El mito de la seguridad del *blockchain*

El pasado 6 de marzo, Schneier On Security se hizo eco de las vulnerabilidades de los *smart contracts* basados en *blockchains* como Ethereum[1]. Uno de los paradigmas de la seguridad lógica, la capacidad de parcheado del código tras el descubrimiento de vulnerabilidades, parece inaplicable a un código cuya principal virtud es su inmutabilidad. Este desajuste conceptual es uno de los ejemplos de la falta de un análisis riguroso de la seguridad asociada a *blockchain*, una tecnología que se extiende por las organizaciones en forma de pilotos rápidos o pruebas de concepto, muchas veces para dar salida a las necesidades de agilidad de los responsables del negocio, y típicamente fuera del control de los departamentos de seguridad.

Juan Jesús León Cobos

Es habitual, a la hora de escribir sobre la seguridad de cualquier tecnología, presentarla inicialmente para poder tener un marco de referencia sobre el cual reflexionar. Sin embargo la tecnología *blockchain* es compleja –según algunos artículos de la prensa generalista, hasta "mágica"– e introducirla aquí sería muy largo. Para establecer a qué nos referimos con *blockchain* nos remitimos a la publicación borrador del NIST "Blockchain Technology Overview"[2] y utilizaremos los conceptos que allí se definen, particularmente el de Proof of Work (PoW) y el de consenso.

El *blockchain* corporativo

Por motivos de espacio tendremos que acotar nuestro análisis de seguridad. Nos centraremos en la utilización de la tecnología por la administración pública y la gran empresa. Hablaremos entonces del *blockchain* corporativo[3].

Debemos distinguir el *blockchain* corporativo del uso corporativo de los *blockchain* asociados a las criptomonedas. Los usos corporativos más naturales de los *blockchain* asociados a criptomonedas serían el uso de "Smart Contracts" en monedas tipo Ethereum y el registro y publicación de transacciones (u otra información) en el "ledger" de una moneda. Los conflictos conceptuales en la seguridad de los "Smart Contracts" a los que hacíamos referencia en la cabecera, y la incertidumbre en el coste[4] del registro y publicación de transacciones en los "ledgers" de las criptomonedas, junto con la progresiva centralización de la minería, hacen poco probable, en opinión de autor, que las grandes corporaciones adopten a gran escala estos usos en el corto plazo. No vamos a analizar por tanto la seguridad de las criptomonedas[5], sobre la cual existen numerosas referencias.

Nos centraremos pues en las soluciones de *blockchain* corporativo que se puedan desplegar en una organización o en varias de manera coordinada[6]. Los definiremos como aquellos esquemas que no tienen una criptomoneda asociada y que se basan en modelos de consenso alternativos al PoW[7].

La alternativa al Proof of Work

Los modelos de consenso basados en PoW incorporan por diseño una serie de ventajas en materia de seguridad (véase la **Figura 1**). Los *blockchain* corporativos, asumiendo que no están asociados a una criptomoneda, no pueden incorporar PoW, al no existir un modelo de recompensa que justifique el gasto asociado a la búsqueda de *hashes*. Así nacen los modelos de consenso alternativos al PoW (véase la **Figura 2**). Estos modelos esencialmente intentan garantizar la consistencia en el sistema de computación distribuido y a la vez prevenir los ataques de nodos potencialmente maliciosos. Sin embargo estos modelos tienen siempre fuertes carencias frente al PoW, y están menos estudiados y probados en la práctica, lo cual introduce incertidumbres[8]. En todo caso no tenemos aquí espacio para explicar las ventajas o inconvenientes de cada modelo de consenso no-PoW, de los cuales por otra parte surgen nuevos cada día.

Fabricando un *blockchain* casero

Para analizar los riesgos asociados a la tecnología de *blockchain* corporativo estableceremos una comparativa frente a una combinación de tecnologías conocidas que proporcionen la misma funcionalidad. No todo el mundo es consciente de que la funcionalidad que se consigue con un *blockchain* sin PoWse puede conseguir combinando un repositorio de datos distribuido y una PKI, por ejemplo.

Supongamos entonces que deseamos orquestar un servicio entre varias entidades, al cual todas las entidades puedan acceder: Las entidades podrán enviar cierto tipo de "transacciones", las cuales deben ser sometidas a ciertas comprobaciones. Una vez comprobadas, serán agrupadas en "documentos", los cuales serán firmados y publicados con una periodicidad establecida. Estableceremos un mecanismo para comprobar la integridad de los documentos una vez publicados. Las entidades deberán también acordar un esquema de autorizaciones de acceso al contenido de los documentos.

