IDENTIFICACIÓN Y CONTROL DE RIESGOS EN PROCESOS VALIDADOS CON BLOCKCHAIN

Cuadernos de ISACA Madrid

Reconocimientos

El Capítulo de Madrid de ISACA (183) desea reconocer la labor de:

Coordinación
Erik de Pablo Martínez, CISA, CRISC, Vocal de Investigación de la Junta Directiva de ISACA Madrid

Editora
María Teresa Avelino, CISA, CISSP, PMP

Coautores
Antonio J. Turel, CISM
Ainoa Inza, CISA

Revisores expertos
Diego Fernández
José Ramón Coz
Claudio Chifra
José Carrillo
Ana González Monzón

Junta Directiva del Capítulo de Madrid de ISACA (183)

Presidente: D. Ricardo Barrasa García

Vicepresidente: D. Antonio Ramos García

Secretario: D. José Miguel Cardona Pastor

Tesorera: Dña. Ana Belén Soriano Herrera

Vocal 1 - Relación con los asociados, Comunicaciones y Marketing: D. Joaquín Castillón Colomina

Vocal 2 - Relación con la Admon. Pública y la Empresa Privada: D. Fernando Hervada Vidal

Vocal 3 - Formación y Relaciones Académicas: D. Vicente Chiva Carbonell

Vocal 4 - Auditoría & GRC: Dña. Vanesa Gil Laredo

Vocal 5 - Seguridad Lógica: D. Eduardo Solís Gómez

Vocal 6 - Eventos: D. Pablo Blanco Íñigo

Vocal 7- Investigación: D. Erik de Pablo

Índice de Contenidos

Contenido

1 Procesos que se pueden validar con Blockchain

No todos los sistemas son aptos para ser implementados con Blockchain. Por ejemplo, si un sistema no es transaccional o no puede ser distribuido, no será viable su implementación de esta manera.

Antes de explorar las distintas formas de utilizar de uso de blockchain en los negocios, los directivos deberían conocer las vulnerabilidades de esta interesante tecnología, ya que, aunque incluye controles que garantizan cierto nivel de seguridad, puede incurrir en riesgos que deben ser contemplados de antemano.

Esta tecnología ha nacido con una aureola de seguridad que rápidamente ha sido aceptada por la industria sin conocer en profundidad cómo funciona realmente o cómo se integran las aplicaciones que hacen uso de ella, lo que supone un riesgo.

Blockchain garantiza a sus usuarios que, una vez que la información ha sido almacenada, nunca podrá ser luego borrada o falsificada. Esto proporciona cierta confidencialidad en sectores que precisan de un férreo control del fraude como por ejemplo el financiero donde, cuando sus profesionales analizan la historia de una transacción que ha sido almacenada, se sienten seguros de que no se ha cometido fraude sobre dicha transacción. En esencia, **blockchain promete no solo la completa seguridad del dato, sino algo más intangible: que nunca será adulterado**. **Como analizaremos en este estudio, blockchain puede llegar a ser tan insegura como otras tecnologías, sobre todo si no se toman las medidas oportunas.**

Diversos estudios realizados por el MIT entre 2011 y 2018 sobre más de 70 violaciones de seguridad sobre blockchain concluyen que, si bien esta tecnología presenta ventajas como el manejo de la confidencialidad o la integra, incurre en diversas vulnerabilidades de seguridad, algunas de ellas intrínsecas a la propia naturaleza de la blockchain o a las implementaciones que se han realizado.

Además, si usamos los denominados “Smart Contracts” para programar los eventos sobre nuestros procesos, nuestros sistemas deben ser programables de forma similar a máquinas de autovending (esto es, autómatas de estados finitos). De este modo, la tecnología blockchain está recomendada para los procesos que:

- Tengan **muchos participantes descentralizados**.
- Precisen confiar en una tercera parte sin el uso (en el caso de las blockchain públicas) de una Autoridad de Certificación (CA).
- Las tareas sean básicamente **transaccionales**.
- Las **transacciones versen sobre un activo**, sea tangible o no.
- **La contabilidad de este activo deba ser descentralizada**.
- En el caso de blockchain públicas, los registros contables deban ser cifrados para preservar su confidencialidad.
- **Precisen de un histórico inmutable** (similar a un diario contable).
- **Precisen de arbitraje automático** de las disputas o reconciliaciones.

- **Precisen de la monitorización real** de la actividad de los reguladores y los regulados.
- Deban demostrar de forma fehaciente la propiedad de los activos y todo el registro transaccional (logs transaccionales).
- No contengan datos de carácter personal o si los contiene, se puedan seudonimizar (ver RGPD). Además, recientemente y en el caso de España, no contenga datos de las administraciones públicas (ver RD. Ley 14/2019).

2 Principales amenazas y sus causas

Los sistemas que hacen uso de la tecnología blockchain suelen ser objeto de vulnerabilidades que afectan mayoritariamente a las dimensiones de Integridad, Autenticidad y Trazabilidad. A continuación, se resumen las más comunes, y se dará al final algún ejemplo actualizado de cómo han sido explotadas recientemente:

- **Bribery:** El atacante consigue que los nodos minen en su propio beneficio. Impacto: Económico, la víctima (minero) pierde dinero.
- **Sybil:** El atacante crea artificialmente nodos mineros para conseguir aumentar su beneficio y/o intentar ataques del 51%. Algunas fuentes consideran que la empresa Chainalysis –dedicada al análisis en profundidad de la red blockchain– perpetró en el 2015 un ataque de este tipo. Impacto: Económico, poder de manipulación del consenso.
- **Punitive forking:** Se fuerza un fork (término usado en programación para denominar a una línea paralela de código fuente) para incluir en *blacklist* las transacciones que no queremos que se validen. Impacto: Económico sobre usuarios y comerciantes, se hace especulación para favorecer a otros.
- **Time jacking:** El atacante actúa contra el protocolo NTP del nodo para impedir que pueda minar por falta de sincronización con el pool de minería. Impacto: Se impide el minado a una red de mineros que trabajan en dicho pool desconectado.
- **Routing attacks:** El atacante impide que el minero se pueda comunicar con la red y también los usuarios con su monedero en la nube, los *exchanges*. Impacto: Impedir el funcionamiento de la red en un área determinada.
- **Man in the middle**: Consiste en la posibilidad de suplantar el origen o destino de las transacciones, usando vulnerabilidades en la generación de direcciones en el caso de algunas blockchains que, por simplicidad, en vez de usar las claves públicas de la PKI, usan una referencia obtenida por un algoritmo a veces vulnerable . Impacto: Económico, se roban fondos de usuarios o comerciantes.
- **Eclipse/Netsplit:** El atacante monopoliza hacia sí mismo todas las comunicaciones. Impacto: Económico, pretende el atacante quedarse para sí con todos los recursos para minado.
- **Deanonimización:** Asociación y publicación de direcciones IP y direcciones de monedero. Impacto: Se pierde la privacidad de las transacciones.
- **Vulnerabilidades de las aplicaciones criptográficas empleadas.** Los algoritmos de cifrado de clave pública todavía no han sido rotos (a falta de la llegada real de la computación cuántica) pero, las implementaciones de algunos protocolos mal implementados, pueden suponer un riesgo**.**
- **Vulnerabilidades en el código de *Smart Contracts***: Si se encuentra un *bug*, afecta a todas las transacciones que se han lanzado al ejecutar el *Smart Contract*. Impacto: Se requiere aplicar un fork a toda la red para corregirlo, lo que a veces es imposible o provoca pérdidas económicas (caso de The DAO y remarcando la posterior división, fork, de la versión Ethereum).
- **Vulnerabilidades en la *virtual machine* de Ethereum**: Pueden ocasionar direcciones incorrectas con pérdida de fondos o transacciones con argumentos incorrectos. Impacto: Requiere reprogramar todos los nodos (al menos un *soft fork*).
- **Cryptojacking:** La víctima es infectada (normalmente al visitar un link en Internet y ejecutársele el código maligno javascript), de modo que acaba minando sin darse cuenta para el atacante. El malware CoinHive es el más empleado por los

ciberdelincuentes. Impacto: Económico y de reputación por la organización que ofrece los servicios web a través de los cuales se explota el malware sin saberlo.

Si bien el grueso de amenazas analizado se focaliza en vulnerabilidades técnicas y operativas, como veremos en el capítulo 3, no hay que menospreciar las amenazas de tipo legal, económico o de imagen que estas vulnerabilidades reportadas pueden provocar.

El mayor conjunto de vulnerabilidades de los últimos años, han sido relacionadas principalmente con los Smart Contracts (contratos inteligentes).

En la siguiente tabla se citan algunos ejemplos de vulnerabilidades contabilizadas por la prestigiosa base de datos global MITRE:

Identificador	Severidad (0-10)	Descripción	Impacto	Referencia principal	Más detalle
CVE-2018–20587	2.1	Las plataformas Bitcoin Core 0.12.0 (a través de 0.17.1) y Bitcoin Knots 0.12.0 (a través de 0.17.x) disponen de un Control de Acceso incorrecto. Explotando esta vulnerabilidad, usuarios locales podrían robar criptomoneda.	Robo económico	https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures#CVE-2018-20587	https://www.cvedetails.com/cve/CVE-2018-20587/
CVE-2018-20421	5.0	La plataforma Go Ethereum 1.8.19 es susceptible de sufrir ataques de tipo Denegación de Servicio. Esto es debido a la posibilidad de reescritura de la longitud de un array dinámico en la memoria y a continuación, la escritura de datos a una única ubicación de memoria con un número de índice largo.	Disponibilidad del Sistem	https://github.com/ethereum/go-ethereum/issues/18289	https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2018-20421 https://www.cvedetails.com/cve/CVE-2018-20421/
CVE-2018-19834	7.5	La plataforma Ethereum, en concreto la que trabaja con tokens ERC20, dispone de una función, BOMBBA (BOMB), vulnerable. Esto es debido a que los atacantes pueden modificar el propietario del token (contrato inteligente), porque la función no comprueba la identidad de quién llama a la función.	Robo de identidad	https://github.com/SmartContractResearcher/SmartContractSecurity/blob/master/New%20Vulnerabilities%20Allow%20Anyone%20to%20Own%20Certain%20ERC20-Based%20Smart%20Contracts(CVE-2018-19830%2C%20CVE-2018-19831%2C%20CVE-2018-19832%2C%20CVE-2018-19833%2C%20CVE-2018-19834)/README.md	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19834 https://nvd.nist.gov/vuln/detail/CVE-2018-19834

