VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

Universidad de Salamanca

Departamento de Informática y Automática

Facultad de Ciencias

Tesis Doctoral

Arquitecturas blockchain para compartir información y optimizar servicios en tiempo de ejecución

Autor:

D. Yeray Mezquita Martín

Directores:

Dr. D. Juan Manuel Corchado Rodríguez

Dr. D. Javier Prieto Tejedor

Noviembre de 2022

VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

University of Salamanca

Department of Computer Science and Automation

Faculty of Sciences

Doctoral Thesis

Blockchain-based architectures for information-sharing and service-optimization at runtime

Author:

D. Yeray Mezquita Martín

Advisors:

Dr. D. Juan Manuel Corchado Rodríguez

Dr. D. Javier Prieto Tejedor

November, 2022

VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

Universidad de Salamanca

Departamento de Informática y Automática

Facultad de Ciencias

Arquitecturas blockchain para compartir información y optimizar servicios en tiempo de ejecución

Autor:

D. Yeray Mezquita Martín

Directores:

Dr. D. Juan Manuel Corchado Rodríguez

Dr. D. Javier Prieto Tejedor

Tribunal

Presidente: Dra. D.ª Angélica González Arrieta

Vocal: Dra. D.ª Patricia Wolf

Secretario: Dr. D. Antonio F. Skarmeta Gómez

Suplentes: Dr. D. Ricardo S. Alonso Rincón y Dra. D.ª Sara Rodríguez González

Fecha de lectura: 18/11/2022

Calificación:

A mi familia

A mis amigos

Al grupo de investigación BISITE

Al blockchain lab:UM

Solicitud de Presentación de Tesis Doctoral

Estimado Coordinador del Programa de Doctorado en Ingenería Informática:

D. Yeray Mezquita Martín, con DNI 71040797-F, y alumno del programa de DOCTORADO EN INGENIERÍA INFORMÁTICA, matriculado en el plan de estudios D015 INGENIERÍA INFORMÁTICA (R.D. 99/2011) y con número de expediente 59:

Solicita que se tenga en consideración la información aportada en este documento con el objeto de poder presentar la Tesis Doctoral con título *Arquitecturas blockchain para compartir información y optimizar servicios en tiempo de ejecución* mediante el formato de compendio de artículos/publicaciones. La información aportada se corresponde con lo establecido en el Procedimiento para la presentación de la Tesis Doctoral en la Universidad de Salamanca en el Formato de Compendio de Artículos/Publicaciones.

A continuación se detallan los documentos adjuntos en esta solicitud:

- Página Inicial especificando que la Tesis Doctoral corresponde a un compendio de trabajos previamente publicados, detallando para cada uno de ellos: referencia de la revista, editorial, DOI y afiliaciones de cada uno de los miembros autores.
- Autorización de los directores para la presentación de la Tesis Doctoral mediante el formato de compendio de artículos/publicaciones.
- Introducción y resumen de la Tesis Doctoral presentada.
    - Introducción.
    - Metodología de investigación.
    - Objetivos de la Tesis Doctoral.
    - Estado del arte.
    - Contribuciones.
    - Publicaciones.
    - Proyectos.
    - Conclusiones.
    - Trabajo futuro.
- Copia completa de las publicaciones originales que conformarán la Tesis Doctoral (artículos, capítulos de libro, libro o libros aceptados o publicados), incluyendo un resumen de la publicación, una introducción con los antecedentes del tema objeto

de estudio, la hipótesis de trabajo y los objetivos de la investigación, así como los principales resultados y conclusiones finales de cada uno de ellos.

En Salamanca, a 5 de octubre de 2022

El doctorando

MEZQUITA MARTIN YERAY - 71040797F

Firmado digitalmente por MEZQUITA MARTIN YERAY - 71040797F
Fecha: 2022.10.05 19:47:09 +02'00'

D. Yeray Mezquita Martín

Autorización de los Directores

En Salamanca, a 03 de octubre de 2022,

HACEMOS CONSTAR:

Que, como directores de la Tesis Doctoral de **Yeray Mezquita Martín**, con DNI 71040797F, autorizamos a presentar la Tesis Doctoral **"Arquitecturas blockchain para compartir información y optimizar servicios en tiempo de ejecución"** mediante la modalidad de compendio de artículos, al disponer de los siguientes artículos publicados:

1. Mezquita, Y., Casado-Vara, R., González Briones, A., Prieto, J., & Corchado, J. M. (2021). Blockchain-based architecture for the control of logistics activities: Pharmaceutical utilities case study. *Logic Journal of the IGPL*, 29(6), 974-985.
2. Mezquita, Y., Parra-Domínguez, J., Pérez-Pons, M. E., Prieto, J., & Manuel Corchado, J. (2022). Blockchain-Based Land Registry Platforms: A Survey on Their Implementation and Potential Challenges. *Logic Journal of the IGPL*.
3. Mezquita, Y., Gil-González, A. B., Martín del Rey, A., Prieto, J., & Corchado, J. M. (2022). Towards a Blockchain-Based Peer-to-Peer Energy Marketplace. *Energies*, 15(9), 3046.

Los directores:

Firmado digitalmente por CORCHADO RODRIGUEZ JUAN MANUEL - 70978310B
Fecha: 2022.10.03 19:02:07 +02'00'

Dr. Juan Manuel Corchado Rodríguez

PRIETO TEJEDOR JAVIER - 11969812Z
Firmado digitalmente por PRIETO TEJEDOR JAVIER - 11969812Z
Fecha: 2022.10.03 09:54:53 +02'00'

Dr. Javier Prieto Tejedor

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

ESCUELA DE DOCTORADO
EDIFICIO MULTIUSOS I+D+I
C/ ESPEJO Nº 2 – 1ª PLANTA. 37007 SALAMANCA
doctorado.usal.es

IMPRIMIR RESTABLECER

D. /Dª. Juan Manuel Corchado

HAGO CONSTAR:

Que soy COAUTOR/A de los siguientes trabajos:

Mezquita, Y., Casado-Vara, R., González Briones, A., Prieto, J., & Corchado, J. M. (2021). Blockchain-based architecture for the control of logistics activities: Pharmaceutical utilities case study. Logic Journal of the IGPL, 29(6), 974-985.

Mezquita, Y., Parra-Domínguez, J., Pérez-Pons, M. E., Prieto, J., & Manuel Corchado, J. (2022). Blockchain-Based Land Registry Platforms: A Survey on Their Implementation and Potential Challenges. Logic Journal of the IGPL.

Mezquita, Y., Gil-González, A. B., Martín del Rey, A., Prieto, J., & Corchado, J. M. (2022). Towards a Blockchain-Based Peer-to-Peer Energy Marketplace. Energies, 15(9), 3046.

Y MANIFIESTO QUE:

☐ Como COAUTOR/A NO DOCTOR/A del trabajo del doctorando _____ expreso mi RENUNCIA a presentar el artículo como parte de otra Tesis Doctoral.

☑ Como COAUTOR/A del trabajo del doctorando Yeray Mezquita Martín acepto que dicho trabajo sea presentado como parte de su Tesis Doctoral y declaro que el doctorando es el autor principal de la investigación recogida en estos trabajos.

Salamanca a 18 de julio de 2022

CORCHADO RODRIGUEZ JUAN MANUEL - 70978310B

Firmado digitalmente por CORCHADO RODRIGUEZ JUAN MANUEL - 70978310B
Fecha: 2022.07.17 13:13:58 +02'00'

Fdo: Juan Manuel Corchado

COMISIÓN ACADÉMICA DEL PROGRAMA DE DOCTORADO

ESCUELA DE DOCTORADO
EDIFICIO MULTIUSOS I+D+I
C/ ESPEJO Nº 2 – 1ª PLANTA. 37007 SALAMANCA
doctorado.usal.es

IMPRIMIR RESTABLECER

D. /Dª. Javier Prieto

HAGO CONSTAR:

Que soy COAUTOR/A de los siguientes trabajos:

Mezquita, Y., Casado-Vara, R., González Briones, A., Prieto, J., & Corchado, J. M. (2021). Blockchain-based architecture for the control of logistics activities: Pharmaceutical utilities case study. Logic Journal of the IGPL, 29(6), 974-985.

Mezquita, Y., Parra-Domínguez, J., Pérez-Pons, M. E., Prieto, J., & Manuel Corchado, J. (2022). Blockchain-Based Land Registry Platforms: A Survey on Their Implementation and Potential Challenges. Logic Journal of the IGPL.

Mezquita, Y., Gil-González, A. B., Martín del Rey, A., Prieto, J., & Corchado, J. M. (2022). Towards a Blockchain-Based Peer-to-Peer Energy Marketplace. Energies, 15(9), 3046.

Y MANIFIESTO QUE:

☐ Como COAUTOR/A NO DOCTOR/A del trabajo del doctorando _____ expreso mi RENUNCIA a presentar el artículo como parte de otra Tesis Doctoral.

☑ Como COAUTOR/A del trabajo del doctorando Yeray Mezquita Martín acepto que dicho trabajo sea presentado como parte de su Tesis Doctoral y declaro que el doctorando es el autor principal de la investigación recogida en estos trabajos.

Salamanca a 18 de julio de 2022

PRIETO TEJEDOR JAVIER - 11969812Z

Firmado digitalmente por PRIETO TEJEDOR JAVIER - 11969812Z
Fecha: 2022.07.17 08:23:38 +02'00'

Fdo: Javier Prieto

COMISIÓN ACADÉMICA DEL PROGRAMA DE DOCTORADO

ESCUELA DE DOCTORADO
EDIFICIO MULTIUSOS I+D+I
C/ ESPEJO Nº 2 – 1ª PLANTA. 37007 SALAMANCA
doctorado.usal.es

IMPRIMIR RESTABLECER

D. /Dª. Alfonso González Briones

HAGO CONSTAR:

Que soy COAUTOR/A de los siguientes trabajos:

Mezquita, Y., Casado-Vara, R., González Briones, A., Prieto, J., & Corchado, J. M. (2021). Blockchain-based architecture for the control of logistics activities: Pharmaceutical utilities case study. Logic Journal of the IGPL, 29(6), 974-985.

Y MANIFIESTO QUE:

☐ Como COAUTOR/A NO DOCTOR/A del trabajo del doctorando _____ expreso mi RENUNCIA a presentar el artículo como parte de otra Tesis Doctoral.

☑ Como COAUTOR/A del trabajo del doctorando Yeray Mezquita Martín acepto que dicho trabajo sea presentado como parte de su Tesis Doctoral y declaro que el doctorando es el autor principal de la investigación recogida en estos trabajos.

Salamanca a 16 de julio de 2022

GONZALEZ BRIONES ALFONSO - 52415611Z

Firmado digitalmente por GONZALEZ BRIONES ALFONSO - 52415611Z
Fecha: 2022.07.16 23:16:15 +02'00'

Fdo: Alfonso González Briones

COMISIÓN ACADÉMICA DEL PROGRAMA DE DOCTORADO

ESCUELA DE DOCTORADO
EDIFICIO MULTIUSOS I+D+I
C/ ESPEJO Nº 2 – 1ª PLANTA. 37007 SALAMANCA
doctorado.usal.es

IMPRIMIR RESTABLECER

D. /Dª. Roberto Casado Vara

HAGO CONSTAR:

Que soy COAUTOR/A de los siguientes trabajos:

Mezquita, Y., Casado-Vara, R., González Briones, A., Prieto, J., & Corchado, J. M. (2021). Blockchain-based architecture for the control of logistics activities: Pharmaceutical utilities case study. Logic Journal of the IGPL, 29(6), 974-985.

Y MANIFIESTO QUE:

☐ Como COAUTOR/A NO DOCTOR/A del trabajo del doctorando _____ expreso mi RENUNCIA a presentar el artículo como parte de otra Tesis Doctoral.

☑ Como COAUTOR/A del trabajo del doctorando Yeray Mezquita Martín acepto que dicho trabajo sea presentado como parte de su Tesis Doctoral y declaro que el doctorando es el autor principal de la investigación recogida en estos trabajos.

Salamanca a 16 de julio de 2022

CASADO VARA ROBERTO CARLOS - 45686237A

Firmado digitalmente por CASADO VARA ROBERTO CARLOS - 45686237A
Fecha: 2022.07.16 21:51:46 +02'00'

Fdo: Roberto Casado Vara

COMISIÓN ACADÉMICA DEL PROGRAMA DE DOCTORADO

ESCUELA DE DOCTORADO
EDIFICIO MULTIUSOS I+D+I
C/ ESPEJO Nº 2 – 1ª PLANTA. 37007 SALAMANCA
doctorado.usal.es

IMPRIMIR RESTABLECER

D. /Dª. Javier Parra

HAGO CONSTAR:

Que soy COAUTOR/A de los siguientes trabajos:

Mezquita, Y., Parra-Domínguez, J., Pérez-Pons, M. E., Prieto, J., & Manuel Corchado, J. (2022). Blockchain-Based Land Registry Platforms: A Survey on Their Implementation and Potential Challenges. Logic Journal of the IGPL.

Y MANIFIESTO QUE:

☐ Como COAUTOR/A NO DOCTOR/A del trabajo del doctorando _____ expreso mi RENUNCIA a presentar el artículo como parte de otra Tesis Doctoral.

☑ Como COAUTOR/A del trabajo del doctorando Yeray Mezquita Martín acepto que dicho trabajo sea presentado como parte de su Tesis Doctoral y declaro que el doctorando es el autor principal de la investigación recogida en estos trabajos.

Salamanca a 16 de julio de 2022

PARRA DOMINGUEZ JAVIER - 70935333K

Firmado digitalmente por PARRA DOMINGUEZ JAVIER - 70935333K
Fecha: 2022.07.16 23:31:04 +02'00'

Fdo: Javier Parra

COMISIÓN ACADÉMICA DEL PROGRAMA DE DOCTORADO

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

ESCUELA DE DOCTORADO
EDIFICIO MULTIUSOS I+D+I
C/ ESPEJO Nº 2 – 1ª PLANTA. 37007 SALAMANCA
doctorado.usal.es

IMPRIMIR RESTABLECER

D. /Dª. Maria Eugenia Pérez Pons

HAGO CONSTAR:

Que soy COAUTOR/A de los siguientes trabajos:

Mezquita, Y., Parra-Domínguez, J., Pérez-Pons, M. E., Prieto, J., & Manuel Corchado, J. (2022). Blockchain-Based Land Registry Platforms: A Survey on Their Implementation and Potential Challenges. Logic Journal of the IGPL.

Y MANIFIESTO QUE:

☐ Como COAUTOR/A NO DOCTOR/A del trabajo del doctorando _____ expreso mi RENUNCIA a presentar el artículo como parte de otra Tesis Doctoral.

☑ Como COAUTOR/A del trabajo del doctorando Yeray Mezquita Martín acepto que dicho trabajo sea presentado como parte de su Tesis Doctoral y declaro que el doctorando es el autor principal de la investigación recogida en estos trabajos.

Salamanca a 19 de julio de 2022

Fdo: Maria Eugenia Pérez Pons

COMISIÓN ACADÉMICA DEL PROGRAMA DE DOCTORADO

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

ESCUELA DE DOCTORADO
EDIFICIO MULTIUSOS I+D+I
C/ ESPEJO Nº 2 – 1ª PLANTA. 37007 SALAMANCA
doctorado.usal.es

IMPRIMIR RESTABLECER

D. /Dª. Ana Belén Gil González

HAGO CONSTAR:

Que soy COAUTOR/A de los siguientes trabajos:

Mezquita, Y., Gil-González, A. B., Martín del Rey, A., Prieto, J., & Corchado, J. M. (2022). Towards a Blockchain-Based Peer-to-Peer Energy Marketplace. Energies, 15(9), 3046.

Y MANIFIESTO QUE:

☐ Como COAUTOR/A NO DOCTOR/A del trabajo del doctorando _____ expreso mi RENUNCIA a presentar el artículo como parte de otra Tesis Doctoral.

☑ Como COAUTOR/A del trabajo del doctorando Yeray Mezquita Martín acepto que dicho trabajo sea presentado como parte de su Tesis Doctoral y declaro que el doctorando es el autor principal de la investigación recogida en estos trabajos.

Salamanca a 18 de julio de 2022

GIL GONZALEZ ANA BELEN - 07973126S

Firmado digitalmente por GIL GONZALEZ ANA BELEN - 07973126S
Fecha: 2022.07.18 09:45:59 +02'00'

Fdo: Ana Belén Gil González

COMISIÓN ACADÉMICA DEL PROGRAMA DE DOCTORADO

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

ESCUELA DE DOCTORADO
EDIFICIO MULTIUSOS I+D+I
C/ ESPEJO Nº 2 – 1ª PLANTA. 37007 SALAMANCA
doctorado.usal.es

IMPRIMIR RESTABLECER

D. /Dª. Angel Martín del Rey

HAGO CONSTAR:

Que soy COAUTOR/A de los siguientes trabajos:

Mezquita, Y., Gil-González, A. B., Martín del Rey, A., Prieto, J., & Corchado, J. M. (2022). Towards a Blockchain-Based Peer-to-Peer Energy Marketplace. Energies, 15(9), 3046.

Y MANIFIESTO QUE:

☐ Como COAUTOR/A NO DOCTOR/A del trabajo del doctorando _____ expreso mi RENUNCIA a presentar el artículo como parte de otra Tesis Doctoral.

☑ Como COAUTOR/A del trabajo del doctorando Yeray Mezquita Martín acepto que dicho trabajo sea presentado como parte de su Tesis Doctoral y declaro que el doctorando es el autor principal de la investigación recogida en estos trabajos.

Salamanca a 17 de julio de 2022

MARTIN DEL REY ANGEL MARIA - 07953200F

Firmado digitalmente por MARTIN DEL REY ANGEL MARIA - 07953200F
Fecha: 2022.07.17 09:52:05 +02'00'

Fdo: Angel Martín del Rey

COMISIÓN ACADÉMICA DEL PROGRAMA DE DOCTORADO

"La victoria más difícil es la victoria sobre uno mismo."

Aristóteles

Resumen

La tecnología blockchain, en base a sus características de transparencia, inmutabilidad, y democracia de los datos, se presenta como el potencial disruptor de la industria actual. El paradigma que presenta la industria hoy, basado en el Internet de las Cosas, genera una gran cantidad de comunicaciones entre los dispositivos, donde pueden existir problemas a la hora de verificar el origen y autoría de los datos generados. Por esta razón, la blockchain se presenta como una tecnología que puede solucionar los problemas mencionados. Sin embargo, la tecnología blockchain no está extenta de sus propios problemas: consumo de energía excesivo para preservar la seguridad en la red, imposibilidad por sí sola para detectar corrupción en el origen de los datos, o las violaciones a la intimidad y privacidad de los usuarios por la transparencia de la información almacenada.

En la literatura se han propuesto soluciones a la hora de enfrentar los desafíos que presenta esta tecnología como, por ejemplo, (i) sustituir el uso de redes públicas por redes permisionadas, optimizando el consumo energético de la red al no ser necesario un algoritmo tan estricto para garantizar su seguridad, (ii) almacenar datos sensibles *off-chain*, utilizando la blockchain como metodo de verificación de la información, resumiéndola con el hash, o (iii) reducir la funcionalidad de las soluciones propuestas, eliminando servicios que potencialmente podrían ofrecer.

En primer lugar, esta investigación realiza un estudio y análisis sobre las soluciones propuestas en la literatura, encontrando que, (i) no hacen frente a todos los desafíos que propone esta tecnología, o (ii) la centralización de su propuesta no justifica la implementación de la red blockchain. Todo esto hace imposible la implementación de estas arquitecturas en un escenario real, donde los marcos regulatorios cada vez son más estrictos.

En base a las carencias encontradas en el Estado del Arte, esta Tesis Doctoral propone dos arquitecturas en diferentes ámbitos: la industria logística farmacéutica y el intercambio de electricidad en mercados automáticos. En el primer caso, se hace uso de modelos de teorías de juegos, para asegurar el buen comportamiento de los actores en la plataforma, además de sistemas de auditabilidad para tener controlado los posibles fallos técnicos que puedan ocurrir en los dispositivos. En el segundo caso, se hace uso de pruebas de conocimiento nulo y firmas en anillo para asegurar la privacidad y seguridad

de los datos y los usuarios. Estas dos arquitecturas hacen frente a los desafíos que propone la tecnología blockchain, y permiten su implementación dentro de cualquier ámbito regulatorio.

Abstract

Blockchain technology, based on its characteristics of transparency, immutability, and data democracy, is presented as the potential disruptor of the current industry. The paradigm presented by the industry today, based on the Internet of Things, generates a large amount of communications between devices, where there may be problems when verifying the origin and authorship of the data generated. For this reason, blockchain is presented as a technology that can solve the aforementioned problems. However, blockchain technology is not exempt from its own problems: excessive energy consumption to preserve network security, impossibility by itself to detect corruption in the origin of the data, or violations to the privacy and intimacy of the users due to the transparency of the stored information.

In the literature, solutions have been proposed to face the challenges presented by this technology: for example, replacing the use of public networks with permissioned networks, optimizing the energy consumption of the network by not requiring such a strict algorithm to guarantee its security, or storing sensitive data *off-chain*, using the blockchain as a method of verifying the information, by hashing it, or simply simplifying and centralizing the functionality of the proposed solutions.

In this research, a study and analysis of the proposed solutions in the literature is carried out, finding that either they do not meet all the challenges proposed by this technology, or the centralization of its proposal does not justify the implementation of the blockchain network. All this makes it impossible to implement these architectures in a real scenario, where regulatory frameworks are increasingly strict.

On the other hand, this Doctoral Thesis proposes two architectures in different fields, the pharmaceutical logistics industry and the exchange of electricity in automatic markets. In the first case, game theory models are used to ensure the good behavior of the actors in the platform, as well as auditability systems to control possible technical failures that may occur in the devices. In the second, use is made of null knowledge tests and ring signatures to ensure the privacy and security of data and users. The analysis shown by these two architectures concludes that both meet the challenges proposed in the field of blockchain technology, the latter being the most complete that can be implemented within any regulatory environment.

Agradecimientos

A mis directores, Juan Manuel y Javier, porque gracias a ellos he tenido oportunidades increíbles en el mundo de la investigación. Por haber contado conmigo para formar parte de su equipo en el grupo de investigación BISITE, y por dirigirme y ayudarme a sacar adelante esta Tesis Doctoral.

A mis compañeros de investigación y colaboradores en las publicaciones durante la misma, especialmente a Ana, Alfonso, Carlitos, Roberto, Parra, Marta, Richi y Eugenia. Esta Tesis Doctoral refleja también vuestro trabajo.

A todos mis compañeros del grupo BISITE a lo largo de este tiempo. Es un placer trabajar con todos vosotros y formar parte de este equipo, tanto a nivel personal como profesional. Gracias por hacer posible esta investigación.

Al Blockchain Lab:UM, por acogerme durante mi estancia en Maribor (Eslovenia) y enseñarme tanto sobre el mundo de la investigación y ayudarme profundizar más en el desarrollo de mi tesis.

Y a mi familia, por hacerme sentir que siempre están ahí, porque gracias a ellos siempre tendré un lugar al que regresar. Gracias a mis sobrinos, que siempre consiguen poner una sonrisa en mi cara, por hacer mucho más ameno cualquier obstáculo en mi camino.

Índice general

Índice de figuras

Índice de tablas

Siglas y acrónimos

AR	**A**ction-**R**esearch
BT	**B**lockchain **T**echnology
BTC	**B**itcoin
DAO	**D**ecentralized **A**utonomous **O**rganization
DApp	**D**ecentralized **A**pplication
DDOS	**D**ecentralized **D**enial **O**f **S**ervices
DEFI	**De**centralized **Fi**nances
DLT	**D**istributed **L**edger **Technology**
DPoS	**D**elegated **P**roof **o**f **S**take
Eth	**E**ther
EVM	**E**thereum **V**irtual **M**achine
GDPR	**G**eneral **D**ata **P**rotection **R**egulation
GUID	**G**lobal **U**nique **Id**entifier
IoT	**I**nternet **o**f **T**hings
MAS	**M**ulti-**A**gent **S**ystem
P2P	**P**eer-**to**-**P**eer
PBFT	**P**ractical **B**izantine **F**ault **T**olerance
PoC	**P**roof **o**f **C**ooperation
PoS	**P**roof **o**f **S**take
PoW	**P**roof **o**f **W**ork
TPS	**T**ransactions **P**er **S**econd
Tx	**T**ransaction
UTXO	**U**nspent **T**ransaction **O**utput

Capítulo 1

Introducción

VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

Capítulo 1

Introducción

Debido a la naturaleza abierta, descentralizada y criptográfica de la tecnología blockchain, es posible (i) evitar intermediarios en las transacciones entre partes no confiables; y (ii) generar un libro de contabilidad inmutable mantenido por la red de nodos, los cuales, mediante el uso de un algoritmo de consenso, consiguen que la cadena de bloques sea a prueba de manipulaciones (Mezquita, Parra, Perez, Prieto, & Corchado, 2019). Es esta naturaleza la que hace pensar a la comunidad científica en el potencial que esta tecnología tiene para la disrupción de la industria tradicional, más enfocada en la centralización de los recursos y servicios ofrecidos por una empresa, siendo esta la responsable de las acciones tomadas en su plataforma. Por otra parte, la inclusión de la tecnología blockchain, podría transicionar este modelo centralizado a uno descentralizado, en el que la responsabilidad se distribuya de forma democrática entre los usuarios de una plataforma, reduciendo el coste de los servicios, y siendo dueños además de los datos generados en la misma, lo que se denomina como democratización de los datos.

Hasta el momento de la realización de esta Tesis Doctoral, la comunidad científica ha propuesto diferentes modelos como forma de solucionar la implantación de esta tecnología en la industria (Mezquita, Casado, et al., 2019; Mezquita, Gil-González, Martín del Rey, Prieto, & Corchado, 2022; Mezquita, Parra-Domínguez, Pérez-Pons, Prieto, & Manuel Corchado, 2022). Sin embargo, muchas carecen en algún punto de lo necesario para ser bien desplegadas en un entorno de producción (Mezquita, Parra-Domínguez, et al., 2022). Por otro lado, las que han sido desplegadas en un entorno de producción, ofertan servicios que aún tienen un gran componente de centralización, muy lejos de la consecución de una democracia plena de datos (Mezquita, Gil-González, et al., 2022). Es por estas razones que la presente Tesis Doctoral investiga un modelo en el

que sea posible la optmización de los servicios, además de proporcionar una democracia de datos en la que los usuarios sean los dueños de su propia información.

El presente Capítulo introductorio está estructurado de la siguiente forma. La Sección 1.1 realiza una introducción a los antecedentes del tema objeto de estudio y describe el problema a tratar. La Sección 1.2 expone la hipótesis de trabajo, así como los objetivos específicos de los distintos trabajos de investigación realizados durante la Tesis Doctoral para alcanzar la respuesta a esta hipótesis. La Sección 1.3 detalla la metodología seguida durante dichos trabajos de investigación. Finalmente, la Sección 1.4 describe la estructura de la memoria de esta Tesis Doctoral.

1.1. Descripción del problema

Existe una tendencia al desarrollo de sistemas distribuidos haciendo uso del paradigma multiagente (Francisco, Mezquita, Revollar, Vega, & De Paz, 2019), ya que estos otorgan una serie de beneficios, como pueden ser: (i) optimización de los tiempos de ejecución, la carga del sistema se encuentra distribuida permitiendo tareas en paralelo; y (ii) mejora en la seguridad del sistema, ya que la distribución de las tareas hace que un atacante necesite atacar diversos actores en la plataforma con el fin de detener el servicio. Este tipo de sistemas se han aplicado a muchos ámbitos, desde la industria agroalimentaria (González-Briones, Castellanos-Garzón, Mezquita Martín, Prieto, & Corchado, 2018), al control de procesos en la industria química (Francisco et al., 2019). A pesar de las ventajas que proporcionan este tipo de sistemas, también acarrean inconvenientes acomo vulnerabilidades a ataques cómo *man-in-the-middle*, robando información o transmitiendo datos erróneos que impiden el buen funcionamiento de la plataforma, y/o *DDOS*, incapacitando partes de la plataforma, se consigue paralizar el servicio.

En este contexto, empiezan a surgir tecnologías basadas en libros de cuentas distribuidos, las conocidas como DLTs por sus siglas en inglés *Distributed Ledger Technologies*. Este tipo de tecnologías aseguran que los canales de comunicación normalmente utilizados por los agentes en servicios de publicación-subscripción (*pub-sub*). Estas tecnologías se utilizan como el tablón de anuncios necesarios para las comunicaciones entre los agentes. Al utilizar un canal distribuido, conformado por una red de computadores, las comunicaciones de la plataforma se aseguran frente a ataques de denegación de servicios,

los cuales deben atacar la red entera para terminar con el canal de comunicaciones del sistema multiagente, el cual tradicionalmente es llevado a cabo por una única entidad, siendo ese el *punto de fallo único* en las plataformas multiagente tradicionales.

La tecnología blockchain es un tipo de DLT, la cual, no sólo provee un canal de comunicaciones más seguro frente a ataques de denegación de servicios, sino que también ayuda al sistema a asegurar el origen de los datos y las comunicaciones entre las partes del sistema, lo que ayuda, no sólo proporcionando resiliencia frente a ataques DDOS, sino también a impedir ataques del tipo *man-in-the-middle* Mezquita, Casado, et al. (2019). Por otra parte, la tecnología blockchain también ofrece la posibilidad de desplegar y utilizar contratos inteligentes. Este tipo de programas son autoejecutables y no necesitan de intermediarios que no generen valor en la plataforma, por lo que, mediante su uso, una plataforma optimiza sus tiempos de ejecución de tareas, además de disminuir los costes de los servicios al disminuir la aparición de intermediarios (Mezquita, Valdeolmillos, González-Briones, Prieto, & Corchado, 2019). Finalmente, todas las bondades que otorga la tecnología blockchain a los sistemas tradicionales, culminan con la aparición de modelos democráticos, en los que son los mismos usuarios los responsables de su actividad en la plataforma, obteniendo también el control y propiedad sobre los datos que ellos mismos generan en ella (Mezquita, Gazafroudi, et al., 2019).

A pesar de las potenciales bondades que tiene la aplicación de esta tecnología a la industria actual, existen numerosos retos que presenta para poder ser utilizada efectivamente (Mezquita, Casado, et al., 2019; Mezquita, Valdeolmillos, et al., 2019):

- Escalabilidad. Para la tecnología blockchain, cuya base es el acuerdo llegado por una red de nodos para la administración de la información, la escalabilidad es un reto al que hacer frente. A mayor tamño de red, mayor es la cantidad de entidades que deben alcanzar un acuerdo, traduciéndose en un mayor número de mensajes enviados a través de la red. Con el fin de acelerar el proceso se pueden utilizar protocolos de consenso (i) que no requieran una gran cantidad de mensajes, y (ii) que sean rápidos a la hora de añadir información a la blockchain. Por otro lado, no todos los protocolos son válidos para todos los tipos de redes, por lo que es necesario elegir con cuidado, qué tipo de red va a ser usada por la plataforma diseñada.

- Formación de la red. El tamaño de la red puede ser un problema, no sólo por la escalabilidad, si no por la seguridad proporcionada. Una red más pequeña es más fácil de atacar y ganar control sobre ella. Una red en la que se pueden crear identidades muy fácilmente también es susceptible a ser atacada. Los tipos de ataques específicos a esta tecnología son los denominados *sybil*, ataques de eclipse, o ataques del 51 %. Para evitar estos ataques se debe fomentar la dificultad para crear una entidad en la red, por ejemplo, las redes blockchain públicas ponen de requisito un gran consumo de recursos o un coste de inversión inicial, lo que impide el *spam* de entidades dentro de estas redes. Por otro lado, las redes permisionadas, asignan roles a entidades conocidas por la red, por lo que se aseguran que estos atacantes no formen parte de ellas.

- Malas prácticas por parte de los usuarios. Los robos de criptomonedas acaecidos, usualmente no tienen nada que ver con la tecnología utilizada, si no con que los usuarios no utilizan contraseñas o medios seguros en los que almacenar sus claves para el manejo de las *wallets*. Otro punto crítico son los *exchanges*, plataformas utilizadas por la gran mayoría de los usuarios de criptoactivos, dónde tienen almacenados información crítica para la gestión de sus *wallets*, siendo susceptibles a ataques dirigidos con el fin de robar la información de estos usuarios. En este aspecto es necesario educar a los usuarios sobre la importancia de utilizar medios seguros para generar y almacenar las claves de sus monederos. Además de no confiar en cualquier plataforma para que gestionen esas claves.

- Malas prácticas por parte de los programadores. Los contratos inteligentes dependen en gran medida de los desarrolladores que los implementen. Si estos no han seguido unas buenas prácticas para asegurar la integridad del contrato, es posible que ocurran fallas y los atacantes los exploten, como ocurrió con el caso del DAO (Buterin, 2016; Daian, 2016). La única forma de solventar este reto es someter los contratos inteligentes a auditorias antes de su despliegue definitivo, además de ofrecer una forma de actualizar dichos contratos tras su despliegue.

- Inmutabilidad de la información almacenada. Debido a la naturaleza de esta tecnología, la información almacenada es inmutable, algo visto como ventaja en algunos campos, pero no siempre es así. Si la información almacenada viene viciada de inicio, la blockchain sólo mantendrá el vicio. Por otro lado, si hay información

sensible almacenada propiedad de un usuario, y este desea eliminarla conforme con la ley, no va a poder hacerlo por esta misma naturaleza. Si se quiere hacer frente a este reto sólo es posible por medio de auditorias periodicas de los dispositivos y actores que añaden información a la blockchain. De esta forma es posible detectar aquellos defectuosos que están añadiendo información viciada sin saberlo. Por otro lado, hacen falta mecanismos de teoría de juegos, en los que se castiguen los comportamientos no deseados en la plataforma, para evitar que de forma intencionada se añada información a la cadena de bloques.

- Transparencia. Que esta tecnología permita la creación de plataformas transparentes puede ser un arma de doble filo, pues en la mayoría de casos la actividad de los usuarios en la plataforma es expuesta lo que conlleva una vulnerabilidad a los derechos sobre la privacidad de los usuarios. Por otro lado, si se generan datos sensibles, estos también serían accesibles por terceros, violando de nuevo los derechos de los mismos. Para hacer frente a este reto sólo se puede hacer uso de técnicas criptográficas que oculten la información almacenada y sólo el usuario conozca la forma de mostrar estos datos. Por otro lado, se pueden utilizar mecanismos de almacenamiento *offchain*, en los que la información crítica es almacenada en un sistema ajeno a la cadena de bloques, mientras que en ella se almacena únicamente el resumen o *hash* de dicha información. Es una solución más centralizada y que no asegura que no se modifique la información almacenada fuera de la cadena de bloques, pero sí que asegura la detección de esta posible modificación. Por otro lado, la anonimicidad sólo se puede conseguir con mecanismos de enmascaramiento de los transactores.

Tras el análisis de todos los retos, y sus posibles soluciones que se presentan en relación a esta tecnología, se puede concluir que una plataforma que desee pasar de la etapa de prueba piloto y llegar al proceso de despliegue, necesita tener en cuenta muchas variables. Algunas de estas variables no tienen que ver con la tecnología blockchain utilizada, pero deben tener en cuenta qué usuarios están en su objetivo, para guiarlos y evitar los posibles problemas acaecidos por malas practicas de su parte. Por otro lado, no es una tarea fácil, primero el identificar todos y cada uno de estos retos, y segundo diseñar una plataforma que les haga frente. Como se expondrá más adelante, en el Capítulo 3, los diseños de la literatura no cubren cada uno de los aspectos estudiados, por lo que se hace

necesario el diseño de un modelo que guíe y ayude a los desarrolladores a implementar este tipo de plataformas, convirtiéndose en el objetivo principal de esta Tesis Doctoral.

1.2. Hipótesis y objetivos

En esta Tesis Doctoral se busca la incentivación a la proliferación de las tecnologías blockchain en la optimización de los servicios en diferentes ámbitos de la industria actual. Primero, se busca entender cuál es el potencial real de las tecnologías blcockhain para disruptir la industria tradicional. Tras ello, se estudian los retos a los que hace frente esta tecnología de forma pormenorizada, tanto técnicos, ya que al ser una tecnología relativamente nueva aún tiene potencial para mejorar, como los relacionados con los marcos regulatorios, ya que este es un gran escollo para este tipo de tecnologías distribuidas, que buscan la automatización de los procesos (Mezquita, Casado, et al., 2019). Por último, se detalla qué se ha hecho en la literatura en diferentes ámbitos: (i) las cadenas de suministro (Mezquita, Casado-Vara, González Briones, Prieto, & Corchado, 2021; Mezquita, González-Briones, et al., 2019), (ii) los registros de la propiedad (Mezquita, Parra, et al., 2019; Mezquita, Parra-Domínguez, et al., 2022), y (iii) los mercados automáticos (Mezquita, Gazafroudi, et al., 2019; Mezquita, Gil-González, et al., 2022). Gracias a ello, se ha podido presentar una evolución a lo largo de la Tesis Doctoral, de diferentes modelos mejorando los trabajos de la literatura previos, mostrando un modelo al que cualquier investigador y desarrollador pueda acudir para sentar las bases de una plataforma basada en tecnología blockchain.

La **Hipótesis** planteada para la realización de esta Tesis Doctoral es que la tecnología blockchain es capaz de optimizar servicios tradicionales de la industria actual, además de facilitar la aparición de nuevos modelos de servicios descentralizados, no posibles con otra tecnología.

En base a esta hipótesis, esta Tesis Doctoral plantea alcanzar el siguiente **objetivo principal**:

investigar y diseñar modelos de arquitecturas basadas en tecnología blockchain, los cuales ayuden a investigadores, diseñadores, y desarrolladores a implementar este tipo de plataformas en el mundo real, pudiendo pasar de la etapa de prueba de concepto o proyecto piloto. Estos modelos harán frente a cada uno de los retos que

la tecnología blockchain plantea, teniendo en cuenta aspectos que otros modelos de la literatura no han tenido y cumpliendo con uno de los marcos legales más restrictivos en el manejo de datos y automatización de servicios, cómo es el de la Unión Europea.

Para alcanzar el objetivo principal, es necesario definir un listado de **objetivos específicos**, que se describen a continuación:

(**OB1**) Desmitificar la tecnología blcokchain, detallando cuáles son las cualidades que su uso puede aportar a los procesos de la industria actual, dominada por el Internet de las Cosas.

(**OB2**) Identificar los requerimientos existentes para que la tecnología blockchain se pueda implementar en ámbitos dónde existe una gran cantidad de comunicaciones entre dispositivos.

(**OB3**) Realizar un estudio del estado del arte en los ámbitos dónde la tecnología blockchain tiene un mayor potencial de disruptir.

(**OB4**) Analizar los retos, motivaciones y problemas abiertos a la hora de aplicar las soluciones propuestas por la literatura.

(**OB5**) Diseñar arquitecturas que completen y mejoren los modelos propuestos previos.

(**OB6**) Validar los modelos propuestos analizando pormenorizadamente, cómo hacen frente a cada uno de los retos identificados.

(**OB7**) Diseñar un plan de trabajo futuro de cara al diseño e implantación de nuevos protocolos que ayuden en la aplicación de estas plataformas en un escenario futurista donde los ordenadores cuánticos sean una realidad, invalidando las técnicas actuales de encriptación e identificación.

1.3. Metodología de investigación

La metodología *investigación-acción* (AR por sus siglas en inglés: *Action-Research*), es una metodología orientada hacia el cambio que ofrece la posibilidad de realizar, de forma simultánea, tanto investigaciones como acciones, por lo que ha ido ganando

cada vez más popularidad e importancia en los proyectos de Ingeniería del Software. El término fue acuñado por Kurt Lewin en 1952 Herreras (2004) surgiendo como respuesta a una necesidad de investigar, ya no limitada sólo al proceso de producción, sino durante un proceso cíclico e iterativo de exploración, actuación, y validación de los resultados obtenidos. Coloquialmente, esta metodología se puede definir como un proceso metodológico para realizar actividades de mejora y mantener aquello sobre lo que se ha mejorado.

El proceso de *investigación* se relaciona con la comprensión pormenorizada del tema a tratar por parte del investigador, cliente, o ambos. Por otro lado, el proceso de *acción* se asocia, generalmente, con la transformación realizada en una determinada comunidad, organización, o proyecto. Según Baskerville (1999), la metodología AR es considerada necesaria para conseguir un escenario de mayor realismo, ya que involucra un contexto real para investigar los resultados de acciones concretas.

De acuerdo con Baskerville (1999), citado por Tüzün, Tekinerdogan, Macit, & İnce (2019), los estudios desarrollados bajo esta metodología comparten cuatro características comunes:

1. una orientación a la acción y al cambio;
2. un enfoque del problema;
3. un proceso orgánico que implica etapas sistemáticas y, a veces, iterativas;
4. así como la colaboración entre los participantes.

En general, la AR consta de cinco fases (Eden & Ackermann, 2018; Tüzün et al., 2019), descritas a continuación junto a lo desarrollado en esta Tesis Doctaral en cada una de ellas:

1. **Diagnóstico:** Esta fase se corresponde con la identificación y planteamiento del problema expuesto en esta Tesis Doctoral. Es necesario delimitar el alcance, proponer una hipótesis y definir los objetivos que se pretenden alcanzar. Para el caso concreto de esta Tesis Doctoral, se procede a identificar y analizar los potenciales beneficios de la tecnología blockchain en la industria, así cómo los retos y problemas que plantea su implementación en un escenario real.

2. **Revisión de la literatura:** En este caso se procede a realizar un estudio sistemático de la literatura. Una revisión sistemática es una síntesis académica de las pruebas sobre un tema claramente presentado que utiliza métodos críticos para identificar, definir y evaluar la investigación sobre el tema (Barn, Barat, & Clark, 2017; Petersen, Feldt, Mujtaba, & Mattsson, 2008). Para lograr los objetivos presentados en esta Tesis Doctoral, hemos propuesto las siguientes preguntas a responder durante la misma:

   (**RQ1**) ¿Qué proporciona la tecnología blockchain a los procesos de la industria actual?

   (**RQ2**) ¿Cuáles son los problemas que plantea su uso?

   (**RQ3**) ¿Qué hay propuesto en la literatura hasta la fecha?

   (**RQ4**) ¿Cómo se puede mejorar?

   Para cada una de las preguntas de investigación planteadas de cara a responder la hipótesis desarrollada en la sección 1.2, se han realizado diferentes trabajos de investigación a lo largo de esta Tesis Doctoral, los cuales se irán mostrando durante el desarrollo de esta memoria.

3. **Solución:** A partir de los resultado obtenidos en las dos fases anteriores, se propone una solución que responda a los objetivos establecidos. En esta Tesis Doctoral se plantean varias arquitecturas que proponen optimizar y mejorar (a nivel de costes, tiempos, y funcionalidades) procesos sobre diferentes ámbitos de la industria, logística y mercados automáticos en este caso.

4. **Evaluación:** Aunque las arquitecturas propuestas no han sido implementadas en un entorno real, sí que se han analizado y evaluado en base a otras arquitecturas, que están siendo utilizadas en casos de uso reales, sobre las que comparten ciertas características. Por ejemplo, respecto a los mercados automáticos de energía, se han mostrado arquitecturas que, si bien no permiten negociaciones automáticas, sí que permiten la trazabilidad de la energía transaccionada, compartiendo una base que permite analizar el posible desempeño de la nueva arquitectura.

5. **Resultados:** Comprende la última fase del ciclo AR. Por medio de las actividades de esta etapa, la comunidad científica valora los resultados obtenidos en base a un conjunto de publicaciones que se someten a evaluación en revistas de alto

impacto, incluyendo *Expert Systems with Applications*, *IGPL*, o *Energies*; además de en congresos y conferencias internacionales, como la *International Conference on Knowledge Management in Organizations* o la *International Conference on Practical Applications of Agents and Multi-Agent Systems*, entre otras.

1.4. Estructura de la Tesis Doctoral

Para validar la hipótesis establecida en esta Tesis Doctoral, definida en el apartado 1.2, se parte de un estudio pormenorizado de la tecnología blockchain, entendiendo qué puede ofrecer al paradigma industrial actual, y cuales son los retos que debe superar para poder hacer un uso efectivo de ella (OB1 y OB2). Tras ello, se procede a estudiar el estado del arte en materia de plataformas y diseños donde esta tecnología es más útil (OB3). Posteriormente se realizará un análisis para validar las arquitecturas y modelos de la literatura sobre los retos identificados (OB4).

Una vez se han detallado y comprendido las ventajas y desventajas de las plataformas propuestas por la literatura, se procede a diseñar modelos propios que mejoren en algún aspecto (por ejemplo más funcionalidades, o mayor privacidad para los usuarios) las arquitecturas previamente existentes (OB5). Finalmente, se analizan las contribuciones realizadas para demostrar que enfrentan, de forma efectiva, los retos planteados a esta tecnología (OB6).

La estructura de esta Tesis Doctoral por compendio de artículos/publicaciones incluye la presentación de las evidencias y resultados originados en el trabajo de investigación llevado a cabo durante la elaboración de esta Tesis Doctoral, así como las publicaciones acreditativas de la investigación realizada. Finalmente, se exponen las conclusiones y las líneas de trabajo futuras (OB7). De este modo, y tal como se ha adelantado, con el fin de facilitar el seguimiento de la investigación, se estructura la memoria de la presente Tesis Doctoral a través de seis Capítulos.

El Capítulo 1 actual describe el problema planteado a resolver, se formula la hipótesis de trabajo, se detallan los diferentes objetivos y se describe la metodología de investigación seguida para la culminación de esta Tesis Doctoral.

El Capítulo 2 presenta una revisión del estado del arte en el que se desmitifican las bondades de la tecnología blockchain, haciendo un enfoque más realista sobre qué puede y qué no puede hacer. Además, se detallan los retos que se han identificado a lo largo de esta Tesis Doctoral y las posibles soluciones aportadas por la literatura en diferentes ámbitos.

El Capítulo 3 describe las contribuciones resultantes de la investigación llevada a cabo y que se compendia en esta Tesis Doctoral. En este capítulo se detallan las arquitecturas presentadas durante esta Tesis Doctoral, mejorando algún aspecto de las estudiadas durante la revisión de la literatura. Además de analizar cómo hacen frente a los retos planteados para su satisfactoria implementación en escenarios reales.

El Capítulo 4 presenta los resultados alcanzados mediante el desarrollo de la investigación que culmina en esta Tesis Doctoral y que se validan a través de un conjunto de publicaciones en revistas científicas, capítulos de libro, conferencias, congresos y workshops internacionales en los cuales se ha contribuido, así como los proyectos de investigación en los que se ha participado. Asimismo, se detallan las estancias llevadas a cabo en organismos de investigación internacionales.

El Capítulo 5 incluye las publicaciones originales que forman parte de esta Tesis Doctoral por compendio de artículos/publicaciones, acompañadas, cada una de ellas, por su correspondiente introducción, conjunto de objetivos, descripción de la metodología de investigación utilizada en cada una, así como las conclusiones de los resultados obtenidos en cada una de dichas publicaciones.

Finalmente, el Capítulo 6 detalla las principales conclusiones que se han obtenido a partir del trabajo de investigación desarrollado en esta Tesis Doctoral y las aportaciones más relevantes realizadas. Además, se definen las líneas para el desarrollo de trabajo futuro que se abren a partir de los resultados de la presente Tesis Doctoral. Para concluir, se incluye el listado de todas las fuentes bibliográficas que se han citado en esta memoria con el propósito de respaldar las afirmaciones y conceptos que se presentan.

Chapter 1

Introduction

VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

Chapter 1

Introduction

Due to the open, decentralized, and cryptographic nature of blockchain technology, it is possible to (i) avoid intermediaries in transactions between untrusted parties; and (ii) generate an immutable ledger maintained by the network of nodes, which, through the use of a consensus algorithm, make the blockchain tamper-proof. It is this nature that makes the scientific community think about the potential that this technology has for the disruption of the traditional industry, more focused on the centralization of resources and services offered by a company, being the one responsible for the actions taken on its platform. On the other hand, the inclusion of blockchain technology could transition this centralized model to a decentralized one, in which responsibility is distributed democratically among the users of a platform, reducing the cost of services, and also being owners of the data generated on the platform, which is called the democratization of data.

Up to the time of the completion of this PhD Thesis, the scientific community has proposed different models as a way to solve the implementation of this technology in the (Mezquita, Casado, et al., 2019; Mezquita, Gil-González, et al., 2022; Mezquita, Parra-Domínguez, et al., 2022) industry. However, many lacks at some point what is needed to be well deployed in a production environment (Mezquita, Parra-Domínguez, et al., 2022). On the other hand, those that have been deployed in a production environment, offer services that still have a large centralization component, far from the achievement of a full data democracy (Mezquita, Gil-González, et al., 2022). It is for these reasons that the present Doctoral Thesis investigates a model in which the optimization of services is possible, in addition to providing a data democracy in which users are the owners of their information.

This introductory chapter is structured as follows. Section 1.1 introduces the background of the subject under study and describes the problem to be addressed. The Section 1.2 exposes the working hypothesis, as well as the specific objectives of the different research works carried out during the Doctoral Thesis to reach the answer to this hypothesis. Section 1.3 details the methodology followed during the research work. Finally, Section 1.4 describes the structure of the report of this Doctoral Thesis.

1.1. Problem description

There is a trend toward the development of distributed systems using the multi-agent paradigm (Francisco et al., 2019), since they provide several benefits, such as (i) optimization of execution times since the system load is distributed allowing parallel tasks; and (ii) improved system security, since the distribution of tasks means that an attacker needs to attack several actors on the platform to stop the service. These types of systems have been applied to many fields, from the agri-food industry (González-Briones, Castellanos-Garzón, et al., 2018), to process control in the chemical industry (Francisco et al., 2019). Despite the advantages provided by this type of systems, they also bring disadvantages as vulnerabilities to attacks such as *man-in-the-middle*, stealing information or transmitting erroneous data that prevent the proper functioning of the platform, and/or *DDOS*, disabling parts of the platform, it is possible to paralyze the service.

In this context, technologies based on distributed ledgers, known as DLTs (Distributed Ledger Technologies), are beginning to emerge. This type of technology ensures that the communication channels are normally used by agents in publish-subscribe services (*pub-sub*). These technologies are used as the necessary bulletin board for communications between agents. By using a distributed channel, consisting of a network of computers, the platform's communications are secured against denial-of-service attacks, which must attack the entire network to terminate the multi-agent system's communications channel, which is traditionally carried out by a single entity, this being the single point of failure in traditional multi-agent platforms.

Blockchain technology is a type of DLT, which not only provides a more secure communications channel against denial-of-service attacks, but also helps the system

to secure the origin of data and communications between the parts of the system, which helps not only to provide resilience against DDOS attacks, but also to prevent *man-in-the-middle* attacks. Mezquita, Casado, et al. (2019) attacks. Moreover, blcokchain technology also offers the possibility to deploy and use smart contracts. These types of programs are self-executing and do not require intermediaries that do not generate value on the platform, so that, through their use, a platform optimizes its task execution times, in addition to lowering the costs of services by reducing the appearance of (Mezquita, Valdeolmillos, et al., 2019) intermediaries. Finally, all the benefits that blockchain technology provides to traditional systems culminate in the emergence of democratic models, in which the users themselves are responsible for their activity on the platform, also gaining control and ownership over the data they themselves generate on the platform (Mezquita, Gazafroudi, et al., 2019).

Despite the potential benefits of applying this technology to today's industry, there are numerous challenges to its effective use (Mezquita, Casado, et al., 2019; Mezquita, Valdeolmillos, et al., 2019):

- Scalability. For blockchain technology, whose basis is the agreement reached by a network of nodes for information management, scalability is a challenge to be faced. The larger the network size, the greater the number of entities that must reach an agreement, resulting in a greater number of messages sent through the network. In order to speed up the process, consensus protocols can be used (i) that do not require a large number of messages, and (ii) that are fast in commissioning the addition of information to the blockchain. On the other hand, not all protocols are valid for all types of networks, so it is necessary to choose carefully what type of network the designed platform will make use of.

- Network formation. The size of the network can be an issue, not only for scalability, but also for the security provided. A smaller network is easier to attack and gain control of. A network in which identities can be created very easily is also susceptible to attack. Specific types of attacks on this technology are the so-called eclipse attacks, or 51% attacks. To avoid these attacks, the difficulty to create an entity in the network should be encouraged, for example, public blockchain networks require a high resource consumption or an initial investment cost, which prevents the spam of entities within these networks. Permissioned networks, on

the other hand, assign roles to entities known to the network, thus ensuring that these attackers are not part of them.