Este es un ejemplo clásico de lo que uno querría lograr con un *blockchain* corporativo. Una forma de organizarlo sería que cada entidad dispusiera de un nodo con su copia de la información relevante, la capacidad de proponer transacciones, de realizar las

[1] "Finding The Greedy, Prodigal, and Suicidal Contracts at Scale", Nicolic et al. 16 Feb 2018

[2] "Blockchain Technology Overview", NISTIR 8202, Draft Enero 2018, https://csrc.nist.gov/publications/detail/nistir/8202/draft

[3] Enterprise Blockchain en la literatura

[4] Siempre habrá un coste, por un lado porque el consenso en las criptomonedas se basa en un modelo de incentivos, y por otro porque el modelo PoW que restringe la creación de bloques tiene un gasto asociado inevitable por bloque. Sin embargo no existen aún modelos teóricos claros sobre cómo va a evolucionar este coste con el tiempo.

[5] En todo caso son fascinantes los esquemas probabilísticos de confirmación frente a los ataques conocidos como "doublés pending", o los riesgos de toma de control basados en teoría de juegos.

[6] Conocidos también como blockchains privados y de consorcio, respectivamente.

[7] No consideramos tampoco modelos alternativos al PoW que incorporen parcialmente PoW, como por ejemplo el de PoA (Proof of Activity). En todas sus versiones el PoW tiene enormes costes asociados, que sólo parecen sostenibles mediante la creación controlada de criptomonedas.

[8] Existen análisis clásicos sobre la problemática del consenso en la computación distribuida, pero más dirigidos a establecer lo que resulta imposible alcanzar que a proporcionar soluciones prácticas.

Figura 1.- Resumen de las ventajas del PoW en aspectos de seguridad, de las cuales carecen a priori los *blockchain* corporativos.

comprobaciones oportunas y de proponer documentos. Un modelo de consenso entre los nodos deberá gestionar la coherencia del conjunto de documentos que se va generando. En todo caso estas entidades tienen bastantes cosas sobre las que ponerse de acuerdo, lo cual no siempre resulta sencillo, sobre todo si hablamos de muchas entidades[9]. También deberá cada entidad nominar ciertos responsables del proceso y gestionar cada una su propio nodo.

Como fórmula alternativa, digamos que las entidades acuerdan simplemente establecer un equipo de personas en el cual confían y dotarles de un presupuesto. Este equipo despliega un servicio en la nube, con servicios remotos de propuesta de transacciones al cual las entidades acceden. El servicio publica los documentos y firma el conjunto de los mismos de forma periódica. Asimismo gestiona el acceso a la información de los usuarios de las entidades. Esta será nuestra "solución clásica" que utilizaremos para comparar.

Hay que mencionar que la distinción entre los *blockchain* corporativos y nuestra solución clásica es meramente teórica. Cada vez surgen más soluciones que se presentan como *blockchain* corporativo a la vez que incorporan una mezcla de tecnologías "*no-blockchain*", desde centralización del cómputo hasta autoridades de certificación. Para nuestro ejercicio de comparación asumiremos que para que una solución sea calificable como *blockchain* corporativo al menos tenga tres características:

- Que el cómputo asociado al *blockchain* esté descentralizado en nodos que se comuniquen entre sí (*peer-top-peer*).
- Que no tenga un esquema de gobierno centralizado, sino un esquema de acuerdo por consenso (que no esté basado en PoW).
- Que no tenga, en definitiva, una Autoridad en la que sea necesario confiar.

No parece que, desde el punto de vista de la seguridad, el blockchain corporativo sea mejor que las soluciones clásicas, al menos a primera vista. Antes al contrario, mucho indica que para el responsable de seguridad, la proliferación de blockchains es un desafío, como lo es la falta de personal y de empresas especializadas en la seguridad de los mismos.

Vamos a estudiar ahora la influencia de estas características frente a la solución clásica en diversos aspectos de la seguridad. Analizaremos aspectos del modelo de gobierno de la seguridad, aspectos de la seguridad de los datos tales como disponibilidad, integridad, confidencialidad, y finalmente otros relacionados con las operaciones de seguridad.

Modelo de gobierno de la seguridad

Empezamos por repasar algunas de las ventajas atribuidas al *blockchain* frente a nuestra solución clásica, desde el punto de vista del gobierno de la seguridad.

