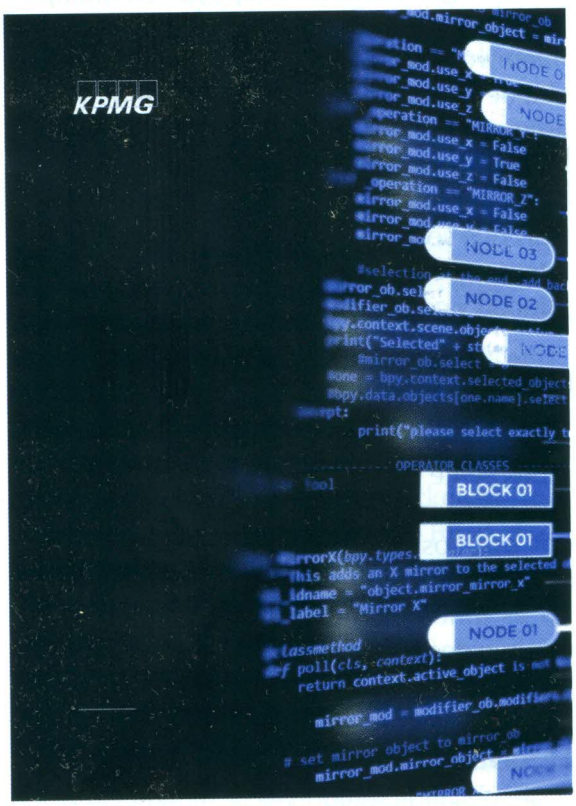
Asegurando la cadena



Ya es una realidad que Blockchain (cadena de bloques) puede cambiar el juego en los servicios financieros y otras industrias. Según noticia de Bloomberg en el 2016 hubo una inversión de US $ 1B en dicha tecnología. Algunos actores incluso ven Blockchain como una tecnología fundamental y disruptiva que permite habilitar y cambiar el procesamiento de negocios, tal como lo conocemos hoy en día en diversas industrias. A continuación presentamos un análisis de KPMG International sobre esta tecnología realizado por la oficina de Estados Unidos y liderado por Eamonn Maguire Global Head of Digital Ledger Services, Kiran Nagaraj, Sam Wyner y LaDarius Goens.

En general, las organizaciones se han centrado directamente en «cómo» pueden utilizar Blockchain para sus negocios. Sin embargo, a medida que más cantidad de pruebas de concepto avanzan hacia implementaciones prácticas y las amenazas cibernéticas crecen rápidamente en número y sofisticación, la seguridad y la gestión de riesgos ya no pueden estar en segundo plano. Además de «cómo», la pregunta entonces se convierte en, «¿es Blockchain seguro para mi negocio?»

La seguridad dependerá de una variedad de factores, muchos de los cuales requiere contar con un sólido marco para la gestión de los riesgos. Considérese, por ejemplo, que hasta la mitad de los ataques por explotación de vulnerabilidades ocurren entre 10 y 100 días después de su publicación, según un estudio realizado por Verizon en el 2016. A continuación, agregue el número de amenazas que ya son conocidas a ese momento. Las tecnologías emergentes tienen un factor de incertidumbre que las acompañan y por eso es necesario contar con una visión integral de los riesgos y amenazas.

Vamos a explorar dos incidentes recientes relacionados con la tecnología Blockchain: qué sucedió, cómo sucedió y cómo pudo haberse prevenido. A continuación, aplicamos las lecciones aprendidas de tales incidentes y de la experiencia de gestión de riesgos y seguridad con otras tecnologías emergentes, para proporcionar un marco que puede ayudar a identificar y responder a las amenazas para una implementación específica de Blockchain.

Las organizaciones se apoyan en múltiples marcos y estándares. El propósito de nuestro framework de Blockchain es habilitar una línea de interrogación completa (y crítica) para asegurar que las implementaciones de Blockchain son seguras y resilientes. Esperamos que las organizaciones adopten las principales prácticas que se sustentan en este framework y las integren con sus capacidades y marcos de seguridad y gestión de riesgos existentes.

■ *¿Es seguro?*

Existe una idea que Blockchain es inherentemente seguro porque sus principios se basan en criptografía e inmutabilidad. Pero dos eventos recientes demuestran que a pesar de sus fortalezas y promesas, Blockchain no es inherentemente seguro e incluso un mínimo descuido puede tener un impacto significativo.

El incidente DAO

En junio de 2016, desaparecieron aproximadamente US$ 50 millones en activos de un recién formado fondo de capital de riesgo digital, - la Organización Autónoma Descentralizada (DAO por sus siglas en inglés). El DAO es una organización virtual horizontal construida dentro de un smart contract en la Blockchain Ethereum. Este smart contract establece reglas que proporcionan a los participantes la posibilidad de votar sobre qué empresas se financiarían utilizando el Ether (una criptomoneda similar a Bitcoin). Cuanto mayor sea la contribución, mayor será el número de votos de cada participante. Cuando finaliza una votación, las monedas de Ether se distribuyen a la billetera de Ether de la empresa y se registran como una transacción inmutable dentro de la Blockchain Ethereum.