- Bad practices by users. Cryptocurrency thefts usually have nothing to do with the technology used, but with the fact that users do not use passwords or secure means in which to store their passwords to manage the wallets. Another critical point are the exchanges, the platforms used by the vast majority of cryptoasset users, where they have stored critical information for the management of their wallets, being susceptible to targeted attacks in order to steal the information of these users. In this regard, it is necessary to educate users about the importance of using secure means to generate and store the keys to their wallets. In addition to not trusting just any platform to manage these keys.

- Bad practices on the part of programmers. Smart contracts depend heavily on the developers who implement them. If they have not followed good practices to ensure the integrity of the contract, it is possible for flaws to occur and attackers to exploit those flaws, as happened in the case of the DAO (Buterin, 2016; Daian, 2016). The only way to solve this challenge is to subject smart contracts to audits before their final deployment, in addition to providing a way to update such contracts after deployment.

- Immutability of stored information. Due to the nature of this technology, the stored information is immutable, something seen as an advantage in some fields, but this is not always the case. If the stored information is corrupted to begin with, the blockchain will only maintain the corruption. On the other hand, if there is information owned by a user and he wants to delete it in accordance with the law, he will not be able to do so because of this very nature. If this challenge is to be met, it is only possible through periodic audits of the devices and actors that add information to the blockchain. In this way it is possible to detect those defective ones that are adding flawed information without knowing it. On the other hand, game theory mechanisms are needed to punish undesired behavior on the platform, to prevent information from being intentionally added to the blockchain.

- Transparency. The fact that this technology allows the creation of transparent platforms can be a double-edged sword, since in most cases the activity of users on the platform is exposed, which leads to a vulnerability to users' privacy rights. On

the other hand, if sensitive data is generated, it would also be accessible by third parties, again violating their rights. To meet this challenge, only cryptographic techniques can be used to hide the stored information and only the user knows how to display this data. On the other hand, offchain storage mechanisms can be used, in which the critical information is stored in a system outside the blockchain, while only the summary or hash of this information is stored in the blockchain. This is a less centralized solution and does not ensure that the information stored outside the blockchain is not modified, but it does ensure its detection. On the other hand, anonymity can only be achieved with transactor masking mechanisms.

After analyzing all the challenges, and their possible solutions that are presented in relation to this technology, it can be concluded that a platform that wants to move from the pilot test stage and reach the deployment process, needs to take into account many variables. Some of these variables do not have to do with the blockchain technology used, but they must take into account which users are in their target, to guide them and avoid possible problems caused by bad practices on their part. On the other hand, it is not an easy task, first to identify each and every one of these challenges, and second to design a platform to address them. As will be discussed later in Chapter 3, the designs in the literature do not cover each of the aspects studied, so it is necessary to design a model to guide and help developers to implement this type of platforms, becoming the main objective of this Doctoral Thesis.

1.2. Hypothesis and objectives

This Doctoral Thesis seeks to encourage the proliferation of blockchain technologies in the optimization of services in different areas of the current industry. First, we seek to understand what is the real potential of blockchain technologies to disrupt the traditional industry. After that, the challenges faced by this technology are studied in detail, both technical, since being a relatively new technology still has potential for improvement, and those related to regulatory frameworks, since this is a major stumbling block for this type of distributed technologies, which seek the automation of processes (Mezquita, Casado, et al., 2019). Finally, it details what has been done in the literature in different areas: (i) supply chains (Mezquita, Casado-Vara, et al., 2021; Mezquita, González-Briones, et

al., 2019), (ii) property registries (Mezquita, González-Briones, et al., 2019; Mezquita, Parra-Domínguez, et al., 2022), and (iii) automatic marketplaces (Mezquita, Gazafroudi, et al., 2019; Mezquita, Gil-González, et al., 2022). Thanks to this, it has been possible to present an evolution along the Doctoral Thesis, of different models improving previous literature works, showing a model to which any researcher and developer can go to lay the foundations of a platform based on blockchain technology.

The **Hypothesis** raised for the realization of this Doctoral Thesis is that blockchain technology can optimize traditional services of the current industry, in addition to facilitating the emergence of new models of decentralized services, not possible with other technology.

Based on this hypothesis, this Doctoral Thesis proposes to achieve the following **main objective**:

research and design models of architectures based on blockchain technology, which will help researchers, designers, and developers to implement this type of platforms in the real world, being able to go beyond the proof-of-concept or pilot project stage. These models will face each of the challenges that blockchain technology poses, taking into account aspects that other models in the literature have not had and complying with one of the most restrictive legal frameworks in data management and service automation, such as that of the European Union.

To achieve the main objective, it is necessary to define a list of **specific objectives**, which are described below:

(**OB1**) Demystify the blcokchain technology, detailing which are the qualities that its use can contribute to the processes of the current industry, dominated by the Internet of Things.

(**OB2**) Identify the existing requirements so that blockchain technology can be implemented in environments where there is a large amount of communication between devices.

(**OB3**) Conduct a state-of-the-art study in the areas where blockchain technology has the greatest potential for disruption.

(**OB4**) Analyze the challenges, motivations and open problems when applying the solutions proposed by the literature.

(**OB5**) Design architectures that complement and improve previous proposed models.

(**OB6**) Validate the proposed models by analyzing in detail how they address each of the identified challenges.

(**OB7**) Design a future work plan for the design and implementation of new protocols that will help in the application of these platforms in a futuristic scenario where quantum computers become a reality, invalidating current encryption and identification techniques.

1.3. Research methodology

The *research-action* (AR) methodology is a change-oriented methodology that offers the possibility of carrying out both research and action simultaneously, which is why it has been gaining more and more popularity and importance in Software Engineering projects. The term was coined by Kurt Lewin in 1952 Herreras (2004) in response to a need for research, no longer limited only to the production process, but during a cyclical and iterative process of exploration, action, and validation of the results obtained. Colloquially, this methodology can be defined as a methodological process to carry out improvement activities and maintain what has been improved.

The process of *research* relates to the detailed understanding of the subject matter by the researcher, client, or both. On the other hand, the process of "action" is generally associated with the transformation made in a given community, organization, or project. According to Baskerville (1999), the AR methodology is considered necessary to achieve a more realistic scenario, since it involves a real context to investigate the results of concrete actions.

According to Baskerville (1999), cited by Tüzün et al. (2019), studies developed under this methodology share four common characteristics:

1. an orientation to action and change;
2. an approach to the problem;

3. an organic process involving systematic and sometimes iterative stages;
4. as well as collaboration among participants.

In general, the RA consists of five phases (Eden & Ackermann, 2018; Tüzün et al., 2019), described below together with what is developed in this Doctoral Thesis in each of them:

1. **Diagnosis:** This phase corresponds to the identification and statement of the problem set out in this Doctoral Thesis. It is necessary to delimit the scope, propose a hypothesis and define the objectives to be achieved. For the specific case of this Doctoral Thesis, we proceed to identify and analyze the potential benefits of blockchain technology in the industry, as well as the challenges and problems posed by its implementation in a real scenario.
2. **Review of literature:**In this case, a systematic review of the literature is carried out. A systematic review is a scholarly synthesis of evidence on a clearly presented topic that uses critical methods to identify, define, and evaluate research on the topic (Barn et al., 2017; Petersen et al., 2008). To achieve the objectives presented in this Doctoral Thesis, we have proposed the following questions to be answered during the dissertation:

   (**RQ1)** What does blockchain technology provide to current industry processes?

   (**RQ2)** What are the issues raised by its use?

   (**RQ3)** What has been proposed in the literature to date?

   (**RQ4)** How can they be improved?

   .

   For each of the research questions posed in order to answer the hypothesis developed in the section 1.2, different research works have been carried out throughout this Doctoral Thesis, which will be shown during the development of this report.
3. **Solution:** Based on the results obtained in the two previous phases, a solution that meets the established objectives is proposed. In this Doctoral Thesis, several architectures are proposed to optimize and improve (in terms of costs, time, and functionalities) processes in different areas of industry, like logistics and automatic markets in this case.

4. **Evaluation:** Although the proposed architectures have not been implemented in a real environment, they have been analyzed and evaluated based on other architectures, which are being used in real use cases, on which they share certain characteristics. For example, concerning automatic energy markets, architectures have been shown that, although they do not allow automatic negotiations, they do allow the traceability of the energy transacted, sharing a base that allows analyzing the possible performance of the new architecture.

5. **Results:** It comprises the last phase of the AR cycle. Through the activities of this stage, the scientific community evaluates the results obtained based on a set of publications that are submitted for evaluation in high-impact journals, including *Expert Systems with Applications*, *IGPL*, or *Energies*, as well as in international congresses and conferences, such as the International Conference on Knowledge Management in Organizations or the International Conference on Practical Applications of Agents and Multi-Agent Systems, among others.

1.4. Doctoral Thesis structure

To validate the hypothesis established in this Doctoral Thesis, defined in section 1.2, we start with a detailed study of blockchain technology, understanding what it can offer to the current industrial paradigm, and what are the challenges that must be overcome to be able to make effective use of it (OB1 and OB2). After that, we proceed to study the state of the art in terms of platforms and designs where this technology is most useful (OB3). Subsequently, an analysis will be carried out to validate the architectures and models in the literature on the identified challenges (OB4).

Once the advantages and disadvantages of the platforms proposed by the literature have been detailed and understood, we proceed to design our own models that improve in some aspect (e.g. more functionalities, greater privacy for users) the previously existing architectures (OB5). Finally, the contributions made are analyzed to demonstrate that they effectively face the challenges posed to this technology (OB6).

The structure of this Doctoral Thesis by compendium of articles/publications includes the presentation of the evidences and results originated in the research work carried out during the elaboration of this Doctoral Thesis, as well as the publications accrediting

the research carried out. Finally, the conclusions and lines of future work are presented (OB7). In this way, and as mentioned above, in order to facilitate the follow-up of the research, the report of this Doctoral Thesis is structured in six Chapters.

Chapter 1 describes the problem to be solved, the working hypothesis is formulated, the different objectives are detailed and the research methodology followed for the completion of this Doctoral Thesis is described.

Chapter 2 presents a review of the state of the art in which the benefits of blockchain technology are demystified, taking a more realistic approach to what it can and cannot do. In addition, it details the challenges that have been identified throughout this PhD Thesis and the possible solutions provided by the literature in different fields.

Chapter 3 describes the contributions resulting from the research carried out and summarized in this Doctoral Thesis. This chapter details the architectures presented during this Doctoral Thesis, improving some aspect of those studied during the literature review. In addition to analyzing how they meet the challenges posed for their successful implementation in real scenarios.

Chapter 4 presents the results achieved through the development of the research that culminates in this Doctoral Thesis and that are validated through a set of publications in scientific journals, book chapters, conferences, congresses and international workshops in which contributions have been provided, as well as the research projects in which the doctoral candidate has participated. Likewise, the stays performed in international research organizations are detailed.

Chapter 5 includes the original publications that form part of this Doctoral Thesis by compendium of articles/publications, accompanied, each one of them, by its corresponding introduction, set of objectives, description of the research methodology used in each one, as well as the conclusions of the results obtained in each one of these publications.

Finally, Chapter 6 details the main conclusions obtained from the research work developed in this Doctoral Thesis and the most relevant contributions made. In addition, the lines for the development of future work that are opened from the results of the present Doctoral Thesis are defined. To conclude, the list of all the bibliographic sources

that have been cited in this report is included in order to support the statements and concepts presented.

Capítulo 2

Estado del Arte

VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

Capítulo 2

Estado del Arte

Se denomina tecnología blockchain (cadena de bloques en español) al conjunto de protocolos de comunicación y criptográficos utilizados para poner de acuerdo una red de pares (P2P, *Peer to Peer* por sus siglas en inglés) en el mantenimiento de un registro inmutable y distribuido (Valdeolmillos, Mezquita, González-Briones, Prieto, & Corchado, 2019). El registro adquiere forma de una cadena de bloques, en los que se almacena la información, de aquí el nombre de la tecnología. Debido a que cada bloque está enlazado con el anterior formando la mencionada cadena, véase Figura 2.1 es necesario reunir una serie de requisitos, dependiendo del tamaño de la red de nodos y los algoritmos de consenso utilizados, a priori imposibles, para modificar la información almacenada en los nodos más profundos de la cadena. Por esta razón se dice que la información almacenada en la cadena de bloques es inmutable. Su primer caso de uso real apareció en 2009 con Bitcoin, diseñado en el *whitepaper* de Satoshi Nakamoto (Nakamoto et al., 2008). Con esta plataforma se buscaba la democratización del dinero, junto a la automatización de los pagos sin necesidad de intermediarios humanos. Extrapolando el caso de uso, muchos autores en la literatura han definido la tecnología blockchain como aquella con el potencial para disruptir la mayoría de los procesos actuales. Existe una gran cantidad de alternativas en cuanto a configuración de la tecnología, siendo cada una óptima para casos de uso específicos, por lo que también es necesario tener en cuenta el estudio de las posibilidades para el desarrollo de cualquier plataforma basada en blockchain. Por ello, en este capítulo se presenta una revisión del estado del arte, en el que se ahondará en los aspectos claves y alternativas que ofrece esta tecnología, en varios ámbitos y escenarios.

Así, en el resto de este Capítulo se procede a describir, de forma progresiva, las características básicas de la tecnología blockchain, cuál es su potencial en el mundo moderno, y qué retos y problemas enfrenta actualmente en cada ámbito de estudio dentro

FIGURA 2.1: Diagrama descriptivo de la estructura interna de datos de una cadena de bloques. En él se puede apreciar el entrelazamiento de los bloques entre sí, cómo la información del bloque predecesor es almacenada en el sucesor,el *hash* en el campo *Prev*.

de la tesis. La Sección 2.1 expone un primer acercamiento a la tecnología blockchain, cómo surgió, qué ofrece su aplicación a la industria actual, y qué problemas conlleva su implementación. La Sección 2.2 analiza en detalle los principios básicos de esta tecnología, sobre los que nos basaremos a la hora de enfrentar los retos que se plantean en el mundo real. La Sección 2.3 describe cómo puede mejorar los ámbitos de la industria estudiados en la presente Tesis Doctoral (plataformas financieras, logísticas, de gobierno electrónico, y microredes de energía inteligentes), así cómo cuáles son los problemas que se plantean a la hora de desarrollar una plataforma basada en blockchain en cada uno de ellos. La Sección 2.4, finalmente, expone las principales conclusiones obtenidas a raíz de este análisis.

2.1. Potencial y límites de la tecnología blockchain

La crisis financiera de 2008 quebró la confianza de la sociedad en los bancos y en las instituciones financieras centralizadas; estas entidades provocaron dicha crisis al prestar grandes sumas de dinero mientras mantenían muy poco en reserva (Earle, 2009; Gros & Roth, 2010). Bitcoin surgió en 2009 como respuesta a las transgresiones y abusos por parte de las mencionadas instituciones. La solución que propuso fue la aparición de una moneda que pudiera funcionar sin una autoridad central, distribuyendo su gobernanza entre los nodos P2P que la mantienen (Nakamoto et al., 2008). Bitcoin se compone de una serie de protocolos criptográficos que transforman por completo el proceso de realizar transacciones, la denominada tecnología blockchain. Tras este primer caso de uso exitoso, irrumpieron en nuevas plataformas de criptomonedas que ofrecen diferentes funcionalidades y aplicaciones, denominada estas como cryptomonedas de segunda generación, véase la Tabla 2.1. El ejemplo más importante es el caso de

Ethereum, segunda moneda en capitalización de mercado, y cuya finalidad es la creación de un entorno para la programación de plataformas descentralizadas, las denominadas dApps (por sus siglas en inglés *decentralized Applications*). Gracias a la implementación de su *Ethereum Virtual Machine* y la creación del lenguaje de programación *Solidity* (Ting, 2017), esta plataforma ofrece el diseño y desarrollo de contratos inteligentes (*smart contracts* en inglés) *Turing* completos.

Tabla 2.1: Tabla resumen de las generaciones de cadenas de bloques.

Generación	**Características**	**Principal exponente**
Primera generación	Esta generación hace referencia a las cadenas de bloques que están basadas en PoW y no permiten el desarrollo de contratos inteligentes Turing-completos.	Bitcoin
Segunda generación	Esta generación hace referencia a las cadenas de bloques que permiten el desarrollo de contratos inteligentes Turing-completos, pero que tienen problemas de escalabilidad masiva.	Ethereum
Tercera generación	Esta generación hace referencia a las cadenas de bloques que permiten el desarrollo de contratos inteligentes Turing-completos, y permiten escalar la plataforma gracias al uso de algoritmos de consenso como el dPOS.	EOS

El uso de la tecnología blockchain ofrece un potencial acercamiento del sistema financiero a una economía verdaderamente democrática construida por la comunidad (Crosby, Pattanayak, Verma, Kalyanaraman, et al., 2016; Mezquita, Gil-González, et al., 2022). La aparición de tantas criptomonedas diferentes, ha ofrecido además un amplio abanico de oportunidades para su adopción en diferentes casos de uso. Por otro lado, la irrupción de los contratos inteligentes, ha propiciado que los casos de uso no se limiten únicamente a las transacciones financieras, sino que también se pueda digitalizar y transaccionar cualquier activo de valor. Esto está suponiendo la aparición de estudios y projectos piloto que buscan propiciar una disrupción en numerosos ámbitos de la industria, como por ejemplo, en sistemas de logística (Mezquita, Casado-Vara, et al., 2021; Mezquita, González-Briones, et al., 2019), gobierno electrónico (Mezquita, Parra, et al., 2019), mercados de energía (Mezquita, Gil-González, et al., 2022), etc. Gracias a la aplicación de la tecnología blockchain, es posible reducir el factor humano al mínimo indispensable, automatizando grandes porciones de los procesos, mientras se eliminan aquellos intermediarios que no aportan valor real al producto final. Además, y sobretodo

en los sistemas IoT (por sus siglas en inglés de *Internet of Things*), la aplicación de esta tecnología ayuda en la identificación de los dispositivos, proporcionando certeza al origen de los datos y seguridad en las comunicaciones (Casado-Vara, Chamoso, De la Prieta, Prieto, & Corchado, 2019; Mezquita, González-Briones, et al., 2019). Por todos los potenciales beneficios, se empieza a hablar de un cambio de paradigma en relación a los procesos mencionados.

Además de todos los potenciales beneficios del uso de esta tecnología, se han estudiado las limitaciones que le afectan a la hora de hacer uso de ella en aplicaciones en producción (Mezquita, González-Briones, et al., 2019):

1. Escalabilidad: Existe un problema de escalabilidad en las aplicaciones basadas en blockchain. Este problema viene ligado al trilema de escalabilidad definido por Vitalik Buterin, el creador de Ethereum. Este trilema asegura que una red blockchain solo puede ser escalable si pierde o en consistencia o en descentralización. Esto quiere decir que a más descentralizada y segura, una red, por ejemplo la red pública de Bitcoin o Ethereum, tiene menor capacidad para gestionar un número alto de transacciones. En una red pública, en la que cualquiera puede formar parte se necesita una alta seguridad y un alto nivel de descentralización. Por este motivo se sacrtifica en escalabilidad para mantener la red. Por otro lado, se puede sacrificar seguridad y centralización si en la red sólo existen nodos conocidos cuyos intereses se alinean con el bienestar de la red, con el objetivo de mejorar la escalabilidad del sistema.

2. Consumo: Algunas redes blockchain hacen uso de una enorme cantidad de recursos energéticos, como es el caso de la red de Bitcoin, para mantener la seguridad en la red. Este tipo de redes utilizan algoritmos de consenso que benefician la seguridad a coste de un consumo ingente de recursos. Por esta razón, hay que pensar en el coste de manutención de este tipo de redes, para saber si se pueden utilizar en un determinado proyecto.

3. Confianza en los datos: A pesar de que se dice que los datos almacenados en la blockchain son inmutables, esto no es sinónimo de confianza en los mismos. Lo único que indica es que los datos almacenados provienen de la fuente que clama su autoría. Por lo que si desde el origen los datos están viciados, lo único que se consigue es perpetuar el vicio. Para desarrollar una plataforma sana basada en la

tecnología blockchain, es necesario diseñar un sistema de auditorías que permita mitigar el problema del vicio en los datos introducidos.

4. Anonimicidad: A día de hoy existe conflicto con la regulación existente (el denominado Reglamento General de Protección de Datos, o *GDPR* por sus sigloas en inglés: *General Data Protection Regulation*) y la información almacenada en blockchain. Por un lado, una de las características de la tecnología blockchain es la transparencia que aporta a cualquier sistema que la utilice, por otro lado, esta misma transparencia puede causar un conflicto con la legislación si la información almacenada es sensible. Además, existe el derecho al olvido en la legislación actual, algo que directamente se opone al mismo fundamento de esta tecnología, en el que no se puede borrar ni modificar la información almacenada. Por este motivo, es necesario pensar en varios enfoques para solventar este problema: i) utilización de la encriptación de la información almacenada; ii) almacenamiento en la blockchain de información resumida (denominado *hashing*) mientras se utilizan otros medios para su almacenamiento, siendo la blockchain sólamente un medio para la verificación de su inmutabilidad.

5. Gestión de la responsabilidad: Por último, no existen mecanismos legales que sean capaces de regular y responsabilizar de la información almacenada en este tipo de sistemas distribuidos. Este es un punto bien discutido en la literatura, dejando claro que es necesario un marco legal conjunto entre países para poder regularlo, algo que de momento parece bastante lejano en el tiempo.

En este capítulo, se realizará una revisión progresiva, tanto de la tecnología blockchain en general, sus características y los principales problemas que enfrenta, cómo de los proyectos realizados en la literatura dentro de los diferentes ámbitos que conciernen a esta tesis. De estos estudios dependerá la justificación del trabajo de investigación realizado en la presente tesis doctoral, dando valor a las aportaciones alcanzadas en ella.

2.2. Tecnología blockchain, principios básicos

Se pueden enumerar como componentes básicos que posee la tecnología blockchain los siguientes: (i) una red de nodos conectados punto a punto (P2P) que mantienen

y gestionan el libro mayor distribuido, (ii) algoritmos de consenso utilizados para la acordar la adición de la información en el libro, (iii) protocolos criptográficos utilizados en diferentes partes del sistema: firmado y almacenamiento de la información, y (iv) en algunas plataformas, máquinas virtuales que permiten la ejecución de contratos inteligentes.

Esta Sección está estructurada siguiendo la enumeración anterior. La Sección 2.2.1 describe los diferentes tipos de redes que se pueden construir en una plataforma basada en blockchain. La Sección 2.2.2 expone las ventajas y desventajas de los algoritmos de consenso más utilizados. La sección 2.2.3, explica cómo se utilizan los protocolos criptográficos en estos sistemas. La sección 2.2.4 detalla la evolución y el uso de los contratos inteligentes dentro de este tipo de plataformas. La Sección 2.2.5, finalmente, discute acerca de los principales retos que se pueden encontrar a la hora de diseñar y construir plataformas basadas en tecnología blockchain.

2.2.1. Tipos de redes

La red de nodos que subyace al sistema se encuentra directamente interconectada punto a punto, formando lo que se denomina red P2P. Cada uno de los nodos que componen la red actúa de forma autónoma, encargándose de gestionar y mantener la información que se almacena en la cadena de bloques. Gracias a esa autonomía, se cosigue obtener un sistema descentralizado en el que no existe un punto único de fallo, ofreciendo resiliencia a las plataformas que hace uso de esta tecnología, añadiendo resiliencia a ataques cómo los de denegación de servicios distribuidos (DDoS, por sus siglas en inglés). Por otro lado, la información de la cadena de bloques está almacenada de forma duplicada en cada nodo, lo que asegura en mayor medida que la información va a ser accesible, incluso durante un ataque, si la red es lo suficientemente grande. Por último, eso también ayuda a la hora de verificar la información, para manipular la información ya almacenada, es necesario ganar el control del 51 % de los nodos, por lo que a mayor cantidad de nodos, más difícil es conseguir el control de tantos.

Visto la importancia de la red nodos dentro de una plataforma basada en tecnología blockchain, podemos proceder a clasificar los tipos de redes que se pueden desplegar en (véase la tabla 2.2) redes públicas, privadas y permisionadas (Mezquita, Casado, et al., 2019):

- Redes públicas: las redes públicas son aquellas constituidas por nodos que tienen libre albedrío para conectarse o desconectarse. Este tipo de redes son las redes más democráticas y descentralizadas, ya que cualquiera puede acceder y formar parte de ellas. Por otro lado, son las redes más propensas a ataques, los nodos que las conforman poseen intereses que no tienen porqué estar alineados con el buen funcionamiento de la plataforma. Por este motivo, en este tipo de redes se hace especial incapié en proteger la información almacenada en la blockchain de los ataques internos, sacrificando normalmente la velocidad de creación de bloques, cómo es el caso de la red de Bitcoin.

- Redes privadas: las redes privadas son aquellas desplegadas y gobernadas por una única autoridad, se convierten en este caso en un sistema centralizado. En este tipo de redes los nodos son bien conocidos y están relacionados con la entidad que despliega la red, de esta forma se asume que van a actuar en base al bien estar de la plataforma, ya que sus intereses se alinean con ella. Las redes privadas no necesitan sacrificar latencia para aumentar la seguridad del sistema. Este tipo de redes puede ser utilizado en plataformas encargadas de la gestión de la comunicación en procesos intragrupo de una misma empresa, siendo la empresa la entidad soberana de la plataforma, y los diferentes departamentos los responsables de los nodos de la red.

- Redes permisionadas: de forma similar a cómo sucede con las redes privadas, en las permisionadas, los nodos tienen restringido el acceso a la red. En este caso, quien despliega y gobierna la red es una cooperativa de entidades que comparten intereses dentro de una plataforma. En este caso la seguridad se asume en que las diferentes interacciones entre entes van a realizarse de forma honesta para evitar su propio perjuicio. En este caso, por ejemplo, se encuentran los sistemas logísticos, en los que productores, transportistas, empresarios y pormenoristas trabajan en conjunción para mejorar la calidad del servicio que ofrecen al consumidor final: la producción, transformación y distribución de productos.

2.2.2. Algoritmos de consenso

Como se ha descrito en el apartado 2.2.1, existe una red de nodos que conforma la base de cualquier plataforma basada en tecnología blockchain. Estos nodos se encargan de

Tabla 2.2: Tabla resumen de los tipos de redes blockchain.

Tipo de red	**Características**	**Ejemplos de uso**
Pública	En este tipo de redes cualquier individuo puede conectarse y formar parte de ella.	Criptomonedas.
Privada	Esta red está gobernada por una única entidad, otorgando roles al resto de nodos conectados.	Comunicaciones intragrupo de una empresa.
Permisionada	La gobernanza de esta red se lleva a cabo de forma cooperativa entre diferentes partes. Cada nodo debe estar identificado para formar parte de la red, restringiendo el acceso a aquellos que no formen parte del consorcio.	Intercambio de bienes entre diferentes partes.

mantener la información almacenada en la cadena de bloques, pero necesitan primero llegar a un acuerdo en qué se va a almacenar. Para ello, la red debe converger en un acuerdo, haciendo uso de lo que denominamos algoritmos de consenso. El algoritmo de consenso es el protocolo utilizado por la red de nodos para acordar qué nodo genera el nuevo bloque y qué información puede estar almacenada en él. El número de estos algoritmos no deja de aumentar, aunque la gran mayoría son variaciones de alguno de los siguientes (Mezquita, Valdeolmillos, et al., 2019):

- **Proof-of-Work** (PoW) es un algoritmo de consenso en el cual un nodo de la red debe resolver un problema criptográfico para añadir un nuevo bloque a la blockchain. El coste computacional y la dificultad de resolver el problema, junto a la energía gastada en encontrar su solución (trabajo), en contra de la simplicidad de su verificación, son razones suficientes para disuadir a los nodos que añaden nuevos bloques (mineros) de realizar transacciones ilegales.

- **Proof-of-Stake** (PoS). En este algoritmo, los mineros se turnan para añadir nuevos bloques a la cadena. La probabilidad de que un minero consiga su turno para añadir un bloque depende del número de monedas depositadas por el minero a modo de participación o inversión en la plataforma (*Stake*). Este algoritmo asume que un nodo va a ser honesto en la creación de un bloque para no perder lo invertido en la plataforma.

- **Practical Byzantine Fault Tolerance** (PBFT). En este tipo de algoritmos de consenso, se define como ronda al proceso de añadir un nuevo bloque a la cadena de bloques. En cada ronda, se selecciona un nodo para que proponga un nuevo

bloque, y luego el bloque se difunde a la red, para que ésta lo valide. El bloque es validado por cada nodo de la red, obteniendo un voto por cada nodo que lo haya validado con éxito. Cuando un bloque recibe 2/3 de los votos de todos los nodos de la red, se considera válido y se añade a la cadena de bloques. Debido a que en este tipo de algoritmos se necesita que sólo 2/3 de los nodos de la red sean honestos, no se puede utilizar en redes públicas, siendo utilizados únicamente en entornos controlados, cómo las redes permisionadas o las privadas.

2.2.3. Criptografía y blockchain

Dentro de una plataforma blockchain, se hace uso de la criptografía con las funciones resumen o hash. Estas funciones lo que hacen es construir una cadena de caracteres encriptados a partir de otra cadena en texto plano. Es un proceso irreversible que se utiliza con el fin de garantizar la integridad de los datos almacenados en la cadena de bloques.

Por otro lado, en este tipo de plataformas también se hace uso de un mecanismo de firma de pares de claves, gracias al cual es posible verificar fácilmente la fuente de los datos generados. Para poder utilizar este tipo de plataformas, un usuario necesita generar una clave aleatoria, la denominada clave privada del par de claves. De esta clave se deriva la segunda del par: la denominadca clave pública. Este mecanismo de criptografía de clave pública se utiliza, no sólo porque permiten una gestión eficiente de las claves, sino también porque es imposible que un atacante obtenga la clave privada incluso conociendo la pública. De esta forma, mientras la clave privada no se vea comprometida, un usuario puede estar seguro de que nadie podrá realizar transacciones en el sistema en su nombre (Huh, Cho, & Kim, 2017).

La forma de identificar un usuario dentro de la plataforma es mediante la dirección de su cuenta, lo que se denomina *wallet* en inglés. Para generar una wallet, el usuario debe realizar un proceso de tres pasos que comienza con la generación de una clave privada aleatoria que sólo debe conocer el propietario. A continuación, mediante una transformación algorítmica unidireccional, se obtiene la clave pública, que se comparte con la red y se utiliza para verificar las firmas realizadas por el usuario con su clave privada. Por último, se realiza un hash de la clave pública para obtener la dirección del

monedero que se utilizará en el intercambio de activos virtuales entre particulares dentro del protocolo blockchain.

El proceso de intercambio de activos es bastante sencillo y comparte los mismos pasos que en todas las cadenas de bloques. La figura 2.2 ilustra cómo un usuario, Alice, quiere iniciar una transacción con Bob de 2 monedas. Para ello, Alice firma la transacción (Tx) con su clave privada y la difunde en la red. A continuación, cada nodo de la red verifica la firma de Alice con su clave pública, y si la comprobación es correcta y se demuestra que la transacción procede de Alice, la red valida que tiene las monedas que quiere gastar. Si todo va bien, la transacción se añade a la cadena de bloques.

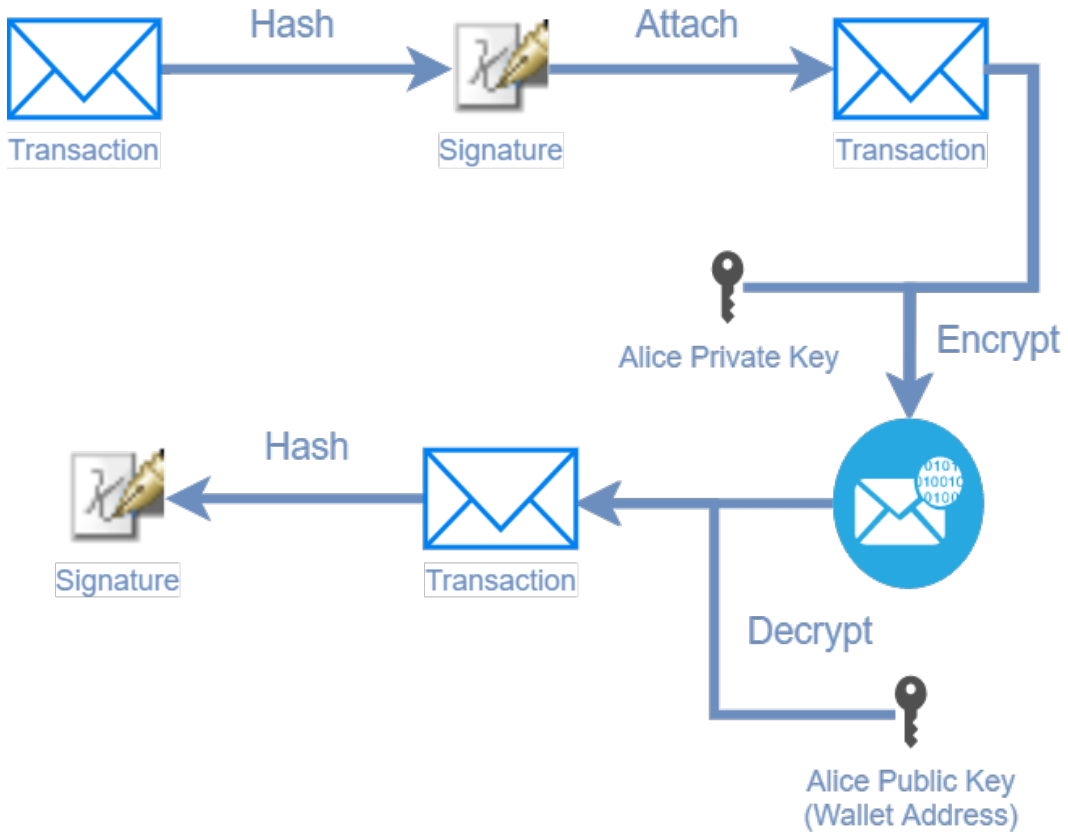

FIGURA 2.2: Diagrama descriptivo del proceso de transacción en la blockchain.

2.2.4. Smart contracts

El lenguaje Bitcoin Script es un lenguaje simple, que no soporta bucles (no Turing-completo), evitando así posibles bucles infinitos en la verificación de las transacciones bitcoin.it (s.f.). Además, como Bitcoin hace uso del modelo UTXO (Unspent Transaction Output) no permite un control de grano fino sobre las

transacciones no utilizadas. En este modelo, se almacena en una base de datos de transacciones todas aquellas no utilizadas por sus propietarios, lo que hace imposible cambiar su estado (Buterin et al., 2014).

Ethereum surge así como una alternativa a Bitcoin que permite la construcción de aplicaciones decentralizadas en la blockchain y la representación de la lógica de negocio en la misma. Para ello, Ethereum ofrece un lenguaje de programación Turing-completo que permite a los usuarios de la blockchain definir sus propias reglas. A diferencia de Bitcoin, Ethereum utiliza un modelo de balance de cuentas para almacenar los activos que poseen los usuarios. Este modelo también permite el uso de diferentes formatos y la transición entre estados de los activos almacenados.

Para evitar el uso excesivo de recursos de computación, red y almacenamiento, evitando así bucles infinitos, el que quiera ejecutar el código de un *smart contract* debe realizar un pago proporcional a la complejidad del código (Buterin et al., 2014). El pago se realiza en *GAS*, que es el precio interno que se utiliza para ejecutar un contrato o una transacción, siendo los mineros los encargados de fijarlo.

La blockchain de Ethereum fue la primera en dar soporte a los *smart contracts* y permitir el desarrollo de Aplicaciones descentralizadas (dApps por sus siglas en inglés). Los *smart contracts* desplegados en la red Ethereum son códigos descentralizados basados en cláusulas *IF-THEN*. Una vez acordadas entre las partes, estas cláusulas son inmutables, automáticas y vinculantes, permitiendo la ejecución del contrato sin necesidad de un tercero. Una vez desarrollado, el código de un *smart contract* se distribuye a todos los participantes de la red blockchain.

Para ser ejecutado, un *Smart Contract* debe recibir un mensaje. Un mensaje es una transacción originada por usuarios, otros *smart contracts*, o eventos con información específica a través de una acción externa. Después de ser ejecutado, toda la red blockchain valida su resultado para evitar que sea falsificado.

Uno de los primeros lenguajes de programación utilizados para construir dApps en Ethereum fue Serpent, pero una auditoría realizada por la empresa de seguridad de blockchain *Zeppelin Solutions* descubrió problemas con el compilador y algunas vulnerabilidades críticas (Casto, 2017). Debido a esto, el lenguaje de programación Solidity ha tomado su lugar, siendo ahora el lenguaje de programación más utilizado en

el desarrollo de contratos inteligentes en la máquina virtual de Ethereum (Casado-Vara, González-Briones, Prieto, & Corchado, 2018; solidity.readthedocs.io, s.f.). Pero aunque este lenguaje de programación no tiene ninguna de las vulnerabilidades descubiertas en su predecesor, sigue siendo muy nuevo, poco conocido por los desarrolladores lo que les hace cometer errores en el desarrollo de *smart contracts* y dApps. Por ejemplo, uno de los exploits más famosos ocurridos en la historia de Ethereum fue el exploit *DAO*. Este exploit se produjo debido a una vulnerabilidad en el patrón de codificación del *smart contract*. Era conocida y estaba siendo arreglada por sus creadores, pero mientras lo hacían, el hacker preparó el exploit para drenar todos los fondos del DAO (Daian, 2016). El *script* consistía en llamar recursivamente a la función "*split*" dentro de sí mismo, recogiendo el Ether del mismo muchas veces con una sola transacción (Buterin, 2016). El segundo mayor ataque a una dApp de Ethereum, fue el llamado Parity Wallet Hack Palladino (2017). Para robar 150.000 Ether (ETH), el atacante envió dos transacciones a cada contrato con vulnerabilidades. Con la primera transacción, el hacker obtuvo la propiedad de la cartera, y con la segunda transfirió todos los fondos de la víctima.

En (Nikolić, Kolluri, Sergey, Saxena, & Hobor, 2018) se ha hecho una clasificación de los *smart contracts* en función del tipo de vulnerabilidad que tienen:

- Codiciosos. Este tipo de *smart contract* es capaz de bloquear los fondos de sus usuarios y luego retenerlos indefinidamente sin liberarlos. Los errores más comunes en los contratos inteligentes codiciosos son que aceptan Ether pero carecen del conjunto de instrucciones que envía el Ether.
- Pródigos. Estos han caído en manos de atacantes y pueden enviar Ether a una dirección que no es la de su propietario.
- Suicidas. Para que su propietario pueda cerrar y matar un *smart contract* en circunstancias críticas como un ataque o por una función obsoleta se suelen implementar funciones suicidas en el contrato inteligente. Cuando una cuenta arbitraria es capaz de invocar estas funciones, el *smart contract* tiene una vulnerabilidad y se denominan a estos contratos suicidas.

2.2.5. Retos en la construcción de plataformas basadas en technología blockchain

El objetivo de esta sección es señalar los factores limitantes de la tecnología blockchain para mejorar plataformas y casos de uso reales. Una plataforma basada en tecnología blockchain, es aquella que hace uso de una red de nodos P2P como (i) canal de comunicaciones seguro y descentralizado entre las diferentes entidades de la plataforma, (ii) método para la creación de un histórico de datos inmutable, y/o (iii) paradigma para la automatización, total o parcial, de la plataforma. Una plataforma basada en blockchain debe incluir: (a) la red de nodos P2P que se encarga de gestionar la información transmitida y que a su vez hacen uso de un algoritmo de consenso y protocolos criptográficos; (b) la lógica de despliegue y ejecución de los contratos inteligentes que automatizan las interacciones entre partes; (c) intermediarios que se encarguen de gestionar el flujo de datos del mundo real necesarios por los contratos inteligentes, los llamados oráculos (Asolo, 2018); y (d) los sistemas de almacenamaiento de la información que se encargan de almacenar y gestionar aquellos datos, que por su naturaleza, no pueden ser almacenados en una blockchain. Existen propuestas de plataformas basadas en blockchain en casi cualquier ámbito de la industria: cadenas de suministro (Daza, Di Pietro, Klimek, & Signorini, 2017), finanzas descentralizadas (Valdeolmillos et al., 2019), administración pública (Mezquita, Parra-Domínguez, et al., 2022), mercados energéticos (Aitzhan & Svetinovic, 2016), ciudades inteligentes (Mezquita, González-Briones, et al., 2021), etc.

A pesar de la creciente popularidad en el diseño de propuestas basadas en blockchain, hay que tener en cuenta que existen numerosos retos a los que se enfrenta para que estas plataformas puedan ser desplegadas en un entorno real(Mezquita, Casado, et al., 2019). Uno de ellos es el coste del mantenimiento de la red de nodos y la energía que utilizan, por lo que hay que distinguir en qué casos la interacción con la blockchain es mínima y se puede hacer uso de una red pública, y en qué casos se hace necesario el despliegue de una red permisionada que consuma poca energía y permita una alta tasa de transacciones por segundo (TPS). Este reto es tratado en el artículo del compendio (Mezquita, Casado-Vara, et al., 2021), dónde se analiza el número de interacciones con la blockchain por parte de los agentes de la plataforma.

Por otro lado, hay que tener en cuenta que un punto crítico de los contratos inteligentes son los oráculos y la ingesta de datos provenientes del mundo real. En este sentido hay que evitar confundir inmutabilidad de los datos almacenados con validez de los mismos. Por ejemplo, en plataformas reales, sobretodo las basadas en dispositivos ÍoT, los dispositivos pueden estar añadiendo datos corruptos a la cadena de bloques, de forma intencionada o no, estos datos no deben ser utilizados, por lo que su entrada en el sistema supone un riesgo para la plataforma. Que estos datos, una vez dentro, sean inmutables, no es equivalente a que sean veraces o válidos (Liang, Zhao, Shetty, & Li, 2017; Mezquita, Casado, et al., 2019). Este reto se detalla en profundidad en la Sección 3.1.

Sin embargo, el mayor obstáculo que presentan las tecnologías basadas en libros mayores distribuidos son los entornos legales. En este caso, la regulación existente es escasa o no existente, por lo que no existen mecanismos sólidos de alocación de la responsabilidad. Por ejemplo, en el caso de la red de Bitcoin, existen enlaces a pornografía infantil, pero como estos enlaces ya no pueden ser borrados por la inmutabilidad de los datos, hay que buscar soluciones que permitan enmascarar estos datos de algún modo sin hacer responsable a la red, sino al perpetuador. Por otro lado, los marcos legales existentes varían mucho de país a país, lo que hacen muy difícil la posibildad de buscar culpables cuando la red atraviesa fronteras. Por último, la GDPR (por sus siglas en inglés: General Data Protection Regulation) dice que es necesario que para cualquier información sensible, el dueño debe de tener la posibilidad de eliminarla, algo que no es posible con la tecnología blockchain. Un uso común en este ámbito es hacer uso de almacenamiento de la información fuera de la cadena de bloques, mientras que en la cadena sólo se almacena el resumen (hash) de esa información para validar que no ha sido corrupta tras su almacenamiento (Lazuashvili, 2019). Este reto es enfrentado en el artículo del compendio (Mezquita, Gil-González, et al., 2022), dónde se diseña un sistema de encriptación de la información que garantiza el anonimato de los usuarios.

El uso de una plataforma descentralizada, cómo pueden ser las redes blockchain, proporcionan seguridad ante ataques tradicionales y evitan la vulnerabilidad denominada *single point of failure* en inglés. Sin embargo, además de los retos ya mencionados, una red blockchain debe proporcionar seguridad ante nuevos tipos de ataques enfocados, específicamente, a controlar las redes blockchain. Algunos de estos ataques se describen a continuación:

- Ataques DDoS (R. Singh, Tanwar, & Sharma, 2020): Un ataque de denegación de servicio distribuido (DDOS por sus siglas en inglés), en informática, es un ataque en el que un perpetrador trata de hacer que un recurso de red no esté disponible para sus usuarios, inundando la red con un gran número de peticiones en un intento de sobrecargar el sistema. Es un ataque que puede sufrir no sólo las plataformas basadas en blockchain, sino cualquier servicio en línea. En el caso de las redes blockchain, utilizan un mecanismo de tarifas con el que cada transacción debe ser pagada, de esta forma no es posible realizar ataques de este estilo a una red pública. En el caso de las redes permisionadas o privadas, que no disponen de este mecanismo de tasas, sólo es posible si el atacante ha conseguido hacerse con la wallet de uno de los usuarios, algo que sólo es posible si el usuario no ha tenido el suficiente cuidado con sus claves.

- Ataques *Sybil* (Calvo & Mathar, 2018): Un ataque *Sybil* es un intento de manipular una red P2P creando múltiples identidades falsas. Para el observador, estas diferentes identidades parecen usuarios normales, pero entre bastidores, una única entidad controla todas estas entidades falsas a la vez. Es importante tener en cuenta este tipo de ataque, especialmente cuando se piensa en las votaciones en línea. Otro ámbito en el que estamos viendo ataques de tipo *Sybil* es en las redes sociales, donde las cuentas falsas pueden influir en el debate público. En el caso de las redes blockchain, se pueden utilizar este tipo de ataques para censurar participantes. Un número de nodos *Sybil* puede rodear otro nodo e impedir que se conecte a los nodos honestos de la red, impidiendo que envíe o reciba información a la red. Este çaso de uso"de un ataque *Sybil* también se llama ataque de Eclipse. Una forma de mitigar los ataques *Sybil* es introducir o aumentar el coste de crear una identidad. Este coste debe ser cuidadosamente equilibrado. Tiene que ser lo suficientemente bajo para que los nuevos participantes no se vean restringidos a la hora de unirse a la red y crear identidades legítimas. También debe ser lo suficientemente alto como para que la creación de un gran número de identidades en un corto período de tiempo sea muy cara. En las redes blockchain basadas en PoW, los nodos que realmente toman decisiones sobre las transacciones son los nodos mineros. La creación de una ïdentidad minera"falsa tiene un coste en el mundo real, a saber, la compra de hardware minero y el consumo de electricidad. Además, tener un gran número de nodos de minería no es suficiente para influir en

la red de forma significativa. Para ello también se necesitan grandes cantidades de potencia de cálculo. Los costes asociados dificultan el ataque *Sybil* a las cadenas de bloques basadas en Proof-of-Work. En redes permisionadas o privadas, este tipo de ataque no se puede realizar ya que los nodos están bien identificados dentro de la red.

- Ataque del 51 % (Kroll, Davey, & Felten, 2013). El tipo de ataque más conocido en las blockchains públicas PoW es el ataque del 51 %. El objetivo de un ataque del 51 % es realizar un gasto doble, lo que significa gastar la misma moneda dos veces. Para realizar un ataque del 51 % en una blockchain, es necesario controlar la mayoría del poder de minado en la red, de ahí el nombre. Un minero malicioso que quiera realizar un doble gasto creará primero una transacción regular gastando sus monedas por un bien o por una moneda diferente en un intercambio. Al mismo tiempo, comenzará a minar una cadena privada. Esto significa que seguirán el protocolo de minería habitual, pero con dos excepciones: i) no incluirán su propia transacción gastando sus monedas en su cadena privada minada y ii) no difundirán los bloques que minen a la red, por lo que la llamamos cadena privada. Si controlan la mayoría del poder de minado, la cadena de los atacantes crecerá más rápido que la cadena honesta. La regla de la cadena más larga en los blockchains PoW rige lo que ocurre en caso de tal bifurcación: la rama que tiene más bloques y, por tanto, representa la cadena creada con una mayor cantidad de potencia de cálculo, se considera la cadena válida. Una vez que el atacante ha recibido el bien u otra moneda comprada con sus monedas, difundirá la rama privada a toda la red. Todos los mineros honestos abandonarán la rama honesta y comenzarán a minar sobre la cadena maliciosa. La red trata la transacción del atacante como si nunca hubiera ocurrido porque el atacante no la incluyó en su cadena maliciosa. El atacante sigue teniendo el control de sus fondos y ahora puede volver a gastarlos. Este tipo de ataques han ocurrido en el pasado en redes públicas que no son lo suficientemente grandes.

2.3. Sistemas distribuidos basados en blockchain, revisión de la literatura

En esta sección vamos a hablar de diferentes ámbitos, tratados a lo largo de la tesis, en los que el uso de la tecnología blockchain tiene el potencial de ayudar a optimizar los procesos llevados a cabo. En cada uno de los apartados, se detallarán, no sólo las bondades que trae el uso de esta tecnología, si no también los problemas que ello acarrea. Además se expondrán los trabajos más relevantes realizados en la literatura por ámbito. La Sección 2.3.1 analiza el ámbito financiero con las criptomonedas como su caso de uso más destacado. La Sección 2.3.2 se centra en las plataformas logísticas donde la tecnología blockchain está muy extendida. La Sección 2.3.3 detalla el potencial uso de esta tecnología en sistemas basados en gobierno electrónico. Por último, la Sección 2.3.4 describe las posibles soluciones en el ámbito de las microrredes eléctrias y el intercambio de energía entre pares.

2.3.1. Finanzas

En el ámbito de las finanzas, la tecnología blockchain se ha utilizado principalmente con el objetivo de democratizar el dinero. Su utilización potencial hace que las reglas de gestión del dinero, como es el caso del Euro o el Dólar, no estén en manos de bancos centrales, si no que estas reglas estén bien definidas y sean conocidas por la comunidad. En este aspecto han aparecido las criptodivisas o criptomonedas, que tienen el potencial para sustituir al dinero fiat[1] en el futuro. Estas no necesitan intermediaros en las transacciones, y tampoco se encuentran en manos de entidades centrales, sino de la comunidad. De ellas han salido diferentes plataformas para satisfacer otros casos, como el intercambio de divisas a través de fronteras de una forma más óptima, cómo el caso de uso de Ripple (Schwartz, Youngs, Britto, et al., 2014).

Debido a la relativa inmadurez de la tecnología blockchain, las criptomonedas se enfrentan a problemas técnicos como la latencia de la red, la gobernanza de la red, la carga de transacciones, etc. Además, aunque la apariencia de una economía verdaderamente democrática es uno de los puntos fuertes del uso de las criptodivisas,

[1]Tipo de dinero que existe por decreto y no tienen una autoridad que lo respalda. Es el dinero que se usa en cada país del mundo, por ejemplo, los Dólares o los Euros son dinero fiat.

también puede convertirse en el mayor problema para su adopción. En ausencia de un organismo que regule las criptodivisas, los usuarios juegan y fomentan las fluctuaciones de su precio, lo que hace que se traten como activos de inversión y no de transacción (Valdeolmillos et al., 2019).

Así, para autores como Fernando Navarro, las criptodivisas son consideradas una excelente vía para el blanqueo de capitales. El autor señala que, según algunos estudios, la subida del mercado en diciembre de 2017 se debió a un movimiento especulativo fruto de un lavado de dinero a gran escala (Cardoso, 2019). Asimismo, Patricia Saldaña señala al Bitcoin como protagonista del blanqueo de capitales a través de la compra de criptodivisas con dinero obtenido de ganancias ilícitas (Taboada, 2017).

Por otro lado, la preocupación por la evasión fiscal ha sido destacada por otro sector de la doctrina. Estudios como los realizados por Rain Xie, Mounteney y García Sigman destacan que, además del blanqueo de capitales, es muy común el uso de estos criptoactivos para transacciones de bienes y servicios ilícitos. El método más habitual es a través de la *Dark Web*, el mercado negro de Internet, para la compra de estupefacientes, armas, o el consumo de pornografía infantil (Lavorgna, 2016; Xie, 2019). García Sigman señala que las criptodivisas están facilitando la compra de estupefacientes en este mercado mayorista en la *Dark Web* (García, 2017).

A pesar de este elevado número de casos, la mayoría de los estados no tienen una amplia regulación sobre el tema, ni siquiera sobre la naturaleza de la criptodivisa. Esto no quiere decir que las criptodivisas no hayan atraído actualmente el interés de los reguladores. Los movimientos de capital que rodean a las criptodivisas han llevado a los gobiernos a preocuparse por los aspectos fiscales y financieros del fenómeno. Sin embargo, ni la falta de regulación ni la vinculación del fenómeno con actos delictivos han supuesto una disminución del desarrollo de las criptomonedas o de la tecnología blockchain que las subyace. Por ello, encontrar el equilibrio adecuado entre la regulación que el fenómeno necesita para garantizar su seguridad jurídica y la flexibilidad ligada a su constante desarrollo es una tarea compleja. Más aún si tenemos en cuenta que el enfoque regulatorio de las criptodivisas varía según el Estado, las organizaciones, o los ámbitos a los que nos refiramos

2.3.2. Plataformas logísticas y sistemas multiagentes

La tecnología blockchain se presenta como una forma de optimizar las plataformas logísticas convencionales. Gracias a la implementación de esta tecnología en los sistemas logísticos es posible ofrecer: i) un menor tiempo de respuesta a la hora de realizar pagos o en momentos en los que aparecen incidencias; ii) confianza al consumidor sobre el origen, condiciones y procesos realizados sobre el producto; iii) facilidad para encontrar responsables sobre hipotéticas malas prácticas que atañen la manufacturación y transporte del producto; iiii) proporcionar seguridad ante ataques de spoofing, o DDoS, ya que la comunicación entre sensores va a ir firmada con las claves proporcionadas por sus identidades en la blockchain, y la se elemina la vulnerabilidad de *single-point-of-failure* al convertirse en un sistema distribuido.

