Universidad Zaragoza
1542

Trabajo Fin de Grado

Sistema de Identidad Auto-Soberana basado en Blockchain para el manejo del historial médico de pacientes.

Blockchain-based Self-Sovereign Identity System for managing patient medical records.

Autor

Miguel Millán Montañés

Directores

Rodrigo Casamayor Moragriega

José Ramón Gállego Martínez

ESCUELA DE INGENIERÍA Y ARQUITECTURA

2022

TRABAJOS DE FIN DE GRADO / FIN DE MÁSTER

Escuela de Ingeniería y Arquitectura Universidad Zaragoza

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD

(Este documento debe remitirse a seceina@unizar.es dentro del plazo de depósito)

D./Dª. MIGUEL MILLÁN MONTAÑÉS ,

en aplicación de lo dispuesto en el art. 14 (Derechos de autor) del Acuerdo de 11 de septiembre de 2014, del Consejo de Gobierno, por el que se aprueba el Reglamento de los TFG y TFM de la Universidad de Zaragoza,

Declaro que el presente Trabajo de Fin de Estudios de la titulación de Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación (Título del Trabajo)

Sistema de Identidad Auto-Soberana basado en Blockchain para el manejo del historial médico de pacientes.

es de mi autoría y es original, no habiéndose utilizado fuente sin ser citada debidamente.

Zaragoza, 02 DE AGOSTO DE 2022

Fdo: MIGUEL MILLÁN MONTAÑÉS

AGRADECIMIENTOS

Quiero agradecer a todas las personas que han formado parte de mi Camino durante mi etapa como estudiante y que han impactado en mi desarrollo personal y profesional.

Gracias a mi familia, que ha estado siempre a mi lado, que ha confiado siempre en mi y que me ha apoyado incondicionalmente.

Gracias a mis "telecompis"por estar siempre ahí, incluso en los momentos más difíciles de esta parte de mi vida, gracias por las infinitas experiencias y recuerdos.

Gracias a Inycom y especialmente a Rodrigo Casamayor por guiarme en el desarrollo de este trabajo haciendo uso de una tecnología completamente nueva y desconocida para mi.

RESUMEN

La digitalización de los procesos en entornos clínicos genera una gran cantidad de datos de carácter sensible que han de almacenarse de forma segura. Además, estos datos se encuentran fragmentados entre los distintos proveedores de servicios sanitarios, dificultando así el acceso al historial completo de un paciente.

En los últimos años se ha desatado un interés por las criptomonedas tan solo comparable a la fiebre del oro o a la explosión de Internet en los años 90. Sin embargo la parte interesante de estos "tokens digitales" es la tecnología que permite su funcionamiento, la Blockchain. Una tecnología que garantiza, mediante la descentralización, la transparencia, autenticidad e inmutabilidad de la información. Todas estas características podrían aplicarse al almacenamiento de datos médicos.

El objetivo de este trabajo es validar el uso de la tecnología Blockchain para el tratamiento de información médica y analizar el estado de implantación actual. Para ello, se ha implementado una plataforma, basada en el framework HyperLedger Indy, que permite a los pacientes acceder a sus analíticas y recetas gracias a la Blockchain. Se ha tenido que investigar a fondo el estado de la tecnología, analizar los distintos proyectos puestos en marcha y la madurez de los mismos, identificar problemas y diseñar e implementar una solución viable.

Índice

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

El rápido avance de la digitalización en los sistemas de salud ha generado en las últimas décadas una gran cantidad de datos sensibles que han de almacenarse de forma segura. Sin embargo, estos sistemas no son actualizados periódicamente y usan software obsoleto, lo que se traduce en que, tan solo en 2021, al menos 45 millones de historiales médicos han sido filtrados y robados [1].

La fragmentación de los datos médicos y la correspondiente dificultad para acceder a ellos causa el 18 % de los errores médicos que conducen a una situación fatal de la administración de medicamentos en un entorno hospitalario [2]. Arreglar estas ineficiencias en la interoperabilidad de los sistemas médicos supondría, además de un ahorro económico de más de 78.000 millones de dólares únicamente en Estados Unidos [3], una drástica disminución de los errores médicos con condiciones fatales.

Además, en los últimos años se ha desatado un interés por las criptomonedas tan solo comparable a la fiebre del oro o a la explosión de Internet en los años 90. Millones de personas han comenzado a interesarse por estas monedas, con el objetivo de ganar dinero y encontrar la próxima revolución. Sin embargo, lo interesante no se encuentra únicamente en estos "tokens digitales". La verdadera revolución viene soportada por la tecnología que hace posible el funcionamiento de estas criptomonedas, la Blockchain.

El objetivo de este trabajo es proponer, justificar e implementar un sistema descentralizado de gestión y almacenamiento de los historiales médicos a través del uso de la tecnología Blockchain, eliminando así las ineficiencias de las arquitecturas actuales. En particular, se va a hacer uso de Hyperledger Indy, un framework que provee todas las herramientas para la gestión de identidad digital en sistemas distribuidos.

El presente trabajo se ha organizado siguiendo la metodología Ciencia del diseño (en inglés, Design science). Esta metodología permite planificar y adaptar el trabajo a medida que se avanza en el desarrollo y se dispone de más información para tomar decisiones. Dado que, el conocimiento sobre la tecnología Blockchain y su aplicación en este ámbito era prácticamente nulo al comenzar, se establecieron unas fases iniciales que, a medida que se ha ido avanzando, se han ido corrigiendo y concretando los planes e iteración tras iteración se ha llegado al resultado que se muestra en esta memoria.

En primer lugar, se estableció que lo más importante era conocer a muy alto nivel el funcionamiento de la Blockchain para entender sus ventajas frente a los modelos tradicionales. Posteriormente, se decidió que se investigaría sobre las potenciales aplicaciones de esta tecnología en el sector sanitario para ver si había algún producto ya desarrollado, y ver si existía justificación suficiente para la realización del caso de uso puesto en marcha en este trabajo.

Habiendo validado el caso de uso gracias a los puntos expuestos en el Capítulo 2 y el Apéndice A, se procedió a investigar en profundidad el funcionamiento de la tecnología Blockchain y a buscar un framework adecuado. A partir de este punto, y con los requisitos del sistema definidos, se comenzó la implementación.

Esta memoria pretende recopilar y reflejar el trabajo realizado durante estos meses para lo cual se organiza en varios capítulos. En el Capítulo 2 se explica en profundidad la tecnología Blockchain y todas las ventajas que tiene; En el Capítulo 3 se profundiza en el estado del arte, es decir, las soluciones que ya existen o que se han diseñado previamente para el caso de uso planteado; En el Capítulo 4 se hace un análisis del problema, en el Capítulo 5, se hace un diseño de la solución para los problemas expuestos y en el Capítulo 6, la implementación de la solución propuesta; por último, en el Capítulo 7 se hacen unas conclusiones y se hacen propuestas sobre el posible trabajo futuro. Por último, en el Apéndice A se hace un exhaustivo análisis de múltiples papers para tratar de justificar la aplicación de la tecnología Blockchain en este caso de uso. En el Apéndice B se detalla el funcionamiento de AlastriaID y por último, en el Apéndice C se explica la dedicación y planificación.

Capítulo 2

Tecnología Blockchain

2.1. ¿Por qué es importante Blockchain?

La tecnología Blockchain nace para solucionar, entre otros muchos, un problema de confianza en las instituciones. Actualmente los pacientes confían en los proveedores sanitarios para que almacenen su información médica de forma segura y para que sea accesible, en caso de necesidad, desde cualquier parte del mundo.

Sin embargo, si el lector ha viajado por España, se habrá dado cuenta de la falta de coordinación de la información entre comunidades autónomas, por no hablar a nivel internacional. Tan solo en España existen 17 sistemas médicos distintos [4] por lo que, en caso de tener un problema en una región diferente a la de residencia habitual, los hospitales no tienen acceso inmediato al historial médico del paciente, dificultando así el tratamiento. Otro ejemplo es el de la ciudad de Boston en la cual existen 26 sistemas de almacenamiento de datos médicos diferentes [5].

Esta fragmentación puede suponer un problema ya que la confianza puede verse mermada por decisiones que escapan al control del individuo. La tecnología Blockchain devuelve el control de la información y de los datos a sus legítimos propietarios, eliminando así los intermediarios.

2.2. Breve historia de la tecnología Blockchain.

Blockchain parece haber nacido en los últimos años pero nada más lejos de la realidad, la primera mención de una tecnología para almacenar documentos en una cadena de bloques de forma segura data de 1991. Durante los siguientes años se fueron haciendo algunas implementaciones al desarrollo de las Blockchains pero sin una gran utilidad [6].

En 1998 aparece el concepto de las monedas digitales. Wei Dai introduce el uso de un registro de transacciones descentralizado, conocido como ledger, y el concepto de Proof of Work, explicado en próximos apartados. Al mismo tiempo, se publica un paper que establece los principios básicos de un "oro digital" y por primera vez se habla de un ledger descentralizado y público. El uso de este ledger crea un entorno de confianza en el que el intercambio de datos se lleva a cabo mediante operaciones cifradas y codificadas, salvaguardando así los intercambios de datos e incrementando la confianza en el sistema.

En 2008 aparece en internet el paper "A-Peer-to-Peer Electronic Cash System" [7] escrito por alguien conocido bajo el pseudónimo de Satoshi Nakamoto. En este documento se detallan los principios de la moneda digital, o criptomoneda, que todo el mundo conoce hoy con el nombre de Bitcoin [8].

La implementación duró tan solo 10 meses, el primer bloque se minó el día 3 de enero de 2009 y la primera transacción se llevó a cabo el 12 de enero de 2009 cuando Satoshi envió 10 Bitcoins a Hal Finney.

Hasta 2013 la tecnología Blockchain se estaba aplicando únicamente a la creación de criptomonedas. En ese año, Vitalik Buterin se da cuenta de la necesidad de crear un lenguaje de programación que permita crear aplicaciones descentralizadas. Así es como Vitalik, junto con su equipo, desarrolló la conocida plataforma de Ethereum.

En esta red, lanzada al público en 2015, se incorpora la posibilidad de crear aplicaciones descentralizadas. Esto expandió el horizonte y las posibilidades de la tecnología Blockchain ya que, a partir de entonces, cualquier usuario podría comenzar a programar sobre una cadena de bloques y conseguir implementar aplicaciones descentralizadas, seguras y transparentes.

2.3. ¿Qué es y cómo funciona Blockchain?

La definición formal de Blockchain es «*Una base de datos digital que contiene información que puede ser usada y compartida simultáneamente dentro de una red descentralizada*».

En otras palabras, es similar a una base de datos convencional puesto que nos permite almacenar información que eventualmente podremos consultar, pero con algunas características especiales que vienen dadas por la descentralización de esta base de datos. Entre estos elementos diferenciadores cabe destacar la inmutabilidad y la integridad de los datos, la transparencia y la trazabilidad de los mismos. En esta base de datos descentralizada se pueden almacenar, además de datos, contratos inteligentes, explicados en la Sección 2.5, y casi cualquier otra información de valor que un usuario desee guardar de forma segura y permanente [9].

Una red Blockchain es una red Peer-to-Peer (P2P), es decir una red en la que todos los nodos operan de igual a igual y de forma sincronizada. Esta sincronización es compleja de gestionar en una red descentralizada, ya que cada participante tiene un reloj interno y un origen de tiempos distinto.

Este problema de sincronización se soluciona agrupando todas las transacciones e interacciones que suceden durante un intervalo de tiempo determinado, en lo que se conoce como un bloque. Serán todos los participantes de la red los que, mediante la utilización de un mecanismo de consenso, se encarguen de verificar que todas las transacciones son correctas y que nadie está manipulando los datos. Para cada uno de estos bloques se calcula su hash mediante una función previamente determinada y dicho hash se introduce al comienzo del siguiente bloque, creando así, una cadena de bloques.

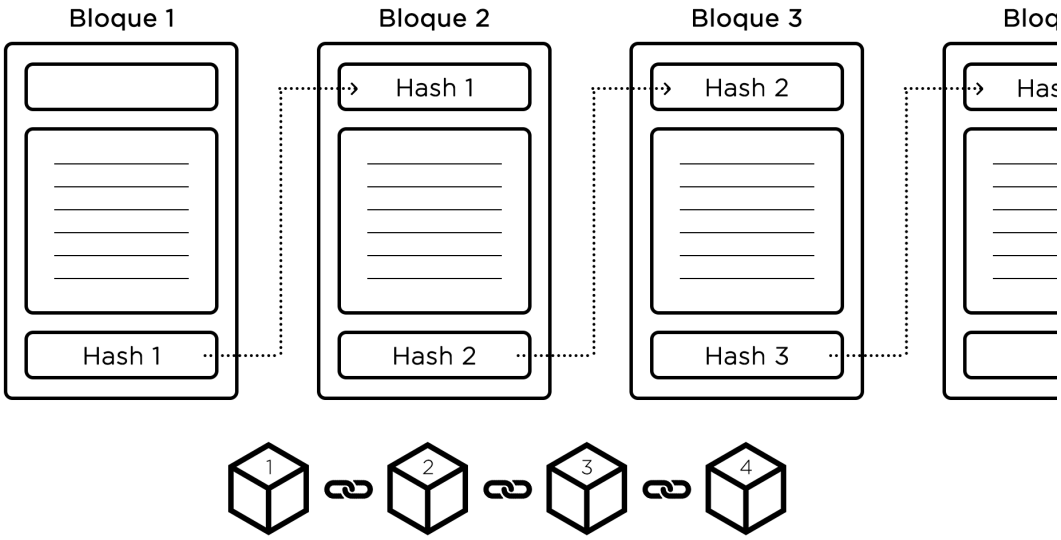

Figura 2.1: Diagrama de la formación de una Blockchain

En cada uno de estos bloques se guardan las transacciones y los smart contracts (explicados en la Sección 2.5) que van en ese bloque junto con la firma de los datos y la firma del bloque anterior. Esta firma es una operación criptográfica de hash, que resume en una secuencia alfanumérica el contenido de ese bloque. Es esta secuencia alfanumérica lo que usa la red para garantizar la integridad de los datos y sirve para mantener un enlace con el bloque anterior. En el caso de que alguien altere la información de un bloque, la firma de ese bloque cambia y el siguiente bloque, al haber guardado la firma, encuentra un conflicto y por tanto la cadena se rompe.

Una vez están todos los nodos sincronizados hay que poner en marcha un sistema de consenso que permita llegar a acuerdos en una red P2P. Para ello existen numerosos protocolos que dan vida a distintas redes, pero, a continuación, se analizan los dos más extendidos como son Proof of Work y Proof of Stake.

2.3.1. Proof of Work (PoW)

En las redes que incorporan este protocolo los nodos compiten por validar transacciones y añadir un bloque a la cadena resolviendo un puzle criptográfico. Estos puzzles requieren de una gran capacidad de cómputo conocido como HashRate por lo que, en caso de querer hacerse con el control de la red, haría falta sumar el 51 % del poder conjunto de todos los nodos.

Por ejemplo, en el caso de Bitcoin, este puzle criptográfico consiste en encontrar un número aleatorio que, tras calcular su hash con la función SHA256, se obtenga una secuencia que comience con un número determinado de ceros [10].