En los días anteriores al ataque, se identificó y publicó una vulnerabilidad de software para la función «split DAO» (división). Esta función fue diseñada originalmente para permitir a los participantes del DAO transferir su saldo de cuenta y ramificar en un nuevo DAO "hijo" si cambiaban de parecer luego de un voto.

Al igual que en una cuenta de depósito tradicional, la red comprueba el saldo del participante y luego la transfiere al DAO "hijo". Cuando finaliza la división, el balance del participante en el DAO original se pondría en cero. La vulnerabilidad publicada mostró que mientras la función de división funcionaba correctamente, permitía a los participantes llamar a otra división antes de que se terminara la primera. Debido a que los saldos no se anularon hasta el final de la división, los atacantes fueron capaces de realizar la misma división una y otra vez, casi 200 veces, hasta que el DAO estaba casi vacío.

La causa de la salida de fondos parece clara: hubo un fallo no intencional en el código de la función «split DAO» del Smart contract DAO. Ethereum, la tecnología Blockchain en la que se basa DAO, funcionó tal como fue diseñada y no se vio comprometida de ninguna manera. El atacante aprovechó al máximo este diseño y el conocimiento del funcionamiento de la propia tecnología Blockchain.

Pero la pregunta es **¿Pudo haberse evitado?** Sí. De acuerdo con la información disponible públicamente, el ataque podría haberse evitado si el código del Smart contract DAO hubiera sido sometido a una revisión formal exhaustiva antes de entrar en funcionamiento. Si bien es fácil saber lo que se debe hacer después de que algo ha ocurrido, estas evaluaciones, revisiones y actividades de prueba son aquellas que se espera que atraviese cualquier aplicación de tipo empresa-

rial antes de ser utilizada en producción, especialmente dado el panorama actual de amenazas cibernéticas.

La brecha de Bitfinex

En agosto de 2016, el intercambio de divisas Bitfinex de Hong Kong sufrió una brecha de seguridad en la que casi 120.000 Bitcoin se eliminaron de las cuentas de clientes. Bitfinex utilizó una serie de medidas de seguridad, incluyendo un sistema de gestión de claves multi-firma, que dividió las claves privadas de la cartera de cada usuario en dos partes diferentes para reducir la probabilidad de un ataque exitoso.

Si bien la causa del ataque no ha sido confirmada por Bitfinex, dos de las tres claves del sistema multi-firma de Bitfinex se almacenaron internamente. La tercera clave fue custodiada por un proveedor de billeteras, BitGo. Las tres claves serían necesarias para realizar una transacción. Independientemente de quién sea el culpable, la realización de controles sistemáticos para prevenir y detectar transacciones análogas implementadas por cualquiera de las partes podría haber ayudado a minimizar las pérdidas sufridas.

Al igual que en el caso DAO, este ataque explotó vulnerabilidades de seguridad dentro de organizaciones individuales y la red Blockchain (Bitcoin en este ejemplo) permaneció completamente funcional y operó como se esperaba.

Nos volvemos a preguntar **¿Pudo haberse evitado?** Sí. El ataque podría haberse evitado si los desarrolladores de Bitfinex y BitGo y sus homólogos de negocios hubieran realizado una revisión en profundidad de la seguridad usando varios escenarios de riesgo durante el ciclo de vida de la transacción de extremo a extremo. Al realizar una revisión de extremo a extremo, estas organizaciones tendrían una mejor oportunidad de identificar y mitigar los riesgos, más allá de los riesgos de TI, como la gestión de claves privadas. Una vez más, mientras que la visión retrospectiva resulta clara, éstas son actividades estándar que se deberían haber realizado típicamente.

Como estos ejemplos ilustran claramente, a pesar de sus fortalezas y promesas, **Blockchain no es intrínsecamente segura, e incluso un pequeño descuido puede tener un impacto significativo.**

■ *¿Es inherentemente defectuoso?*

No, las bases y la arquitectura no son inherentemente defectuosas. En el caso del incidente DAO independientemente de la solución elegida, la arquitectura subyacente funcionó como se esperaba.

Los aspectos técnicos de estos incidentes, incluyendo el impacto potencial en la inmutabilidad de una cadena de bloques, han sido ampliamente cubiertos en distintos artículos. Teniendo en cuenta la arquitectura subyacente y los fundamentos, todavía se puede considerar fiable. Esto nos permite centrarnos en cómo las organizaciones pueden adoptar un enfoque más orientado al negocio para la construcción de soluciones Blockchain que sean seguras y resilientes. Porque Blockchain está aquí para quedarse y su adopción sólo aumentará.

