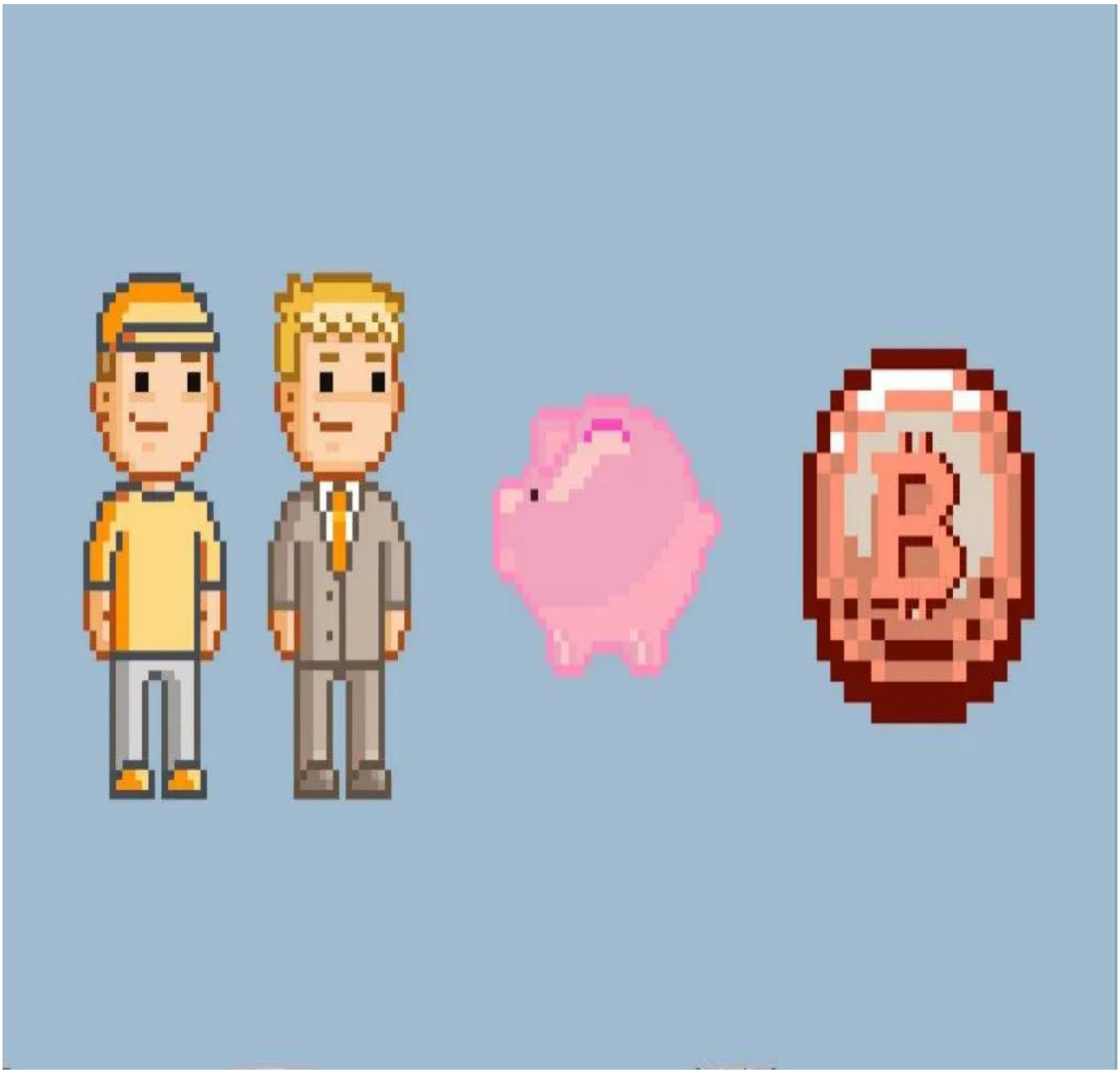
Para hacernos una idea de la dificultad del problema que estos mineros resuelven, supongamos el problema de determinar la letra de un NIF a partir de un numero dado. Es una operación trivial que cualquier programador puede escribir fácilmente. Sin embargo, el problema a la inversa se puede complicar: encontrar un NIF que termine en la letra P y cuyos guarismos sumen más de 78 (en este caso comienza a ser atractivo intentar encontrarlo no de forma determinista sino mediante una búsqueda aleatoria de números de NIF).