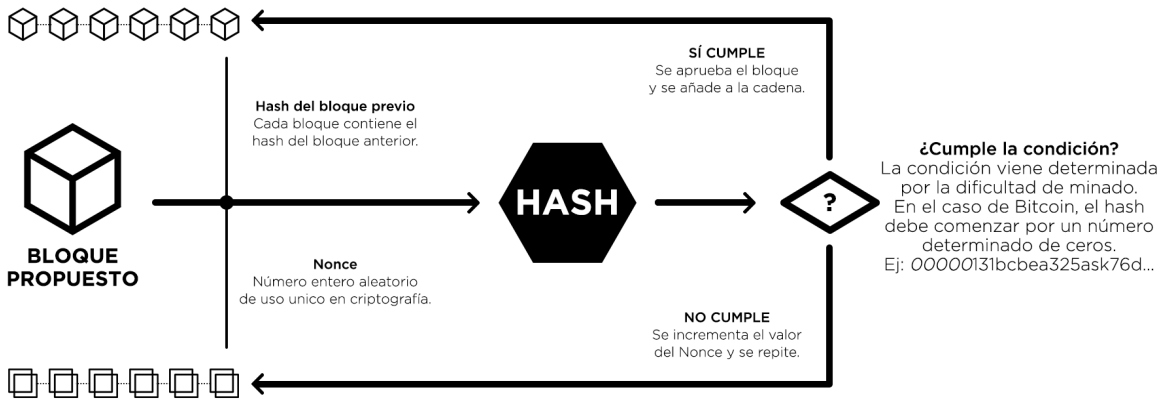

Figura 2.2: Diagrama explicativo de Proof Of Work.

Sin embargo, a pesar de ser uno de los primeros protocolos en ponerse en práctica y garantizar la seguridad ante ataques, la escalabilidad de estas redes es muy limitada. Las redes más conocidas como Bitcoin o Ethereum tienen un throughput, o rendimiento, de 7 y 15 transacciones por segundo (TPS) respectivamente. Esto, comparado con las más de 1500 que procesa la red Visa, se queda corto para conseguir una adopción masiva [11].

A mayores, el consumo energético es desproporcionadamente elevado. Se estima que la red de Bitcoin, que opera sobre este protocolo, consume más de 100 TWh/año, una cantidad similar a la de muchos países [12]. Si bien hay que tener en cuenta que el sistema financiero global consume 7 veces más, surge la necesidad de diseñar un protocolo más eficiente, que siga manteniendo la seguridad y que, a ser posible, aumente el throughput de la red.

2.3.2. Proof of Stake (PoS)

Al igual que el protocolo PoW, Proof of Stake busca conseguir un consenso entre los nodos de una red P2P. Sin embargo, en este caso los nodos no compiten por validar transacciones sino que la propia red es la que selecciona de forma pseudoaleatoria quién es el encargado de añadir un bloque a la cadena. La elección se realiza en base a parámetros como el tiempo desde el último bloque validado, el valor económico del nodo, parámetros de confianza y una importante aleatorización.

Los usuarios que quieran participar en la red deben aportar una cierta cantidad económica a su nodo. De esta forma garantizan la integridad de las transacciones que validan ya que, en caso de validar un bloque malicioso, la red lo detectaría y podría llegar a penalizar económicamente al nodo que lo creó en primer lugar. Por tanto, manipular la red para beneficio propio tiene un coste más elevado para el actor malicioso que los beneficios que podría obtener.

Proof of Stake no solo es un protocolo más eficiente en cuanto a la energía que consume sino que también es capaz de procesar más TPS. Este mayor throughput permite a estas redes ser mucho más escalables y las hace idóneas para la construcción de aplicaciones de uso cotidiano. A mayores, gracias al bajo consumo que requiere un nodo, más gente puede participar en la red, haciendo que estos sistemas sean mucho más descentralizados que aquellos que incorporan PoW.

2.4. Tipos de redes

En los puntos anteriores se ha visto cómo la tecnología Blockchain se construye sobre el concepto de descentralización haciendo uso de numerosos nodos que permiten validar y comprobar que el sistema funciona correctamente. Estas redes P2P se pueden clasificar en *permisionadas*, del inglés permissioned, o *no permisionadas* en función de quién puede participar en la red.

2.4.1. Redes Blockchain no permisionadas

A día de hoy, estas redes son las más utilizadas en las aplicaciones de criptomonedas, ya que Bitcoin, Ethereum y otras muchas se basan en este tipo de redes. La característica principal de estas redes es que cualquier persona puede participar en la red convirtiéndose en un validador de bloques y recibir recompensas en la criptomoneda asociada.

Esto permite que las redes no permisionadas tengan una mayor descentralización lo cual, a su vez, garantiza una mayor seguridad en la red ya que cuantos más validadores haya, más complicado es hacerse con el control de la Blockchain. Gracias a la elevada descentralización, también consiguen acabar con la censura, o al menos reducirla drásticamente porque nadie tiene el control de la infraestructura.

Sin embargo, dados los protocolos de consenso que usan, las redes no permisionadas son muy lentas y tienen un throughput muy reducido. Esto afecta directamente a la escalabilidad de las soluciones que se quieran construir sobre la red haciendo la adopción masiva de las mismas muy compleja. La gobernanza de la red recae también en todos los usuarios por lo que en muchas ocasiones se pueden producir divisiones insalvables en las opiniones de los validadores creándose así un "split" en la Blockchain. Estas divisiones en las cadenas son contraproducentes para los proveedores de servicios que en muchas ocasiones tienen que invertir más para adaptar sus infraestructuras a estos cambios.

2.4.2. Redes Blockchain permisionadas

Este tipo de redes son menos populares y su principal diferencia con las no permisionadas es la necesidad de autenticación para participar en la red. Esto permite que no sea necesario un sistema de recompensas para el correcto funcionamiento como podría tener las redes de Bitcoin o Ethereum que recompensan a sus validadores, o mineros, con una cantidad de criptomonedas. Es decir, las redes permisionadas no tienen una criptomoneda asociada.

La necesidad de una autenticación y el hecho de que solo un grupo reducido de usuarios puedan participar en la red, es decir, autorización, hace que el consenso sea mucho más sencillo y, por tanto, el throughput de esta solución sea muy elevado. Esto es fundamental si se quiere construir aplicaciones que requieran de una gran escalabilidad con el tiempo. Además, al no tener una criptomoneda asociada y ser menos validadores, los costes de operación de estas redes son muy reducidos con respecto a las redes no permisionadas.

Sin embargo, las redes permisionadas están mucho más centralizadas ya que no puede participar en ellas cualquier persona y por tanto suele haber menos transparencia. Otra potencial desventaja debido a la mayor centralización es la mayor facilidad para la censura.

	Permisionadas	**No Permisionadas**
Acceso	Limitado a aquellos que pasen los mecanismos de autenticación.	Cualquier usuario se puede convertir en validador dentro de la red.
Criptomoneda	No tienen una criptomoneda asociada a la red.	Tienen una criptomoneda asociada a la red.
Descentralización	Descentralización limitada debido al reducido número de validadores.	Mayor descentralización debido al elevado número de validadores.
Seguridad	Si los controles de acceso son eficientes y la gestión de la red es buena se puede conseguir un nivel de seguridad elevado.	Un elevado número de validadores garantiza la seguridad ante potenciales ataques.

	Permisionadas	**No Permisionadas**
Escalabilidad	Gran capacidad de escalado debido al elevado throughput.	Los complejos protocolos de consenso impiden la escalabilidad.
Costes	Los costes por operación son muy reducidos.	Los protocolos necesarios para el funcionamiento elevan los costes drásticamente.

Tabla 2.1: Diferencias entre redes permisionadas y no permisionadas.

2.5. Smart Contracts

Un smart contract o contrato inteligente es el equivalente a un contrato físico pero completamente digital. Para su correcto funcionamiento, el código necesario para la creación del Smart Contract (SC) se introduce en la cadena de bloques y los nodos serán los encargados de ejecutar la lógica del contrato de manera autónoma cuando se den una serie de condiciones previamente establecidas que lo disparen [13].

Los SC son la solución definitiva para garantizar la correcta ejecución de un contrato ya que no requieren de confianza en una tercera parte. Al estar programados en la Blockchain son inmutables, es decir, una vez las dos partes lo firman y se añade a la cadena de bloques, nadie lo puede modificar. Además, gracias a la descentralización, una sola persona no puede forzar la ejecución del Smart Contract ya que hace falta el consenso de la red.

Los Smart Contracts dependen de un input que confirma que lo establecido se ha completado. Esto puede suponer un problema puesto que los Smart Contracts no se pueden detener. Una vez se establece, aunque sea por error, que las condiciones pactadas se cumplen, la cadena de bloques ejecutará el Smart Contract. Para solucionar el problema de la ejecución por error, nacen los oráculos.

Los oráculos, del inglés oracles, son plataformas que actúan de puente entre la Blockchain y los datos que se encuentran off-chain, es decir, fuera de la cadena de bloques. Son los encargados de introducir los datos necesarios para la ejecución de un Smart Contract en forma de una transacción para que queden almacenados dentro de un bloque. Sin embargo, este puede ser un fallo crucial ya que si la ejecución de los Smart Contracts depende de una entidad centralizada, el objetivo de garantizar la

confianza mediante la descentralización queda comprometido [14].

Existen numerosos protocolos para garantizar la veracidad de la información de forma descentralizada. Uno de los más utilizados, Chainlink, utiliza un conjunto de nodos, también en una red descentralizada, que se encargan de verificar los datos off-chain antes de proveerlos al Smart Contract. Para poder formar parte de un oráculo, los usuarios deben aportar una cierta cantidad económica a la red para que, en caso de aportar información falsa, sean penalizados.

Gracias a la implementación de los Smart Contracts se pueden crear aplicaciones funcionales completamente descentralizadas (DApps). A mayores, gracias a la descentralización, el servicio de estas aplicaciones está garantizado todo el tiempo puesto que basta un nodo en funcionamiento para poder usar el servicio.

Las DApps creadas gracias a los contratos inteligentes permiten aplicar la tecnología Blockchain a cualquier sector imaginable abriendo así un mundo de posibilidades entre las que se encuentra la identidad digital autosoberana detallada a continuación.

2.6. Identidad digital auto-soberana

Según un informe del Banco Mundial, más de 1000 millones de personas no tienen acceso a una prueba de identidad o DNI que les permita acceder, entre otras cosas, a tratamientos médicos [15]. Cuando se habla de sistemas de identificación no se hace referencia únicamente a la infraestructura puesta en marcha por los Estados para identificar a sus ciudadanos, sino también a las identidades virtuales mediante cuentas de Google o Facebook.

Estas últimas son ofrecidas por compañías con intereses propios que recopilan la información que genera el usuario para uso privado, o para venderla sin su consentimiento explícito, provocando así una pérdida de confianza en las grandes instituciones. Surge pues, la necesidad de diseñar una alternativa que respete los datos y la información de los usuarios.

Un identificador digital descentralizado (DID) es un número único que representa a un individuo, a día de hoy se usa el correo electrónico o el número de teléfono. Sin embargo, estos identificadores, así como la información que está asociada a ellos, dependen de entidades ajenas al control del individuo que pueden revocar el acceso en cualquier momento. Los sistemas de identidad soberana autogestionados (en inglés, Self-Sovereign Identity o SSI) ofrecen una mayor seguridad, privacidad e integridad que las identidades digitales proporcionadas por las grandes empresas tecnológicas.

SSI funciona de una forma muy sencilla basándose en el uso de criptografía asimétrica: un usuario tiene una cuenta única que llamaremos wallet o cartera en la que se almacenan los pares de claves público-privadas necesarias para el funcionamiento del sistema. Generalmente, la clave pública es la dirección de la cartera y cualquier persona puede acceder a ella para comprobar que se trata de dicho usuario. Las claves privadas están almacenadas de forma segura en la cartera.

Por ejemplo, una receta médica, al ir a una farmacia e identificarte con tu DID, el sistema comprueba que efectivamente, el médico Bob ha emitido una receta para un medicamento concreto. Bob ha tenido que firmar previamente la receta con su clave privada y como la clave pública está en el ledger, se puede comprobar fácilmente que ha sido emitida por un médico y no ha sido falsificada. También se puede comprobar que la receta no ha sido modificada ya que el hash de la misma se almacena en la Blockchain.

Mientras el mundo se vuelve cada vez más interconectado, los individuos muestran y publican información personal, crean múltiples nombres de usuario y contraseñas dejando un rastro digital en numerosas plataformas. Un sistema de SSI eliminaría la necesidad de tener distintos nombres de usuario y contraseñas ya que una persona podría autenticarse con su propia identidad digital.

Capítulo 3

Estado del arte

En este capítulo se procede a hacer un análisis de múltiples publicaciones científicas sobre la aplicación de la tecnología Blockchain en el sector sanitario. El objetivo es identificar las alternativas ya existentes, el estado de este campo de investigación y los problemas a los que se enfrenta el almacenamiento de datos médicos que se tratarán de solucionar más adelante.

3.1. Revisión bibliográfica

Es fundamental conocer el estado de la implantación de la tecnología Blockchain en los sistemas sanitarios y cómo se encuentra la investigación científica en este campo. De esta manera se obtiene un conocimiento sobre la existencia de soluciones al problema expuesto en los puntos anteriores, y si es así, poder analizar la arquitectura utilizada y la viabilidad de su implementación.

En este caso se ha hecho uso del repositorio y buscador de Ebsco así como del explorador del IEEE para la búsqueda de papers relacionados. Se comienza la búsqueda usando como palabras clave "blockchain" y "healthcare" para ver el estado de la investigación en este campo. Al tratarse de una tecnología nueva, sin ningún tipo de estandarización y tratando de aplicarla a un caso de uso específico, el número de papers de calidad encontrados ha sido reducido.

A continuación se adjunta una tabla con algunos de los artículos escogidos y se clasifican según si desarrollan el concepto de blockchain en sistemas de salud sin entrar en detalles técnicos (adopción) o según si se basan en las arquitecturas o soluciones técnicas (implementación). Todos los papers escogidos se encuentran analizados en detalle en el Apéndice A.

Paper	Adopción	Implementación
1.- A survey on opportunities and challenges of Blockchain technology adoption for revolutionary innovation [16].	X	
2.- Cross-domain Design of Blockchain Smart Contract for Library and Healthcare Privacy [17].		X
3.- Integrating Blockchain Technology into Healthcare [18].	X	
4.- Integrating Blockchain Technology in Healthcare via Active Learning [19].	X	
5.- Blockchain technology in healthcare big data management: Benefits, Applications and Challenges [20].	X	
6.- Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity [21].		X
7.- Privacy and Security Problems of National Health Data Warehouse: A Convenient Solution for Developing Countries [22].	X	
8.- MedRec: Using Blockchain for Medical Data Access and Permission Management [23].		X
9.- MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain [24].		X

Tabla 3.1: Papers analizados.

Tras finalizar con el análisis de los trabajos previos, que se puede encontrar en el Apéndice A, se concluye que es necesario un cambio de paradigma en la forma de gestionar los sistemas sanitarios. La seguridad es un pilar fundamental del almacenamiento de datos y sin embargo, un tercio de las brechas de seguridad están relacionadas con la industria sanitaria [25]. Al tener los datos completamente cifrados y únicamente accesibles por el poseedor de la clave privada, o aquellos autorizados por el propietario, estas brechas de seguridad se verán reducidas drásticamente.

De implementarse una solución basada en un ledger público, los pacientes podrán analizar que médicos han accedido a su historial, cuándo y qué modificaciones han hecho en él, etc. Gracias a la trazabilidad que proporciona, la tecnología Blockchain tiene el potencial de terminar con el fraude médico.

Por último, gracias a la elevada seguridad y al uso de un ledger público, se podrán agregar los datos médicos de forma anónima, siempre que el paciente lo consienta, para contribuir a la investigación. De esta manera los grupos médicos tendrán a su disposición una mayor cantidad de datos para poder procesar y utilizar en sus investigaciones.

Sin embargo, no son todo ventajas ya que, según el análisis de los papers estudiados, a día de hoy el almacenamiento de grandes cantidades de datos directamente en una Blockchain ralentizaría el sistema y tiene un coste económico muy elevado que haría inviable la implementación de la solución. Otro problema, no menor, es la elevada regulación vigente de protección de datos, que entre otras cosas, obliga a almacenar los datos en los propios centros médicos. Esto impide el desarrollo tecnológico y la implementación de otras soluciones más eficientes y que podrían contribuir a mejorar la calidad del servicio médico.