El mayor logro del *blockchain* es el abandono de la necesidad de una autoridad. Este abandono no parece una ventaja por sí. Desde el punto de vista de la seguridad, para saber si es mejor poner los huevos en muchos cestos o en uno solo (y vigilar bien ese cesto), necesitaríamos conocer la seguridad de cada cesto. El *blockchain* sustenta su seguridad en que el modelo de cooperación entre nodos es inviolable frente a nodos maliciosos, salvo que sean muchos. El modelo PoW garantiza, en efecto, que la creación masiva de nodos maliciosos no

[9] Salvo, claro está, que una entidad domine a las demás y establezca sus reglas, mientras que el resto pueden adherirse o no.

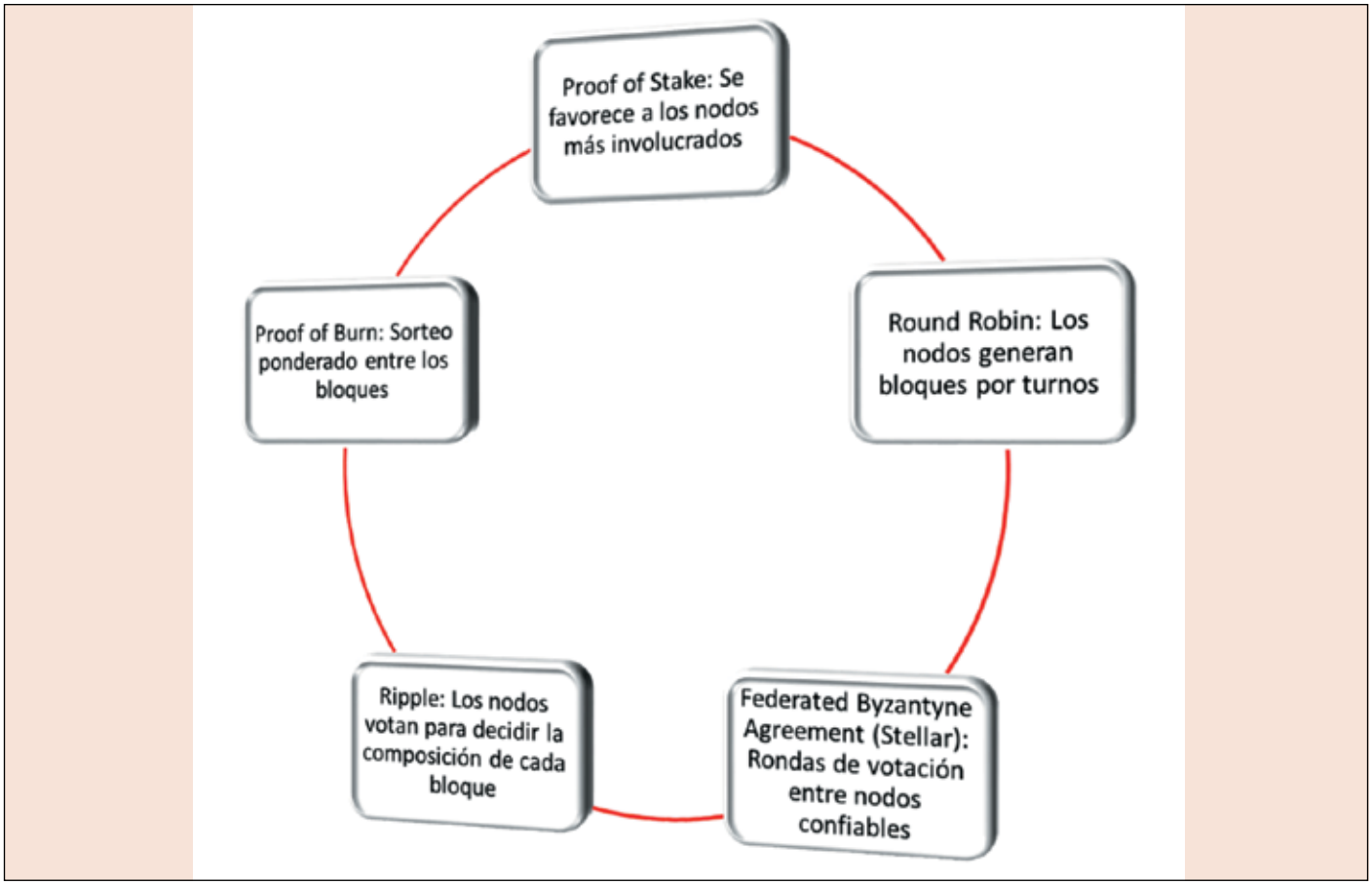

Figura 2.- Modelos de consenso alternativos para decidir qué nodo genera cada bloque y resolver conflictos (a vista de pájaro).

proporciona una ventaja, imposibilitando el llamado "sybil attack" [10]. En un *blockchain* corporativo la seguridad radicaría en la supuesta dificultad de varias de las entidades participantes para ponerse de acuerdo [11] y en el diseño del modelo de consenso y del software asociado.