Identificador	Severidad (0-10)	Descripción	Impacto	Referencia principal	Más detalle
CVE-2018-19831	7.5	Cryptbond Network (CBN) implementa contratos inteligentes en la plataforma Ethereum, en concreto la que trabaja con tokens ERC20. Utilizan la función ToOwner() y ésta permite a un atacante cambiar el propietario del token (contrato inteligente), porque la función no comprueba la identidad de quién llama a la función.	Robo de identidad	https://github.com/SmartContractResearcher/SmartContractSecurity/blob/master/New%20Vulnerabilities%20Allow%20Anyone%20to%20Own%20Certain%20ERC20-Based%20Smart%20Contracts(CVE-2018-19830%2C%20CVE-2018-19831%2C%20CVE-2018-19832%2C%20CVE-2018-19833%2C%20CVE-2018-19834)/README.md	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19831
CVE-2018-17968	5.0	La implementación de una plataforma de apuestas, creada sobre Ethereum por Ruletkalo, contempla una función que pretende ser aleatoria [random()]. Dicha función genera un valor predecible de detectar en el contrato inteligente (la apuesta).	Manipulación de apuestas	https://github.com/TEAM-C4B/CVE-LIST/tree/master/CVE-2018-17968	https://www.cvedetails.com/vulnerability-list/vendor_id-19430/year-2018/Ruletkaio.html https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17968
CVE-2019-15947	5.0	La plataforma Bitcoin Core 0.18.0 guarda, en memoria, los datos de la cartera (wallet.dat), de forma no cifrada por medio de bitcoin-qt. Un atacante podría reconstruir el citado archivo (wallet.dat) del usuario atacado. Esto incluiría saber la clave privada, por medio del comando grep "6231 0500".	Robo de claves	https://gist.github.com/oxagast/50a121b2df32186e0c48411859d5861b	https://www.cvedetails.com/cve/CVE-2019-15947/
CVE-2018-15890	10	La plataforma EthereumJ 1.8.2 contempla un problema en ois.readObject. En concreto, en una clase de java, crypto/ECKey.java. El minado de un nuevo bloque, por un nodo, produce la ejecución arbitraria de comandos del SO en el servidor.	Intromisión en el Sistema y posibilidad de ejecución de comandos	https://github.com/frohoff/ysoserial/ https://github.com/ethereum/ethereumj/issues/1161 https://github.com/ethereum/ethereumj	https://www.cvedetails.com/cve/CVE-2018-15890/ https://nvd.nist.gov/vuln/detail/CVE-2018-15890

3 Identificación de los Riesgos

A continuación, se presentan los riesgos más comunes identificados respecto a blockchain.

- **Riesgos derivados de la naturaleza de las transacciones:**
  - **Race attack:** Se genera un doble gasto debido a que el comerciante acepta el pago como bueno antes de que la transacción haya sido confirmada, lo que le causa perjuicios económicos.
  - **Finney attack:** Ídem que al race attack, con la colaboración de un minero que incluye la transacción fraudulenta en un bloque. Igual que en el caso anterior, afecta al comerciante.
  - **Vector76 attack:** Un minero genera dos nodos con dos transacciones idénticas, una con mayor valor, y otra con menos valor para forzar la aceptación de la de mayor valor. Requiere sacrificar un bloque sin minar. En este caso se ven afectados tanto comerciantes como usuarios como intermediarios.
  - **Alternative history attack:** Un atacante envía una transacción y seguidamente genera un fork con la transacción de vuelta. Consume mucho *hashrate* (recursos computaciones en el cálculo de hashes de bloques). Afecta a comerciantes.

- **Riesgos derivados del uso de Smart Contracts:**
  - **Dificultad de programar** como triggers las cláusulas del contrato o condiciones del cambio de estado. Lenguaje natural versus lenguaje de programación.
  - **Imposibilidad de cambiar a posteriori** un SmartContract sin provocar un fork de toda la blockchain.
  - Necesidad por parte del Oráculo de **acceso a datos e interpretaciones** del mundo real (contextualización).
  - Problemas con la **disponibilidad de los oráculos** que provocarían la parada de la ejecución de los smartcontracts.
  - Problemas inherentes del **lenguaje de programación**, que introducen vulnerabilidades explotables (funciones existentes cuya programación maliciosa da lugar a canalización de fondos, por ejemplo, como ocurrió en el caso del ataque The DAO).
  - **Fallos en la ejecución de los smartcontracts** por errores típicos de programación (tales como no verificar identificadores o tipos de datos).

- **Riesgos tecnológicos asociados a las plataformas y protocolos:**
  - **Concentración de poder** en los coordinadores de los pools de mineros, pudiendo llegar incluso a superar el 51% y a hacerse con el control total de la blockchain.
  - **Seguridad de las credenciales**: Existen riesgos de abuso de las credenciales tanto en la parte cliente (por el almacenamiento de la clave privada sin protección o incluso en la nube en servicios gestionados por intermediario lo que a veces provoca por vulnerabilidades que dichas claves sean expuestas), como en dispositivos hardware vulnerables (muchos de los que se comercializan no están debidamente certificados).
  - **Almacenamiento creciente** sin posibilidad de borrado: Por la propia naturaleza de blockchain, la información se replica en todos los nodos, de

modo que algunas blockchains ocupan TB y TB de información, que seguirá incrementándose.

- **Obsolescencia de la criptográfica**, por el incremento de la potencia de computación o desarrollo de nuevos algoritmos que minen la seguridad proporcionada por la criptografía de curva elíptica y los algoritmos usados actualmente.
- **Dificultad a la hora de escoger la plataforma de blockchain más adecuada**. Hay muchos desarrollos y no todos ellos son opensource. Más bien la tendencia es a desarrollar proyectos ad hoc, esta falta de normalización en la implementación dificulta la "seguridad desde el diseño" debido al gran número de tecnologías y lenguajes de programación empleados. Además, existe cierto grado de "cautividad" si se opta por algunas de las plataformas blockchain actualmente disponibles, pues no están tan abiertas las opciones. Al final, las organizaciones deben minimizar este riesgo que, en cualquier caso, afecta a todas las tecnologías por igual.
- **Riesgos de persistencia indebida de la información**, así como de errores introducidos, ya que no es posible modificar la cadena de bloques a posteriori.

