Blockchain en la administración electrónica

Autor: **Javier Casado Cadarso**
Director: **Víctor García Font**
PRA: **Rosa Borge Bravo**

Máster Universitario en Administración y Gobierno Electrónico
TFM profesional
Enero 2019

Índice

Resum

El sector públic espanyol està vivint una veritable revolució com a conseqüència de l'adopció generalitzada de l'administració electrònica. Es tracta d'un canvi no només tecnològic, sinó organitzatiu i cultural. La introducció d'eines tecnològiques està derivant en profunds canvis interns en el model organitzatiu de les administracions i en les seves relacions.

D'altra banda, els sistemes de xarxes distribuïdes basades en tecnologies de cadenes de blocs (blockchain technology en la seva denominació anglesa), estan emergint com un canvi disruptiu en l'àmbit de la tecnologia. Tot i que ja està impactant profundament en molts àmbits, com l'economia o el comerç, la seva aplicació en l'àmbit governamental i administratiu és una àrea que està encara per desenvolupar. Realment pot aportar beneficis en aquesta matèria? Com es podria aplicar aquesta tecnologia en processos administratius?

Per conèixer quanta veritat hi ha en aquest fenomen i quins beneficis pot aportar al món de l'administració electrònica, aquest treball fa una anàlisi del funcionament de les xarxes basades en blockchain, amb la xarxa Bitcoin com a principal referent i una revisió de l'encara escassa bibliografia existent en aquesta matèria. Posteriorment, analitza els recursos tecnològics en què es basen els sistemes d'administració electrònica desplegats en l'actualitat per veure com es poden veure beneficiats amb les funcionalitats proveïdes per blockchain. Finalment, es proposa l'ús d'una xarxa basada en cadena de blocs com a registre comú, centralitzat i fefaent dels expedients tramitats per les administracions públiques i els documents que els integren.

Resumen

El sector público español está viviendo una verdadera revolución como consecuencia de la adopción generalizada de la administración electrónica. Se trata de un cambio no solo tecnológico, sino organizativo y cultural. La introducción de herramientas tecnológicas está derivando en profundos cambios internos en el modelo organizativo de las administraciones y en sus relaciones.

Por otra parte, los sistemas de redes distribuidas basadas en tecnologías de cadena de bloques (*blockchain technology* en su denominación anglosajona), están emergiendo como un cambio disruptivo en el ámbito de la tecnología. Sin embargo, aunque ya está impactando profundamente en muchos ámbitos, como en la economía o en el comercio, su aplicación en el ámbito gubernamental y administrativo es un área que está todavía por desarrollar. ¿Realmente puede aportar beneficios en esta materia? ¿Cómo podría aplicarse esta tecnología en los procesos administrativos?

Para conocer cuánto de cierto hay en este fenómeno y qué beneficios puede aportar al mundo de la administración electrónica, este trabajo hace un análisis del funcionamiento de las redes

basadas en cadenas de bloques, con la red Bitcoin como principal referente y una revisión de la todavía escasa bibliografía existente en esta materia. Posteriormente, analiza los recursos tecnológicos en los que se basan los sistemas de administración electrónica desplegados en la actualidad para ver cómo pueden verse beneficiados con las funcionalidades provistas por blockchain. Finalmente, se propone el uso de una red basada en cadena de bloques como registro común, centralizado y fehaciente de los expedientes tramitados por las administraciones públicas y los documentos que los integran.

Abstract

The Spanish public sector is experiencing a real revolution as a result of the widespread adoption of electronic administration. It is a change not only technological, but organizational and cultural. The introduction of technological tools is leading to profound internal changes in the organizational model of administrations and their relationships.

On the other hand, distributed network systems based on blockchain technologies are emerging as a disruptive technological change. However, although it is already having a profound impact in many areas, such as the economy or trade, its application in e-government and administrative field is still in development. Can it really bring benefits in this matter? How could this technology be applied in administrative processes?

To know how much truth there is in this phenomenon and what benefits it can bring to the world of e-government, this work makes an analysis of networks based on blockchain, with the Bitcoin as the main reference and a review of the still scarce bibliography existing in this matter. Subsequently, it analyzes the technological resources on which the e-administration systems currently deployed are based to see how they can benefit from the functionalities provided by blockchain. Finally, the use of a blockchain based network is proposed as a common, centralized and reliable record of the files processed by public administrations and the documents that comprise them.

Palabras clave

Administración electrónica, gobierno electrónico, interoperabilidad, cadena de bloques, blockchain

Abreviaturas

AGE: Administración General del Estado

BTC: criptomoneda Bitcoin

CSV: código seguro de verificación de documentos electrónicos

DAO: *decentralized autonomous organization*, organización autónoma descentralizada

ĐApps: aplicaciones descentralizadas

DIR3: Directorio Común de Unidades Orgánicas y Oficinas

DLT: *Distributed Ledger Technology*, tecnología de libro contable distribuido

ENI: Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

ENS: Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

ETH: criptomoneda Ether

LFE: Ley 59/2003, de 19 de diciembre, de firma electrónica

LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

LPAC: Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

LRJ: Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público

LTBG: Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno

NTI: Normas Técnicas de Interoperabilidad

NTIDE: Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico

NTIEE: Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico

P2P: red de pares (peer to peer)

PAG: Punto de Acceso General electrónico de la Administración

POW: *proof of work*, prueba de trabajo

POS: *proof of stake*, prueba de participación

RCB: redes distribuidas basadas en tecnologías de cadena de bloques (*blockchain*)

Red SARA: Sistemas de Aplicaciones y Redes para las Administraciones

SIA: Sistema de Información Administrativa

SSI: self-sovereign identity, identidad digital soberana

TIC: Tecnologías de la información y las comunicaciones

UTC: tiempo universal coordinado

1. Introducción

A poco que se indague en la literatura disponible acerca de la tecnología de redes basadas en cadena de bloques (RCB), se tiene la sensación de que nos encontramos ante una verdadera revolución tecnológica.

Sin embargo, también existen voces críticas que cuestionan el grado de innovación que realmente aporta esta tecnología. Algunas personas muy reconocidas en el ámbito de las nuevas tecnologías como Steve Wozniak, se refieren a blockchain como una nueva burbuja tecnológica (Rooney, 2018). Otros lo consideran una tecnología inmadura con un largo trecho por recorrer antes de ser completamente funcional (varios).

Entonces ¿estamos ante una auténtica evolución tecnológica o se trata de un nuevo *hype* alimentado por la red? (Konstantinidis et alt., 2018).

Los defensores de las redes distribuidas basadas en tecnologías de cadena de bloques (en adelante RCB), las presentan como una panacea para resolver casi cualquier necesidad de gestión de la información, pero su materialización práctica no resulta en absoluto evidente. Svein Ølnes, investigador del Western Norway Research Institute, describe la situación actual como *un proceso de maduración que necesita pasar de un enfoque centrado en lo tecnológico a un enfoque basado en las necesidades reales* (2017 b).

Para Greta Bull, de CGAP (Consultative Group to Assist the Poor), *la cuestión clave no es si blockchain funciona o no, sino si lo hace mejor y de manera más eficiente que otras tecnologías ya existentes en el mercado* (Bull, 2018).

Para conocer cuánto de cierto hay en este fenómeno y qué beneficios puede aportar en el ámbito de la administración electrónica, este trabajo comienza con una introducción que ocupa el capítulo 1, hace un análisis del funcionamiento de las RCB a lo largo del capítulo 2 tomando la red Bitcoin como principal referente. Las secciones 2.3 y 2.4 describen la evolución de las RCB y su tipología, respectivamente. Posteriormente, en el capítulo 3 se hace una revisión de la literatura acerca de blockchain en proyectos de gobierno electrónico. En el capítulo 4 se revisan de forma somera los recursos tecnológicos en los que se basan los sistemas de administración electrónica para, ya en el capítulo 5, analizar los posibles usos de las RCB en la administración electrónica, con los beneficios y riesgos derivados de su aplicación.

Finalmente, en el capítulo 6 se propone el uso de una RCB como registro común, centralizado y fehaciente, para los expedientes y documentos tramitados por las administraciones públicas. Se analiza el tipo de RCB más adecuado y su uso por los interesados y la propia administración para el acceso a los expedientes y sus documentos, así como por otras administraciones, para el cumplimiento del derecho del interesado a no aportar documentos que ya se encuentren en poder

de cualquier administración. El registro permitirá también la puesta a disposición de expedientes administrativos entre administraciones según lo previsto en el Esquema Nacional de Interoperabilidad y en las correspondientes Normas Técnicas de Interoperabilidad.

2. Cómo funcionan las RCB. Bitcoin

2.1 Definición

La tecnología que da soporte a las redes basadas en cadena de bloques apareció por primera vez en el artículo *Bitcoin: A Peer-to-Peer Electronic Cash System*, de Satoshi Nakamoto (2008), un seudónimo del que todavía no se conoce identidad real. Partiendo de varias tecnologías ya existentes, propuso un prototipo para un sistema financiero electrónico descentralizado sin el control de las entidades bancarias tradicionales que garantizara la privacidad en las transacciones de forma similar a como sucede con el dinero en metálico (Nakamoto, 2008).

De forma resumida, una RCB es un libro contable distribuido que es compartido entre los nodos que integran la red. En ese registro se anotan todas las transacciones efectuadas entre los participantes, previa verificación de las mismas a través de un mecanismo de consenso. De esta forma, es la propia red la que ofrece la confianza necesaria para que los participantes operen en el sistema de intercambio. Cada transacción debe ser aprobada por una mayoría de los participantes en la red para que la operación sea confirmada y almacenada en el libro contable. Las anotaciones se reflejan en todos los nodos de la red y se vinculan de forma permanente con las anotaciones precedentes, de manera que el libro resulta prácticamente inalterable y asegura la trazabilidad de todas las transacciones registradas. De esta concepción como un gran libro de contabilidad (*ledger*) deviene una de las denominaciones para las RCB: *Distributed Ledger Technology* (DLT).

De forma resumida, una red de cadena de bloques es una tecnología que reemplaza las bases de datos individuales por un libro mayor distribuido de información compartida, lo que debería derivar en una mayor seguridad y accesibilidad (Ølnes, 2017 b).

El término *Bitcoin* hace referencia tanto al protocolo de red definido por Nakamoto, como a la propia red que da soporte al sistema de intercambio financiero (*Bitcoin*, con mayúscula), como a la *criptomoneda* con la que se opera en el sistema, conocida como *bitcoin*, *BTC* de forma abreviada. Como ejemplo del funcionamiento de una RCB describimos el funcionamiento de la red Bitcoin.

2.2 El modelo de Bitcoin

La red Bitcoin comenzó a operar en 2009, siguiendo el diseño propuesto por Nakamoto. Se trata de una *red p2p*, un tipo de red de gran estabilidad y resistente a fallos, de código abierto, en la

que todos los *nodos* conectados comparten toda la información intercambiada a través de la red desde su puesta en marcha, el 3 de enero de 2009 con el llamado *bloque Génesis*. El archivo de la red Bitcoin está próximo a los 200 gigabytes en enero de 2019. Concretamente, supera los 198.000 Mb a 7 de enero de 2019 (fuente: https://www.blockchain.com/es/charts/blocks-size). Esta gran base de datos es conocida como el libro de contabilidad de Bitcoin (*bitcoin ledger*).

Se trata de una red abierta a la que cualquiera puede conectarse mediante un programa cliente que convierte a su equipo en un nodo más de la red. Puede verse un mapa interactivo de los nodos existentes en la red en https://bitnodes.earn.com/nodes/live-map/).

A través de esta red se transmiten *transacciones*, anotaciones de intercambios de ciertas cantidades de *bitcoins* entre dos direcciones de la red: una dirección de origen cuyo saldo reconocido en la red debe ser igual o superior a la cantidad a intercambiar y una dirección de destino cuyo saldo se incrementará en la cantidad transferida. La direcciones de origen y de destino son direcciones electrónicas carentes de información identificativa de su titular y se generan cuando alguien hace uso de un programa cliente para la red Bitcoin. Cada dirección lleva asociadas a las direcciones de origen y destino de la transacción un par de claves criptográficas, pública y privada, utilizadas para firmar electrónicamente la transacción desde la dirección de origen. Las transacciones incluyen las cantidades a transferir en fracciones de bitcoin conocidas como *satoshis*: 1 BTC = 10^8 *satoshis*.

Existen diferentes tipos de nodos en la red Bitcoin:

- **Nodos que sólo emiten transacciones** (*broadcast only node*). Tienen limitada capacidad de cálculo y se limitan a enviar transacciones a la red.
- **Nodos que propagan las transacciones** (*relay node*). Reenviar las transacciones por toda la red, comprueban que éstas están bien construidas y son válidas. Estos nodos pueden ser:
    - **completos**: contienen una copia completa de la cadena de bloques.
    - **parciales**: disponen solo de la información más reciente de la cadena de bloques.
- **Nodos mineros**. Nodos dedicados al cálculo de nuevos bloques (minado). También emiten y transmiten transacciones. Los mineros compiten entre sí por ser el más rápido en calcular el nuevo bloque a agregar a la cadena.

