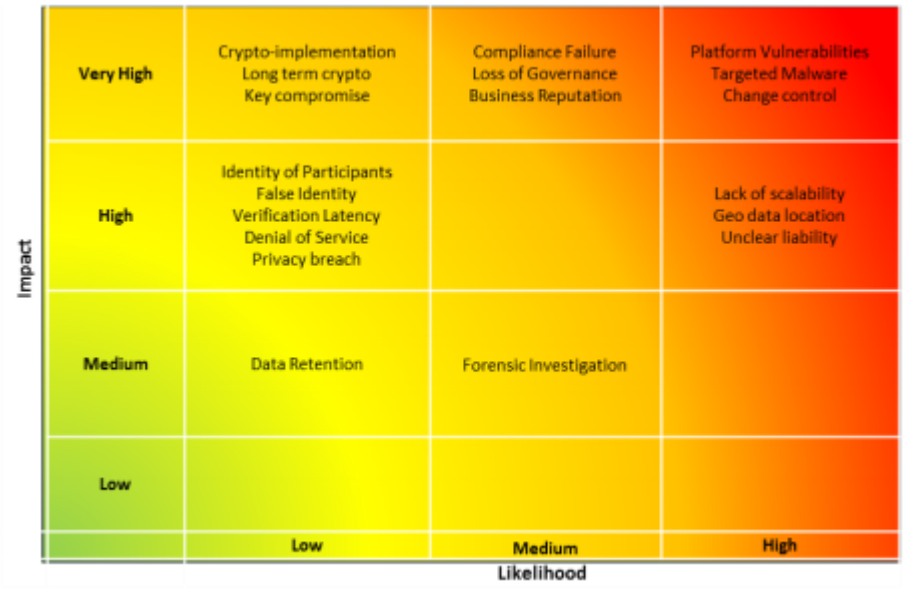
Blockchain Risks

Como hemos aprendido en los dos anteriores posts, blockchain reduce tremendamente la posibilidad de que surjan errores. Además, los registros no pueden ser modificados por nadie una vez que se han añadido. Debido a que cada transacción se registra y se verifica, la integridad de los registros está garantizada. Por ello, mucha gente del sector IT plantea el hecho de que auditar sistemas basados en blockchain va a ser innecesario. Pero ¿es eso cierto?

Sin duda alguna es totalmente falso.En este post voy a resaltar los principales riesgos que se deben tener en cuenta cara a la auditoría de un sistema con tecnología blockchain. Tal y como hace referencia Deloitte en uno de sus artículos sobre blockchain y sus riesgos, el blockchain se puede dividir en dos tipos: "permissionless and permissioned chains", esto es, cadenas sin permiso y autorizadas.[1] Blockchain sin permiso permite que cualquiera sin ningún tipo de verificación participe en la red de transacciones. Sin embargo, las autorizadas están formadas por responsable o responsables que evalúan la participación de una persona u entidad en el entorno blockchain.

La mayoría de los riesgos que hoy en día se plantean no van asociados al tipo de blockchain del que se use. Ya que, es cierto que un riesgo está directamente relacionado con la integridad de los eslabones que componen la cadena blockchain, pero los grandes riesgos que realmente asustan a los expertos son independientes a ello. Después de informarme bien, y leer y releer una enorme cantidad de artículos en lo que refiere a este tema, me gustaría destacar una tabla publicada por ISACA que recopila de manera muy visual los posibles riesgos del blockchain y su relevancia. [2]



Como se puede observar, categorizan los riesgos según su impacto y su probabilidad. Siendo de color verde los riesgos de menos importancia y difuminándose a color rojo los que aumentan su relevancia. En ISACA entienden por críticos, los siguientes riesgos:

- Plataform Vulnerabilities:

  La integridad del blockchain está determinada por la plataforma de software sobre la cual se ejecuta. Si la plataforma se considera poco fiable, ello afecta al blockchain.

- Targeted Malware:

  La infraestructura que admite el blockchain está sujeta a todas las amenazas y vulnerabilidades habituales. Ningún software está exento de ataques, y hay que tenerlo en cuenta.

- Change control:

  Abuso del privilegio de administración y cambio no autorizado en la infraestructura.

Además de estos tres posibles riesgos que ISACA destaca como los riesgos con mayor grado de impacto/probabilidad, me gustaría destacar desde mi punto de vista los principales riesgos en cuanto a seguridad se refiere: el acceso o control de acceso, la robustez del cifrado y la seguridad individual de cada nodo. Respecto a la seguridad de cada nodo, hay un dicho que me viene a la cabeza: "una cadena es tan débil, como el eslabón más débil de esta". En este caso ocurre lo mismo, por ello es imprescindible disponer de planes de contingencia adecuados. A su vez, es cierto que el blockchain se caracteriza por estar cifrado, pero es de destacar que existen infinidad de algoritmos de cifrado. Y, no todos poseen el mismo nivel de seguridad.

En conclusión, puesto que estamos tratando una tecnología emergente, la mayoría de información y opiniones respecto a sus posibles riesgos son meras suposiciones. Suposiciones que se basan en experiencias pasadas, experiencias que se basan en casos similares. Lo que nadie duda, es que esta tecnología ha venido para quedarse. Sin embargo, hasta que no se quede y se estandarice, no se podrá hacer una lista cerrada de los riesgos que implica. Lo que está claro es que a poca gente le gustan los cambios, y es porque con los cambios surgen riesgos que hasta el momento no se planteaban. El blockchain implica cambios y por lo tanto, implica nuevos riesgos. En lo que auditoría respecta, cualquier gran empresa o profesional que se quiera centrar en auditar esta nueva tecnología debe estar al tanto de los cambios que implica dicha tecnología, tanto de los casos que triunfen como de los que fracasen, y aprender de ellos. Deben ir perfeccionando la técnica de auditar según se vaya perfeccionando la tecnología.

Referencias:

[1]: Blockchain risk management (Prakash Santhana and Abhishek Biswas, 2017),https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-blockchain-risk-management.pdf

[2]: Blockchain and Risk (Mike Small CEng, abril 2016), https://m.isaca.org/chapters8/Northern-England/Events/Documents/blockchain.pdf