Una de las tecnologías más usadas para la optmización de las plataformas logísticas es implementarlas con sistemas multiagente. Un sistema multiagente es un sistema informático compuesto por múltiples agentes inteligentes que interactúan entre sí. Los sistemas multiagente se utilizan para resolver problemas complejos y consiguen muy buenos resultados (Francisco et al., 2019). Los sistemas multiagente se utilizan en una amplia gama de aplicaciones. (Gazafroudi et al., 2017) presenta un sistema multiagente para el uso inteligente de la electricidad en una casa inteligente y, por tanto, un aumento de su eficiencia energética.

La aplicación de un sistema multiagente a la industria logística no es una idea nueva, en (K. Li, Zhou, Liu, & Li, 2018) se propone un sistema multiagente para dar solución al problema logístico. Además, otra aplicación exitosa de los sistemas multiagente es el problema de la computación distribuida Banerjee & Hecker (2017), así como el control predictivo de modelos distribuidos en la industria química Francisco et al. (2019).

De entre una serie de sistemas que integran blockchain y sistemas multiagente destaca el trabajo de (Aitzhan & Svetinovic, 2016). Este trabajo propone el uso de ambas tecnologías para aumentar la seguridad y la privacidad en redes energéticas descentralizadas. En Yuan & Wang (2016) los autores proponen un modelo que emplea agentes y blockchain para un sistema de transporte compartido.

Además, hay otras aplicaciones de blockchain y sistemas multiagente, como (Daza et al., 2017), en el que los autores proponen un modelo innovador de blockchain para

plataformas IoT. En (Mezquita, González-Briones, et al., 2019) se propone un sistema multiagente basado en blockchain, que simula el seguimiento de activos agroalimentarios en una cadena de suministro agroalimentaria. Se han utilizado contratos inteligentes y dispositivos sellados para asegurarse de que los datos almacenados en la blockchain son de confianza.

En base al estudio de la literatura, se puede extraer que la tecnología blockchain en este ámbito se utiliza como: (i) histórico de datos inmutable en el que se almacenan las diferentes etapas y transformaciones de los productos transportados, (ii) tablón informativo al que los consumidores pueden acudir para conocer la procedencia de un producto, y (iii) plataforma de pagos en la que el dinero entre las partes fluye automáticamente una vez la transacción de los bienes se ha confirmado.

A pesar de todas las bondades listadas, existen ciertos retos que se deben tener en cuenta a la hora de implementar la tecnología blockchain en los sistemas logísticos. Para empezar, es necesario hacer uso de una red, lo suficientemente resiliente como para soportar ataques, tanto internos como externos. Por otro lado, es necesario implementar un sistema de auditorías para probar que los datos utilizados en las comunicaciones pueden ser confiables y no se tratan de un fallo en el sistema o un intento de manipulación. De los modelos estudiados no se tienen en cuenta todas problemas que se plantean en este escenario, incentivo suficiente para investigar sobre este ámbito en la presente tesis.

2.3.3. Plataformas de gobierno electrónico

Para lograr plenamente la automatización y distribución de los procesos en el ámbito registral, los gobiernos electrónicos deben dotar a sus sistemas y procesos de un registro único, transparente, e inmutable con el que los ciudadanos se sientan seguros y tranquilos al hacer uso de las funcionalidades ofertadas por los gobiernos. Esta definición concuerda con la de la tecnología blockchain, siendo esta un potencial candidato para permitir el desarrollo e implementación de los gobiernos electrónicos del futuro. Aunque el uso de esta tecnología no eliminará completamente los intermediarios, sí que se ha podido demostrar cómo puede optimizar procesos como el registral (Mezquita, Parra, et al., 2019). Gracias a la implementación de esta tecnología en los procesos ofertados por los gobiernos electrónicos, es posible democratizar el acceso a los datos, lo que conlleva la

eliminación de la corrupción, la reducción del coste debido a la eliminación de algunos intemediarios humanos, junto a la mejoría de los tiempos en los que se ejecutan los servicios gracias a la parcial automatización. En este ámbito, hay que prestar especial atención a la forma en la que se hace uso de esta tecnología, ya que de un modo incorrecto, lo que sería una solución a la corrupción, puede simplemente ser una fachada de falsa sensación de seguridad (Lazuashvili, Norta, & Draheim, 2019).

Desde 2017, más de la mitad de los hogares de los países en desarrollo tienen acceso a Internet, por lo que es real la viabilidad de este tipo de sistemas de adopción de la administración electrónica (Mavilia & Pisani, 2019). En África, por ejemplo, encontramos el caso de Ghana. En países como este, menos desarrollados y donde la situación política es bastante inestable, no es extraño que se den casos de corrupción en cuanto a la propiedad de los ciudadanos. En este tipo de situaciones, donde los índices de corrupción del gobierno son muy altos, los funcionarios públicos alteran los títulos de las propiedades registradas asignándolas a otros o a ellos mismos. En el caso de los países en desarrollo, otro factor que refuerza este problema es el hecho de que los ciudadanos no tienen fácil acceso a la información. Aunque no se trata sólo de una cuestión de acceso a la información, también es un reto para el país africano, ya que alrededor del 90 % de la tierra no está registrada oficialmente (Kshetri & Voas, 2018). Ghana es uno de los países que ha impulsado y se ha sumado al proyecto blockchain junto a empresas multinacionales que llevan años trabajando en el sector del blockchain, junto a startups locales que conocen el área y los posibles inconvenientes que pueden existir. En el caso de Ghana, están trabajando de la mano de IBM y Bitland (Cano, 2017) para modernizar y hacer inmutable el registro de la propiedad. Utilizan *OpenLedger* para crear una blockchain pública distribuida, a la que se espera que se conecten más empresas con el tiempo.

La tecnología blockchain también está empezando a aplicarse a nivel gubernamental en Asia. En particular, en Japón, que está viendo la viabilidad y las implicaciones del uso de esta tecnología. El gobierno de Japón está desarrollando proyectos sobre los usos de la tecnología blockchain para el registro de la propiedad y la gestión y unificación de todos los procedimientos relacionados con el registro de la propiedad (Lemieux, 2017). La intención de utilizar la tecnología blockchain en Japón es unificar todos los datos sobre las propiedades vacías o sin dueño, los terrenos y espacios improductivos, los propietarios desconocidos y los inquilinos o usuarios no identificados ante los organismos.

La consolidación de estos datos y su disponibilidad para todos los organismos pertinentes a través de la blockchain contribuyen al avance de varios objetivos nacionales, como: fomentar la reutilización del suelo, promover la compraventa, controlar la reurbanización, optimizar la recaudación de impuestos y diseñar planes relacionados con el medio ambiente. Aunque no hay más información sobre las pruebas realizadas en diferentes ciudades japonesas desde el verano de 2018, se espera que cubra todo Japón en 2022 (Finch, 2019).

En el contexto de Suecia, los bancos y las autoridades estatales tienen acceso a la base de datos del registro de la propiedad, mientras que el vendedor y el comprador, los actores más importantes de una transacción de tierras, no tienen ese privilegio. Por ello, el Gobierno pretende implantar un sistema de registro de la propiedad basado en blockchain, en el que todos los actores de una transacción tengan los mismos privilegios (McMurren, Young, & Verhulst, 2018). Sin embargo, para poder llevar a cabo el cambio en el acceso registral en los ámbitos legales y en el registro de todas sus propiedades (Lazuashvili, 2019), debe haber una modificación legal. En junio de 2016, el sistema de regulación sueco de la propiedad publicó un informe bajo el título "The Land Registry Blockchain". Formaba parte de un proyecto sobre las posibilidades de utilizar blockchain como solución técnica para las transacciones inmobiliarias. El proyecto se centraba en el proceso de contratación porque actualmente, y según su ordenamiento jurídico, consta de dos pasos: un contrato de venta y una escritura de venta (el primero puede registrarse como venta pendiente y el segundo como venta final). En su estado actual, el proceso desde la firma de un contrato hasta el registro de la escritura de compraventa dura entre tres y seis meses. Aun así, en el proceso de firma, muchos documentos se firman en papel y se envían por correo ordinario, por lo que las firmas e identificaciones digitales serán un componente del proyecto (que requiere inversión en tiempo y dinero). Las actualizaciones en el Registro de la Propiedad deben ser comprobadas por la autoridad reguladora y, en una solución a largo plazo, el Registro de la Propiedad seguirá siendo el encargado de hacer cumplir la ley. El objetivo final es que, con el uso de una blockchain permisionada en su prueba de concepto, el proceso de adición de información se centralice en el Estado, sin dejar de ofrecer un alto nivel de transparencia. En este caso, la blockchain se llama *permisionada* porque sólo un número limitado de actores, de la agencia de registro, puede aprobar los bloques de datos que se van a almacenar en la blockchain. Además, esta blockchain es abierta porque todos los ciudadanos suecos tienen acceso a la información

almacenada en ella. El proyecto sueco es un ejemplo de Blockchain como tecnología adaptada al registro, no como una nueva categoría de registro de la propiedad, sino como una modernización y adaptación de las nuevas tecnologías hacia la eficiencia jurídica.

Por otro lado, Georgia es un país que ha iniciado un proyecto de creación de un sistema de registro de la propiedad basado en la tecnología blockchain en 2016 y, desde entonces, la Agencia Nacional de Registro Público sigue actuando como tercero ejecutor (Shang & Price, 2019). En la actualidad, los títulos pueden emitirse en formato digital y registrarse utilizando la tecnología blockchain. Sin embargo, el proceso no está totalmente automatizado, los interesados tienen que ir a las oficinas del gobierno para obtener el certificado de la tierra antes de hacer una transacción con ella. Además, la tecnología de cadena de bloques utilizada es sólo una capa de seguridad a prueba de manipulaciones haciendo uso de la blockchain de Bitcoin, utilizada por el gobierno. Esto significa que el proceso sigue siendo centralizado por el gobierno y no es un proceso automático (Lazuashvili et al., 2019). En este caso se ha propuesto un registro de la propiedad en blockchain como solución para los estados con déficit institucional, ya que se cree que se puede emitir un certificado de "propiedad" de bajo coste desde un ordenador. Sin embargo, un "derecho real", efectivo contra toda ley, necesita una infraestructura institucional que lo proteja. Sin instituciones legales no hay "derecho real" ni propiedad, sino expectativas, normas sociales, hechos o posesión. Si el propietario no puede acudir a los tribunales para reclamar o defender su derecho, su existencia es dudosa. En el caso de Georgia, su marco legislativo permite la aplicación de este tipo de soluciones, ya que cuenta con la suficiente flexibilidad como para permitir al gobierno almacenar los datos de sus ciudadanos (Lazuashvili et al., 2019).

En resumen, el uso de la tecnología blockchain como sistema de almacenamiento en el que la información generada, junto con los contratos inteligentes que contienen la lógica para gobernar la plataforma, se almacenan en una base de datos distribuida, lo que permite a los gobiernos crear un libro mayor de transacciones público y transparente para todos los ciudadanos y un mecanismo anticorrupción probado. Además, el uso de firmas digitales en el protocolo de comunicación y una huella digital de los datos con sello de tiempo, obtenida con un algoritmo de hashing, como mecanismo de validación de la información, son herramientas muy potentes para preservar el tipo de archivos generados en los sistemas de registro de la propiedad. Además, el uso de una red de nodos como guardián de la información facilita su recuperación en cualquier circunstancia, al

eliminar el punto único de fallo de los sistemas centralizados. Sin embargo, se puede concluir que el marco legal de un país es un gran obstáculo a la hora de tratar de automatizar completamente cualquier plataforma donde sus usuarios tienen una gran disparidad de intereses. Por ello, es necesaria una legislación que ampare el uso de los contratos inteligentes y que proteja los derechos de los ciudadanos que los utilizan en caso de que se produzca un fallo. Por otro lado, con el auge de las regulaciones que pretenden proteger la privacidad de los usuarios, cualquier solución basada en blockchain debe encontrar la forma de ocultar esos datos, al tiempo que permite su verificación.

2.3.4. Microredes de energía inteligentes

La importancia del uso de la tecnolgoía blockchain en los sistemas de microredes de energía inteligentes radica en que permiten un mercado energético entre pares, automático, y descentralizado. De forma análoga a lo que ocurre con las criptomonedas, el uso de esta tecnología permite transaccionar energía entre agentes autónomos que pueden negociar entre sí con activos reales digitalizados, por ejemplo, energía y divisas tokenizadas. Sin embargo, en la literatura no se han explotado completamente estas posibilidades, ya que hay que hacer frente a retos como: i) la anonimicidad de los usuarios, ii) la ocultación de las actividades realizadas, iii) la gobernanza de la red de nodos.

En la literatura, encontramos algunos trabajos que discuten el uso de plataformas de microrredes basadas en blockchain para crear mercados energéticos, centrándose en características específicas como el uso de criptomonedas, la descentralización, la seguridad, la privacidad y las estimaciones de estado (Aitzhan & Svetinovic, 2018; Dorri, Kanhere, Jurdak, & Gauravaram, 2017; Imbault, Swiatek, De Beaufort, & Plana, 2017; Mengelkamp et al., 2018; Pop et al., 2018).

Pichler et al. en (Pichler et al., 2018) estudiaron casos de uso en el mundo real de plataformas basadas en la tecnología blockchain y cuyo objetivo era permitir el intercambio directo de energía entre sus actores. Las plataformas estudiadas tienen un objetivo común general: crear mercados locales basados en comunidades de energía renovable. Sin embargo, comparten los mismos contras: no intentan crear un mercado autónomo y no ofrecen un anonimato y privacidad reales a sus usuarios (véase la tabla 2.3).

Un ejemplo que funciona es la red Pylon (network, 2018), una startup española que hace uso de la tecnología Litecoin basada en una red blockchain permisionada, combinada con un contador inteligente para certificar los flujos de energía y permitir las transacciones virtuales con el uso de su propio token. Utiliza un algoritmo de consenso *Proof of Cooperation* (PoC), y su principal objetivo es crear una base de datos neutral, que no esté gobernada por las empresas que venden la energía, para ayudar al usuario a decidir cómo optimizar los costes energéticos. Hicieron su plataforma de código abierto para recibir ayuda de la comunidad en caso de que se necesite algún tipo de mejora para su red. En Eslovenia, SunContract (Suncontract, 2017) ha creado un mercado de transacciones entre pares de energía basado en BT. Hacen uso de un criptoactivo dentro de la red Ethereum para utilizarlo en el intercambio de energía entre las entidades que participan en la plataforma.

Por otro lado, está Enosi (Enosi, 2018), una empresa australiana cuyo objetivo es similar al de SunContract: crear una comunidad de pares que intercambien energía directamente entre ellos. Mediante el uso de contadores inteligentes, rastrean, igualan y liquidan la producción y el consumo de energía. Gracias a la plataforma, los productores pueden ofrecer directamente un precio al consumidor final, con precios más baratos en lugar de los artificiales que tienen los oligopolios energéticos en el mercado tradicional.

En el caso de la microrred de Brooklyn (Goranović et al., 2017), LO3 desarrolló los elementos de la red transactiva (TAG-e), que permiten el intercambio de energía entre pares, el equilibrio de la red o la gestión de emergencias de la misma. Un TAG-e se compone de dos elementos: un contador eléctrico y un ordenador. Su función es leer la información sobre el estado de la red y compartirla con otros TAG-e para actuar sobre la información recogida. El mercado creado con esta plataforma permite el comercio de energía entre pares con precios fijos; sin embargo, las negociaciones automáticas dentro de él no están permitidas.

En base al estudio de la literatura, se puede extraer que la tecnología blockchain en el ámbito de la administración electrónica se utiliza como: (i) histórico de datos inmutable en el que se almacenan las ofertas de energía que existen en la plataforma, (ii) tabla de información a la que acuden los consumidores para seleccionar qué ofertas comprar, y (iii) plataforma de pagos en la que el dinero fluye una vez se ha recibido la energía por parte de los compradores.

Tabla 2.3: Comparación de las startups estudiadas.

Proyecto	**Descripción**	**Pros**	**Cons**
Pylon Network (network, 2018)	El objetivo principal es crear una base de datos neutral. Hace uso de su tecnología Litecoin basada en la cadena de bloques autorizada. Hace uso de un algoritmo de consenso Proof of Cooperation (PoC). Además, un contador inteligente (METRON) certifica los flujos de energía y permite las transacciones virtuales utilizando su propio token.	· Código abierto · Escalable · Latencia · Mejora precios	· Nada sobre la privacidad de los usuarios · No está diseñada para crear un mercado autónomo y automático
SunContract (Suncontract, 2017)	El objetivo principal es crear un mercado que permita a los clientes comerciar con energía sin necesidad de intermediarios. Gestionan un mercado de transacciones energéticas P2P basado en BT desde hace más de 2 años. Permiten realizar transacciones virtuales de energía utilizando su propio token.	· Escalable · Latencia · Mejora precios	· Nada sobre la privacidad de los usuarios · No está diseñada para crear un mercado autónomo y automático
Enosi (Enosi, 2018)	Su principal objetivo es crear un mercado que permita a los clientes de energía comerciar con ella sin necesidad de intermediarios. Certifican los flujos de energía a través de contadores inteligentes.	· Escalable · Latencia · Mejora precios	· Nada sobre la privacidad de los usuarios · No está diseñada para crear un mercado autónomo y automático
Brooklyn Micro-grid Network (Goranović et al., 2017)	Este proyecto creó un mercado local de energía en Brooklyn. Gracias a este proyecto, los prosumidores pueden intercambiar su excedente de energía con sus vecinos.	· Escalable · Latencia · Mejora precios	· Nada sobre la privacidad de los usuarios · No está diseñada para crear un mercado autónomo y automático

2.4. Conclusiones

Este Capítulo ha presentado un análisis del Estado del Arte de la tecnología blockchain en los diferentes entornos industriales tratados durante la tesis: las plataformas y arquitecturas propuestas en el pasado, los retos acaecidos del uso y aplicación de la tecnología blockchain a los sistemas tradicionales, y cómo están tratando de hacerles frente. Por último, la subsección 2.3.3 ha mostrado las conclusiones referentes a la necesidad de buscar nuevos enfoques a la hora de enfrentar los desafíos aparecidos. Entre las conclusiones extraídas podemos destacar las siguientes:

- **La tecnología blockchain se presenta como una tecnología habilitante clave en la optimización y democratización de muchos de los procesos industriales actuales**. Dentro del ecosistema de tecnologías para la Industria 4.0, la tecnología blockchain se puede utilizar en combinación con otras tecnologías, como el IoT y los sistemas multiagente, para eliminar intermediarios que no aportan valor a diferentes productos de la industria, cómo pueden ser la trazabilidad de los bienes en las plataformas logísticas, la implementación de un sistema de administración electrónica libre de corrupción, o la aparición de mercados de energía automáticos entre dispositivos. Sin embargo, es necesario hacer frente a diferentes retos, tanto de origen tecnológico (por ejemplo la escalabilidad del sistema, o el gobierno de la red distribuida), como de origen socioadministrativo (por ejemplo, una regulación actualizada sobre este tipo de sistemas para amparar al consumidor y resolver conflictos, o el almacenamiento y tratamiento de los datos sensibles de los usuarios).

  En este sentido, la Sección 3.1 describe el planteamiento del problema a resolver en relación a las necesidades básicas que este tipo de sistemas debe proveer para optimizar de forma real las plataformas tradicionales de la industria actual.

- **La tecnología blockchain permite eliminar intermediarios que no aportan valor en cualquier tipo de cadena de suministro, además de agilizar los procesos de intercambio de vienes entre partes, y los pagos asociados**. En comparación al modelo tradicional, en el que existen intermediarios que no aportan un valor real al producto final, pero que sí encarecen el precio, el uso de la tecnología blockchain, y en especial los contratos inteligentes que se pueden

implementar en ella, se puede rastrear, de forma confiable, cualquier producto en este tipo de sistemas, identificando los intermediarios que sólo encarecen el precio sin aportaciones reales al producto final. Por otro lado, gracias a estos mismos contratos inteligentes, es posible realizar pagos instantáneos, una vez se ha verificado la recepción del producto, además de identificar y castigar, de forma automática, a aquellos intermediarios que no han cumplido con su parte del contrato.

Alineada con esta conclusión, la Sección 3.2 presenta el despliegue de un modelo teórico para este tipo de sistemas, en él se han podido identificar los principales retos que propone el uso de la tecnología blockchain en cualquier plataforma de este estilo. Gracias a ello, se proponen soluciones que permitirán hacer frente a dichos retos y desplegar este tipo de sistemas en un entorno real.

- Aunque **la tecnología blockchain tiene el potencial para eliminar la corrupción dentro de los gobiernos y la administración pública** no son pocos los problemas que hay que tener en cuenta a la hora de aplicar esta tecnología en estos entornos.

  A este respecto, la Sección 2.3.3 ha presentado un estudio sobre cómo diferentes países están presentando su propia versión de aplicación de esta tecnología a la administración pública, en concreto el registro de la propiedad.

- **La aplicación de tecnología blcockhain a determinados mercados, permite su automatización y optimización**, no sólo en lo referente a la eliminación de la necesidad de un supervisor humano, sino a la optimización de las negociaciones por parte de los diferentes agentes de la plataforma, lo que tiene el potencial de mejorar las ganancias y el bienestar global de las plataformas y usuarios implicados.

  En relación con este punto, la Sección 3.3 presenta el diseño de una plataforma que enfrenta los retos identificados a lo largo de esta Tesis Doctoral, y permite el intercambio local de energía, con negociaciones autónomas gracias a la aplicación de la tecnología blockchain y el uso de contratos inteligentes.

Para hacer frente a lo anterior, el siguiente Capítulo, Capítulo 3, recopila las contribuciones de esta Tesis Doctoral, donde se plantean posibles soluciones a los retos

que aparecen al implementar la tecnología blockchain en la industria actual, obtenidos de las conclusiones extraídas durante este Capítulo.

Capítulo 3

Contribuciones

VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

Capítulo 3

Contribuciones

Desde hace algunos años, la tecnología blockchain va ganando fuerza en el mundo industrial. En la actualidad, su caso de uso más conocido, las criptomonedas, han conseguido aumentar el flujo de capital en su mercado a los 221 mil millones de dólares en 2020.[1] Este éxito en el campo de las finanzas descentralizadas (o *Defi* por sus siglas en inglés de Decentralized Finances) ha conseguido que la tecnología gane popularidad entre la comunidad investigadora y se vea potencial para disruptir la industria tradicional actual. Hoy día, ya existen proyectos en los que se está trabajando para adaptar esta tecnología a ámbitos como las cadenas de suministro (Mezquita, Casado-Vara, et al., 2021; Mezquita, González-Briones, et al., 2019), los mercados energéticos (Aitzhan & Svetinovic, 2016; Mezquita, Gil-González, et al., 2022), sistemas de transporte compartido de vehículos (Yuan & Wang, 2016), o la administración electrónica (Mezquita, Parra, et al., 2019; Yildiz, 2007). Gracias al uso de protocolos de consenso en redes de nodos distribuidas y controlados por entidades con intereses dispares, se consigue obtener una democratización en los procesos industrialesmencionados. Estos, tradicionalmente gobernados por una entidad central encargada del mantenimiento y buen funcionamiento de la plataforma, pasan ahora a ser gobernados por los participantes de la red (Mezquita, Casado, et al., 2019). Gracias a que esta tecnología permite el despliegue de contratos inteligentes, autogestionados, hace que la gestión del ciclo de vida de estas plataformas ya no sea necesaria la participación de terceros que deban mediar entre las partes (Mezquita, Valdeolmillos, et al., 2019).

En este Capítulo se describen de forma detallada las contribuciones resultado de las investigaciones llevadas a cabo en esta Tesis Doctoral. En primer lugar, se llevará a cabo una descripción de la problemática a resolver y que conforma en gran medida

[1] Datos obtenidos de la capitalización total del criptomercado en tiempo real a través de www.tradingview.com. Fecha de acceso 9 de junio 9, 2020

la motivación del trabajo de investigación presentado en este Tesis Doctoral. Dicha motivación y la formulación final del problema son el resultado de investigaciones previas realizadas en el ámbito de la tecnología blockchain, y sus aplicaciones a sistemas basados en IoT (Mezquita, Casado, et al., 2019; Mezquita, González-Briones, et al., 2019; Mezquita, Valdeolmillos, et al., 2019; Valdeolmillos et al., 2019). Además, se procederá a detallar las bases de esta Tesis Doctoral, sentadas gracias a los mencionados trabajos de investigación que se realizarón al principio de la misma. Estas bases empezaron por adquirir una profunda comprensión de lo que está pasando entorno a la tecnología blockchain, empezando por su caso de uso más exitoso: las cryptomonedas (Valdeolmillos et al., 2019). Seguidamente se prosiguió a estudiar y recopilar información acerca de los contratos inteligentes y su viabilidad real dentro de un marco regulatorio como el español (Mezquita, Valdeolmillos, et al., 2019). Tras ello, le siguió una investigación sobre qué requisitos son necesarios para poder hacer uso de la tecnología blockchain dentro de una plataforma IoT (Mezquita, Casado, et al., 2019). Una vez estudiados estos pilares clave para proseguir la Tesis Doctoral en el ámbito de la tecnología blockchain, se proporcionó una arquitectura basada en un sistema multiagente para el control de las actividades logísticas, tomando la industria alimentaria como caso de uso (Mezquita, González-Briones, et al., 2019), y siendo el precursor de la primera de las arquitecturas propuestas en el compendio de artículos.

Posteriormente, y como resultado del conocimiento adquirido a partir de las anteriores investigaciones, y en la revisión del estado del arte, expuesta en el Capítulo 2 y publicada por varios de los artículos ya descritos, aunque principalmente por el publicado en Mezquita, Parra-Domínguez, et al. (2022), se detallan las **dos contribuciones más importantes de esta Tesis Doctoral** (Mezquita, Casado-Vara, et al., 2021; Mezquita, Gil-González, et al., 2022):

- El diseño de un modelo para la trazabilidad de bienes en la industria farmacéutica, haciendo uso de contratos inteligentes y teoría de juegos para la penalización de las entidades del sistema que no cumplen con sus cometidos. En este modelo se hace frente a todos los retos que se han identificado hasta la fecha, mayormente de tipo tecnológico, y que supone una mejora del modelo propuesto en (Mezquita, González-Briones, et al., 2019).

- El diseño de una plataforma de negociación e intercambio de energía dentro del ámbito de las microrredes. Siendo este sistema la culminación de la Tesis Doctoral, en la que se tienen encuenta aspectos, no sólo de ámbito tecnológico, si no también regulatorio, con el fin de adaptar estas plataformas a los marcos legislativos actuales de la Unión Europea.

El resto del Capítulo está estructurado de la siguiente manera. La Sección 3.1 describe el planteamiento del problema, así como las investigaciones previas que han contribuido a su formulación. La Sección 3.2 detalla la arquitectura diseñada para implementar en las cadenas logísticas de la industria farmacéutica la tecnología blochchain. La Sección 3.3 expone, de una manera pormenorizada, los avances realizados respecto a la anterior arquitectura, en un escenario desafiante cómo el de la creación de un mercado automático de energía. La Sección 3.4, finalmente, expone las principales conclusiones extraídas a partir de las contribuciones llevadas a cabo.

3.1. Descripción del problema

El mundo interconectado en el que vivimos genera información de la que podemos extraer conocimientos a partir del uso de objetos cotidianos. Al colocar sensores y actuadores en esos objetos, estos envían y reciben datos a través de Internet y les permiten interactuar con su entorno sin necesidad de la intervención humana. El concepto utilizado para definir esta red de dispositivos que interconectan el mundo real con el virtual es el de *Internet de las Cosas* (Chamoso, González-Briones, Rodríguez, & Corchado, 2018). Al dotar a los objetos cotidianos de la capacidad de medir casi cualquier fenómeno del mundo real, gracias a la instalación de sensores, podemos extraer conocimiento de los datos generados. Con ese conocimiento, podemos predecir algunos eventos y llevar a cabo acciones preventivas. Además, si instalamos actuadores en estos objetos, conseguimos una mayor capacidad de maniobra al conseguir una reacción automática y que los propios objetos se comuniquen entre sí y operen en su entorno. Todo ello se basa en mediciones y/o predicciones realizadas previamente de forma automática (Francisco et al., 2019).

La mejora de la capacidad de respuesta que ofrece el IoT hace que este concepto sea muy popular en temas de optimización de recursos, muy demandados en la industria actual, debido a su ahorro de costes (*Smart Grids* (Gazafroudi, Afshar, & Bigdeli, 2015), *Smart*

Home (González-Briones, Chamoso, De La Prieta, Demazeau, & Corchado, 2018), *Smart Farming* (González-Briones, Castellanos-Garzón, et al., 2018), *Smart Cities* (Briones et al., 2018)). Además, este tipo de plataformas pueden ser utilizadas en la automatización de servicios que mejoren la experiencia del usuario, dándole más información para mejorar sus decisiones (*Smart Supply Chain* (Christopher, 2016), *Connected Health* (Kvedar, Coye, & Everett, 2014)). Aunque estas posibilidades hacen muy atractivo el uso de las plataformas de IoT, también se enfrentan a muchos retos: la privacidad es una preocupación creciente, ya que las empresas tienen cada vez más acceso a la información sobre nuestra vida cotidiana, y la seguridad de los dispositivos, que, debido al continuo intercambio de información entre ellos a través de Internet, se vuelven vulnerables a los ataques que ponen en peligro la integridad y origen de los datos (Lin & Bergmann, 2016).

Debido a los problemas de las plataformas IoT que se han mencionado, autores en la literatura como (Khan & Salah, 2018), proponen el uso de la tecnología blockchain para asegurar el intercambio de datos en estas plataformas y obtener sistemas de trazabilidad fiables. Aunque, cada vez hay más trabajos sobre diferentes casos de uso que contemplan su aplicación (Mezquita, Casado, et al., 2019), la mayoría de las arquitecturas propuestas en la literatura no hacen una descripción exhaustiva de cómo han conseguido superar los defectos de la tecnología blockchain a la hora de implementarla en este tipo de plataformas, siendo el trabajo publicado por Yue, Wang, Jin, Li, & Jiang (2016) un ejemplo de ello.

Sin embargo, aunque la tecnología blockchain se presenta como una solución a los sistemas IoT, y por ende, a la industrua actual basada en este paradigma, aparecen también una serie de problemas que se describen a continuación:

- **Capacidad de almacenamiento y escalabilidad**. A medida que pasa el tiempo, y se realizan más transacciones dentro del sistema, los nodos necesitan más recursos para almacenarlas, ya que la cantidad de datos generados crece continuamente. Una de las posibles soluciones utilizadas por algunas cadenas de bloques como Bitcoin, es hacer uso de diferentes tipos de nodos con diferentes funcionalidades en la red, por ejemplo, nodos completos que tienen la cadena completa de bloques y se encargan de los procesos de verificación, enrutamiento y minería; y nodos ligeros, que almacenan sólo una parte del historial de transacciones realizadas en

la plataforma, cuyo único objetivo es proporcionar los datos a los usuarios que lo soliciten (Palai, Vora, & Shah, 2018). En cuanto al problema de la escalabilidad de la red, depende del protocolo de consenso utilizado, véase la Tabla 3.1. Es posible utilizar una red blockchain pública como servicio para garantizar que la tecnología tenga una seguridad probada (Mezquita, Gazafroudi, et al., 2019). En este escenario, los factores limitantes provienen del tiempo que necesita la red pública para procesar las peticiones de la plataforma IoT; otro factor es el coste de almacenamiento de las transacciones realizadas. Una alternativa es hacer uso de una blockchain permisionada, desplegando su red dentro del sistema IoT. Los nodos de este tipo de plataformas deben ser conocidos, por lo que tienen un Identificador Único Global (GUID por sus siglas en inglés: *Global Unique Identifier*) con un rol determinado en la plataforma. Para estos sistemas, los protocolos considerados más rápidos son los basados en algoritmos de consenso Bizantino tolerantes a fallos (BFT por sus siglas en inglés) (Vukolić, 2015), dando una latencia casi de velocidad de red para la confirmación de transacciones (Bessani, Sousa, & Alchieri, 2014). Uno de los problemas de los algoritmos de consenso BFT, es que se pueden explotar sus estampas de tiempo y ser vulnerables a los ataques DDoS (Miller, Xia, Croman, Shi, & Song, 2016). Por esta razón, una solución preferible es utilizar otro tipo de protocolo de consenso, como por ejemplo Proof of Stake (PoS) o una de las variantes descritas en Bentov, Gabizon, & Mizrahi (2016). Este tipo de algoritmos de consenso son mucho más rápidos que las soluciones PoW, aunque existe la teoría del"*nothing at stake*", que afirma que estos algoritmos pueden sufrir por la creación de un gran número de bifurcaciones debido al proceso de validación al añadir nuevos bloques (Martinez, 2018). Existe otra alternativa al concepto común de blockchain, diseñada para su uso en plataformas IoT: El Tangle (Popov, 2018). El Tangle es un grafo acíclico dirigido (DAG por sus siglas en inglés) que almacena las transacciones en bloques vinculados a dos anteriores, a diferencia de los bloques de cualquier blockchain que están vinculados linealmente. Para almacenar una nueva transacción en el DAG, el que quiere añadirla tiene que encontrar si dos transacciones anteriores en el borde del Tangle, están en conflicto con la historia del tangle. Este mecanismo de consenso permitiría que el DAG fuera ejecutado por los dispositivos de borde de una plataforma IoT sin un gran gasto de energía. Realizar una nueva transacción ayuda a validar dos anteriores, por lo que este tipo

de sistemas será escalable por naturaleza, permitiendo que el Tangle crezca más rápido a medida que se realicen más transacciones entre dispositivos.

Tabla 3.1: Tabla comparativa sobre escalabilidad en diferentes tecnologías de algoritmos de consenso.

Algoritmo de Consenso	**Capacidad de escalar**	**Principal uso**
PoW	Baja	Redes públicas en las que sea necesaria un alto nivel de seguridad.
PoS	Moderada	Redes públicas, aunque, aunque existe la teoría del"*nothing at stake*", poniendo en riesgo su integridad.
PBFT	Alta	Redes primadas o permisionadas donde los nodos son conocidos y se puede tener cierto nivel de confianza.

- **Seguridad**. Algunos expertos recomiendan el uso de blockchain para proporcionar una capa de seguridad en cualquier plataforma de IoT (Dorri et al., 2017). La cadena de bloques puede confirmar que los datos almacenados en ella proceden de los dispositivos IoT de los que dicen proceder. El problema viene, como se explicó en la Sección 2.2.5, cuando esas fuentes envían datos corruptos, debido al vandalismo, un cortocircuito, la desconexión, el clima, etc. Las fuentes de datos corruptos no siempre son maliciosas de forma intencionada, pero si los datos corruptos se almacenan en la cadena de bloques, quedarán almacenados en ese estado para siempre. Debido a este escenario, tenemos que probar a fondo los dispositivos IoT antes de que se instalen en el sistema y se conecten a una cadena de bloques. Además, tienen que estar sellados para evitar que el software se modifique y que los sensores conectados a él queden expuestos y se deterioren. Por último, para hacer viable una plataforma como ésta, es necesario auditar periódicamente este tipo de dispositivos IoT (Liang et al., 2017). Una plataforma basada en blockchain hace que la comunicación para compartir información entre dispositivos sea inviolable. Al dar a cada dispositivo un GUID, actúan como pares y sólo tienen que firmar y cifrar la información con su clave privada, lo que permite a la cadena de bloques saber que la información que recibe procede de la fuente que realmente la ha firmado y de nadie más. Gracias a esto y a su propiedad a prueba de manipulaciones por diseño, el sistema puede tener tanto la máxima capacidad a prueba de hackeos como de engaños. Por último, hay que tener en cuenta que una red blockchain, que no sea lo suficientemente grande, y no tenga un mecanismo de filtrado de peticiones, puede

ser víctima de un ataque DDoS, cómo se explicó previamente en la Sección 2.2.5. En relación a otro tipos de ataques, es muy difícil que se produzcan en entornos privados o permisionados, a menos que el atacante gane completo control sobre la mayoría de nodos del sistema.

- **Anonimato y privacidad de los datos**. Para proteger algunos datos sensibles y privados de los usuarios de una plataforma IoT, se puede utilizar el mecanismo de clave pública de la tecnología blockchain para cifrarlos. Este mecanismo puede utilizarse desde el exterior de los dispositivos al llamar a los servicios proporcionados por una red de blockchain, o puede desplegarse en el dispositivo implementando el protocolo de seguridad dentro de él, véase Tabla 3.2. El tiempo de respuesta de la primera posibilidad depende de la latencia de la red, mientras que la segunda depende de las características del dispositivo. Para agilizar este proceso, es posible integrar un hardware criptográfico de seguridad en el dispositivo (A. Singh, Chawla, Ko, Kar, & Mukhopadhyay, 2018). Gracias a este hardware, el proceso de cifrado y firma es más rápido y menos costoso computacionalmente, lo que permite a los dispositivos típicos de IoT hacer uso de este mecanismo criptográfico sin depender de la latencia de la red.

Tabla 3.2: Tabla comparativa de los tiempos de encriptación utilizando diferentes métodos.

Método de encriptación	**Requisitos**
Desde una red blockchain	Se considera una petición a un servicio en la nube, por lo que depende principalmente de la carga de trabajo que tenga la blockchain en ese momento y de la latencia de red.
Desde el propio dispositivo	Se requiere hardware específico, o será un proceso lento.

- **Contratos inteligentes**. Uno de los problemas de este tipo de programas es que el código se distribuye sólo para ser verificado, no para compartir las tareas y ganar poder computacional. Esta es una limitación que ha llevado a la implementación y ejecución de contratos inteligentes simples y baratos, en términos de coste computacional. Otro problema es que los contratos inteligentes necesitan una fuente de información de confianza, por ejemplo un sensor de temperatura que diga si una cadena de frío está rota o no. Por esta razón, los dispositivos que proporcionan esa información deben ser probados a fondo antes de ser integrados

en cualquier plataforma operada por contratos inteligentes (Miller et al., 2016). Además,se hace indispensable la utilización de sistemas de auditoría que se encarguen de verificar periódicamente el buen funcionamiento de los mencionados dispositivos. Durante esta Tesis Doctoral se ha colaborado en una primera aproximación de desarrollo de estos tipos de dispositivos (González-Briones et al., 2019). Esto es importante no sólo para evitar el almacenamiento de datos corruptos en la cadena de bloques, sino también para garantizar que estamos utilizando datos no manipulados en la ejecución de los contratos inteligentes.

- **Cuestiones legales**. La legislación española dice en el artículo 1290 de su código civil: "los contratos válidamente celebrados podrán ser resueltos en los casos establecidos por la ley". Lo mismo ocurre con el resto de artículos redactados para la terminación de los contratos, lo que significa que todo contrato debe ofrecer una forma de terminarlo. Gracias a la naturaleza inmutable de los Smart Contracts desplegados en una red blockchain, es imposible eliminarlos por completo. La única solución para actualizar o terminar un contrato inteligente activo, es desplegar uno nuevo con cláusulas actualizadas. El antiguo smart contract debería ser capaz de redirigir las peticiones que reciba al nuevo, por lo que este planteamiento es válido, al menos para la legislación española actual (Mezquita, Valdeolmillos, et al., 2019). Otro aspecto importante en cuanto a cuestiones legales, es la forma en que se protegen los derechos de los inversores que ponen su dinero en criptodivisas. Algunos países como Malta han comenzado a crear medidas de regulación para las actividades realizadas dentro de las plataformas basadas en el libro mayor distribuido para proteger y ofrecer garantías a las personas que hacen uso de estas tecnologías Valdeolmillos et al. (2019).

La explicación previa realizada nos permite tener un punto de partida a la hora de empezar a diseñar sistemas basados en blockchain, que serán aplicados al paradigma actual industrial, compuesto mayormente por redes de dispositivos IoT. De esta forma, la contribución principal de esta tesis es el diseño de modelos de despliegue de este tipo de sistemas, que sean capaces de enfrentar de una forma satisfactoria los retos planteados, con el fin de implementar plataformas basadas en blockchain, que optimicen servicios típicos del paradigma industrial actual en tiempo de ejecución. En las siguientes secciones se detallan los trabajos realizados en este aspecto.

La Sección 3.2 propone una arquitectura MAS basada en blockchain para las cadenas de suministro de la industria farmacéutica. Esta arquitectura proporciona (i) seguridad en las comunicaciones, (ii) confianza en la trazabilidad de los bienes transportados a lo largo de la cadena, (iii) una plataforma capaz de eliminar a los intermediaros que no aportan valor al producto final pero que encarecen su precio, y (iv) optimización en los tiempos de los pagos respecto a los de la industria logística actual. Para su diseño se han hecho frente a los retos de (a) escalabilidad, poniendo especial énfasis en la organización de las estructuras de datos, su almacenamiento en blockchain, y las interacciones que serán efectuadas durante el ciclo de vida del proceso; (b) seguridad, haciendo uso de una red blockchain pública probada; (c) contratos inteligentes, mostrando la necesidad de las auditorías para evitar, por ejemplo, que se falsifiquen datos tomados de sensores; y (d) cuestiones legales, diseñando los contratos con cláusulas de cierre, castigo, y sin almacenar información sensible.

La Sección 3.3 propone una arquitectura MAS basada en blockchain para la creación de un mercado energético automático descentralizado. Esta arquitectura proporciona (i) seguridad en las comunicaciones, (ii) optimización de las retribuciones obtenidas por cada actor, (iii) eliminación los intermediarios que no aportan valor pero que encarecen el precio de la energía, (iV) bajada de los tiempos de espera en referencia a los pagos efectuados. Para su diseño se han hecho frente a los retos de (a) escalabilidad, diseñando un sistema de búsqueda de agentes y comunicación directa entre ellos; (b) seguridad, haciendo uso de una red permisionada que irá creciendo con el tiempo, conforme nuevos usuarios se vayan aceptando en el mercado; (c) anonimato y privacidad, puesto que en esta plataforma, los datos almacenados son críticos en el corto plazo, se ha diseñado un sistema para la encriptación de estos datos y para el enmascaramiento de la identidad de los actores; (d) contratos inteligentes, mostrando la necesidad de auditorías periódicas en los medidores inteligentes utilizados para medir el envío y recepción de energía a y por la red; (e) cuestiones legales, proveyendo a los contratos de cláusulas de cierre, a los usuarios de anonimidad real, y de un sistema de encriptación a los datos almacenados.

3.2. Arquitectura MAS basada en blockchain para la trazabilidad de suministros en la industria farmacéutica

La logística se ocupa del transporte de productos entre las partes. Actualmente es un área importante para las empresas. Sin embargo, el problema de este sector es que su escala puede provocar retrasos e incumplimientos en la entrega de mercancías, así como otras cuestiones. Además, los grandes distribuidores necesitan un gran volumen de trabajadores para satisfacer la gran demanda de las tiendas. Todo esto puede contribuir a que se produzcan grandes retrasos en la tramitación de los pedidos y aumenta la posibilidad de perder algunos de ellos (T. Li, Sun, Bolić, & Corchado, 2016). En un intento de resolver este problema, las empresas han automatizado todos sus procesos, lo que ha contribuido a un aumento significativo del número de empresas y distribuidores en el sector de la logística. Sin embargo, el aumento de la cantidad de datos digitalizados y la expansión de las empresas en Internet, hace que el riesgo de ataques a sus bases de datos sea también mayor. Los piratas informáticos pueden pretender modificar, robar, o borrar los datos almacenados (Lima, de Castro, & Corchado, 2015).

En esta sección se presenta una arquitectura diseñada y presentada por (Mezquita, Casado-Vara, et al., 2021), como una forma alternativa de resolver el problema presentado. El caso de estudio realizado en este trabajo, una plataforma para la gestión de la cadena de suministro en el ámbito farmacéutico, considera dos escenarios diferentes. En primer lugar, proporcionamos seguridad a los datos de las empresas implicadas en el sector logístico mediante la inclusión de la tecnología blockchain. En segundo lugar, se utilizarán sistemas multiagente para gestionar el problema de la organización de los procesos realizados en la plataforma.

Se ha demostrado que los sistemas multiagente proporcionan soluciones eficientes a una enorme variedad de problemas (Wooldridge & Jennings, 1995). Estos incluyen, entre otros, el uso de agentes para la clasificación de imágenes (Coria, Castellanos-Garzón, & Corchado, 2014), el control descentralizado de redes Najafi et al. (2018), los problemas en tiempo real (Carrascosa, Bajo, Julián, Corchado, & Botti, 2008), el control predictivo distribuido de modelos (Casado-Vara et al., 2019; Francisco et al., 2019), y aplicaciones de sistemas IoT (Casado-Vara & Corchado, 2018).

En esta arquitectura se propone un nuevo modelo que hace uso de la tecnología blockchain, los contratos inteligentes, y un sistema multiagente para proteger los datos del sector logístico farmacéutico al tiempo que agiliza las actividades logísticas. Además, el sistema multiagente es capaz de coordinar todos los servicios logísticos (González-Briones, Castellanos-Garzón, et al., 2018), mejorando la eficiencia del sector logístico. Al hacer uso de tecnología blockchain, el modelo propuesto protege los datos generados dentro de la plataforma de manipulaciones posteriores a su almacenamiento. Además,gracias a los contratos inteligentes utilizados para controlar el funcionamiento de la plataforma, es posible eliminar los intermediarios que no aportan valor (Mezquita, Casado, et al., 2019). Los retos en los parámetros logísticos, como los retrasos en la entrega, la pérdida de documentación, el desconocimiento de la procedencia de los productos, los errores, etc., pueden minimizarse e incluso evitarse por completo gracias a esta implementación. Con los mecanismos de seguridad que otorga el uso de la tecnología blockchain, es posible, además, crear un marco de comunicaciones de confianza entre los actores y dispositivos de la plataforma. Gracias a ello es mucho más difícil que se produzcan ciberataques como los denominados *phishing* y *man in the middle* (Khan & Salah, 2018; Kshetri, 2017).

Por otro lado, el sistema multiagente utiliza contratos inteligentes para controlar y validar el flujo de trabajo de la plataforma, mientras que la red blockchain se encarga de almacenar las transacciones realizadas por los agentes (Durić, 2017). Aunque se habla mucho del uso de blockchain en los servicios logísticos, no ha habido muchas plataformas que lo implementen y evalúen en escenarios de uso reales (Tijan, Aksentijević, Ivanić, & Jardas, 2019). Además, este tipo de sistemas no se han propagado lo suficiente, porque las empresas que podrían beneficiarse de ellos, carecen de información y por lo tanto no invierten suficiente dinero en la implementación de dichas soluciones (Hackius & Petersen, 2017).

3.2.1. Arquitectura

El modelo propuesto, véase la Tabla 3.3, consta de los siguientes elementos: (i) una red pública blockchain, ajena al despliegue de la plataforma y usada como servicio, y en ella se almacenan todas las transacciones y despliegan los contratos inteligentes, ya usada en otros trabajos como (Mezquita, González-Briones, et al., 2019); (ii) contratos

inteligentes que gestionarán las transacciones realizadas entre las diferentes partes; y (iii) un sistema multiagente que permite la ejecución de todas estas operaciones de una forma distribuida. En esta sección describimos cómo funciona este modelo.

Tabla 3.3: Tabla de las principales características de la arquitectura MAS basada en blockchain para la trazabilidad de suministros en la industria farmacéutica.

Característica	**Descripción**
Escalabilidad	Se prevee que este sistema no va a escalar más de los cientos de actores interactuando.
Anonimato	En esta plataforma, puesto que no existe información crítica de los usuarios que se vaya a almacenar en la blockchain, no es necesario proporcionar anonimato.
Red blockchain	En esta arquitectura se propone el uso de una red blockchain como un servicio. La tecnología estudiada para este caso es el uso de la red de Ethereum.
Encriptación	Puesto que la información generada por esta plataforma no es crítica, y de hecho, se requiere transparencia para que el consumidor final conozca el proceso de los productos que está adquiriendo, no se va a encriptar la información.
Almacenamiento	Puede ser mucho el volumen de datos tomados por los dispositivos, por eso la información que se almacena en blockchain es relativa a lotes de productos. Por otro lado, la información de los sensores es almacenada *off-chain* y sólo se usa la red cómo un método de verificación, almacenando los *hashes* de los datos.

Las partes implicadas en una operación comercial disponen de dispositivos inteligentes que monitorizan el estado de cada operación. El caso de estudio se llevó a cabo en el sector farmacéutico, en la Figura 3.1 se muestran los miembros del proceso. El cliente (farmacias), el productor (empresas farmacéuticas) y las empresas de transporte. En este caso de uso, los clientes tienen sensores que controlan el número de medicamentos almacenados en la farmacia, el tipo de medicamentos vendidos y la cantidad de dinero almacenada. En cuanto a las empresas farmacéuticas, tienen sensores encargados de conocer las existencias disponibles y los niveles de producción actuales. Por último, las empresas de transporte tienen sensores en cada uno de sus vehículos de transporte para controlar la posición de la carga. Todos estos elementos conforman la Red de Sensores Inalámbricos (WSN por sus siglas en inglés *Wireless Sensor Network*) que supervisa las operaciones en el sector farmacéutico.

Dentro de la WSN que monitoriza las operaciones realizadas en el caso de uso presentado, existen dispositivos inteligentes que se encargan de crear las transacciones con los datos monitorizados. Esas transacciones son enviadas a la red blockchain por los dispositivos

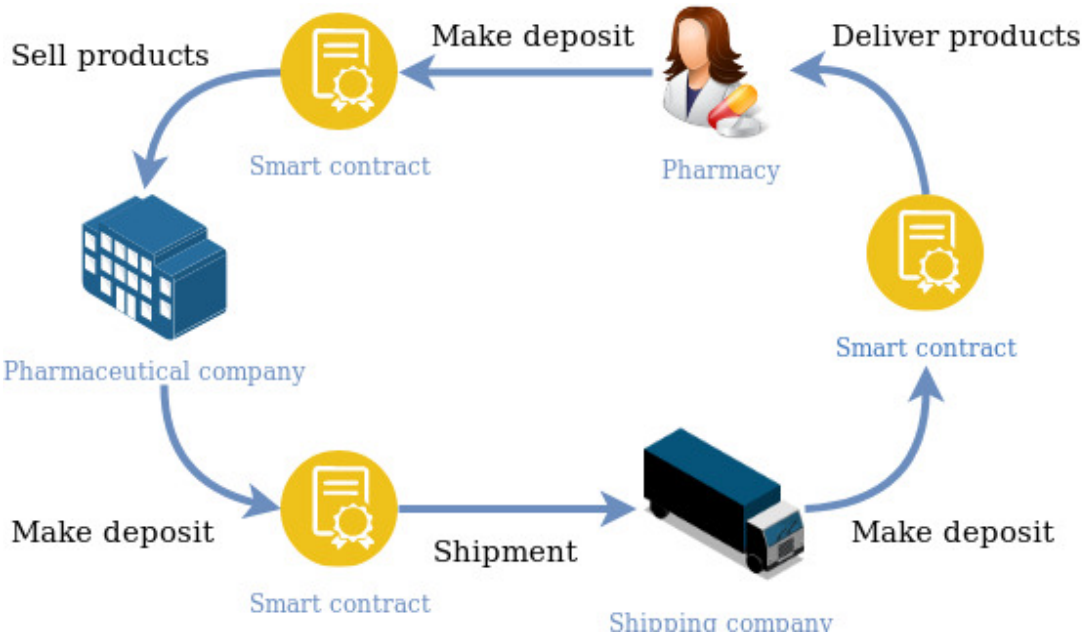

FIGURA 3.1: En el flujo de trabajo propuesto el cliente (Farmacia) hace un depósito en el contrato inteligente para la compañía farmacéutica que le vende los productos. La compañía farmacéutica delega los productos al transportista, mediante previo depósito de dinero en el contrato inteligente, para pagar al transportista y una parte adicional a modo de fianza por si existe algún problema con los productos antes de su transporte. El transportista firma la recepción y realiza un depósito proporcional al coste de los productos en el contrato inteligente, para cubrir cualquier problema que pueda pasar durante el viaje. Finalmente, el cliente (farmacia) cuenta con sensores que le indican si los productos han sido recibidos y en buen estado. Una vez se aceptan los productos, los pagos bloqueados en el contrato inteligente son transferidos a sus respectivos destinatarios y las fianzas liberadas.

inteligentes. En la blockchain, junto con los datos generados, también se almacenan los contratos inteligentes que controlan el flujo de trabajo de la plataforma.