En la red Bitcoin existe un *token* o criptomoneda de la que se entrega una cantidad predefinida como recompensa cada vez que un nodo dedicado al minado obtiene un bloque válido, el bitcoin, cuyo símbolo es BTC. Nakamoto estableció un número máximo de 21 millones de bitcoins en total. Su finalidad es fomentar la presencia en la red de nodos mineros, quienes ven así compensado su esfuerzo de cálculo. Además, el emisor de una transacción puede incluir una recompensa voluntaria para el nodo minero que incluya con éxito su transacción en un bloque, de manera que tenga preferencia para ser incluida en un bloque en lugar de otras y sea considerada válida lo antes posible. El conjunto de transacciones transmitidas a la red a la espera de ser incluidas en un bloque válido se conoce como *mempool*.

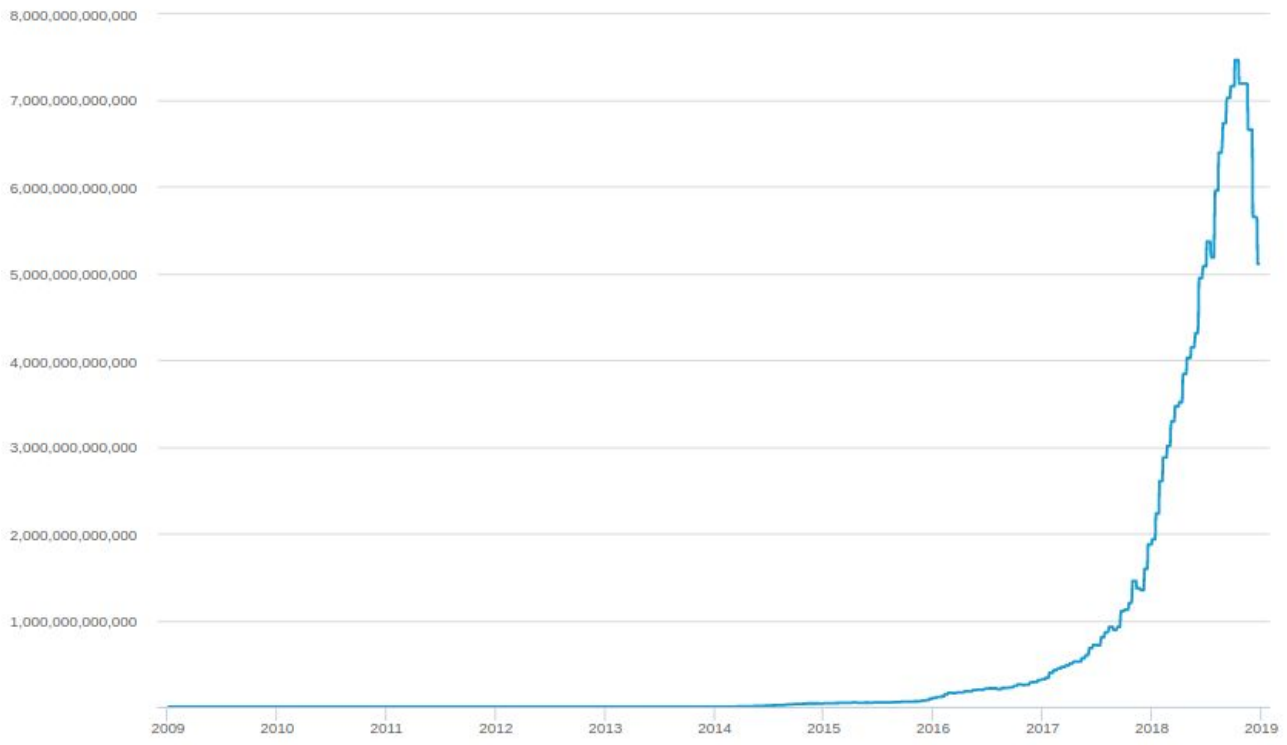
El Minado

Las transacciones enviadas a la red se agrupan en *bloques* de un tamaño máximo establecido en 1 Mb de información. En este bloque se incluye, además de algunas de las transacciones pendientes, otra información como:

- un *nonce* o número aleatorio de tamaño fijo (32 bits), que puede variar libremente.
- un *hash* o resumen criptográfico del bloque anterior en la cadena.

Una vez construido el bloque completo, se calcula su hash criptográfico, un resumen de todo el bloque que es obtenido mediante la aplicación de un algoritmo matemático a la información incluida en el bloque. El hash o resumen tiene siempre un tamaño fijo y un hash concreto es el resultado de un conjunto de información determinado, de manera que cualquier cambio en la información del bloque, por mínimo que sea, da como resultado un hash completamente distinto.

Imagen 1: evolución de la dificultad relativa de obtención de un bloque



Fuente: https://www.blockchain.com/

Para que un bloque sea considerado válido, su hash debe cumplir una serie de requisitos establecidos para incrementar la dificultad de su cómputo: por ejemplo que el hash comience por 16 dígitos a 0 (ver la prueba de trabajo). Si se calcula el hash y resulta no ser válido porque no cumple con los requisitos exigidos, se debe modificar el número aleatorio incluido en el bloque (nonce) y se vuelve a realizar el cálculo. Cuando se obtiene un bloque válido, el bloque se envía a la red para que sea incluido en la cadena de bloques.

El proceso seguido para obtener un bloque válido es conocido como *minado* y resulta muy costoso en capacidad de cómputo, según el nivel de exigencia de los requisitos a cumplir por el hash vigentes en cada momento. En la Imagen 1 podemos observar el incremento de la dificultad de obtención de un hash válido a lo largo del tiempo.

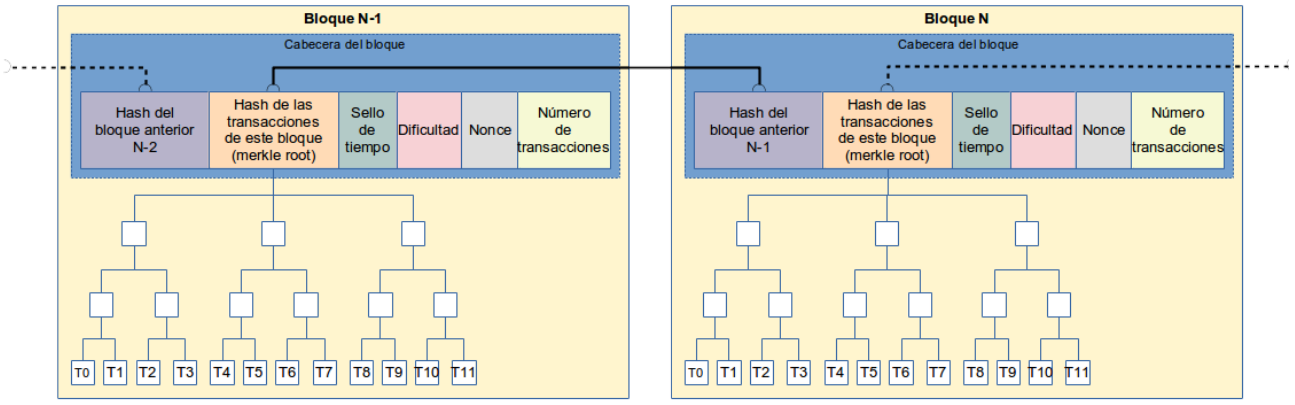
Nakamoto estableció una recompensa que recibe el nodo que encuentre un nuevo bloque válido a incorporar a la cadena de bloques. Inicialmente fueron 50 BTC, pero Nakamoto estableció la premisa de que la recompensa se reduciría un 50% cada 4 años, de manera que actualmente, es de 12,5 BTC por bloque.

La cadena de bloques

Cada bloque que se añade a la cadena de bloques incluye el resumen criptográfico del último bloque válido, quedando así vinculado (*encadenado*) con el bloque anterior por su hash. Esta técnica garantiza la inmutabilidad de la información integrada en la cadena de bloques, ya que una alteración de una transacción cualquiera provocará la modificación del resumen del bloque donde se incluye que ya no se corresponderá con el resumen encadenado en el siguiente bloque, invalidando así su contenido.

La imagen 2 representa cómo se enlazan dos bloques consecutivos en la cadena, mientras que la imagen 3 muestra de forma gráfica este funcionamiento.

Imagen 2: enlace entre bloques en la cadena



Elaboración propia

Imagen 3

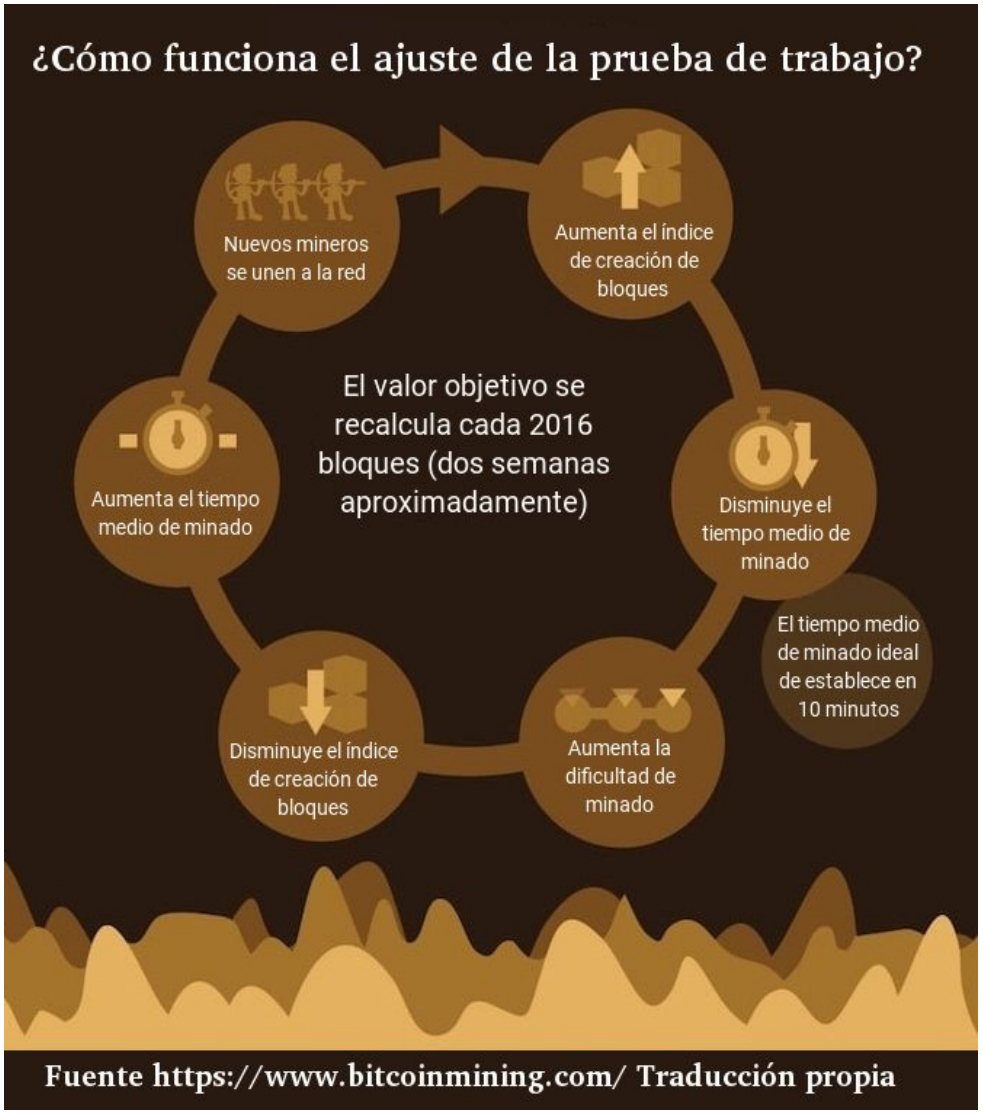
La prueba de trabajo

La dificultad implícita en llegar a encontrar un hash válido se regula estableciendo unos requisitos más o menos exigentes a cumplir por el hash. Este nivel de dificultad variable se conoce como prueba de trabajo (*proof of work* o *POW*) y permite regular la frecuencia temporal con la que se obtiene un nuevo bloque en la red que, en el caso de Bitcoin, se establece en 10 minutos por bloque. La dificultad se ajusta cada 2016 bloques, basándose en el tiempo requerido para generar los 2016 bloques anteriores. Las imágenes 4 y 5 representan este funcionamiento.

