Blockchain: Riesgos asociados (3/5)

Author : ibonreinoso

Categories : Auditoría, Certificación y Calidad de Sistemas Informáticos

Date : 22 noviembre, 2018

Buenas de nuevo! Si eres un nuevo lector y no has leído mis anteriores entradas, te invito a que te acerques a las anteriores entradas. En la primera entrada [enlace], hablé de qué era Blockchain; la arquitectura que tenía, cómo funcionaba y sus respectivos beneficios. Después, en el segundo artículo [enlace] (anterior a este) realicé una reflexión para primeramente comprender los riesgos y después ver qué directivas e iniciativas regulativas existían para proteger y guiar a toda organización que estuviera interesada en incluir estas “cadenas de bloques”; además hice un pequeño análisis donde ya identificábamos algunas cuestiones que planteaban si realmente existía una compatibilidad con la ley RGPD.

Volviendo al presente, el objetivo de este post será identificar los riesgos potenciales asociados a Blockchain. Pero antes de nada, veamos qué es un riesgo:

“Contingencia o posibilidad de un daño” [1]

Entonces, todo aquello que pudiera ser un problema por el daño que supone se define como eso mismo. Dentro del contexto empresarial, más concretamente en Sistemas de Información, me gustaría hacer especial hincapié en que los riesgos no sólo están en la tecnología como buenamente se suele pensar.
Es obvio asumir que utilizar una tecnología concreta debes aceptar que esta puede fallar. Sin embargo, existen más actores rodeando no sólo a las tecnologías sino que también a las propias organizaciones y sociedades a las que forman y donde están. Por otra parte, ya en 2016 ISACA había identificado riesgos potenciales, de los que hablaré a continuación. Muestra de ello, se expone la figura 1[2], que básicamente es un Heatmap donde en función de la probabilidad y el impacto se muestran los riesgos para Blockchain:

Figura 1: Tabla de riesgos para Blockchain en función de la probabilidad e impacto.

La tabla se interpreta de la siguiente manera: “cuanto más rojo, mayor cuidado” hay que tener, mayor riesgo e impacto implican. Como si fuera un semáforo de riesgos.

Según ISACA, podríamos ponderar en varios niveles estos riesgos. En un primer nivel (en color rojo), se encuentran el control de cambios, las vulnerabilidades y la gestión y control del cambio. En un segundo nivel (en color “ámbar”), se encuentran los riesgos asociados a la pérdida de control y cumplimiento legislativo. En un tercer nivel, riesgos asociados a la privacidad y retención de la información además de la encriptación, entre otros.

Es algo lógico; primeramente, hay que gestionar el cambio de paradigma que implicaría dentro de una organización. Después, ¿Sirve para toda la infraestructura de la que se nutre la organización?¿O sólo en parte? Desde luego, son preguntas que al menos, deben ser planteadas. Después, al ser una tecnología tan vanguardista, desconocemos por donde flaquea. ¿Y si se detectase una vulnerabilidad? ¿Estaríamos dispuestos a asumir este riesgo?

Desde un punto de vista legislativo, se deben tener en cuenta las directivas y leyes. Las tecnologías, pertenecientes a corporaciones, deben cumplir sus responsabilidades legales. Ejemplo de reglamento lo es la RGPD (por nombrar una, no por ello única). Si esta cambia, la manera en la que Blockchain está diseñada para nuestro caso de uso debe ser al menos analizada y ver si realmente no tiene implicaciones; en caso contrario, se debería abordar todo un proyecto de adecuación (como ya se ha ido viendo con el boom de los cookies). La incorporación de Blockchain ya tendrá un ROI bastante alto y la Empresa deberá tener especial interés en mantenerlo en producción, esto es, mucho valor tendrá que aportar BlockChain para asumir este riesgo tan alto.

Por último, discutamos los riesgos de color verde. Es evidente que habría que plantearse la generación de claves y cómo gestionarlos. ¿Quien se responsabilizará de eso?¿Cada cuanto se generarían nuevas claves, si es que se hacen?¿Qué pasaría si la clave pública se fuga?[3] Además, ¿Quienes serían los agentes verificadores?¿Por qué ellos?¿Tendrían más responsabilidades?¿Serían personas o sólo máquinas, de manera automática? A todo esto, habría que añadirle una serie de cuestiones en torno a la capa de persistencia: ¿De qué manera persistimos esta información?¿Bajo qué condiciones validamos? En definitiva, existen muchísimos riesgos que, desde luego, hay que tratar de abordarlos antes de dar pie a la implantación de esta tecnología. Hay que valorar si realmente merece la pena invertir en esto mismo, si realmente aporta valor y utilidad directa. Hay que mantener la prudencia, no vaya a ser que demos un paso en falso.

En el próximo post hablaré de los controles que se pueden aplicar para los riesgos en esta

tecnología. Hemos identificado varias cuestiones que deberán ser abordadas, intentaremos minimizar o al menos mitigar los mismos.

1. Real Academia de España, Buscador de RAE, http://dle.rae.es/?id=WT8tAMI, acceso el 22 de noviembre de 2018.

2. Blockchain and Risk (Mike Small CEng, abril 2016), https://m.isaca.org/chapters8/Northern-England/Events/Documents/blockchain.pdf., acceso el 22 de noviembre de 2018.

3. "Seguridad de contactos inteligentes basados en Blockchain II - Vulnerabilidades y riesgos" (Stefan Beyer, marzo de 2018), https://www.securityartwork.es/2018/03/20/seguridad-de-contratos-inteligentes-basados-en-blockchain-ii-vulnerabilidades-y-riesgos/, acceso el 22 de noviembre de 2018.