Un sistema multiagente controla todo el proceso. La arquitectura del sistema multiagente se compone de las siguientes capas (ver Figura 3.2).

1. **Capa de cliente:** esta capa consta de tres tipos diferentes de agentes que gestionan las farmacias. Entre ellos se encuentran el agente de gestión de datos, que mantiene actualizado el stock de la farmacia; el agente que se encarga de realizar los pedidos y el que verifica la entrega de los productos adquiridos, cambiando su estado en la blockchain a través de contratos inteligentes.

2. **Capa de origen:** esta capa consta de: dos agentes que reciben los pedidos de los farmacéuticos y otro agente que realiza los pedidos a la empresa de transporte para llevar la mercancía a las farmacias. La tarea de otro agente es el control de

los niveles de stock y producción. Por último, hay un agente encargado de verificar si se cumplen las condiciones del contrato inteligente.

3. **Capa de envío de productos:** esta capa consta de: un agente que gestiona los pedidos entrantes, otro agente que gestiona la flota de vehículos y, por último, un agente que verifica los contratos inteligentes.

4. **Capa de gestión del flujo de trabajo:** esta capa consta de dos agentes: un agente de gestión del flujo de trabajo y un agente de control de contratos inteligentes este agente. Esta capa se encarga de crear los contratos inteligentes, guardar el dinero mientras se realizan las transacciones y aplicar las penalizaciones en caso de incumplimiento de los contratos inteligentes.

Así, uno de los agentes incluidos en cada una de las 4 capas verifica que se cumplan los términos del contrato inteligente. Por ejemplo, cuando se inicia un contrato inteligente entre una farmacia y una empresa farmacéutica para la compra de medicamentos, ambos a un conjunto de términos. La farmacia paga los medicamentos, pero el dinero es guardado en la blockchain por una entidad de control, en este caso el agente que verifica el contrato inteligente. Cuando la farmacia recibe los medicamentos que pidió, este agente confirma que se han cumplido las condiciones del contrato inteligente y paga automáticamente al farmacéutico la suma de dinero acordada.

3.2.2. Interacciones con la red blockchain

Una vez diseñado el sistema multiagente, se ha estudiado el número de veces que la plataforma interactúa con la blockchain. En este modelo, las transacciones realizadas en un flujo de trabajo normal para la compra de productos, se detallan de la siguiente manera:

- En la capa de cliente, cuando un cliente quiere comprar un producto, se realiza una transacción de fondos del cliente al contrato inteligente. Además, cada vez que un lote de artículos llega a su destino final, se actualiza el estado del lote y se ejecuta una transacción, en la que se actualiza el estado del lote, y el contrato inteligente libera los fondos transaccionados desde el cliente al propietario del producto. Esto significa que en un flujo de trabajo normal, se realizan tres transacciones en esta capa.

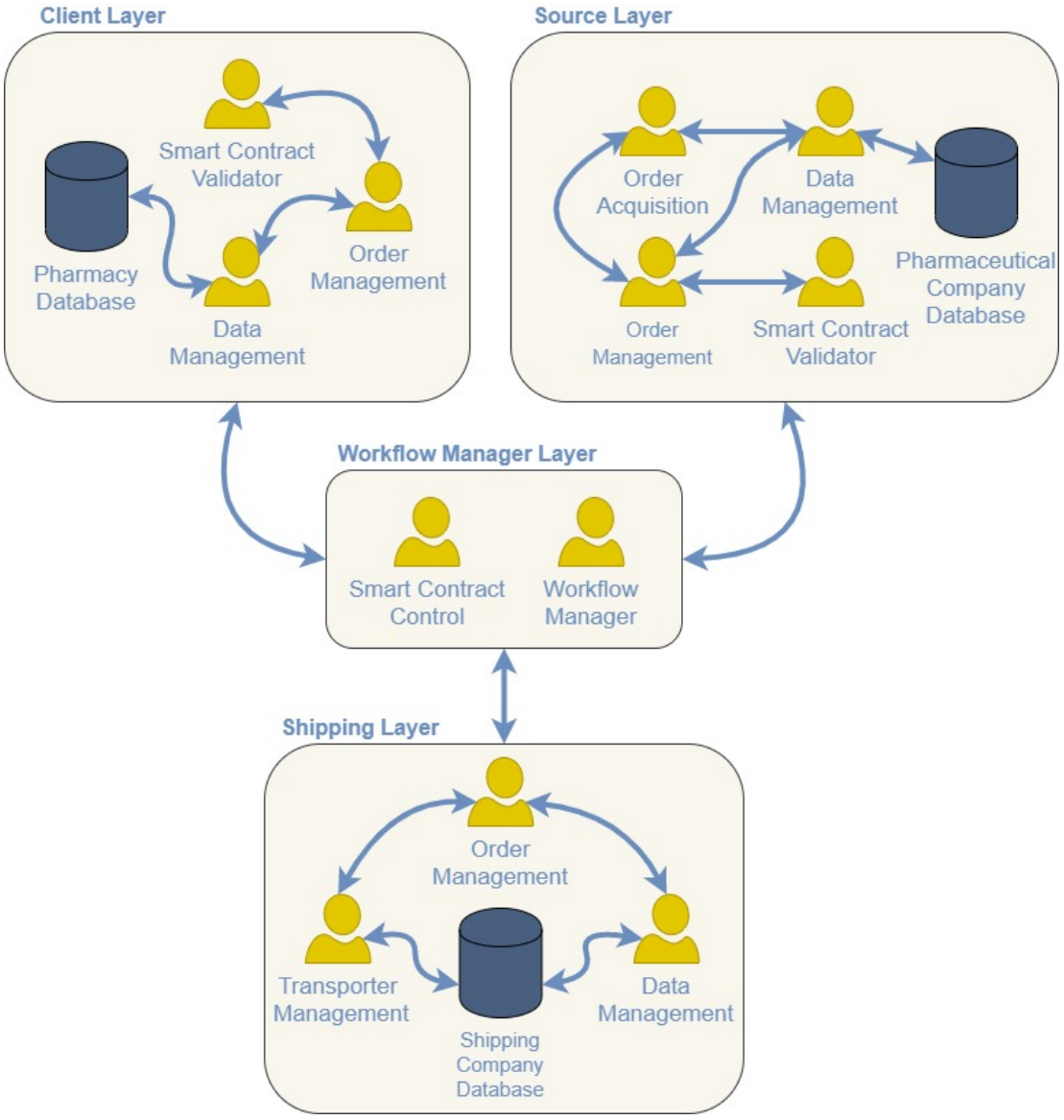

FIGURA 3.2: Arquitectura multiagente: 1) Capa cliente: en esta capa se encuentran las farmacias. 2) Capa de origen: en esta capa se encuentran las empresas farmacéuticas. 3) Capa de envío: esta capa gestiona las empresas de transporte. 4) Capa de gestión del flujo de trabajo: Esta capa contiene un agente que controla todo el flujo de información y un agente que se encarga de que se cumplan las condiciones del contrato inteligente.

- En la capa de origen, se realiza una transacción cuando se pone a la venta un lote de productos, otra cuando se vende y cuando se envía. La última transacción consiste en asegurar el pago realizado por el cliente en el contrato inteligente, de forma que el vendedor no recibe el pago hasta que se confirma que el pedido ha sido entregado correctamente. Si no hay ningún problema con el pedido, los fondos se devuelven al vendedor, lo que hace un total de cinco transacciones en una ejecución normal.

- En la capa de gestión del flujo de trabajo sólo se realizan transacciones con la blockchain cuando un agente quiere formar parte de la plataforma y un agente la abandona. Una transacción por cada actualización del estado de los agentes.
- En la capa de envío sólo se transfiere el pago al contrato inteligente cuando se envía un nuevo pedido. Los fondos se entregan al vendedor en el caso de que haya habido algún problema con el envío. En caso contrario, se devuelven al transportista.

Tras estudiar las interacciones de la plataforma con la blockchain, descubrimos que se realizan un mínimo de diez transacciones cuando se entrega un lote de productos de un vendedor a un cliente final. Esta cifra no tiene en cuenta el número de transacciones realizadas en los casos en que un nuevo vendedor, cliente o transportista quiere formar parte de la plataforma.

Para calcular el coste de ejecución de los servicios de la red blockahin, tenemos que conocer el precio de ejecución de cada transacción. Tomando el caso de Ethereum, elegido para este caso de uso, y según (Ryan, 2017), el precio de ejecución de una transacción equivale a 0,1€, que multiplicado por el número de transacciones en un flujo de trabajo normal del sistema, la cantidad de dinero que necesitan todos los interesados para mantener el sistema es de 1€ por lote de productos que se transan de un interesado a otro.

Una de las razones por las que se ha seleccionado la blockchain de Ethereum es porque ofrece el mejor soporte para la integración de la plataforma y, además, utiliza el lenguaje de programación python, web3.py (Ethereum, s.f.). Además, si suponemos que hay un centenar de compradores y vendedores, la plataforma realiza cientos de transacciones en una iteración normal del flujo de trabajo. Dicho esto, el tiempo necesario para realizar un intercambio de activos entre vendedor y comprador es del orden de días, y la media diaria de transacciones de la blockchain de Ethereum es de 610000 (ConsenSys, 2018), entonces, podemos asumir que la plataforma propuesta puede ser gestionada por la red Ethereum.

En nuestro estudio, se ha demostrado que el precio para el intercambio de un lote de activos entre diferentes partes interesadas es de aproximadamente 1€. Si tenemos que comparar con el modelo tradicional que utiliza intermediarios humanos en el proceso

de verificación (Benjamin & Wigand, 1995), el flujo de trabajo de nuestra plataforma propuesta es más barato y más rápido.

3.2.3. Conclusiones y posibles mejoras

Esta arquitectura ha sido diseñada para apoyar el desarrollo de plataformas logísticas basadas en blockchain. Aunque ofrece una gran seguridad y transparencia, estas dos características se pueden volver un problema si tenemos en cuenta la escalabilidad y privacidad de los usuarios.

Respecto a la escalabilidad, por ejemplo, en un sistema logístico en el que sólo interviene un consorcio de empresas farmacéuticas, que hacen exportaciones a un número limitado de paises, en el que, como se ha analizado, sólo necesitan hacer transacciones del orden de los centenares por día, es aceptable. Pero si tuviese que escalar al orden de los miles, con un consorcio de consorcios por ejemplo, la red caería, aumentando muchísimo su latencia, empeorando, por ende, la calidad del servicio y aumentando su precio. Alternativas a ello sería utilizar redes blockchain públicas que hagan uso de otros algoritmos de consenso más optimizados para una gran actividad en la red.

En cuanto a la anonimicidad y protección de los datos, se descubrió cómo algo primordial y necesario en casi cualquier tipo de plataforma distribuida, en el artículo publicado por (Mezquita, Parra-Domínguez, et al., 2022) explicado en el Capítulo 2. La anonimicidad no es posible obtenerla en ninguna de las redes públicas capaces de implementar contratos inteligentes, lo que dió pie a encaminar la rama de la investigación a conseguir una anonimicidad real dentro de las plataformas blockchain, culminando esta tesis con el artículo publicado por (Mezquita, Gil-González, et al., 2022) y explicado en la Sección 3.3.

3.3. Arquitectura MAS basada en blockchain para la creación de un mercado automático y distribuido de energía

Tras lo estudiado en esta Tesis Doctoral, se ha identificado como la anonimidad y la protección de los datos uno de los mayores retos que la tecnología blockchain, debe

hacer frente actualmente. Para ello, decidimos enfocar el estudio en un caso de uso que necesite una total anonimicidad de los datos. El caso de uso que elegimos fue el de una microred eléctrica en el que los usuarios negocian e intercambian energía de forma automática. Este caso de estudio es muy interesante porque una brecha de información puede dejar expuestos a los ciudadanos a: i) cuánta energía consumen y en qué periodos lo hacen más, evidenciando que hay momentos en los que los hogares pueden estar vacíos; ii) cuánta energía vende cada usuario, pudiendo extrapolar la situación anterior; y iii) cuánto dinero ingresa o gasta cada usuario, una gran violación de su privacidad.

En esta sección se describirá la arquitectura presentada para la resolución del problema planteado. Debido a la naturaleza de este tipo de sistemas, será imposible utilizar una blockchain pública como en la arquitectura anterior. En este caso será necesario un consorcio de pares entre los usuarios de la microrred eléctrica para crear una red blockchain permisionada que haga uso de un protocolo de consenso como PBFT, PoS o dPOS, donde se supone que todos los participantes de la red se conocen y tienen el objetivo común de querer que la plataforma funcione.

Una de las características de las que carecen las empresas estudiadas en el estado del arte presentado en el Capítulo 2 es el desarrollo de una plataforma donde se permita la negociación automática entre los actores. El modelo que presentamos y publicamos en (Mezquita, Gil-González, et al., 2022) hace uso de un juego no cooperativo entre consumidores y productores que regulará el precio del mercado de la energía de forma autónoma, permitiendo así que los actores optimicen sus retribuciones de forma individual y en base a sus necesidades del momento. Nuestro modelo y sus interacciones con la blockchain se explican detalladamente para ayudar a las startups y a los emprendedores a desarrollar este tipo de sistema. Además, el escenario propuesto en nuestro trabajo se basa en un horizonte rodante como el propuesto por Long et al. Long, Wu, Zhou, & Jenkins (2018), pero con una ventana temporal de una hora para hacer más viables las transacciones dentro de la red blockchain.

Debido a la importancia del cumplimiento con el Reglamento General de Protección de Datos (GDPR) (*European Parliament and Council: Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive)*, 2016), se necesita realizar una selección cuidadosa de los datos que se van a recoger y almacenar en

la blockchain, así como los datos que deben ser encriptados y ocultados de otros actores. Además, es necesario garantizar la integridad y autenticidad de los datos protegiéndolos y protegiendo los canales de comunicación de usuarios no autorizados (Pichler et al., 2018). Otro problema de la plataforma propuesta es su fuerte dependencia del marco legislativo del país donde se va a instalar. Se necesitan leyes que regulen la transacción de energía renovable entre pares dentro de las comunidades, como en el caso de Bélgica, Grecia y Alemania (Pichler et al., 2018).

3.3.1. Arquitectura

En esta sección, describiremos el diseño de la arquitectura propuesta, que tiene como objetivo: i) descentralizar el mercado de la energía, ii) automatizar, en la medida de lo posible, el mercado de la energía en pequeñas comunidades, iii) y proporcionar anonimato y privacidad a sus usuarios. En la literatura estudiada en el Capítulo 2, existen propuestas en funcionamiento que cumplen con algunos de los requisitos mencionados, aunque no todos juntos.

La arquitectura propuesta seguirá el paradigma de sistemas multiagente distribuidos (MAS) que, en combinación con la tecnología blockchain, permite la distribución de los procesos y el control de la plataforma. En la arquitectura propuesta se han juntado características de diferentes trabajos estudiados en la literatura, permitiendo así un control descentralizado de la plataforma sin un único punto de fallo y permitiendo un proceso de negociación entre los pares de la red, además de cumplir con el GDPR (*European Parliament and Council: Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive)*, 2016).

- A través del MAS se consigue el control y la gestión de la plataforma de la microrred, así como la negociación entre pares de la energía en el mercado. Sin embargo, para lograr la descentralización total de la plataforma, se requiere el uso de una plataforma blockchain, en la que los contratos inteligentes desplegados serán utilizados por los agentes en el flujo de trabajo de la plataforma. Gracias a este enfoque: (i) conseguiremos una plataforma descentralizada sin un único punto de fallo; (ii) proporcionaremos confianza a los usuarios y agentes de la plataforma

de que los acuerdos se cumplirán, y en caso de que no lo hagan, fomentaremos la confianza de que la plataforma compensará a los que se comporten mientras castiga a los agentes que no lo hagan; y (iii) permitiremos la optimización de los precios de la energía transaccionada dentro de la plataforma, equilibrándolos al tiempo que se maximizan las retribuciones de cada tipo de actor implicado.

- Los contadores inteligentes leen la energía consumida y/o producida por cada hogar. Están conectados a cada casa independiente, representando un par en la red de microrredes. Cada contador inteligente está conectado a Internet e interactúa con la cadena de bloques en nombre del hogar.además, el agente que negocia con sus pares para comprar o vender energía debe desplegarse aquí o en un dispositivo conectado al contador inteligente.
- El uso de una red de blockchain permite distribuir la comunicación y las interacciones entre los agentes de la plataforma. La red se utiliza no sólo como un registro histórico en el que cada agente almacena su actividad en la plataforma, sino que también se utiliza como un sistema de validación y a prueba de manipulaciones que les ayudará a confiar en la plataforma y en las actividades de los agentes involucrados. Además, los contratos inteligentes desplegados en la red ayudan al control del flujo de trabajo de la plataforma.
- La información almacenada en la blockchain está encriptada, manteniendo los datos ocultos a los demás. Es posible mantener un registro verificado y encriptado en la blockchain mediante el uso de protocolos de conocimiento nulo (ZKP por sus siglaas en inglés: *Zero Knowledge Proofs*). Además, mediante el uso de firmas en anillo, la identidad de las entidades que almacenan información dentro de la blockchain se mantiene en secreto.

3.3.1.1. Asunciones de seguridad

En esta sección se detallan los supuestos de seguridad del marco y el tratamiento de los datos generados en la plataforma. La implementación de la tecnología blockchain en esta plataforma garantiza la aplicación de un protocolo de identificación seguro entre los actores. Además, la información almacenada es a prueba de manipulaciones, y los contratos inteligentes desplegados permiten el control descentralizado de la plataforma, asegurando que no habrá un único punto de fallo propenso a ataques.

En cuanto al almacenamiento de los datos generados, que se utilizarán para crear los modelos predictivos que ayudarán al buen funcionamiento del sistema, cada actor será responsable de ellos. Suponemos que cada actor es responsable de proporcionar un punto de acceso a sus datos para que pueda controlar a quién da acceso a los mismos. Para cada hora, se puede crear un lote con los datos generados, almacenando en la blockchain un hash de dichos datos que ayudará a verificar que no han sido modificados posteriormente. El uso de sistemas de auditoría permite generar datos de confianza. De lo contrario, sería imposible saber que los datos generados no han sido modificados antes del almacenamiento de su hash en la blockchain (Mezquita, Casado, et al., 2019).

En cuanto a los protocolos de privacidad propuestos, garantizan que la información almacenada en la cadena de bloques no podrá ser leída por terceros sin permiso, ni será posible identificar o rastrear la actividad de los usuarios. Esta información que se almacena es, por ejemplo, las ofertas de energía publicadas, el dinero pagado por las transacciones de energía o la cantidad de energía transaccionada. La única vulnerabilidad de esta plataforma es cuando un atacante roba las claves de un usuario. Sin embargo, esto no es posible por el mero hecho de utilizar la plataforma; sólo puede ocurrir si el usuario no es lo suficientemente cuidadoso con las contraseñas utilizadas o con el lugar donde se almacenan las claves.

En este trabajo se han hecho suposiciones de seguridad de que la red de nodos de blockchain es lo suficientemente grande como para que no sea fácil tirarla mediante un ataque de Denegación de Servicios Distribuidos (DDOS). También se ha asumido que los actores que forman parte de la plataforma se benefician más de su buen funcionamiento que de intentar sabotearla. Diferentes actores podrían coludirse entre sí para conseguir un mayor beneficio, pero este escenario no es realista según el estudio realizado por (van Leeuwen, AlSkaif, Gibescu, & van Sark, 2020). Teniendo en cuenta los supuestos anteriores, podemos decir que los actores de la plataforma se beneficiarán de la creación de esta plataforma y de la competencia entre ellos más que de intentar sabotear el proceso de negociación y el bienestar de la plataforma.

3.3.1.2. Sistema multiagente

En esta sección se describe en detalle la estructura de la MAS. Está dividida en cuatro subsistemas diferentes, en los que los agentes se agrupan según su función dentro de la

plataforma (ver Figura 3.3). A continuación se describen detalladamente los diferentes subsistemas y los agentes que los componen:

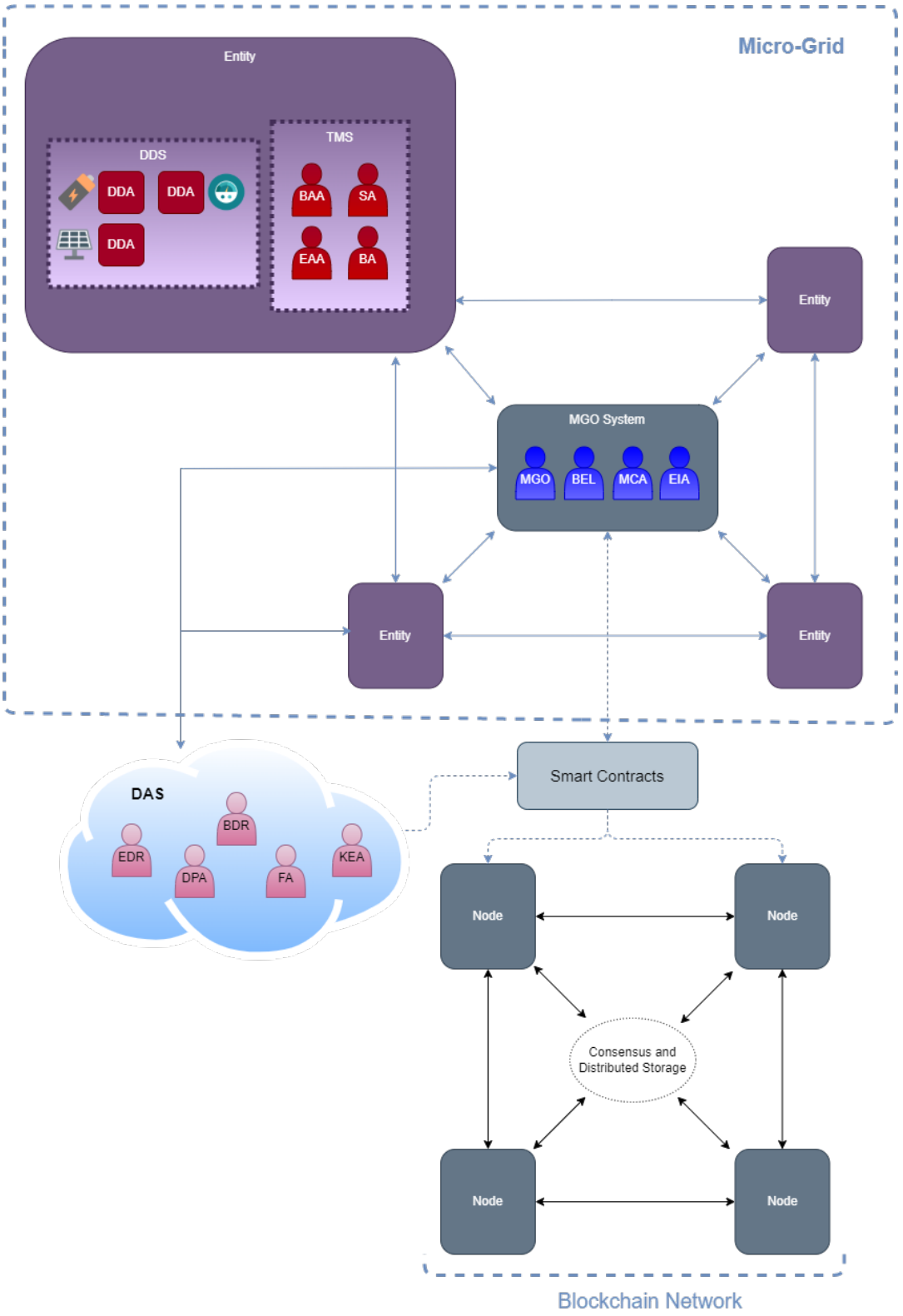

FIGURA 3.3: Arquitectura de la plataforma propuesta.

- **S**istema de Controladores de Dispositivos (DDS). Este sistema agrupa todos los agentes encargados de la gestión y control de los diferentes dispositivos inteligentes de la plataforma (por ejemplo, baterías, contadores inteligentes, paneles fotovoltaicos). Estos agentes pueden interactuar con la red blockchain, por lo que también tienen un monedero asignado para identificar y seguir su actividad dentro de la plataforma, ayudando así en el proceso de auditoría. Los agentes encargados de supervisar el estado de los paneles fotovoltaicos (por ejemplo, su producción de energía, la tensión y la corriente proporcionadas, y sus potencias activas y reactivas) son los agentes fotovoltaicos (PVA). Almacenan esos datos en la blockchain, lo que ayuda a sus propietarios a monitorizarlos y a la vez a poseer esa información que podrían vender en el futuro. Las baterías son monitorizadas por agentes llamados Battery State Agents (BSA). Almacenan en la blockchain datos relacionados con el estado de una batería, su capacidad de carga y descarga, y su estado de carga actual. El agente que almacena los datos relacionados con el flujo de corriente desde o hacia un hogar es el Agente del Contador Inteligente (SMA).

- Sistema de Operadores del Micro-grid (MGOS). En este sistema se agrupan todos aquellos agentes que se encargan de monitorizar, controlar y gestionar el estado y buen crédito de la microrred. Estos agentes también están conectados a la blockchain, almacenando la información relevante que favorece la trazabilidad de la monitorización de la microrred, los flujos de energía hacia y desde la red de la compañía eléctrica, el balance de la energía de la microrred y el nivel de tensión (Agente Operador de la Microrred o MGO), o las transacciones de energía realizadas desde la red a la microrred y viceversa (Agente Interactor del Mercado Externo o EMI). Además, este sistema posee una serie de baterías que mejoran el equilibrio de la carga de la red, gobernadas por los agentes del Estado de Carga (SOC). Esta parte de la plataforma se mantiene económicamente mediante las penalizaciones a los usuarios que no cumplen su parte de los contratos y mediante el intercambio de energía entre la red externa y la microrred.

- Sistema Analítico de Datos (DAS). Este sistema es crucial para la plataforma ya que es el encargado de agrupar a todos aquellos agentes que se encargan del mercado de datos y de la creación de modelos predictivos, los cuales son requeridos por el resto de agentes del sistema para poder inferir la cantidad de energía que

esperan obtener en la próxima hora, la que podrían vender y la que necesitarán comprar en base a su consumo pasado. Los agentes encargados de leer los datos proporcionados por los otros subsistemas de la plataforma en la blockchain y fusionarlos con los datos procedentes de otras fuentes de datos externas se denominan Agentes Lectores de Datos (DRA). Los agentes que crean y actualizan nuevos modelos de comportamiento bajo demanda son los Agentes Extractores de Conocimiento (KEA). Los agentes que realizan predicciones basadas en estos modelos y en la información extraída del entorno son los Agentes Pronósticos (AF). El subsistema se beneficia del mercado de datos creado con la incorporación de la tecnología blockchain a la plataforma. Como se ha encontrado en otros trabajos en la literatura, también es posible mejorar la creación de los modelos con el uso de la tecnología blockchain mediante la aplicación de un marco de aprendizaje federado similar al propuesto en (Peng et al., 2021).

- Sistema de Gestión de Transacciones (TMS). En este subsistema se agrupan todos aquellos agentes que se encargan de la negociación e intercambio de energía dentro de la microrred. Estos agentes hacen uso de la red blockchain para publicar y buscar ofertas de energía, así como para registrar los acuerdos que se producen. Los agentes encargados de publicar las ofertas son los Agentes Vendedores (SA), mientras que los que las buscan para comprar son los Agentes Compradores (BA). Los agentes de este sistema negocian entre sí directamente y hacen uso del DAS para estimar la energía que necesitarán para comprar y/o vender. Como una forma de mejorar el proceso de búsqueda en la blockchain, se podría utilizar una capa de middleware para optimizar la búsqueda de información (ofertas en este caso) dentro de la blockchain, como la propuesta de (Wu, Peng, Guo, Yang, & Xiao, 2021).

3.3.1.3. Despliegue de la plataforma

En la plataforma propuesta, hay tres tipos de actores: los consumidores que reciben la energía que compran a la red, los paneles fotovoltaicos como productores que producen la energía y la vierten en las baterías, y las baterías como prosumidores que almacenan y distribuyen la energía (por ejemplo, consumida por sus propietarios o, si sobra, vertida a la microrred para obtener un beneficio). También hay actores que se encargan del

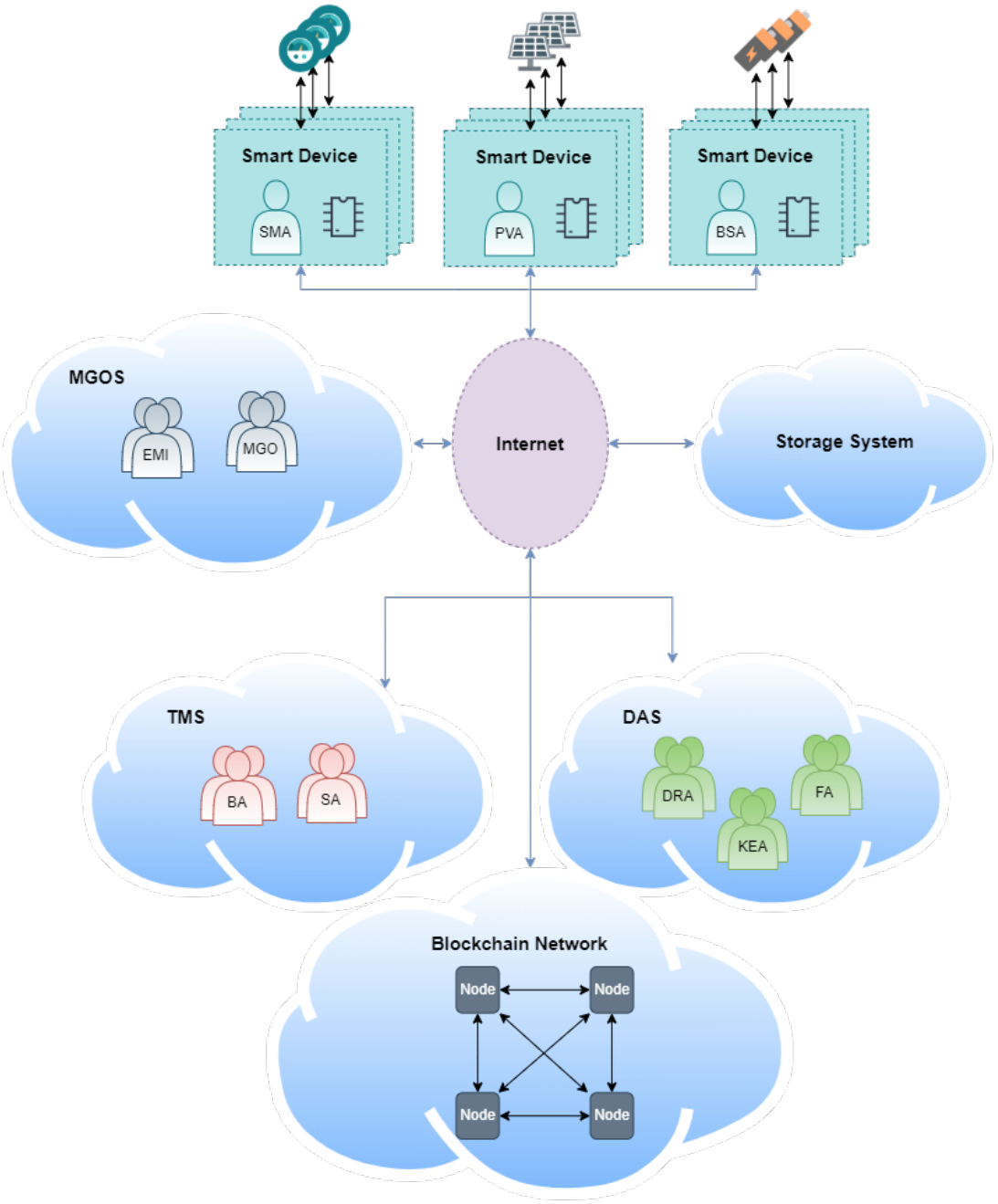

FIGURA 3.4: Diagrama con el despliegue de la plataforma, en él se observa cómo todas las comunicaciones dentro de la plataforma se realizan a través de internet, excepto las de los agentes encargados de controlar los dispositivos inteligentes que deben de estar conectados físicamente a estos. Cada una de las nubes representa una organización virtual en el que los agentes pueden o no estar ejecutándose desde el mismo servidor.

buen crédito de la microrred y que, además, obtienen un beneficio al conectarla a la red externa. Por último, hay otros actores que ayudan al buen funcionamiento de la plataforma, como los encargados de cambiar el dinero fiduciario por el digital y viceversa.

Como se muestra en la Figura 3.4, las interconexiones entre las partes de la plataforma

se realizan a través de Internet, en la creación de servicios en la nube. Los agentes de la plataforma encargados de la extracción de conocimiento con respecto a los datos de la plataforma necesitan una gran potencia de cálculo; Por lo tanto, la infraestructura se subcontrata a un proveedor (por ejemplo, Amazon Web Services, Google Cloud o Azure). La red de blockchain, controlada por los agentes de la plataforma, es accesible a las partes y no necesita una gran potencia de cálculo; sólo se requiere un ordenador por participante que esté siempre encendido. Los agentes encargados de controlar los dispositivos inteligentes deberán estar desplegados en ellos o en un sistema, como una Raspberry Pi, que tenga acceso directo a los mismos. El resto de los agentes sólo necesitan ser desplegados en ordenadores que siempre tengan acceso a Internet y no tienen ningún requisito especial.

3.3.2. Interacciones con la red blockchain

La presente Sección detalla los mecanismos y protocolos utilizados para la integración de la tecnología blockchain y la plataforma. La Sección 3.3.2.1 describe qué tipo de red se necesita para este tipo de plataformas junto a los contratos inteligentes desarrollados para este caso de uso. La Sección 3.3.2.2 detalla cómo son los algoritmos y protocolos criptográficos utilizados para asegurar la privacidad de los usuarios y protección de los datos.

3.3.2.1. Tecnología blockchain y contratos inteligentes

El diseño de la plataforma propuesta se basa en la negociación, el pago y el intercambio de energía. En ventanas de tiempo de una hora, los agentes negocian los precios de la energía en función de la cantidad que desean transar durante la hora siguiente. La plataforma utilizará una red blockchain permisionadas, gobernada en consorcio por los agentes que actúan en el mercado. Una red de blockchain permisionada permite un alto rendimiento de las transacciones con un coste muy bajo.

El uso de una red permisionada se propone porque consigue dos cosas que no se pueden lograr usando una red permissionless (Mezquita, Parra, et al., 2019): (i) la velocidad de las transacciones, al existir sólo nodos conocidos dentro de la red, es posible hacer uso de algoritmos de consenso más rápidos a costa de un cierto nivel de seguridad; (ii) la

escalabilidad del sistema, debido a las características mencionadas, al no requerir una gran capacidad computacional para alcanzar el consenso, el sistema es escalable; (iii) los protocolos de la red pueden adaptarse a los requerimientos del sistema durante el desarrollo, por ejemplo, con la adición de protocolos ZKP y firmas en anillo que no están disponibles en ninguna blockchain pública que permita el despliegue de contratos inteligentes.

En una blockchain permisionada, sólo los actores verificables pueden participar en la plataforma propuesta. Si nuevos actores, por ejemplo, nuevos hogares, quieren participar en el mercado creado dentro de la microrred, tienen que hacer una propuesta a la plataforma; aquí, en un consorcio y no de forma automatizada, los actores de la microrred votarán si les dejan entrar o no. Si los actores sospechan que el nuevo actor que intenta entrar en la plataforma no tiene buenas intenciones o tiene intenciones que no están alineadas con el bienestar de la plataforma, no se le permitirá entrar. En cambio, si se trata de un hogar típico que quiere beneficiarse del buen uso de la plataforma, le permitirán entrar. En resumen, la blockchain de consorcio propuesta en este marco debe ser gobernada por igual por todos los nodos de la blockchain; todos tienen los mismos derechos de voto.

Debido a las características de la red blockchain utilizada, la plataforma necesitará un margen para almacenar los acuerdos realizados por los agentes. En la plataforma propuesta, el margen es de 5 min, tiempo suficiente para que la red valide la información de la plataforma (Combi, 2017). En esa ventana de tiempo de 5 min, los agentes no pueden continuar sus negociaciones. Entonces, después de 55 min, los agentes sólo firmarán los acuerdos que más les beneficien tras el periodo de negociación. De esta forma, los precios de la energía se fijan por cada lote de energía negociado de forma independiente, dependiendo únicamente de la oferta y la demanda, y cada comprador y vendedor tomará sus propias decisiones en función de su situación y de las retribuciones que desee.

En la plataforma, los contratos inteligentes se utilizan para generar tokens que representan la cantidad (en KWh) de energía disponible para el intercambio en las baterías. La virtualización de esta energía se consigue utilizando el estándar de tokens fungibles de Ethereum ERC20. El uso de estándares es importante para futuras extensiones del sistema, así como para la mejora de la interoperabilidad.

En la plataforma propuesta, se utiliza un contrato inteligente para controlar el flujo de trabajo de la plataforma (véase la Figura 3.5). La secuencia habitual de pasos que sigue la plataforma es descrita a continuación:

1. A través de la función *PublishInfo()*, los agentes pueden identificarse en la plataforma. Pueden almacenar datos en relación a cómo otros agentes pueden iniciar negociaciones con ellos, el hogar al que pertenecen, etc. Con esa información, es posible que los agentes autorizados realicen procesos de auditoría, así como el seguimiento de su actividad en la plataforma. Este paso debe realizarse la primera vez que se despliega un agente en el sistema.

2. Para publicar cualquier oferta de energía en la plataforma, los autores deben llamar a la función *MakeOffer()*. Los agentes pueden calcular la energía prevista superávit que se podría vender a la red y crear una oferta con la cantidad de energía prevista para la siguiente horario.

3. Cuando un agente predice la necesidad de comprar energía para la siguiente ventana de tiempo, tendrá que llamar a la función *GetOffers()*. Esta función devolverá toda la información relacionada con las ofertas publicadas para la siguiente ventana temporal. A continuación, el agente iniciará el proceso de negociación directamente con todos los editores de ofertas.

4. Durante el proceso de negociación, los agentes intentan llegar a un equilibrio sobre el precio de la energía y la cantidad que se debe comprar. El precio de la energía vendida tiene una restricción superior, que es el precio de la energía comprada fuera de la red. También tiene una restricción inferior, que es el precio mínimo necesario para producir la energía. Entre esos umbrales, los agentes tienen autonomía para decidir; pueden utilizar el algoritmo de negociación que les resulte más cómodo siempre que intercambie mensajes siguiendo la ontología definida por la plataforma de comunicaciones. Los agentes negocian en función de diferentes parámetros como la energía necesaria para comprar o vender, el tiempo que queda para finalizar la negociación, el número de compradores o vendedores, la cantidad de energía que se espera generar o consumir en la siguiente ventana de tiempo, etc. Cuando se alcancen los últimos minutos de la negociación, cada agente vendedor empezará a pactar la venta de la energía a aquellos que ofrezcan los precios más altos hasta que se agote la energía. Los agentes compradores harán lo contrario: comprarán a

los precios más bajos ofrecidos por los vendedores durante su negociación. Debido a las restricciones, se garantiza que toda la energía se agotará; ningún comprador comprará de la red principal mientras haya energía disponible en el sistema. Por lo tanto, cada agente debe tener un tiempo de espera para obtener respuestas de una oferta. Si no reciben una respuesta durante ese tiempo muerto, tendrán que abandonar la oferta e intentar llegar a un acuerdo con la siguiente mejor oferta de su lista. De este modo se garantiza un punto de equilibrio y se evita quedar atrapado en infinitos períodos de espera.

5. Después de negociar el precio y la cantidad de energía a vender y a quién, el vendedor puede publicar en la blockchain a quién, cuánto y por cuánto vende la energía con la función *AllowTransaction()*.

6. Por último, cuando los contadores inteligentes correspondientes han detectado el flujo de energía que entra y sale de una vivienda, se pueden realizar pagos automáticos llamando a la función *MakeTransaction()*.

Para que la plataforma funcione de forma óptima, la cantidad de energía disponible para intercambiar en el mercado debe ser auditable. Se necesita una garantía de que esta energía existe en la plataforma, por lo que los contadores inteligentes encargados de leer esta energía de las baterías y virtualizarla en tokens para su venta se someten a procesos de auditoría periódicos para asegurar su correcto funcionamiento (Mezquita, Casado, et al., 2019). Además, los contadores inteligentes se encargan de leer el flujo de energía que entra y sale de las viviendas, otro elemento crítico para el buen funcionamiento de la plataforma. En este sentido, llamamos oráculos a los contadores inteligentes, ya que son los encargados de virtualizar los datos del mundo real en los contratos inteligentes, un punto crítico de cualquier plataforma basada en blockchain y del que hay que ser muy cauteloso (Gatteschi, Lamberti, Demartini, Pranteda, & Santamaría, 2018).

Cada agente de la plataforma que interactúa de una u otra forma con la red blockchain necesita hacer uso de un monedero. Algunos agentes, como los encargados de utilizar el dinero virtual en los intercambios, necesitan obtener ese dinero previamente. Por ejemplo, si un hogar consume más energía de la que produce, necesitará poner dinero fiduciario en la plataforma; por lo tanto, se necesitará un consorcio de agentes humanos y/o máquinas para virtualizar el dinero introducido y acuñar más tokens que lo

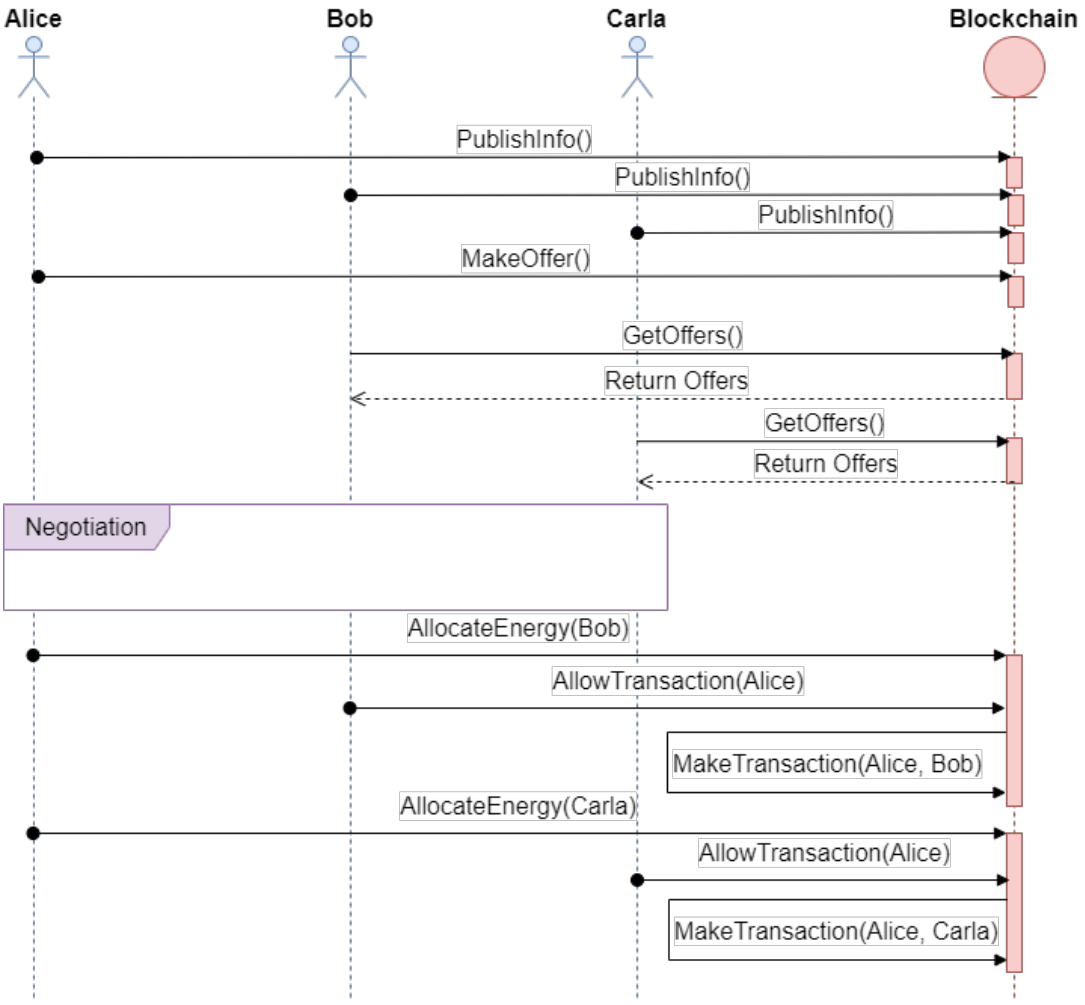

FIGURA 3.5: Diagrama UML de un ejemplo de flujo de trabajo de la plataforma propuesta.

representen. Además, deberán permitir la retirada de dinero real cuando un usuario decida sacar parte del dinero virtual para utilizarlo fuera de la plataforma.

3.3.2.2. Protocolos para preservar la anonimicidad

Uno de los problemas que se plantean en la literatura del estado del arte es el de la privacidad del usuario y la protección de datos, necesarios para cumplir con el GDPR. En este sentido, el modelo propuesto se ha diseñado utilizando protocolos basados en ZKPs utilizados por la criptomoneda Monero y descritos en (Van Saberhagen, 2013). Gracias al uso de estos protocolos, es posible ocultar los usuarios que realizan transacciones dentro de una blockchain así como la información relacionada (Roy Walker, 2018).

El protocolo de firmas en anillo se utiliza para que los actores puedan llamar a los contratos inteligentes de forma anónima. Este protocolo requiere lo que se denomina una Imagen Clave (Roy Walker, 2018), obtenida a partir de una lista de claves públicas seleccionadas aleatoriamente (véase la Figura 3.6). La clave pública del actor que realiza la transacción también es necesaria, ya que la transacción debe ser firmada. Dado que todas las claves seleccionadas tienen la misma probabilidad de realizar la transacción, no es posible asociar la transacción con el usuario real. Además, estos grupos de actores se improvisan aleatoriamente a partir del conjunto de transacciones.

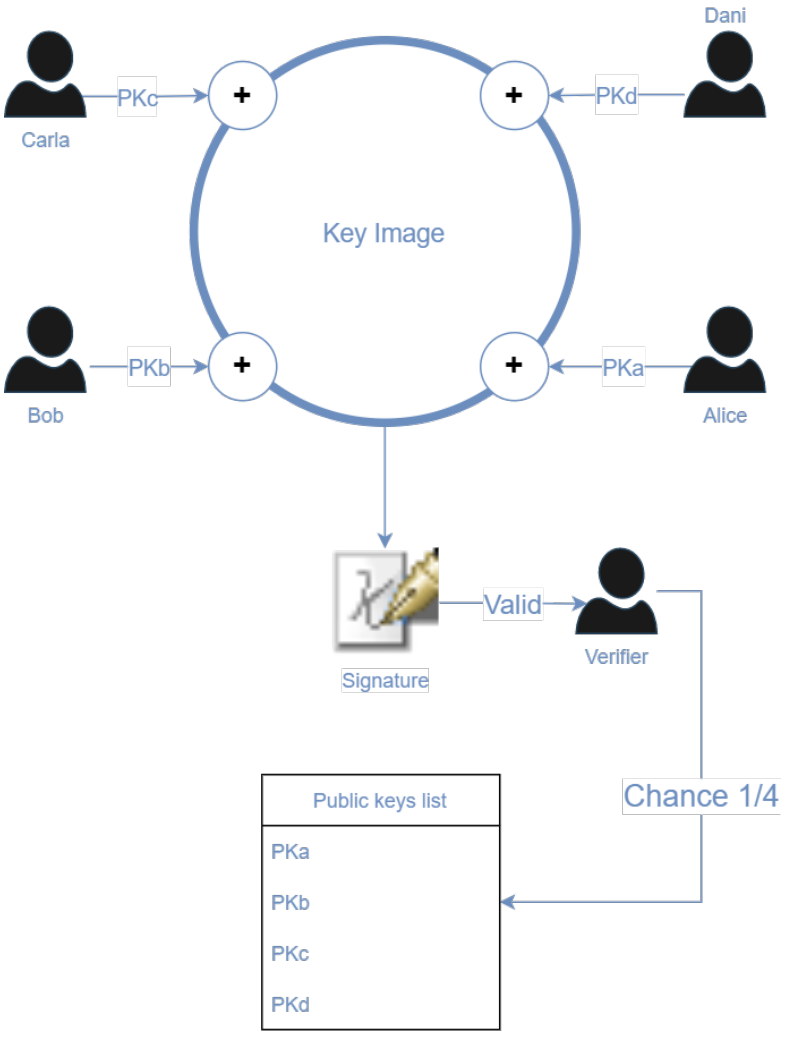

FIGURA 3.6: Imagen clave, creada a partir de una lista de las firmas de los usuarios Bob, Alice, Carla y Dani.

Para complementar el proceso de firma de transacciones en anillo y garantizar el anonimato de los actores dentro del sistema, se utilizan direcciones furtivas en los contratos inteligentes para identificar a los actores. Es imposible vincular estas direcciones a un usuario; sin embargo, un usuario puede identificar las direcciones

sigilosas que le pertenecen. Aprovechando las propiedades de las curvas elípticas (Roy Walker, 2018), una dirección stealth (P) se define mediante la ecuación (3.1):

$$P = F + S \tag{3.1}$$

donde F se define en (3.2), y S es la clave pública del receptor de la transacción.

$$F = Hash(rS) * G \tag{3.2}$$

donde r es una clave privada aleatoria generada por el actor que emite la transacción, y G es el punto base de la curva elíptica.

Para identificar qué dirección furtiva pertenece a un usuario, gracias a las propiedades de la ecuación (3.3), el actor puede hacer un hash del producto de la clave pública de la dirección (R) y su clave privada (s), luego hay que sumar la clave pública (S), y el resultado final es la dirección furtiva. Para que un usuario pueda demostrar que una dirección sigilosa le pertenece, necesita recuperar la clave privada única generada para esa transacción. Haciendo un hash del producto de la clave pública de la dirección furtiva (R) y la clave privada del usuario (s), y añadiendo después la clave privada s al hash obtenido, es posible recuperar la clave privada de un solo uso de la dirección (r). Entonces, es necesario firmar las transacciones de esa dirección con esa clave para demostrar la propiedad.

$$rS = rsG = rGs = Rs \tag{3.3}$$

donde R es la clave pública de la clave privada generada aleatoriamente, y s es la clave privada del receptor de la transacción.

El uso de estos protocolos aumenta la necesidad de potencia computacional de cada agente que hace uso de ellos. En la Figura 3.5, se puede estudiar el número de veces que cada agente debe escribir en la blockchain, haciendo uso de estos protocolos, dentro de un sistema basado en el marco propuesto. Los agentes sólo tienen que escribir la información en los siguientes casos:

1. Cuando se registran en el sistema y se almacena la información relacionada con ellos. En todo el ciclo de vida de la plataforma, esto ocurre una vez para cada agente.

2. Al final de cada hora, cada agente escribe en la blockchain el acuerdo alcanzado durante el proceso de negociación. Por ejemplo, si Alice llega a un acuerdo con Bob y Carla, entonces Alice tendrá que crear dos transacciones. En cambio, según el ejemplo, Bob y Carla sólo necesitan crear una cada uno. Este paso dependerá del número de agentes implicados, pero con los límites de tiempo propuestos –de 5 a 10 minutos– en una blockchain permisionada, es tiempo suficiente para no sobrecargar la red, los agentes, ni extenuar sus recursos computacionales. Por lo tanto, el rendimiento no se verá afectado con un incremento de los usuarios y la actividad.

3.3.3. Conclusiones y posibles mejoras

Este modelo, diseñado y desarrollado por (Mezquita, Gil-González, et al., 2022), propone una arquitectura innovadora de base tecnológica para una microrred inteligente totalmente distribuida y autónoma, la cual puede dar soporte a nuevas formas de negocio en el mercado energético inteligente. Con una tarificación independiente y dinámica entre los transactores de la red, la propuesta presentada permite crear un Mercado Local de Energía (MLE por sus siglas en inglés *Local Energy MArket*) para lograr la eficiencia en el transporte y la distribución de la energía frente al modelo de distribución tradicional.