El minero hace algo similar: de forma muy simplificada, se trata de agrupar un número de transacciones pendientes en la red de bitcóin (emitidas por los usuarios de la red), comprobar que son efectivamente válidas -los usuarios que las emiten disponen de fondos para ello-, añadir una referencia al último bloque aceptado como válido y con toda esta información resolver un problema de carácter matemático con estos datos conocido como *hashcash*. El desafío es tan complejo que la única forma garantizada de encontrar una solución es ir probando opciones aleatoriamente, pero una vez encontrada una solución candidata el resto de agentes en la red pueden validarla fácilmente (de la misma forma que es fácil, con un NIF candidato, comprobar que sus dígitos suman más de 78 y que la letra es la P) y, si se trata de un bloque correcto, darlo como válido.

La referencia al último bloque válido es importantísima porque es lo que dota a la cadena de bloques de la característica de la inmutabilidad. Dado que los bloques van refiriéndose unos a otros, es imposible tratar de falsear un bloque del pasado sin que eso impacte en el nodo más reciente, situación fácilmente detectable.

Esto que acabamos de describir es una cadena de bloques, *blockchain* o *ledger* distribuido y es, sin duda, la mayor innovación de bitcóin porque impide la falsificación de los asientos contables por agentes maliciosos que estuvieran involucrados en la red (recordemos que bitcóin es una red pública a la que cualquiera puede conectarse) Esta contribución sin duda pasará a los libros de ingeniería como una solución genérica al difícil reto del consenso en sistemas distribuidos de ordenadores.

INFOGRAFÍA – GUÍA BÁSICA DE LAS CRIPTOMONEDAS



¿En qué consiste exactamente el dinero digital? ¿Cómo funciona? ¿Cuántas tipos de monedas existen? ¿Cuál es su valor? A continuación publicamos en formato infográfico una guía básica para iniciarte en el mundo de las criptomonedas y no perderte en el camino. IR A LA INFOGRAFÍA

En 1996 Nick Szabo definió el contrato inteligente como una solución de software que permite establecer compromisos declarados digitalmente entre partes de tal forma que:
1.- Sean aplicables cuando cualquiera de las partes así lo reclame.
2.-Cada parte pueda observar el compromiso que adquiere la otra parte en el contrato.
3.- Cada parte pueda verificar la aplicabilidad de las cláusulas del contrato en cualquier momento.
4.- El contrato sólo afecte a las partes que lo firman, y no a terceros no involucrados.

Si, bajo el prisma de esto cuatro criterios, contemplamos la solución de bitcóin al problema de los pagos descentralizados llegaremos a la conclusión de que bitcóin es una plataforma de contratos inteligentes, pero para una tipología muy concreta de contratos: aquellos en los que una parte declara poseer ciertos fondos en bitcóin y manifiesta su voluntad de transferirlos a otra parte.

El reto radica en cómo se puede generalizar la solución de la cadena de bloques (aplicada como se ha visto con éxito en bitcóin) para poder dar cabida a contratos de todo tipo. Dicha solución será necesariamente más complicada, pero de conseguirla estaríamos dando un salto cualitativo similar al que existe entre una calculadora y un iPhone. Mientras la primera es un dispositivo de función fija, el iPhone es mucho más: una plataforma que origina un ecosistema de aplicaciones (entre ellas, la calculadora).