Imagen 4


¿Qué es la prueba de trabajo?
Es el método que asegura que la información contenida en un nuevo bloque ha sido costosa en su generación
Requiere potencia de cálculo
Que supone:
HARDWARE
ENERGÍA
TIEMPO
Por el contrario, resulta sencillo para otros comprobar que se ajusta a los requisitos
EN LA PRÁCTICA
INICIO
Propuesta de nuevo bloque
Cabecera del último bloque
Composi-ción y cálculo del hash
NONCE (número aleatorio)
Incremento y nuevo recálculo
Número HASH
Valor Objetivo
Comparar
¿Está dentro del valor objetivo?
NO
SÍ
Determina
Dificultad de minado
Resuelta la prueba de trabajo
¡Recom-pensa de minado!

Imagen 5



El mecanismo de consenso

Puede suceder que dos nodos mineros obtengan al mismo tiempo dos bloques válidos diferentes, conteniendo cada uno de ellos transacciones diferentes. Cada minero envía a la red su bloque candidato para que sea aceptado por los demás nodos e incorporado a sus copias de la cadena de bloques.

Como la difusión de los bloques está sujeta a la latencia propia de las redes de gran extensión, cada bloque candidato se añadirá a la copia de la cadena de bloques original existente en los nodos de la red más próximos a cada uno, dando lugar a dos versiones diferentes de la cadena (*bifurcación*). A los pocos minutos será propuesto un nuevo bloque vinculado a uno de los bloques candidatos anteriores que extenderá una de las dos versiones de la cadena. A la larga, una de las bifurcaciones presentará una versión de la cadena más extensa que la otra.

Las bifurcaciones se resuelven por el mecanismo del consenso, según el cual los nodos de la red darán por válida la versión más extensa de la cadena, la que presenta una mayor prueba de trabajo acumulado, mientras que el bloque candidato que no ha resultado elegido, así como todos los bloques que pudieran haberse añadido detrás de él, serán desechados y sus transacciones volverán al mempool a la espera de volver a ser procesadas.

La existencia de una única cadena de bloques en la red permite comprobar la validez de todas las operaciones incluidas a lo largo de toda la cadena desde su origen y confirmar así los saldos disponibles para cada dirección de la red. Las operaciones de validación de los bloques que integran la cadena resultan mucho más rápidas que las de cálculo de nuevos bloques, al no tener que buscar un resumen sujeto a unos requisitos concretos, sino simplemente, verificar que el resumen de cada bloque corresponde al contenido del bloque a validar.

Los bloques creados, su vinculación con el anterior y el siguiente bloque, las transacciones que incluye cada bloque, las recompensas obtenidas por el nodo minero y otros datos, se pueden consultar a través de exploradores de la cadena de bloques, que representan de forma visual todo lo descrito. Un buen ejemplo es https://www.blockchain.com/es/charts/.

Las carteras digitales

Como hemos indicado, Bitcoin fue diseñada como un sistema financiero electrónico descentralizado en el que las transacciones almacenadas describen intercambios de criptomonedas entre dos nodos. Las herramientas mediante las que los usuarios del sistema financiero mantienen sus saldos de criptomonedas se conocen como carteras o monederos digitales (*wallets* en inglés). Se trata de aplicaciones cliente de la red Bitcoin que permiten gestionar direcciones de red desde las que enviar y recibir las cantidades intercambiadas en las transacciones y los saldos asociados a estas direcciones.

Los contratos inteligentes

El concepto de *smart contract* o contrato inteligente fue creado por Nick Szabo en 1994. Consiste básicamente en programas alojados en la RCB que contienen una serie de condiciones que deben cumplirse y las obligaciones a las que están sujetas las partes intervinientes en el contrato. Los contratos pueden incluir tanto recompensas como sanciones que se ejecutarán una vez que se cumplan las condiciones establecidas en el contrato. En rigor, su nombre puede inducir a equívoco, pues no se trata de contratos en la acepción jurídica del término, sino más bien de *pequeños programas autoejecutables que utilizan código de programación para conseguir que la ejecución de acuerdos de voluntad sencillos, no dependa de la contraparte ni de terceros* (Stokes & Freire, 2017).

Con la puesta en marcha de Bitcoin, Nakamoto también creó el entorno necesario para el desarrollo de los contratos inteligentes propuestos por Szabo, al disponer simultáneamente de un sistema de pagos y de una red segura como soporte para los programas a ejecutar. Sin embargo, ha sido la red *Ethereum* la que ha dado el impulso definitivo a los contratos inteligentes, tal como se explica en la sección 2.3.

Retos de las RCB

La existencia de criptomoneda en una red puede convertirse en un riesgo para la independencia de la propia red. El alto valor de algunas criptomonedas ha dado lugar a equipos informáticos especializados en tareas de minado (*ASICs*) y al fenómeno de las granjas de minado, donde centenares y hasta miles de esos equipos especializados cooperan para obtener las recompensas asociadas a la generación de bloques.

La concentración de nodos de red en pocas manos no es una cuestión trivial. Si una mayoría de nodos llega a estar controlada por una misma organización, ésta podría modificar la cadena de bloques a su antojo aprovechando su posición de dominio en el consenso, produciéndose el conocido como *ataque del 51%*. Otro posible ataque es el denominado *ataque Sybil* (Douceur, 2002), consistente en crear identidades falsas con el objeto de llegar a obtener el control mayoritario de una red.

Otro factor a considerar en una RCB pública es el consumo energético. El alto valor de la criptomoneda ha incrementado la participación en la red de nodos mineros atraídos por los beneficios que reporta el minado, aumentando la dificultad de la prueba de trabajo. Así, miles de equipos compiten mundialmente para crear un bloque válido que sólo uno de ellos logrará generar, de manera que el resto calcula de forma infructuosa con el consiguiente consumo energético global. Estudios recientes estiman que la minería de bitcoin ya supone el 1% del consumo energético mundial (Narayanan, 2018).

Otro riesgo de las RCB es el creciente aumento del tamaño del archivo completo de la cadena de bloques. Este crecimiento podría provocar la existencia de un menor número de nodos completos, con el consiguiente efecto de centralización del control último de la red.

2.3 Evolución de las RCB

El diseño de Nakamoto para Bitcoin obtuvo un gran éxito como plataforma de pagos electrónicos y ha servido de inspiración para el desarrollo de muchas redes similares. Actualmente existen más de 2000 criptomonedas y su número continúa en aumento (https://coinmarketcap.com/, 2018).

El modelo de cadena de bloques también ha servido como base para el desarrollo de aplicaciones orientadas a otros fines, en lo que se ha dado en llamar *blockchain 2.0* (Bheemaiah, 2015). En las

RCB se registran transacciones de la más variada naturaleza, de forma descentralizada y sin necesidad de un tercero de confianza. Las aplicaciones que ya operan sobre RCB en el mundo real son en su mayoría con fines financieros, aunque también se están desarrollando proyectos en otros ámbitos, tanto del sector privado como público (Konstantinidis et alt., 2018). Cabe mencionar el sector de los seguros, el comercio internacional, el suministro y la distribución de energía, la logística y las cadenas de distribución, los servicios de protección social, los servicios sanitarios, el comercio electrónico, etc.

Una de las mayores evoluciones sobre el modelo de Nakamoto fue introducida en enero de 2014 por Vitalik Buterin, quien publicó *A Next Generation Smart Contract & Decentralized Application Platform*, el documento que dio origen a *Ethereum*. *Ethereum* es una RCB que soporta un lenguaje de programación *Turing completo* que permite crear contratos inteligentes mucho más avanzados. Con ella, pueden crearse sistemas pensados para nuevas finalidades simplemente escribiendo la lógica en unas pocas líneas de código. *Ethereum* se ha consolidado como plataforma multipropósito de software distribuida, pública, de código abierto, basada en blockchain que permite desarrollar aplicaciones descentralizadas (*ĐApps*) que ofrecen soluciones a necesidades diversas y que se almacenan en la RCB. Están escritas en Solidity, lenguaje de programación propio de *Ethereum*. También tiene su criptomoneda, el Ether (ETH) y actualmente es la tercera RCB en capitalización de mercado (https://coinmarketcap.com/, 2018).

Otro de los avances aportados por Buterin con *Ethereum* han sido las *DAO*, organizaciones descentralizadas de funcionamiento autónomo en las que la propia organización se ejecuta a través de reglas codificadas en forma de contratos inteligentes alojados en la RCB. Su prestigio está lastrado por el incidente conocido precisamente como '*The DAO*' en el que un hacker robó 50 millones de dólares en Ether por un fallo existente en el código de programación que opera estas organizaciones descentralizadas.

En la actualidad, varias de las RCB más importantes están evolucionando su mecanismo de consenso basado en la prueba de trabajo (PoW) hacia otros mecanismos de consenso distribuido, como el mecanismo de la prueba de participación (PoS por las siglas en inglés de *Proof of Stake*). Es el caso de la propia *Ethereum* o de las redes Peercoin, Neucoin o Nxt. En este mecanismo, los nodos participantes en el consenso disponen de mayor peso de decisión cuanto mayor sea su prestigio en la red o la relevancia que le haya sido asignada por el administrador, si se trata de una red privada (ver la siguiente sección). La relevancia de cada uno de los nodos mineros se establece según el número de criptomonedas que el nodo ponga en juego en el cálculo de un bloque, en una especie de *apuesta* por la validez del bloque minado. Se fundamenta en la suposición de que cuanta mayor cantidad de criptomonedas hayan sido acumuladas por un nodo, mayor será su interés en que la red se mantenga segura y confiable.

La aparición de *Ethereum* aumentó la versatilidad de las RCB al permitir la incorporación a las cadena de bloques de cualquier tipo de dato, pudiendo así utilizarse como *registro de operaciones, como sistema de contabilización, o como mecanismo de documentación de datos, procesos, bienes inmateriales o derechos de todo tipo, incluso sin contenido económico* (Ibáñez, 2018). Esta versatilidad y las posibilidades que presentan los contratos inteligentes suponen para algunos autores que estudian la potencialidad de las RCB en el sector público, las principales fortalezas de su futuro en este ámbito (Ølnes, 2017 b).

2.4 Tipologías de redes blockchain

Según el tipo de acceso a los datos y los permisos necesarios para poder generar nuevos bloques, existen diversos modelos de RCB. En el modelo propuesto por Wüst y Gervais (2017), los nodos participantes en una RCB asumen uno de estos **tres roles**:

- **Escritor** o validador: cualquier entidad autorizada para escribir en una cadena de bloques. Rol asumido por los participantes involucrados en el protocolo de consenso que ayudan a hacer crecer la cadena de bloques, correspondiente a los nodos mineros.
- **Lector**: cualquier entidad de la red que no está extendiendo la cadena de bloques, puede generar nuevas transacciones o simplemente leer, analizar o auditar la cadena de bloques.
- **Controlador**: nodos dedicados a la regulación de la red y al mantenimiento del software de la cadena de bloques.

Según la forma de **participación en el mecanismo de consenso**, las RCB pueden ser:

- **Sin permisos**: son redes abiertas que no disponen de una entidad central que administre la membresía. Cualquiera puede unirse o salir de ellas y participar como escritor en cualquier momento.
- **Con permisos**: son redes en las que los nodos son autorizados por una o varias entidades conocidas que administran la membresía. Únicamente los nodos autorizados y previa identificación pueden acceder a la cadena de bloques y participar con el rol para el que hayan sido autorizados, sean lectores o escritores. Este tipo de cadenas permiten procesar un mayor número de transacciones por segundo, ofrecen capas adicionales de confidencialidad y su funcionamiento supone un menor consumo de energía frente al modelo público y sin permisos.

Otra clasificación de las RCB se basa en el **carácter público o privado del acceso a los datos**:

- **Redes públicas**: cualquiera puede acceder y leer los datos registrados en la cadena.
- **Redes privadas**: sólo los nodos autorizados pueden leer la información almacenada. No requieren de una criptomoneda que incentive la participación de nodos en el sistema de consenso porque los nodos que hacen esa función han sido dedicados por los promotores de la red.

La combinación de estas tipologías produce la siguiente clasificación de tipos de RCB:

Tabla 1: Tipos de redes basadas en cadena de bloques

Tipos de redes RCB		
	RCB con permisos	**RCB sin permisos**
Lectura pública de la cadena	Acceso abierto a datos y transacciones + Participación con membresía en el consenso	Acceso abierto a datos y transacciones + Participación abierta en el consenso
Lectura privada de la cadena	Acceso con membresía a datos y transacciones + Participación con membresía en el consenso	

Elaboración propia

Redes públicas y sin permisos en las que cualquiera puede acceder y leer los datos registrados en la cadena. No garantizan plenamente la privacidad de la actividad desarrollada por los participantes, sin embargo, mediante el uso de técnicas criptográficas, es posible diseñar una cadena de bloques sin permisos con una capa que garantice la confidencialidad de la información almacenada, como es el caso de Zerocash (Ben-Sasson et alt., 2014). Bitcoin y Ethereum son ejemplos de cadenas de bloques públicas y sin permisos.