Las soluciones mencionadas han sido diseñadas e implementadas en la red Blockchain de Ethereum lo cual supone unos costes de operación muy elevados. A precio actual de la criptomoneda asociada a dicha red (Ether), el coste de hacer cualquier modificación a un historial médico ascendería a $0.2 [25]. Esa cantidad puede parecer poco, pero si agregamos los millones de transacciones de este estilo que se llevarían a cabo durante un año, el aumento de costes sería inviable para la implantación.

Es por todo esto que es necesario buscar un Framework que incorpore todas las ventajas de la tecnología Blockchain, trazabilidad, transparencia, seguridad y descentralización y que a la vez el coste de operación sea reducido. Además, este framework debería tener implementado un modelo de identidad digital sobre el que poder construir el almacenamiento de datos médicos.

3.2. Posibles framework de trabajo

Como se ha visto anteriormente, un sistema de SSI eliminaría la necesidad de tener distintos nombres de usuario y contraseñas ya que una persona podría autenticarse con su propia identidad digital. El objetivo de este punto es buscar y analizar las distintas alternativas de sistemas de SSI para elegir sobre cuál basar la solución para la gestión de historiales médicos.

Con este objetivo en mente, se han analizado varios sistemas entre los que en este documento se detallan los tres que más encajan con el caso de uso sobre el que se está trabajando: Veramo, Hyperledger Indy y Alastria ID.

3.2.1. Veramo

Veramo es una evolución del proyecto de uPort cuya misión era crear un internet descentralizado que devolviese el control de la información a los individuos [26]. Es un framework de JavaScript que fue diseñado para ser flexible y modular, lo que permite la fácil adaptación a múltiples casos de uso.

Veramo se compone de un núcleo que proporciona todas las funcionalidades disponibles en la API y permite la implementación de diversos plugins. El agente puede ser el encargado de gestionar las claves, los DID, las credenciales... Sus funciones dependen de los plugins instalados [27].

Este framework no incorpora un sistema ya creado sino que permite al diseñador implementar el modelo de SSI que desee y gestionar las credenciales y los DID como desee gracias a su potente API.

Figura 3.1: Logotipo de Veramo.

3.2.2. Alastria ID

Alastria es una organización sin ánimo de lucro que promueve la economía digital mediante el desarrollo de tecnologías distribuidas. Esta organización, integrada por numerosas empresas, tiene como objetivo proveer una infraestructura estándar para crear un modelo de identidad digital conocido como Alastria ID [28].

En el desarrollo de este modelo de DID, Alastria ID, han trabajado personas con múltiples perfiles y se ha colaborado directamente con AENOR para crear un primer estándar de gestión de identidad digital basado en Blockchain. También han trabajado con otras muchas entidades de estandarización para que el modelo cumpla con todas las normativas vigentes como el reglamento general de protección de datos (RGPD).

Para el correcto funcionamiento de este modelo se crean tres tipos de usuarios distintos o entidades. Los proveedores de servicios, los emisores y los usuarios operan entre ellos para verificar la identidad, emitir credenciales y proveer servicios. La información personal, como la clave privada u otros datos, está almacenada en el dispositivo físico del usuario como podría ser el móvil o en un servidor y nunca directamente en el ledger.

El sistema de credenciales puesto en marcha es muy potente ya que se basa en los estándares publicados por el World Wide Web Consortium (W3C). Incluyen múltiples campos entre los que se incluye un identificador de red o un número que representa el nivel de confianza de la credencial. Estas credenciales son compartidas entre los emisores y los usuarios.

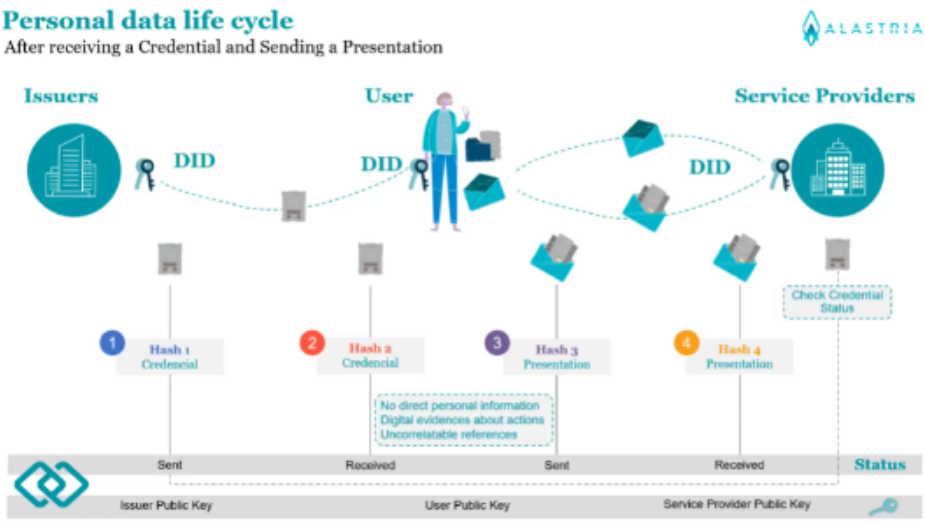

Figura 3.2: Flujo de emisión de una credencial con el modelo de Alastria ID.

Una característica fundamental de este modelo es el uso de un doble hash que permite garantizar la privacidad de las acciones de los usuarios, se puede observar en la Figura 3.2 [29]. Cuando el emisor envía una credencial al usuario, su hash se calcula con la credencial y con el DID del emisor. Cuando el usuario quiere usar la credencial se vuelve a calcular el hash con la credencial y el DID del usuario. De esta manera la credencial es la misma, pero el hash que se registra en el ledger es distinto, haciendo imposible ver qué credenciales usa cada usuario. Sólo los actores involucrados en la comunicación pueden entender la información que se ha compartido, Blockchain solo presenta evidencias digitales sobre acciones pasadas y nunca información personal directa.

Alastria ID permite también la revocación de credenciales y la supresión de las presentaciones de forma sencilla, basta con que el emisor o el usuario cambien el estado de la misma en la Blockchain. Es así como cuando el proveedor de servicios analice la credencial o la presentación, verá que está revocada y por tanto no es válida [29].

3.2.3. Hyperledger Indy

Hyperledger es una organización sin ánimo de lucro que busca agrupar la infraestructura y los recursos necesarios para asegurar el crecimiento estable de los proyectos basados en ecosistemas Blockchain open-source [30]. Dentro de esta organización se crean múltiples frameworks, especializados en campos muy variados, para trabajar con ledgers distribuidos de forma sencilla. De todos estos frameworks el más interesante para este caso de uso es Hyperledger Indy.

Indy es un framework que proporciona las herramientas, librerías y componentes necesarios para la creación, gestión de identidades digitales basado en Blockchain. Esta solución es compatible y permite la interoperabilidad entre diferentes redes Blockchain o puede ser usada de forma independiente con una red propia [31].

Este proyecto dentro del ecosistema de Hyperledger se construye en dos capas completamente independientes y muy diferenciadas. En este modelo cada capa aporta una parte vital para el funcionamiento del sistema de SSI.

- **Indy Plenum:** Esta capa busca implementar el protocolo de consenso y el ledger necesario para que funcione la Blockchain de forma completamente autónoma. A pesar de haber sido optimizada para construir un sistema de identidad

autosoberana, puede ser utilizada como una Blockchain general.

- **Indy Node:** Esta capa se construye sobre la infraestructura de red que implementa Plenum e introduce todos los protocolos necesarios para construir un sistema de SSI. Su arquitectura modular ha sido programada en Python y permite una mayor versatilidad, además de haber sido puesta a prueba en numerosas ocasiones.

Esta Blockchain de Hyperledger Indy es una red permisionada cuya arquitectura se compone de tres tipos de nodos diferenciados: validadores, observadores y nodos regulares. Los nodos validadores son los encargados de gestionar los accesos de lectura y escritura, e implementar el sistema de consenso. Los segundos, gestionan la lectura y se mantienen sincronizados con los nodos validadores mientras que los nodos regulares son el resto de usuarios.

Para poder escribir en el ledger un usuario tiene que pedir acceso de escritura a todos los nodos validadores y recibir una cantidad significativa de autorizaciones para poder hacerlo. Para conseguir una autorización es necesario que los nodos validadores conozcan el rol asociado al DID que solicita el acceso. En cuanto a la autorización de lectura el usuario únicamente necesita hacer una petición a un nodo validador y recibir respuesta del mismo. En el ledger se almacenan las claves y los DID públicos, así como información de revocación de credenciales u otros datos de interés para el sistema, pero nunca información privada.

Capítulo 4

Análisis del problema

El objetivo de este trabajo es buscar una solución tecnológica a la fragmentación de los datos médicos entre múltiples sistemas, ayudando a reducir los potenciales errores debidos a la falta de información sobre un paciente en caso de emergencia. Todo esto debe hacerse de forma transparente para los usuarios ya que, si el uso de esta tecnología complicara de alguna manera el funcionamiento de los sistemas actuales, es muy probable que no llegara a implementarse.

Aspirar a hacer un sistema para solucionar todos los problemas que existen a día de hoy en la gestión de los datos médicos, usando además una tecnología disruptiva, como es la Blockchain, sería un trabajo colosal que escaparía a las horas destinadas para un Trabajo Fin de Grado. Es por esto que dentro del caso de uso se ha decidido centrar los esfuerzos en aproximar una solución a los problemas más básicos.

4.1. Fragmentación de los datos médicos

Como se ha mencionado anteriormente, la fragmentación de la información entre diversos hospitales y sistemas médicos es un grave problema que puede llegar a tener consecuencias fatales.

Imaginemos, por ejemplo, que Bob tiene que viajar a otro país y sufre un accidente en el destino. En el correspondiente servicio de urgencias, Alice carece de información médica básica sobre Bob, lo cual dificulta en gran medida el tratamiento. En caso de necesitar datos básicos como el grupo sanguíneo o el estado general previo al accidente del paciente (mediante una analítica u otros datos relevantes), Alice deberá ponerse en contacto con la embajada o el organismo competente para que le transfieran la información sobre el paciente.

Estos procedimientos son costosos y pueden llegar a pasar horas hasta que Alice reciba el historial médico de Bob. Además, si Bob no acude siempre al mismo hospital, sino que alterna entre diversos centros médicos, es muy probable que el historial que reciba Alice no esté completo.

Una vez Alice recibe la información requerida, es muy probable que la forma de representar los datos en el país de origen de Bob sea diferente a la forma que tiene Alice. La carencia de estandarización a la hora de escribir los informes médicos puede añadir una capa de dificultad a la hora de interpretar la información y contribuir a un potencial error grave.

Es por esto que se considera fundamental encontrar una solución tecnológica que agrupe todas las intervenciones y actualizaciones del historial médico de un paciente como Bob bajo un mismo paraguas. Gracias a la unificación de la información clínica de los individuos, se puede estandarizar el formato de los datos y de los informes para que todos los médicos, independientemente del lugar del mundo donde se encuentren, rellenen los datos de igual manera.

4.2. Fraude médico

El robo de identidad médica es un problema real que se produce cuando alguien usa información personal para obtener recetas, comprar dispositivos médicos, presentar reclamaciones ante proveedores de seguros, etc. [32]. Esto es un grave problema ya que en muchas ocasiones, el paciente puede tener problemas al recibir atención médica...

Este problema necesita también de una solución que permita autenticar, siempre y en todo lugar, a los pacientes y a los médicos. El sistema que se diseñe debería incluir también la opción de emisión de recetas de medicamentos que fueran trazables y gracias a las cuales, la farmacia pudiera verificar que la receta ha sido emitida por un médico.

4.3. Complejidad de acceso

Si el lector ha solicitado alguna vez su historial médico, sabrá de la complejidad burocrática que estos trámites requieren. Es por esto, y dado que los datos médicos son una parte fundamental de la identidad de una persona, que se debe diseñar una solución sencilla de usar y que sea accesible para todo el mundo con un ordenador.

Los usuarios deberían ser capaces de crear una cuenta en el sistema y poder usarlo para ver sus datos médicos básicos, así como las analíticas pasadas y recetas que tenga pendientes. Todo esto de forma intuitiva y sencilla.

Capítulo 5

Diseño de la solución

En el Capítulo 4 se han visto los problemas actuales de los sistemas de almacenamiento de datos médicos tradicionales y se han detallado tres puntos principales que se deberían mejorar inicialmente. Son estos problemas los que se pretenden solucionar en este trabajo gracias a la aplicación de la tecnología Blockchain.

5.1. Solución conceptual

Como se ha explicado en la Sección 4.1, la fragmentación de los datos médicos es un grave problema y puede acarrear graves errores. Es por esto que se propone la creación de una aplicación basada en tecnología Blockchain como solución a este problema.

La tecnología Blockchain tiene una serie de beneficios, explicados en el Capítulo 2, cómo podría ser la trazabilidad y la inmutabilidad de los datos. Gracias al uso de un ledger, o registro de transacciones descentralizado, la información almacenada en él va a estar siempre disponible independientemente del lugar o momento.

El uso de esta tecnología es un pilar fundamental para garantizar el acceso a la información médica y poder verificar en todo momento la autenticidad e integridad de los datos obtenidos. Además, Blockchain permite estandarizar el formato de la información, homogeneizando así todos los informes y facilitando el tratamiento del paciente en cualquier lugar del mundo.

Otro problema a tratar de solventar en este trabajo es el fraude médico explicado en la Sección 4.2. El fraude se origina en el momento en el que no existe un mecanismo de verificar la identidad del médico firmante de una receta. Nuevamente, esto se puede solucionar con la aplicación de la tecnología Blockchain ya que, gracias a la trazabilidad, una farmacia puede autenticar el origen de una receta y comprobar fácilmente que ha sido emitida por un médico.

Por último, teniendo en cuenta que cada usuario tendrá una cuenta única, podrá acceder a sus datos médicos en cualquier momento sin tener que pasar por largos procesos burocráticos.

Es fundamental comprender que todas estas operaciones se hacen de forma anonimizada en la red y únicamente los participantes de una interacción conocen el origen y destino de las mismas. Es decir, toda la información se encuentra cifrada y almacenada de forma segura, únicamente el usuario propietario de la información puede acceder a la misma.

5.2. Requisitos de la solución

Una vez visto a alto nivel la propuesta para solventar los problemas expuestos en el Capítulo 4, en este punto se pretende concretar la solución en una serie de requisitos funcionales que debe cumplir el sistema. Para facilitar su implementación se han dividido en varias fases.

Fase 1: Gestión de cuentas y almacenamiento de datos básicos:

Esta primera fase es la más básica y fundamental para conseguir un sistema de almacenamiento de datos médicos distribuido. El sistema debe ser capaz de guardar información básica como el Nombre y Apellidos, número de la seguridad social y/o seguro privado. En cuanto a los datos médicos debe almacenar el grupo sanguíneo, alérgenos y enfermedades crónicas.

En el sistema se definen dos roles, o tipos de usuario, principales, el de Paciente y el de Doctor. Según qué rol tenga asignado un usuario, podrá acceder a unas opciones o a otras, si bien aclarar que los médicos pueden acceder a las mismas opciones que los pacientes más las propias.

RF-01: Registro en el sistema.	
Descripción:	El sistema permitirá crear una cuenta de usuario.
Usuario:	-

Tabla 5.1: Requisito funcional 1.

En el proceso de registro de un nuevo usuario se pedirá nombre, apellido y una contraseña. Para simplificar el uso de la aplicación, el usuario introducirá si desea ser médico o paciente. En una aplicación real se implementarían otras entidades como una Universidad que emitiera un título de medicina a un usuario y que fuera este título el que le otorgue el rol de médico en el sistema. En este caso se emitirá un certificado automáticamente al seleccionar médico como rol del nuevo usuario.