No queda claro que gestionar la seguridad de cada equipo de cada entidad resulte más sencillo o barato que gestionar la seguridad del único equipo que gestiona nuestra solución clásica. En el caso del equipo unificado será necesario establecer controles internos. Es posible que crear este equipo sea, desde un punto de vista operativo de las entidades, más difícil que lograr que cada entidad cree y gestione su propio equipo. Pero el modelo de seguridad que mejor conocemos es el de la gestión de la seguridad en un equipo gestionado bajo una autoridad.

El modelo de seguridad del *blockchain*, por otro lado, requiere una confianza casi absoluta en que la solución tecnológica no permite a un nodo malicioso aprovecharse de los demás. Pero la realidad es que, a día de hoy, los modelos de consenso que no se basan en PoW no proporcionan esa seguridad. Incluso si existiera tal modelo, necesitaríamos un mecanismo para arbitrar un conflicto de consistencia. En teoría no debe darse tal conflicto, pero en la práctica asumir tal cosa equivale a depositar también plena confianza en que el software que automatiza el modelo no tiene fallos.

El problema de las vulnerabilidades del software, en el caso de un blockchain, parece de solución complicada. Las entidades responsables de los nodos deberán coordinar entre sí las puestas en producción de nuevas versiones o parches. Esto siempre parece más difícil que cuando el software está centralizado, como sucede en la solución clásica.

Seguridad de los datos: Integridad

Asumamos por un momento la confianza en las personas que gestionan el servicio, sea *blockchain* o clásico. Veamos hasta qué punto un atacante externo podría subvertir nuestro sistema. Un conocido paradigma del *blockchain* en la garantía de la inmutabilidad del "ledger", en nuestro caso de la cadena de documentos. En los modelos con PoW esta garantía se basa en la imposibilidad física de recalcular una cadena coherente de *hashes*, debido a la enorme capacidad de cómputo necesaria [12]. Por el contrario tanto el *blockchain* corporativo como la solución clásica deben asegurar la integridad de la información con las habituales firmas digitales.

[10] Esto se debe esencialmente a que la capacidad de proponer bloques no depende del número de nodos controlados sino del porcentaje controlado de la capacidad de hash total disponible.

[11] O desde otro punto de vista, la seguridad dependería de la dificultad de los equipos de cada entidad dedicados al servicio para ponerse de acuerdo unos con otros para realizar un ataque.

[12] La imposibilidad de realizar una tarea por falta de recursos es una hipótesis clásica en seguridad.

En nuestra solución clásica, la gestión de la claves se haría como lo hace una CA clásica. En el caso del *blockchain* corporativo, si no se adopta una CA clásica deberíamos construir una "web of trust" al estilo PGP. Ambos modelos tiene en común la necesidad de custodiar las claves. Si un atacante se hiciera con las claves apropiadas podría construir una cadena de documentos válida (desde el punto de vista criptográfico), no necesitaría una imposible potencia de cálculo para ello.

La confianza en la integridad del *blockchain* corporativo por tanto se deberá basar en las mismas premisas que en la solución clásica, y los desafíos para compartir claves entre entidades son los conocidos en una PKI. No parece que aquí utilizar un *blockchain* corporativo sea ni más ni menos seguro, a priori, que utilizar una solución clásica.

Seguridad de los datos: Disponibilidad

El problema de la disponibilidad en el caso de la solución clásica lo hemos delegado al uso de las tecnologías de nube. Obviamente las nubes tienen su porcentaje (bajo) de indisponibilidad. Pero de la misma forma, la gestión de la computación y el almacenamiento distribuidos entre nodos sólo puede garantizar la disponibilidad de servicio con una cierta probabilidad, si imponemos la condición de consistencia[13]. No parece por tanto que la tecnología *blockchain* o el uso de la nube en nuestra solución clásica presenten muchas diferencias en este sentido.