Redes privadas y con permisos: requieren autorización tanto para acceder al contenido de la cadena de bloques como para participar en el mecanismo de consenso. Solo los nodos autorizados pueden conectarse a la red, sean lectores o escritores. Un ejemplo es la red Chain.com, empresa de tecnología que coopera con organizaciones para el uso de RCB en el área de productos y servicios financieros. También destaca el caso de Ripple, cuya red *XRP* está siendo utilizada por diversas entidades financieras como plataforma para transacciones internacionales de gran velocidad y bajo coste (Wüst y Gervais, 2017).

Redes públicas con permisos en las que cualquier nodo puede acceder a la red y leer el contenido de la cadena, pero solo los nodos previamente autorizados pueden participar en el mecanismo de consenso y generar nuevos bloques.

Las denominadas **redes federadas** suponen un caso específico de redes tanto privadas como públicas con permisos en las que el control de acceso y gestión de la red es compartido por las diversas organizaciones usuarias de la red, quienes designan cuáles de sus nodos van disponer de acceso a la red y cuáles de ellos realizarán las tareas de minería de bloques y de mantenimiento de la infraestructura. Corda (del consorcio R3) o Hyperledger, proyecto de código abierto nacido en diciembre de 2015 y albergado en la Fundación Linux son ejemplos de este tipo de RCB.

El modelo de RCB federadas está ganando apoyos entre el mundo empresarial por ofrecer mejoras en aspectos en los que otros modelos resultan ineficientes: son rápidas frente a la lentitud de las redes públicas; no tienen problemas de escalabilidad porque el número de nodos está siempre bajo control; el coste de transacción es mucho menor que en las redes públicas porque no necesitan incrementar el grado de dificultad del minado; el consumo energético es también mucho menor; no están amenazadas por ataques del 51% u otros ataques cibernéticos, puesto que la membresía está controlada y se accede siempre desde entornos seguros regulados por las normas de las que las organizaciones federadas se hayan dotado (Anwar, 2018).

Un ejemplo de implementación de este modelo de red federada en una infraestructura semipública es la creada por el consorcio Alastria en España (https://alastria.io/), que cuenta alrededor de 70 de las mayores empresas e instituciones de distintos sectores. Está desarrollada sobre *Ethereum* y el principal proyecto iniciado por este consorcio tiene como objetivo construir un sistema de identificación digital a través del estándar "*ID Alastria*".

3. Revisión de la literatura y proyectos desarrollados sobre RCB

Los principales documentos analizados en la revisión de la literatura existente relacionada con el objetivo de este trabajo han sido:

#	Autor(es)	Año	Título	Tipo de publicación
1	Alketbi, A., Nasir, Q., & Talib, M. A.	2018	Blockchain for government services-Use cases, security benefits and challenges	Documento de sesión
2	Anand, A., Kok, A., Makala, B. et alt.	2018	The Legal Aspects of Blockchain	Libro
3	Batubara, F. R., Ubacht, J., & Janssen, M.	2018	Challenges of blockchain technology adoption for e-government: a systematic literature review	Documento de sesión
4	Goderdzishvili, N., Gordadze, E., & Gagnidze, N.	2018	Georgia's blockchain-powered property registration: Never blocked, always secured - Ownership data kept best!	Documento de sesión
5	Hou, H.	2017	The application of blockchain technology in E-government in China	Documento de sesión
6	Ibáñez J.	2018	Blockchain : Primeras cuestiones en el ordenamiento español	Libro
7	Jun, M.	2018	Blockchain government - a next form of infrastructure for the twenty-first century	Artículo de revista
8	Konashevych, O.	2017	The concept of the blockchain-based governing: Current issues and general vision	Documento de sesión
9	Meijer, D., & Ubacht, J.	2018	The Governance of Blockchain Systems from an Institutional Perspective, a Matter of Trust or Control?	Documento de sesión
10	Nordrum, A.	2017	Govern by blockchain dubai wants one platform to rule them all, while Illinois will try anything	Artículo de revista

11	Ølnes, S.	2016	Beyond Bitcoin Enabling Smart Government Using Blockchain Technology	Capítulo de libro
12	Ølnes, S., & Jansen, A.	2017	Blockchain Technology as Infrastructure in Public Sector – an Analytical Framework	Documento de sesión
13	Ølnes, S., Ubacht, J., & Janssen, M.	2017	Blockchain in government: Benefits and implications of distributed ledger technology for information sharing	Artículo de revista
14	Porxas, N., & Conejero, M. (2018)	2018	Tecnología blockchain: funcionamiento, aplicaciones y retos jurídicos relacionados	Artículo de revista
15	Wüst, K., Gervais, A.	2017	Do you need a Blockchain?	Artículo de revista

En general, los documentos analizados estiman que las RCB tienen potencial para hacer más eficientes los procesos administrativos, mejorando la prestación de los servicios públicos y la confianza en los mismos (Alketbi, Konashevych,...). Se mencionan algunas de las diferentes iniciativas puestas en marcha por diversos Estados que están explorando el potencial de las RCB, pero la mayor parte de ellos aborda la cuestión todavía de una forma conceptual, sin vinculación con un entorno empírico (Batubara, 2018).

Entre todos los trabajos analizados, destacan las investigaciones que lleva a cabo Svein Ølnes, investigador del Western Norway Research Institute especializado en el análisis del impacto de la tecnología en las administraciones, de quién se recogen tres aportaciones.

El nivel de confianza atribuido a las RCB *per se* es de tal envergadura que existen autores que hablan de una posible usurpación de las funciones propias de los gobiernos por parte de las RCB. En este sentido, Ølnes (2017 b) cita a Davidson, De Filippi, & Potts (2016) y a Atzori (2015), quienes aseguran que los gobiernos intuyen la necesidad de poder administrar y controlar la tecnología que vaya a servir de soporte para la provisión de servicios relacionados con los valores públicos. El papel que desempeñan las administraciones en los ámbitos en los que se implanten las RCB podía verse relegado por la tecnología y aquéllas deberían preservarse la potestad de control sobre las RCB necesarias para ello. Esto incluiría el establecimiento, ejecución, mantenimiento y control de acceso a dichas redes.

Ølnes (2017 b) identifica como posibles ámbitos de aplicación de las RCB en la administración la identidad digital; el archivo de sentencias judiciales; la financiación de obras; el rastreo de las transacciones económicas; registros como el registro civil, el de la propiedad o el empresarial; el voto electrónico; el control de licencias comerciales; los pasaportes; registros penales e incluso registros fiscales.

Una de las carencias de las RCB señaladas por Ølnes (2017 b) es su falta de estandarización, requisito imprescindible para garantizar la interoperabilidad actualmente exigida en los procesos administrativos. Por otra parte, indica que un intento de estandarización en fases en las que la tecnología pudiera no estar suficientemente madura, podría derivar en la elección de un estándar inadecuado.

También Ølnes propone un modelo en el que el gobierno se convertiría en proveedor de servicios RCB compartidos, utilizando una infraestructura que permita a los diferentes niveles administrativos (central, local, autonómico…) y a las agencias públicas, crear una aplicación basada en RCB que garantizase el cumplimiento de la legislación de forma segura y confiable, así como la validez de la información. Para hacer viable esta propuesta, se necesita tecnología, pero también estandarización de modelos de datos para la interoperabilidad (2017 2).

Por último, en una de sus aportaciones (2016), Ølnes describe un caso de uso de una RCB como registro de certificaciones académicas, un buen punto de partida para el tipo de aplicación de las RCB que se propone en este mismo trabajo.

Por su parte, Hou (2017) se muestra optimista tanto en las posibilidades que ofrecen las RCB en los sistemas de gobierno como con los resultados obtenidos por el caso que es objeto de su estudio, *Guangdong Province Big Data Comprehensive Experimental Area*, en el distrito de Chancheng, en la ciudad china de Foshan. Sin embargo, también aboga por la adopción de un estándar y de una plataforma generalista basada en blockchain para fomentar el desarrollo y la rápida adopción de esta tecnología entre los gobiernos.

En general, la falta de madurez de las RCB se contempla como uno de los mayores retos para su adopción, un problema común a todas las tecnologías emergentes; pero también se alude con frecuencia a la necesidad de asumir cambios organizativos, de nuevas gobernanzas y de aceptación de los cambios tecnológicos. En (Batubara, 2018), los autores inciden en la falta de evidencias prácticas aportadas por los investigadores en lo referente a los beneficios y posibles mejoras que podrían aportar las RCB al sector público.

Así lo reconocen también Ølnes y Jansen (2017) en su propuesta para una infraestructura de información basada en RCB para el sector público. Su documento aspira a describir cómo implementar una plataforma basada en una cadena de bloques abierta, que podría ser con permisos o sin permisos (ver sección 2.4). Tras un repaso por varios proyectos basados en RCB impulsados por el sector público en varios países, proponen una tabla para estimar los beneficios potenciales y los retos previsibles en una implementación de las RCB en sistemas de gobierno y dejan abiertas para futuras investigaciones, cuestiones como si están las instituciones preparadas para la adopción de las RCB y cuáles son los principales impedimentos para ello, o cual sería la tipología de RCB más apropiada (ver sección 2.4).

En este punto, cabe mencionar la aportación de Wüst y Gervais (2017), quienes presentan un árbol de decisión que pretende ayudar a determinar si resulta adecuado el uso de RCB en un proyecto cualquiera y qué tipo de red es la más conveniente en cada caso (ver Imagen 6).

En la línea de analizar algunos de los proyectos basados en RCB impulsados por el sector público, el trabajo de Jun (2018) repasa los más destacados y concluye que la adopción de las RCB como sustituto de la burocracia tradicional no sólo es posible, sino inevitable y aporta cinco principios que deberían aplicarse en ese proceso de adopción:

1. Elaboración de una normativa reguladora de las RCB con rango de Ley
2. Divulgación transparente de los datos y del código fuente
3. Implementación de una administración capaz de ejecutarse de manera autónoma
4. Construir un sistema de gobierno basado en la democracia directa
5. Hacer un gobierno autónomo distribuido

Menos ambiciosa resulta la aportación de Nordrum (2017) en su análisis acerca de lo divergentes que resultan los proyectos basados en RCB desarrollados en Dubai e Illinois, diferencias que achaca a lo incipiente de esta tecnología, específicamente la que soporta los contratos inteligentes.

El trabajo de Goderdzishvili et alt. (2018) analiza el caso de uso de las RCB en el registro de la propiedad del estado de Georgia, un proyecto piloto con excelentes resultados de reducción de tiempo y coste que los autores cifran en el 95%. Los autores afirman que la administración estatal ya está planeando la extensión del uso de las RCB a todas las funciones registrales y a otros ámbitos de su actuación administrativa.

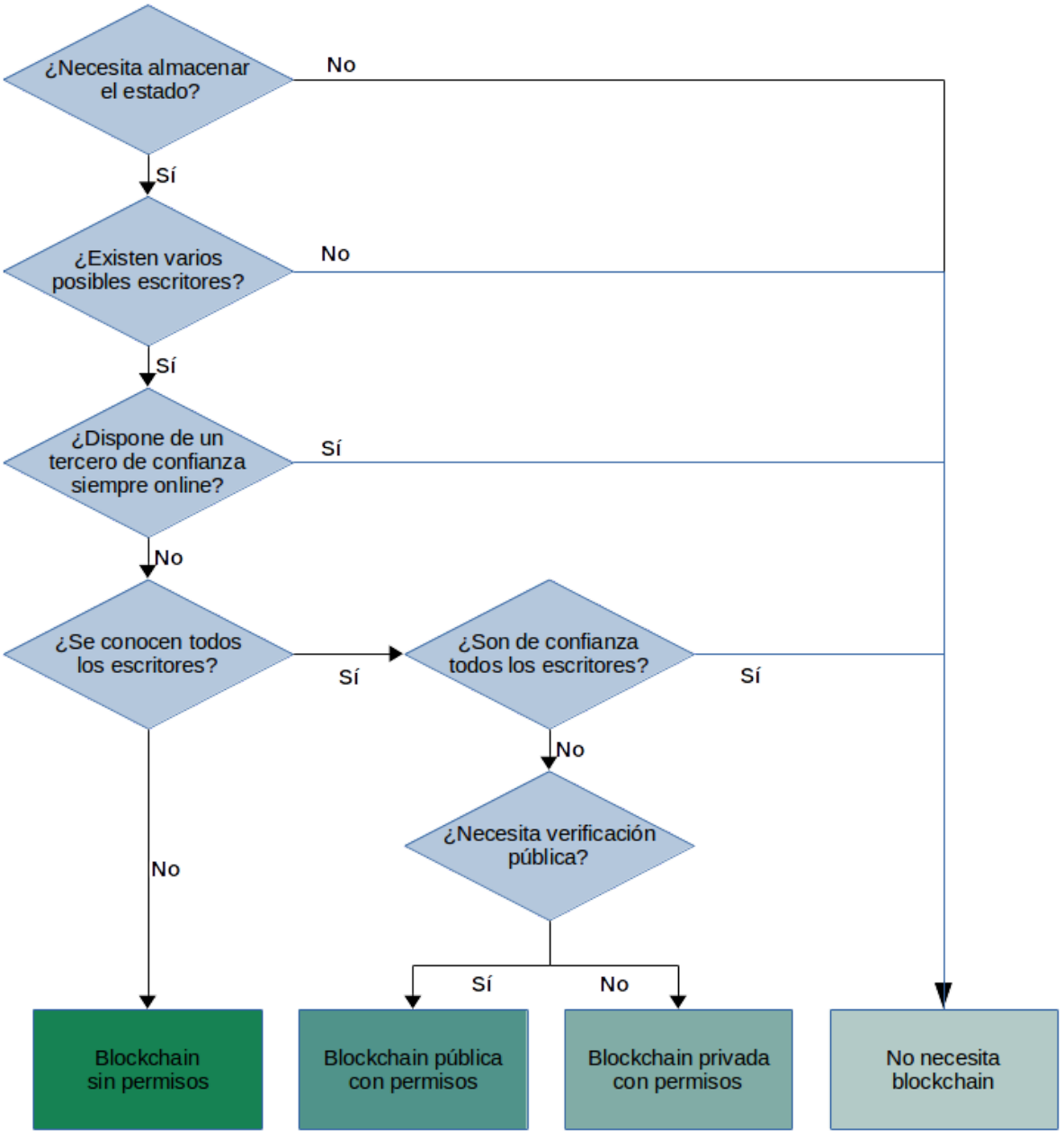
Por último, hay que destacar dos documentos de especial relevancia para el área de estudio de este trabajo: el libro de Ibáñez *Blockchain: Primeras cuestiones en el ordenamiento español* (2018) y el artículo de Porxas y Conejero (2018). El interés de ambos documentos reside en que analizan las RCB desde el punto de vista del ordenamiento jurídico español, con las posibles implicaciones de su adopción en diferentes ámbitos y en que ambos son muy recientes.