RF-02: Control de acceso al sistema.	
Descripción:	El sistema permitirá iniciar sesión cada vez que se desee acceder al perfil de usuario.
Usuario:	Paciente y médico

Tabla 5.2: Requisito funcional 2.

En este requisito, el sistema solicitará al usuario una contraseña para poder acceder al perfil con toda la información médica.

RF-03: Creación de información básica.	
Descripción:	El sistema permitirá al usuario rellenar su información personal.
Usuario:	Paciente y médico

Tabla 5.3: Requisito funcional 3.

Este tercer requisito de nuevo se hace para simplificar el caso de uso. En una aplicación real, si bien el concepto y funcionamiento técnico sería el mismo, el usuario debería personarse en una oficina del órgano correspondiente para validar que sus datos sean correctos antes de enviarlos al ledger.

Una vez iniciada sesión, el usuario podrá acceder a su información personal introducida durante el registro. Esto permitirá en caso de emergencia, tener acceso siempre y en todo lugar a la póliza de seguro o a los datos básicos como el grupo sanguíneo o alérgenos.

RF-04: Acceso a información básica de usuario.	
Descripción:	El sistema permitirá al usuario visualizar su información personal.
Usuario:	Paciente y médico

Tabla 5.4: Requisito funcional 4.

Fase 2: Creación de analíticas estandarizadas y almacenamiento:

Esta segunda fase es vital para que, en caso de emergencia, los médicos puedan acceder a un historial de analíticas del paciente. Es por esto que se plantea la estandarización de las analíticas en un formato universal e igual para todos los médicos que usen el sistema. Las analíticas se guardarán en la cuenta del usuario en la Blockchain y serán accesibles desde cualquier lugar del mundo.

RF-05: Creación de una analítica.	
Descripción:	El sistema permitirá al usuario emitir una analítica a un usuario paciente.
Usuario:	Médico

Tabla 5.5: Requisito funcional 5.

Esta analítica se creará basándose en un esquema introducido en el ledger por el "gobierno" de forma que todos los médicos usarán el mismo formato. Cada vez que se cree una analítica, el médico creará lo que se conoce en Indy como una definición de credencial y la enviará al paciente para que pueda almacenarla.

El proceso óptimo de emisión sería con la creación de un QR por parte del paciente, el médico debería escanear el código para que la API obtuviera las credenciales necesarias para emitir la credencial. En este caso y debido al tiempo limitado del trabajo, se ha optado por introducir estos datos de forma manual.

RF-06: Consultar analíticas.	
Descripción:	El sistema permitirá al usuario ver los resultados del historial de analíticas hechas.
Usuario:	Paciente

Tabla 5.6: Requisito funcional 6.

Las analíticas se mostrarán en orden de la fecha de emisión de más nuevas a más antiguas. De esta manera el usuario podrá acceder a ellas y enseñarlas más cómodamente.

RF-07: Mostrar analíticas.	
Descripción:	El sistema permitirá al usuario crear un código QR, el cual siendo escaneado, otro usuario podrá acceder a la información de las analíticas.
Usuario:	Paciente y médico.

Tabla 5.7: Requisito funcional 7.

Para facilitar todavía más si cabe, el usuario podrá generar un código QR que al escanearlo mostrará toda la información necesaria para el correcto tratamiento.

Fase 3: Emisión y visualización de recetas.

Para evitar el fraude médico explicado en el Capítulo 4 se plantea un tercer y último caso de uso por el cual los médicos podrán emitir recetas a los pacientes. De esta manera, y haciendo que únicamente los usuarios con el rol de médicos puedan crear recetas, se disminuiría la posibilidad de fraude.

Esto es fundamental ya que, en caso de duda las farmacias podrían contar con scripts que revisaran todas las interacciones en el ledger y verificar que, efectivamente, el usuario emisor de la credencial es un médico.

RF-08: Emitir receta.	
Descripción:	El sistema permitirá al usuario crear una receta para un paciente concreto.
Usuario:	Médico.

Tabla 5.8: Requisito funcional 8.

A la hora de crear estas recetas, se establecerá una fecha de vencimiento tras la cual, no se podrán obtener los medicamentos y el médico deberá volver a emitir otra receta nueva. En este caso, es la API la encargada de mostrar al usuario las recetas que están dentro de plazo y generar un código QR en caso de querer tramitarla.

RF-09: Ver recetas.	
Descripción:	El sistema permitirá al usuario ver las recetas en fecha.
Usuario:	Paciente y Médico.

Tabla 5.9: Requisito funcional 9.

5.3. Herramientas a usar

5.3.1. Hyperledger Indy

En el Capítulo 3 de este trabajo se ha detallado el Estado del Arte, es decir, se han expuesto las distintas alternativas que existen a día de hoy para la gestión de identidad digital con tecnología Blockchain. Es en este punto en el que se explica por qué se ha escogido Hyperledger Indy como framework de trabajo para la implementación ya que se ha tenido que llegar a un compromiso modelo/eficiencia.

Figura 5.1: Logotipo de Hyperledger Indy.

En primer lugar se investigó Veramo, una alternativa muy potente para la creación de sistemas de identidad digital autosoberana (SSI). Sin embargo, este framework no provee de un modelo implementado sino que da las herramientas necesarias para que lo implemente el usuario a su gusto. Esto es muy potente pero se desvía del objetivo principal del trabajo, que es la construcción de un sistema de almacenamiento de datos médicos. Es por esto que la opción queda descartada, el coste de tiempo que supondría diseñar un modelo de SSI sería equivalente a otro TFG.

En segundo lugar se encuentra Alastria ID, un potente modelo de identidad digital descentralizado (DID) que cumple a la perfección las directrices marcadas por el RGPD. A pesar de contar con el mejor modelo de los tres, la implementación técnica se encuentra en una etapa muy temprana y poder trabajar con él es muy complejo e ineficiente. Tras intentar durante varios días la instalación y la puesta en marcha de todos los elementos necesarios para poder trabajar, se decidió descartar debido a la inmadurez del sistema.

Si bien Hyperledger Indy no ha sido diseñado en colaboración con AENOR para cumplir el RGPD, tiene un modelo muy eficiente y ya operativo con el que poder trabajar para llevar a cabo la solución propuesta a los problemas mencionados. Es por esto que se hará uso del Indy SDK (kit de desarrollo de Indy) con las correspondientes librerías [33].

5.3.2. Red de pruebas

Para poder comenzar la construcción de una aplicación sobre Indy es necesario poner en funcionamiento una red Blockchain. Para crear esta red de pruebas sobre la que poder interactuar, se va a hacer uso de la potencia de los contenedores Docker.

Figura 5.2: Logotipo de Docker.

Docker es un proyecto de código abierto que automatiza el despliegue de aplicaciones dentro de contenedores de software, proporcionando una capa adicional de abstracción y automatización de virtualización de aplicaciones en múltiples sistemas operativos [34].

Es una herramienta que permite eliminar tareas de configuración repetitivas. Es una plataforma completa extremo a extremo que está diseñada para funcionar durante todo el ciclo de vida de una aplicación [34].

5.3.3. Lenguaje de programación

Para la parte de implementación se ha elegido Python como lenguaje de programación. Esto se debe a que la mayoría de la documentación sobre Hyperledger Indy se encuentra en Python. Además, si bien se había usado este lenguaje en asignaturas de la carrera, esta era una buena oportunidad para profundizar y mejorar las habilidades de desarrollo con Python.

Figura 5.3: Logotipo de Python.

Cabe destacar que Python es un lenguaje de programación orientado a objetos, claro y potente. Además, viene con una gran librería que admite muchas tareas de programación como conectarse a servidores web, buscar texto, leer y modificar archivos... Por último, puede ser ejecutado en cualquier máquina ya sea Windows, Mac OS, Linux... lo cual lo hace ideal para mejorar la compatibilidad [35].

5.3.4. Frontend

Uno de los requisitos fundamentales es que el uso de una infraestructura basada en Blockchain, no suponga un impedimento a la hora de usar el sistema. Es por esto que se ha de trabajar en un Frontend intuitivo y accesible para todo perfil de usuario.

Para ello se ha decidido construir la aplicación web con HTML y Bootstrap. Este último es un kit de herramientas para el diseño del Frontend muy potente y repleto de funciones [36]. Permite personalizar el sistema con componentes prediseñados, optimizando el proceso y centrando los esfuerzos en la implementación tecnológica de la Blockchain.

Figura 5.4: Logotipo de Bootstrap.

5.3.5. Gestión de tareas

Al hacerse el trabajo en colaboración con la empresa Inycom, se ha hecho uso de sus herramientas de planificación como podría ser Microsoft Teams. Este software ha permitido centralizar todos los procesos en la misma herramienta: Las reuniones de seguimiento semanales se han hecho por Teams, los grupos de trabajo han permitido almacenar información útil y coordinar los horarios de trabajo.

5.4. Arquitectura del sistema

5.4.1. Explicación general

Tras estudiar los papers enumerados en el Capítulo 3 y expuestos en detalle en el Apéndice A, se ha buscado mantener el diseño de la arquitectura lo más sencillo posible. Es por ello que se plantea la creación de una API que haga de intermediario entre el usuario y la infraestructura Blockchain.

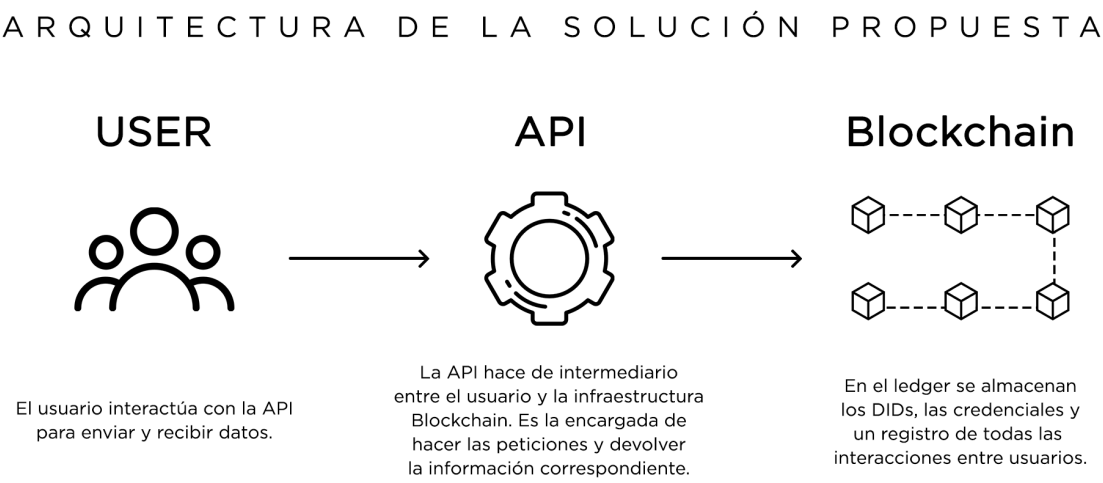

Figura 5.5: Arquitectura de la solución propuesta.

En la solución propuesta, el usuario hará las peticiones a la API a través del Frontend desarrollado en HTML con peticiones POST y GET. En función de la página en la que se encuentre el usuario y la acción que quiera llevar a cabo, la API hará unas operaciones en la Blockchain u otras. Estas operaciones podrán ir desde crear una nueva cuenta con las credenciales aportadas por el usuario, hasta crear una analítica por parte de un doctor a un paciente.

5.4.2. Credenciales

Una credencial es un tipo de documento que acredita a alguien para algún propósito. Es fundamental comprender el funcionamiento de las credenciales en Hyperledger Indy, ya que la emisión de una credencial sigue varias fases empezando por la creación de un esquema.

El esquema de una credencial es el esqueleto en el que se incluirá el nombre, la versión y los atributos que va a almacenar la credencial. Este esquema ha de ser enviado a la red Blockchain por un usuario autorizado, en este caso se simula una institución central como podría ser el Ministerio de Sanidad. Una vez creado el esqueleto, se podrán crear todas las credenciales deseadas siempre con el mismo formato.

En la definición de la credencial se puede añadir el contenido en claro, es decir sin cifrar y/o codificado con el cifrado a elegir. En el caso de este trabajo, y para facilitar la comprensión de la arquitectura, se incluyen los datos tanto codificados como en claro.

Una vez el emisor ha construido la credencial, se tiene que enviar a la Blockchain. Esto se hace siguiendo un flujo estándar definido por Hyperledger Indy. En primer lugar el emisor hace una oferta de la credencial, esto suele ser opcional. A continuación, el receptor solicita la credencial, aportando un código secreto del enlace que vincula al emisor con el receptor. Finalmente, el emisor genera la credencial y se la entrega al titular que la almacenará en su cuenta en la Blockchain.

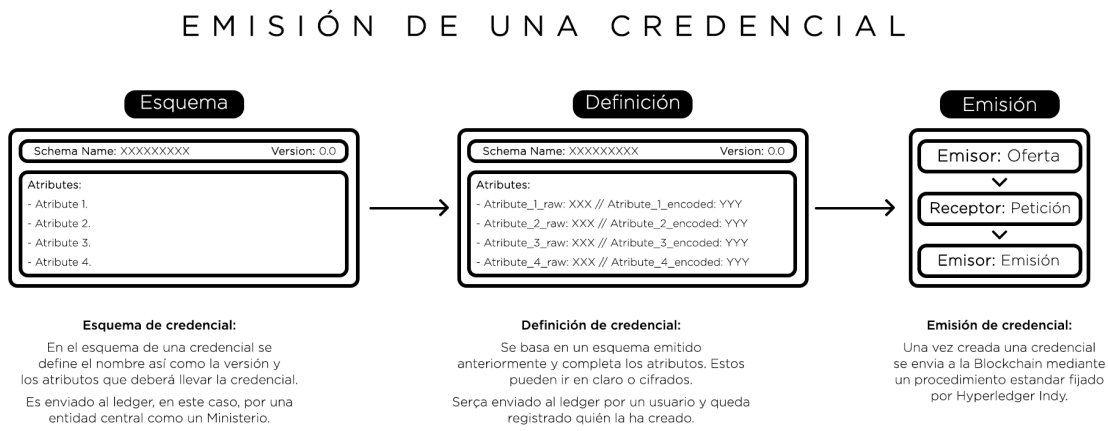

Figura 5.6: Proceso de emisión de una credencial en Hyperledger Indy.

Capítulo 6

Implementación

Para una mayor eficiencia en el desarrollo del trabajo, la fase de implementación se ha dividido en varias partes. La creación de una red de pruebas sobre las que se trabajará posteriormente, la construcción de una API y el diseño de una interfaz de usuario sencilla.

6.1. Indy Node

El objetivo de esta fase es simular una red Blockchain con la que podamos trabajar. Para ello se va a hacer uso de la herramienta Docker y la imagen del nodo de Indy proporcionada por Hyperledger en sus repositorios.

Para poder trabajar se simula un conjunto de 8 nodos, cuyo conjunto conocido como "pool" será usado como infraestructura de red. A estos nodos se les asignan los puertos 9701 - 9708 para que puedan operar entre ellos. Como puede intuir el lector, lo óptimo sería contar con una red principal cuyos nodos no fueran contenedores Docker en una misma máquina, sino que estuvieran descentralizados en múltiples localizaciones y gestionados por distintas entidades. Sin embargo, para facilitar el trabajo y dado que no existe algo similar con Hyperledger Indy, se simula esta red en local.

Por supuesto, para poder trabajar con Indy, tendremos que instalar el SDK. Una vez instalado y con la red de pruebas funcionando, se ejecutan los scripts de prueba para verificar el correcto funcionamiento del sistema. Tras instalar todo lo necesario y comprobar el correcto funcionamiento de las herramientas, se procede a iniciar el desarrollo de la API que habilitará las funcionalidades detalladas en el Capítulo 5

6.2. API

Como se ha visto en la Sección 5.3, la Application Programming Interface (API), es la encargada de interactuar con la Blockchain y devolver la información relevante al usuario.