Y este reto del que hablamos no es sencillo, porque dotar a una cadena de bloques de la capacidad de gestionar contratos arbitrarios supone dotarla de la capacidad de plasmar esos contratos como código y su ejecución.

La idea es tan potente que recientemente han surgido múltiples iniciativas para generalizar la idea de la cadena de bloques. Probablemente la más popular, por su carácter *open source* y por la habilidad en llegar a una solución viable (aunque no sin sus retos) es *Ethereum.*

> Ethereum es la cadena de bloques, diferente a la de bitcóin, más popular por su carácter open source y por la habilidad en llegar a una solución viable (aunque no sin sus retos)

Ethereum plantea una cadena de bloques diferente de la de bitcóin donde en lugar de emitirse transacciones simples de carácter contable lo que se emiten son contratos descritos en un lenguaje de programación (*Solidity*) inspirado en *Javascript*, lenguaje con el que muchos programadores están familiarizados. Estos contratos especificados formalmente en *Solidity* quedan registrados en la cadena de bloques y son firmados por las partes participantes (de forma no repudiable) quedando listos para su invocación por cualquiera de las partes a su interés: cuando eso suceda, un minero de la red *Ethereum* evaluará el código del contrato y, si se dan las condiciones necesarias, determinará qué sucede con los activos vinculados por medio de ese contrato a cada una de las partes.

Al igual que la red bitcóin, *Ethereum* dispone de su propia moneda, el ether. Sin embargo, su razón de ser es algo diferente: además de servir como almacenamiento de valor (convirtiéndose, de facto, en una criptomoneda más), la única forma de ejecutar una transacción en la red de *Ethereum* (por ejemplo, dar de alta un contrato, firmarlo, invocarlo…) es mediante el pago en ethers. Esto otorga a la moneda de *Ethereum* un carácter más parecido al de una materia prima que es capaz de poner en movimiento toda la maquinaria de smart contracts de *Ethereum*.

Cabe mencionar que *Ethereum* no es el único jugador en la arena de las plataformas de contratos inteligentes, que se encuentra en ebullición. La Linux Foundation apadrina la iniciativa *Hyperledger*, de similar propósito e incluso el propio carácter open source de *Ethereum* ha dado lugar a otras plataformas como *Quorum* creadas por compañías como JP Morgan Chase.

Vídeo

Descentralización, seguridad, confianza y eficiencia

Blockchain, la revolución tecnológica más allá de bitcóin

¿En qué consiste la tecnología en la que se sustentan las monedas criptográficas?¿Por qué todo el mundo habla de ellas? Te explicamos de forma clara en qué consiste la cadena de bloques y sus posibles revolucionarias aplicaciones.

Llegados a este punto, conviene apartarse de tecnicismos y considerar hasta qué punto llega el impacto previsible de la cadena de bloques. Todas las prestaciones, algoritmos matemáticos, redes de nodos sirven para un único objetivo: plasmar en forma de código cualquier tipo de acuerdo que sea concebible y poder ejecutar ese mismo código sin una entidad o autoridad central que deba supervisar toda la operación del sistema.

Con esta capacidad disruptiva los sistemas basados en cadena de bloques pueden llegar a convertirse, de forma deseablemente transparente para el consumidor final, en plataformas que habiliten todo tipo de servicios y productos por definir, que podríamos clasificar en dos grandes grupos.

En este primer grupo podríamos ver las plataformas basadas en cadenas de bloques como un sistema por el cual los actuales jugadores que ejercen de grandes agentes de autoridad, confianza o simplemente dueños de la información podrían conectarse entre ellos y generar servicios y productos cuyo valor consistiría precisamente en la integración de estos de grandes agentes.

Se puede incluir aquí los casos recientes de entidades bancarias que utilizan las cadenas de bloques para la emisión internacional de operaciones de transferencia de fondos, o las iniciativas orientadas en el campo del comercio internacional a la implantación de cuentas de escrow entre compañías de países diferentes.