En el contexto mencionado, este trabajo ha estudiado la implantación y desarrollo de microrredes inteligentes que permitirían la entrada de más entidades, cuyo objetivo es el autoconsumo y ganar dinero con el exceso de energía generada, como competidores en el mercado energético. Si es posible introducir más actores en el mercado de la energía que puedan competir por los ingresos en el mercado energético, la regularización de los precios ya no es necesaria. Dado que las transacciones de energía entre entidades de una microrred que están más cerca unas de otras son más baratas y mejores que las realizadas entre entidades lejanas, la ley de mercado de la oferta y la demanda funcionaría, haciendo innecesaria su actual regularización. Por último, se ha propuesto el uso de firmas en anillo y protocolos ZKP para asegurar la privacidad de los usuarios

y la protección de los datos almacenados dentro de la plataforma, cumpliendo así con el GDPR.

En la fase de redacción de esta Tesis Doctoral, la propuesta de arquitectura se encuentra en la fase de implementación como proyecto piloto. En términos generales, para futuros trabajos, esto permitirá el diseño de algoritmos de consenso *ad hoc* para el mercado energético. De este modo, será posible validar el modelo propuesto como una pauta estándar para plataformas similares. Esto contribuirá a reducir los costes de desarrollo y a fomentar la adopción del sistema por parte de empresas y particulares.

3.4. Conclusiones

Hoy en día, cada vez son más los ámbitos y campos en los que la tecnología blockchain tiene el potencial de disruptir. Esto es debido a que cada vez más se utilizan dispositivos IoT que se comunican de forma masiva entre sí, por lo que la aplicación de esta tecnología puede ayudar a evitar ataques a estos intercambios de información. Dentro del campo de la seguridad, también es posible de dotar a los sistemas de un canal de comunicaciones o de "tablón de anuncios" distribuido y que aumenta la resilencia de las plataformas, eliminando el punto único de fallo. Además, su naturaleza inmutable hace que sea imposible alterar los datos ya almacenados sin que los actores lo detecten.

Por otro lado, la tecnología blockchain no se queda sólo en realizar aportaciones a la seguridad e integridad de los datos. También permite el despliegue y aplcación de contratos inteligentes con los que controlar y gobernar el flujo de trabajo de una plataforma. De esta manera se democratizan los procesos, pasando a ser controlados por las entidades que funcionan en ellos, no sólo de una autoridad central. Además, esta democratización trae consigo la expulsión de todos aquellos intermediarios que encarecen un producto o servicio sin aportar valor real. Esto implica una mayor automatización de los procesos, con lo que conlleva una optimización tanto en costes como en tiempo de ejecución. Tras lo estudiado en este Capítulo, se pueden extraer las siguientes conclusiones:

- Un punto importante en este nuevo tipo de sistemas "democráticos", es que hay que tener en cuenta los **intereses de los actores en la plataforma**, y velar por

que el buen funcionamiento de la misma sea suficiente incentivo para que cada uno sólo quiera trabajar en pos de su bienestar.

En este sentido, las soluciones propuestas en la Sección 3.2 y la Sección 3.3 muestran los procedimientos seguidos para enfrentar este reto. En caso de que el análisis de seguridad y las asunciones realizadas no sean suficientes, es necesario crear un sistema de incentivos y castigos que, de alguna forma, sea suficiente para premiar los comportamientos deseables, mientras se hacen menos atractivos aquellos que no queremos que aparezcan en el sistema.

- Otro aspecto destacado es el del **almacenamiento y tratamiento de los datos** generados en este tipo de plataformas. Se puede conseguir que cada uno de los actores sea el dueño mismo de sus datos, algo que no sucede con los sistemas tradicionales. Sin embargo, estos datos también están expuesto al dominio de la red, por lo que la privacidad es violada en caso de que se almacenen datos sensibles.

  Por esta razón, en la Sección 3.3, se ha demostrado necesaria la aplicación de técnicas de criptografía y protocolos de barajeo de transacciones. Para lograr este objetivo, es necesario recurrir a los protocolos ZKP y a las firmas en anillo, para asegurar la privacidad en estos sistemas, manteniendo la posibilidad de trazabilidad de la información.

- Finalmente, en esta Tesis Doctoral se ha demostrado que la **aplicación de la tecnología blockchain a procesos de la industria** es viable y, además, proporciona una optimización de los mismos respecto a sus variantes tradicionales.

  Para conseguir los objetivos mencionados, a lo largo del presente Capítulo, se han mostrado aquellos puntos más relevantes sobre los que cualquier investigador o desarrollador que trabaje con plataformas basadas en tecnología blockchain va a necesitar tener en cuenta para llevar a buen puerto estos proyectos.

Capítulo 4

Evidencias y Resultados

VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

Capítulo 4

Evidencias y Resultados

Este Capítulo muestra las publicaciones en revistas científicas y congresos internacionales que han contribuido en el desarrollo de esta Tesis Doctoral y reflejan los resultados de las diferentes líneas de investigación que se han llevado a cabo. La Sección 4.1 expone los trabajos publicados en revistas científicas, conferencias y workshops internacionales, expuestas en orden cronológico inverso. La Sección 4.2 describe los proyectos en los que se ha participado y de los que se ha nutrido esta Tesis Doctoral. La Sección 4.3 detalla las estancias llevadas a cabo en organismos de investigación internacionales gracias a las cuales se ha profundizado en el desarrollo de esta Tesis Doctoral.

4.1. Publicaciones

En primer lugar, se detallan las diferentes publicaciones llevadas a cabo en revistas científicas internacionales, capítulos de libro, así como congresos internacionales y workshops, relacionadas con las líneas de investigación que han llevado a la elaboración de esta Tesis Doctoral. En cada bloque, se presentan las entradas en orden cronológico inverso según la fecha de publicación. En el caso de las revistas científicas internacionales, se señalan en **negrita** aquellas que forman parte de la Tesis Doctoral como compendio de artículos/publicaciones. Asimismo, se refleja en azul el factor de impacto[1] y el cuartil al que pertenece cada revista internacional según el año de publicación o, en su defecto, el último factor de impacto disponible antes de la publicación del artículo o, en caso de que la revista no contara aún con factor de impacto en la fecha de publicación, el factor de impacto del primer año calculado para la revista tras la publicación del artículo.

[1]Factor de impacto según el JCR – *Journal Citation Reports*.

4.1.1. Publicaciones en revistas científicas internacionales

1. González-Briones, A., Castellanos-Garzón, J. A., Mezquita Martín, Y., Prieto, J., & Corchado, J. M. (2018). A framework for knowledge discovery from wireless sensor networks in rural environments: a crop irrigation systems case study. *Wireless Communications and Mobile Computing.* [JCR 2.146 – Q2 (*2018*)].

2. Francisco, M., Mezquita, Y., Revollar, S., Vega, P., & De Paz, J. F. (2019). Multi-agent distributed model predictive control with fuzzy negotiation. *Expert Systems with Applications, 129, 68-83.* [JCR 8.665 – Q1 (*2019*)].

3. González-Briones, A., Mezquita, Y., Castellanos-Garzón, J. A., Prieto, J., & Corchado, J. M. (2019). Intelligent multi-agent system for water reduction in automotive irrigation processes. *Procedia Computer Science, 151, 971-976.* [CiteScore 3.6 (*2019*)].

4. Castellanos-Garzón, J. A., Mezquita Martín, Y., Jaimes Sánchez, J. L., López García, S. M., & Costa, E. (2020). A Genetic Programming Strategy to Induce Logical Rules for Clinical Data Analysis. *Processes, 8(12), 1565.* [Impact Factor 3.352 (*2019*)].

5. **Mezquita, Y., Casado-Vara, R., González Briones, A., Prieto, J., & Corchado, J. M. (2021). Blockchain-based architecture for the control of logistics activities: Pharmaceutical utilities case study. *Logic Journal of the IGPL, 29(6), 974-985.* [JCR 0.868 – Q2 (*2021*)].**

6. **Mezquita, Y., Parra-Domínguez, J., Pérez-Pons, M. E., Prieto, J., & Manuel Corchado, J. (2022). Blockchain-Based Land Registry Platforms: A Survey on Their Implementation and Potential Challenges. *Logic Journal of the IGPL.* [JCR 0.868 – Q2 (*2021*)].**

7. **Mezquita, Y., Gil-González, A. B., Martín del Rey, A., Prieto, J., & Corchado, J. M. (2022). Towards a Blockchain-Based Peer-to-Peer Energy Marketplace. *Energies, 15(9), 3046.* [JCR 3.252 – Q3 (*2022*)].**

4.1.2. Capítulos de libro

1. Mezquita, Y., Casado, R., Gonzalez-Briones, A., Prieto, J., Corchado, J. M., & AETiC, A. (2019). Blockchain technology in IoT systems: review of the challenges. En *Annals of Emerging Technologies in Computing (AETiC), Print ISSN, 2516-0281.*

2. Gazafroudi, A. S., Mezquita, Y., Shafie-khah, M., Prieto, J., & Corchado, J. M. (2020). Islanded microgrid management based on blockchain communication. En *Blockchain-based Smart Grids (pp. 181-193).* Academic Press.

4.1.3. Publicaciones en congresos internacionales y workshops

1. Valdeolmillos, D., Mezquita, Y., González-Briones, A., Prieto, J., & Corchado, J. M. (2019, June). Blockchain technology: a review of the current challenges of cryptocurrency. En *International Congress on Blockchain and Applications (pp. 153-160).* Springer, Cham.

2. Mezquita, Y., González-Briones, A., Casado-Vara, R., Chamoso, P., Prieto, J., & Corchado, J. M. (2019, June). Blockchain-based architecture: a mas proposal for efficient agri-food supply chains. En *International Symposium on Ambient Intelligence (pp. 89-96).* Springer, Cham.

3. Mezquita, Y., Gazafroudi, A. S., Corchado, J. M., Shafie-Khah, M., Laaksonen, H., & Kamišalić, A. (2019, October). Multi-agent architecture for peer-to-peer electricity trading based on blockchain technology. En 2019 *XXVII International Conference on Information, Communication and Automation Technologies (ICAT) (pp. 1-6).* IEEE.

4. Mezquita, Y., Alonso, R.S., Casado-Vara, R., Prieto, J., & Corchado, J.M. (2021). A review of k-NN algorithm based on classical and quantum machine learning. En *International Symposium on Distributed Computing and Artificial Intelligence* (pp. 189-198). Springer, Cham.

5. Mezquita, Y., Valdeolmillos, D., González-Briones, A., Prieto, J., & Corchado, J. M. (2019, July). Legal aspects and emerging risks in the use of smart contracts

based on blockchain. En *International Conference on Knowledge Management in Organizations (pp. 525-535)*. Springer, Cham.

6. Martín, Y. M., Parra, J., Pérez, E., Prieto, J., & Corchado, J. M. (2020). Blockchain-Based Systems in Land Registry, A Survey of Their Use and Economic Implications. En *CISIS, 2020, 13-22*.

7. González-Briones, A., Castellanos-Garzón, J. A., Mezquita-Martín, Y., Prieto, J., & Corchado, J. M. (2019, May). A multi-agent system framework for autonomous crop irrigation. En 2019 *2nd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6)*. IEEE.

8. Mezquita, Y., Gil-González, A. B., Prieto, J., & Corchado, J. M. (2021, October). Cryptocurrencies and Price Prediction: A Survey. En *International Congress on Blockchain and Applications (pp. 339-346)*. Springer, Cham.

9. Valdeolmillos, D., Mezquita, Y., & Ludeiro, A. R. (2019, June). Sensing as a service: An architecture proposal for big data environments in smart cities. En *International Symposium on Ambient Intelligence (pp. 97-104)*. Springer, Cham.

10. Mezquita, Y. (2019, June). Internet of things platforms based on blockchain technology: a literature review. En *International Symposium on Distributed Computing and Artificial Intelligence (pp. 205-208)*. Springer, Cham.

11. Castellanos-Garzón, J. A., Ramos, J., Martín, Y. M., Paz, J. F. D., & Costa, E. (2018, May). A genetic programming approach applied to feature selection from medical data. En *International Conference on Practical Applications of Computational Biology & Bioinformatics (pp. 200-207)*. Springer, Cham.

12. Mezquita, Y., González-Briones, A., Casado-Vara, R., Wolf, P., Prieta, F. D. L., & Gil-González, A. B. (2021, April). Review of privacy preservation with blockchain technology in the context of smart cities. En *Sustainable Smart Cities and Territories International Conference (pp. 68-77)*. Springer, Cham.

13. Mezquita, Y., Parra, J., Perez, E., Prieto, J., & Corchado, J. M. (2019, May). Blockchain-Based Systems in Land Registry, A Survey of Their Use and Economic Implications. En *Computational Intelligence in Security for Information Systems Conference (pp. 13-22)*. Springer, Cham.

14. Mezquita, Y. (2020, June). Public Tendering Processes Based on Blockchain Technologies. En *International Symposium on Ambient Intelligence (pp. 247-250)*. Springer, Cham.

15. Mezquita, Y. (2020, June). Energy Markets with Blockchain Technology. En *International Congress on Blockchain and Applications (pp. 161-164)*. Springer, Cham.

16. Domínguez, J. P., Pons, M. E. P., Martín, Y. M., & Rodríguez, J. M. C. (2020). Beneficios de la incorporación de la tecnología blockchain en el proceso de registro de la propiedad. En *Blockchain: Impacto en los sistemas financiero, notarial, registral y judicial (pp. 1029-1043)*. Aranzadi Thomson Reuters.

17. Castellanos-Garzón, J. A., Mezquita Martín, Y., Jaimes S, J. L., & López G, S. M. (2018, June). A Data Mining Approach Applied to Wireless Sensor Neworks in Greenhouses. En *International Symposium on Distributed Computing and Artificial Intelligence (pp. 431-436)*. Springer, Cham.

4.2. Proyectos

A continuación se listan los diferentes proyectos financiados a nivel europeo, nacional o regional en los que se ha participado como miembro del equipo investigador contratado en el transcurso del desarrollo de las investigaciones que han conducido a esta Tesis Doctoral, en orden cronológico inverso. Para cada uno de ellos, se detalla la entidad o entidades financiadoras, su localización, la entidad donde tuvo lugar el proyecto y su ubicación, el nombre del programa bajo el paraguas del cual se financió el proyecto, así como las fechas de inicio y fin del mismo.

1. TECTONIC: TEchnological Consortium TO develop sustaiNabIlity of underwater Cultural heritage

   - Modalidad de proyecto: De investigación fundamental (incluyendo excavaciones arqueológicas, etc.).
   - Ámbito geográfico: Unión Europea
   - Grado de contribución: Coordinador/a científico/a

- Entidad de realización: Universidad de Salamanca Tipo de entidad: Universidad
- Ciudad entidad realización: Salamanca, Castilla y León, España
- Nombres investigadores principales (IP, Co-IP,...): Mauro Francesco La Russa
- Entidad/es financiadora/s:
  a) Comisión Europea Tipo de entidad: Comisión Europea
  b) Ciudad entidad financiadora: Madrid, Comunidad de Madrid, España
- Tipo de participación: Coordinador
- Nombre del programa: H2020-MSCA-RISE-2019 (Marie Skłodowska-Curie Research and Innovation Staff Exchange)
- Cód. según financiadora: 873132
- Fecha de inicio-fin: 01/02/2020 - 31/01/2024 Duración: 4 años
- Entidad/es participante/s:
  a) 3D RESEARCH SRL
  b) CONSEJO NACIONAL DE INVESTIGACIONES CIENTIFICAS Y TECNICAS (CONICET)
  c) CONSIGLIO NAZIONALE DELLE RICERCHE
  d) FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS; MINISTERO PER I BENI E LE ATTIVITA CULTURALI
  e) PANEPISTIMIO PATRON
  f) PROLEXIA SARL
  g) SYNPO AKCIOVA SPOLECNOST
  h) UNIVERSITA DELLA CALABRIA
  i) VoXel Interaction Design
- Cuantía total: 1.062.600 € Cuantía subproyecto: 138.000 €
- Porcentaje en subvención: 100

2. CHROMOSOME: Change and analysis of consumer behaviour at smart homes via social machine

   - Modalidad de proyecto: De investigación fundamental (incluyendo excavaciones arqueológicas, etc.).

- Grado de contribución: Coordinador del proyecto total, red o consorcio
- Entidad de realización: Universidad de Salamanca Tipo de entidad: Universidad
- Ciudad entidad realización: Salamanca, Castilla y León, España
- Nombres investigadores principales (IP, Co-IP,...): Javier Prieto Tejedor
- Nº de investigadores/as: 4
- Entidad/es financiadora/s:
  a) Fundación Salamanca Ciudad de Cultura y Saberes Tipo de entidad: Fundación
  b) Ciudad entidad financiadora: Salamanca, Castilla y León, España
- Tipo de participación: Investigador principal
- Nombre del programa: Programa de Atracción del Talento
- Fecha de inicio-fin: 01/09/2018 - 31/08/2021 Duración: 3 años
- Cuantía total: 510.000 €

3. Grupo Operativo SOSTVAN: ESTRATEGIAS TECNOLÓGICAS PARA LA MEJORA DE LA SOSTENIBILIDAD DEL SECTOR GANADERO DE VACAS NODRIZAS (20190020007279).

   - Entidad/es financiadora/s: Fondo Europeo Agrícola de Desarrollo Rural (FEADER). Ministerio de Agricultura, Pesca y Alimentación.
   - Ciudad/es entidad/es financiadora/s: Bruselas (Unión Europea) y Madrid (España).
   - Entidad donde el proyecto tuvo lugar: Universidad de Salamanca.
   - Ciudad entidad donde el proyecto tuvo lugar: Salamanca (España).
   - Nombre del programa: Ayudas a la ejecución de proyectos de innovación de interés general por grupos operativos de la Asociación Europea para la innovación en materia de productividad y sostenibilidad agrícolas, dentro del Programa Nacional de Desarrollo Rural 2014-2020.
   - Fecha de inicio – Fecha de fin: 08/2019 - 06/2021.

4. PLATINUM: Plataforma horizontal de smart data y deep learning para la industria y aplicación al sector manufacturero (RTC-2017-6401-7).

- Entidad/es financiadora/s: FEDER / Ministerio de Ciencia, Innovación y Universidades – Agencia Estatal de Investigación.
- Ciudad/es entidad/es financiadora/s: Bruselas (Unión Europea) y Madrid (España).
- Entidad donde el proyecto tuvo lugar: Universidad de Salamanca.
- Ciudad entidad donde el proyecto tuvo lugar: Salamanca (España).
- Nombre del programa: Retos-Colaboración 2017.
- Fecha de inicio – Fecha de fin: 01/2018 – 06/2020.

5. El Aprendizaje-Servicio desde la base de la informática

   - Ciudad entidad realización: Salamanca, Castilla y León, España
   - Tipo de participación: Coordinador
   - Nombre del investigador/a principal (IP): Javier Prieto Tejedor
   - Importe concedido: 1.000 €
   - Entidad financiadora: Universidad de Salamanca Tipo de entidad: Universidad
   - Tipo de convocatoria: Competitivo
   - Ámbito geográfico: Universitaria
   - Fecha de inicio-fin: 01/09/2020 - 30/06/2021

6. Plataforma Inteligente para la evaluación del rendimiento académico

   - Ciudad entidad realización: Salamanca, Castilla y León, España
   - Tipo de participación: Coordinador
   - Nombre del investigador/a principal (IP): Javier Prieto Tejedor
   - Importe concedido: 1.500 €
   - Entidad financiadora: Universidad de Salamanca Tipo de entidad: Universidad
   - Tipo de convocatoria: Competitivo
   - Ámbito geográfico: Universitaria
   - Fecha de inicio-fin: 01/09/2019 - 30/06/2020

7. KokusAI Machine: Sistema de Soporte a la Decisión en la Internacionalización de PYMEs basado en algoritmos Machine Learning

   - Modalidad de proyecto: De investigación industrial Ámbito geográfico: Autonómica
   - Grado de contribución: Coordinador del proyecto total, red o consorcio
   - Entidad de realización: Universidad de Salamanca Tipo de entidad: Universidad
   - Ciudad entidad realización: Salamanca, Castilla y León, España
   - Nombres investigadores principales (IP, Co-IP,...): Javier Prieto Tejedor
   - Nº de investigadores/as: 5
   - Entidad/es financiadora/s: Junta de Castilla y León Tipo de entidad: Junta
   - Ciudad entidad financiadora: Valladolid, Castilla y León, España
   - Tipo de participación: Investigador principal
   - Nombre del programa: PRUEBAS DE CONCEPTO Y PROTECCIÓN DE RESULTADOS
   - Cód. según financiadora: PC-TCUE18-20_005
   - Fecha de inicio-fin: 18/12/2018 - 19/12/2019
   - Entidad/es participante/s: Glocal Asian
   - Cuantía total: 9.840 €
   - Porcentaje en subvención: 100

8. Eco-Rural-IoT: Application of techniques and intelligent algorithms aimed to reduce the consumption of power and water in mixed farming environments by means of IoT devices.

   - Entidad/es financiadora/s: Comisión Europea – TETRAMAX (H2020-EU.2.1.1.-761349).
   - Ciudad/es entidad/es financiadora/s: Bruselas (Unión Europea) y Aachen (Alemania).
   - Entidad donde el proyecto tuvo lugar: Nebusens, S.L.
   - Ciudad entidad donde el proyecto tuvo lugar: Salamanca (España).

- Nombre del programa: TETRAMAX-VALUECHAIN-TTX-1.
- Fecha de inicio – Fecha de fin: 09/2018 – 10/2019.

9. IOTEC: Development of technological capabilities in the industrial application of the Internet of Things (IoT).
   - Entidad/es financiadora/s: European Regional Development Fund (ERDF) within the framework of the Interreg program V-A Spain-Portugal 2014-2020 (PocTep).
   - Ciudad/es entidad/es financiadora/s: Bruselas (Unión Europea).
   - Entidad donde el proyecto tuvo lugar: Universidad de Salamanca.
   - Ciudad entidad donde el proyecto tuvo lugar: Salamanca (España).
   - Nombre del programa: Interreg program V-A Spain-Portugal 2014-2020 (PocTep).
   - Fecha de inicio – Fecha de fin: 07/2016 – 06/2019.
10. Dream-GO. Enabling Demand Response for short and real-time Efficient And Market based smart Grid Operation - An intelligent and real-time simulation approach. H2020-MSCA-RISE-2014, MSCA-RISE-2014, SEP-210162060. Grant Agreement number 641794.
    - Entidad/es financiadora/s: Comisión Europea.
    - Ciudad/es entidad/es financiadora/s: Bruselas (Unión Europea).
    - Entidad donde el proyecto tuvo lugar: Nebusens, S.L. Ciudad entidad donde el proyecto tuvo lugar: Salamanca (España).
    - Nombre del programa: H2020-MSCA-RISE-2014.
    - Fecha de inicio – Fecha de fin: 02/2015 – 01/2019.

4.3. Estancias internacionales

A continuación se detalla las estancias internacionales llevadas a cabo fuera de España en instituciones de enseñanza superior de prestigio, realizando trabajos de investigación relacionados con esta Tesis Doctoral.

1. Blockchain Lab:UM (Univerza v Mariboru).

    - Maribor, Eslovenia.
    - Fecha de inicio – Fecha de fin: 02/03/2020 – 01/07/2020
    - Tareas desarrolladas: trabajo en el proyecto Platinum, estudio del estado del arte en el ámbito de las criptomonedas, estudio sobre los retos que afrontan las criptomonedas y los proyectos públicos basados en tecnologías distribuidas como la tecnología blockchain.

    Como resultado de dicha estancia se originaron publicaciones, como Domínguez, Pons, Martín, & Rodríguez (2020); Mezquita, Gil-González, Prieto, & Corchado (2021); Mezquita, González-Briones, et al. (2021).

2. 3D Research s.r.l.

    - Rende (CS), Italy
    - Fecha de inicio – Fecha de fin: 06/09/2022 – 04/11/2022
    - Tareas desarrolladas: trabajo en el proyecto TECTONIC, estudio de líneas de trabajo futuro y finalización de escritura de esta Tesis Doctoral.

1. Blockchain Lab:UM (Univerza v Mariboru).

    - Maribor, Eslovenia.
    - Fecha de inicio – Fecha de fin: 02/03/2020 – 01/07/2020
    - Tareas desarrolladas: trabajo en el proyecto Platinum, estudio del estado del arte en el ámbito de las criptomonedas, estudio sobre los retos que afrontan las criptomonedas y los proyectos públicos basados en tecnologías distribuidas como la tecnología blockchain.

Capítulo 5

Publicaciones acreditativas de la investigación realizada

VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

Capítulo 5

Publicaciones acreditativas de la investigación realizada

Al tratarse de una Tesis Doctoral por compendio de artículos/publicaciones, el presente Capítulo recoge las publicaciones originales que el desarrollo de esta investigación ha generado. La Sección 5.1 incluye, en primer lugar, un artículo que presenta un *framework* para el desarrollo de una plataforma multiagente basada en blockchain, que optmizaría los procesos logísticos mediante el uso de contratos inteligentes, utilizando un caso de estudio de la industria farmacéutica como ejemplo (Mezquita, Casado-Vara, et al., 2021). La Sección 5.2, por su parte, presenta un artículo que describe, de forma detallada, una revisión del estado del arte y los retos existentes a la implementación en el mundo de la administración electrónica de las plataformas basadas en blockchain (Mezquita, Parra-Domínguez, et al., 2022). Finalmente, la Sección 5.3 expone una publicación que presenta un framework para el diseño e implementación de una plataforma distribuida basada en la tecnología blockchain y que permite la creación de mercados automáticos de energía en entornos locales, aunando todo lo estudiado durante la tesis y haciendo frente a todos los retos que una plataforma de este tipo se enfrenta actualmente, no sólo en el ámbito tecnológico, sino también regulatorio (Mezquita, Gil-González, et al., 2022).

5.1. Blockchain-based architecture for the control of logistics activities: Pharmaceutical utilities case study

Autores: Yeray Mezquita[a], Roberto Casado-Vara[a], Alfonso González Briones[a], Javier Prieto[a], Juan M. Corchado[a].

Afiliaciones:

[a]BISITE Research Group, University of Salamanca, Edificio I+D+i, C/ Espejo, Salamanca 37007, Spain.

Publicado en: *Logic Journal of the IGPL, Volumen 29*(6), pp. 974–985.

D.O.I.: `https://doi.org/10.1093/jigpal/jzaa039`

Fecha de publicación: 08 September 2020.

Factor de Impacto: 0.868 - Q2 (*2021*).

5.1.1. Introducción

La logística se ocupa del transporte de productos entre las partes. Actualmente es un área importante para las empresas. Sin embargo, el problema de este sector es que su escala puede provocar retrasos e incumplimientos en la entrega de mercancías, así como otras cuestiones. Además, los grandes distribuidores necesitan un gran volumen de trabajadores para satisfacer la gran demanda de las tiendas. Todo esto puede contribuir a que se produzcan grandes retrasos en la tramitación de los pedidos y aumenta la posibilidad de perder algunos de ellos T. Li et al. (2016). Para intentar solucionar este problema, las empresas han automatizado todos sus procesos, lo que ha contribuido a un aumento significativo del número de empresas y distribuidores en el sector de la logística. Sin embargo, el aumento de la cantidad de datos digitalizados y la expansión de las empresas en Internet, hace que el riesgo de ataques a sus bases de datos sea también mayor. Los piratas informáticos pueden intentar modificar, robar o borrar los datos almacenados (Lima et al., 2015). En este trabajo proponemos un nuevo modelo que hace uso de la tecnología blockchain, los contratos inteligentes y un sistema multiagente para proteger los datos del sector logístico Tapia, Fraile, Rodríguez, Alonso, & Corchado (2013) al tiempo que agiliza las actividades logísticas. Además, el sistema multiagente es

capaz de coordinar todos los servicios logísticos González-Briones, Castellanos-Garzón, et al. (2018), mejorando la eficiencia del sector logístico.

El modelo propuesto en este artículo Mezquita, Casado-Vara, et al. (2021) es capaz de proteger los datos generados dentro de la plataforma para que no sean manipulados gracias al uso de la tecnología blockchain. Además, con el uso de contratos inteligentes para controlar el funcionamiento de la plataforma es posible eliminar intermediarios que no aportan valor al producto. Los retos en sistemas logísticos como los retrasos en la entrega, la pérdida de documentación, el desconocimiento de la procedencia de los productos, los errores humanos, etc., pueden minimizarse e incluso evitarse con la implementación de la tecnología blockchain. Con los mecanismos de seguridad que otorga el uso de esta tecnología, es posible crear un marco de comunicaciones de confianza entre los actores de la plataforma, protegiendo el sistema frente a ciberataques como el *phishing* y el *man in the middle* Khan & Salah (2018); Kshetri (2017).

5.1.2. Objetivos

Este trabajo se enmarca dentro de las diferentes investigaciones y experimentaciones que se han realizado sobre soluciones que combinan tecnologías IoT, entornos multiagente, y tecnología blockchain. Gracias a estos trabajos se han podido identificar los requisitos técnicos necesarios para la implementación y despliegue de este tipo de sistemas los cuales han servido cómo base del resto de investigación realizada en esta tesis. En este sentido, los objetivos concretos perseguidos por la investigación recogida en esta publicación incluyeron, por tanto:

- Investigar el uso de la tecnología blockchain en el ámbito logístico, qué puede aportar y qué retos afronta.
- Identificar los requerimientos existentes en entornos IoT y sistemas multiagentes para poder combinarlos con la tecnología blockchain.
- Diseñar una arquitectura multicapa para el framework basada en organizaciones virtuales distribuidas, mediante el uso de agentes flexibles y adaptables, que permita cubrir las necesidades de gestión del sistema de una forma optimizada respecto a las aquitecturas tradicionales.

- Implementar contratos inteligentes que ofrezcan fiabilidad a las diferentes partes del sistema cuando interactúen entre sí, haciendo uso de un sistema de penalizaciones a las partes implicadas que no cumplan con los contratos estipulados.

5.1.3. Conclusiones

Este trabajo presentó un nuevo enfoque en el uso de contratos inteligentes para mejorar los servicios logísticos en el entorno de la industria farmacéutica. La novedad de este trabajo radica en el uso de la tecnología blockchain para el almacenamiento de todos los intercambios de información del sistema y habilitar la utilización de contratos inteligentes. El modelo propuesto hace uso de los contratos inteligentes para gestionar de forma más eficiente todo el proceso logístico. Gracias a esta automatización, los intermediarios humanos que no aportan valor al producto dejan desaparecen.

Otra novedad de este trabajo es el uso de agentes que verifican que ambas partes se atengan a los términos de un contrato inteligente. Si los agentes detectan que alguna de las partes no cumple con las condiciones establecidas, se impone una penalización y los agentes guardan el dinero en la entidad de control hasta que se cumplan las condiciones acordadas. Esto hace que nuestro modelo sea más eficiente que los modelos tradicionales. Además, es capaz de seguir y autentificar los pedidos. Se introduce un modelo de penalización por incumplimiento de los contratos inteligentes.

Nuestro modelo puede ser utilizado para mejorar cualquier sistema logístico que aún dependa de intermediarios humanos que verifiquen pagos y/o transacciones entre terceros. Es altamente eficiente y seguro porque está automatizado por el sistema multiagente y el uso de los contratos inteligentes. Al incorporar blockchain dotamos al sistema logístico de sólidas características de seguridad, sobretodo en el ámbito de la trazabilidad de la información y la identificación de los actores que intervienen. Los envíos pueden ser rastreados, el origen y los destinos autentificados, y la prueba de todas las transacciones puede ser almacenada y mantenida inalterada dentro de la cadena de bloques.

Blockchain-Based Land Registry Platforms: A Survey on Their Implementation and Potential Challenges

YERAY MEZQUITA*, *BISITE Digital Innovation Hub, University of Salamanca, 37007, Salamanca, Spain.*

JAVIER PARRA-DOMÍNGUEZ, *BISITE Digital Innovation Hub, University of Salamanca, 37007, Salamanca, Spain.*

MARÍA E. PÉREZ-PONS, *BISITE Digital Innovation Hub, University of Salamanca, 37007, Salamanca, Spain.*

JAVIER PRIETO, *BISITE Digital Innovation Hub, University of Salamanca, Salamanca, Spain and AIR Institute, IoT Digital Innovation Hub, Salamanca, 37007, Spain.*

JUAN MANUEL CORCHADO, *BISITE Digital Innovation Hub, University of Salamanca, Salamanca, Spain and AIR Institute, IoT Digital Innovation Hub, Salamanca, 37007, Spain.*

Abstract

In recent years it has been demonstrated that the use of the traditional property registry models involves the risk of corruption along with long waiting times. This paper points out the main problems associated with conventional models and makes a survey of the new ones that are based on blockchain technology. This type of model is already being developed as a proof of concept by different countries. With the use of this technology in land registry systems, it is possible to improve the transparency of the processes as well as optimize costs and execution time. To show the theoretical results of this study, the Spanish land registry has been taken as an example of a use case scenario.

Keywords: Blockchain, land registry, e-government, challenges, survey.

1 Introduction

One of the concerns of governments today is the optimization of the bureaucratic processes carried out in property registry systems. This optimization is understood as the improvement in the profitability of their management, the increase in the speed at which those processes are carried out and the reduction of the ambiguities that occur in the processing of data [26]. The e-government concept, based on the precepts of optimization and reduction of ambiguities, is beginning to develop into a bureaucracy. Through the internet it is possible to provide the different governments

*E-mail: yeraymm@usal.es

Vol. 00, No. 0, © The Author(s) 2022. Published by Oxford University Press.
https://doi.org/10.1093/jigpal/jzac010

with features such as standardization, departmentalization, operational profitability, construction of coordination networks, collaboration with external entities and citizen services [30, 32, 34].

In today's industry, several models are being applied to allow for the automation and distribution of their processes, obtaining very good results [8, 10]. To fully achieve the automation and distribution of processes in the registry field, e-governments must make use of a technology that provides the system with a unique and immutable registry, the blockchain [21]. The study of the use of blockchain technology has been extended to many areas, beyond those underlying the economy of the so-called cryptocurrencies (Bitcoin, Ethereum, EOS, Tron) [33], especially for the areas that use some type of record, such as in the identification of objects in a unique way [20, 27], for the traceability of assets [24], for the audit of insured goods [9, 29] or in the creation of data markets between machines [5, 23, 35].

One of the main aspects by which the use of blockchain technology is spreading to so many different areas is the possibility of implementing smart contracts, which can be automated, eliminating the need for a human intermediary [25]. Since the code of these contracts is stored in the blockchain in an immutable way, and each one of its executions is verified by the set of nodes that make up the blockchain network, it becomes feasible to automate processes that involve actors with different interests who do not trust each other. The studies developed to date in e-government all provide a sufficiently powerful tool for local governments to reinvent themselves, deepening, in this case, the e-government paradigm. Thanks to the supportive structure that blockchain technology offers, e-governments can provide the citizens with automated processes, like the management of digital identification and the safe handling of documents [36]. It is precisely in the latter where, as a platform for various applications in e-government, blockchain technology shows great potential to authenticate and properly store different types of documents, such as property records, birth and marriage certificates, vehicle registration, (business) licenses, educational certificates, student loans, social benefits and votes cast in any election process [28].

Specifically, the current work focuses on the advantages of applying blockchain to the property registry process, mainly following the strategic precepts of transparency, understood as the democratization of the access to different data and the reduction of corruption through distributed storage; economic cost reduction, due to the realization and validation of a transaction without human intervention; and the technological precepts of resilience and security of the data.

This work contributes with (i) a review of the pilots currently being developed with different governments around the world, in the context of blockchain-based land registries; (ii) the potential benefits of a platform like this being implemented in a country like Spain; and (iii) the natural evolution of the e-government paradigm towards the use of this kind of systems is discussed, along with the challenges that are faced. Because of all the contributions achieved with this paper, public and private researchers and practitioners alike will benefit from this work.

This introduction is followed by a review of the studies that have been conducted around the world with blockchain-based systems on different land registries, in Section 2. Then, the research development is established, where current times and costs are detailed, in Section 3. Finally, the research is discussed in Section 4 and the conclusions are drawn in Section 5.

2 Blockchain and land registry around the world

Each country has its property registry system, and this section will address property registration cases that use blockchain technology or are in the process of adopting this system. Blockchain technology can be applied in many legal fields [1], and, although it will not be discussed in this paper, blockchain technology has also been proposed as a tool to solve legal issues with displaced

persons or refugees, not only as a regulatory agency for countries but also to solve transaction costs for displaced persons or for receiving aid for refugees and cross-border collaborations.

By 2017, more than half of all households in developing countries have access to the Internet, so they can make a model based on blockchain technology viable [18]. In Africa, e.g. we find the case of Ghana. In countries like this, which are less developed and where the political situation is quite unstable, it is not strange that there are cases of corruption in terms of citizens' property. In this kind of situation, where the government's corruption rates are very high, government officials alter titles to registered properties by assigning them to others or themselves. In the case of developing countries, another factor that reinforces this problem is the fact that citizens do not have easy access to information. Although it is not only a question of access to information, it is also a challenge for the African country since around 90% of the land is not officially registered [12].

Ghana is one of the countries that has promoted and joined the blockchain project together with multinational companies that have been working for years in the blockchain sector, along with local startups that know about the area and the possible disadvantages that may exist. In the case of Ghana, they are working hand in hand with IBM and Bitland [2] to modernize and make the land registry immutable. They use *OpenLedger* to create a distributed public blockchain, which more companies are expected to connect to over time.

Blockchain technology is also beginning to be applied at the government level in Asia. In particular, Japan, which is seeing the feasibility and implications of using this technology. The government of Japan is developing projects on the uses of blockchain technology for property registration and the management and unification of all procedures related to the property registry [17].

The intention of using blockchain technology in Japan is to unify all data on empty or unowned properties, land and unproductive spaces, unknown owners and unidentified tenants or users before agencies. The consolidation of these data and their availability to all relevant agencies through the blockchain contribute to the advancement of several national objectives, such as encouraging land reuse, promoting sale and purchase, controlling redevelopment, optimizing tax collection and designing plans related to the environment. Although there is no more information about the trials carried out in different Japanese cities since the summer of 2018, it is expected to cover all of Japan in 2022 [7].

Within the context of Sweden, banks and state authorities have access to the land registry's database, while the seller and buyer, the most important stakeholders of a land transaction, do not have that privilege. Because of that, the government is aiming at the implementation of a land registry system based on blockchain, where all the actors of a transaction have the same privileges [19]. However, to be able to carry out the change in registry access in the legal fields and in the registration of all its properties [13], there must be a legal modification.

In June 2016, the Swedish property regulator published a report under the title 'The Land Registry Blockchain'. It was part of a project on the possibilities of using blockchain as a technical solution for real estate transactions. The project focused on the contracting process because currently, and according to its legal system, it consists of two steps: a contract sale and a deed of sale (the former can be registered as a pending sale and the latter as the final sale). In its current state, the process from the signing of a contract to the registration of the deed of sale takes between 3 and 6 months. Even so, in the signing process, many documents are signed on paper and sent by ordinary mail, so digital signatures and identification will be a component of the project (which requires investment in time and money).

Updates in the land registry must be checked by the regulatory authority and, in a long-term solution, the land registry will remain in charge of enforcing the law. The final aim is that, with the use of a *permissioned* blockchain in its proof of concept, the process of adding information is

centralized in the state, while still offering a high level of transparency. In this case, the blockchain is called *permissioned* because only a limited number of actors, from the registration agency, can approve the blocks of data that are going to be stored in the blockchain. Besides, this blockchain is open because all Swedish citizens have access to the information stored in it. The Swedish project is an example of blockchain as a technology adapted to registration, not a new category of property registration, but as modernization and adaptation of new technologies towards legal efficiency.

On the other hand, Georgia is a country that has begun a project to create a land registry system based on blockchain technology in 2016 and, since then, the National Public Registry Agency continues to act as a third-party enforcer [31]. Today, titles can be issued in digital format and recorded using blockchain technology. However, the process is not fully automated, the stakeholders have to go to the offices of the government to get the certificate of the land before making a transaction with it. Also, the blockchain technology used is just a layer of tamper-proof security with the Bitcoin blockchain, used by the government. This means, the process is still centralized by the government and is not an automatic process [14].

A blockchain property registry has been proposed as a solution for the states with an institutional deficit, as it is believed that a low cost 'property' certificate can be issued from a computer. However, a 'real right', effective against all law, needs an institutional infrastructure to protect it. Without legal institutions there is no 'real right' or property, but rather expectations, social norms, facts or possession. If the owner cannot go to court to claim or defend their right, its existence is doubtful. In the case of Georgia, its legislative framework allows for the implementation of this kind of solution because it has enough flexibility to let the government store their citizen's data [14].

As mentioned in the previous cases, each country finds different incentives that lead them to opt for the use of blockchain technology, see summary in Table 1. These technologies have different purposes but they converge in the fact of the need for a more immutable and effective property registry and use blockchain technologies as a lever for it. This way, the land registry and legal entities, in general, ensure maximum security in the documents, as well as get rid of possible cases of corruption. The daily market transaction sequence rule [16], concerning the rights over individual land or title registries have been a feature of title registry systems as opposed to the original deed systems where this rule was unknown. This new rule improves the security status of the land registry by limiting access to persons who can consult or extract information. According to this rule, the property registry cannot be entered if the person concerned is not registered as the authorized person. The land registrar must check that the registered person has given his consent or has been part of a legal procedure.

To summarize, making use of blockchain technology as a storage system in which the information generated, along with the smart contracts containing the logic to govern the platform, are stored in a distributed database, allowing governments to create a public ledger of transactions that is transparent to all citizens and a proven anti-corruption mechanism. Besides, the use of digital signatures in the communication protocol and a time-stamped fingerprint of the data, obtained with a hashing algorithm, as a mechanism for validating the information, are very powerful tools for preserving the kind of files generated in land registry systems. Also, the use of a network of nodes as the keeper of the information facilitates its retrieval under any circumstances, due to getting rid of a single point of failure of centralized systems.

3 Benefits of blockchain technology in land registry

This paper focuses on the benefits and contributions that the use of blockchain technology in land registries would have if used in the case of the Spanish land registry system. To reap the benefits

TABLE 1. Summary of studied frameworks per country.

Country	Framework summary
Ghana [2, 12]	In the case of Ghana, they are working hand in hand with IBM and Bitland to modernize and make the land registry immutable. They use *OpenLedger* to create a distributed public blockchain, which more companies are expected to connect to over time.
Japan [7, 17]	The intention of using blockchain technology in Japan is to unify all data on empty or unowned properties, land and unproductive spaces, unknown owners and unidentified tenants or users before agencies. Although there is no more information about the trials carried out in different Japanese cities since the summer of 2018, it is expected to cover all of Japan in 2022.
Sweden [13, 19]	To be able to carry out the change in registry access in the legal fields and in the registration of all its properties, there must be a modification in the Swedish legislation. The final aim is that, with the use of a *permissioned* blockchain in its proof of concept, the process of adding information is centralized in the state, while still offering a high level of transparency. Besides, this blockchain is open because all Swedish citizens have access to the information stored in it. The Swedish project is an example of Blockchain as a technology adapted to registration, not a new category of property registration, but as modernization and adaptation of new technologies towards legal efficiency.
Georgia [14, 31]	Georgia has begun a project to create a land registry system based on blockchain technology in 2016. Today, titles can be issued in digital format and recorded using blockchain technology. However, the process is not fully automated, the stakeholders have to go to the offices of the government to get the certificate of the land before making a transaction with it. Also, the process is still centralized by the government and is not fully automated. A blockchain property registry has been proposed as a solution for the states with an institutional deficit, as it is believed that a low cost 'property' certificate can be issued from a computer. However, a 'real right', effective against all law, needs an institutional infrastructure to protect it. Without legal institutions there is no 'real right' or property, but rather expectations, social norms, facts or possession. In the case of Georgia, its legislative framework allows for the implementation of this kind of solution because it has enough flexibility to let the government store their citizen's data.

of using a blockchain-based platform for the optimization of the Spanish land registry system, the general architecture must be as described in Figure 1. In that figure, one observes that the system is governed by the smart contracts deployed within the blockchain: (i) a buyer (citizen who wants to buy a property) reaches an agreement with a seller (a citizen that wants to sell the discussed property) on the price of the land; (ii) the buyer then applies for a credit to the bank and pays the agreed money to the seller; (iii) a set of smart contracts then reflects the transaction and they are in charge of updating the information of the paid credit to the bank; (iv) when the credit payment is finished, a smart contract raises an alarm with the information of the property for the government; (v) and finally, the government issues the certificate with the legal rights of the buyer as the current

6 *Blockchain-Based Land Registry Platforms*

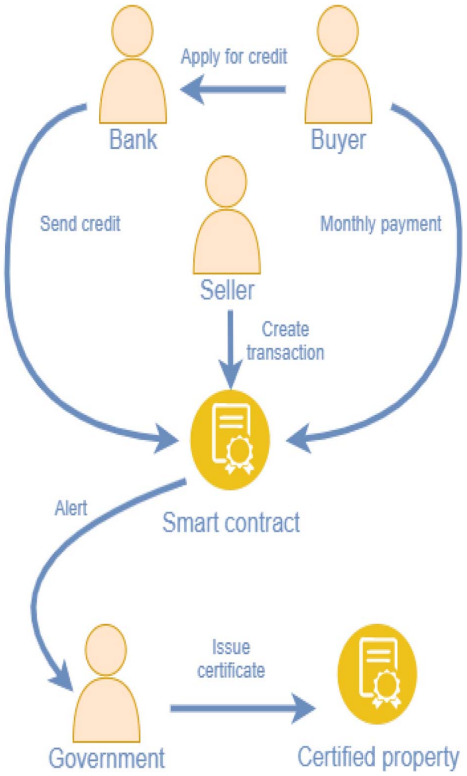

FIGURE 1. Generic model for optimizing land registry processes.

owner of the property. Being the blockchain network the main element of the system it is possible to create a democratic, tamper-proof and transparent platform [22].

One of the possibilities of how blockchain technology can be theoretically used in the Spanish land registry is to make use of an external public blockchain as a service. In those kinds of blockchains, it is not restricted access to the networks, therefore they are prone to attacks and need strong consensus algorithms to gain resilience against them. A public Bitcoin blockchain is used in the case of Georgia. However, it is only used as a tamper-proof security layer and as a governor of the platform. The issuance of certificates to be signed by the parties is done through the government, so it is not used for the democratization of the process. On the other hand, because state personnel is involved, the automation of the process is not achieved either [14].

To add new blocks of transactions, in the case of the Etherum and Bitcoin public networks, the Proof of Work (PoW) consensus algorithm is being used. The PoW algorithm avoids the spamming of false data inside the blockchain, by making solving it more computationally expensive than verifying it. Although, as shown in Figure 1, the platform should be governed by Turing-complete smart contracts, so in this case, blockchain networks like Bitcoin cannot be used. The main problem of PoW consensus algorithms is that they spent a great amount of energy, so alternatives like Proof of Stakeand Delegated Proof of Stake have arisen in other public blockchains [33]. Either way, in the case that the low latency of these networks does not allow for the deployment of a platform of this

scale, it would be possible to create a public blockchain with the nodes of the Spanish estate and the individuals and companies that want to take part in the process.

Another possibility is to use a permissioned blockchain network, in which the nodes that manage it are identified and have well-defined roles inside the network. Thanks to this approach it is not necessary to use energy-eager and low-latency consensus algorithms, because the nodes of the network are known and reliable. On the other hand, the system will be more centralized, but as in the case of Ghana, it can be expected that the network will grow as time passes with the addition of nodes managed from different sources.

In every technological scenario, the private data of a person cannot be stored publicly because of data protection laws. Therefore, the Spanish estate has to continue managing and storing that information on its private servers.

For our study, we have selected three variables that have a direct and immediate effect in the case that the blockchain technology is applied to the Spanish land registry. The current situation is then compared with what is expected.

3.1 Time

This point details the time needed to be able to carry out a query or make a record. It is based on the minimum formal times excluding any anomaly that might occur. At present, there are some special dispatch periods such as for the legalization of the minutes books of Communities of Owners, set at 5 working days if there is no incidence, or for the issue of certificates, set at 4 working days per property, in the same circumstance of lack of incidence.

In addition to the 15 working days for the formalization of the said register, the time for consultation or request may vary and may also be extended if it is or is not accepted or modifications have to be made. In the case that blockchain technology is used, the registration or consultation is immediate. In a matter of seconds, the transactions can be carried out. Even in the worst-case scenario, in a high-latency public network, the registration can be done in a matter of hours, an incredible upgrade compared to the days that have to pass with the current system.

3.2 Economic resources

In this section, we detail only the part of economic resources at the level of fees or direct cost of registering a property. The costs derived from waiting times, travel or other indirect costs that occur with legal processes in Spain today is taken into account. Currently, in any case, the price of registration will never be less than 24.04 euros or more than 2,181.67 euros. The cost per transaction is in the order of cents, as it does not require either labour or printed certificates.

3.3 Inconsistencies and corruption

This point details some inconsistencies that may emerge in the registration process due to the human factor, in addition to corruption and possible advantageous movements of properties associated with changes of government. With blockchain, any change or alteration is recorded so that it is always possible to check and see if any discordance has occurred. Another inconsistency that may exist are the differences between the property registry and the cadastre. There have been many political cases of corruption that appear every year with the property registry [3, 4, 6, 11].

4 Discussion

The evolution of society and new technologies makes it clear that there is a need for government systems that, although they have different characteristics, all see the light under the paradigm of incorporating new forms of governance, e-government. One of the supports of the new paradigm is the use of blockchain technology, where the fight against corruption and cost reduction are conformed as guarantees of this technology, but it is precisely in conjunction with the different governments where both fields have to be properly adapted.

In the first place, in the development of blockchain technology linked to the property registry, it is important to know about the existence of certain flexibility that requires precisely a solid governance of the network. These types of governments also need to be able to adapt to changes in functions such as data management and the responsibility of governments themselves [14]. Secondly, it is important to note that more research is needed to create trust, disintermediation, organizational transformation and governance models under new e-government designs [22]. Thirdly, it should be borne in mind that the incorporation and adaptation to this type of technology, which is still under development, requires periodic audits so that the evolving technology and the forms of government that in turn adapt to it are aligned, mitigating possible undesirable consequences for society [21].

In the research carried out in this work, we have identified some must-have features for a blockchain-based land registry platform: (i) blockchain technology can enable a decentralized platform and bring with itself democracy to the data, but, if not used properly, it is just a facade to of false protection, like in the case of Georgia where security risks of data tampering remain [14]; (ii) it is needed that the regulation of a country covers the use of digital self-enforcing contracts, or smart contracts, to allow the self-governance of the platform while legally covering failures in the execution of a smart contract [25]; and (iii) the private data of the citizens must be protected by the government while ensuring the proper life cycle of the platform.

Finally, and in addition to the above, it is worth noting the evolution towards distribution and decentralization that computer systems are following over the years. In this evolution, three well-differentiated stages can be observed:

- The first and traditional stage of these systems consists of the use of a centralized data system in which a single owner is in charge of adding, modifying and deleting the data generated within a platform. The rest of the users are exposed to the decisions that this owner has with his data. These systems include the vast majority of current applications, such as Google Drive or Facebook.
- The next and logical evolutionary step for computer systems is when user data is not exposed to the discretion of an owner. It occurs when blockchain technology is used in a computer system to maintain records in which users need to have confidence that they have not been manipulated after their creation. However, their governance, which depends on the proper functioning of the smart contracts that underlie the functionality of these systems, is generally in the hands of a single organization. Examples of these systems are in the area of decentralized applications created in Ethereum or Tron. This step is also taken by governments that want to make use of blockchain technology for the implementation of automated land registration. Although the data generated is controlled in a decentralized and distributed way within a network of independent nodes controlled by different entities, the way to govern such an application, and therefore how users can interact with it, is decided by a single organization.
- The last stage identified is where the governance of a system is given by the users themselves. They can interact with each other directly without the need for intermediaries. Besides, the control of the data generated in the platform is decentralized and distributed in the same way as

in the previous step. These systems are achieved through the use of smart contracts that allow users to be part of the government when some condition is met and how this government can change the way applications work. But for such a system to be adopted by a state, this kind of technological advance must be taken into account by the legislation of the countries. For the described reasons, the European Directive on Information Society and Electronic Commerce [15] has established in its article 34 that every member state of the European Union must adjust its legislation on contracts that are executed by electronic means. This should enable corporate governance through this type of system and the use of intelligent contracts.