- **Riesgos jurídicos y normativos:**
  - **Ausencia de un sistema jurídico** adaptado a la nueva situación: No se consideran los entornos *"trustless"* (sin autoridad central de confianza) y descentralizados como es el caso de blockchain. Los servicios de blockchain no están sometidos tampoco al Reglamento (UE) 910/2014 (eIDAS) pero no están prohibidos.
  - **Falta de arbitraje**: No hay un marco jurídico para dirimir disputas relacionadas con el uso de blockchain. En España, ciertos colectivos están promocionando la incorporación de un "oráculo judicial" que permita la resolución de controversias en un entorno jurídico reglado por un marco legal completo. La incorporación de este tipo de condicionante, si bien introduce complejidad en la programación de los Smart Contracts, permite incrementar la seguridad jurídica de los usuarios. Incluir un nuevo marco jurídico haría excesivamente compleja su implementación. Este marco jurídico evolucionaria y haría muy difícil su adaptación a posteriori.
  - **La Irreversibilidad de las transacciones se considera un hecho abusivo**: Aunque a menudo la irreversibilidad es deseable, en algunos puede suponer la vulneración de derechos fundamentales y hacer además imposible corregir errores aun cuando hayan sido detectados y probados como tales. Además, legalmente tiene muchas implicaciones.
  - **Abuso de la prestación del consentimiento**, que al estar expresado en términos tecnológicos y no debidamente explicados pueden suponer un abuso para el cliente.
  - **Suplantación de identidad**: Al no contar con una autoridad de certificación y de verificación de la identidad de los participantes y los nodos, pueden darse casos de suplantación ya que la identidad en blockchain es alegada y no se hacen controles de las evidencias necesarias. En países donde la gestión de la identidad está más desarrollada, como es el caso de España y otros muchos países europeos, y donde ya se ha desarrollado un marco robusto de verificación de la identidad en entornos electrónicos, la utilización de estos sistemas introduce riesgos innecesarios de suplantación de identidad o incluso de creación de identidades falsas.
  - **Riesgos financieros**: No adecuación al marco normativo financiero. Vulnera la normativa PSD2 que hace énfasis en el conocimiento de los usuarios (KYC) y en la prevención del blanqueo de capitales. En la actualidad se está realizando una gestión de la identidad de los usuarios asociados a los

servicios de Exchange con el objetivo de incorporar confianza y prevenir delitos amparados en el pseudo-anonimato que provee blockchain.

- **Cumplimiento del GDPR (protección de datos)**: Los derechos de olvido, cancelación y rectificación de los datos no se garantizan en blockchain sobre plataformas públicas ya que pueden acabar habiendo datos personales en transacciones que, por la naturaleza de blockchain, no podrán ser borradas sin provocar un fork sobre toda la plataforma. Esto es especialmente crítico.

- **Perspectiva global de los Riesgos en migración de proyectos estándar a proyectos basados en blockchain:**

  Antes de abordar la migración de un proyecto convencional a uno sobre blockchain es preciso analizar los pros y contras que puede haber, considerando los riesgos descritos anteriormente y los descritos a continuación:

  - **Riesgos del alcance**, precisando exactamente los requisitos y objetivos de la cadena de bloques en el marco del proyecto. Blockchain utiliza herramientas complejas para su implementación, y es preciso hacer una gestión concienciada de las credenciales, así como ser conscientes del gasto energético y de almacenamiento, además de los riesgos tecnológicos específicos de la tecnología.
  - **Riesgos de la planificación**, ya que la novedad de la tecnología de la cadena de bloques tal y como se ha generalizado y difundido puede ocasionar retrasos y problemas de comunicación de requisitos con proveedores y clientes, para lo que se debe planificar un margen. Las implementaciones de cadenas de bloques, debido a su popularidad actual, están reflejando un rápido dinamismo en detección de vulnerabilidades, por lo que es preciso tener en cuenta la necesidad de monitorización y elaboración de correcciones en proyectos que usen esta tecnología.
  - **Riesgos relacionados con los recursos**, ya que la tecnología blockchain es relativamente novedosa y no hay muchos perfiles que tengan suficiente dominio de las competencias y habilidades necesarias. Será preciso además considerar que durante el desarrollo del proyecto se presenten cambios en la situación económica del sector al que se dedica la empresa o cambios macroeconómicos
  - **Riesgos relacionados con la confidencialidad y privacidad de la información**, para lo que se deberá de realizar un análisis exhaustivo de gestión y acceso a la información y las posibles necesidades de cifrado previo (total o parcial) a la introducción en la cadena de bloques.
  - **Riesgo de volatilidad de los precios**, si usamos una blockchain pública, ya que el valor del premio de la criptomoneda usada para pagar el minado de las transacciones fluctúa libremente.
  - La **gestión de las identidades y acceso** es crucial para garantizar la seguridad de la blockchain. Con una blockchain privada es preciso evaluar la implantación de una PKI propia o el uso de una PKI reconocida con un prestador de servicios de confianza cualificado (qTSP, según sus siglas en inglés), lo que podría convertir a una blockchain más en una DLT que en una blockchain.

4 Marco para el control de Riesgos

Un Marco de Control de Riesgos es el conjunto de procedimientos en base a estándares o metodologías de gestión de riesgos que detalla el **procedimiento de identificación, evaluación, gestión y monitorización de los riesgos para un determinado proceso o elemento clave para una organización**. Al ser los procesos basados en blockchain, como hemos visto, susceptibles de un determinado tipo de riesgos, también **deben estar tanto la metodología como el proceso de gestión adaptados a la misma**. La metodología empleada es la orientada a escenarios de riesgos, donde se plantean cómo se pueden materializar los riesgos, la facilidad de dicha materialización, el impacto que podría suponer junto con qué perfil de atacante o vulnerabilidad estaría detrás del mismo. Los controles asociados serían tanto detectivos como preventivos, reactivos (mitigadores, supresores) y cómo actuarían sobre el riesgo en cuestión.

Los escenarios de riesgo deben ser identificados, analizados y gestionados **periódicamente**. La periodicidad en un entorno tecnológico como blockchain debe ser continua en el caso de blockchain públicas y con una periodicidad algo menor en el caso de las privadas, en base a cuán expuesta esté la blockchain corporativa.