Otro caso podría ser un hipotético catastro en la cadena de bloques, donde cualquier particular (o cualquier

otro sistema) podría integrarse para consultar de manera sencilla la información del registro de la propiedad, o quizá, mediante una aplicación operada desde la misma notaría, realizar modificaciones al mismo.

En estos casos, el factor diferencial y donde radica la ventaja para el debe ser en la mayor agilidad y menores comisiones de la operativa dado que el proceso es automático y prácticamente instantáneo. La cadena de bloques ejercería aquí una función similar a una API[1], permitiendo integrar servicios de forma sencilla y fiable.

Descentralización total

Este escenario, más radical, va más allá de que un órgano o agente central exponga la información en una cadena de bloques. En estos escenarios, la propia cadena de bloques se convierte en el agente generador de confianza, haciendo innecesaria la presencia de un regulador.

Si bien parece claro que este escenario tiene fuertes implicaciones que deberán ser previstas y resueltas por la legislación futura, ya se están dando casos de usos de este tipo, por ejemplo, en las llamadas ICOs (iniciales de *Initial Coin Offering*) donde una empresa pone a la venta sus activos digitales a inversores que participarán en la oferta con la esperanza de que esos activos se revaloricen en un futuro. En este caso la transacción se realiza directamente entre compañía e inversor, de forma totalmente privada y sin que intervenga ningún tipo de mercado bursátil.
Los retos.

La tecnología alrededor de la cadena de bloques (tanto en *Ethereum* como en el resto de plataformas) se encuentra sumida en una intensa actividad creadora. Cada pocas semanas aparecen nuevas plataformas con sus propios *frameworks* de trabajo, que prometen hacer más sencilla la vida de los desarrolladores de contratos inteligentes y de los usuarios de los mismos. Resulta imposible predecir cuáles de estas nuevas plataformas serán las que finalmente se impongan en la industria lo cual expone el conocido riesgo de los adoptares tempranos de la tecnología.

> Las cadenas de bloques se enfrentan al problema del éxito: según crece la red y aumenta su uso, igualmente se complica mantener o reducir la velocidad con la que las transacciones son validadas (ya sean monetarias como en bitcóin, ya sean de ejecución de contratos inteligentes como en Ethereum)

Siendo la propia operación de la cadena de bloques una operación computacionalmente costosa, este coste se traslada igualmente a cualquier modelo de negocio que se desee implementar sobre esta tecnología. A modo

de ejemplo: el coste de almacenar en una cadena de bloques algo tan aparentemente trivial como unas cuantas imágenes asciende a decenas de miles de dólares. Si bien es cierto que se trataría de un almacenamiento descentralizado, replicado y con una durabilidad de décadas -siempre que hubiera nodos conectados a esa cadena de bloques-, el coste de un servicio similar en un proveedor de nube pública como *Amazon Web Services* sería del orden de céntimos.

Por otro lado, las cadenas de bloques se enfrentan al problema del éxito: según crece la red y aumenta su uso, igualmente se complica mantener o reducir la velocidad con la que las transacciones son validadas (sean de carácter monetario como en Bitcoin, sean de ejecución de contratos inteligentes como en *Ethereum*).

En la cadena de bloques la identidad de un usuario no viene dada por su nombre o cualquier identificador sino por ese par de claves criptográficas de los que hablábamos al principio. La gestión de secretos criptográficos no es algo especialmente sencillo ni tan siquiera para los ingenieros: no hablemos ya de los consumidores finales, con el reto adicional que la pérdida de una de estas credenciales significa automática la pérdida irrecuperable de todos los activos a los que esta credencial tenía legítimo acceso. Pocos usuarios finales, salvo los que vienen del mundo de la tecnología, son conscientes de la importancia de la custodia y salvaguardia de sus firmas criptográficas. Esta gestión de contraseñas hace que, a día de hoy, para el usuario final el adentrarse en plataformas como *Ethereum* sea una aventura que le lleva a probar navegadores alternativos, plugins, y en general toda una literatura que se le escapa y le dificulta entender exactamente qué está haciendo con su dinero (por muy criptográfico que sea)

Sin embargo, probablemente el primer reto es delimitar qué categorías de problemas tiene sentido resolver mediante contratos inteligentes o cadenas de bloques. Recordemos que es clave la generación del consenso entre diferentes partes sin la necesidad de una autoridad central. Si esto no forma parte de los requisitos fundamentales del problema a resolver, hay que considerar seriamente la posibilidad de utilizar soluciones tradicionales.