La complejidad de este trabajo, además de la investigación previa, reside en el uso de una tecnología completamente nueva y con muy poca documentación disponible. Es en este punto en el que se detallan todos los elementos que necesitan programarse para conseguir cumplir los requisitos establecidos en el Capítulo 5.

Al poner en marcha la API es necesario hacer una serie de ajustes iniciales antes de que los usuarios puedan conectarse y operar con normalidad. El primer paso es establecer una conexión entre la API y la infraestructura Blockchain, o más concretamente con el pool de nodos. Una vez hecho esto, se procede a simular una entidad central como podría ser el Ministerio de Sanidad y se envía a la Blockchain el esquema de varias credenciales para que la API pueda usarlas en cualquier momento: Perfil de usuario, acreditación de médico, analítica y prescripción médica.

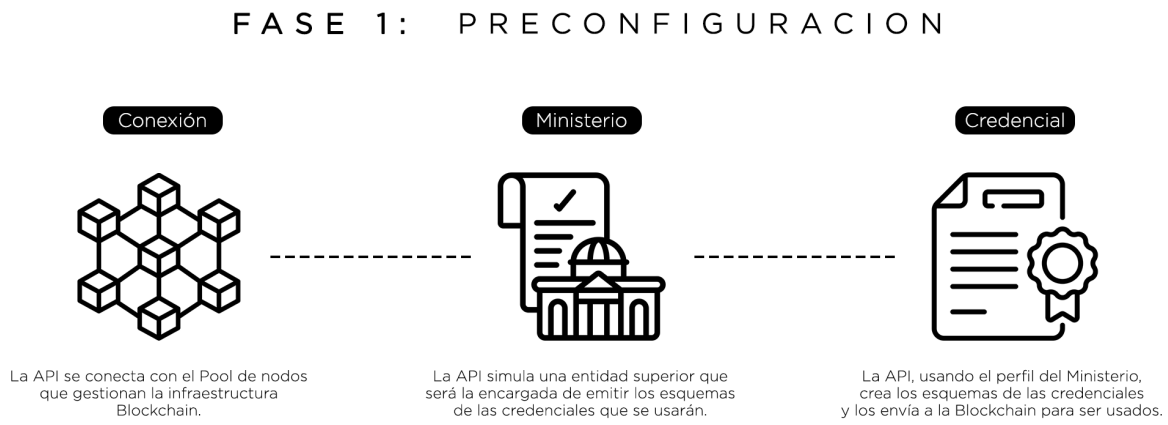

Figura 6.1: Proceso conexión con la pool de nodos y creación de esquemas.

Una vez establecida la conexión con el pool de nodos y los esquemas de las credenciales que se van a usar han sido enviados a la Blockchain, se procede a implementar el registro de usuarios para que cualquier persona pueda participar en el sistema. El proceso de registro cuenta con varias fases a alto nivel explicadas en los requisitos RF-01 y RF-03. En la siguiente figura se muestra un diagrama de lo que se ha implementado.

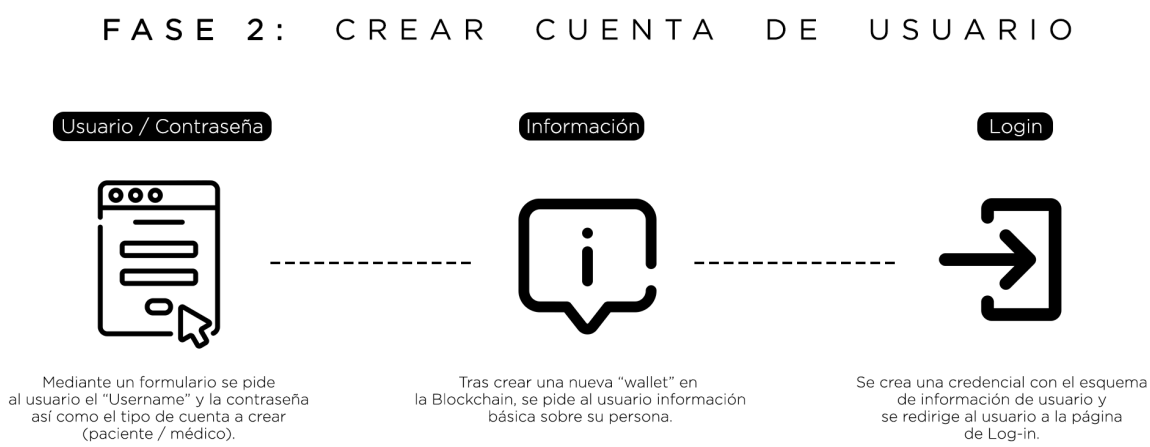

Figura 6.2: Proceso de registro de nuevo usuario en el sistema.

La creación de distintos DIDs únicos para cada usuario es fundamental para garantizar la privacidad en el sistema. Cuando un paciente se comunica con su médico, lo hará con su identificador digital dedicado para establecer una conexión con su médico, de igual manera cuando reciba un certificado del gobierno. De esta manera, cualquier persona que examine las transacciones del ledger verá las interacciones, pero no podrá determinar nunca el origen o el destino de las mismas.

Para poder visualizar toda la información el usuario deberá iniciar sesión en el sistema. El proceso de inicio de sesión consiste en permitir a la API acceder a la cuenta del usuario en la Blockchain, o wallet, y extraer los datos que se mostrarán en la pantalla principal de la aplicación. Esto se relaciona con los requisitos RF-02 y RF-04.

Figura 6.3: Proceso de inicio de sesión en el sistema.

La aplicación debe ser capaz de diferenciar si el usuario que está iniciando sesión es un médico o no, esta identificación se lleva a cabo en el proceso de inicio de sesión. La API inicia una búsqueda en la wallet del usuario para ver si tiene una credencial que acredite que es médico. El formato de esta credencial se puede ver en la siguiente figura.

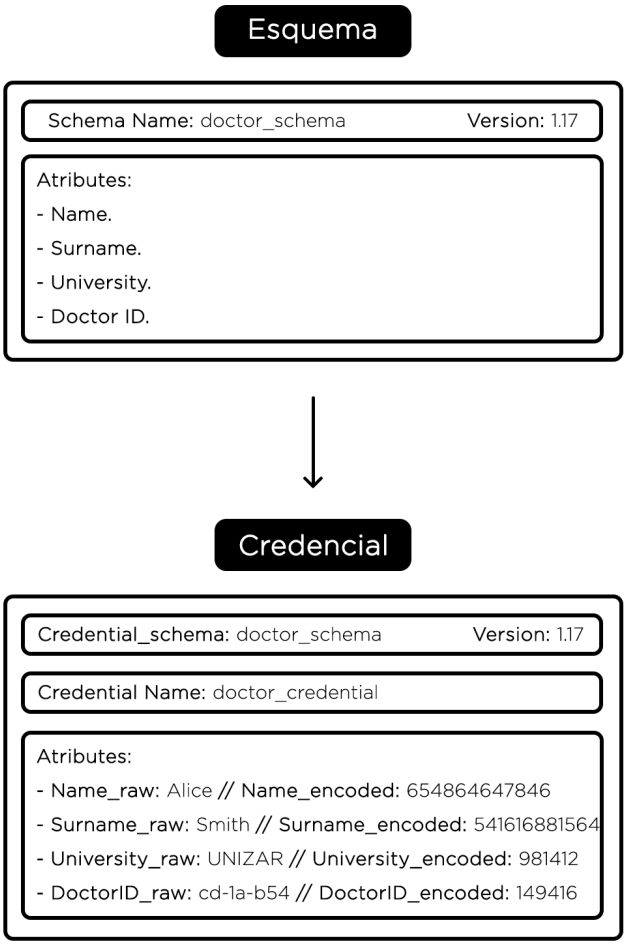

Figura 6.4: Esquema y definición de una credencial de médico.

En caso de tener la credencial de doctor se mostrará una verificación en la página principal y el usuario podrá acceder a las opciones de crear analítica y crear prescripción, opciones reservadas únicamente para médicos.

El siguiente paso es permitir a los médicos crear analíticas y/o prescripciones médicas, este proceso es prácticamente idéntico en ambos casos y queda detallado en los requisitos del RF-05 al RF-09. El primer paso es la creación de una esquema para las credenciales que se van a usar con el objetivo de estandarizar el formato de la información ya que todas las analíticas y receta seguirán el mismo esquema.

En este caso, es una entidad central la que crearía el esquema de la credencial, determinando qué parámetros debe contemplar una analítica médica o una receta. Es entonces cuando un usuario, solo aquellos que tengan una credencial de doctor, podrá coger el esquema, crear una definición y enviarle la nueva analítica al paciente.

El uso de credenciales permite a las farmacias verificar el origen de una receta y reducir el fraude médico. Gracias a que las credenciales guardan el identificador (DID) del usuario que las ha creado, una farmacia podría verificar la veracidad del origen de la receta solicitando al DID del usuario emisor pruebas de que es médico. Lo interesante de este proceso es que la farmacia no necesita saber el nombre o el identificador del médico que ha emitido la receta, simplemente necesita una respuesta por parte de la Blockchain sobre si ese usuario tiene una credencial que certifica que es médico o no. Este proceso garantiza la privacidad de los usuarios a la vez que garantiza la seguridad y permite reducir el fraude.

Para poder visualizar las analíticas y las prescripciones se mostrarán ordenadas por fecha y permitirán al usuario desplegar toda la información en forma de un pop-up con un código QR que almacenará la información seleccionada.

Por último, el usuario debe poder cerrar sesión en el sistema. Este proceso es muy sencillo, al acceder al Log Out, la API simplemente cierra la wallet y queda lista para ser usada por otro usuario. Todo el código desarrollado se puede encontrar aquí.

6.3. Interfaz de usuario

Se ha establecido previamente la importancia de la interfaz en el sistema. Aquellos lectores que hayan hecho uso de infraestructura Blockchain y aplicaciones descentralizadas sabrán lo poco intuitivas que son estas. Es por esto que se ha diseñado un Frontend adecuado para el uso de todos los públicos.

En la Figura 6.5 se puede ver la pantalla inicial de la página web, aquí el usuario encontrará información relevante sobre el proyecto, como podrían ser los problemas actuales del almacenamiento de datos médicos o la necesidad de incorporar la tecnología Blockchain. Esta información se puede encontrar ampliada en la página de fundamentales o haciendo click sobre el botón principal de “Learn More”.

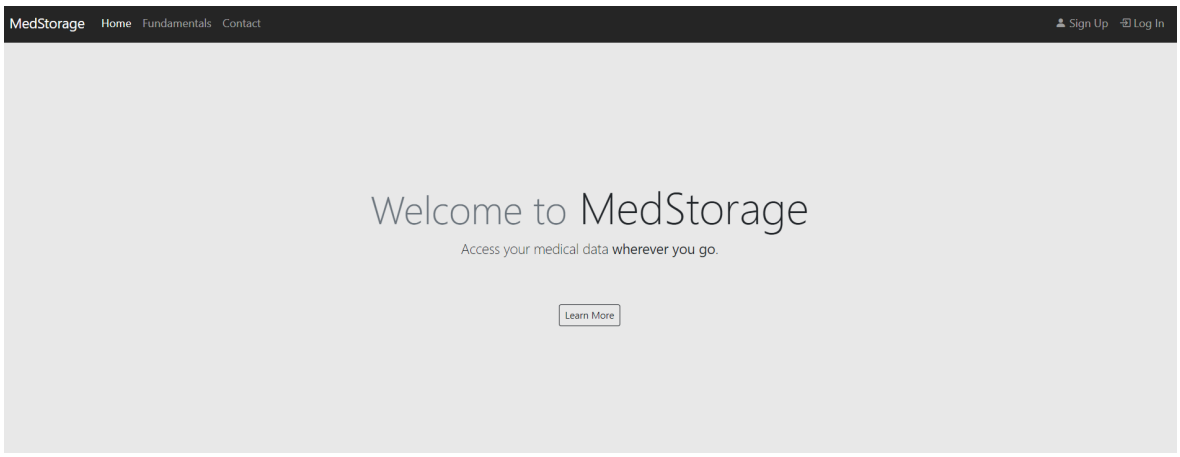

Figura 6.5: Página principal de la aplicación web.

Para crear una cuenta, el usuario puede acceder desde el botón de “Sign Up” en la esquina superior derecha de la pantalla para comenzar con el proceso de registro. El primer paso es rellenar su nombre y apellido, así como una contraseña a elección. También, para simular los dos tipos de perfiles, se puede elegir si el usuario que se está creando es paciente o doctor.

En caso de que el usuario ya tenga una cuenta creada en el sistema podrá navegar a la página de inicio de sesión, bien con la barra superior o con el enlace que aparece en la parte inferior de la Figura 6.6

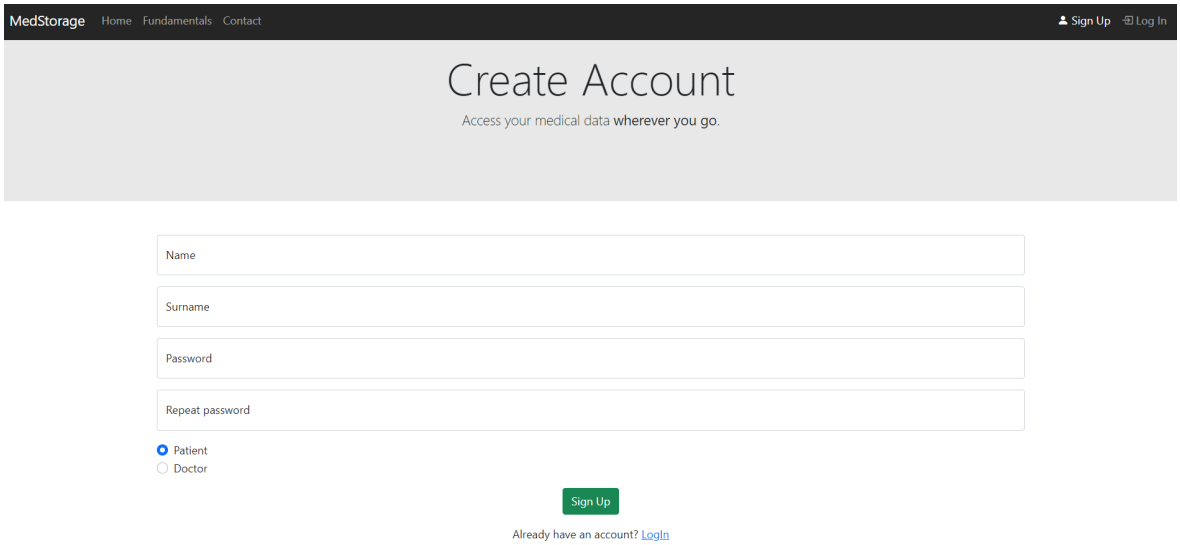

Figura 6.6: Página de registro en la aplicación web.

El siguiente paso es rellenar información básica de usuario, como la fecha de nacimiento, el DNI o el número de seguridad social. También se permite añadir una mínima información médica como el grupo sanguíneo o alergias. Lo óptimo sería que esta información fuera rellenada con un supervisor que garantizara la veracidad de la información, para este caso de uso se añade directamente al perfil.