En lo que respecta al uso de RCB en el sector público, Porxas y Conejero destacan el proyecto e-Estonia (https://e-estonia.com/) como abanderado en la prestación de servicios digitales, el caso del Bank of England o del gobierno de Suecia en su aplicación a las transacciones inmobiliarias. Fuera de Europa, centra su atención en los ejemplos de países como Ghana, Kenia y Nigeria o en la emisión de monedas virtuales de curso legal previstas en Canadá y Japón (Porxas y Conejero, 2018).

Sobre los retos jurídicos relacionados con la adopción de RCB, Porxas y Conejero inciden en la cautela con que las instituciones y órganos reguladores advierten constantemente en sus comunicaciones, opiniones y estudios cuando mencionan a estas tecnologías. Particularmente, destacan 1) la falta de regulación de estos medios, 2) el alto riesgo que rodea a estas inversiones, 3) su falta de liquidez y su alta volatilidad, 4) la información deficiente de los proyectos y 5) los

posibles fallos de la tecnología. Según las autoras, en tanto se regulan jurídicamente las RCB, debe aplicarse la normativa ya existente a los productos de tecnología innovadora, lo cual plantea verdaderos retos jurídicos derivados de la complejidad de los productos tecnológicos (Porxas y Conejero, 2018).

Imagen 6: Árbol de decisión de Wüst y Gervais



Elaboración propia

4. La tecnología en la administración electrónica

4.1 Concepto y normativa

La conocida como *administración electrónica*, es definida por la Unión Europea como *el uso de las tecnologías de la información y las comunicaciones (TIC) en las administraciones públicas, combinado con cambios organizativos y nuevas aptitudes, con el fin de mejorar los servicios públicos y los procesos democráticos y reforzar el apoyo a las políticas públicas* (COM (2003) 567 UE). Una definición que se centra en la adopción de las TIC por parte de las administraciones públicas, si bien reconoce que este proceso va mucho más allá de la mera adopción de soluciones tecnológicas y supone cambios organizativos con efectos en las políticas públicas y en la percepción que los ciudadanos tienen de su administración.

Actualmente, las principales normas que regulan este ámbito en España son:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPAC)
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante LRJ)
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante ENS)
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (en adelante ENI)
- Normas Técnicas de Interoperabilidad de desarrollo del ENI (NTI)
- Ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante LFE)
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (en adelante LTBG)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD)

Existe otra normativa que también es de aplicación en este ámbito, aunque con menor importancia que la ya citada. Para una referencia completa, puede consultarse el código de administración electrónica editado por el BOE, que compendia toda la normativa vigente en esta materia.

Las administraciones públicas desarrollan su labor y se relacionan entre sí y con los ciudadanos mediante la aplicación de los procedimientos administrativos. Estos procedimientos están diseñados para la ejecución de forma objetiva e imparcial de las competencias y funciones que les han sido atribuidas por la Ley y se materializan en documentos creados por las administraciones tramitadoras o recibidos de personas físicas y jurídicas. Los documentos administrativos son el

testimonio escrito de las diferentes actuaciones administrativas que tienen lugar a lo largo de cada uno de esos procedimientos.

La LPAC señala que la tramitación electrónica debe constituir la actuación habitual de las administraciones y en el art. 70 establece que los expedientes electrónicos *tendrán formato electrónico y se formarán mediante la agregación ordenada de cuantos documentos, pruebas, dictámenes, informes, acuerdos, notificaciones y demás diligencias deban integrarlos, así como un índice numerado de todos los documentos que contenga cuando se remita.* El expediente electrónico se regula en la *Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico* (en adelante NTIEE).

Esta obligación de utilizar el formato electrónico en los expedientes implica que sean electrónicos los documentos administrativos que los integran y que ambos, tanto expedientes como documentos, sean elaborados de acuerdo a lo previsto en el ENI y en las NTI que lo desarrollan. En el caso del documento electrónico, su regulación se recoge en la *Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico* (en adelante NTIDE).

4.2 Implementación electrónica

Desde un punto de vista tecnológico, la elaboración de documentación administrativa consiste en la confección de documentos consignados en un formato informático y constan de tres componentes (art. 26 LPAC y NTIDE):

- **Contenido**, entendido como conjunto de datos o información del documento. Regulado en la *Resolución de 3 de octubre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Catálogo de estándares*
- **Firma(s) electrónica(s)** de funcionarios, de terceros y sellos de tiempo, en su caso.
- **Metadatos**, regulados en la NTIDE y la NTIEE

De manera que los principales recursos tecnológicos utilizados en la elaboración de la documentación administrativa son:

- formatos de documentos
- firmas electrónicas
- sellos de tiempo
- certificados electrónicos
- autoridades de certificación
- códigos seguros de verificación
- metadatos

La firma electrónica consiste en el uso de sistemas de criptografía asimétrica de doble clave utilizados para cifrar el resumen o *hash* de los objetos a firmar, de manera que resulte imposible su alteración posterior sin que se invalide la firma (*garantía de integridad*). En este punto, interviene un prestador de servicios de certificación en quien las partes confían y que es el encargado de garantizar que el par de claves utilizado en la elaboración de una firma electrónica corresponde de forma única e inequívoca al firmante (*garantía de identidad*). A estas dos garantías esenciales de la firma electrónica, se les suele añadir la conocida como *garantía de no repudio*, entendiendo como tal el hecho de que el firmante no puede negar su autoría en la firma producida por existir un conjunto de evidencias asociadas a la firma que así lo demuestran.

Un uso adicional de la firma es el conocido como *sello de tiempo*, consistente la utilización de recursos similares a los descritos para la firma electrónica con la finalidad de que la autoridad de certificación agregue información específica y fehaciente sobre el momento en que se produce esa firma electrónica. Se utiliza para dejar constancia del momento en que tuvo lugar un acto administrativo concreto o la existencia de un documento, cuestión relevante a efectos de procedimiento administrativo por la importancia de los plazos en el mismo.

También se reconoce como sistema de firma válida para la actuación electrónica automatizada el uso del código seguro de verificación o CSV (art. 42.b LRJ), consistente en la asociación de un código único a cada documento que permite comprobar la integridad de dicho documento mediante el acceso a la sede electrónica correspondiente.

4.3 El acceso a la documentación administrativa

Actualmente, las administraciones almacenan sus expedientes y documentos electrónicos en sus propios repositorios, tanto locales como en la nube. En muchas ocasiones, la documentación administrativa debe ser puesta a disposición de terceros que, en virtud de una norma, tienen derecho a conocer el contenido de la misma. Típicamente, se trata de los interesados en el expediente administrativo u otras administraciones públicas que requieren los expedientes administrativos para llevar a cabo sus funciones de control externo (Tribunal de Cuentas, Cámaras de Cuentas Autonómicas, etc…) o la Administración de Justicia

La LPAC reconoce a los interesados una serie de derechos relacionados con la documentación administrativa:

- Derecho a comunicarse a través de un Punto de Acceso General Electrónico de la Administración (art. 13)
- Derecho a no aportar documentos que ya obren en las AAPP, para lo que se presumirá que la consulta es autorizada salvo que conste oposición expresa (art. 28)
- Derecho a conocer el estado de tramitación de sus expedientes, y a obtener copias de los documentos (art. 53)

Esto obliga a las administraciones a compartir entre sí información relativa a la documentación de la que disponen y proporcionar los documentos correspondientes a otras administraciones que pudieran requerirlos para la tramitación de nuevos expedientes.

Se estima que el número de administraciones públicas existentes en España supera las 18.000 (Núñez, 2016), con sus correspondientes sedes electrónicas, portales de transparencia, portales de datos abiertos, etc. Esta disgregación constituye un auténtico hándicap para el ciudadano que necesita obtener documentación administrativa tanto de contenido personal como documentación de acceso público. Asimismo, constituye un desafío para una administración que necesite acceder a cualquier documento que el ciudadano manifieste que ya obra en poder de otra administración y deba ser obtenido directamente de ésta.

El Punto de Acceso General

Con este fin, la LPAC dispone en el artículo 13 la existencia de un Punto de Acceso General electrónico de la Administración (en adelante PAG) a través del que los ciudadanos podrán comunicarse con la administración y ejercer su derecho de acceso y obtención de copias de los documentos contenidos en los procedimientos (art. 53).

Por otra parte, el acceso a la documentación administrativa debe garantizar el derecho a la confidencialidad y a la protección de los datos personales que constan en gran parte de los expedientes administrativos. Esta es la razón por la que el acceso al PAG se realiza previa identificación del ciudadano y la documentación que se pone a su disposición se limita a aquélla en la que consta como interesado.

En lo que respecta a las administraciones públicas, el intercambio de expedientes electrónicos, a los efectos de remisión y puesta a disposición, se realizará según lo dispuesto en la NTIEE, donde se especifica la información y el formato que deberá tener el índice electrónico del expediente y los metadatos obligatorios que deberán asociarse al expediente administrativo. El índice electrónico es *un objeto digital que contiene la identificación sustancial de los documentos electrónicos que componen el expediente debidamente ordenada para reflejar la disposición de los documentos, así como otros datos con el fin de preservar la integridad y permitir la recuperación del mismo*, en los términos del artículo 70.3 de la LPAC.

La propuesta de uso de una RCB en el ámbito de la administración electrónica que se hace en el capítulo 6 de este trabajo persigue dar respuesta a estas necesidades de puesta a disposición y acceso a la documentación entre administraciones y a los interesados en los expedientes tramitados.

5. Blockchain en la administración electrónica

La actual expansión de los servicios de administración y gobierno electrónico (*e-government*) impulsados por las administraciones públicas está coincidiendo en el tiempo con las investigaciones sobre las aplicaciones de las RCB, de manera que son numerosas las iniciativas que indagan sobre las posibles aplicaciones de esta tecnología en el ámbito de la gestión pública, hasta el punto que el estudio de Konstantinidis identifica este ámbito como el que cuenta con un mayor número de investigaciones en desarrollo (Konstantinidis et alt., 2018).

Las RCB pueden tener diferentes aplicaciones en el terreno del gobierno electrónico: plataforma para sistemas de voto electrónico; sistema de registro, tanto fehaciente como trivial, de documentos públicos o propiedades; contabilidad pública y mecanismo de auditoría empresarial; infraestructura de identidad digital; centro de contratación; mecanismo de transmisión de derechos de contenido patrimonial o, finalmente, espacio de cumplimiento normativo de carácter tributario y de derecho administrativo (Ibánez, 2018). El abanico de posibilidades que ofrece es enorme y por la propia naturaleza de la materia administrativa, requiere tanto del diseño de soluciones tecnológicas como de la adopción de medidas regulatorias asociadas que doten al sistema de la validez y garantías jurídicas exigibles en derecho, tal como analiza la obra de Ibáñez (2018).