5 Conclusions

Although the concern of the different estates has always been to comply with the appropriate criteria of efficiency, these criteria are helped by the monitoring and compliance with certain protocols linked, some of them, to the rise of new technologies. The so-called e-government paradigm includes different protocols that go deeper into the idea of approaching services and bringing them closer to citizens, and blockchain technology is part of this. It is at this point that this work highlights the importance of this technology in the proper development of certain public policies. Specifically, this study focuses on the process of property registration.

Aware that there are already different countries that apply blockchain technology to the tracking of property-related records, although in a pilot way, we have observed that it has been possible for property registration organizations to reduce their intermediary role and to focus on the development, maintenance and governance of the application of blockchain technology to the platforms and applications that serve citizens. Understanding the previous results as positive for public governance, the involvement in the progress towards transparency, among other characteristics that support good governments, is more than clear and determined if they start applying the most disruptive technologies.

To conclude this work, we have to note that some serious challenges arise when implementing this technology in the property registry of a country, which must be addressed in future works. The legal framework of a country is a big obstacle when trying to fully automatize any platform where their user has a great disparity of interests. Because of that, it is needed legislation that covers the use of smart contracts while protecting the rights of the citizens that use them in the case a failure appears. On the other hand, with the rise of regulations that are meant to protect the users' privacy, any blockchain-based solution must find a way to hide those data, while allowing their verification [14] the need for conducting research about the legislative framework of Georgia for supporting the further development of this blockchain project.

Funding

The research of Y. Mezquita is supported by the pre-doctoral fellowship from the University of Salamanca and Banco Santander. This research was also partially supported by the project 'Computación cuántica, virtualización de red, edge computing y registro distribuido para la inteligencia artificial del futuro' (reference: CCTT3/20/SA/0001) financed by Institute for Business Competitiveness of Castilla y León, and the European Regional Development Fund.

References

[1] H. Arslanian and F. Fischer. Blockchain as an enabling technology. In *The Future of Finance*, pp. 113–121. Springer, 2019.

[2] M. R. Cano. *Social Blockchain Revolution*. PhD Thesis, Universitat Pompeu Fabra, 2017.
[3] F. Chiodelli and S. Moroni. Corruption in land-use issues: a crucial challenge for planning theory and practice. *Town Planning Review*, **86**, 437–455, 2015.
[4] J. Collindres, M. Regan and G. Panting. Using blockchain to secure honduran land titles. *Fundacion Eleutra, Honduras*, 2016.
[5] T. N. Dinh and M. T. Thai. AI and blockchain: a disruptive integration. *Computer*, **51**, 48–53, 2018.
[6] A. Doig. Asking the right questions? addressing corruption and eu accession: the case study of turkey. *Journal of Financial Crime*, **17**, 9–21, 2010.
[7] S. Finch. Japan shows yen for blockchain innovation. September 2019. [Accessed; 18/04/2020].
[8] M. Francisco, Y. Mezquita, S. Revollar, P. Vega and J. F. De Paz. Multi-agent distributed model predictive control with fuzzy negotiation. *Expert Systems with Applications*, **129**, 68–83, 2019.
[9] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda and V. Santamaría. Blockchain and smart contracts for insurance: is the technology mature enough? *Future Internet*, **10**, 20, 2018.
[10] A. González-Briones, J. A. Castellanos-Garzón, Y. M. Martín, J. Prieto and J. M. Corchado. A framework for knowledge discovery from wireless sensor networks in rural environments: a crop irrigation systems case study. *Wireless Communications and Mobile Computing*, **2018**, 2018.
[11] F. Jiménez, M. Villoria and M. G. Quesada. Badly designed institutions, informal rules and perverse incentives: local government corruption in spain. *Lex Localis*, **10**, 363, 2012.
[12] N. Kshetri and J. Voas. Blockchain in developing countries. *It Professional*, **20**, 11–14, 2018.
[13] N. Lazuashvili. Integration of the blockchain technology into the land registration system. In *A case study of Georgia*. PhD Thesis, 05 2019.
[14] N. Lazuashvili, A. Norta and D. Draheim. Integration of blockchain technology into a land registration system for immutable traceability: a case study of Georgia. In *International Conference on Business Process Management*, pp. 219–233. Springer, 2019.
[15] Directiva 2000/31/ce del Parlamento Europeo y del Consejo de 8 de Junio de 2000, June 2000. [Accessed 23/12/2019].
[16] Reglas de Funcionamiento de los Mercados Diario e Intradiario de Producción de Energía Eléctrica, Junio 2018. [Accessed 23/12/2019].
[17] V. L. Lemieux. Evaluating the use of blockchain in land transactions: an archival science perspective. *European Property Law Journal*, **6**, 392–440, 2017.
[18] R. Mavilia and R. Pisani. Blockchain and catching-up in developing countries: the case of financial inclusion in africa. *African Journal of Science, Technology, Innovation and Development*, 1–13, 2019.
[19] J. McMurren, A. Young and S. Verhulst. Addressing transaction costs through blockchain and identity in swedish land transfers. In *Blockchain Technologies for Social Change*, GovLab, ed, 2018.
[20] Y. Mezquita. Internet of things platforms based on blockchain technology: a literature review. In *International Symposium on Distributed Computing and Artificial Intelligence*, pp. 205–208. Springer, 2019.
[21] Y. Mezquita, R. Casado, A. Gonzalez-Briones, J. Prieto and J. M. Corchado. Blockchain technology in iot systems: review of the challenges. *Annals of Emerging Technologies in Computing (AETiC)*, **3**, 17–24, 2019.
[22] Y. Mezquita, R. Casado-Vara, A. G. Á. Briones, J. Prieto and J. M. Corchado. Blockchain-based architecture for the control of logistics activities: pharmaceutical utilities case study. *Logic Journal of the IGPL*.

[23] Y. Mezquita, A. S. Gazafroudi, J. M. Corchado, M. Shafie-Khah, H. Laaksonen and A. Kamišalić. Multi-agent architecture for peer-to-peer electricity trading based on blockchain technology. In *The 2019 XXVII International Conference on Information, Communication and Automation Technologies (ICAT)*, pp. 1–6. IEEE, 2019.

[24] Y. Mezquita, A. González-Briones, R. Casado-Vara, P. Chamoso, J. Prieto and J. M. Corchado., eds. Blockchain-based architecture: a MAS proposal for efficient agri-food supply chains. In *International Symposium on Ambient Intelligence*, pp. 89–96. Springer, 2019.

[25] Y. Mezquita, D. Valdeolmillos, A. González-Briones, J. Prieto and J. M. Corchado., eds. Legal aspects and emerging risks in the use of smart contracts based on blockchain. In *International Conference on Knowledge Management in Organizations*, pp. 525–535. Springer, 2019.

[26] J.M.M. Reque. Fines del proceso de la tercería de propiedad y su problemática frente al derecho registral. 2019.

[27] B. Notheisen, J. B. Cholewa and A. P. Shanmugam. Trading real-world assets on blockchain. *Business & Information Systems Engineering*, **59**, 425–440, 2017.

[28] S. Ølnes and A. Jansen. Blockchain technology as s support infrastructure in e-government. In *International Conference on Electronic Government*, pp. 215–227. Springer, 2017.

[29] M. Raikwar, S. Mazumdar, S. Ruj, S. S. Gupta, A. Chattopadhyay and K.-Y. Lam. A blockchain framework for insurance processes. In *The 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–4. IEEE, 2018.

[30] N. Rose. Government and control. *British Journal of Criminology*, **40**, 321–339, 2000.

[31] Q. Shang and A. Price. A blockchain-based land titling project in the republic of georgia: Rebuilding public trust and lessons for future pilot projects. *Innovations: Technology, Governance, Globalization*, **12**, 72–78, 2019.

[32] A. T.-K. Ho. Reinventing local governments and the e-government initiative. *Public Administration Review*, **62**, 434–444, 2002.

[33] D. Valdeolmillos, Y. Mezquita, A. González-Briones, J. Prieto and J. M. Corchado., eds. Blockchain technology: a review of the current challenges of cryptocurrency. In *International Congress on Blockchain and Applications*, pp. 153–160. Springer, 2019.

[34] D. M. West. E-government and the transformation of service delivery and citizen attitudes. *Public Administration Review*, **64**, 15–27, 2004.

[35] D. Wörner and T. vonBomhard. When your sensor earns money: exchanging data for cash with bitcoin. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*, pp. 295–298. ACM, 2014.

[36] M. Yildiz. E-government research: reviewing the literature, limitations, and ways forward. *Government Information Quarterly*, **24**, 646–665, 2007.

Received 20 February 2021

5.2. Blockchain-Based Land Registry Platforms: A Survey on Their Implementation and Potential Challenges

Autores: Yeray Mezquita[a], Javier Parra[a], María Eugenia Pérez-Pons[a], Javier Prieto[a,b], Juan Manuel Corchado[a,b]

Afiliaciones:

[a]Bisite Research Group, University of Salamanca. Salamanca, Spain.

[b]Air Institute, IoT Digital Innovation Hub, Salamanca, Spain.

Publicado en: *Logic Journal of the IGPL***D.O.I.:** `https://doi.org/10.1093/jigpal/jzac010`

Fecha de publicación: 15 de febrero de 2022.

Factor de Impacto: 0.868 - Q2 (*2021*).

5.2.1. Introducción

Una de las preocupaciones de las administraciones públicas en la actualidad es la optimización de los procesos burocráticos llevados a cabo en los sistemas de registro de la propiedad. Esta optimización se entiende como la mejora de la rentabilidad de su gestión, el aumento de la velocidad con la que se realizan dichos procesos y la reducción de las ambigüedades que se producen en el tratamiento de los datos (Millones Reque, 2019). El concepto de administración electrónica, basado en los preceptos de optimización y reducción de ambigüedades, está empezando a desarrollarse en la burocracia. A través de Internet es posible dotar a las distintas administraciones de características como la estandarización, la departamentalización, la rentabilidad operativa, la construcción de redes de coordinación, la colaboración con entidades externas y los servicios al ciudadano (Rose, 2000; Tat-Kei Ho, 2002; West, 2004).

En base a lo anteriormente descrito, este trabajo publicado por Mezquita, Parra-Domínguez, et al. (2022), se centra en las ventajas de la aplicación de la tecnología blockchain al proceso de registro de la propiedad, siguiendo principalmente los preceptos estratégicos de transparencia, entendida como la democratización del acceso a los diferentes datos y la reducción de la corrupción a través del almacenamiento distribuido; reducción de costes económicos, debido a la realización y validación de una transacción

sin intervención humana; y los preceptos tecnológicos de resiliencia y seguridad de los datos.

5.2.2. Objetivos

Este trabajo se centra en el ámbito de lo ya desarrollado e implementado en respecto a las plataformas basadas en blockchain, con una pequeña vuelta de tuerca: ver cómo los gobiernos piensan en sacar partido a esta tecnología. Se ha elegido esta temática ya que en las investigaciones previas se demostró que no es cuestión técnica el que la tecnología blockchain no haya sido adoptada masivamente, por lo que se busca comprender qué es lo que realmente la está frenando, siendo este tema un tema candente con mucho auge. En este sentido, los objetivos concretos perseguidos por la investigación recogida en esta publicación incluyeron, por tanto:

This work contributes with i) a review of the pilots currently being developed with different governments around the world, in the context of blockchain-based land registries; ii) the potential benefits of a platform like this being implemented in a country like Spain; iii) the natural evolution of the e-government paradigm towards the use of this kind of systems is discussed, along with the challenges that are faced. Because of all the contributions achieved with this paper, public and private researchers, and practitioners alike will benefit from this work.

- Estudiar los proyectos piloto diseñados y desarrollados actualmente en diferentes estados dentro del contexto de las plataformas de registro de propiedades basadas en tecnología blockchain.
- Entender los potencial de esta tecnología dentro de la plataforma de registro de propiedades español como caso hipotético de estudio.
- Describir los principales problemas a los que se está enfrentando esta tecnología en los diferentes proyectos estudiados.
- Desarrollar una discusión basada en la evolución natural del paradigma de gobierno electrónico hacia este tipo de sistemas.

5.2.3. Conclusiones

Aunque la preocupación de los diferentes estados ha sido siempre la de cumplir con los criterios de eficiencia adecuados, estos criterios se ven favorecidos por el seguimiento y cumplimiento de determinados protocolos vinculados, algunos de ellos, al auge de las nuevas tecnologías. El llamado paradigma de la administración electrónica incluye diferentes protocolos que profundizan en la idea de acercar los servicios a los ciudadanos, formando la tecnología blockchain parte de ello. Es en este punto donde el trabajo realizado en Mezquita, Parra-Domínguez, et al. (2022) destaca la importancia de esta tecnología en el correcto desarrollo de determinadas políticas públicas. En concreto, este estudio se centra en el proceso de registro de la propiedad.

Conscientes de que ya existen diferentes países que aplican la tecnología blockchain al seguimiento de los registros de la propiedad, aunque de forma piloto, se ha observado que ha sido posible que, los organismos de registro de la propiedad que hacen uso de esta tecnología, reduzcan su papel de intermediarios y se centren en el desarrollo, mantenimiento y gobierno de la aplicación de la tecnología blockchain a las plataformas y aplicaciones que dan servicio a los ciudadanos. Entendiendo los resultados anteriores como positivos para la gobernanza pública, la implicación en el avance hacia la transparencia, entre otras características que sustentan los buenos gobiernos, es más que clara y determinada si se empiezan a aplicar las tecnologías más disruptivas.

A modo de conclusión del trabajo presentado, hay que señalar que surgen algunos retos serios a la hora de implementar esta tecnología en el registro de la propiedad de un país. El marco legal de un país es un gran obstáculo a la hora de intentar automatizar completamente cualquier plataforma donde su usuario tiene una gran disparidad de intereses. Por ello, es necesaria una legislación que ampare el uso de los contratos inteligentes a la vez que proteja los derechos de los ciudadanos que los utilizan en el caso de que aparezca algún tipo de fallo. Por otro lado, con el auge de las regulaciones que pretenden proteger la privacidad de los usuarios, cualquier solución basada en blockchain debe encontrar la forma de ocultar esos datos, al tiempo de permitir su verificación.

Blockchain-based architecture for the control of logistics activities: Pharmaceutical utilities case study

YERAY MEZQUITA*, *BISITE Digital Innovation Hub, University of Salamanca, Edificio Multiusos I+D+i, 37007 Salamanca, Spain.*

ROBERTO CASADO-VARA, *BISITE Digital Innovation Hub, University of Salamanca, Edificio Multiusos I+D+i, 37007 Salamanca, Spain.*

ALFONSO GONZÁLEZ BRIONES, *BISITE Digital Innovation Hub, University of Salamanca, Edificio Multiusos I+D+i, 37007 Salamanca, Spain.*

JAVIER PRIETO, *BISITE Digital Innovation Hub, University of Salamanca, Edificio Multiusos I+D+i, 37007 Salamanca, Spain.*

JUAN M. CORCHADO, *BISITE Digital Innovation Hub, University of Salamanca, Edificio Multiusos I+D+i, 37007 Salamanca, Spain, Department of Electronics, Information and Communication, Faculty of Engineering, Osaka Institute of Technology, 535-8585 Osaka, Japan, Universiti Malaysia Kelantan, Kelantan, Malaysia.*

Abstract

Logistics services involve a wide range of transport operations between distributors and clients. Currently, the large number of intermediaries are a challenge for this sector, as it makes all the processes more complicated. To face that problem, we propose a system that uses smart contracts to remove intermediaries and speed up logistics activities. Our new model combines smart contracts and a multi-agent system in a single platform to improve the current logistics system by increasing organization, security and getting rid of several human intermediaries to automate its processes, making distribution times significantly faster. Also, with this kind of approach, it is possible to apply penalties to parties that do not comply with the terms of using this platform.

Keywords: Blockchain, smart contract, multi-agent system, logistical utilities.

1 Introduction

Logistics is concerned with transporting products between parties. It is currently an important area for companies. However, the problem of this sector is that its scale may lead to delays and defaults in the delivery of goods as well as other issues. In addition, large distributors need a large volume of

*E-mail: yeraymm@usal.es

Vol. 00, No. 0, © The Author(s) 2020. Published by Oxford University Press.
doi:10.1093/jigpal/jzaa039

workers to meet the high demand of stores. All this may contribute to big delays in order processing and increases the possibility of losing some of them [31]. In an attempt to solve this problem, companies have automated all their processes, contributing to a significant increase in the number of businesses and distributors in the logistics sector.

However, an increase in the amount of digitized data and the expansion of Internet companies means that the risk of attacks on their databases is also greater. Hackers may intend to modify, steal or delete data [16, 34].

We suggest an alternative way of solving this problem. The case study conducted in this work, a pharmaceutical utilities platform, considers two different scenarios [33]. Firstly, we provide security to the data of the companies involved in the logistics sector by including blockchain. Secondly, multi-agent systems will be used to manage the organization's problem [32]. It has been proven that multi-agent systems provide efficient solutions to a huge variety of problems [54]. These include, but are not limited to, the use of agents for image classification [18], decentralized network control [39], real-time problems [11], distributed model predictive control [12, 24] and Internet of things (IoT) applications [15, 25].

In this paper, we propose a new model that makes use of blockchain technology, smart contracts and a multi-agent system to protect the data of the logistics sector [50] while speeding up logistic activities. In addition, the multi-agent system is capable of coordinating all the logistic services [14], improving the efficiency of the logistics sector.

The proposed model is capable of protecting the data generated within the platform from being tampered thanks to the use of a blockchain. Also, with the use of smart contracts to control the operation of the platform, it is possible to remove intermediaries [19, 43].

The challenges in logistics parameters, such as delays in delivery, loss of documentation, unknown source of products, errors, etc., can be minimized and even avoided by blockchain implementation. With the security mechanisms granted by the use of blockchain technology, it is possible to create a framework for trusted communications between the actors of the platform. Thanks to that, it is much more difficult to make cyber-attacks such as phishing and man in the middle [28, 29].

On the other hand, the multi-agent system uses smart contracts to control and validates the workflow of the platform, while the blockchain network is in charge of storing the transactions carried out by the agents [22]. Although there is a lot of discussion on the use of blockchain in logistical services, there have not been many platforms that would implement and evaluate it in real use case scenarios [51]. In addition, this type of systems have not been propagated sufficiently because the companies that could benefit from them, lack information and therefore do not invest enough money in the implementation of such solutions [27].

Our approach is a functional prototype which has been evaluated empirically. Furthermore, it has been proven that it resists third-party attacks, such us phishing and man in the middle. In the case study, the payments between stakeholders have been automated, which makes this logistic model more efficient than a traditional one.

This paper starts by providing a background in Section 2 of what is blockchain technology and how it works. In Section 3, the designed model is proposed and described, while in Section 4 it has been done an analysis of how this platform carries out a normal workflow and its associated monetary costs, while its advantages are evaluated in line with the conventional model. Finally, a conclusion is provided in Section 5.

2 Background

A blockchain is a distributed data structure that is replicated and shared among the members of a network [9]. It was introduced with Bitcoin [40] to create a distributed ledger that would enable the automation of transactions while solving the double-spending problem [44].

To ensure the authenticity of the stored transactions, it is first necessary to ensure the integrity of the nodes of the network that support the blockchain by implementing a consensus algorithm [13]. With this algorithm, the nodes of the network are able to agree on the information they must keep stored and who will be the next one that adds a new block of data.

There is an increasing number of consensus algorithms with their own variations. The most widespread algorithms are the ones that work best, this is why they, or some of their variations, are used by the vast majority of blockchain networks [38].

In the two most popular blockchain networks, Bitcoin and Ethereum, the consensus algorithm [26, 56] used is called proof of work (PoW). The basis of this protocol is that the node that wants to add a new block of data to the blockchain, called miner, must follow a series of steps in order to complete the task successfully and obtain the reward [40]:

1. Gather the transactions that the miner is interested in storing in the blockchain.
2. Create a Merkle tree with the hashes of the transactions in the leaves. In order to create the root of the tree, the transactions are being hashed by pairs, creating the inner elements of the tree. Those elements are hashed by pairs again, to create another layer of inner elements, repeating this process until there is no more than one element in the most inner layer of the tree [3].
3. Create the new block with the following fields in the block header [41]:
   - Version: the number of the version used to create this header. It is used to track software/protocol upgrades.
   - Previous block hash: a reference to the previous block of the blockchain. The hash of the block is used to get its identifier [5, 16, 47].
   - Merkle tree root: the Merkle tree root obtained in the previous step.
   - Timestamp: the approximate creation time of this block (seconds from Unix epoc).
   - Difficulty target: the difficulty level used to create this block in the PoW algorithm.
   - Nonce: it is a number that the miner inserts in order to make the hash of the block, once all the fields are filled, it falls within the upper limit established by the difficulty target of the algorithm.
4. Using a trial-and-error method, the miner searches for a nonce that meets the requirements of adding the new block.
5. Once the nonce is found, the mined block is broadcasted to the network in order to be validated.

Thanks to this mechanism, blockchain's ledger of logged transactions becomes immutable [52]. To attack this mechanism, an entity or organization needs to have more than the 51% of the network hash rate power, something pretty difficult to acquire in the case of blockhains like Bitcoin or Ethereum [1, 21].

The link established by the blocks forms the blockchain [4, 10]. Sometimes, a part of the network has received different legal blocks than the other part due to concurrence issues, creating different blockchains, called forks [7, 42]. When this situation happens, it is the consensus mechanism used by the network the one that says which one of the forked blockchains will be accepted by the entire network, discarding the other one [46].

Another key feature of the systems that make use of blockchain technology is that the communications between the entities and the blockchain are encrypted point to point. This is achieved by the

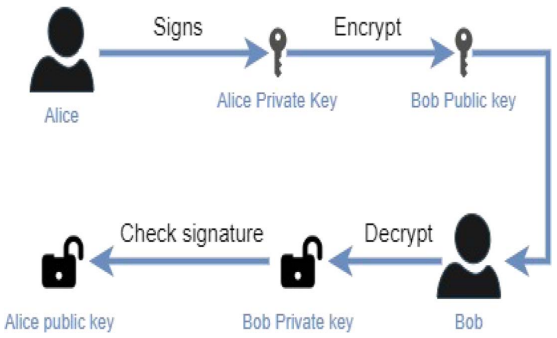

FIGURE 1. Graph of a typical public-key-based mechanism in communications.

use of public-key cryptography mechanism [53]. The basic operation of this mechanism consists of using one key pair per entity, one key is public and can be known by everyone, while the other one is private and is kept for the entity alone [36].

As shown in Figure 1, the public key is used normally by other entities to cipher a message that is supposed to be read only by the owner of that key [35]. Then the owner deciphers it with their private key. Also, the private key is used to sign the messages sent by the owner, while its public key is used to verify its signature by the receivers. So, when an entity wants to use the blockchain to make a transaction, it signs the message with its private key to let the network know it wants to make a transaction, while helping the nodes to verify that message comes from him.

With the implementation of blockchain technology in this platform, smart contracts are included to make transactions between different entities faster and more effective use. Nick Szabo introduced this concept in 1994 and defined a smart contract as 'a computerized transaction protocol that executes the terms of a contract' [48]. Szabo suggested that the clauses of contracts could be transferred to code, thus reducing the need for intermediaries in transactions between parties. In the blockchain context, a smart contract is a script that is stored on a blockchain [49].

Smart contracts have a unique address in a blockchain (i.e. they are in a block with a hash that identifies it). We can trigger a smart contract in a transaction by indicating its address on the blockchain. It is executed independently and automatically in a prescribed manner on every node in the network, according to the data contained in the triggered transaction [38].

A multi-agent system is a computerized system composed of multiple intelligent agents that interact with each other. Multi-agent systems are used to solve complex problems and achieve very good results [24]. Multi-agent systems are used in a wide range of applications. Gazafroudi *et al.* [25] presented a multi-agent system for the intelligent use of electricity in a smart home and thus, an increase in its energy efficiency.

The application of a multi-agent system to logistics is not a new idea; in [30], a multi-agent system is proposed to provide a solution to the logistical problem. In addition, another successful application of multi-agent systems is the problem of distributed computing [6], as well as the distributed model predictive control in the chemical industry [24].

From a range of systems that integrate blockchain and multi-agent systems, the work of [2] is worthy of mention. This work proposes the use of both technologies to increase security and privacy in decentralized energy networks. In [55], authors proposed a model that employs agents and blockchain for a ride-sharing system.

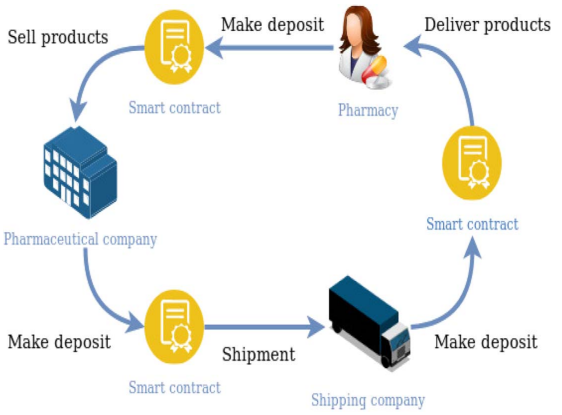

FIGURE 2. Graph based on smart contract for pharmaceutical logistics sector.

In addition, there are other applications of blockchain and multi-agent systems, like [20], in which the authors proposed an innovative blockchain model for IoT platforms. In [37], a blockchain-based multi-agent system is proposed; it simulates the tracking of agri-food assets in an agri-food supply chain. Smart contracts and sealed devices have been used to make sure that the data stored in the blockchain can be trusted.

However, after looking at the state of the art, we believe that the current blockchain and multi-agent system models have some shortcomings. We propose a new model that leverages smart contracts and multi-agent systems, making use of audit systems that will help trust the data created in the blockchain in a similar way as in [37] but adapted to this use case.

In this model, the network of Ethereum is also used as the mechanism to control the workflow of the platform through the smart contracts deployed in it. Thanks to the use of the smart contracts and the blockchain in the communications layer as well as in the storage layer, the management efficiency of the logistics system increases, automating the workflow and removing the failure and time delays caused by humans. This paper describes a case study which verified the proposed model, it focused specifically on logistics transport in the pharmaceutical sector.

3 Methodology

This paper presents a new model which consists of the following elements: a public blockchain network that is used as a service and all transactions and smart contracts are stored in it, like in [37]; smart contracts that will manage commercial transactions between the different parties; and a multi-agent system that enables the execution of all of these operations. In this section, we describe how our model works.

The parties involved in a business operation have smart devices which monitor the status of each operation. The case study was conducted in the pharmaceutical sector; Figure 2 shows process members: the client (pharmacies), the producer (pharmaceutical companies) and the shipping companies.

In this use case, the clients have sensors that monitor the number of drugs stored in the pharmacy, the type of drugs sold and the amount of money stored. Regarding the pharmaceutical companies,

they have sensors in charge of knowing the available stock and current production levels. Finally, transportation companies have sensors on each of their transport vehicles to monitor the position of the cargo. All these elements make up the wireless sensor network (WSN) that monitors operations in the pharmaceutical sector.

Within the WSN that monitors the operations carried out in this use case, there are smart devices that are responsible for creating the transactions with the monitored data. Those transactions are sent to the blockchain network by the smart devices. In the blockchain, along with the data generated, it also stored the smart contracts that control the workflow of the platform.

A multi-agent system controls the whole process. The architecture of the multi-agent system consists of the following layers (see Figure 3):

1. Client layer: this layer consists of three different types of agents that manage pharmacies. These include the data management agent that keep updated the stock of the pharmacy and the agent that is responsible for placing orders and that which verifies the delivery of the purchased products, changing its state in the blockchain through smart contracts.
2. The source layer contains the following agents: two agents receive orders from pharmacists and another agent places orders with the transport company in order to take the goods to the pharmacies. Another agent's task is the control of stock and production levels. Finally, there is an agent responsible for verifying whether smart contract conditions are fulfilled.
3. Shipping layer has the following agents: an agent that manages the incoming orders, another agent that manages the fleet of vehicles and, finally, an agent that verifies smart contracts.
4. Workflow management layer is composed of two agents, a workflow management agent and a smart contract control agent this agent. This layer is in charge of creating smart contracts, keeping the money while making transactions and applying penalties in case of non-compliance with the smart contracts.

Thus, one of the agents included in each of the 4 layers verifies that the smart contract terms are abided to. For instance, when the workflow of a smart contract smart contract is initiated between a pharmacy and a pharmaceutical company for the purchase of medicine, both have to agree on a set of terms. The pharmacy pays for the drugs, but money is kept in the blockchain by a control entity, in this case the agent that verifies the smart contract. When the pharmacy receives the drugs it ordered, this agent confirms that the conditions of the smart contract have been fulfilled and automatically pays the pharmacist the agreed sum of money.

4 Results

Once the multi-agent system has been designed, the number of times the platform interacts with the blockchain has been studied. In this model, the transactions carried out in a normal workflow to purchase products are detailed as follows:

– In the client layer, when a client wants to buy a product, a transaction of funds from the client to the smart contract is carried out. Also, whenever a batch of items arrives at its final destination, the state of the batch is updated and a transaction is executed, in which it is updated the state of the batch, and the smart contract releases the funds transacted from the client to the owner of the product. This means that in a normal workflow, three transactions are carried out in this layer.

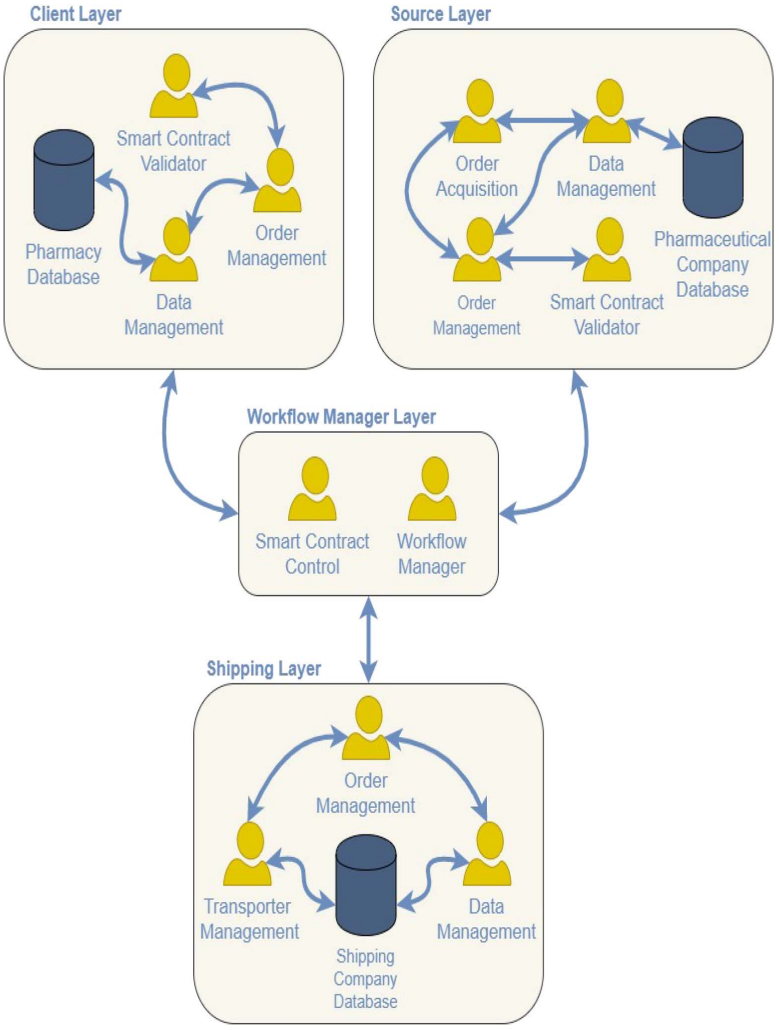

FIGURE 3 Multi-agent architecture. (i) Client layer: the pharmacies are found in this layer. (ii) Source layer: this layer contains pharmaceutical companies. (iii) Shipping layer: this layer manages transport companies. (iv) Workflow management layer: this layer contains an agent that controls the entire information flow and an agent which ensures that smart contract conditions are fulfilled.

– In the source layer, a transaction is carried out a transaction when a batch of products is put on sale, another when it is sold and when it is being shipped. The last transaction involves securing the payment made by the client in the smart contract, so that the seller does not receive the payment until it has been confirmed that the order has been delivered correctly. If nothing is wrong with the order, the funds are returned to the seller, making a total of five transactions in a normal execution.

- The workflow manager layer only makes transactions with the blockchain when an agent wants to be part of the platform and an agent leaves it. One transaction for each update of the agents status.
- The shipping layer only transfers the payment to the smart contract when a new order is being shipped. The funds are given to the seller in the case it has been any problem with the shipment. Otherwise, they are returned to the transporter.

After studying the interactions of the platform with the blockchain, we found out that a minimum of ten transactions are carried out when a batch of products are delivered from a seller to a final client. This number does not take into account the number of the transactions made in cases where a new seller, client or transporter wants to be a part of the platform.

To calculate the cost of executing the services of the blockahin network, we have to know the price of executing each transaction. In the case of Ethereum, the one chosen for this use case, and according to [45], the execution price of a transaction is equivalent to 0.1€, which multiplied by the number of transactions in a normal workflow of the system, the amount of money needed by all the stakeholders to keep the system up is 1€ per batch of products that are transacted from a stakeholder to another.

One of the reasons for which the Ethereum blockchain has been selected is because it offers the best support for the integration of the platform and moreover it uses the Python programming language, web3.py [23]. Also, if we assume that there are a hundred buyers and sellers, then hundreds of transactions are being carried out by the platform in a normal workflow iteration. Being said that, the time needed to perform an exchange of assets between seller and buyer is in the order of days, and the daily average number of transactions of the Ethereum blockchain is 610000 [17], then we can assume that the proposed platform can be managed by the Ethereum network.

In our study, it has been shown that the price for exchanging a batch of assets between different stakeholders is about 1€. If we have to compare to the traditional model that uses human intermediaries in the verification process [8], the workflow of our proposed platform is cheaper and faster.

5 Conclusion

This paper presents a new smart contract approach to improving logistics services. The novelty of this paper lies in the use of a blockchain for the storage of all the transaction of information in the logistical process. The proposed model makes use of smart contracts to manage the entire logistics process of a pharmaceutical supply chain more efficiently. By automating the processes with the use of smart contracts, human intermediaries are no longer needed.

Another novelty of this paper is the use of agents who verify that both parties abide to the terms of a smart contract. If the agents detect that either of the parties is not fulfilling the established conditions, a penalty is imposed and the agents keep money in the control entity until the conditions agreed upon are met. This makes our model more efficient than current models. Moreover, it is able to track and authenticate orders. A penalties pattern is introduced for breach of smart contracts.

Our model can be used to improve any logistics system that still relies in human intermediaries that verify payments and/or transactions between non-trusted parties. It is highly efficient and secure because it is automated by the multi-agent system. By incorporating blockchain, we provide the logistics system with solid security features. Shipments can be tracked, origin and destinations authenticated, and proof of all transactions can be stored and maintained unaltered in the blockchain.

Future lines of research include improving the multi-agent system by introducing new agents for the monitoring of procedures. In addition, our model could be enhanced by integrating a case-based reasoning system.

Acknowledgements

This work was developed as part of 'Virtual Ledger Technologies DLT/Blockchain y Cripto-IOT sobre organizaciones virtuales de agentes ligeros y su aplicación en la eficiencia en el transporte de última milla', ID SA267P18, project cofinanced by Junta Castilla y León, Consejería de Educación and FEDER funds. Also, the research work carried out by Yeray Mezquita is supported by the pre-doctoral fellowship from the University of Salamanca and Banco Santander.

References

[1] Academy Binance. What is a 51% attack? (October 2019). https://www.binance.vision/security/what-is-a-51-percent-attack, accessed: 04/10/2019.

[2] N. Z. Aitzhan and D. Svetinovic. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, **15**, 840–852, 2016.

[3] N. Z. Andrew. Blockchain fundamentals #1: what is a Merkle tree? (February 2018). https://medium.com/byzantine-studio/blockchain-fundamentals-what-is-a-merkle-tree-d44c529391d7, accessed: 01/10/2019.

[4] A. M. Antonopoulos. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, Inc., 2014.

[5] A. Back. Hashcash—a denial of service counter-measure, 2002.

[6] S. Banerjee and J. P. Hecker. A multi-agent system approach to load-balancing and resource allocation for distributed computing. In *First Complex Systems Digital Campus World E-Conference 2015*, pp. 41–54. Springer, 2017.

[7] L. Becerra-Bonache and M. D. J. López. Linguistic models at the crossroads of agents, learning and formal languages. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, **3**, 67–87, 2014.

[8] R. Benjamin and R. Wigand. Electronic markets and virtual value chains on the information superhighway. *MIT Sloan Management Review*, **36**, 62, 1995.

[9] J. Bremer and S. Lehnhoff. Decentralized coalition formation with agent-based combinatorial heuristics. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, **6**, 29–44, 2017.

[10] R. C. Cardoso and R. H. Bordini. A multi-agent extension of a hierarchical task network planning formalism. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, **6**, 5–17, 2017.

[11] C. Carrascosa, J. Bajo, V. Julián, J. M. Corchado and V. Botti. Hybrid multi-agent architecture as a real-time problem-solving model. *Expert Systems with Applications*, **34**, 2–17, 2008.

[12] R. Casado-Vara, P. Chamoso, F. De la Prieta, J. Prieto and J. M. Corchado. Non-linear adaptive closed-loop control system for improved efficiency in iot-blockchain management. *Information Fusion*, **49**, 227–239, 2019.

[13] R. Casado-Vara and J. M. Corchado. Blockchain for democratic voting: how blockchain could cast off voter fraud. *Oriental Journal of Computer Science and Technology*, **11**, 01–03, 2018.

[14] R. Casado-Vara, P. Novais, A. B. Gil, J. Prieto and J. M. Corchado. Distributed continuous-time

fault estimation control for multiple devices in iot networks. *IEEE Access*, **7**, 11972–11984, 2019.

[15] R. Casado-Vara, F. Prieto-Castrillo and J. M. Corchado. A game theory approach for cooperative control to improve data quality and false data detection in wsn. *International Journal of Robust and Nonlinear Control*, **28**, 5087–5102, 2018.

[16] R. Casado-Vara, A. Martin-del Rey, S. Affes, J. Prieto and J. M. Corchado. Iot network slicing on virtual layers of homogeneous data for improved algorithm operation in smart buildings. *Future Generation Computer Systems*, **102**, 965–977, 2020.

[17] ConsenSysConsenSys Ethereum by the numbers (December 2018). https://media.consensys.net/ethereum-by-the-numbers-3520f44565a9, accessed: 04/10/2019.

[18] J. A. G. Coria, J. A. Castellanos-Garzón and J. M. Corchado. Intelligent business processes composition based on multi-agent systems. *Expert Systems with Applications*, **41**, 1189–1205, 2014.

[19] Â. Costa, P. Novais, J. M. Corchado and J. Neves. Increased performance and better patient attendance in an hospital with the use of smart agendas. *Logic Journal of IGPL*, **20**, 689–698, 2011.

[20] V. Daza, R. Di, I. Klimek and M. Signorini. Connect: contextual name discovery for blockchain-based services in the iot. In *2017 IEEE International Conference on Communications (ICC)*, pp. 1–6. IEEE, 2017.

[21] Q. DuPont. Experiments in algorithmic governance: a history and ethnography of "the dao," a failed decentralized autonomous organization. In *Bitcoin and Beyond (Open Access)*, pp. 157–177. Routledge, 2017.

[22] B. O. Durić. Organisational metamodel for large-scale multi-agent systems: first steps towards modelling organisation dynamics. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, **6**, 2017, 2017.

[23] EthereumEthereum A python interface for interacting with the Ethereum blockchain and ecosystem. https://web3py.readthedocs.io/en/stable/.

[24] M. Francisco, Y. Mezquita, S. Revollar, P. Vega and J. F. De Paz. Multi-agent distributed model predictive control with fuzzy negotiation. *Expert Systems with Applications*, **129**, 68–83, 2019.

[25] A. S. Gazafroudi, T. Pinto, F. Prieto-Castrillo, J. Prieto, J. M. Corchado, A. Jozi, Z. Vale and G. K. Venayagamoorthy. Organization-based multi-agent structure of the smart home electricity system. In *2017 IEEE Congress on Evolutionary Computation (CEC)*, pp. 1327–1334. IEEE, 2017.

[26] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf and S. Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 3–16. ACM, 2016.

[27] N. Hackius and M. Petersen. Blockchain in logistics and supply chain: trick or treat? In *Proceedings of the Hamburg International Conference of Logistics (HICL)*, pp. 3–18. Epubli, 2017.

[28] M. A. Khan and K. Salah. Iot security: review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, **82**, 395–411, 2018.

[29] N. Kshetri. Can blockchain strengthen the internet of things? *IT Professional*, **19**, 68–72, 2017.

[30] K. Li, T. Zhou, B.H. Liu and H. Li. A multi-agent system for sharing distributed manufacturing resources. *Expert Systems with Applications*, **99**, 32–43, 2018.

[31] T. Li, S. Sun, M. Bolić and J. M. Corchado. Algorithm design for parallel implementation of the smc-phd filter. *Signal Processing*, **119**, 115–127, 2016.

[32] T. Li, S. Sun, J. M. Corchado and M. F. Siyau. A particle dyeing approach for track continuity

for the smc-phd filter. In *17th International Conference on Information Fusion (FUSION)*, pp. 1–8. IEEE, 2014.

[33] T. Li, S. Sun, J. M. Corchado and M. F. Siyau. Random finite set-based bayesian filters using magnitude-adaptive target birth intensity. In *17th International Conference on Information Fusion (FUSION)*, pp. 1–8. IEEE, 2014.

[34] A. C. E. Lima, L. N. de Castro and J. M. Corchado. A polarity analysis framework for twitter messages. *Applied Mathematics and Computation*, **270**, 756–767, 2015.

[35] C. C. Lo and Y. J. Chen. Secure communication mechanisms for gsm networks. *IEEE Transactions on Consumer Electronics*, **45**, 1074–1080, 1999.

[36] D. Massessi. Blockchain public/private key cryptography in a nutshell. (October 2018). https://medium.com/acoinmonks/blockchain-public-private-key-cryptography-in-a-nutshell-b7776e475e7c, accessed: 04/10/2019.

[37] Y. Mezquita, A. González-Briones, R. Casado-Vara, P. Chamoso, J. Prieto and J. M. Corchado. Blockchain-based architecture: a mas proposal for efficient agri-food supply chains. In *International Symposium on Ambient Intelligence*, pp. 89–96. Springer, 2019.

[38] Y. Mezquita, D. Valdeolmillos, A. González-Briones, J. Prieto and J. M. Corchado. Legal aspects and emerging risks in the use of smart contracts based on blockchain. In *International Conference on Knowledge Management in Organizations*, pp. 525–535. Springer, 2019.

[39] S. Najafi, S. Talari, A. S. Gazafroudi, M. Shafie-khah, J. M. Corchado and J. P. Catalão. Decentralized control of dr using a multi-agent method. In *Sustainable Interdependent Networks*, pp. 233–249. Springer, 2018.

[40] S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system, 2008.

[41] PrasannaPrasanna What is the blockchain data structure? (November 2018). https://cryptoticker.io/en/blockchain-data-structure/, accessed: 01/10/2019.

[42] P. Rodríguez, N. Duque and D. A. Ovalle. Multi-agent system for knowledge-based recommendation of learning objects using metadata clustering. In *International Conference on Practical Applications of Agents and Multi-Agent Systems*, pp. 356–364. Springer, 2015.

[43] S. Rodríguez, F. de La Prieta, D. I. Tapia and J. M. Corchado. Agents and computer vision for processing stereoscopic images. In *International Conference on Hybrid Artificial Intelligence Systems*, pp. 93–100. Springer, 2010.

[44] M. Rosenfeld. Analysis of hashrate-based double spending. Dec. 2012. https://www.bitcoil.co.il/Doublespend.pdf.

[45] D. Ryan. Calculating costs in ethereum contracts (May 2017). https://hackernoon.com/ether-purchase-power-df40a38c5a2f, accessed: 04/10/2019.

[46] G. Santos, T. Pinto, V. Zita, I. Praça and H. Morais. Enabling communications in heterogeneous multi-agent systems: electricity markets ontology. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, **5**, 15–42, 2016.

[47] F. I. P. Standards. Secure hash standard (August 2002). https://csrc.nist.gov/csrc/media/publications/fips/180/2/archive/2002-08-01/documents/fips180-2.pdf, accessed: 02/25/2004.

[48] N. Szabo. Smart contracts. *Virtual School*, 1994.

[49] N. Szabo. The Idea of Smart Contracts. Nick Szabo's Papers and Concise Tutorials 6, 1997.

[50] D. I. Tapia, J. A. Fraile, S. Rodríguez, R. S. Alonso and J. M. Corchado. Integrating hardware agents into an enhanced multi-agent architecture for ambient intelligence systems. *Information Sciences*, **222**, 47–65, 2013.

[51] E. Tijan, S. Aksentijević, K. Ivanić and M. Jardas. Blockchain technology implementation in logistics. *Sustainability*, **11**, 1185, 2019.

[52] D. Valdeolmillos, Y. Mezquita, A. González-Briones, J. Prieto and J. M. Corchado. Blockchain technology: a review of the current challenges of cryptocurrency. In *International Congress on Blockchain and Applications*, pp. 153–160. Springer, 2019.

[53] J. Weise. *Public Key Infrastructure Overview*, pp. 1–27. Sun BluePrints OnLine, 2001.

[54] M. Wooldridge and N. R. Jennings. Intelligent agents: theory and practice. *The Knowledge Engineering Review*, **10**, 115–152, 1995.

[55] Y. Yuan and F. Y. Wang. Towards blockchain-based intelligent transportation systems. In *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, pp. 2663–2668. IEEE, 2016.

[56] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang. An overview of blockchain technology: architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557–564. IEEE, 2017.

Received 1 March 2019

5.3. Towards a Blockchain-Based Peer-to-Peer Energy Marketplace

Autores: Yeray Mezquita[a], Ana Belén Gil-González[a], Angel Martín Del Rey[b], Javier Prieto[a], Juan Manuel Corchado[a]

Afiliaciones:

[a]Bisite Research Group, University of Salamanca. Salamanca, 37007, Spain.

[b]Department of Applied Mathematics, Institute of Fundamental Physics and Mathematics, University of Salamanca. Salamanca, 37008, Spain.

Publicado en: *Energies, Volumen 15.*

D.O.I.: `https://doi.org/10.3390/en15093046`

Fecha de publicación: 21 de abril de 2022.

Factor de Impacto: 3.252 - Q2 (*2021*).

5.3.1. Introducción

La red eléctrica tradicional actual está diseñada para transportar energía a largas distancias. Este requisito del sistema tradicional implica que existen ciertas limitaciones, como la capacidad máxima de tensión que soportan las líneas de distribución(Hirst & Kirby, 2001). Cuando se sobrepasa esta capacidad, el calor generado por una línea puede provocar su caída o rotura, lo que da lugar a inestabilidades en el suministro de energía, como fluctuaciones de fase y de tensión. Como la capacidad de una línea depende de su longitud y de la tensión de transmisión, una solución es crear líneas más cortas y distribuir las funcionalidades de la red eléctrica actual en redes inteligentes más pequeñas. Estas redes se denominan microrredes inteligentes o *smart microgrids*, que son un tipo de sistema energético discreto que incluye fuentes de energía apropiadas, así como cargas eléctricas que proporcionan energía a consumidores residenciales, comerciales, industriales y gubernamentales. El objetivo principal de las microrredes inteligentes es proporcionar energía asequible a zonas independientes de la red principal de suministro eléctrico, optimizando al mismo tiempo la transmisión de la energía.

En el contexto actual de generación de energía, gracias a fuentes renovables como la solar o la eólica, y junto con la aparición de un nuevo tipo de actor que consume y

produce energía dentro del sistema -los llamados prosumidores-, las microrredes tienen el potencial de sustituir al sistema tradicional de transmisión de energía en un futuro próximo(Fang, Misra, Xue, & Yang, 2011). Sin embargo, el auge de las microrredes inteligentes viene acompañado de algunos retos que hay que afrontar. Estos retos van desde la vulnerabilidad de las plataformas a los ataques DDOS, hasta la aparición de intermediarios que no contribuyen a la distribución de energía, pero que acaban encareciéndola(Memon & Kauhaniemi, 2015).

En este artículo, publicado por Mezquita, Gil-González, et al. (2022), se propone un sistema multiagente distribuido (MAS por sus siglas en inglés: *Multi-Agent System*) basado en la tecnología blockchain para permitir el control descentralizado de una plataforma de microrred, con la que permitir un intercambio automatizado de energía entre sus actores. En el sistema propuesto, el MAS gestiona el flujo de trabajo de la microrred, por ejemplo, las negociaciones entre pares en el mercado local, o el correcto equilibrio de la red energética. Mediante el uso de una red blockchain, el control de la plataforma se distribuye entre los agentes, al tiempo que se mejora la resiliencia del canal de comunicación entre ellos. Esto permite el despliegue de una plataforma sin un único punto de fallo. Además, los trabajos de investigación existentes no tienen en cuenta el anonimato y la privacidad de los usuarios, algo que también se aborda en el modelo propuesto.

5.3.2. Objetivos

Esta publicación se enmarca en la fase final del desarrollo de la tesis, en la que se pone en conjunto todo lo investigado hasta la fecha. Aquí se tienen en cuenta, no sólo las limitaciones técnicas de la implementación de la tecnología blockchain en un sistema real, sino que también se consideran las limitaciones relacionadas con la jurisprudencia de los marcos legislativos actuales en la Unión Europea. Gracias a lo estudiado en el resto de la tesis, en este artículo se presenta un MAS que podría ser implementado en el mundo real, finalizando esta tesis. A este respecto, y tal como se ha definido en los *Objetivos Específicos* en el Capítulo 1, de cara a esta publicación se establecieron los siguientes objetivos:

- Diseñar una plataforma distribuida en la que se optimice y promueva, en este caso, la aparición de mercados energéticos locales y automáticos, y que cumpla con el marco legislativo actual de la Unión Europea.
- Eliminar la necesidad de regulación respecto a los mercados energéticos.
- Ayudar a la implantación de modelos energéticos que no dañen el medio ambiente, cómo la adopción de las renovables por parte de los ciudadanos comunes.
- Promover, en general, el uso de la tecnología blockchain para la aparición de procesos más democráticos y optimizados que los de los sistemas tradicionales.

5.3.3. Conclusiones

Este manuscrito destaca y analiza conceptos y tecnologías como la tecnología blockchain, las microrredes inteligentes y los algoritmos de negociación que se han aplicado al mercado de la energía. Además, este trabajo elabora la propuesta de una arquitectura innovadora basada en alta tecnología de una microrred inteligente totalmente distribuida y autónoma para apoyar nuevas formas de negocio en el mercado de la energía inteligente. Con una tarificación independiente y dinámica entre los transactores de la red, la propuesta presentada permite crear un mercado local de energía (LEM por sus siglas en inglés: *Local Energy Market*) para lograr la eficiencia en el transporte y la distribución de energía en comparación con el modelo de distribución tradicional.

En el contexto mencionado, este trabajo ha estudiado la implantación y desarrollo de microrredes inteligentes que permitirían la entrada de más entidades, cuyo objetivo es el autoconsumo y ganar dinero con el exceso de energía generada, como competidores en el mercado energético. Si es posible introducir más actores en el mercado de la energía que puedan competir por los ingresos en el mercado energético, la regularización de los precios ya no es necesaria. Dado que las transacciones de energía entre entidades de una microrred que están más cerca unas de otras son más baratas y mejores que las realizadas entre entidades lejanas, la ley de mercado de la oferta y la demanda funcionaría, haciendo innecesaria su actual regularización. Por último, se ha propuesto el uso de firmas en anillo y protocolos ZKP (protocolos de conocimiento nulo por sus siglas en inglés: *Zero-Knowledge Proofs*) para garantizar la privacidad de los usuarios y

la protección de los datos almacenados dentro de la plataforma, cumpliendo así con la ley general de protección de datos.

energies

MDPI

Article

Towards a Blockchain-Based Peer-to-Peer Energy Marketplace

Yeray Mezquita [1,*], Ana Belén Gil-González [1], Angel Martín del Rey [2], Javier Prieto [1] and Juan Manuel Corchado [1]

[1] BISITE Research Group, University of Salamanca, 37007 Salamanca, Spain; abg@usal.es (A.B.G.-G.); javierp@usal.es (J.P.); corchado@usal.es (J.M.C.)
[2] Department of Applied Mathematics, Institute of Fundamental Physics and Mathematics, University of Salamanca, 37008 Salamanca, Spain; delrey@usal.es
* Correspondence: yeraymm@usal.es

Abstract: Blockchain technology is used as a distributed ledger to store and secure data and perform transactions between entities in smart grids. This paper proposes a platform based on blockchain technology and the multi-agent system paradigm to allow for the creation of an automated peer-to-peer electricity market in micro-grids. The use of a permissioned blockchain network has multiple benefits as it reduces transaction costs and enables micro-transactions. Moreover, an improvement in security is obtained, eliminating the single point of failure in the control and management of the platform along with creating the possibility to trace back the actions of the participants and a mechanism of identification. Furthermore, it provides the opportunity to create a decentralized and democratic energy market while complying with the current legislation and regulations on user privacy and data protection by incorporating Zero-Knowledge Proof protocols and ring signatures.