Como todos los procedimientos que siguen el ciclo de Deming se debe dar de forma retroalimentadas las fases de **(1) Identificación de escenarios de riesgos (2) Evaluación de dichos escenarios (3) Gestión de Riesgos (4) Monitorización y optimización del proceso.**

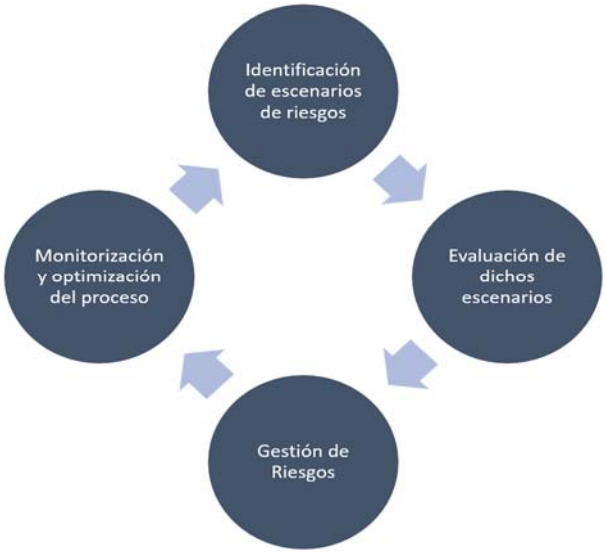

Ilustración 1: Marco de control de riesgos

La mayor parte de los riesgos sobre los que hay que actuar son debidos al uso de blockchains públicas donde las reglas del juego están predefinidas. A continuación, se muestra la tabla con el marco propuesto y los controles a gestionar según lo descrito en el capítulo 3:

Origen	Categoría	Escenarios de riesgo [ER]	Controles	Cumplimiento	Disponibilidad	Privacidad Confidencialidad	Integridad	Autenticación y Trazabilidad
Riesgos Operaciones de los procesos validados con blockchains públicas **[RT]**	**Fraude**	**[ER1-RT]** Pago de la comisión por la transacción y luego no se confirma (pierde dinero el cliente transaccional)	**[C1]** Se respetan los tiempos de validación y verificación de todas las transacciones emitidas previa a su publicación	**X**			**X**	**X**
	Fraude	**[ER2-RT]** El cliente final consigue no pagar la comisión (y el minero tiene que asumir la pérdida de la comisión. Esto ocurre con transacciones por valor de lo que hay en la cuenta, y mineros que validan la transacción antes de cobrar la comisión)	**[C2]** Se establece el principio de responsabilidad individual, determinando lo que realiza cada usuario.	**X**		**X**	**X**	**X**
	Fraude	**[ER3-RT]** Un minero trata de añadir un bloque a la cadena, siempre eligiendo la transacción que más le beneficie (competencia desleal sin respetar orden de llegada)	**[C3]** Se revisan los registros de los dispositivos y sistemas asociados	**X**				**X**
	Hacktivismo	**[ER4-RT]** Un atacante trata de romper la cadena oficial de bloques, generando entonces	**[C4]** Control de los mecanismos de consenso en la blockchain	**X**			**X**	

Origen	Categoría	Escenarios de riesgo [ER]	Controles	Cumplimiento	Disponibilidad	Privacidad Confidencialidad	Integridad	Autenticación y Trazabilidad
		otra cadena alternativa (toma el control de los bloques sucesivos)						
Riesgos para el Negocio debido al uso de **los Smarts Contracts** en blockchains públicas **[RSC]**	**Empresarial**	**[ER1-RSC]** Dificultad para automatizar (programar) algunas cláusulas exigidas por alguna de las partes	**[C5]** Aplicar Metodologías de Especificación funcional (Verificación de pre y post condiciones)	**X**	**X**	**X**	**X**	**X**
	Empresarial	**[ER2-RSC]** La no posibilidad de modificar un Smart Contract después de que se haya firmado	**[C6]** Control de la operación de hard y soft forks por una autoridad superior en la blockchain	**X**			**X**	
	Operaciones	**ER3-RSC]** Fallo de implementación (parámetros de configuración/programación) de un Smart Contract	**[C7a]** Calidad del software: Aplicar herramientas de verificación de código dinámico		**X**		**X**	
	Empresarial	**[ER4-RSC]** Un atacante utiliza de manera maliciosa una función legítima habitual en SC	**[C7b]** Calidad del software: Verificar el código utilizando como referencia repositorios de vulnerabilidades identificadas del lenguaje	**X**			**X**	
Riesgos Tecnológic	**Concienciación**	**[ER1-RTG]** Falta de conocimiento y formación en la gestión de las claves privadas	**[C8]** Formación y Concienciación en el uso de las claves	**X**		**X**		**X**

Origen	Categoría	Escenarios de riesgo [ER]	Controles	Cumplimiento	Disponibilidad	Privacidad Confidencialidad	Integridad	Autenticación y Trazabilidad
os Generales **[RTG]**	**Fraude**	**[ER2-RTG]** Vulnerabilidades en las aplicaciones de los monederos electrónicos que pueden ser empleadas para robos	**[C9]** Certificación funcional y criptológica de las aplicaciones por una entidad acreditada (CCN en España, por ejemplo)	**X**	**X**	**X**	**X**	**X**
	Fraude	**[ER3-RTG]** Vulnerabilidades en los monederos electrónicos implementados en hardware	**[C10]** Certificación de los dispositivos por una entidad acreditada (CCN, por ejemplo)	**X**	**X**	**X**	**X**	**X**
	Empresarial	**[ER4-RTG]** Falta de mantenimiento software de las blockchains por falta de estandarización y/o colaboración (muchos lenguajes de programación)	**[C11]** Se efectúa un control de cambios en mantenimiento de aplicaciones y de las configuraciones de control	**X**	**X**	**X**	**X**	**X**
	Fraude	**[ER5-RTG]** Posibilidad de suplantar la identidad de un usuario de la red blockchain porque no existe una Autoridad de Certificación centralizada	**[C12]** Se establece un procedimiento de autorización y seguimiento de las Altas y Bajas de usuarios	**X**	**X**	**X**	**X**	**X**
	Privacidad	**[ER6-RTG]** Exposición de identidades en internet por revelación de IPs contra claves públicas	**[C13]** Se define, implanta y se revisa periódicamente los estándares y configuraciones de seguridad de los sistemas frontera con internet	**X**		**X**	**X**	**X**