5.1 Las RCB en la administración electrónica

Si circunscribimos el análisis del uso de las RCB al ámbito de la administración electrónica, entendida ésta en los límites de la normativa contemplada en el capítulo 4, las materias en las que puede resultar adecuado el uso de una RCB son:

Registros

Las administraciones públicas mantienen libros de registro donde realizan asientos y anotaciones de intercambio en los que centralizan información relevante, de manera que están en disposición de consultarla cuando sea necesario (Porxas y Conejero, 2018). En el ámbito de la administración electrónica, se mantienen registros de documentos (art. 16 LPAC) y de habilitaciones de funcionarios y de apoderamientos de terceros (art. 5 y 6 LPAC). Los registros de titularidades de propiedad inmobiliaria, de propiedad intelectual, de patentes y marcas, etc… quedan fuera de ese ámbito de regulación.

La validez de estos registros descansa en el concepto de fe pública, entendida como *la calidad que el Estado otorga a una serie de personas en virtud de la cual se consideran ciertos y veraces los hechos que reflejan* (Guías jurídicas Wolters Kluwer). La fe pública se articula de forma

práctica mediante la habilitación a algún funcionario, sea un secretario de habilitación nacional, un registrador, un notario… capacitado para dejar constancia fehaciente de hechos, acuerdos o del contenido de los registros, entre otros.

La características de las RCB de constancia pública, transparencia, irrevocabilidad e inmutabilidad, las hacen candidatas idóneas para ser utilizada como registro de información con prueba de movimientos y trazabilidad, tal como reconocen varios autores (Porxas y Conejero, 2018) (Goderdzishvili et alt., 2018) (Alketbi et alt., 2018) (Ølnes, 2017 b), especialmente las RCB con permisos (Ibáñez, 2018).

Identificación digital

La LPAC regula los sistemas de identificación y firma electrónica en los artículos 9 a 11. El art. 9 obliga a las administraciones públicas a verificar la identidad de los interesados en el procedimiento administrativo, tanto en sus relaciones presenciales como electrónicas. El concepto de *identidad digital* aúna las tecnologías utilizadas para la acreditación de la identidad y la expresión de la voluntad de las personas en el ámbito electrónico. Con esta finalidad se utilizan recursos que combinan las conocidas como las tres garantías de identidad: algo que se sabe (una contraseña, un pin...), algo que se tiene (un dispositivo móvil, una tarjeta inteligente…) y algo que se es (información biométrica como una huella digital, reconocimiento facial…).

En este campo, la tecnología blockchain ha hecho una aportación destacada: las plataformas de identidad digital soberana o *self-sovereign identity* (SSI), que *generan en la red un token (en un bloque de la cadena) donde se contienen todos los atributos o características que permiten la identificación de la persona* (Ibáñez, 2018). De nuevo cabe mencionar el caso de la plataforma española de identidad digital Alastria (https://alastria.io/#1), que aspira a unificar la identidad digital soberana de personas de nacionalidad española.

Contratación pública

Las RCB aplicadas a la contratación pública están aportando beneficios en aspectos como la necesaria confidencialidad de las ofertas recibidas en una licitación, las posibilidades de uso de los contratos inteligentes para automatizar el proceso de adjudicación o las evidencias temporales, de integridad y de inmutabilidad de los documentos y actos administrativos que se producen a lo largo del proceso de licitación pública.

De nuevo cabe mencionar la plataforma Alastria, que cuenta entre sus asociados con el Gobierno de Aragón, primera Comunidad Autónoma que se integra en este consorcio multisectorial que desarrolla la primera RCB pública permisionada de ámbito nacional. Entre sus primeros proyectos, se encuentra el uso de una RCB para el registro de las ofertas que se reciben para los contratos públicos y su evaluación automatizada mediante contratos inteligentes. También se va a estudiar la posibilidad de utilizar la cadena de bloques para la constitución de avales y garantías asociados a los contratos públicos.

Actuación administrativa automatizada

El artículo 41 de la LRJ define la actuación administrativa automatizada como *cualquier actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público*. A su vez, el proyecto de Reglamento de desarrollo de la LPAC y la LRJ, actualmente en fase de borrador, establece que la forma de tramitación preferente para llevar a cabo una actuación administrativa cualquiera, será la actuación administrativa automatizada, lo cual da una idea de la intención del legislador de potenciar al máximo esta figura.

En esta materia, las RCB pueden resultar de gran ayuda al aportar una verificación distribuida de las actuaciones que se llevan a cabo, combinada con la inmutabilidad de las operaciones anotadas en el libro maestro. Estas evidencias propias de las RCB, convenientemente respaldadas por una normativa acorde, pueden actuar como garantes en la actuación automatizada u otros procesos sin intervención directa de personas, permitiendo aumentar su cobertura y prescindir de recursos que requieren de terceros de confianza, como la firma con sello de órgano.

Otros usos administrativos

Las RCB pueden resultar beneficiosas en el ámbito administrativo en otros asuntos, como la práctica de notificaciones, el intercambio de información y la interoperabilidad entre administraciones, la práctica de diligencias cruzadas, el intercambio de asientos registrales, etc… (Ibáñez, 2018).

5.2 Retos de la aplicación de las RCB en la administración

Como ya se vio en la revisión bibliográfica, el principal riesgo señalado por los investigadores en la adopción temprana de las tecnologías basadas en las RCB es la falta de estandarización (Ølnes, 2017 b). La falta de madurez de las RCB se considera como uno de los mayores retos para su adopción de manera generalizada. Por otra parte, forzar un estándar demasiado prematuro podría acarrear la ralentización de la tecnología y causar futuros problemas de interoperabilidad y optimización.

También se señalan con frecuencia otros problemas asociados a las RCB de índole tecnológica, como es la lentitud en la grabación de nuevas transacciones. Este es un problema con particular incidencia en el caso de las RCB públicas, con demoras del orden de minutos en la grabación y

confirmación de transacciones, pero que en el caso de las redes con permisos se reducen a segundos o incluso fracciones de segundo (Ølnes, 2017 b). También se suelen señalar sus problemas de escalabilidad, ineficiencia de recursos computacionales y energéticos o de tamaño de la cadena de bloques como retos para su adopción masiva (Batubara et alt., 2018).

En cuanto a los retos a superar de carácter normativo, ya se ha indicado también (Porxas y Conejero, 2018) (Ibáñez, 2018) la necesidad de una regulación clara de la materia, especialmente para poder ser utilizada con garantías en el ámbito administrativo.

Otro de los retos planteados por las RCB es la preservación a largo plazo de los registros almacenados en la cadena de bloques (Hou, 2017), asunto nada trivial en el ámbito administrativo en el que se encuentra perfectamente regulada la conservación de la información en archivos electrónicos en los que los documentos deben conservarse durante diferentes plazos según su relevancia. También debe analizarse cómo se procedería a su expurgo si la información almacenada en la cadena de bloque resulta inmutable.

Tal como señala Ølnes respecto al proyecto sobre RCB desarrollado por la administración tributaria noruega, uno de los problemas apuntados en sus conclusiones es la inmutabilidad de la información registrada y el ejercicio del derecho de supresión, más conocido como derecho al olvido reconocido por el RGPD y la LOPDGDD española (Ølnes, 2017 b).

También cabe señalar que las RCB no están exentas de posibles fallos de la tecnología. Si bien la red Bitcoin ha dado pruebas de gran fiabilidad y resistencia a los ataques, otras redes han resultado afectadas por graves incidentes de seguridad, como es el caso de Ethereum y el ya mencionado ‘The DAO’.

6. Repositorio centralizado de referencias a documentos y expedientes electrónicos elaborados por las administraciones públicas

En este trabajo proponemos utilizar una RCB como registro centralizado para la documentación elaborada por las administraciones públicas. Su finalidad es dar respuesta a las necesidades de puesta a disposición y acceso a la documentación entre administraciones y a los interesados vista en el apartado 4.3.

Las **administraciones** accederán al registro a través de la red SARA para la puesta a disposición de expedientes administrativos a las administraciones que, en virtud de una norma, deban obtener dichos expedientes en el formato previsto en el ENI y en las NTI, permitiendo obtener su índice directamente de la información obrante en la RCB, así como los documentos que lo integran a través de los correspondientes servicios o urls consignados en la anotación de cada documento. Mediante este acceso se da respuesta al derecho de los ciudadanos a no aportar documentos que ya obren en poder de las administraciones públicas.

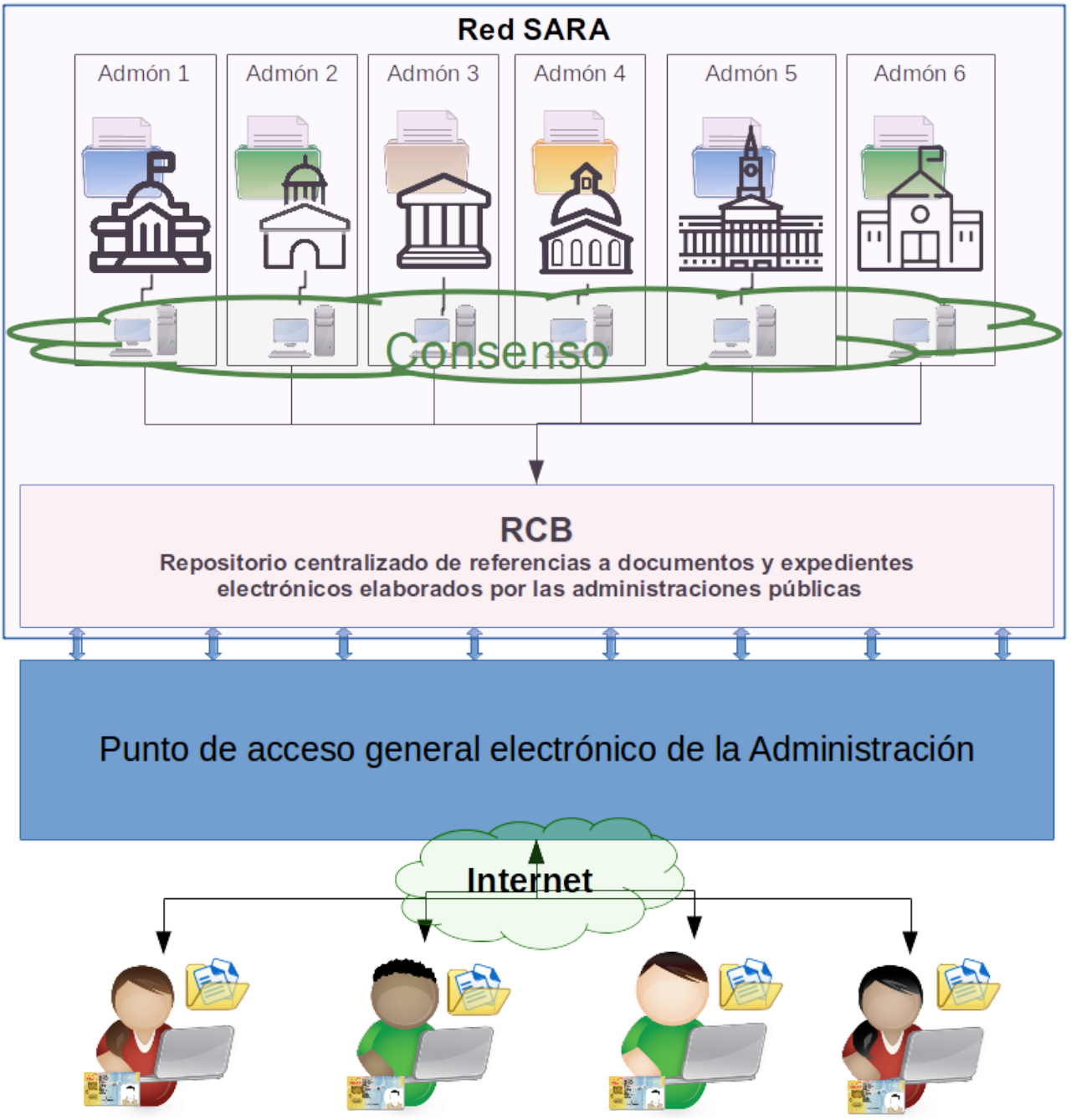
Para los **ciudadanos**, este registro se configura como un sistema de información documental asociado al Punto de Acceso General, al que los interesados pueden acceder previa identificación, para conocer los documentos que conforman un expediente administrativo en el que consten como interesados.

Las anotaciones en este registro serán transacciones en una RCB en las que se hará constar la información correspondiente a cada expediente que las administraciones elaboren y a cada documento que forme parte de un expediente: identificación de la entidad tramitadora, metadatos obligados por el ENI para cada documento y expediente, su hash o resumen, código seguro de verificación asociado por la administración tramitadora a dicho documento, interesados en el expediente, url o servicio web que permite recuperarlo y nivel de autorización de acceso (ver detalle en la sección 6.3).