Ambos incidentes examinados subrayan la necesidad de una visión integral del riesgo. En cada caso, muchas de las vulnerabilidades y defectos de diseño podrían haber sido abordados previamente, si se hubiese aplicado disciplina para identificar, evaluar y mitigar los riesgos durante el diseño o las pruebas.

Hay lecciones que aprender de estos y otros incidentes, pero también lo más importante son las lecciones aprendidas de décadas de seguridad y experiencia en gestión de riesgos con otras tecnologías tradicionales y emergentes.

Podríamos mencionar que **el gran entusiasmo por esta tecnología innovadora y su prometedor potencial han eclipsado el enfoque en las posibles amenazas y riesgos.**

Asegurar la cadena

KPMG ha construido un marco de seguridad y gestión de riesgos que proporciona un enfoque de extremo a extremo para identificar y responder a las amenazas de seguridad y los riesgos tecnológicos para una implementación de Bockchain.

Este marco se desarrolló a través de la identificación de prácticas líderes a través de diez dimensiones claves que son aplicables a través de un típico ciclo de vida de implementación de Blockchain, desde la estrategia y el caso de negocio hasta la operación y el mantenimiento.

Mientras que algunas dimensiones dentro de este marco, como la Gestión de Datos y la Segregación, son típicamente parte de las capacidades existentes para los departamentos de Seguridad y Riesgo dentro de las organizaciones, otras como Mecanismo de Consenso, Administración de Permisos de Cadena y Criptografía, Gestión de Claves y Tokenización, pueden ser totalmente nuevos y deberán considerarse para su inclusión en marcos y normas existentes.

Aplicación del marco de seguridad y riesgos de Blockchain de KPMG

En el ciclo de vida de implementación se podrá tener en cuenta prácticas que nos permitan tener una visión integral de los riesgos y seguridad para poder gestionar posibles amenazadas. A continuación presentamos algunos puntos a considerar durante las etapas del ciclo de vida.

Etapa de estrategia y caso de negocio:

- La necesidad de almacenamiento en caliente o en frío de las claves privadas.
- Establecer estándares mínimos y máximos para los niveles de activos en cada tipo de almacenamiento.
- Establecer requisitos de privacidad de datos para los datos de las transacciones en cadena.
- Identificar procesos alternativos y redundantes fuera de la cadena para escenarios específicos.

Etapa de requisitos y desarrollo:

- Asegurar la revisión de los contratos inteligentes para evaluar todos los posibles escenarios de entrada y salida.
- Asegurar que los nodos tengan la capacidad configurable para detener la transmisión o aceptación de datos de otros nodos durante eventos de seguridad.
- Utilizar formato multi-firma para evitar el uso inapropiado o no autorizado de claves privadas.
- Asegurar que la infraestructura y software Blockchain utilizan procedimientos de gestión de vulnerabilidades.

Prueba y despliegue:

- Asegurar que las claves privadas de producción no se utilicen durante las pruebas.
- Probar las transacciones de extremo a extremo para validar que los datos mostrados en la capa de aplicación coincidan con el libro mayor.
- Probar contratos inteligentes utilizando conjuntos de datos de prueba de manipulaciones y todos los escenarios identificados.
- Probar escenarios de anulación de consenso antes de la implementación en producción.

Operaciones y mantenimiento:

- Mantener registros de acceso detallados para todo acceso a claves privadas, incluyendo cualquier intento de leer claves privadas.
- Supervisar activamente los nodos para detectar ataques de denegación de servicio.
- Obtener informes de control de seguridad de todos los participantes y proveedores Blockchain periódicamente.

- Prueba y despliegue de parches dentro del SLA acordado conjuntamente por la red.

■ *En definitiva*

Muchos anticipan que Blockchain irrumpirá y transformará significativamente los modelos de negocio en los servicios financieros, la asistencia sanitaria y más allá. Sin embargo, la expectativa sobre esta tecnología innovadora y su prometedor potencial ha eclipsado un verdadero enfoque en las posibles amenazas y riesgos. A medida que Blockchain continúa creando un impulso significativo y se encuentra con la realidad, las empresas no pueden hacer caso omiso de la seguridad y la gestión de riesgos por mucho más tiempo. Blockchain puede incluso proporcionar una falsa sensación de seguridad a través de algunas características básicas en torno a la criptografía y la inmutabilidad. Ahora es el momento de aplicar un enfoque de gestión de riesgos.

En el futuro, creemos que las consideraciones de seguridad y riesgo, incluyendo las discutidas en este artículo, guiarán los casos de uso y las implementaciones de Blockchain a través de las industrias.

Al analizar las lecciones aprendidas de ejemplos recientes de incidentes relacionados con Blockchain y de décadas de experiencia en seguridad y gestión de riesgos, las organizaciones pueden estar mejor equipadas para implementar soluciones seguras y resilientes alrededor de esta tecnología emergente.