Origen	Categoría	Escenarios de riesgo [ER]	Controles	Cumplimiento	Disponibilidad	Privacidad Confidencialidad	Integridad	Autenticación y Trazabilidad
	Disponibilidad	**[ER7-RTG]** Ataques DoS a la red blockchain aunque la capacidad de resiliencia es una de sus fortalezas estrella.	**[C14]** Se define e implanta el ciclo de tratamiento contra los ataques DoS		**X**			**X**
	Disponibilidad	**[ER8-RTG]** Colapso de la red debido al elevado número de transacciones a gestionar (falta de recursos computacionales)	**[C15]** Se analiza y concluye sobre las necesidades de disponibilidad y continuidad de los dispositivos	**X**	**X**			**X**
	Fraude	**[ER9-RTG]** Hackeo masivo de las claves de los monederos y/o claves privadas almacenadas en la nube	**[C16a]** Se asegura la existencia de credenciales y contraseñas y su correcto mantenimiento (cifrado)	**X**	**X**	**X**	**X**	
	Fraude	**[ER10-RTG]** Explotación de obsolescencia criptográfica para la obtención de claves privadas a partir de las públicas, obteniendo control de las carteras	**[C16b**] Monitorización de avances tecnológicos para la revocación y reemisión de credenciales si se materializa el riesgo.			**X**	**X**	**X**
Riesgos Jurídicos y Normativos **[RJN]**	**Legal**	**[ER1-RJN]** No hay un sistema jurídico adaptado para proteger y arbitrar posibles disputas entre los usuarios que utilizan blockchain	**[C17]** Se define, se implanta y se revisa periódicamente el procedimiento de mediación, debido a conflictos entre usuarios	**X**		**X**	**X**	**X**
	Legal	**[ER2-RJN]** La irreversibilidad de las transacciones podría vulnerar los derechos	**[C18]** Se define, implanta y se revisa periódicamente los estándares y configuraciones de seguridad	**X**	**X**	**X**	**X**	**X**

Origen	Categoría	Escenarios de riesgo [ER]	Controles	Cumplimiento	Disponibilidad	Privacidad Confidencialidad	Integridad	Autenticación y Trazabilidad
		fundamentales y la imposibilidad de corregir errores posteriores						
	Concienciación	**[ER3-RJN]** Podría ocurrir que los clientes no tuvieran el conocimiento suficiente en tecnología y por ello no se asegurarían las garantías suficientes por el posible abuso contra el cliente	**[C19]** Se efectúan programas de formación (concienciación) y entrenamiento a la población	**X**		**X**	**X**	**X**
	Cumplimiento	**[ER4-RJN]** El no cumplimiento de la normativa financiera PSD2	**[C20]** Se implanta y se revisa periódicamente la normativa PSD2	**X**	**X**			**X**
	Cumplimiento	**[ER5-RJN]** El no cumplimiento de la normativa de privacidad GDPR	**[C21]** Se implanta y se revisa periódicamente la normativa GDPR	**X**		**X**	**X**	**X**
	Fraude/Cumplimiento	**[ER6-RJN]** No hay un marco de control antifraude definido	**[C22]** Se define un marco de control antifraude	**X**		**X**	**X**	**X**
Riesgos a Nivel Económico, Orden Público	**Economía Mundial**	**[ER1-RNM]** Posible quiebra de la economía de todos los países que estén utilizando blockchain como medio operativo de las transacciones financieras o validación de procesos industriales críticos.	**[C23]** Se han definido y formalizado políticas, normas y procedimientos que aseguren un nivel de seguridad adecuado	**X**	**X**	**X**	**X**	**X**

Origen	Categoría	Escenarios de riesgo [ER]	Controles	Cumplimiento	Disponibilidad	Privacidad Confidencialidad	Integridad	Autenticación y Trazabilidad
(Mundial) **[RNM]**	**Hacktivismo**	**[ER2-RNM]** Robos o pérdidas masivas de dinero a conjuntos de la población localizados.	**[C24]** Se protege a las personas ante ciberataques	**X**	**X**	**X**		**X**
	Ciberguerra	**[ER3-RNM]** Desestabilización (orden social) de uno o varios países que estén utilizando blockchain como medio operativo de las transacciones financieras.	**[C25]** Existe un control de Seguridad física		**X**	**X**	**X**	**X**
	Ciberterrorismo	**[ER4-RNM]** Financiación ilegal a grupos terroristas, bandas criminales, etc.	**[C26]** Se monitoriza el funcionamiento de los dispositivos			**X**		**X**
	Economía Mundial	**[ER5-RNM]** Especulación para el beneficio global desmesurado de unos pocos grupos de interés.	**[C27]** Se conciencia a la población y se educa en valores para el progreso y mantenimiento ejemplar y el compañerismo	**X**			**X**	
	Fraude	**[ER6-RNM]** Delitos monetarios como el blanqueo o evasión de capitales.	**[C28]** Se controla la ejecución de las tareas planificadas			**X**		**X**
	Hacktivismo	**[ER7-RNM]** Grupo organizado de poder entre los mineros (>50%) y con ello haciéndose con el control total de la blockchain.	**[C29]** Se supervisa el entorno de control de los servicios externalizados	**X**	**X**	**X**	**X**	**X**

Origen	Categoría	Escenarios de riesgo [ER]	Controles	Cumplimiento	Disponibilidad	Privacidad Confidencialidad	Integridad	Autenticación y Trazabilidad
	Técnica	**[ER8-RNM]** Falta de suministro eléctrico suficiente para abastecer alguna zona geográfica entre los ciudadanos	**[C30]** Se ha dimensionado correctamente la infraestructura de suministro a la población y ésta es compatible con las estaciones de suministro disponibles en los ciudadanos	**X**	**X**			
	Fraude	**[ER9-RNM]** Falta de honradez de algunos ***exchanges***	**[C31]** Se establece la segregación de responsabilidades organizativas, con sus claras funciones y con la necesaria auditoría periódica independiente	**X**	**X**	**X**	**X**	**X**

5 Implementación de un modelo de control en entornos blockchain

Una vez estructurado el Marco de Control de Riesgos, pasamos a implementar su modelo de control.