Keywords: blockchain; energy market; multi-agent system; negotiation; distributed ledger technology

Citation: Mezquita, Y.; Gil-González, A.B.; Martín del Rey, A.; Prieto, J.; Corchado, J.M. Towards a Blockchain-Based Peer-to-Peer Energy Marketplace. *Energies* **2022**, *15*, 3046. https://doi.org/10.3390/en15093046

Academic Editor: Mohamed Benbouzid

Received: 3 March 2022
Accepted: 19 April 2022
Published: 21 April 2022

1. Introduction

The current traditional power grid is designed to transport energy over long distances. This characteristic of the traditional system implies that certain limitations exist, such as the maximum voltage capacity supported by the distribution lines [1]. When this capacity is exceeded, the heat generated by a line can cause it to sag or break, resulting in power supply instabilities such as phase and voltage fluctuations. Because the capacity of a line depends on its length and the transmission voltage, one solution is to create shorter lines and distribute the functionalities of the current power grid in smaller smart networks. These networks are called smart micro-grids, which are a type of discrete energy system that includes appropriated energy sources as well as power loads that provide power to residential, commercial, industrial, and governmental consumers. The main purpose of smart micro-grids is to provide affordable energy to areas independently of the main power supply network while optimizing the transmission of the energy.

In the current context of energy generation, thanks to renewable sources such as solar or wind, and together with the emergence of a new type of actor that consumes and produces energy within the system—the so-called prosumers—micro-grids have the potential to replace the traditional energy transmission system in the near future [2]. However, the rise of smart micro-grids comes with some challenges that must be faced. These challenges range from the vulnerability of platforms to DDOS attacks, to the emergence of intermediaries that do not contribute to energy distribution but end up making it more expensive [3].

In the past, some authors have proposed strategies for energy management on micro-grid platforms. For example, in [4], the excess or shortage of energy could be compensated by exchanging it with the utility grid or other external sources. However, that paper did not allow for direct energy exchange between individuals, nor did it allow for the automation

and distribution of the platform. Without the use of blockchain technology, democratized energy markets could not be created. A blockchain network acts as a reliable distributed ledger that is governed by the platform and where information of value is stored. The network can be utilized to distribute the control and governance of the smart grid, along with the communication that is carried out within it, thus avoiding the single point of failure and eliminating those intermediaries that do not give any value to the platform. Moreover, blockchain technology (BT) provides a mechanism for protecting the actors against identity theft by signing direct communications between peers [5].

After studying the literature on this topic, it was found that none of the works had been able to propose a truly decentralized platform that enables peer-to-peer energy trading, automatically, and with dynamic prices. For this reason, we propose a distributed Multi-Agent System (MAS) based on blockchain technology to enable decentralized control over a micro-grid platform that allows for an automated exchange of energy between its actors. In the proposed system, the MAS manages the workflow of the micro-grid, e.g., the negotiations between peers in the local market, or the correct balancing of the energy network. By using a blockchain network, the control of the platform is distributed between the agents while the resilience of the communication channel between them is improved. This allows for the deployment of a platform without a single point of failure. Moreover, existing research works do not take into consideration users' anonymity and privacy, something that we would also like to tackle with the proposed framework.

This paper shows a thorough study of the most important features of blockchain technology and smart micro-grids in Section 2. Section 3 studies how previous works in the literature tackle the challenges of using blockchain technology in smart micro-grids. Furthermore, the section studies how automated negotiation between machines could be achieved and its viability. Section 4 describes the proposed platform, which is a combination of a MAS and a blockchain network for improved decentralization, as well as the security of the platform, along with the viability of the creation of a local automated energy market that optimizes the payoffs for the micro-grid stakeholders. Finally, Section 5 draws up conclusions and some final remarks on the conducted research.

Contributions

This work is relevant for designers, developers, and practitioners alike who are working in the field of energy distribution and renewable energy adoption and who will get the most benefits from the proposed framework. The main contributions of this paper are as follows:

- The design of a framework that will help developers to create new platforms that allow for the appearance of automatic peer-to-peer energy markets with dynamic prices.
- The proposed framework also provides user flexibility in the negotiation algorithms used. They will be able to implement the algorithm they want depending on their needs, with the only prerequisite being that the communications between agents follow the same ontology.
- The framework designed also provides anonymity to their users, complying with the current data regulations.
- Following the proposed framework, the future platforms developed and deployed will be more democratic and decentralized, thus eliminating the single point of failure.

2. Conceptual Foundations of Micro-Grid Platforms and Blockchain Technology

Traditional power grids deliver energy from a few central generators to a large number of consumers. This creates a closed market in which energy prices are dictated in a monopolistic way. Sometimes, to avoid abusive pricing by companies towards consumers, states need to implement regulatory measures, with the European Union [6,7] being an example in this case.

In the face of this monopolistic behavior, the literature has proposed the distribution of the traditional main grid into smaller micro-grids [2]. These micro-grids are comprised of a set of loads and generators. The set of generators can be composed of individual houses with solar panels on the roof. The entry of more entities into the energy market reduces the risk of oligopolies and avoids the intervention of states by imposing the use of regularization measures. This way, the energy market is converted into a more democratic market in which the offer and demand of energy will be the only factors that can regulate the energy price.

Micro-grid platforms make use of a great number of Internet of Things (IoT) devices that exchange crucial information between them. The continuous communication between the devices allows for the distribution of the management and control of any IoT platform. This helps with the optimization of the workflow of the system, but not without some drawbacks [8].

- Heavy reliance on exchanged messages. Since each part of the system is controlled by an independent entity, the other entities have to trust the messages received to understand the system's global state. If a malicious entity could somehow modify the content of those messages, the proper functioning of the entire platform would be compromised.
- Reliance on the truthfulness of the transmitted data. Entities of the platform have to rely on the fact that the data transmitted have not been tampered with by the sender entity to make an unfair profit. In addition, it is a possibility that databases will be attacked in order to steal, modify, or delete sensitive information about the entities that are taking part in the system's workflow.

In the literature, the use of BT has been proposed to overcome the listed flaws of this kind of platform. BT consists of a peer-to-peer (P2P) network of nodes, governed by a consensus algorithm that dictates how the information is stored within the network. This technology allows for the creation of a distributed ledger where anything of value can be stored.

The use of a blockchain network within any IoT system makes it possible to distribute the process workflow while eliminating other centralized entities [8]. In addition, by eliminating the single point of failure factor of centralized platforms, protection against some traditional forms of cyberattacks is gained. In this way, the blockchain is used as a bulletin where important information about the system is stored. Furthermore, the data stored within the blockchain network are kept in the same state after their storage, which means that the information is tamper-proof [9].

Within a blockchain-based system, a cryptographic mechanism of pairs of asymmetric keys is used, which signs and encrypts the data transmitted. Hence, as long as the blockchain network is big enough, the consensus algorithm keeps the information in a consistent state [10], the keys are not compromised, and the information transmitted and stored is secure from any attack, thus maintaining its integrity and authorship [11]. If this mechanism is also used in the exchange of messages between individuals of the system, then the messages are protected from being read and modified by unauthorized third parties [12].

A user needs to generate a random private key to make use of a blockchain protocol. This key is usually part of a cryptography mechanism that uses a key pair mechanism: the random private key mentioned and a public one derived from that. This public-key cryptography mechanism is used, not only because they allow for an efficient management of the keys, but also because it is impossible for an attacker to obtain the private key even when knowing the public one.

To interact with a blockchain protocol, an individual needs to generate at least one wallet address as an identifier. It is a three-step process, which starts with the generation of a random private key that only the owner should know. Then, through a one-way algorithmic transformation, the public key is obtained, which is shared with the network and is used to verify the signatures made by the user with their private key. Finally, the

public key is hashed in order to obtain the wallet address to be used in the exchange of virtual assets between individuals within the blockchain protocol.

The process of exchanging assets is quite straightforward and shares the same steps as in every blockchain. Figure 1 illustrates how a user, Alice, wants to initiate a transaction with Bob with 2 coins. To do that, Alice signs the transaction (*Tx*) with her private key and broadcasts it in the network. Then, each node of the network verifies Alice's signature with her public key, and if the check is correct and the transaction is proven to have come from Alice, the network validates that she has the coins she wants to spend. If everything goes well, the transaction will be added to the blockchain.

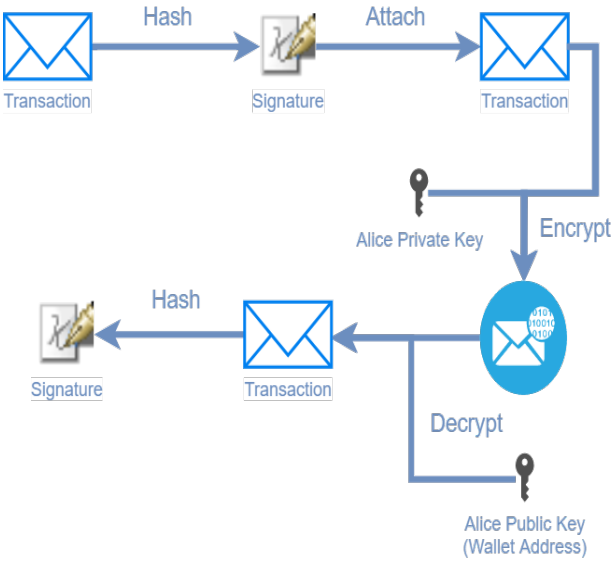

Figure 1. Example of the signature mechanism in a transaction.

2.1. Blockchain Consensus Algorithms

A consensus algorithm describes the mechanism that allows all agents in the system to coordinate in a distributed environment. It constitutes the only source of truth. Thanks to the consensus algorithm employed by the network of nodes, it is possible to keep the information stored and replicated in a consistent state. Among the functions of any consensus algorithm is ensuring that there is only one blockchain in the system, which can be an issue when a part of the network accepts a blockchain while the remaining nodes accept a different one (Fork). The consensus algorithm should enable the convergence of the chains into one as soon as possible. Moreover, it should offer resilience against attempts by malicious actors to take over the network and guarantee that there will not be any consensus failure when nodes try to add new blocks of data to the blockchain. Keeping the data stored in a blockchain makes it more difficult for attackers to take down the services of a system, and the attacker is forced to take down the majority of them to successfully hack the data [8].

There is a great variety of consensus algorithms, including the Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) (see Table 1), or any of their variants that are the most widespread and have proven their effectiveness in practice [13].

Table 1. Comparison between consensus algorithms and their common usage.

Algorithm	Scalability	Consistency	Decentralization	Usage
PoW	No	Yes	Yes	Public blockchains
PoS	Yes	No	Yes	Public and permissioned blockchains
PBFT	Yes	Yes	No	Permissioned blockchains

PoW requires work to be performed by the miner and then verified by the network. The work required usually consists of the performance of a series of operations, algorithms, and mathematical calculations to be solved by the miners. These calculations vary and are different depending on the blockchain network they want to participate in. Each mathematical problem posed can only be solved by a very high computational calculation, which then encourages the nodes to behave in a certain way on the platform as compared with the simplicity of verifying the block mined. The greater problem of this algorithm is that a network using a consensus algorithm based on PoW wastes a massive amount of energy and is very slow. Therefore, it is not environmentally friendly and also not suitable for platforms that need to store information quickly [14].

PoS algorithms are based on the assumption that those who own more units of a PoS-based coin are especially interested in the survival and good functioning of the network that gives value to those coins. Therefore, they are the most suited to bearing the responsibility of protecting the system from possible attacks. That is why the protocol rewards them with lower difficulty in finding blocks (it is inversely proportional to the number of coins they prove to possess). The PoS algorithm has a theoretical vulnerability called the Nothing at Stake Theory, which has not been proven in practice. That theory states that forks in the blockchain network will occur more frequently [15].

In a PBFT consensus algorithm, all nodes communicate with each other, with the objective that honest nodes reach an agreement on the state of the system following the majority rule. Nodes not only have to verify that the message comes from a specific node, but they also have to verify that the message has not been tampered with. For the model to work, it is assumed that the number of simultaneous malicious nodes can never be equal to or greater than one-third of the total number of nodes. Therefore, the more nodes there are in the system, the more difficult it will be to reach that third. It is called practical in the sense that this proposal can work in asynchronous environments. This algorithm is used only in permissioned platforms and cannot be used in a public one, where nodes can access it freely [16].

In [17], the authors discussed the "blockchain trilemma", a term coined by Ethereum's founder Vitalik Butering to explain the problem of developing blockchain technology. According to this study, no blockchain satisfies the following three characteristics: scalability, consistency, and decentralization (see Table 1). For example, PoW solves the consistency and decentralization problems, but it lacks scalability. On the other hand, PoS can offer scalability and decentralization, but at the cost of consistency. Finally, PBFT-based algorithms can solve consistency problems while being scalable, but they centralize the process.

2.2. Blockchain Accessibility

The implementation of blockchain technology in the real world depends on the accessibility of the network underlying this kind of platform. If a player needs permission to be part of the blockchain network, it is said that it is a permissioned one. These kinds of networks are used in platforms where the actors are known, although they each have different interests. On the other hand, if anyone can be part of the network without requirements, the network is called a public blockchain.

A public blockchain, based on PoW, is less efficient in terms of reaching consensus and therefore managing transactions per second because it offers a truly decentralized ecosystem with proven security against attacks, with Bitcoin and Ethereum being their main representatives [10] (see Table 1). Public blockchains that make use of another consensus

algorithm, such as PoS or any of its variants, are far more efficient, although they lose some consistency. Blockchain networks that use PBFT-based consensus algorithms could only be used in permissioned environments because they lose decentralization in favor of scalability; to have consistency, it is required that the actors are known.

2.3. Smart Contracts

Another relevant aspect of some blockchain technologies is that they allow for the deployment and execution of coded scripts called smart contracts. Those scripts, due to the immutability feature of the blockchain technology, are considered self-enforcing and are used to automatize some processes, such as payments between entities within a platform that would otherwise need human intervention and/or that of third parties [18]. The code of smart contracts is transparent to the players that can make use of it, which means that they know the programmed clauses that rule it. Then, when those parties agree to use a smart contract, the workflow of the interactions between them is governed by the rules coded in the smart contract, all without the need for human hands to verify the process [19]. A smart contract ensures that the agreement will be carried out automatically when the conditions agreed upon are met [20].

3. Related Work on Micro-Grid Platforms Based on BT

Blockchain technology has been used to improve the performance of a broad range of platforms in today's industries. The state of the art encompasses, to enumerate a few examples, the pharmaceutical industry [21,22], the agri-food sector [23,24] as well as healthcare [8,25–27] and education services [28–30].

In this section, we will detail a small study on the state of the art related to the use of blockchain technology in the field of micro-grid platforms. Then, it will be followed by a study on the automatic negotiation algorithms that have been proposed in order to understand the requirements that need to be implemented in this type of platform.

3.1. Blockchain Technology and Micro-Grid Platforms

In the literature, we found some works that discussed the use of blockchain-based micro-grid platforms to create energy markets, focusing on specific characteristics such as the use of cryptocurrencies, decentralization, security, privacy, and state estimations [12,31–34].

Pichler et al. [35] studied real-world use cases of platforms based on blockchain technology and whose aim was to allow for the direct exchange of energy between its actors. The platforms studied have a general common aim: to create local markets based on renewable energy communities. However, they share the same cons: they do not try to create an autonomous market, and they do not offer real anonymity and privacy to their users (see Table 2).

A working example is the Pylon network [36], a Spanish startup that makes use of its permissioned blockchain-based Litecoin technology combined with a smart meter to certify energy flows and enable virtual transactions with the use of their own token. It makes use of a Proof of Cooperation (PoC) consensus algorithm, and its main aim is to create a neutral database, one that is not governed by the companies that sell the energy,in order to help the user decide how to optimize the energy costs. They made their platform open source to receive help from the community in case any kind of improvement is needed for their network. In Slovenia, SunContract [37] has created a market for peer-to-peer transactions of energy based on BT. They launched a crypto-asset within the Ethereum network in order to use it in the exchange of energy between the entities that are participating in the platform. On the other hand, there is Enosi [38], an Australian company whose aim is similar to that of SunContract: to create a community of peers transacting energy directly between them. By using smart metering, they trace, match, and settle energy production and consumption. Because of the platform, the producers can directly offer a price to the end consumer, with cheaper prices instead of the artificial ones that the power oligopolies have in the traditional energy market.

In the case of the Brooklyn micro-grid [39], LO3 developed the TransActive Grid elements (TAG-e), which allows for the exchange of energy between peers, the balancing of the grid, or the emergency management of the network. A TAG-e is composed of two elements: an electric meter and a computer. They are meant to read the information on the state of the grid and share it with other TAG-e in order to act upon the collected information. The market created with this platform allows for the trading of energy between peers with fixed prices; however, automatic negotiations within it are not permitted.

Table 2. Comparison of the studied startups.

Project	Description	Pros	Cons
Pylon Network [36]	The main aim is to create a neutral database. Makes use of its permissioned blockchain-based Litecoin technology. It makes use of a Proof of Cooperation (PoC) consensus algorithm. In addition, a smart meter (METRON) certifies energy flows and enables virtual transactions using their own token.	• Open source • Scalable • Latency • Improve prices	• Nothing about user's data privacy • It is not designed to create an autonomous market
SunContract [37]	The main aim is to create a marketplace that allows customers to trade energy without the need for intermediaries. They managed a market for P2P energy transactions based on BT for more than 2 years. They enable virtual energy transactions using their own token.	• Scalable • Latency • Improve prices	• Nothing about user's data privacy • It is not designed to create an autonomous market
Enosi [38]	Their main aim is to create a marketplace that allows the energy customers to trade energy without the need for intermediaries. They certify energy flows via smart metering.	• Scalable • Latency • Improve prices	• Nothing about user's data privacy • It is not designed to create an autonomous market
Brooklyn Micro-grid Network [39]	This project created a local energy marketplace in Brooklyn. Bacuase of it, prosumers can trade their energy surplus with their neighbors.	• Scalable • Latency • Improve prices	• Nothing about user's data privacy • It is not designed to create an autonomous market

3.2. Negotiation Algorithms on BT-Based Micro-Grid Platforms

Due to the increase in the production of renewable energy, grid consumers need to be flexible in adjusting their energy consumption. This adjustment occurs through different demand response mechanisms: either by reducing electricity consumption during hours where the global consumption is at its highest (peak hours) or by discouraging the consumption during those hours by affecting the prices with financial incentives. Regarding the last demand response mechanism, it is possible to implement it in a negotiation process based on the law of supply and demand. Then, peers of the network can trade energy directly through a local P2P network, thus allowing for the movement of local funds within the local economy [40] (see Figure 2).

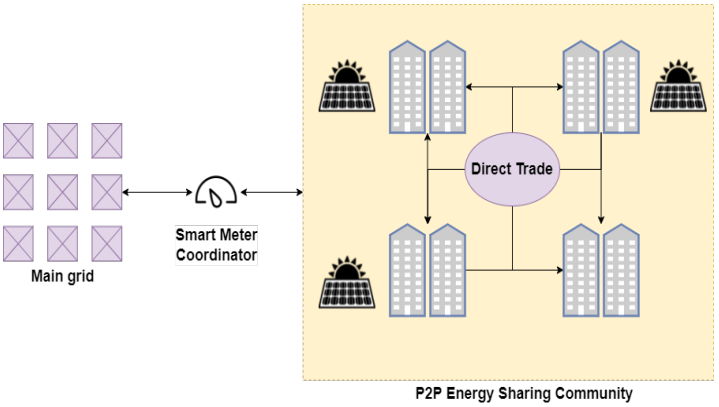

Figure 2. Basic diagram of a micro-grid architecture. The actors of the P2P network exchange energy locally and can potentially sell energy outside the community thanks to the existence of a smart meter coordinator.

In the study by Long et al. [41], in order to optimize the energy prizes for the players participating in the micro-grid community, they proposed a non-linear programming optimization algorithm with a rolling horizon of 30 min. The method proposed made use of a model based on the supply and demand proposed in [42]. In this model, the prices of energy fluctuate through the day, with a constraint that the price of the energy generated within the micro-grid should never be higher than the price of the energy bought from outside the grid. Moreover, the prize of the energy sold to the external grid must always be higher than that of the energy sold within the micro-grid. In this work, it was found that the smart meter coordinator was the most vulnerable part of the architecture proposed. The possibility of the smart meter being hacked was not considered, since BT was a mechanism that was required to avoid this kind of vulnerability while distributing the control of the activities and the negotiations carried out within the community.

Authors of [43] modeled a micro-grid scenario in which two variants appear, one based on cooperation between the different actors on the platform, and the other in which the actors play more selfishly in the market. This platform is only viable when all costs are equally shared between all households; therefore, there is no automated negotiation between the peers of the platform proposed. In this paper, it was also stated that a real scenario wherein all the actors collaborate is not feasible.

The companies studied in Section 3.1 allow for the trading of energy at a fixed price given by the producer. In other theoretical works such as that by Noor et al. [44], to allow for the exchange of energy with dynamic prizes, a game theory-based model was proposed. In this work, the blockchain network was used to distribute the control of the platform along with the exchange of information as a transparent energy market was created. Here, the actors that formed part of the platform negotiated the price of the energy in an automatic manner using a non-cooperative game-based algorithm to optimize their payoffs, based on the energy load of the entire grid. An important downside of this approach is that the system must know which specific appliances are connected throughout the entire network; this, along with the fact that no mechanism of encryption is used to store the data within the blockchain, creates a great privacy problem for the users.

3.3. Literature Review Conclusions and Manuscript Objectives

The present paper aims to create a transparent energy market with proven distributed security. Because of the nature of this kind of system, it will be impossible to use a public blockchain such as Ethereum due to its high fees and slow speed. A consortium of peers in the micro-grid will be needed to create a permissioned network that makes use of a

protocol such as PBFT, PoS, or dPOS, where it is assumed that all the network's participants are known and have the common goal of wanting the platform to work.

One of the features that the companies studied are lacking is the use of an automatic negotiation between the players of each platform. Our model makes use of a non-cooperative game between the consumers and producers that will regulate the energy market price in an autonomous way, thus allowing the stakeholders optimize their payoffs. Our model and its interactions with the blockchain are thoroughly explained to help startups and entrepreneurs to develop this kind of system. Furthermore, the scenario proposed in our work is based on a rolling horizon such as the one proposed by Long et al. [41], but with a time window of an hour to make the transactions more viable in the actual Ethereum network.

In the literature, compliance with the General Data Protection Regulation (GDPR) [45] has been found to be an important issue. Because of this, a careful selection of which data are to be collected and stored in the public ledger is needed, as well as which data must be encrypted and hidden from unauthorized peers. Moreover, ensuring the integrity and authenticity of the data is required by protecting it and the communication channels from unauthorized users [35]. Another issue of the proposed platform is its heavy dependence on the legislative framework of the country where it is to be installed. Laws that regulate the transaction of renewable energy between peers within communities are needed, such as in the case of Belgium, Greece, and Germany [35].

4. Proposed Architecture Design

In this section, we will describe the design of the proposed architecture, which aims to: (i) decentralize the energy market, (ii) automate, as much as possible, the energy market in small communities, (iii) and provide anonymity and privacy to its users. In the literature studied in the Section 3, there are working proposals that meet some of the above-mentioned requirements, although not all of them together.

The proposed architecture will follow the paradigm of distributed Multi-Agent Systems (MAS), which, in combination with blockchain technology, allows for the distribution of the processes and the control of the platform. The use of multi-agent systems was chosen because other works successfully achieved their main objective with the use of this paradigm, with the optimization and decentralization of platforms of any kind [46]. In the proposed architecture, features from different works studied in the literature have been put together, thus enabling decentralized control over the platform without a single point of failure and allowing for a negotiation process between the peers of the network as well as complying with the GDPR.

- Through the MAS, the control and management of the micro-grid platform is achieved, along with the negotiation between peers for energy in the market. However, to achieve full decentralization of the platform, the use of a blockchain platform is required, in which the smart contracts deployed will be used by the agents in the workflow of the platform. Thanks to this approach: (i) we will achieve a decentralized platform without a single point of failure; (ii) we will provide confidence to platform users and agents that agreements would be enforced, and in case they are not, encourage trust that the platform will compensate those who behave while punishing those agents who do not; and (iii) we will allow for the optimization of the prices of the energy transacted within the platform, balancing them while maximizing the payoffs of each kind of actor involved.
- The smart meters read the energy consumed and/or produced by each household. They are connected to each independent house, representing a peer in the micro-grid network. Each smart meter is connected to the internet and interacts with the blockchain on behalf of the household. Moreover, the agent who negotiates with their peers to buy or sell energy should be deployed here or in a device connected to the smart meter.
- The use of a blockchain network allows for the distribution of the communication and the interactions between the agents of the platform. The network is used not only as a

historical log in that each agent stores their activity on the platform, but it is also used as a validation and tamper-proof system that will help them to trust the platform and the activities of the actors involved. In addition, the smart contracts deployed in the network help in the control of the workflow of the platform.

- The information stored in the blockchain is encrypted, maintaining the data hidden from others. It is possible to maintain a verified and encrypted log in the blockchain by using Zero-Knowledge Proof (ZKP) protocols. Furthermore, by using ring signatures, the identity of the entities that store information within the blockchain is kept secret.

4.1. Blockchain Technology and Smart Contracts

The design of the proposed platform is based on the negotiation, payment, and exchange of energy. In time windows of one hour, agents negotiate the energy prices based on the amount they wish to transact during the following hour. The platform will use a permissioned blockchain, governed in a consortium way between the market actors. A permissioned blockchain network, as seen in the background section, allows for a high transaction output but with a very low cost.

The use of a permissioned network is proposed because it achieves two things that cannot be achieved using a permissionless network [47]: (i) transaction speed, since there are only known nodes within the network, it is possible to make use of faster consensus algorithms at the cost of a certain level of security; (ii) system scalability, because of the above-mentioned characteristics, by not requiring a large computational capacity to reach consensus, the system is scalable; (iii) the network protocols can be adapted to the system requirements during development, e.g., with the addition of ZKP protocols and ring signatures that are not available in any permissionless blockchain that allows for the deployment of smart contracts.

In a consortium blockchain, only verifiable actors are allowed to take part in the proposed platform. If new actors, e.g., new households, want to take part in the created market within the micro-grid, they have to make a proposition to the platform; here, in a consortium and not in an automated way, the actors of the micro-grid will vote if they will let them enter or not. If the actors suspect that the new actor trying to enter the platform has no good intentions or has intentions that are not aligned with the well-being of the platform, they will not be allowed to enter. On the other hand, if it is a typical household that wants to benefit from the good use of the platform, they will allow it to enter. To summarize, the consortium blockchain proposed in this framework should be governed equally by all the nodes of the blockchain; they all have equal voting rights.

Due to the characteristics of the blockchain network used, the platform will need a margin to store the agreements carried out by the agents. In the proposed platform, the margin is 5 min, enough time for the network to validate the information of the platform [48]. In that time window of 5 min, agents cannot continue their negotiations. Then, after 55 min, the agents will only sign the agreements that best benefit them after the negotiation period. In this way, the energy prices are fixed by each batch of energy independently negotiated, dependent only on the supply and demand, and each buyer and seller will make their own decisions based on their situation and the payoffs they want.

On the platform, smart contracts are used to generate tokens that represent the amount (in KWh) of energy available for exchange in the batteries. The virtualization of this energy is achieved by using Ethereum's fungible token standard: ERC20. Making use of standards is important for future system extensions as well as for the improvement of interoperability.

In the proposed platform, a smart contract is used to control the workflow of the platform (see Figure 3). The usual sequence of steps followed by the platform is described below:

1. Through the function *PublishInfo()*, agents can identify themselves on the platform. They can store data in relation to how other agents can initiate negotiations with them, the household they belong to, etc. With that information, it is possible for authorized actors to carry out auditory processes as well as to track their activity on the platform. This step should be performed the first time an agent is deployed in the system.

2. To publish any energy offer on the platform, authors should call the function *MakeOffer()*. Agents can calculate the forecasted energy surplus that could be sold to the network and create an offer with the predicted amount of energy for the next time window.
3. When an agent predicts a need to buy energy for the next time window, it will need to call the function GetOffers(). This function will return all the information related to the offers published for the next time window. Then, the agent will start the negotiation process directly with all the publishers of offers.
4. During the negotiation process, the agents try to reach an equilibrium on the price of the energy and the amount that must be bought. The price of the energy sold has an upper constraint, which is the price of the energy bought from outside the grid. It also has a lower constraint, which is the minimum price needed to produce the energy. Between those thresholds, agents have the autonomy to decide; they could use whatever negotiation algorithm they find more comfortable with as long as it exchanges messages following the ontology defined by the platform communications. The agents negotiate on the basis of different parameters such as the energy needed to buy or sell, the time left to finish the negotiation, the number of buyers or sellers, the amount of energy to be expected to generate or consume in the next time window, etc. When the last minutes of the negotiation are reached, each seller agent will start agreeing to sell the energy to those that offer the higher prices until the energy is all sold out. The buyer agents will do the opposite—they will buy at the lower prices given by the sellers during their negotiation. Because of the constraints, it is ensured that all the energy will be sold out; no buyer will buy from the main grid while energy is still available within the system. Therefore, each agent should have a time out to get answers from an offer. If they do not receive an answer during that time out, they will have to drop the offer and try to reach an agreement with the next best offer on their list. This will ensure an equilibrium point while avoiding getting stuck in infinite waiting periods.
5. After negotiating the price and the amount of energy to sell and to whom, the seller can publish on the blockchain to whom, how much, and for how much they are selling the energy with the function *AllowTransaction()*.
6. Finally, when the corresponding smart meters have detected the flow of energy to and from a house, automatic payments can be made by calling the function *MakeTransaction()*.

For the platform to function optimally, the amount of energy available to exchange within the market must be auditable. A guarantee is needed that this energy exists on the platform, so the smart meters in charge of reading this energy from the batteries and virtualizing it into tokens for sale undergo periodic auditing processes to ensure its proper functioning [47]. In addition, the smart meters are in charge of reading the energy flow in and out of the houses, another critical element for the proper functioning of the platform. In this sense, we call smart meters oracles, since they are in charge of virtualizing real-world data in smart contracts, a critical point of any platform based on blockchain and of which it is necessary to be very cautious [49].

Each agent of the platform interacting in one way or another with the blockchain network needs to make use of a wallet. Some agents, such as those in charge of using virtual money in exchanges, need to obtain that money beforehand. For example, if a household consumes more energy than it produces, it will need to put fiat money on the platform; hence, a consortium of human agents and/or machines will be needed to virtualize the money introduced and mint more tokens that represent it. In addition, they must allow the withdrawal of real money when a user decides to take out part of the virtual money for use outside the platform.

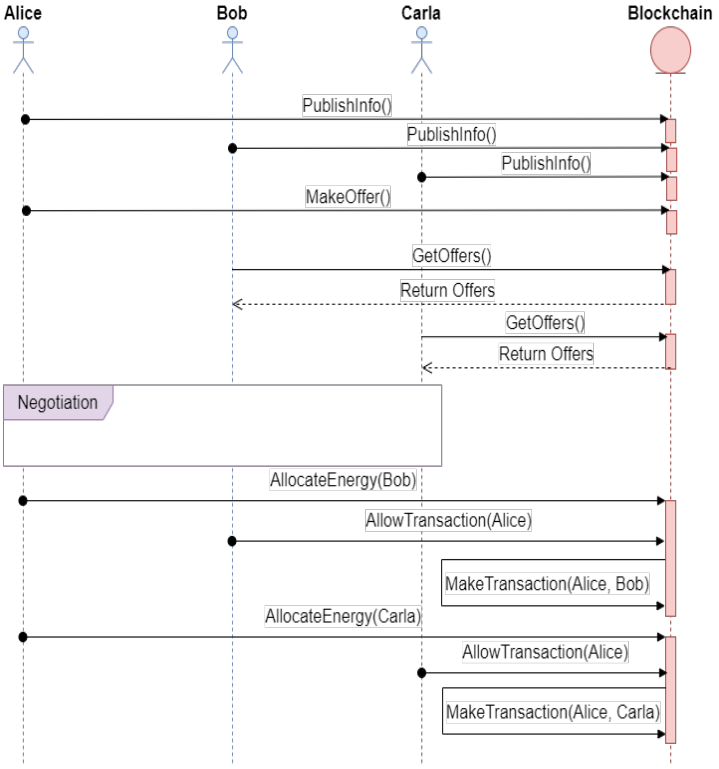

Figure 3. UML diagram of a sample workflow of the proposed platform.

4.2. Privacy Preservation Protocols

One of the problems that arise in state-of-the-art literature is that of user privacy and data protection, which are needed to comply with the GDPR. In this regard, the proposed model has been designed using protocols based on ZKPs used by the Monero cryptocurrency and described in [50]. Thanks to the use of these protocols, it is possible to hide the users who perform transactions within a blockchain as well as the related information [51].

For example, in [52], the authors proposed a framework that allows people who have been in close contact with infectious disease patients to be traced. Moreover, the authors proposed the use of ZKP to protect patient information based on bulletproofs [53].

The ring signatures protocol is used to allow actors to call smart contracts anonymously. This protocol requires what is called a Key Image [51], obtained from a list of randomly selected public keys (see Figure 4). The public key of the actor performing the transaction is also required since the transaction must be signed. Given that all the selected keys have the same probability of performing the transaction, it is not possible to associate the transaction with the real user. In addition, these groups of actors are improvised randomly from the pool of transactions.

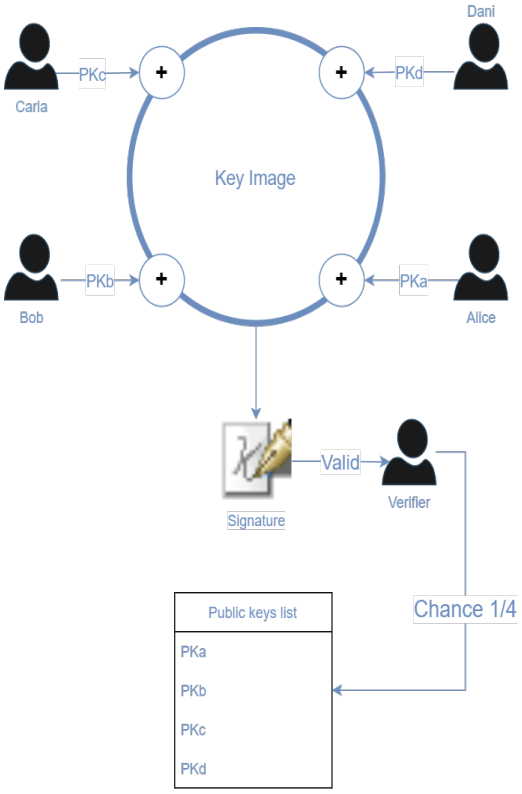

Figure 4. Key image, created from a list of the signatures of the users Bob, Alice, Carla, and Dani.

To complement the ring transaction signing process and ensure the anonymity of the actors within the system, stealth addresses are used in the smart contracts to identify actors. It is impossible to link these addresses to a user; however, a user can identify the stealth addresses that belongs to it. Taking advantage of the properties of elliptic curves [51], a stealth address (P) is defined by Equation (1):

$$P = F + S \tag{1}$$

where F is defined in (2), and S is the public key of the recipient of the transaction.

$$F = Hash(rS) * G \tag{2}$$

where r is a random private key generated by the actor that emits the transaction, and G is the base point of the elliptic curve.

To identify which stealth address belongs to a user, thanks to the properties of Equation (3), the actor can hash the product of the address public key (R) and its private key (s), then the public key (S) has to be added, and the final result is the stealth address. For a user to prove that a stealth address belongs to them, they need to recover the one-time private key generated for that transaction. By hashing the product of the stealth-address public key (R) and the user private key (s), and then adding the private key s to the obtained hash, it is possible to recover the one-time private key of the address (r). Then, it is necessary to sign the transactions from that address with that key to prove the ownership.

$$rS = rsG = rGs = Rs \tag{3}$$

where R is the public key of the randomly generated private key, and s is the private key of the transaction recipient.

The use of these protocols increases the need for the computational power of each actor that makes use of them. In Figure 3, it is possible to study the number of times each agent must write to the blockchain, thus making use of these protocols, within a system based on the proposed framework. The agents only need to write the information in the following cases:

1. When they are registered within the system and store information related to them. In the whole life cycle of the platform, this occurs once for each agent.
2. At the end of each hour, every agent writes in the blockchain the agreement reached during the negotiation process. For example, if Alice reaches an agreement with Bob and Carla, then Alice will need to create two transactions. On the other hand, according to the example, Bob and Carla only need to create one each.

This step will depend on the number of agents involved, but with the time limits proposed—from 5 to 10 min—in a permissioned blockchain, it is enough time to not overcharge the agents and their computational resources. Therefore, the performance will not be affected when the system escalates.

4.3. Security Model

This section details the security assumptions made by the framework and how the data generated within the platform are treated. The implementation of blockchain technology in this platform ensures the application of a secure identification protocol between the actors. Furthermore, the information stored is tamper-proof, and the smart contracts deployed allow for the decentralized control of the platform, ensuring that there will not be a single point of failure that will be prone to attacks.

Regarding the storage of the generated data, which will be used to create the predictive models that will help with the proper functioning of the system, each actor will be responsible for them. We assume that each actor is responsible for providing an access point to their data so that they can control to whom they give access to the data. For each hour, a batch can be created with the generated data, storing in the blockchain a hash of such data that will help to verify that it has not been modified afterwards. The use of auditability systems allows for the generation of data that can be trusted. Otherwise, it would be impossible to know that the generated data has not been modified before the storage of its hash in the blockchain [47].

As for the proposed privacy protocols, they ensure that the information stored in the blockchain cannot be read by third parties without permission, nor will it be possible to identify or track user activity. This information that is stored is, for example, the energy bids posted, the money paid for energy transactions, or the amount of energy transacted. The only vulnerability of this platform is when an attacker steals the keys of a user. However, this is not possible just by using the platform; it can only happen if the user is not careful enough with the passwords used or with where the keys are stored.

In this work, we have made security assumptions that the network of blockchain nodes is large enough so that it is not easy to throw it from a typical Distributed Denial of Services (DDOS) attack. It has also been assumed that the actors that are part of the platform benefit more from its proper functioning than from trying to sabotage it. Different actors could collude with each other to achieve a greater benefit, but this scenario is not realistic based on the study conducted by [43]. Having in mind the previous assumptions, we can thus say that the actors of the platform will benefit from the creation of this platform and the competition between them rather than in trying to sabotage the negotiation process and the well-being of the platform.

4.4. Multi-Agent System

This section will describe the MAS structure in detail. It is divided into four different subsystems, in which the agents are grouped according to their function within the platform

(see Figure 5). The following is a detailed description of the different subsystems and the agents that comprise them:

- Device Driver System (DDS). This system groups all the agents in charge of the management and control of the different smart devices of the platform (e.g., batteries, smart meters, PV panels). These agents are allowed to interact with the blockchain network, so they also have an assigned wallet to identify and track their activity within the platform, thus helping in the auditing process. The agents in charge of monitoring the state of the PV panels (e.g., their energy production, the provided voltage and current, and their active and reactive powers) are the PV agents (PVA). They store those data in the blockchain, which helps their owners to monitor them while also owning that information which they could sell in the future. The batteries are monitored by agents called Battery State Agents (BSA). They store in the blockchain data related to the state of a battery, its charge and discharge capability, and its current state of charge. The agent that stores the data related to the flow of current from or to a household is the Smart Meter Agent (SMA).
- Micro-grid Operator System (MGOS). In this system, all those agents that are responsible for monitoring, controlling, and managing the status and good credit of the micro-grid are grouped together. These agents are also connected to the blockchain, storing the relevant information that favors the traceability of the micro-grid monitoring, flows of power to and from the utility network, the balance of the micro-grid power, and the voltage level (Micro-grid Operator agent or MGO), or the energy transactions made from the grid to the micro-grid and vice versa (External Market Interactor Agent or EMI). In addition, this system owns a series of batteries that improve the balance of the grid load, governed by the State Of Charge agents (SOC). This part of the platform is economically maintained by the penalties of users who do not fulfill their part of the contracts and by the exchange of energy between the external grid and the micro-grid.
- Data Analytic System (DAS). This system is crucial for the platform as it is in charge of grouping all those agents that are in charge of the data market and the creation of predictive models, which are required by the rest of the agents of the system to be able to infer the amount of energy they expect to obtain in the next hour, that which they could sell, and that which they will need to buy based on their past consumption. The agents in charge of reading the data provided by the other subsystems of the platform on the blockchain and merging it with data coming from other external data sources are called Data Reader Agents (DRA). The agents that create and update new behavioral models on demand are the Knowledge Extractor Agents (KEA). The agents that make predictions based on these models and the information extracted from the environment are the Forecasting Agents (FA). This subsystem benefits from the data market created with the addition of blockchain technology to the platform. As it has been found in other works in the literature, it is also possible to improve the creation of the models with the use of blockchain technology by applying a federated learning framework similar to the one proposed in [54].
- Transaction Manager System (TMS). In this subsystem, all those agents that are responsible for the negotiation and exchange of energy within the micro-grid are grouped. These agents make use of the blockchain network to publish and search for energy offers as well as register the agreements that take place. The agents in charge of publishing the offers are the Seller Agents (SA), while those who search for them in order to buy are the Buyer Agents (BA). The agents in this system negotiate with each other directly and make use of the DAS to estimate the energy they will need to buy and/or sell. As a way to improve the search process in the blockchain, a middleware layer could be used to optimize the search for information (offers in this case) within the blockchain, such as the one proposed in [55].

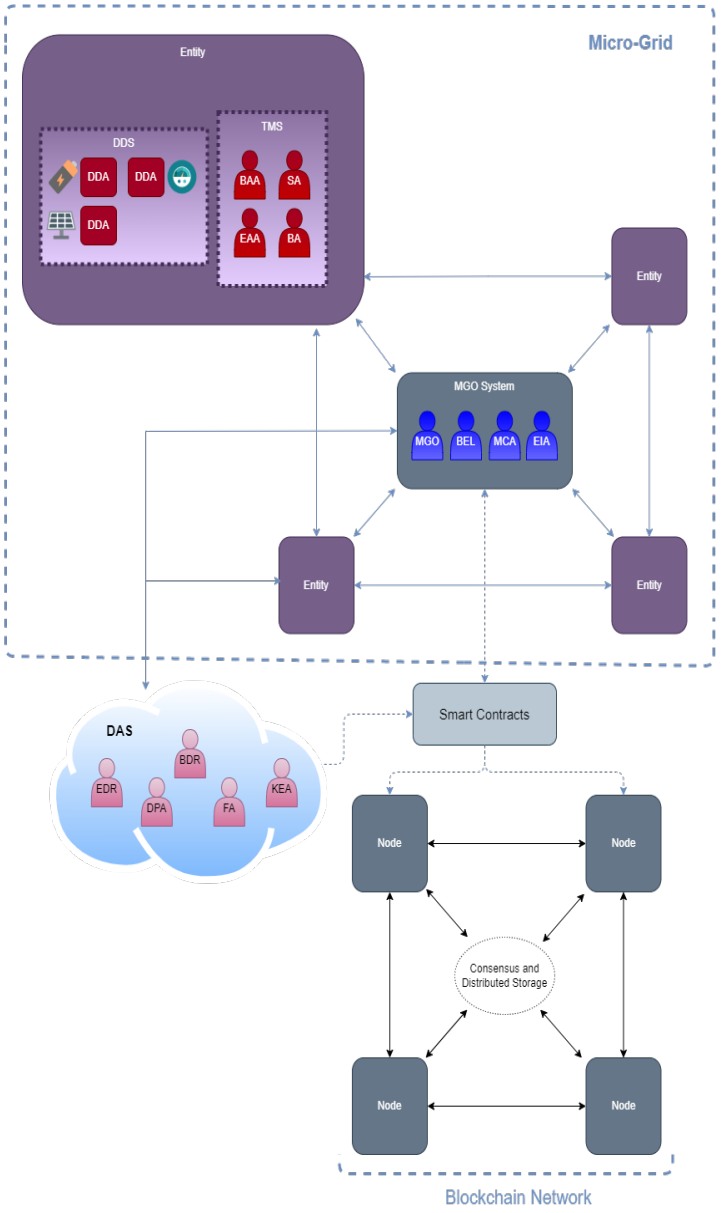

Figure 5. Proposed platform architecture.

4.5. Deployment of the Platform

In the proposed platform, there are three types of actors: consumers who receive energy that they buy from the grid, PV panels as producers that produce the energy and dump it into batteries, and batteries as prosumers who store and distribute the energy (e.g., consumed by their owners, or, if leftover, dumped into the micro-grid to make a profit). There are also actors who are in charge of the good credit of the micro-grid and who additionally make a profit by connecting it to the external grid. Finally, there are other

players who help the platform to function properly, such as those in charge of exchanging fiat money for digital money and vice versa.

As shown in Figure 6, the interconnections between the parts of the platform are made through the Internet, in the creation of cloud services. The platform agents in charge of knowledge extraction with regard to the platform data needs large computational power; hence, the infrastructure is outsourced to a provider (e.g., Amazon Web Services, Google Cloud, or Azure). The blockchain network, controlled by the platform actors, is accessible to the parties and does not need high computational power; only one computer per participant is required to be always on. The agents in charge of controlling the smart devices will need to be deployed in them or in a system such as a Raspberry Pi that has direct access to them. The rest of the agents only need to be deployed in computers that always have access to the Internet and do not have any special requirements.

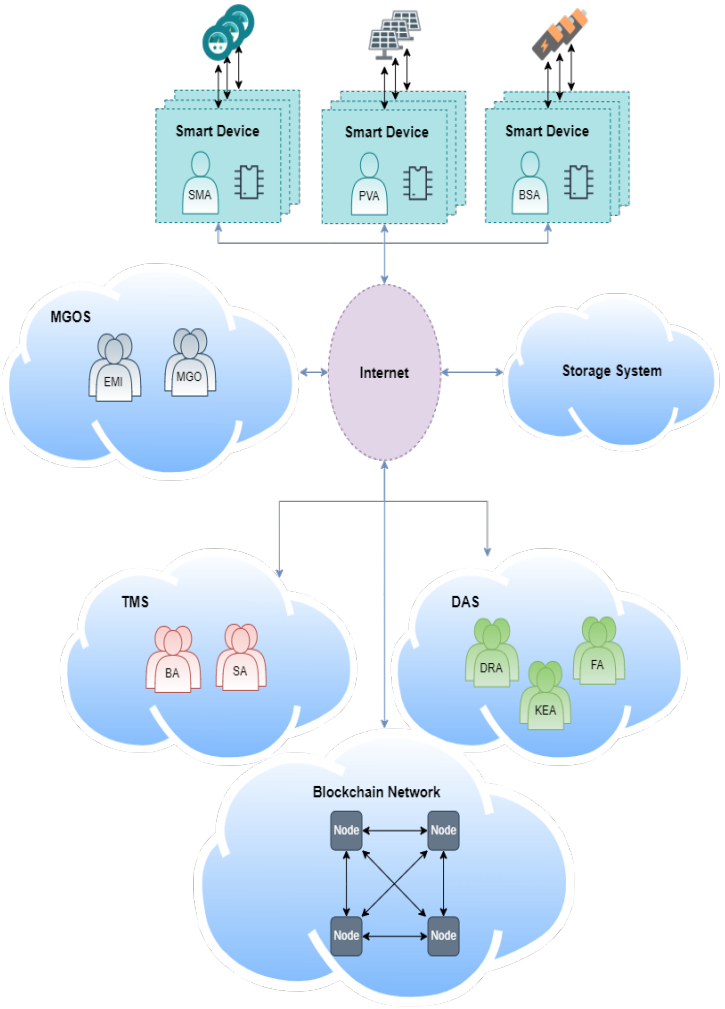

Figure 6. Platform deployment diagram.

5. Conclusions and Future Work

This manuscript highlights and discusses concepts and technologies such as blockchain, smart micro-grids, and negotiation algorithms that have been applied to the energy market. Furthermore, this work elaborates on the proposal of an innovative high-technology-based architecture of a fully distributed and autonomous smart micro-grid to support new forms of business in the smart energy market. With independent and dynamic pricing between the transactors in the network, the proposal presented makes it possible to create a Local Energy Market (LEM) in order to achieve efficiency in the transmission and distribution of energy as compared to the traditional distribution model.

In the mentioned context, this paper has studied the implementation and development of smart micro-grids that would allow for the entrance of more entities, whose aim is self-consumption and making money with the excess energy generated, as competitors in the energy market. If it is possible to introduce more actors into the power market that can compete for revenue in the energy market, the regularization of prices is no longer necessary. Because the energy transactions between entities of a micro-grid that are closer to each other are cheaper and better than those made between distant entities, the market law of supply and demand would work, thus making their current regularization unnecessary. Finally, the use of ring signatures and ZKP protocols has been proposed to ensure the privacy of the users and the protection of the data stored within the platform, thus complying with the GDPR.

In general terms, for future work, the designed proposal should be implemented as a pilot project. This will allow for the design of ad hoc consensus algorithms for the energy market. In this way, it will be possible to validate the proposed framework as a standard guideline for similar platforms. This will help to reduce development costs and encourage the adoption of the system by companies and individuals.

Author Contributions: Funding acquisition, J.P. and J.M.C.; Investigation, Y.M.; Methodology, Y.M. and A.B.G.-G.; Project administration, Y.M.; Supervision, A.B.G.-G., A.M.d.R., J.P. and J.M.C.; Writing—original draft, Y.M. and A.B.G.-G.; Writing—review & editing, Y.M., A.B.G.-G. and A.M.d.R. All authors have read and agreed to the published version of the manuscript.

Funding: The research of Yeray Mezquita is supported by the pre-doctoral fellowship from the University of Salamanca and co-funded by Banco Santander. Besides this work has been partially supported by the Institute for Business Competitiveness of Castilla y León, and the European Regional Development Fund under grant CCTT3/20/SA/0002 (AIR-SCity project).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hirst, E.; Kirby, B. *Transmission Planning for a Restructuring US Electricity Industry*; Consulting in Electric-Industry Restructuring: Washington, DC, USA, 2001.
2. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart grid—The new and improved power grid: A survey. *IEEE Commun. Surv. Tutor.* **2011**, *14*, 944–980. [CrossRef]
3. Memon, A.A.; Kauhaniemi, K. A critical review of AC Microgrid protection issues and available solutions. *Electr. Power Syst. Res.* **2015**, *129*, 23–31. [CrossRef]
4. Bui, V.H.; Hussain, A.; Kim, H.M. A multiagent-based hierarchical energy management strategy for multi-microgrids considering adjustable power and demand response. *IEEE Trans. Smart Grid* **2016**, *9*, 1323–1333. [CrossRef]
5. Tosh, D.K.; Shetty, S.; Liang, X.; Kamhoua, C.; Njilla, L. Consensus protocols for blockchain-based data provenance: Challenges and opportunities. In Proceedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, USA, 19–21 October 2017; pp. 469–474.
6. Cameron, P.D.; Brothwood, M. *Competition in Energy Markets: Law and Regulation in the European Union*; Oxford University Press: Oxford, UK, 2002.
7. Von Danwitz, T. Regulation and Liberalization of the European Electricity Market-A German View. *Energy* **2006**, *27*, 423.