Las anotaciones harán uso de las plataformas que la AGE ha puesto en marcha para articular los servicios de administración electrónica comunes, como es el caso del Directorio Común de Unidades Orgánicas y Oficinas (DIR3) para identificar a los órganos tramitadores o el Sistema de Información Administrativa (SIA) para asociar los expedientes a los procedimientos administrativos de cada entidad.

La RCB no albergará físicamente los documentos y expedientes registrados. Éstos permanecerán en los repositorios de la administración emisora y serán registrados en la RCB, que dejará así constancia del momento de su generación.

Imagen 7: Registro de documentación administrativa sobre RCB



Elaboración propia

Las ventajas derivadas de la implantación de este registro frente al sistema actual, en que cada administración conoce de manera exclusiva los expedientes y documentos que tramita son:

- Mayor transparencia en la información sobre la documentación administrativa, que pasa a ser común a todas las administraciones.
- Constancia temporal de cada documento garantizada directamente por la RCB.
- Integridad e inmutabilidad de los documentos registrados en la RCB, proporcionada por la inclusión de su CSV y su hash en la anotación en la cadena de bloques.
- Obtención directa por parte de las administraciones del índice electrónico de los expedientes registrados y sus documentos.
- Obtención de documentos por parte de los interesados a través del Punto de Acceso General desde cualquier administración tramitadora.

Como desventaja, se debe apuntar que los beneficios del uso de una RCB para funciones de registro, mencionados en el apartado 5, se basan fundamentalmente en la constancia pública, la transparencia, la irrevocabilidad y la inmutabilidad de las anotaciones realizadas en la cadena de bloques. Al basarse el modelo propuesto en una RCB privada, el carácter público de constancia de las anotaciones se pierde, quedando limitada a las administraciones usuarias del sistema. Únicamente los casos en los que el contenido del registro sea completamente público podrán beneficiarse de todas las ventajas provistas por las RCB, tal como sucede en el caso de la red bitcoin, cuyo principal valor deriva del carácter público, abierto y distribuido de su registro.

6.1 Adecuación y tipo de RCB más conveniente

Para determinar si resulta adecuado el uso de una RCB en el caso de uso propuesto en este trabajo y qué tipo de red es la más apropiada, usaremos el árbol de decisión propuesto por Wüst y Gervais (2017) (ver Imagen 6).

En la decisión acerca de si es necesario almacenar el estado de la documentación registrada, la respuesta es afirmativa: la finalidad de la red propuesta es almacenar de forma fehaciente la información sobre los expedientes administrativos y sus documentos.

La segunda decisión cuestiona si existirán varios posibles escritores. El modelo propuesto pretende prestar servicio a todas las administraciones públicas. Éstas deberán poder anotar en la cadena de bloques las referencias a cuantos expedientes y documentos elaboren en el desarrollo de sus competencias, así que la respuesta es afirmativa.

La tercera decisión cuestiona la posibilidad de disponer de un tercero de confianza siempre en línea como garante de las anotaciones realizadas. El registro que se propone pretende que sean

las propias administraciones públicas quienes realicen las anotaciones y que la propia cadena de bloques asegure la información que contiene, haciendo innecesario un tercero de confianza.

Respecto a si todas las entidades autorizadas para hacer anotaciones en la cadena se conocen, la respuesta es afirmativa: sólo las administraciones públicas previamente autorizadas podrán realizar anotaciones en la RCB.

Para la siguiente decisión, hay que considerar que la finalidad del registro propuesto es que las administraciones usuarias dejan constancia fehaciente de la documentación elaborada ante las demás, como prueba de transparencia pública de la actuación administrativa. De manera que, aunque todos los posibles escritores pudieran ser de confianza, actúan como si no lo fuesen en aras de la transparencia.

Finalmente, a la cuestión sobre si es necesaria la verificación pública del contenido de la cadena, la respuesta es negativa. Para garantizar el derecho a la protección de datos personales, el acceso al contenido de la cadena no puede ser público.

La aplicación del árbol de Wüst y Gervais lleva finalmente a la adopción de una RCB de tipo privada con permisos del apartado 2.4. Se trata de una red a la que sólo los nodos autorizados pueden acceder, tanto para la lectura de su contenido como para participar en el mecanismo de consenso o generar nueva información a agregar a la cadena.

6.2 Usuarios y nodos

Las administraciones públicas serán las responsables de gestionar los nodos con capacidad para registrar transacciones y para crear nuevos bloques en la cadena. La administración de la membresía podría corresponder bien a una administración que actuará como responsable del sistema o a un organismo participado por varias administraciones.

Las administraciones disponen de un conjunto de infraestructuras de comunicaciones y servicios básicos que conecta las redes de las Administraciones Públicas Españolas e Instituciones Europeas, facilitando el intercambio de información y el acceso a estos servicios. Es la llamada Red SARA, que en nuestro modelo, proporcionará una capa adicional de seguridad al exigirse que los nodos autorizados por las administraciones para generar transacciones y participar en el mecanismo de consenso accedan exclusivamente a través de esta infraestructura de red. Este acceso asegura que los nodos pertenecen a una administración pública.

El acceso identificado a través de la red interadministrativa, permitirá ofrecer servicios exclusivos a aquellas administraciones que, en base a una norma, dispongan de un nivel de acceso privilegiado, como es el caso de la administración de justicia o de los órganos de control externo (Tribunal de Cuentas o Cámaras de Cuentas Autonómicas) en sus funciones de fiscalización.

El acceso de los ciudadanos a la información custodiada en la cadena de bloques se realiza con identificación electrónica a través del Punto de Acceso General y la información obtenida será, exclusivamente, la correspondiente a los expedientes en los que conste como interesado.

6.3 El registro de documentos y expedientes como transacciones en una RCB

Las transacciones a registrar en el modelo propuesto estarán constituidas por anotaciones de registro de documentos y de expedientes electrónicos que se agruparán en bloques. Los bloques estarán encadenados entre sí mediante la inclusión del resumen criptográfico del bloque anterior en cada nuevo bloque que se genere, tal como se ha descrito en el funcionamiento de las redes RCB. Entre los tipos de redes RCB existentes, proponemos la utilización de una red Ethereum con acceso privado, dada su capacidad para alojar en la cadena de bloques cualquier tipo de dato (ver sección 2.3). A continuación, se propone una estructura de contenido para estas anotaciones, una para realizar el registro de expedientes electrónicos y otra para registrar documentos.

Tabla 2: Anotaciones de expedientes en la cadena de bloques

<table>
<tr><td></td><td colspan="3">Anotaciones [1...n] de expedientes</td></tr>
<tr><td rowspan="8">Anotaciones [1...n] de expedientes</td><td>Versión</td><td colspan="2">Valor utilizado para control de futuras versiones de este modelo</td></tr>
<tr><td>DIR3</td><td colspan="2">Identificador de la entidad tramitadora</td></tr>
<tr><td>Time</td><td colspan="2">Sello de tiempo actual en segundos desde 1970-01-01T00:00 UTC</td></tr>
<tr><td>Nivel de acceso al expediente</td><td colspan="2">Público, interesados o privado</td></tr>
<tr><td></td><td colspan="2">Metadatos obligatorios expediente electrónico (Anexo 1 NTIEE)</td></tr>
<tr><td></td><td>Metadato</td><td>Valor</td></tr>
<tr><td rowspan="2">Metadatos obligatorios</td><td>Versión NTI</td><td>Identificador normalizado de la versión de la Norma Técnica de Interoperabilidad de Expediente electrónico conforme a la cual se estructura el expediente</td></tr>
<tr><td>Identificador</td><td>Identificador normalizado del expediente</td></tr>
</table>

		Órgano	Identificador normalizado de la administración responsable de la tramitación del procedimiento (DIR3)
		Fecha de apertura	Fecha de apertura del expediente
		Clasificación	Procedimiento administrativo con el que se relaciona el expediente (SIA)
		Estado del expediente en el momento de intercambio	Abierto, cerrado, índice para remisión cerrado
		Interesado [1...n]	Si ciudadano o persona jurídica: DNI, NIE, NIF o similar. Si administración DIR3
		Valor CSV	Valor del CSV asociado al expediente

Tabla 3: Anotaciones de documentos en la cadena de bloques

	Anotaciones [1...n] de documentos	
Anotaciones [1...n] de documentos	Versión	Valor utilizado para control de futuras versiones de este modelo
	DIR3	Identificador de la entidad tramitadora
	Time	Sello de tiempo actual en segundos desde 1970-01-01T00:00 UTC
	Valor CSV	Valor del CSV asociado al documento
	Hash del documento	Resumen criptográfico Sha-2 del documento
	Identificador de expediente	Identificador normalizado del expediente al que pertenece (ver tabla 3)
	Path en el expediente	Ruta con la ubicación del documento en la estructura de carpetas del expediente
	Nivel de acceso al documento	Público, interesados o privado
	Acceso al documento	Servicio web, url…
		Metadatos obligatorios documento electrónico (Anexo 1 NTIDE)

		Metadato	Valor
	Metadatos obligatorios	Versión NTI	Identificador normalizado de la versión de la Norma Técnica de Interoperabilidad de Documento electrónico conforme a la cual se estructura el documento electrónico
		Identificador	Identificador normalizado del documento
		Órgano	Identificador normalizado de la administración generadora del documento o que realiza la captura del mismo (DIR3)
		Fecha de captura	Fecha de alta del documento en el sistema de gestión documental
		Origen	Indica si el contenido del documento fue creado por un ciudadano o por una administración
		Estado de elaboración	Indica la naturaleza del documento
		Nombre de formato	Formato lógico del fichero de contenido del documento electrónico
		Tipo documental	Descripción del tipo documental del documento

Elaboración propia

7. Conclusiones

Los beneficios potenciales de las RCB en su uso en el ámbito del gobierno y la administración electrónica son prometedores. La información contenida en una RCB está asegurada y certificada por los nodos que la registran, quienes la comprueban y validan mediante mecanismos de consenso, de manera que resulta innecesario el concurso de un tercero de confianza. Además, su carácter distribuido ofrece sistemas seguros de gran estabilidad y resistencia a los ataques. Su seguridad, combinada con su resistencia al fraude y la manipulación, convierten a este tipo de redes en candidatas ideales para alojar información administrativa.

Sin embargo, su uso presenta todavía numerosas incógnitas constatadas en los proyectos analizados en la bibliografía revisada, debidas principalmente a que se trata de una tecnología poco evolucionada y carente de un estándar normalizado. Esta situación lastra especialmente su adopción en la administración electrónica, una materia en la que la regulación normativa y procedimental juega un papel central. Tampoco se trata de una tecnología que ofrezca algo completamente nuevo que no se pueda hacer con una simple base de datos por ejemplo, sino que hace lo mismo que otras herramientas ya existentes pero añadiendo una serie de garantías adicionales como la integridad e inmutabilidad de la información almacenada y que la confianza en su contenido la proporcionan los propios participantes en el sistema.

El caso de uso de una RCB que se propone en este trabajo consiste en una plataforma que funciona como un registro de toda la documentación administrativa que se tramita en cualquier administración pública española y que sirve de fuente de información para las propias administraciones públicas y para los servicios proporcionados a los ciudadanos a través del Punto de Acceso General.

En el proceso de diseño se han encontrado retos, como el hecho de que la información administrativa está sujeta a la confidencialidad derivada del derecho a la protección de los datos personales que constan en los documentos, lo cual obliga a renunciar al uso de una RCB pública. La consecuencia es la pérdida de una de las fortalezas de estos sistemas: su carácter público y descentralizado. Se trata de nuevo de una dicotomía clásica en el ámbito administrativo: el difícil equilibrio entre la transparencia y la protección de datos.

El resultado es un sistema que aporta pocos beneficios frente al uso de una base de datos, tan sólo el carácter distribuido de la RCB que aporta tanto estabilidad y seguridad ante posibles ataques malintencionados como la garantía de constancia de los documentos entre las propias administraciones derivada de la participación de las mismas en el mecanismo de consenso.

En definitiva, aunque el uso de las tecnologías basadas en cadenas de bloques prometen deparar grandes beneficios en el ámbito administrativo, su implementación no resulta en absoluto evidente y necesitan mayor madurez, más investigación sobre sus posibles aplicaciones y una regulación específica que reconozca sus puntos fuertes para impulsar su adopción con garantías en la administración electrónica.

8. Referencias y bibliografía

Alketbi, A., Nasir, Q., & Talib, M. A. (2018). *Blockchain for government services-Use cases, security benefits and challenges*. En *2018 15th Learning and Technology Conference, L and T 2018*. Consultado en https://doi.org/10.1109/LT.2018.8368494

Anand, A., Kok, A., Makala, B. et alt. (2018). *The Legal Aspects of Blockchain*. UNOPS. Consultado en https://www.blockchainpilots.nl/books Accedido el 10/01/2019.