En primer lugar, es preciso determinar **quién o quienes deben implementar los Controles de Riesgos**. En el caso de las blockchain públicas (Bitcoin, Ethereum, etc.) no existe una autoridad de control como tal que pueda asegurar la implantación de los controles. Tan sólo existe una idea de quorum o cuota superior al 50% que hace que se validen los forks, que serían precisos para implementar muchos de los controles necesarios.

En el caso de las blockchain de consorcio (Alastria, por ejemplo), debería ser tomada la decisión por la mayoría de los nodos participantes e impuestos dichos controles.

En el caso de las blockchain corporativas (la mayoría de los casos de implementación de blockchains con propósitos empresariales, nuestro consejo es que la decisión debería recaer en Negocio (CEO) frente al hábito de tomarla TI (CIO) , amparándose en este caso en lo complejo de la tecnología.

El motivo es que no estamos ante un control de activos de TI sin consecuencia sino que estamos tratando procesos de negocio y estamos tomando alternativas que, como ya hemos visto, impactan no sólo en un proceso en particular sino en toda una organización.

Otra cosa es que la implantación de este modelo tenga consecuencias en TI y deban estar alineados perfectamente (filosofía de COBIT). De este modo, proponemos este marco de gobernanza a elegir (COBIT2019), que cubriría la mayoría de los controles detectados.

A continuación, se ofrece el mapeo de los controles del capítulo anterior contra los controles, objetivos o procesos de Cobit2019

CONTROL	COBIT 2019	COMENTARIOS
[C1] Se respetan los tiempos de validación y verificación de todas las transacciones emitidas previa a su publicación	**BAI.07** Gestionar la aceptación y la transición de los cambios de TI **APO.14** Gestionar los Datos	Se puede enfocar la validación de una transacción como la verificación de datos críticos para el negocio
[C2] Se establece el principio de responsabilidad individual, determinando lo que realiza cada usuario (prevención de usuarios genéricos)	**APO.03** Gestionar la Arquitectura Empresarial	Trazabilidad de acciones, se supone englobado en lo que se considera la Arquitectura Empresarial
[C3] Se revisan los registros de los dispositivos y sistemas asociados	**BAI.10** Gestionar la configuración	Se supone que se trata de controlar los activos, su situación y su funcionamiento adecuado
[C4] Control de los mecanismos de consenso	**EDM.01** Asegurar el establecimiento y el mantenimiento del marco de gobierno	Se trata de que exista gobernanza en el control de las reglas y políticas globales de la blockchain, en particular las que afectan a transacciones
[C5] Aplicar Metodologías de Especificación funcional (Verificación de pre y post condiciones)	**BAI.07** Gestionar la aceptación y la transición de los cambios de TI	Se trata de incluir las reglas de aceptación de las aplicaciones y mecanismos software
[C6] Control de la operación de hard y soft forks por una autoridad superior en la blockchain	**BAI.06** Gestionar los cambios de TI	Hard y soft forks se consideran cambios con impacto significativo.

CONTROL	COBIT 2019	COMENTARIOS
[C7a] Calidad del software: Aplicar herramientas de verificación de código dinámico	**APO.11** Gestionar la calidad, **APO13** Gestionar la seguridad	Calidad y seguridad mediante la verificación del código dinámico
[C7b] Calidad del software: Verificar el código utilizando como referencia repositorios de vulnerabilidades identificadas del lenguaje	**APO13** Gestionar la seguridad	Calidad y seguridad mediante la verificación de las vulnerabilidades (por ejemplo con OWASP o similares ref.)
[C8] Formación y Concienciación en el uso de las claves	**BAI.10** Gestionar la configuración	Se trata de dar las pautas sobre el manejo del activo Claves.
[C9] Certificación funcional y criptológica de las aplicaciones por una entidad acreditada (CCN en España, por ejemplo)	**MEA.03** Gestionar el cumplimiento de los requerimientos externos **MEA.04** Gestionar el aseguramiento	Se diferencia del control C7 en que en este caso se aborda un proceso de verificación formal con una entidad externa por lo que se supone que se controlan los procesos conforme a los estándares externos
[C10] Certificación de los dispositivos por una entidad acreditada (CCN, por ejemplo)	**MEA.04** Gestionar el aseguramiento	Sería una acreditación de los sistemas empleados
[C11] Se efectúa un control de cambios en mantenimiento de aplicaciones y de las configuraciones de control	**BAI.06** Gestionar los cambios de TI	Mantenimiento controlado en situaciones en las que no se suele controlar
[C12] Se establece un procedimiento de autorización y seguimiento de las Altas y Bajas de usuarios	**APO.02.02** Gestionar el personal contratado y **APO.02.03** Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización	Se entiende que los usuarios propios de la organización. Del acceso a los sistemas en general sería DSS.02.01 (Gestionar la identidad del usuario y el acceso lógico)
[C13] Se define, implanta y se revisa periódicamente los estándares y configuraciones de seguridad de los sistemas frontera con internet (Seguridad Perimetral)	**DSS0.6** Gestionar los controles de los procesos de negocio	Mantener la integridad de la información y los controles
[C14] Se define e implanta el ciclo de tratamiento contra los ataques DoS	**DSS.05** Gestionar los servicios de seguridad	Se minimiza el impacto de incidentes críticos como este del DoS
[C15] Se analiza y concluye sobre las necesidades de disponibilidad y continuidad de los dispositivos	**DSS.04** Gestionar la Continuidad	Adaptación rápida para mantener los procesos de negocio críticos
[C16a] Se asegura la existencia de credenciales y contraseñas y su correcto mantenimiento	**BAI.10** Gestionar la configuración y **DSS.05** Gestionar los servicios de seguridad	Configuración porque se tratan de datos importantes y servicios de seguridad en cuanto al mecanismo de autenticación.
[C16b] Monitorización de avances tecnológicos para la revocación y reemisión de credenciales si se materializa el riesgo.	**DSS.04** Gestionar la Continuidad **APO12.01** Factores y elementos de riesgos emergentes	Planificación de actuaciones en caso de obsolescencia criptográfica, así como la evaluación de los avances para poner en práctica el plan de continuidad
[C17] Se define, se implanta y se revisa periódicamente el procedimiento de mediación, debido a conflictos entre usuarios	**DSS.02** Gestionar las peticiones y los incidentes del servicio	Resolución de peticiones contradictorias, problemas, etc.
[C18] Se define, implanta y se revisa periódicamente los estándares y configuraciones de seguridad (en general, teórico, arquitectura)	**DSS.05** Gestionar los servicios de seguridad	Se trata de comprobar que los recursos de TI dedicados a garantizar la seguridad funcionan correctamente.
[C19] Se efectúan programas de formación (concienciación) y entrenamiento a la población	**BAI.08** Gestionar el conocimiento	Proporcionar la información a todos los interesados para poder tomar decisiones y hacer uso de los recursos de TI adecuadamente.