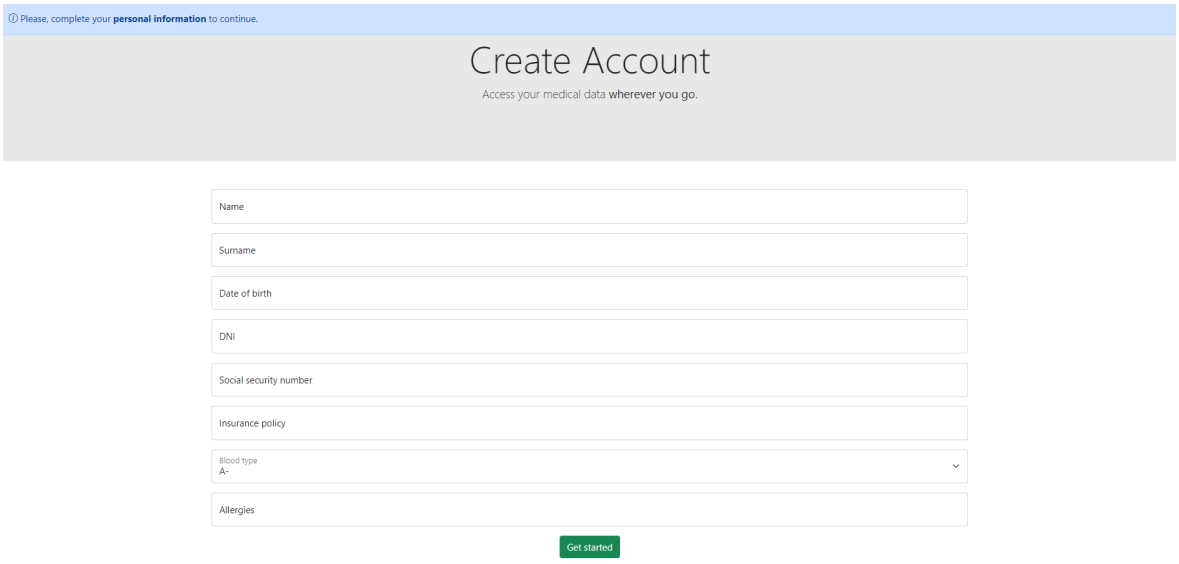

Figura 6.7: Página para completar datos personales en la aplicación web.

Una vez añadida la información al perfil, se ha completado el proceso de registro y el usuario es redireccionado a su página principal. En ella podrá observar de un vistazo toda la información relevante que aporta el sistema como los datos de perfil, las analíticas y las recetas médicas que tiene activas.

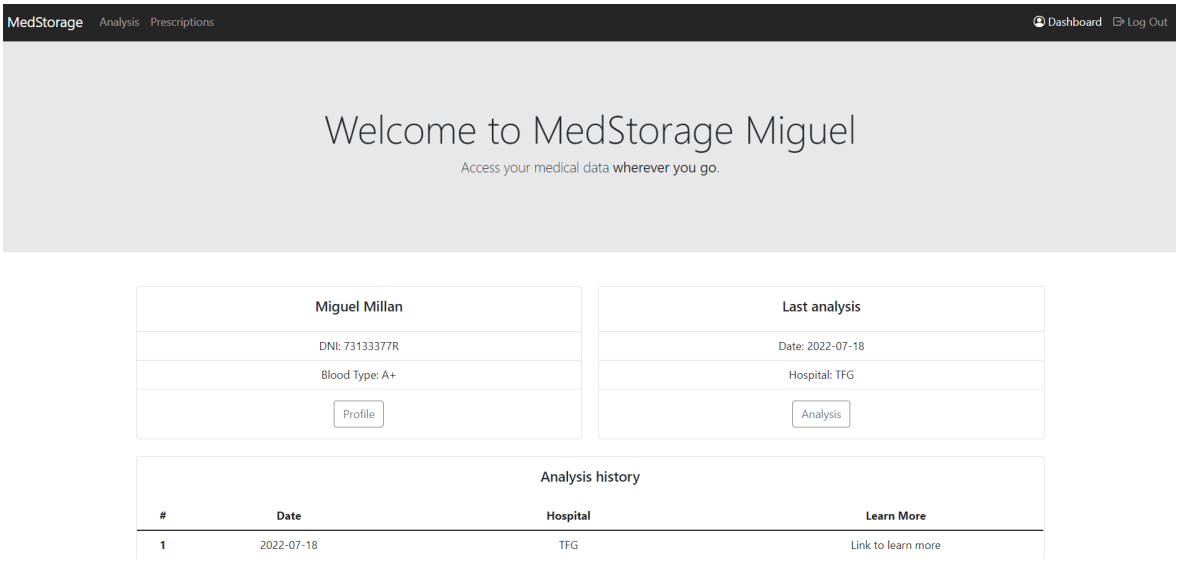

Figura 6.8: Página principal de usuario o "dashboard" en la aplicación web.

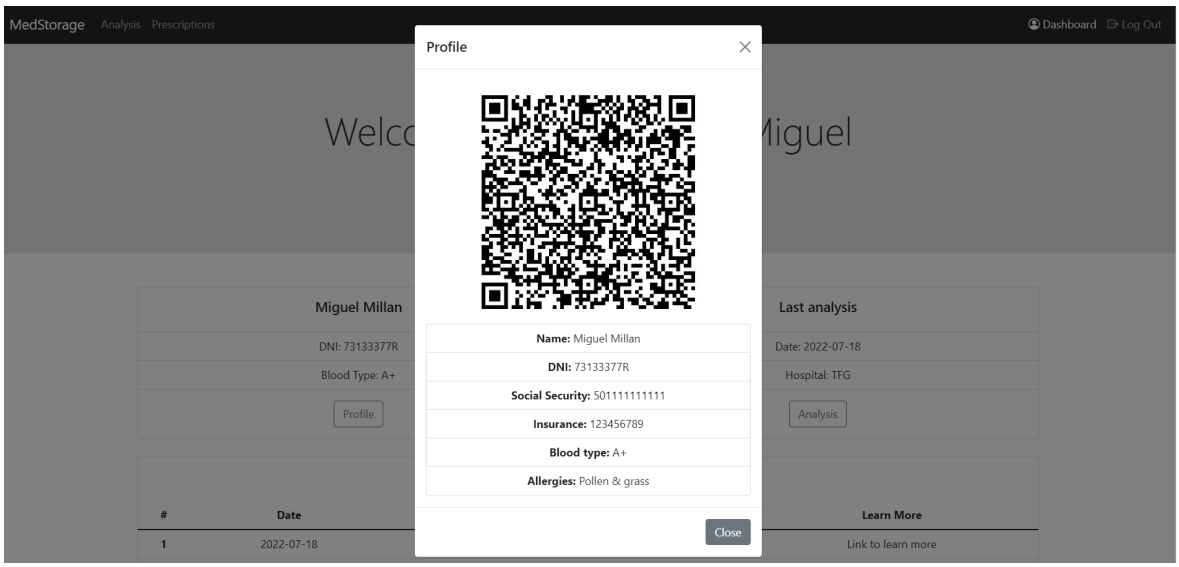

Figura 6.9: Pop-Up con la información seleccionada en la aplicación web.

Si el usuario quiere compartir su información básica con un hospital o su última analítica puede hacerlo accediendo desde las dos tarjetas superiores. Es entonces cuando se desplegará un pop-up con todos los datos y un QR que el hospital podrá escanear para recibir los datos.

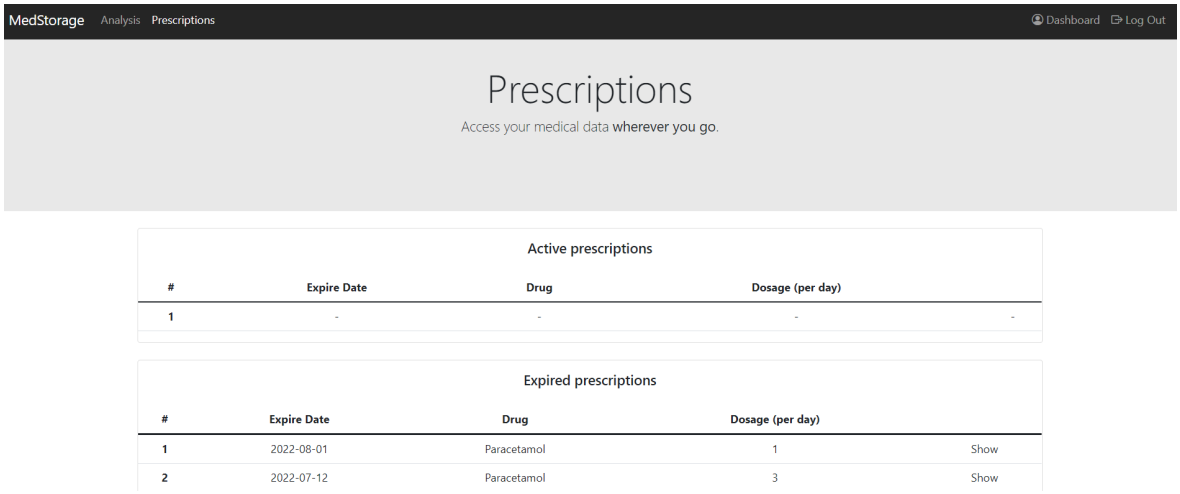

Figura 6.10: Página con las recetas médicas de un usuario en la aplicación web.

En este punto el resto de páginas tienen una interfaz similar a las mostradas en las anteriores figuras. La página de crear analítica y receta es similar al formulario que se puede ver en la Fig. 6.7 y la página de analíticas muestra todas las analíticas ordenadas por fecha. De igual manera, en las recetas se muestra una lista con las vigentes y otra con las ya expiradas por fecha.

La interfaz diseñada se ha hecho lo más intuitiva ya que, algo que se tenía claro desde el principio, es que el uso de una tecnología tan nueva como es la Blockchain, no podía suponer una barrera de entrada para los usuarios.

Capítulo 7

Conclusiones y trabajo futuro

7.1. Conclusiones

Tras finalizar el trabajo, me gustaría concluir haciendo hincapié en que la tecnología Blockchain tiene un enorme potencial de impactar en numerosos aspectos de nuestras vidas. En este trabajo se han centrado los esfuerzos en un objetivo: proponer, justificar e implementar un sistema descentralizado de gestión y almacenamiento de los historiales médicos a través del uso de esta nueva tecnología.

A lo largo de este trabajo se ha hecho una labor de investigación muy detallada en el campo de la tecnología Blockchain aplicada al sector sanitario. Se ha tratado de construir, en la medida de lo posible, sobre los avances descubiertos en la fase del estado del arte. Una vez detallados los requisitos de la plataforma, y durante su construcción, se fue visualizando un enorme potencial de mejora y funcionalidades extras.

Con el objetivo cumplido sólo cabe añadir una serie de mejoras que podrían, y probablemente deberían explorarse en caso de querer profundizar en la implementación de este sistema.

7.2. Trabajo futuro

Como adición a lo que se ha implementado en este trabajo, en primer lugar se deberían añadir varios tipos de usuario más, como un usuario "Hospital" que permita ver y gestionar los pacientes ingresados, las medicinas a suministrar a cada uno, los médicos que trabajan en él, etc. Esto sería de gran utilidad para conseguir la implantación de inicio a fin de la tecnología Blockchain en los procesos hospitalarios.

Segundo, la creación de un tipo de usuario "Farmacia", que incorpore todas las funcionalidades de verificación de las credenciales del doctor en caso de duda. Además, este perfil debería poder llevar un registro de todos los medicamentos que han vendido y a quién. Si bien el hacer que en el sistema actual únicamente puedan crear recetas los médicos ayuda a la reducción del fraude, dotar a las farmacias de un perfil propio ayudaría a mejorar la eficiencia del proceso y añadir una segunda verificación.

Por supuesto, habría que establecer relaciones nuevas entre los cuatro tipos de usuarios que existirían (pacientes, médicos, hospitales y farmacias). Por ejemplo, un hospital debería ser capaz de contratar y despedir a un médico, lo cual se haría creando un sistema de emisión y revocación de credenciales.

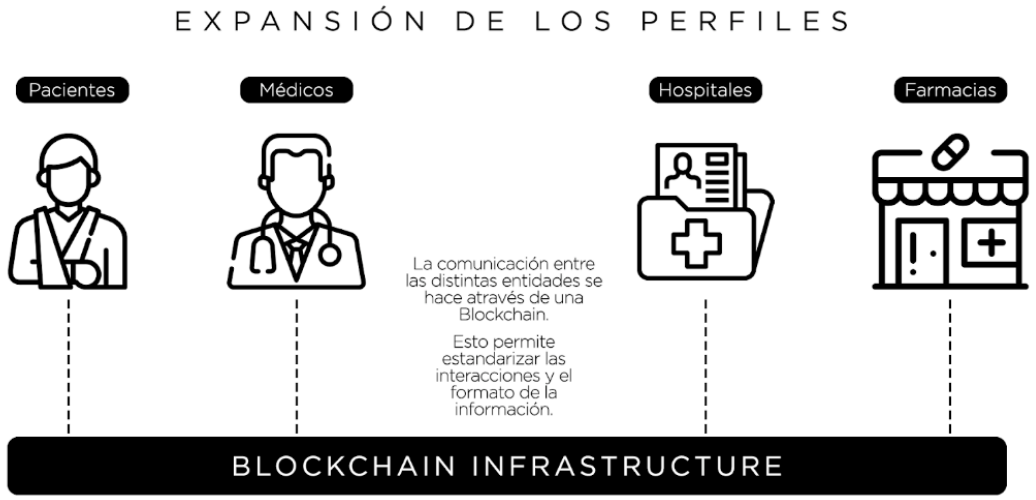

Figura 7.1: Propuesta de ampliación de los perfiles existentes.

Por último, la implementación del caso de uso se ha basado en Hyperledger Indy, lo cual a largo plazo podría ser un problema. Esta opción de gestión de Identidad Digital es de las soluciones más potentes y de las únicas que tienen una infraestructura lista para ser usada en la actualidad. Sin embargo, esta solución no está optimizada para el sector médico y tampoco existe ninguna aproximación, ni en el mercado ni en los papers analizados para este trabajo.

Es por esto que, para no depender del desarrollo de una entidad ajena, se plantea el desarrollo de una Blockchain propia que funcione gracias a la colaboración entre los hospitales que deseen hacer uso de esta infraestructura. Como incentivo para que los hospitales participen en la red y mantengan nodos que garanticen la descentralización, y con ella todas las propiedades que se han explicado sobre la Blockchain, se plantea un sistema de cesión de datos.

Es bien conocido que para las labores de investigación los datos son fundamentales, por tanto, la nueva arquitectura de red debería premiar a los hospitales que mantengan nodos operativos y participen en la red, con los datos médicos, anonimizados, de aquellos usuarios que den su autorización.

Este trabajo es una aproximación de la tecnología Blockchain al almacenamiento de datos médicos para ver la viabilidad de estos sistemas. Sin embargo, si se pretende profundizar en la implementación de un sistema similar, es de vital importancia consultar a la comunidad médica y a los expertos que van a trabajar a diario con esta herramienta. Al final del día, la tecnología es una herramienta para facilitar el trabajo a los profesionales de la medicina y son ellos los que deberían establecer las bases y los que deben aportar el conocimiento médico sobre el que construir aplicaciones e infraestructuras que ayuden a mejorar su trabajo.

Bibliografía

[1] Steve Alder. Largest healthcare data breaches of 2021. *HIPAA Journal*, December 30, 2021.

[2] Rateb Jabbar, Noora Fetais, Moez Krichen, and Kamel Barkaoui. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pages 310–317, 2020.

[3] Steven Fenves Michael Gruninger Vipul Kashyap Bettijoyce Lide James Nell Ravi Raman Ram D. Sriram Conrad Bock, Lisa Carnahan. Healthcare strategic focus area: Clinical informatics. pages 0–33, 2005.

[4] Constitución española, 1978.

[5] Mike Orcutt. Who will build the health-care blockchain? *MIT Technology Review*, September 15, 2017.

[6] JavaTPoint. Blockchain tutorial: History of blockchain. *Java T Point*, -.

[7] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Bitcoin.org*, 2008.

[8] Martin Petkov. History of blockchain. *StormGain*, March 23, 2021.

[9] SAP. ¿qué es la tecnología de blockchain? *SAP Blog*, -.

[10] Cointelegraph. Proof-of-stake vs. proof-of-work: Differences explained. *Cointelegraph*, 2021.