Anwar, H. (2018). *2019 The Year of the Federated Blockchain – Blockchain Consortium Simply Explained*. En *101blockchains.com*. Consultado el 10 de enero de 2019 en https://101blockchains.com/federated-blockchain/

Atzori, M. (2017). *Blockchain Technology and Decentralized Governance:Is the State Still Necessary?* En *Journal of Government & Regulation*. Consultado en https://doi.org/10.22495/jgr_v6_i1_p5

Batubara, F. R., Ubacht, J., & Janssen, M. (2018). *Challenges of blockchain technology adoption for e-government: a systematic literature review*. En *Proceedings of the 19th Annual International Conference on Digital Government Research Governance in the Data Age - dgo '18* (pp. 1–9). New York, New York, USA: ACM Press. Consultado en https://doi.org/10.1145/3209281.3209317

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). *Zerocash: Decentralized anonymous payments from bitcoin*. En Proceedings - IEEE Symposium on Security and Privacy. Consultado en https://doi.org/10.1109/SP.2014.36

Bheemaiah, K. (2015). *Block Chain 2.0: The Renaissance of Money*. En *Wired*. Consultado el 12 de diciembre de 2018 en https://www.wired.com/insights/2015/01/block-chain-2-0/

Bull, G. (2018). *Blockchain: A Solution in Search of a Problem?* Consultado el 17 de octubre de 2018 en http://www.cgap.org/blog/blockchain-solution-search-problem

Buterin, V. (2014). *A Next Generation Smart Contract & Decentralized Application Platform*. *Etherum White Paper*. Consultado en https://doi.org/10.5663/aps.v1i1.10138

Casino, F., Dasaklis, T. K., & Patsakis, C. (2018). *A systematic literature review of blockchain-based applications: Current status, classification and open issues*. Consultado en https://doi.org/10.1016/j.tele.2018.11.006

Davidson, S., De Filippi, P., & Potts, J. (2016). *Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology*. En *SSRN Electronic Journal*. Consultado en https://doi.org/10.2139/ssrn.2811995

Douceur, J. R. (2002). *The Sybil Attack*. En *Peer-to-Peer Systems - 1st International Workshop* (Vol. 2429, pp. 251–260). Consultado el 18 de octubre de 2018 en http://search.ebscohost.com/login.aspx?direct=true&db=&AN=&site=eds-live

Goderdzishvili, N., Gordadze, E., & Gagnidze, N. (2018). *Georgia's blockchain-powered property registration: Never blocked, always secured - Ownership data kept best!*. En *ACM International Conference Proceeding Series*. Consultado en https://doi.org/10.1145/3209415.3209437

Hou, H. (2017). *The application of blockchain technology in E-government in China*. En *2017 26th International Conference on Computer Communications and Networks, ICCCN 2017*. Consultado en https://doi.org/10.1109/ICCCN.2017.8038519

Ibáñez J. (2018). *Blockchain : Primeras cuestiones en el ordenamiento español*. Madrid:Dykinson. Consultado en http://mendeley.csuc.cat/fitxers/0773a74c22bee295dc97ae459e69a7fb

Konashevych, O. (2017). *The concept of the blockchain-based governing: Current issues and general vision*. En *Proceedings of the European Conference on e-Government, ECEG*, 79–85.

Konstantinidis, I., Siaminos, G., Timplalexis, C., Zervas, P., Peristeras, V., & Decker, S. (2018). *Blockchain for business applications: A systematic literature review*. En *Lecture Notes in Business Information Processing* (Vol. 320, pp. 384–399). Consultado en https://doi.org/10.1007/978-3-319-93931-5_28

Jun, M. (2018). *Blockchain government - a next form of infrastructure for the twenty-first century*. En *Journal of Open Innovation: Technology, Market, and Complexity*, *4*(1), 7. Consultado en https://doi.org/10.1186/s40852-018-0086-3

Meijer, D., & Ubacht, J. (2018). *The Governance of Blockchain Systems from an Institutional Perspective, a Matter of Trust or Control?*. En *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age* (p. 90:1--90:9). New York, NY, USA: ACM. Consultado en https://doi.org/10.1145/3209281.3209321

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Satoshi Nakamoto Institute. Consultado el 14 de octubre de 2018 en http://nakamotoinstitute.org/bitcoin/

Narayanan, A. (2018). *Written Testimony of Arvind Narayanan Associate Professor of Computer Science, Princeton University United States Senate, Committee on Energy and Natural Resources Hearing on Energy Efficiency of Blockchain and Similar Technologies*. Consultado el 22 de octubre de 2018 en https://www.cell.com/joule/fulltext/S2542-4351

Nordrum, A. (2017). *Govern by blockchain dubai wants one platform to rule them all, while Illinois will try anything*. *IEEE Spectrum*. Consultado en https://doi.org/10.1109/MSPEC.2017.8048841

Núñez, F. (2016). *España: Un Estado con un "puzle" de 18.850 administraciones*. *El Mundo* (26 de junio de 2016). Consultado el 10 de enero de 2019 en https://www.elmundo.es/economia/2016/06/26/576ae93222601d985f8b45f0.html

Ølnes, S. (2016). *Beyond Bitcoin Enabling Smart Government Using Blockchain Technology*. En *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (pp. 253–264). Consultado en https://doi.org/10.1007/978-3-319-44421-5_20

Ølnes, S., & Jansen, A. (2017 a). *Blockchain Technology as Infrastructure in Public Sector – an Analytical Framework*. En *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Consultado en https://doi.org/10.1007/978-3-319-64677-0_18

Ølnes, S., Ubacht, J., & Janssen, M. (2017 b). *Blockchain in government: Benefits and implications of distributed ledger technology for information sharing*. En *Government Information Quarterly*, *34*(3), 355–364. Consultado en https://doi.org/10.1016/j.giq.2017.09.007

Porxas, N., & Conejero, M. (2018). *Tecnología blockchain: funcionamiento, aplicaciones y retos jurídicos relacionados*. En *Actualidad Juridica* (1578-956X), (48)

Rooney, K. (2018). *Apple co-founder Steve Wozniak says the hype around blockchain signals a bubble*. CNBC (26 de junio de 2018). Consultado el 10 de enero de 2019 en https://www.cnbc.com/2018/06/26/apple-co-founder-steve-wozniak-says-blockchain-hype-signals-bubble.html

Shermin, V. (2017). *Disrupting governance with blockchains and smart contracts*. En *Strategic Change*. Consultado en https://doi.org/10.1002/jsc.2150

Sward, A., Vecna, I., & Stonedahl, F. (2018). *Data Insertion in Bitcoin's Blockchain*. En *Ledger*. Consultado en https://doi.org/10.5195/LEDGER.2018.101

Szabo, N. (1997). *Formalizing and securing relationships on public networks*. En *First Monday*. Consultado en https://doi.org/10.5210/fm.v2i9.548

Stokes, M., & Freire, G. (2017). *Smart Contracts*. En *Actualidad Jurídica* (1578-956X) (46), págs. 124–127

Wolters Kluwer (2019). *Guías jurídicas*, [en línea]. Madrid. Consultado el 6 de enero de 2019 en http://guiasjuridicas.wolterskluwer.es

Wüst, K., & Gervais, A. (2017). *Do you need a Blockchain?* IACR Cryptology EPrint Archive. Consultado en https://doi.org/10.1109/CVCBT.2018.00011

ANEXO I: Glosario

ASIC: acrónimo de *application-specific integrated circuit* o circuito integrado de aplicación específica. Se trata de circuitos diseñados para un uso en particular, en el caso de los equipos de minado, son circuitos especializados en el cálculo de números hash de acuerdo al algoritmo que se utilice en la red de la criptomoneda a minar: SHA-256 en el caso de Bitcoin..

Ataque del 51% o ataque Sybil: en el supuesto de que alguien malintencionado llegara a controlar la mayor parte de la red, podría modificar la cadena de bloques a su antojo imponiendo la información que desee, aprovechando su posición de dominio en el consenso.

Bloque: un registro incluido en la cadena de bloques que contiene confirmaciones de transacciones pendientes. En la red Bitcoin, se genera un nuevo bloque aproximadamente cada 10 minutos. Éste incluye las nuevas transacciones y se anexa a la cadena de bloques mediante el proceso del minado. Una vez incluido el bloque en la cadena, las transacciones se confirman mediante la propagación del bloque por la red.

Cadena de bloques: es un registro público de las transacciones realizadas con una criptomoneda a lo largo del tiempo en orden cronológico. La cadena de bloques es pública y se comparte entre todos los usuarios de la red p2p. Se utiliza para verificar la integridad de las transacciones y para prevenir el doble gasto.

Contrato inteligente (*Smart contract*): "*mecanismo que involucra activos digitales y dos o más partes, donde algunas o todas las partes ponen activos y los activos se redistribuyen automáticamente entre esas partes de acuerdo con una fórmula basada en ciertos datos que no se conocen en el momento en que se inicia el contrato*" (Buterin, 2014).

Criptomoneda: se refiere al dinero que sólo se transfiere por medios electrónicos. También se conoce como *moneda digital* o *moneda electrónica*.

Firma electrónica: conjunto de datos electrónicos que acompañan o que están asociados a un documento u operación electrónica, que permiten identificar al firmante de forma inequívoca y asegurar la integridad del documento o datos firmados.

Hash: un hash, o resumen, es un conjunto de información electrónica de longitud fija, producida por un algoritmo que se aplica sobre una cantidad arbitrariamente grande de datos. Un hash concreto siempre será el resultado de los mismos datos; sin embargo, cualquier modificación de la información, por mínima que sea, producirá como resultado un hash completamente distinto.

Mempool: conjunto de transacciones verificadas como válidas que han sido transmitidas a la red de la cadena de bloques y que están a la espera de ser incluidas en un bloque válido. Estas

transacciones son verificadas por los nodos mineros y eventualmente, añadidas a un nuevo bloque que se enlazará en la cadena de bloques.

Minado: proceso de cálculo de un nuevo bloque que se añadirá a la cadena de bloques. El bloque debe cumplir una serie de requisitos que lo hacen muy costoso de calcular para ser válido. El nodo minero que antes logre calcular un bloque válido recibe una recompensa por su trabajo en forma de criptomonedas. La finalidad del minado es asegurar que nadie usa las monedas dos veces (*doble gasto*) y que nadie pueda introducir en el sistema criptomonedas falsas.

Monederos (*Wallets*): sistemas diseñados para guardar criptomonedas de forma segura. Contienen una clave privada que permite gastar los bitcoins asignados a la dicha clave en la cadena de bloques. Cada monedero muestra la cantidad de criptomonedas que contiene y permite transferir (pagar) una cantidad específica a otro monedero, como un monedero tradicional. Existen muchos tipos de monederos: alojados en la nube, monederos sin conexión, dispositivos hardware específicos, monederos impresos en papel... Una buena relación de monederos disponibles puede encontrarse en https://bitcoin.org/es/elige-tu-monedero.

Nonce: número de valor aleatorio que forma parte de cada bloque y que el minero puede variar libremente. El nodo minero calcula el hash del bloque que está preparando, alterando el valor del nonce hasta que consigue un hash que cumpla con los criterios de dificultad establecidos en ese momento.

Programa de minado: clientes de la red Bitcoin diseñados para el cálculo de nuevos bloques. Son más complejos que los monederos y requieren disponer de una copia de la cadena de bloques completa. El programa cliente desarrollado por la comunidad bitcoin es Bitcoin Core, si bien dos más populares son CGminer y BFGminer, que son programas de línea de comandos. Existen numerosas alternativas, algunas de las cuales pueden consultarse en https://www.bitcoinmining.com/bitcoin-mining-software/

Prueba de trabajo (*proof of work* o *POW*): la prueba de trabajo garantiza que crear un nuevo bloque sea difícil y suponga un gran trabajo computacional. El minero deben resolver un puzzle matemático consistente en construir un bloque cuyo hash comience con cierto número de ceros. Para ello, puede variar libremente el valor del nonce y calcular el hash correspondiente al bloque de forma reiterada hasta obtener un valor válido.

Red peer-to-peer (*p2p*): es una tipología de red de ordenadores en la que sus nodos se comportan como iguales entre sí, de manera que todos ellos actúan simultáneamente como clientes y servidores permitiendo el intercambio directo de información entre los ordenadores interconectados. Habitualmente, este modelo se construye como una red superpuesta sobre otras redes públicas, como Internet.

Red SARA: conjunto de infraestructuras de comunicaciones y servicios básicos que conecta las Administraciones Públicas Españolas e instituciones europeas, facilitando el intercambio de información y el acceso a los servicios.

Token: ver criptomoneda.

Transacción: una sección de datos firmados electrónicamente que se transmite a la red. Este conjunto de datos incluye una referencia a una transacción anterior y contiene una cantidad de criptomonedas que pasan a estar disponibles desde una dirección de origen a una dirección de destino. Las transacciones se almacenan en bloques que forman parte de la cadena.

Turing completo: en teoría informática, se aplica a las máquinas o lenguajes de programación que pueden hacer cualquier cálculo que cualquier otra computadora es capaz de hacer (en otras palabras, es programable).