¿Necesita el cliente de un banco que su entidad utilice una cadena de bloques para almacenar sus movimientos y ejecutar operaciones? Ya existe una relación de confianza suficiente entre banco y cliente, y ésta además se encuentra protegida por un organismo regulador, por lo que la transparencia y trazabilidad de la cadena de bloques poco aporta en este caso.

La integración con el mundo *off*

En el momento en que hablamos de contratos que relacionan activos o condiciones que salen del dominio digital (por ejemplo, la formalización de una hipoteca o la entrega de una mercancía) la situación se complica: debe existir un agente (conocido como Oráculo) al que ambas partes conceden la autoridad para trasladar los acontecimientos del mundo offline al mundo de lo digital de forma que sean accionables por los contratos inteligentes. En los ejemplos vistos anteriormente, estos oráculos estarían gestionados por los agentes de aduanas o los registros de la propiedad.

Como decíamos al principio el uso principal de la criptografía en las cadenas de bloques no es el cifrado, sino la firma de las transacciones para evitar que un agente pueda desdecirse de aquello que en un momento dado ha emitido. Dado que la cadena de bloques no se puede editar una vez que ha sido validada por los participantes en la red, cuestiones como el derecho al olvido o la corrección de algún dato legalmente disputable quedan en entredicho. Estas cuestiones, además, van a cobrar mayor importancia según entren en vigor normativas como el nuevo RGPD.

Toda solución basada en contratos inteligentes no deja de ser una solución a un problema expresada en la forma de un producto de software. Y los programadores sabemos que una cosa es un programa y otra bien distinta un producto de software, del que no sólo es complejo demostrar que está libre de errores (un contrato inteligente puede ser igual de difícil de depurar que cualquier otro programa) sino que también es complicado

poner en funcionamiento, como recientemente ha sido noticia en el caso de alguna empresa que ha perdido una inversión especialmente notable en términos económicos por un error en el entrecomillado de una línea.

El corolario aquí es que los contratos inteligentes deben estar sometidos durante su proceso de construcción a técnicas de control de calidad y seguimiento del ciclo de vida como cualquier otra solución de software.

Conclusión

la necesariamente optimista visión de los creadores de Ethereum es la de que la capacidad de su plataforma de ejecutar no ya contratos sino código arbitrario de forma distribuida y consistente la convertirá en una suerte de gran computador mundial que dejaría obsoleta la forma de construir aplicaciones existente en la actualidad: el código de los contratos desplegados en Ethereum estará disponible para ser ejecutado siempre y cuando siga habiendo ordenadores conectados a la red de Ethereum.

Los detractores plantean el problema de la escalabilidad: la propia necesidad de seguridad y control de fraude contradice la necesidad de rapidez y eficiencia de recursos de esta supuesta computadora global.

Finalizaremos este rápido repaso con una última reflexión: resulta difícil vaticinar cuál de los dos bandos tiene razón, ni si será Ethereum u otro competidor el que finalmente se impondrá al resto. De momento basta ver la inversión y la proliferación de estas plataformas como para entender que la trayectoria es ascendente y como para recordar que, de aquellas toscas máquinas que en los años 40 trataban de descifrar el código Enigma, llegaron los ordenadores de hoy que con su interconexión masiva han dado lugar a la transformación digital.

Si el mundo de las cadenas de bloques está en una fase como la del primer ENIAC… ¿supondrá su madurez el siguiente paso en la revolución digital?