[11] Kai Sedgwick. No, visa doesn't handle 24,000 tps and neither does your pet blockchain. *Bitcoin.com*, April 20, 2018.

[12] Kevin Helms. Banking system uses significantly more energy than bitcoin, research shows. *Bitcoin.com*, May 16, 2021.

[13] MinimalSm. Introduction to smart contracts: What is a smart contract? *ethereum.org*, Aug. 1, 2022.

[14] Paul de Havilland. What is a blockchain oracle. *cryptobriefing.com*, Jun. 17, 2019.

[15] Anna Diofasi Jing Lu Vyjanty T Desai. The global identification challenge: Who are the 1 billion people without proof of identity? *World Bank*, April 25, 2018.

[16] Phan The Duy, Do Thi Thu Hien, Do Hoang Hien, and Van-Hau Pham. A survey on opportunities and challenges of blockchain technology adoption for revolutionary innovation. In *Proceedings of the Ninth International Symposium on Information and Communication Technology*, SoICT 2018, page 200–207, New York, NY, USA, 2018. Association for Computing Machinery.

[17] Yu-Jie Jessica Kuo and Jiann-Cherng Shieh. Cross-domain design of blockchain smart contract for library and healthcare privacy. In *Proceedings of the 4th International Conference on Medical and Health Informatics*, ICMHI 2020, page 122–126, New York, NY, USA, 2020. Association for Computing Machinery.

[18] Jhanvi Devangbhai Vyas, Meng Han, Lin Li, Seyedamin Pouriyeh, and Jing Selena He. Integrating blockchain technology into healthcare. In *Proceedings of the 2020 ACM Southeast Conference*, ACM SE '20, page 197–203, New York, NY, USA, 2020. Association for Computing Machinery.

[19] Bertony Bornelus, Hongmei Chi, and Guillermo A. Francia. Integrating blockchain technology in healthcare via active learning. In *Proceedings of the 2020 ACM Southeast Conference*, ACM SE '20, page 122–126, New York, NY, USA, 2020. Association for Computing Machinery.

[20] Mahmood A. Bazel, Fathey Mohammed, and Mazida Ahmed. Blockchain technology in healthcare big data management: Benefits, applications and challenges. In *2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, pages 1–8, 2021.

[21] Rateb Jabbar, Noora Fetais, Moez Krichen, and Kamel Barkaoui. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pages 310–317, 2020.

[22] Shahidul Islam Khan and Abu Sayed Latiful Hoque. Privacy and security problems of national health data warehouse: a convenient solution for developing countries.

In *2016 International Conference on Networking Systems and Security (NSysS)*, pages 1–6, 2016.

[23] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30, 2016.

[24] Mingyue Wang, Yu Guo, Chen Zhang, Cong Wang, Hejiao Huang, and Xiaohua Jia. Medshare: A privacy-preserving medical data sharing system by using blockchain. *IEEE Transactions on Services Computing*, pages 1–1, 2021.

[25] Rateb Jabbar, Noora Fetais, Moez Krichen, and Kamel Barkaoui. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pages 310–317, 2020.

[26] uPort. uport has evolved: Introducing the next generation of decentralized identity. *uPort.me*, -.

[27] Veramo Community. Veramo documentation. *GitHub*, Jun. 10, 2022.

[28] Alastria Community. Alastria construye tu futuro. *alastria.io*, 2019.

[29] Alastria Community. Alastria id. *alastria.io*, 2019.

[30] Hyperledger Foundation. Hyperledger. *hyperledger.org*, -.

[31] Hyperledger Foundation. Hyperledger indy. *hyperledger.org*, -.

[32] Comisión federal del comercio USA. Lo que hay que saber sobre el robo de identidad médica. *FTC*, 2021.

[33] Hyperledger Foundation. Indy sdk. *GitHub*, Feb. 25, 2021.

[34] Docker Inc. Developers love docker. businesses trust it. *docker.com*, -.

[35] Python. Beginnersguide/overview. *docker.com*, Sept. 18, 2019.

[36] Bootstrap. Build fast, responsive sites with bootstrap. *getbootstrap.com*, -.

Anexos

Anexos A

Revisión bibliográfica

Como consecuencia de la exhaustiva investigación sobre el trabajo hecho hasta la fecha en el campo de la tecnología Blockchain para la gestión de datos médicos, se han generado una serie de documentos que pueden aportar un alto valor para el lector.

En este Anexo A se incluyen las conclusiones extraídas de cada uno de los papers comentados en el cuarto capítulo de este trabajo.

A.0.1. Blockchain Adoption, Implementation and Integration in Healthcare Application Systems:

En este paper [16] se muestra una fotografía de cómo se encuentra la investigación de la tecnología Blockchain en los sistemas médicos. Clasifica diversos papers de interés según si están centrados en adopción, implementación o integración.

Se llega a la conclusión de que el desarrollo de la investigación en este campo es muy prematuro y se encuentra en las primeras etapas. La adopción es prácticamente nula por parte de los hospitales y sistemas de salud ya que en gran medida depende de las decisiones tomadas por los gobernantes.

A.0.2. A survey on opportunities and challenges of Blockchain technology adoption for revolutionary innovation:

En este paper [17] se hace una discusión de cómo se encuentra la tecnología Blockchain a nivel general. Incluye encuestas sobre la inversión de las empresas en I+D+i y otros temas que podrían resultar de interés. Se hace también una descripción del funcionamiento de la tecnología Blockchain y de sus tipos.

En su punto 4.4 habla sobre los sistemas de salud. Identifica problemas como la dificultad a la hora de que un paciente acceda a su historial médico, el desconocimiento del uso que se le da a sus datos médicos y habla de la necesidad de un sistema global que cuente con un formato estandarizado para garantizar la eficiencia en el tratamiento de los pacientes.

En 2018 el grupo alemán Camelot Consulting desarrolló una solución para almacenar datos médicos encriptados en una Blockchain. Tencent también usa su plataforma Blockchain TrustSQL para almacenar estos datos.

También habla sobre una startup estona llamada Healthureum que ha diseñado una plataforma basada en Ethereum para integrar los datos médicos, esta aplicación ya se está implementando en el sistema de salud de la India y está recibiendo buenas críticas.

Llega a la conclusión de que la tecnología tiene un potencial muy grande para modificar los sistemas productivos tal y como los conocemos hoy en día. Sin embargo, establece que queda mucho trabajo de desarrollo y nos encontramos en una etapa muy temprana.

A.0.3. Cross-domain Design of Blockchain Smart Contract for Library and Healthcare Privacy:

Este paper [18] diseña un sistema de Smart Contracts (SC) para gestionar una librería. Puede parecer que no tenga mucha relación con el caso de uso tratado en este TFG, pero en el paper hace una serie de alusiones a cómo podría aplicarse una solución similar al sector médico.

En su punto tercero propone una solución de SC para los sistemas de salud. Esta solución se basa en un caso de uso aplicado a un sistema de préstamo de libros detallado en el punto 2 y consiste en lo siguiente:

Un usuario ejecuta un Smart Contract de Borrowing, es decir, de préstamo. Este SC es el encargado de comprobar que el usuario tiene permiso para pedir un libro, fija la fecha de devolución, activa la base de datos que entrega el libro y actualiza el estado de la misma. Para la devolución del libro funciona de la misma manera, si se ha pasado la fecha de devolución, el SC ejecutará automáticamente la devolución el e-book.

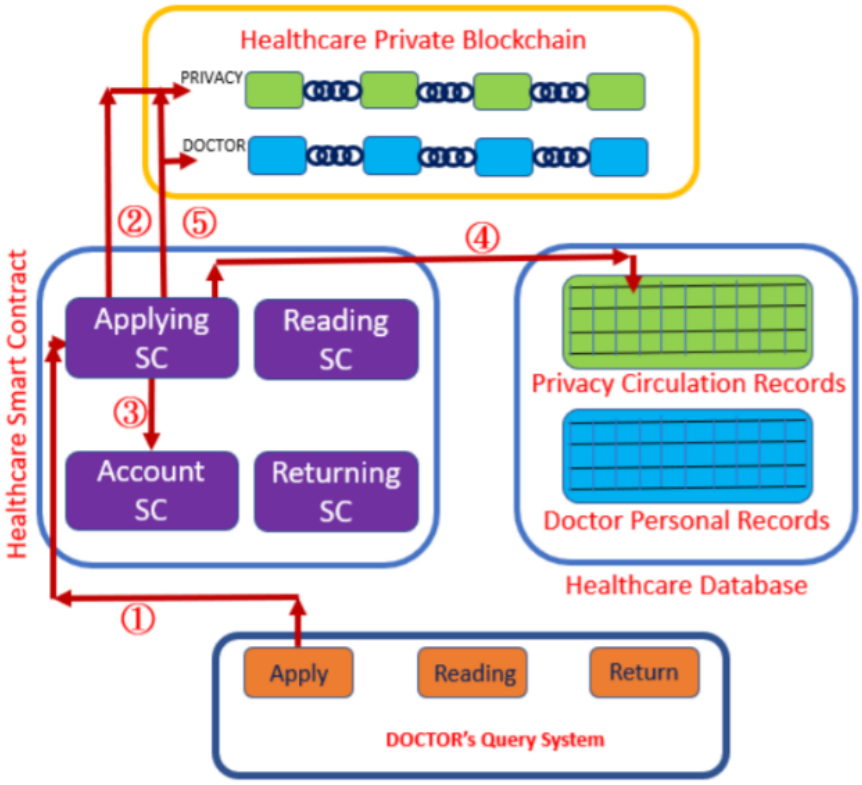

Figura A.1: Flujo de datos propuesto para un sistema de salud.

Como conclusión propia sobre este paper, es un sistema que puede resultar atractivo para controlar el acceso a los datos. Sin embargo, los propios datos se encuentran almacenados en una base de datos centralizada, eliminando así todas las ventajas de Blockchain con respecto a la custodia de los propios datos.

A.0.4. Integrating Blockchain Technology into Healthcare:

En este paper [19] se implementa un SC en Ethereum con el objetivo de tener los historiales médicos almacenados de forma segura y reducir así el número de filtraciones de datos.

Detalla diversos problemas que aparecen en los sistemas sanitarios como el fraude. Llega a la conclusión de que el fraude se suele originar gracias a la falta de control de los historiales por parte del software usado a día de hoy para su almacenamiento.

Otro problema importante es la regulación gubernamental ya que hay mucha burocracia que deben cumplir las soluciones de software, sobre todo con las normativas de protección de datos. Esto ralentiza la innovación y se terminan usando sistemas obsoletos, poco seguros e ineficientes.

A mayores, este paper hace un análisis de los registros de salud electrónicos, llegando a la conclusión de que son muy poco seguros y las transferencias de datos médicos en muchas ocasiones son lentas y están abiertas a ataques y filtraciones. Además, hay numerosas entidades que forman parte y que interfieren en el proceso, haciendo la adopción de un sistema global mucho más complicado.

En cuanto a la arquitectura, el sistema propuesto como solución, encripta la información personal con la clave privada del usuario. Cada paciente puede dar acceso a entidades de confianza como podría ser su hospital habitual o su compañía de seguros.

Se implementa también un SC para realizar los pagos entre la entidad aseguradora, el paciente y el médico. Cada vez que un nuevo usuario solicita un seguro, se crea un identificador único que se usa para poder trazar el uso. El sistema verifica la autenticidad de las direcciones.

A.0.5. Integrating Blockchain Technology in Healthcare via Active Learning:

En este paper [20] se hace una introducción a los potenciales usos de Blockchain en la industria y más concretamente en el sector de la sanidad. El grupo de trabajo puesto en marcha usando la metodología de trabajo explicada en el paper, tiene como objetivo construir una D-App que permita la creación de 3 perfiles: Doctores, investigadores y pacientes. Sin embargo, en este artículo únicamente se plantea la solución y no se llega a implementar nada.

A.0.6. Blockchain technology in healthcare big data management: Benefits, Applications and Challenges:

En este paper [21] se detalla cómo la Blockchain tiene el potencial de reducir e incluso eliminar muchos de los retos más significativos en la gestión del big data médico. Problemas y retos que van desde la privacidad, seguridad y trazabilidad hasta la inmutabilidad y la propiedad de los datos.

Detalla las principales ventajas de usar Blockchain para gestionar los sistemas de salud. Destaca la privacidad de los datos y la seguridad, habla del coste de las brechas de seguridad y de como Blockchain soluciona esto introduciendo sistemas trustless. También destaca la interoperabilidad y la "estandarización" ya que a día de hoy cada centro suele tener sistemas diferentes haciendo muy complejo el envío de datos.

En tercer lugar se encuentra la precisión de los datos, esto se debe a que con los sistemas actuales el historial completo de un paciente se encuentra dividido entre numerosos hospitales y agencias de seguros. Con un sistema basado en Blockchain esto se unificaría y se estandarizaría el formato de los datos. Esto es lo que se ha tratado de llevar a cabo en este TFG.

Por último habla de los costes de procesado y de la facilidad de hacer auditorías avanzadas gracias a las propiedades que aporta esta tecnología de ledger distribuído (Blockchain).

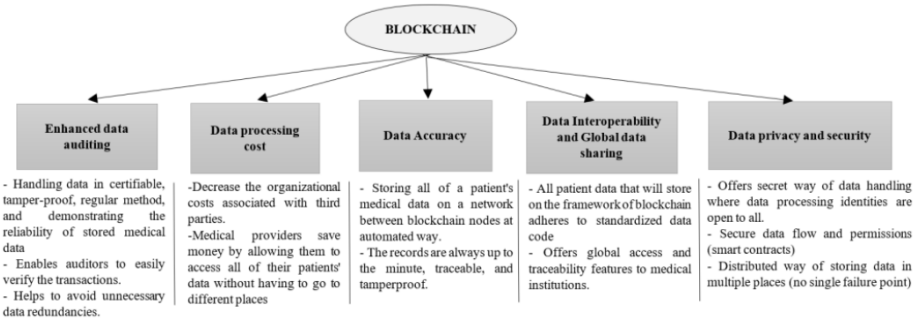

Figura A.2: Beneficios de la tecnología Blockchain en los sitemas sanitarios.

Detalla también cuales son las áreas de los sistemas de salud en las que Blockchain puede tener un impacto positivo. La primera, como es de esperar, es la gestión de los historiales médicos de los pacientes. Otro aspecto importante es la trazabilidad de la cadena de producción de los fármacos, con la inclusión de Blockchain en este proceso se evitaría que entre el 10-30 % de los medicamentos vendidos en países del tercer mundo sean falsos.

En tercer lugar se habla de la potencial mejora en la investigación médica. La Blockchain garantiza la integridad de la información y aumenta la transparencia de los análisis hechos.

Uno de los principales objetivos de aplicar la tecnología Blockchain es acabar con los retrasos, en caso de emergencia el médico tiene que tener acceso inmediato al historial del paciente. De esta manera el usuario puede dar acceso a los hospitales cercanos y si se diera un problema estos tienen acceso inmediato. Esto se puede combinar con los grandes fallos de seguridad que sufre la telemedicina, con Blockchain se elimina esto. Por último recalca el uso de esta tecnología para la gestión de facturas y pagos de las entidades aseguradoras de un paciente.

En su apartado quinto habla de los retos y fallos que los autores ven en el uso de la tecnología Blockchain. Entre los problemas se detecta el elevado coste del almacenamiento de datos, la escalabilidad y los problemas legales. Otro posible problema es la incapacidad de modificar un dato sin coste y por último la escasa adopción.

A.0.7. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity:

En este paper [22] se introduce BiiMED, una solución Blockchain que busca la interoperabilidad e integridad a la hora de compartir los datos médicos. En la introducción hace hincapié en la necesidad de garantizar la interoperabilidad de los datos, ya que un retraso en el acceso al historial médico puede causar efectos fatales en una emergencia.