8. Mezquita, Y.; Casado-Vara, R.; González Briones, A.; Prieto, J.; Corchado, J.M. Blockchain-based architecture for the control of logistics activities: Pharmaceutical utilities case study. *Log. J. IGPL* **2021**, *29*, 974–985. [CrossRef]
9. Liang, X.; Shetty, S.; Tosh, D.; Kamhoua, C.; Kwiat, K.; Njilla, L. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Madrid, Spain, 14–17 May 2017; pp. 468–477.
10. Buterin, V. Ethereum: Platform Review. In *Opportunities and Challenges for Private and Consortium Blockchains*; Available online: http://www.smallake.kr/wp-content/uploads/2016/06/314477721-Ethereum-Platform-Review-Opportunities-and-Challenges-for-Private-and-Consortium-Blockchains.pdf (accessed on 19 April 2022).
11. Huh, S.; Cho, S.; Kim, S. Managing IoT devices using blockchain platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 19–22 February 2017; pp. 464–467.
12. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
13. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
14. Beikverdi, A.; Song, J. Trend of centralization in Bitcoin's distributed network. In Proceedings of the 2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Takamatsu, Japan, 1–3 June 2015; pp. 1–6.
15. Martinez, J. Understanding Proof of Stake: The Nothing at Stake Theory. 2018. Available online: https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027 (accessed on 9 October 2019).
16. Witherspoon, Z. A Hitchhiker's Guide to Consensus Algorithms. 2017. Available online: https://hackernoon.com/a-hitchhikers-guide-to-consensus-algorithms-d81aae3eb0e3 (accessed on 9 October 2019).
17. Abadi, J.; Brunnermeier, M. *Blockchain Economics*; Technical Report; National Bureau of Economic Research: Cambridge, MA, USA, 2018.
18. Sikorski, J.J.; Haughton, J.; Kraft, M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Appl. Energy* **2017**, *195*, 234–246. [CrossRef]
19. Weber, I.; Xu, X.; Riveret, R.; Governatori, G.; Ponomarev, A.; Mendling, J. Untrusted business process monitoring and execution using blockchain. In *International Conference on Business Process Management*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 329–347.
20. Khaqqi, K.N.; Sikorski, J.J.; Hadinoto, K.; Kraft, M. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. *Appl. Energy* **2018**, *209*, 8–19. [CrossRef]
21. Schöner, M.M.; Kourouklis, D.; Sandner, P.; Gonzalez, E.; Förster, J. *Blockchain Technology in the Pharmaceutical Industry*; Frankfurt School Blockchain Center: Frankfurt, Germany, 2017.
22. Sylim, P.; Liu, F.; Marcelo, A.; Fontelo, P. Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention. *JMIR Res. Protoc.* **2018**, *7*, e10163. [CrossRef]
23. Galvez, J.F.; Mejuto, J.; Simal-Gandara, J. Future challenges on the use of blockchain for food traceability analysis. *TrAC Trends Anal. Chem.* **2018**, *107*, 222–232. [CrossRef]
24. Kamath, R. Food traceability on blockchain: Walmart's pork and mango pilots with IBM. *J. Br. Blockchain Assoc.* **2018**, *1*, 3712. [CrossRef]
25. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef]
26. Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–17 September 2016; pp. 1–3.
27. Ekblaw, A.; Azaria, A.; Halamka, J.D.; Lippman, A. A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. In Proceedings of the IEEE Open & Big Data Conference, Vienna, Austria, 22–24 August 2016; Volume 13, p. 13.
28. Turkanović, M.; Hölbl, M.; Košič, K.; Heričko, M.; Kamišalić, A. EduCTX: A blockchain-based higher education credit platform. *IEEE Access* **2018**, *6*, 5112–5127. [CrossRef]
29. Grech, A.; Camilleri, A.F. Blockchain in Education. 2017. Available online: https://www.pedocs.de/volltexte/2018/15013/pdf/Grech_Camilleri_2017_Blockchain_in_Education.pdf (accessed on 19 April 2022).
30. Funk, E.; Riddell, J.; Ankel, F.; Cabrera, D. Blockchain technology: A data framework to improve validity, trust, and accountability of information exchange in health professions education. *Acad. Med.* **2018**, *93*, 1791–1794. [CrossRef]
31. Pop, C.; Cioara, T.; Antal, M.; Anghel, I.; Salomie, I.; Bertoncini, M. Blockchain based decentralized management of demand response programs in smart energy grids. *Sensors* **2018**, *18*, 162. [CrossRef]
32. Imbault, F.; Swiatek, M.; De Beaufort, R.; Plana, R. The green blockchain: Managing decentralized energy production and consumption. In Proceedings of the 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Milan, Italy, 6 June 2017; pp. 1–5.

33. Aitzhan, N.Z.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 840–852. [CrossRef]
34. Mengelkamp, E.; Gärttner, J.; Rock, K.; Kessler, S.; Orsini, L.; Weinhardt, C. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. *Appl. Energy* **2018**, *210*, 870–880. [CrossRef]
35. Pichler, M.; Meisel, M.; Goranovic, A.; Leonhartsberger, K.; Lettner, G.; Chasparis, G.; Vallant, H.; Marksteiner, S.; Bieser, H. Decentralized Energy Networks Based on Blockchain: Background, Overview and Concept Discussion. In Proceedings of the International Conference on Business Information Systems, Colorado Springs, CO, USA, 8–10 June 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 244–257.
36. Pylon Network Team. Pylon Network Whitepaper. The Energy Blockchain Platform. 2018. Available online: https://pylon-network.org/wp-content/uploads/2019/02/WhitePaper_PYLON_v2_ENGLISH-1.pdf (accessed on 6 November 2019).
37. Suncontract. Suncontract Whitepaper. An Energy Trading Platform that Utilises Blockchain Technology to Create A New Disruptive Model for Buying and Selling Electricity. 2017. Available online: https://suncontract.org/wp-content/uploads/2020/12/whitepaper.pdf (accessed on 6 November 2019).
38. Aliyev, N.; Brooks, S.; Hale, M.; Hoy, S. Enosi Green Paper 2018. Available online: https://github.com/enosi/green-paper/blob/master/enosi-green-paper.pdf (accessed on 19 April 2022).
39. Goranović, A.; Meisel, M.; Fotiadis, L.; Wilker, S.; Treytl, A.; Sauter, T. Blockchain applications in microgrids an overview of current projects and concepts. In Proceedings of the IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, China, 28 October–1 November 2017; pp. 6153–6158.
40. Koirala, B.P.; Koliou, E.; Friege, J.; Hakvoort, R.A.; Herder, P.M. Energetic communities for community energy: A review of key issues and trends shaping integrated community energy systems. *Renew. Sustain. Energy Rev.* **2016**, *56*, 722–744. [CrossRef]
41. Long, C.; Wu, J.; Zhou, Y.; Jenkins, N. Peer-to-peer energy sharing through a two-stage aggregated battery control in a community Microgrid. *Appl. Energy* **2018**, *226*, 261–276. [CrossRef]
42. Liu, N.; Yu, X.; Wang, C.; Li, C.; Ma, L.; Lei, J. Energy-sharing model with price-based demand response for microgrids of peer-to-peer prosumers. *IEEE Trans. Power Syst.* **2017**, *32*, 3569–3583. [CrossRef]
43. van Leeuwen, G.; AlSkaif, T.; Gibescu, M.; van Sark, W. An integrated blockchain-based energy management platform with bilateral trading for microgrid communities. *Appl. Energy* **2020**, *263*, 114613. [CrossRef]
44. Noor, S.; Yang, W.; Guo, M.; van Dam, K.H.; Wang, X. Energy Demand Side Management within micro-grid networks enhanced by blockchain. *Appl. Energy* **2018**, *228*, 1385–1398. [CrossRef]
45. European Parliament and Council: Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (Data Protection Directive). 2016. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (accessed on 9 December 2021).
46. Francisco, M.; Mezquita, Y.; Revollar, S.; Vega, P.; De Paz, J. Multi-agent distributed model predictive control with fuzzy negotiation. *Expert Syst. Appl.* **2019**, *129*, 68–83. [CrossRef]
47. Mezquita, Y.; Casado, R.; Gonzalez-Briones, A.; Prieto, J.; Corchado, J.M.; AETiC, A. Blockchain technology in IoT systems: Review of the challenges. *Ann. Emerg. Technol. Comput.* **2019**, *3*, 17–24. [CrossRef]
48. Combi, C. What Are Blockchain Confirmations and Why Do They Matter? 2017. Available online: https://coincentral.com/blockchain-confirmations/ (accessed on 19 April 2022).
49. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaría, V. Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet* **2018**, *10*, 20. [CrossRef]
50. Van Saberhagen, N. CryptoNote v 2.0. 2013. Available online: https://www.getmonero.org/ru/resources/research-lab/pubs/whitepaper_annotated.pdf (accessed on 19 April 2022).
51. Roy Walker. The Battle for Blockchain Privacy: Monero. 2018. Available online: https://medium.com/all-things-venture-capital/privacy-protocol-analysis-monero-c116d7c2106f (accessed on 19 April 2022).
52. Peng, Z.; Xu, C.; Wang, H.; Huang, J.; Xu, J.; Chu, X. P2b-trace: Privacy-preserving blockchain-based contact tracing to combat pandemics. In Proceedings of the 2021 International Conference on Management of Data, Xi'an, China, 20–25 June 2021; pp. 2389–2393.
53. Bünz, B.; Bootle, J.; Boneh, D.; Poelstra, A.; Wuille, P.; Maxwell, G. Bulletproofs: Short proofs for confidential transactions and more. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 21–23 May 2018; pp. 315–334.
54. Peng, Z.; Xu, J.; Chu, X.; Gao, S.; Yao, Y.; Gu, R.; Tang, Y. VFChain: Enabling verifiable and auditable federated learning via blockchain systems. *IEEE Trans. Netw. Sci. Eng.* **2021**, *9*, 173–186. [CrossRef]
55. Wu, H.; Peng, Z.; Guo, S.; Yang, Y.; Xiao, B. VQL: Efficient and Verifiable Cloud Query Services for Blockchain Systems. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *33*, 1393–1406. [CrossRef]

Capítulo 6

Conclusiones y Trabajo Futuro

VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

Capítulo 6

Conclusiones y Trabajo Futuro

El uso de la tecnología blockchain ofrece el potencial de acercar el sistema financiero a una economía verdaderamente democrática y comunitaria. Además, la posibilidad de implementar contratos inteligentes hace que los escenarios de uso no se limiten a las transacciones financieras, si no que cualquier activo valioso puede ser digitalizado y comercializado. Esto ha propiciado la aparición de investigaciones y proyectos piloto que pretenden desencadenar el cambio en diversos sectores industriales, como los sistemas logísticos (Mezquita, Casado-Vara, et al., 2021; Mezquita, González-Briones, et al., 2019), la administración electrónica (Mezquita, González-Briones, et al., 2019), los mercados energéticos (Mezquita, Gil-González, et al., 2022), etc. Con la tecnología blockchain se puede minimizar el factor humano, automatizar la mayoría de los procesos, y eliminar los intermediarios que no aportan valor real al producto final.

Sin embargo, no son pocos los retos a los que se enfrenta la implementación de esta tecnología en un escenario real. En esta Tesis Doctoral, además de la identificación de los retos a los que se enfrenta, se ha realizado un estudio de cómo otros trabajos de la literatura se han enfrentado a ellos en diversos ámbitos, teniendo en cuenta, de forma principal, cómo los estados están enfoncando sus propias soluciones, ya que de ellos depende la regulación necesaria para el porvenir de las tenologías distribuidas. Así mismo, en esta Tesis Doctoral también han aportado soluciones a estos retos, presentando dos arquitecturas que mejoran las ya existentes en la literatura, que pueden ser implementadas en escenarios reales de diferentes ámbitos de la industria.

Por lo tanto, este capítulo sirve para concluir la tesis y presentar posibles direcciones para el trabajo futuro. La Sección 6.1 expone las conclusiones extraídas del trabajo de investigación realizado en el marco de esta Tesis Doctoral y su relación con los objetivos

fijados al principio de la misma. La Sección 6.2 sugiere posibles direcciones para la investigación futura que surgen de los resultados y conclusiones de esta Tesis Doctoral.

6.1. Conclusiones

La tecnología blockchain tiene el potencial para disruptir, en términos de optimizar a la vez que democratizar, el paradigma industrial actual. Gracias a los principios de transparencia e inmutabilidad de los datos, añadido al uso de protocolos de criptográficos de identificación de los usuarios, puede añadir una capa adicional a las plataformas que mejore, no sólo la capacidad de trazabilidad de la información generada dentro de los sistemas, sino también la seguridad en las comunicaciones de los dispositivos que los conforman. Además, el desarrollo de contratos inteligentes permite la automatización de los servicios proporcionados por la industria actual. Por estos motivos ha sido objeto de estudio en esta Tesis Doctoral, llegando a las siguientes conclusiones:

- A pesar de que son importantes las bondades apuntadas, la tecnología blockchain ha sido **víctima de muchos mitos** al no haberse tenido en cuenta todos los **retos que enfrentan las DLTs**, y en especial la blockchain.

  Los desafíos a los que enfrenta esta tecnología pueden resumirse en: (i) escalabilidad de los sistemas, (ii) viabilidad del consumo energético de las redes, (iii) confianza de los datos provenientes del mundo real, (iiii) anonimicidad de los usuarios y su información generada, y (v) gestión de la responsabilidad en este tipo de plataformas. En la literatura previa, se había hecho incapié en la escalabilidad y viabilidad de los sistemas en cuanto a coste energético. Pero los trabajos de la literatura han dejado por tratar el resto de temas en alguna medida Mezquita, Casado, et al. (2019), o las plataformas en producción que hacen uso de esta tecnología suelen ser más bien simples y con un nivel alto de centralización (Mezquita, Gil-González, et al., 2022). Además, se suele asumir que los usuarios que forman parte de una de estas plataformas buscan el bienestar de la misma porque ganan más de un correcto funcionamiento, pero hay veces que fallos pueden ocurrir, incluso entre máquinas, por lo que nunca se tienen en cuenta el desarrollo de sistemas de auditabilidad que revisen el buen funcionamiento de estos sistemas. En esta Tesis Doctoral se ha conseguido desmitificar esta tecnología, desarrollando

sobre los retos que enfrenta y hasta qué punto puede ser beneficiosa, o no, para diferentes ámbitos de la industria actual (como las cadenas de suministro, los registros de propiedad, y los mercados automáticos), lo que ***responde a RQ1****.*

- Por otro lado, la forma de tener en cuenta la privacidad de los datos en este tipo de plataformas es mediante el almacenamiento off-chain de la información, algo que, si bien cumple con la GDPR, centraliza el proceso, perdiendo la democracia que se busca al utilizar este tipo de sistemas.

  En esta Tesis Doctoral se ha propuesto el uso de ZKPs y firmas en anillo para la encriptación de los datos y el uso de contratos inteligentes de forma anónima. Esta es una forma novedosa que no ha sido propuesta en la literatura pero que permitiría conservar la democracia de los datos, dejando que sean los usuarios los dueños de sus propios datos, generados de la interacción con la plataforma. Tras lo expuesto en esta Tesis Doctoral se puede asumir que se ha respondido ***tanto a RQ2 como a RQ3.***

- En este sentido, la principal contribución de esta Tesis Doctoral ha sido la investigación y diseño de este tipo de plataformas. Gracias al trabajo presentado aquí, investigadores y desarrolladores se benefician de modelos de arquitectura sobre los que pueden iterar para optimizar y/o implementar en escenarios reales.

  Esto es un avance respecto a lo ya propuesto en la literatura porque las arquitecturas presentadas en el Capítulo 3 mejoran, no sólo funcionalidad en muchos casos, si no que también cumplen rigurosamente con marcos legales rigurosos cómo el de la Unión Europea, además de favorecer la democratización de los datos, ya que se eliminan esos intermediarios encargados de almacenar la información fuera de la cadena de bloques, ***respondiendo a RQ4****.*

De este modo, tras ver respondidas en esta conclusión las preguntas de investigación planteadas para esta Tesis Doctoral en el capítulo 1, nos permitimos afirmar que se ha cumplido tanto con el objetivo principal, lo que permite comprobar la hipótesis también planteada en el Capítulo 1, como con los objetivos específicos que fueron definidos en el mismo:

(**OB1**) *Se procede a desmitificar la tecnología blcokchain, detallando cuáles son las cualidades que su uso puede aportar a los procesos de la industria actual, dominada por el Internet de las Cosas.*

En este sentido, se muestra en la Sección 2.2, qué puede y qué no puede hacer esta tecnología. Desarrollando sobre los posibles mitos y los problemas que enfrentan, por ejemplo el desarrollo de contratos inteligentes (Mezquita, Valdeolmillos, et al., 2019).

(**OB2**) *Identificar los requerimientos existentes para que la tecnología blockchain se pueda implementar en ámbitos dónde existe una gran cantidad de comunicaciones entre dispositivos.*

En relación con este objetivo, se desarrolla en la Sección 3.1, cómo se puede hacer uso de esta tecnología, teniendo en cuenta los desafíos presentados y publicados en Mezquita, Casado, et al. (2019).

(**OB3**) *Realizar un estudio del estado del arte en los ámbitos dónde la tecnología blockchain tiene un mayor potencial de disruptir.*

A este respecto, en el estado del arte detallado en el Capítulo 2 y publicado a lo largo de varios artículos Mezquita, Casado-Vara, et al. (2021); Mezquita, Gil-González, et al. (2022, 2021); Mezquita, González-Briones, et al. (2019, 2021); Mezquita, Parra-Domínguez, et al. (2022); Valdeolmillos et al. (2019), se muestran ámbitos de la industria que potencialmente más pueden ser disruptidos por la tecnología blcockhain.

(**OB4**) *Analizar los retos, motivaciones y problemas abiertos a la hora de aplicar las soluciones propuestas por la literatura.*

También en el Capítulo 2, y en específico en la Sección 2.3 se analizan las arquitecturas presentadas en la literatura, dejando claro que las soluciones propuestas, o bien son demasiado simples, o bien existe alguno de los desafíos que no han tenido en cuenta y por ello no pueden terminar siendo implementadas en un escenario real.

(**OB5**) *Diseñar arquitecturas que completen y mejoren los modelos propuestos previos.*

En las Secciones 3.2 y 3.3 se detallan los modelos propuestos. En la Sección 3.2 se detalla una arquitectura que hace especial énfasis en la necesidad de

hacer uso de teorías de juegos para el óptimo funcionamiento de las plataformas logísticas. Además, se muestra la posibilidad de hacer uso de una red blockchain pública, en un entorno en el que se busca la mayor transparencia posible de las transacciones realizadas en torno a los bienes de la cadena. En este aspecto, cualquier consumidor es capaz de realizar el seguimiento y trazabilidad de cualquier producto sin necesidad de ningún tipo de permisos.

Por su parte, en la Sección 3.3, se detalla un modelo para el intercambio de energía automático entre pares de una microred eléctrica. Este modelo es más complejo y requiere de una privacidad extrema, ya que los datos generados son muy delicados y una exposición de los mismos, vulnerabiliza a los usuarios. Aquí se detalla el uso de las ZKPs con el objetivo de encriptar la información almacenada, además de anonimizar a los usuarios al utilizar firmas en anillo. Este tipo de plataformas sólo pueden utilizarse en redes permisionadas, ya que no existe ninguna red pública que haya desarrollado el uso de contratos inteligentes y sea completamente anónima.

(**OB6**) *Validar los modelos propuestos analizando pormenorizadamente, cómo hacen frente a cada uno de los retos identificados.*

A lo largo del Capítulo 4 se muestra el análisis de las publicaciones realizadas, mostrando sus puntos fuertes respecto a las soluciones presentadas anteriormente en la literatura.

(**OB7**) *Diseñar un plan de trabajo futuro de cara al diseño e implantación de nuevos protocolos que ayuden en la aplicación de estas plataformas en un escenario futurista donde los ordenadores cuánticos sean una realidad, invalidando las técnicas actuales de encriptación e identificación.*

A partir de los resultados y conclusiones obtenidos durante el desarrollo del trabajo de investigación que culmina en esta Tesis Doctoral, se ha elaborado un plan de trabajo con las nuevas líneas de investigación que se abren de cara al futuro, resumidas en la Sección 6.2 a continuación.

6.2. Líneas Futuras de Investigación

Las arquitecturas propuestas en esta Tesis Doctoral hacen frente a los desafíos de la tecnología blcockhain para permitir su implementación en escenarios reales. Sin embargo, estas arquitecturas no podrían operar en un paradigma de computación cuántica con el diseño actual. Partiendo de este punto se pueden considerar las siguientes líneas de investigación futuras de cara a optimizar el rendimiento de los diseños presentados y hacerlos resistentes a un paradigma que puede que sea más cercano de lo que creemos (Mezquita, Alonso, Casado-Vara, Prieto, & Corchado, 2020).

(**LI1**) *Estudio y diseño de algoritmos criptográficos de firmado.* Con la llegada del paradigma de computación cuántica, los algoritmos criptográficos utilizados en las tecnologías blockchain actuales, durante el proceso de autenticación de usuarios, se quedarían obsoletos. Por esta razón se abre una nueva vía de investigación en este ámbito para el diseño y desarrollo de este tipo de algoritmos, con el fin de acelerar su implementación antes de que todas las redes blockchain queden expuestas.

(**LI2**) *Estudio y diseño de nuevos protocolos ZKP.* En un escenerario post-computación cuántica, se hace necesario el diseño de técnicas criptográficas que permitan encriptar la información y validarla con pruebas de conocimiento nulo. Por otro lado, se abre además una vía para el diseño de modelos de redes capaces de ejecutar este tipo de protocolos en contratos inteligentes.

(**LI3**) *Implementación de las plataformas en diversos escenarios reales.* Otra vía de trabajo futuro que se abre, es la evaluación de los modelos propuestos en escenarios reales, con el fin de poder evaluar qué algoritmos y protocolos son más óptimos para cada caso, por ejemplo en el caso de los ZKPs, el consenso entre los nodos de la red blockchain, los sistemas de auditabilidad que se pueden emplear, o los algoritmos de teorías de juego más óptimos para cada caso de estudio concreto.

Chapter 6

Conclusions and Future Work

VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

Chapter 6

Conclusions and Future Work

The use of blockchain technology offers the potential to bring the financial system closer to a truly democratic and communitarian economy. Moreover, the possibility of implementing smart contracts means that usage scenarios are not limited to financial transactions, but any valuable asset can be digitized and traded. This has led to the emergence of research and pilot projects that aim to trigger change in various industrial sectors, such as logistics systems (Mezquita, Casado-Vara, et al., 2021; Mezquita, González-Briones, et al., 2019), e-government (Mezquita, González-Briones, et al., 2019), energy markets (Mezquita, Gil-González, et al., 2022), etc. With blockchain technology, the human factor can be minimized, most processes can be automated, and intermediaries that do not add real value to the final product can be eliminated.

However, the challenges faced by the implementation of this technology in a real scenario are not few. In this Doctoral Thesis, in addition to the identification of the challenges faced, a study has been made of how other works in the literature have faced them in various fields, taking into account, mainly, how the states are focusing their own solutions, since the necessary regulation for the future of distributed technologies depends on them. Likewise, in this Doctoral Thesis they have also provided solutions to these challenges, presenting two architectures that improve those already existing in the literature, which can be implemented in real scenarios in different areas of the industry.

This chapter therefore serves to conclude the thesis and present possible directions for future work. Section 6.1 presents the conclusions drawn from the research work carried out within the framework of this Doctoral Dissertation and their relation to the objectives set at the beginning of the dissertation. Section 6.2 suggests possible directions for future research arising from the results and conclusions of this Doctoral Thesis.

6.1. Conclusions

The blockchain technology has the potential to disrupt, in terms of optimizing as well as democratizing, the current industrial paradigm. Thanks to the principles of transparency and immutability of data, added to the use of cryptographic protocols for user identification, it can add an additional layer to platforms that improves not only the traceability of the information generated within systems, but also the security of the communications of the devices that make them up. In addition, the development of smart contracts allows the automation of the services provided by the current industry. For these reasons it has been the subject of study in this Doctoral Thesis, reaching the following conclusions:

- Although the benefits mentioned above are important, blockchain technology has been the v**ictim of many myths** as all the **challenges faced by DLTs**, and especially blockchain, have not been taken into account.

  The challenges faced by this technology can be summarized as: (i) scalability of the systems, (ii) viability of the energy consumption of the networks, (iii) trust of data from the real world, (iiii) anonymity of the users and their generated information, and (v) liability management in this type of platform. In previous literature, emphasis had been placed on the scalability and feasibility of the systems in terms of energy cost. But the works in the literature have left the remaining issues unaddressed to some extent Mezquita, Casado, et al. (2019), or the platforms in production that make use of this technology tend to be rather simple and with a high level of centralization (Mezquita, Gil-González, et al., 2022). In addition, it is usually assumed that users who are part of one of these platforms seek the welfare of the platform because they gain more from a correct operation, but there are times when failures can occur, even between machines, so the development of auditability systems that review the proper functioning of these systems are never taken into account. In this Doctoral Thesis we have managed to demystify this technology, developing on the challenges it faces and to what extent it can be beneficial, or not, for different areas of the current industry (such as supply chains, property registries, and automated markets), which ***answers RQ1****.*

- On the other hand, the way to take into account data privacy in this type of platforms is through off-chain storage of the information, something that, although it complies with the GDPR, centralizes the process, losing the democracy that is sought when using this type of systems.

  In this Doctoral Thesis, the use of ZKPs and ring signatures for data encryption and the use of smart contracts in an anonymous way has been proposed. This is a novel way that has not been proposed in the literature but that would allow to preserve the democracy of the data, letting the users be the owners of their own data, generated from the interaction with the platform. After what has been exposed in this Doctoral Thesis, it can be assumed that ***both RQ2 and RQ3 have been answered****.*

- In this sense, the main contribution of this Doctoral Thesis has been the research and design of this type of platforms. Thanks to the work presented here, researchers and developers benefit from architectural models on which they can iterate to optimize and/or implement in real scenarios.

  That is an advance over what has already been proposed in the literature because these architectures improve not only functionality in many cases, but also rigorously comply with strict legal frameworks such as that of the European Union, in addition to favoring the democratization of data, since those intermediaries responsible for storing information outside the blockchain are eliminated, ***responding to RQ4****.*

Thus, after seeing answered in this conclusion the research questions posed for this Doctoral Thesis in Chapter 1, we can affirm that both the main objective has been fulfilled, which allows us to verify the hypothesis also posed in Chapter 1, and the specific objectives that were defined therein:

(**OB1**) *We proceed to demystify the blcokchain technology, detailing the qualities that its use can bring to the processes of today's industry, dominated by the Internet of Things.*

In this regard, it is shown in Section 2.2, what this technology can and cannot do. Developing about the possible myths and the problems they face, for example the development of smart contracts (Mezquita, Valdeolmillos, et al., 2019).

(**OB2**) *Identify the existing requirements so that blockchain technology can be implemented in areas where there is a large amount of communication between devices.*

In relation to this objective, it is developed in Section 3.1, how this technology can be used, taking into account the challenges presented and published in Mezquita, Casado, et al. (2019).

(**OB3**) *Conduct a study of the state of the art in the areas where blockchain technology has the greatest potential for disruption.*

In this regard, the state of the art detailed in Chapter 2 and published across several articles Mezquita, Casado-Vara, et al. (2021); Mezquita, Gil-González, et al. (2022, 2021); Mezquita, González-Briones, et al. (2019, 2021); Mezquita, Parra-Domínguez, et al. (2022); Valdeolmillos et al. (2019), shows areas of the industry potentially most likely to be disrupted by blockchain technology.

(**OB4**) *Analyze the challenges, motivations and open problems when applying the solutions proposed by the literature.*

Also in Chapter 2, and specifically in Section 2.3, the architectures presented in the literature are analyzed, making it clear that the proposed solutions are either too simple, or there are some of the challenges that have not been taken into account and therefore cannot be implemented in a real scenario.

(**OB5**) *Designing architectures that complement and improve the previous proposed models.*

The proposed models are detailed in Sections 3.2 and 3.3. Section 3.2 details an architecture that makes special emphasis on the need to make use of game theories for the optimal functioning of logistics platforms. In addition, the possibility of making use of a public blockchain network is shown, in an environment in which the greatest possible transparency of the transactions carried out around the goods in the chain is sought. In this aspect, any consumer is able to track and trace any product without the need for any type of permissions.

In Section 3.3, a model for automatic energy exchange between peers of an electric microgrid is detailed. This model is more complex and requires extreme

privacy, since the data generated is very sensitive and its exposure would make users vulnerable. The use of ZKPs is detailed here with the objective of encrypting the stored information, in addition to anonymizing the users by using ring signatures. This type of platform can only be used in permissioned networks, since there is no public network that has developed the use of smart contracts and is completely anonymous.

(**OB6**) *Validate the proposed models by analyzing in detail how they address each of the challenges identified.* Throughout the Chapter 4 shows the analysis of the publications made, showing their strengths with respect to the solutions previously presented in the literature.

(**OB7**) *Design a future work plan for the design and implementation of new protocols that will help in the application of these platforms in a futuristic scenario where quantum computers become a reality, invalidating current encryption and identification techniques.*

Based on the results and conclusions obtained during the development of the research work that culminates in this Doctoral Thesis, a work plan has been drawn up with the new lines of research that are open for the future, summarized in the following section, Section 6.2.

6.2. Future Lines of Research

The architectures proposed in this PhD Thesis address the challenges of blcockhain technology to enable its implementation in real scenarios. However, these architectures could not operate in a quantum computing paradigm with the current design. From this point, the following lines of future research can be considered in order to optimize the performance of the presented designs and make them resilient to a paradigm that may be closer than we think (Mezquita et al., 2020).

(**RL1**) *Study and design of cryptographic signing algorithms.* With the advent of the quantum computing paradigm, the cryptographic algorithms used in current blockchain technologies, during the user authentication process, would become obsolete. For this reason, a new avenue of research is opened in this area for the

design and development of this type of algorithms, in order to accelerate their implementation before all blockchain networks are exposed.

(**RL2**) *Study and design of new ZKP protocols.* In a post-quantum computing scenario, it is necessary to design cryptographic techniques to encrypt information and validate it with zero-knowledge proofs. On the other hand, it also opens a way for the design of network models capable of executing this type of protocols in smart contracts.

(**RL3**) *Implementation of the platforms in different real scenarios.* Another avenue of future work that opens up, is the evaluation of the proposed models in real scenarios, in order to be able to evaluate which algorithms and protocols are more optimal for each case, for example in the case of ZKPs, the consensus between the nodes of the blockchain network, the auditability systems that can be employed, or the most optimal game-theoretic algorithms for each specific case study.

Bibliografía

Aitzhan, N. Z., & Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, *15*(5), 840–852.

Aitzhan, N. Z., & Svetinovic, D. (2018). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, *15*(5), 840–852.

Asolo, B. (2018, December). *Blockchain oracles explained.* Descargado de `https://www.mycryptopedia.com/blockchain-oracles-explained/` ([Accessed; 04/10/2019])

Banerjee, S., & Hecker, J. P. (2017). A multi-agent system approach to load-balancing and resource allocation for distributed computing. En *First complex systems digital campus world e-conference 2015* (pp. 41–54).

Barn, B., Barat, S., & Clark, T. (2017). Conducting systematic literature reviews and systematic mapping studies. En *Proceedings of the 10th innovations in software engineering conference* (pp. 212–213).

Baskerville, R. L. (1999). Investigating information systems with action research. *Communications of the Association for Information Systems*, *2*(1), 19.

Benjamin, R., & Wigand, R. (1995). Electronic markets and virtual value chains on the information superhighway. *MIT Sloan Management Review*, *36*(2), 62.

Bentov, I., Gabizon, A., & Mizrahi, A. (2016). Cryptocurrencies without proof of work. En *International conference on financial cryptography and data security* (pp. 142–157).

Bessani, A., Sousa, J., & Alchieri, E. E. (2014). State machine replication for the masses with bft-smart. En *2014 44th annual ieee/ifip international conference on dependable systems and networks* (pp. 355–362).

bitcoin.it (Ed.). (s.f.). *Script bitcoin.* Descargado de `https://en.bitcoin.it/wiki/Script` (Accessed: 04/10/2019)

Briones, A. G., Chamoso, P., Rivas, A., Rodríguez, S., Prieta, F. D. L., Prieto, J., & Corchado, J. M. (2018). Use of gamification techniques to encourage garbage recycling. a smart city approach. En *International conference on knowledge management in organizations* (pp. 674–685).

Buterin, V. (2016, June). *Critical update re: Dao vulnerability.* Descargado de `https://ethereum.github.io/blog/2016/06/17/critical-update-re-dao-vulnerability/` ([Accessed; 04/10/2019])

Buterin, V., y cols. (2014). A next-generation smart contract and decentralized application platform. *white paper*, *3*, 37.

Calvo, J. A. L., & Mathar, R. (2018). Secure blockchain-based communication scheme for connected vehicles. En *2018 european conference on networks and communications (eucnc)* (pp. 347–351).

Cano, M. R. (2017). *Social blockchain revolution* (Tesis Doctoral, Universitat Pompeu Fabra). Descargado de `https://bit.ly/363alRM`

Cardoso, F. N. (2019). Criptomonedas (en especial, bitcóin) y blanqueo de dinero. *Revista electrónica de ciencia penal y criminología*(21), 14.

Carrascosa, C., Bajo, J., Julián, V., Corchado, J. M., & Botti, V. (2008). Hybrid multi-agent architecture as a real-time problem-solving model. *Expert Systems with Applications*, *34*(1), 2–17.

Casado-Vara, R., Chamoso, P., De la Prieta, F., Prieto, J., & Corchado, J. M. (2019). Non-linear adaptive closed-loop control system for improved efficiency in iot-blockchain management. *Information Fusion*, *49*, 227–239.

Casado-Vara, R., & Corchado, J. M. (2018). Blockchain for democratic voting: how blockchain could cast off voter fraud. *Orient. J. Comp. Sci. Technol*, *11*(1).

Casado-Vara, R., González-Briones, A., Prieto, J., & Corchado, J. M. (2018). Smart contract for monitoring and control of logistics activities: pharmaceutical utilities case study. En *The 13th international conference on soft computing models in industrial and environmental applications* (pp. 509–517).

Casto, A. (2017, August). *One of ethereum's earliest smart contract languages is headed for retirement.* Descargado de `https://www.coindesk.com/one-of-ethereums-earliest-smart-contract-languages-is-headed-for-retirement` ([Accessed; 04/10/2019])

Chamoso, P., González-Briones, A., Rodríguez, S., & Corchado, J. M. (2018). Tendencies of technologies and platforms in smart cities: a state-of-the-art review. *Wireless Communications and Mobile Computing*, *2018*.

Christopher, M. (2016). *Logistics & supply chain management*. Pearson Uk.

Combi, C. (2017, May). *What are blockchain confirmations and why do they matter?* Descargado de `https://coincentral.com/blockchain-confirmations/` ([Online; updated 10-October-2018])

ConsenSys. (2018, December). *Ethereum by the numbers.* Descargado de `https://media.consensys.net/ethereum-by-the-numbers-3520f44565a9` ([Accessed; 04/10/2019])

Coria, J. A. G., Castellanos-Garzón, J. A., & Corchado, J. M. (2014). Intelligent business processes composition based on multi-agent systems. *Expert Systems with Applications*, *41*(4), 1189–1205.

Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., y cols. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.

Daian, P. (2016, June). *Analysis of the dao exploit.* Descargado de `http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/` (Accessed: 04/10/2019)

Daza, V., Di Pietro, R., Klimek, I., & Signorini, M. (2017). Connect: Contextual name discovery for blockchain-based services in the iot. En *2017 ieee international conference on communications (icc)* (pp. 1–6).

Domínguez, J. P., Pons, M. E. P., Martín, Y. M., & Rodríguez, J. M. C. (2020). Beneficios de la incorporación de la tecnología blockchain en el proceso de registro de la propiedad. En *Blockchain: Impacto en los sistemas financiero, notarial, registral y judicial* (pp. 1029–1043).

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for iot security and privacy: The case study of a smart home. En *2017 ieee international conference on pervasive computing and communications workshops (percom workshops)* (pp. 618–623).

Durić, B. O. (2017). Organisational metamodel for large-scale multi-agent systems: first steps towards modelling organisation dynamics. *Adv. Distrib. Comput. Artif. Intell. J*, *6*(3), 2017.

Earle, T. C. (2009). Trust, confidence, and the 2008 global financial crisis. *Risk Analysis: An International Journal*, *29*(6), 785–792.

Eden, C., & Ackermann, F. (2018). Theory into practice, practice to theory: Action research in method development. *European Journal of Operational Research*, *271*(3), 1145–1155.

Enosi. (2018, April). *Enosi whitepaper. providing consumers with choice, transparency and efciency.* Descargado de `https://bit.ly/33wANTj` ([Online; Last visited 06-November-2019])

Ethereum. (s.f.). *A python interface for interacting with the Ethereum blockchain and ecosystem.* Autor. Descargado de `https://web3py.readthedocs.io/en/stable/`

European parliament and council: Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (data protection directive). (2016). Descargado de `https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679` ([Accessed; 09/12/2021])

Fang, X., Misra, S., Xue, G., & Yang, D. (2011). Smart grid—the new and improved power grid: A survey. *IEEE communications surveys & tutorials*, *14*(4), 944–980.

Finch, S. (2019, September). *Japan shows yen for blockchain innovation.* Descargado de `https://www.asiapropertyawards.com/en/japan-shows-yen-for-blockchain-innovation` ([Accessed; 18/04/2020])

Francisco, M., Mezquita, Y., Revollar, S., Vega, P., & De Paz, J. F. (2019). Multi-agent distributed model predictive control with fuzzy negotiation. *Expert Systems with Applications*, *129*, 68–83.

García, L. I. (2017). Narcotráfico en la darkweb: los criptomercados. *URVIO Revista Latinoamericana de Estudios de Seguridad*(21), 191–206.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet*, *10*(2), 20.

Gazafroudi, A. S., Afshar, K., & Bigdeli, N. (2015). Assessing the operating reserves and costs with considering customer choice and wind power uncertainty in pool-based power market. *International Journal of Electrical Power & Energy Systems*, *67*, 202–215.

Gazafroudi, A. S., Pinto, T., Prieto-Castrillo, F., Prieto, J., Corchado, J. M., Jozi, A., ... Venayagamoorthy, G. K. (2017). Organization-based multi-agent structure of the smart home electricity system. En *2017 ieee congress on evolutionary computation*

(cec) (pp. 1327–1334).

González-Briones, A., Castellanos-Garzón, J. A., Mezquita Martín, Y., Prieto, J., & Corchado, J. M. (2018). A framework for knowledge discovery from wireless sensor networks in rural environments: a crop irrigation systems case study. *Wireless Communications and Mobile Computing*, *2018*.

González-Briones, A., Chamoso, P., Casado-Vara, R., Rivas, A., Omatu, S., & Corchado, J. M. (2019). *Internet of things platform to encourage recycling in a smart city.* Elsevier, Amsterdam.

González-Briones, A., Chamoso, P., De La Prieta, F., Demazeau, Y., & Corchado, J. M. (2018). Agreement technologies for energy optimization at home. *Sensors*, *18*(5), 1633.

Goranović, A., Meisel, M., Fotiadis, L., Wilker, S., Treytl, A., & Sauter, T. (2017). Blockchain applications in microgrids an overview of current projects and concepts. En *Iecon 2017-43rd annual conference of the ieee industrial electronics society* (pp. 6153–6158).

Gros, D., & Roth, F. (2010). The financial crisis and citizen trust in the european central bank. *CEPs working document*(334).

Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: trick or treat? En *Proceedings of the hamburg international conference of logistics (hicl)* (pp. 3–18).

Herreras, E. B. (2004). La docencia a través de la investigación-acción. *Revista iberoamericana de educación*, *35*(1), 1–9.

Hirst, E., & Kirby, B. (2001). *Transmission planning for a restructuring us electricity industry.* Consulting in Electric-Industry Restructuring.

Huh, S., Cho, S., & Kim, S. (2017). Managing iot devices using blockchain platform. En *2017 19th international conference on advanced communication technology (icact)* (pp. 464–467).

Imbault, F., Swiatek, M., De Beaufort, R., & Plana, R. (2017). The green blockchain: Managing decentralized energy production and consumption. En *2017 ieee international conference on environment and electrical engineering and 2017 ieee industrial and commercial power systems europe (eeeic/i&cps europe)* (pp. 1–5).

Khan, M. A., & Salah, K. (2018). Iot security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, *82*, 395–411.

Kroll, J. A., Davey, I. C., & Felten, E. W. (2013). The economics of bitcoin mining, or bitcoin in the presence of adversaries. En *Proceedings of weis* (Vol. 2013).

Kshetri, N. (2017). Can blockchain strengthen the internet of things? *IT professional*, *19*(4), 68–72.

Kshetri, N., & Voas, J. (2018). Blockchain in developing countries. *It Professional*, *20*(2), 11–14.

Kvedar, J., Coye, M. J., & Everett, W. (2014). Connected health: a review of technologies and strategies to improve patient care with telemedicine and telehealth. *Health affairs*, *33*(2), 194–199.

Lavorgna, A. (2016). How the use of the internet is affecting drug trafficking practices.

Lazuashvili, N. (2019). *Integration of the blockchain technology into the land registration system. a case study of georgia* (Tesis Doctoral). doi: 10.13140/RG.2.2.35689 .13920/1

Lazuashvili, N., Norta, A., & Draheim, D. (2019). Integration of blockchain technology into a land registration system for immutable traceability: A casestudy of georgia. En *International conference on business process management* (pp. 219–233).

Lemieux, V. L. (2017). Evaluating the use of blockchain in land transactions: An archival science perspective. *European Property Law Journal*, *6*(3), 392–440.

Li, K., Zhou, T., Liu, B.-h., & Li, H. (2018). A multi-agent system for sharing distributed manufacturing resources. *Expert Systems with Applications*, *99*, 32–43.

Li, T., Sun, S., Bolić, M., & Corchado, J. M. (2016). Algorithm design for parallel implementation of the smc-phd filter. *Signal Processing*, *119*, 115–127.

Liang, X., Zhao, J., Shetty, S., & Li, D. (2017). Towards data assurance and resilience in iot using blockchain. En *Milcom 2017-2017 ieee military communications conference (milcom)* (pp. 261–266).

Lima, A. C. E., de Castro, L. N., & Corchado, J. M. (2015). A polarity analysis framework for twitter messages. *Applied Mathematics and Computation*, *270*, 756–767.

Lin, H., & Bergmann, N. W. (2016). Iot privacy and security challenges for smart home environments. *Information*, *7*(3), 44.

Long, C., Wu, J., Zhou, Y., & Jenkins, N. (2018). Peer-to-peer energy sharing through a two-stage aggregated battery control in a community microgrid. *Applied energy*, *226*, 261–276.

Martinez, J. (2018, June). *Understanding proof of stake: The nothing at stake theory.* Descargado de `https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027` ([Accessed; 09/10/2019])

Mavilia, R., & Pisani, R. (2019). Blockchain and catching-up in developing countries: The case of financial inclusion in africa. *African Journal of Science, Technology, Innovation and Development*, 1–13.

McMurren, J., Young, A., & Verhulst, S. (2018). Addressing transaction costs through blockchain and identity in swedish land transfers. *Blockchain Technologies for Social Change, GovLab*.

Memon, A. A., & Kauhaniemi, K. (2015). A critical review of ac microgrid protection issues and available solutions. *Electric Power Systems Research*, *129*, 23–31.

Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C. (2018). Designing microgrid energy markets: A case study: The brooklyn microgrid. *Applied Energy*, *210*, 870–880.

Mezquita, Y., Alonso, R. S., Casado-Vara, R., Prieto, J., & Corchado, J. M. (2020). A review of k-nn algorithm based on classical and quantum machine learning. En *International symposium on distributed computing and artificial intelligence* (pp. 189–198).

Mezquita, Y., Casado, R., Gonzalez-Briones, A., Prieto, J., Corchado, J. M., & AETiC, A. (2019). Blockchain technology in iot systems: review of the challenges. *Annals of Emerging Technologies in Computing (AETiC), Print ISSN*, 2516–0281.

Mezquita, Y., Casado-Vara, R., González Briones, A., Prieto, J., & Corchado, J. M. (2021). Blockchain-based architecture for the control of logistics activities: Pharmaceutical utilities case study. *Logic Journal of the IGPL*, *29*(6), 974–985.

Mezquita, Y., Gazafroudi, A. S., Corchado, J. M., Shafie-Khah, M., Laaksonen, H., & Kamišalić, A. (2019). Multi-agent architecture for peer-to-peer electricity trading based on blockchain technology. En *2019 xxvii international conference on information, communication and automation technologies (icat)* (pp. 1–6).

Mezquita, Y., Gil-González, A. B., Martín del Rey, A., Prieto, J., & Corchado, J. M. (2022). Towards a blockchain-based peer-to-peer energy marketplace. *Energies*, *15*(9), 3046.

Mezquita, Y., Gil-González, A. B., Prieto, J., & Corchado, J. M. (2021). Cryptocurrencies and price prediction: A survey. En *International congress on*

blockchain and applications (pp. 339–346).

Mezquita, Y., González-Briones, A., Casado-Vara, R., Chamoso, P., Prieto, J., & Corchado, J. M. (2019). Blockchain-based architecture: a mas proposal for efficient agri-food supply chains. En *International symposium on ambient intelligence* (pp. 89–96).

Mezquita, Y., González-Briones, A., Casado-Vara, R., Wolf, P., Prieta, F. d. l., & Gil-González, A.-B. (2021). Review of privacy preservation with blockchain technology in the context of smart cities. En *Sustainable smart cities and territories international conference* (pp. 68–77).

Mezquita, Y., Parra, J., Perez, E., Prieto, J., & Corchado, J. M. (2019). Blockchain-based systems in land registry, a survey of their use and economic implications. En *Computational intelligence in security for information systems conference* (pp. 13–22).

Mezquita, Y., Parra-Domínguez, J., Pérez-Pons, M. E., Prieto, J., & Manuel Corchado, J. (2022). Blockchain-based land registry platforms: A survey on their implementation and potential challenges. *Logic Journal of the IGPL*.

Mezquita, Y., Valdeolmillos, D., González-Briones, A., Prieto, J., & Corchado, J. M. (2019). Legal aspects and emerging risks in the use of smart contracts based on blockchain. En *International conference on knowledge management in organizations* (pp. 525–535).

Miller, A., Xia, Y., Croman, K., Shi, E., & Song, D. (2016). The honey badger of bft protocols. En *Proceedings of the 2016 acm sigsac conference on computer and communications security* (pp. 31–42).

Millones Reque, J. M. (2019). Fines del proceso de la tercería de propiedad y su problemática frente al derecho registral.

Najafi, S., Talari, S., Gazafroudi, A. S., Shafie-khah, M., Corchado, J. M., & Catalão, J. P. (2018). Decentralized control of dr using a multi-agent method. En *Sustainable interdependent networks* (pp. 233–249). Springer.

Nakamoto, S., y cols. (2008). Bitcoin: A peer-to-peer electronic cash system.

network, P. (2018, December). *Pylon network whitepaper. the energy blockchain platform.* Descargado de `https://pylon-network.org/pylon-network-blockchain` ([Online; Last visited 06-November-2019])

Nikolić, I., Kolluri, A., Sergey, I., Saxena, P., & Hobor, A. (2018). Finding the greedy, prodigal, and suicidal contracts at scale. En *Proceedings of the 34th annual*

computer security applications conference (pp. 653–663).

Palai, A., Vora, M., & Shah, A. (2018). Empowering light nodes in blockchains with block summarization. En *2018 9th ifip international conference on new technologies, mobility and security (ntms)* (pp. 1–5).

Palladino, S. (2017, July). *The parity wallet hack explained.* Descargado de `https://blog.openzeppelin.com/on-the-parity-wallet-multisig-hack-405a8c12e8f7/` (Accessed: 04/10/2019)

Peng, Z., Xu, J., Chu, X., Gao, S., Yao, Y., Gu, R., & Tang, Y. (2021). Vfchain: enabling verifiable and auditable federated learning via blockchain systems. *IEEE Transactions on Network Science and Engineering*, *9*(1), 173–186.

Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2008). Systematic mapping studies in software engineering. En *12th international conference on evaluation and assessment in software engineering (ease) 12* (pp. 1–10).

Pichler, M., Meisel, M., Goranovic, A., Leonhartsberger, K., Lettner, G., Chasparis, G., ... Bieser, H. (2018). Decentralized energy networks based on blockchain: Background, overview and concept discussion. En *International conference on business information systems* (pp. 244–257).

Pop, C., Cioara, T., Antal, M., Anghel, I., Salomie, I., & Bertoncini, M. (2018). Blockchain based decentralized management of demand response programs in smart energy grids. *Sensors*, *18*(1), 162.

Popov, S. (2018). The tangle. *White paper*, *1*(3).

Rose, N. (2000). Government and control. *British journal of criminology*, *40*(2), 321–339.

Roy Walker. (2018). *The battle for blockchain privacy: Monero.* (`https://medium.com/all-things-venture-capital/privacy-protocol-analysis-monero-c116d7c2106f`)

Ryan, D. (2017, May). *Calculating costs in ethereum contracts.* Descargado de `https://hackernoon.com/ether-purchase-power-df40a38c5a2f` ([Accessed; 04/10/2019])

Schwartz, D., Youngs, N., Britto, A., y cols. (2014). The ripple protocol consensus algorithm. *Ripple Labs Inc White Paper*, *5*, 8.

Shang, Q., & Price, A. (2019). A blockchain-based land titling project in the republic of georgia: Rebuilding public trust and lessons for future pilot projects. *Innovations: Technology, Governance, Globalization*, *12*(3-4), 72–78.

Singh, A., Chawla, N., Ko, J. H., Kar, M., & Mukhopadhyay, S. (2018). Energy efficient and side-channel secure cryptographic hardware for iot-edge nodes. *IEEE Internet of Things Journal*, *6*(1), 421–434.

Singh, R., Tanwar, S., & Sharma, T. P. (2020). Utilization of blockchain for mitigating the distributed denial of service attacks. *Security and Privacy*, *3*(3), e96.

solidity.readthedocs.io (Ed.). (s.f.). *Introduction to smart contracts.* Descargado de `https://solidity.readthedocs.io/en/latest/introduction-to-smart-contracts.html` ([Accessed; 04/10/2019])

Suncontract. (2017, April). *Suncontract whitepaper. an energy trading platform that utilises blockchain technology to create a new disruptive model for buying and selling electricity.* Descargado de `https://suncontract.org/tokensale/res/whitepaper.pdf` ([Online; Last visited 06-November-2019])

Taboada, P. S. (2017). ¿por qué las organizaciones criminales utilizan criptomonedas? los bitcoins en el crimen organizado. *El Criminalista Digital. Papeles de Criminología*(6), 1-41.

Tapia, D. I., Fraile, J. A., Rodríguez, S., Alonso, R. S., & Corchado, J. M. (2013). Integrating hardware agents into an enhanced multi-agent architecture for ambient intelligence systems. *Information Sciences*, *222*, 47–65.

Tat-Kei Ho, A. (2002). Reinventing local governments and the e-government initiative. *Public administration review*, *62*(4), 434–444.

Tijan, E., Aksentijević, S., Ivanić, K., & Jardas, M. (2019). Blockchain technology implementation in logistics. *Sustainability*, *11*(4), 1185.

Ting, L. T. (2017, July). *Beginners guide to ethereum (3) — explain the genesis file and use it to customize your blockchain.* Descargado de `https://bit.ly/3jjogO3` ([Accessed; 09/10/2019])

Tüzün, E., Tekinerdogan, B., Macit, Y., & İnce, K. (2019). Adopting integrated application lifecycle management within a large-scale software company: An action research approach. *Journal of Systems and Software*, *149*, 63–82.

Valdeolmillos, D., Mezquita, Y., González-Briones, A., Prieto, J., & Corchado, J. M. (2019). Blockchain technology: a review of the current challenges of cryptocurrency. En *International congress on blockchain and applications* (pp. 153–160).

van Leeuwen, G., AlSkaif, T., Gibescu, M., & van Sark, W. (2020). An integrated blockchain-based energy management platform with bilateral trading for microgrid communities. *Applied Energy*, *263*, 114613.

Van Saberhagen, N. (2013). Cryptonote v 2.0.

Vukolić, M. (2015). The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. En *International workshop on open problems in network security* (pp. 112–125).

West, D. M. (2004). E-government and the transformation of service delivery and citizen attitudes. *Public administration review*, *64*(1), 15–27.

Wooldridge, M., & Jennings, N. R. (1995). Intelligent agents: Theory and practice. *The knowledge engineering review*, *10*(2), 115–152.

Wu, H., Peng, Z., Guo, S., Yang, Y., & Xiao, B. (2021). Vql: Efficient and verifiable cloud query services for blockchain systems. *IEEE Transactions on Parallel and Distributed Systems*, *33*(6), 1393–1406.

Xie, R. (2019). Why china had to ban cryptocurrency but the us did not: A comparative analysis of regulations on crypto-markets between the us and china. *Wash. U. Global Stud. L. Rev.*, *18*, 457.

Yildiz, M. (2007). E-government research: Reviewing the literature, limitations, and ways forward. *Government information quarterly*, *24*(3), 646–665.

Yuan, Y., & Wang, F.-Y. (2016). Towards blockchain-based intelligent transportation systems. En *2016 ieee 19th international conference on intelligent transportation systems (itsc)* (pp. 2663–2668).

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, *40*(10), 1–8.