CONTROL	COBIT 2019	COMENTARIOS
[C20] Se implanta y se revisa periódicamente la normativa PSD2	**EDM.01** Asegurar el establecimiento y el mantenimiento del marco de gobierno	Normativa de doble factor en las transacciones, entre otras cosas
[C21] Se implanta y se revisa periódicamente la normativa GDPR	**APO.14** Gestionar los Datos	En concreto, los datos de carácter personal
[C22] Se define un marco de control antifraude	**EDM.01** Asegurar el establecimiento y el mantenimiento del marco de gobierno	Incorporar al marco de control los elementos antifraude
[C23] Se definen y formalizan políticas, normas y procedimientos que aseguren un nivel de seguridad adecuado	**APO.01** Gestionar el marco de gestión de TI	Las políticas y normas son parte del marco de gestión.
[C24] Se protege a las personas ante ciberataques	**DSS.05** Gestionar los servicios de seguridad	Se supone que los servicios de seguridad protegen a todos.
[C25] Existe un control de Seguridad física	**DSS.01.02** Gestionar el Entorno e instalaciones **DSS.02.02** Gestión y control del acceso a los CPDS	Gestión de las operaciones en general, gobernado por MEA04. El acceso dependerá de si es propio o no, en cualquier caso estamos hablando de controlar el acceso a los equipos de procesamiento, y esto es complejo si muchos nodos no son corporativos sino particulares.
[C26] Se monitoriza el funcionamiento de los dispositivos	**BAI.10** Gestionar la configuración	Monitorización
[C27] Se conciencia a la población y se educa en valores para el progreso y mantenimiento ejemplar y el compañerismo	**APO.08** Gestionar las relaciones	Facilitar el conocimiento, habilidades y comportamientos correctos
[C28] Se controla la ejecución de las tareas planificadas	**DSS.01** Gestionar las operaciones	Gestión de la ejecución de las tareas.
[C29] Se supervisa el entorno de control de los servicios externalizados	**APO.10** Gestionar los proveedores	Adicionalmente podría aplicar **APO.09** Gestionar los Acuerdos de Nivel de Servicio
[C30] Se ha dimensionado correctamente la infraestructura de suministro a la población y ésta es compatible con las estaciones de suministro disponibles en los ciudadanos	**BAI.04** Gestionar la disponibilidad y la capacidad	Se diferencia de continuidad en se trata de capacidad.
[C31] Se establece la segregación de responsabilidades organizativas**,** con sus claras funciones y con la necesaria auditoría periódica independiente	**DSS.02.03** Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización	Equivalentemente APO01.02. Establecer roles y responsabilidades, pero este control afecta sólo a TI y el control debe ser a nivel global

Recomendaciones generales para implementar procesos empresariales:

- En primer lugar, realizar un análisis riguroso de los riesgos asociados a blockchain y el desarrollo de un plan de mitigación de los mismos.
- En segundo lugar, normalizar la arquitectura de uso de la tecnología.
- Incorporar los sistemas que vayan a hacer uso de la plataforma blockchain como para del propio sistema ISMS a nivel organizaciones, para garantizar que, al menos, se llevan a cabo las mismas medidas de mitigación que para el resto de sistemas.
- Utilizar blockchains públicas únicamente en procesos no críticos para la organización, considerando los datos que se van a introducir en las cadenas de bloques y el impacto de normativas transversales (como GDPR, PSD2, PCIDSS, etc.). Priorizar si es posible la utilización de blockchain privadas en las que la entidad puede tener algún control sobre los cambios, la identidad y la ubicación física y lógica de los nodos.

- En caso de utilizar blockchains de consorcio, asegurarse de que implemente eficazmente los controles propuestos.
- Control de identidades a nivel empresarial, PKI propia o bien de una Autoridad de Certificación, nunca embebida o generada por la propia aplicación de blockchain (que se suele dar cuando se usan blockchains públicas).
- En el caso de utilizar aplicaciones monedero, que sean certificadas y auditarlas para detectar problemas.
- Segregación de tareas a la hora de controlar las claves. Claves protegidas con contraseña y almacenadas en sitio diferente al de su explotación.
- Si se usa hardware para monederos y/o generación de claves que sea certificado (CCN o similar).
- Hay que tener cuidado con los protocolos y aplicaciones criptográficas. Existe un riesgo latente para la criptografía asimétrica a un horizonte todavía lejano de posible rotura por computación cuántica, pero hemos considerado que es muy difícil de poner en contexto, porque sería realmente un cisne negro o gris. Sin embargo, sí que hay que considerar los riesgos que introducen las implementaciones deficientes que se pueden encontrar a día de hoy.
- Verificar los mecanismos de implementación de forks. Que se puedan implementar y cómo y por quién.
- Controlar el código fuente y verificar la seguridad del usado en la programación de Smart contracts.
- Verificar las especificaciones funcionales usadas para la programación de Smart Contracts.

$