Seguridad de los datos: Confidencialidad

A priori la capacidad de gestionar la confidencialidad se debería basar en el cifrado de datos, con lo cual volvemos a encontrarnos con el problema de la responsabilidad en la custodia de claves cuando no existe una autoridad.

Desde el punto de vista de la privacidad, el cifrado parece desde luego la única respuesta en el caso del uso de la tecnología *blockchain*. Por más que técnicamente no sea equivalente destruir una clave a borrar los datos, uno puede disminuir los riesgos cuanto sea necesario mediante una garantía de la destrucción de claves. Sin embargo parece difícil cuantificar esta garantía sin una custodia de claves centralizada.

Desde el punto de vista de la regulación, lo que es seguro es que GDPR[14] no ha sido concebido con la tecnología *blockchain* en mente. La cuestión de quién es el responsable de un dato situado en un "ledger" distribuido y modificable por consenso sólo puede tener respuesta con el tiempo, dependiendo de las interpretaciones del regulador. Está claro al menos que el uso de una solución clásica, en este caso, tiene muchas menos incertidumbres que el uso de *blockchain*.

Seguridad en las operaciones

Sin duda el aspecto clave aquí es la falta de madurez de la tecnología *blockchain*. Es este un problema asociado a todas las nuevas tecnologías, que como es habitual se resolverá con tiempo, experiencia y... parches.

Desde el punto de vista de la regulación, lo que es seguro es que GDPR no ha sido concebido con la tecnología blockchain en mente. La cuestión de quién es el responsable de un dato situado en un "ledger" distribuido y modificable por consenso sólo puede tener respuesta con el tiempo, dependiendo de las interpretaciones del regulador. Está claro al menos que el uso de una solución clásica, en este caso, tiene muchas menos incertidumbres.

El problema de las vulnerabilidades del software, en el caso de un *blockchain*, parece de solución complicada. Las entidades responsables de los nodos deberán coordinar entre sí las puestas en producción de nuevas versiones o parches. Esto siempre parece más difícil que cuando el software está centralizado, como sucede en la solución clásica.

Conclusión

No parece que, desde el punto de vista de la seguridad, el *blockchain* corporativo sea mejor que las soluciones clásicas, al menos a primera vista. Antes al contrario, mucho indica que para el responsable de seguridad, la proliferación de *blockchains* es un desafío, como lo es la falta de personal y de empresas especializadas en la seguridad de los mismos. Los *blockchains* pueden dar una nueva respuesta a los problemas de coordinación entre entidades, no tanto por aportar nueva tecnología como por sustituir los acuerdos entre personas por acuerdos entre sistemas de información. De manera que conviene irse preparando.

Lo que parece descartable tras un primer análisis es que un *blockchain* sea la respuesta a la necesidad de mejora de la seguridad de las arquitecturas clásicas. Algunos se empeñan en decir lo contrario, al confundir las características del *blockchain* con las de las criptomonedas, extrapolando aspectos clave de la seguridad de estas últimas, conseguidos utilizando PoW, al *blockchain* corporativo. Por su parte los legos están encantados de haber descubierto en el bitcoin el control de integridad, la computación distribuida y la replicación de datos, que convenientemente dotados de un aura de anarquía y descentralización avalan esta tecnología como la nueva piedra filosofal de los inversores en tecnologías de la información.

Más información

En un artículo como este sólo es posible plantear algunas cuestiones. El autor ha constatado que existen buenas fuentes de información en seguridad de *blockchain*, aunque no pueda decir que abundan. Una fuente excelente es el portal "Blockchain at Berkeley"[15] y en especial las interesantísimas "lectures" de su canal en YouTube. Para una interesante presentación sobre la seguridad de las criptomonedas véase, por ejemplo, este video[16]. Para entender mejor los desafíos asociados a los demás modelos de consenso, véase, por ejemplo, este otro video[17]. ■

Juan Jesús León
Director de Productos y Nuevos Desarrollos
GMV

[13] Un resultado clásico de computación distribuida es que no es posible garantizar a la vez la disponibilidad y la consistencia en caso de fallo en las comunicaciones usando un protocolo determinista.

[14] General Data ProtectionRegulation

[15] https://blockchain.berkeley.edu/

[16] "Lecture 6: How to destroy bitcoin: game theory and attacks", https://www.youtube.com/watch?v=Y_dBl-iLeMc

[17] David Mazières: "The Stellar Consensus Protocol", Talks at Google, https://www.youtube.com/watch?v=vmwnhZmEZjc