En segundo lugar, habla de la importancia de prevenir errores manuales, ya que tener la información fragmentada puede llegar a ser un grave problema. Por último habla de cómo en muchas ocasiones se hacen pruebas duplicadas por falta de información, como solución plantea la aplicación de Blockchain. Gracias a la trazabilidad y a otras características de esta tecnología se podrían reducir los costes administrativos y el gasto médico.

Hace un análisis sobre los problemas actuales de los sistemas de almacenamiento de datos médicos y encuentra problemas similares al resto de papers como la escasa seguridad o la falta de homogeneización de los historiales. Otro problema fundamental es el enorme tamaño que tienen estos historiales médicos llegando algunos a alcanzar los 650 Tbytes.

BiiMED pretende ser la solución para compartir datos entre centros médicos y se compone de distintos módulos: El primero es un sistema de gestión de acceso que permite a los hospitales conectarse unos con otros y compartir los historiales médicos. El segundo módulo es la implementación de una tercera parte que se encargue de auditar para validar los datos compartidos mediante la comparación del hash recibido con el hash de la información almacenada originalmente. El diagrama de flujo completo se puede observar a continuación.

En el paper se hace un análisis de los costes que supondría aplicar esta solución y

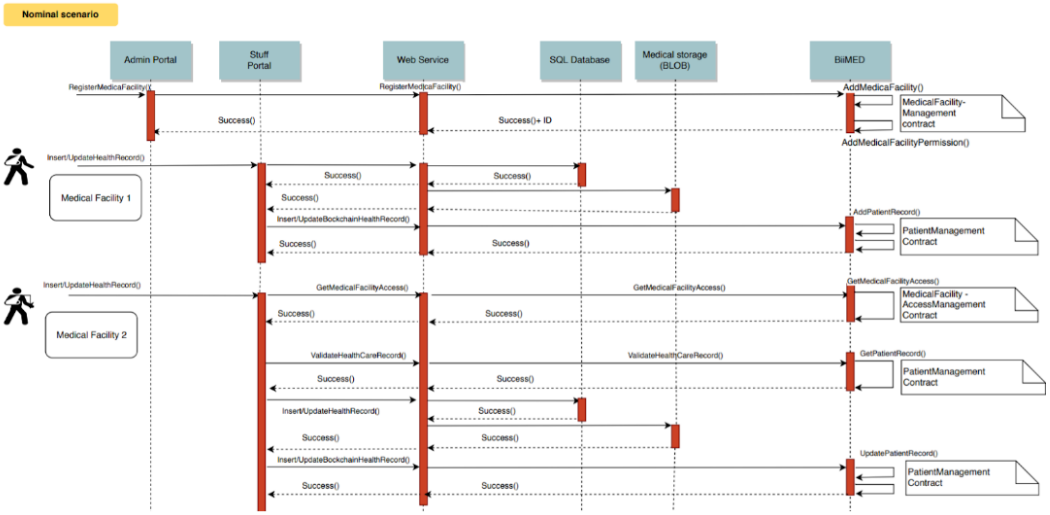

Figura A.3: Diagrama de flujo del sistema BiiMED

se compara con las soluciones tradicionales, sin embargo, como contribución propia, se detecta que está desfasado ya que usa un precio 1 ETH = $140. A día de hoy, habría que multiplicar por 10 los costes que aparecen en el paper.

Como conclusión, BiiMED es una buena sobre la que trabajar, el diagrama de flujo es interesante y se puede modificar y adaptar a las necesidades establecidas para este TFG.

A.0.8. Privacy and Security Problems of National Health Data Warehouse: A Convenient Solution for Developing Countries:

En este paper [23] se detalla el proceso de vinculación de registros almacenados en distintas entidades y que pertenecen al mismo usuario. En los países desarrollados todos los individuos tienen y conocen su número de la seguridad social, se les asignan identificadores... Sin embargo en países subdesarrollados no tienen sistemas de identificación para todos los ciudadanos y no existe un enlace entre distintos centros médicos.

Es por esto que es necesaria la creación de un sistema de identidad digital que permita la vinculación de los registros de datos médicos a un individuo concreto.

A.0.9. MedRec: Using Blockchain for Medical Data Access and Permission Management:

MedRec [24] es un sistema de gestión de historiales médicos basado en Blockchain. Es una solución modular que permite integrar el almacenamiento local de datos existente, facilitando así la interoperabilidad y haciendo los sistemas adaptables. Incorpora incentivos a los agentes del sector a participar en la red siendo recompensados con acceso a los datos de forma agregada.

En estos sistemas es fundamental dar una imagen de transparencia al usuario. Sin embargo, es necesario incluir cierta flexibilidad en el sistema ya que algunos datos médicos, como evaluaciones psicológicas u otra información que el paciente no debería conocer inmediatamente, queden ocultos.

En cuanto a la implementación, el sistema notifica a todos los interesados en una acción de forma que estén todos informados de quién tiene acceso a qué información y en qué momentos. Incorpora una centralización de toda la información de acceso y modificación del historial médico de un usuario.

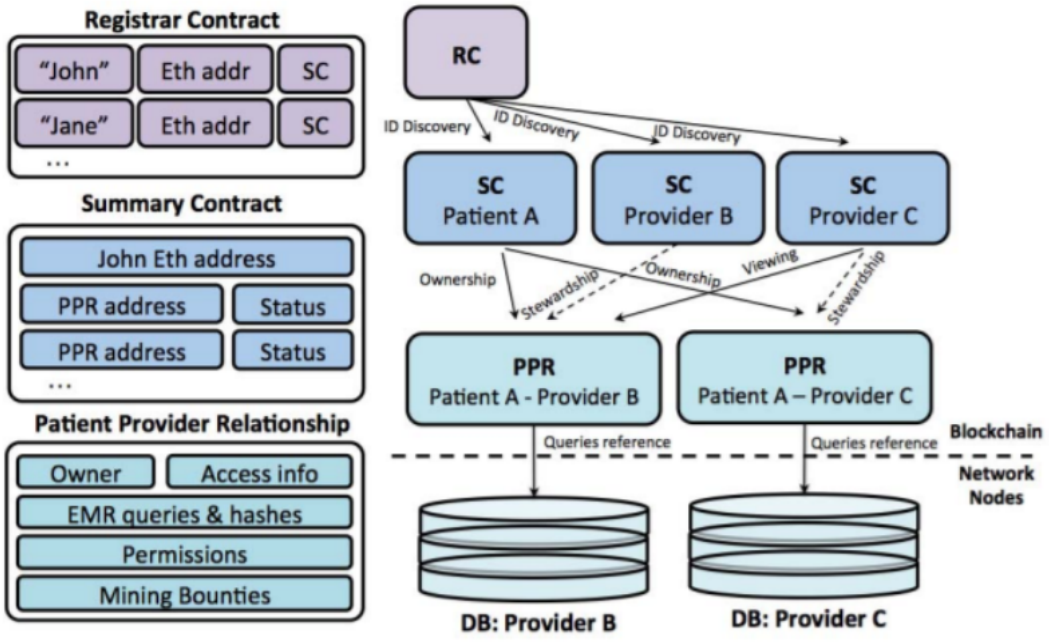

Figura A.4: Modelo de Smart Contracts de MedRec.

Se crean tres tipos de SCs para gestionar el sistema. El primero es el de registro que mapea la dirección de Ethereum con un nombre de usuario. El segundo es el "Patient-Provider Relationship Contract" que se lanza uno nuevo entre dos nodos cuando uno almacena y gestiona información del otro y se define quien es cada agente.

Además indica la dirección y los permisos que hacen falta para acceder a la base de datos donde está almacenado el historial médico. Por último los "Summary Contracts" que se mantienen una lista de referencia representando las interacciones entre participantes.

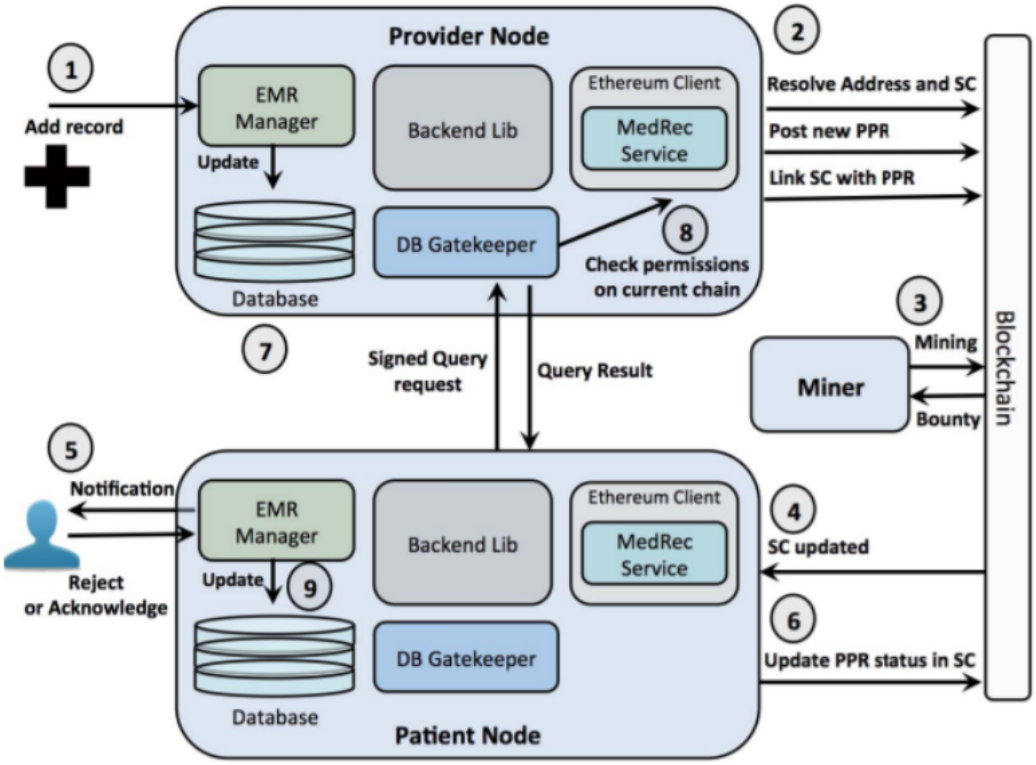

Figura A.5: Diferencia de nodos en el sistema propuesto.

Esta solución incluye una librería de backend, un cliente de Ethereum, un gestor de acceso a las bases de datos (generalmente SQL en servidores) y un gestor de historiales médicos. En su sistema de incentivos tienen en cuenta las recompensas de Ethereum.

Anexos B

Alastria ID en profundidad

En este Anexo B se profundiza en el funcionamiento del modelo de Alastria ID. La intención inicial era utilizar este framework debido al modelo utilizado para gestión de Identidad Digital. Además, se hizo una investigación exhaustiva del modelo antes de comenzar con la implementación que, sin lugar a dudas, puede aportar al lector una buena visión del estado en el que se encuentran estos proyectos.

Alastria es una organización sin ánimo de lucro que promueve la economía digital mediante el desarrollo de tecnologías distribuídas. Es una organización multisectorial cuyo objetivo con Alastria ID es crear un estándar y proveer la infraestructura necesaria para la creación de identidad digital. La estructura general de la organización combina la colaboración entre empresas para la construcción de la arquitectura y promueve la competición a nivel de servicio.

En el desarrollo del modelo de Alastria ID han trabajado personas de múltiples perfiles, desde técnicos hasta asesores legales. Se ha trabajado con AENOR y muchas otras entidades para que el desarrollo del primer estándar de gestión de identidad digital con Blockchain cumpla todas las normativas vigentes.

En el modelo desarrollado existen tres entidades principales, el usuario, los emisores y los proveedores de servicios. La información personal de cada usuario está almacenada en su wallet privada que puede estar alojada en el propio móvil o en un servidor, siempre cifrado con las claves.

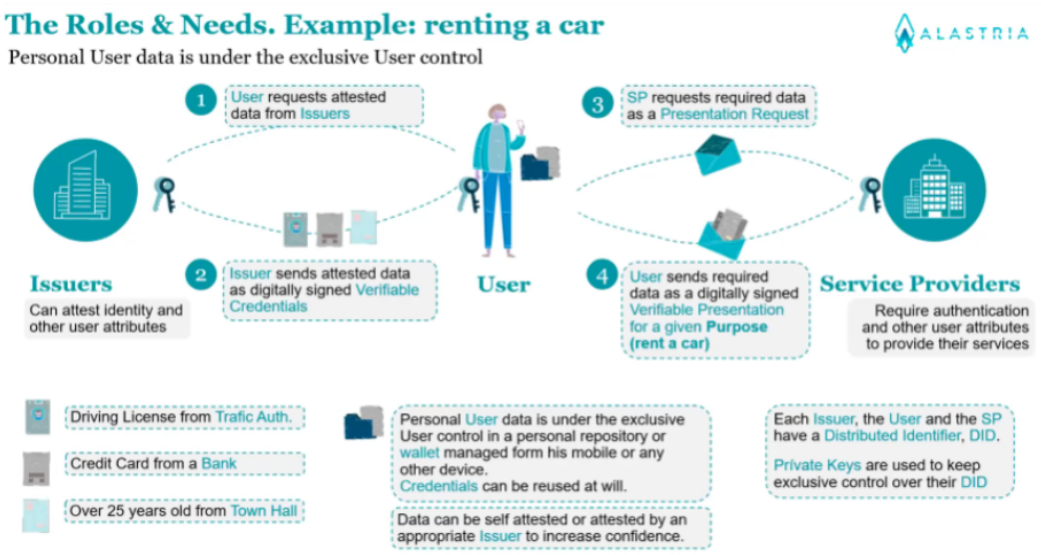

Figura B.1: Roles y requisitos del modelo de Alastria.

Una credencial es la base del estándar W3C, esta credencial tiene varios campos entre los que se incluye el network identification (id de la red donde se guarda), un level of assurance que mide el nivel de confianza de la credencial. Estas credenciales se pueden agregar en lo que se conoce como "presentaciones" con una serie de campos.

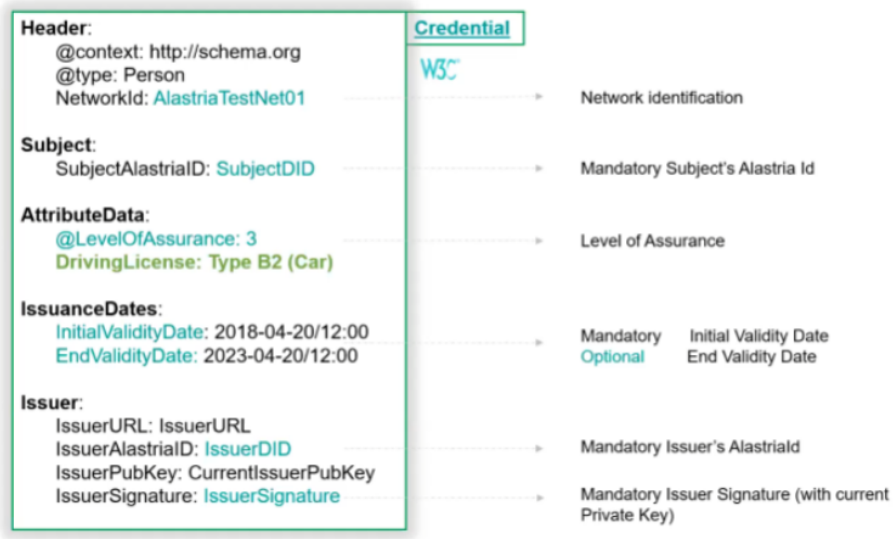

Figura B.2: Modelo de credencial usada en Alastria.

El hash de la clave pública está almacenada en el ledger para que el resto de usuarios puedan verificarla. Se almacena también el hash del estado de la credencial que podría ser (enviada, recibida, revocada...) y lo mismo puede pasar con las presentaciones. Cualquier persona puede consultar el estatus de una credencial. Nunca se almacena información de usuario en la blockchain, solo evidencias de acciones realizadas por el usuario.

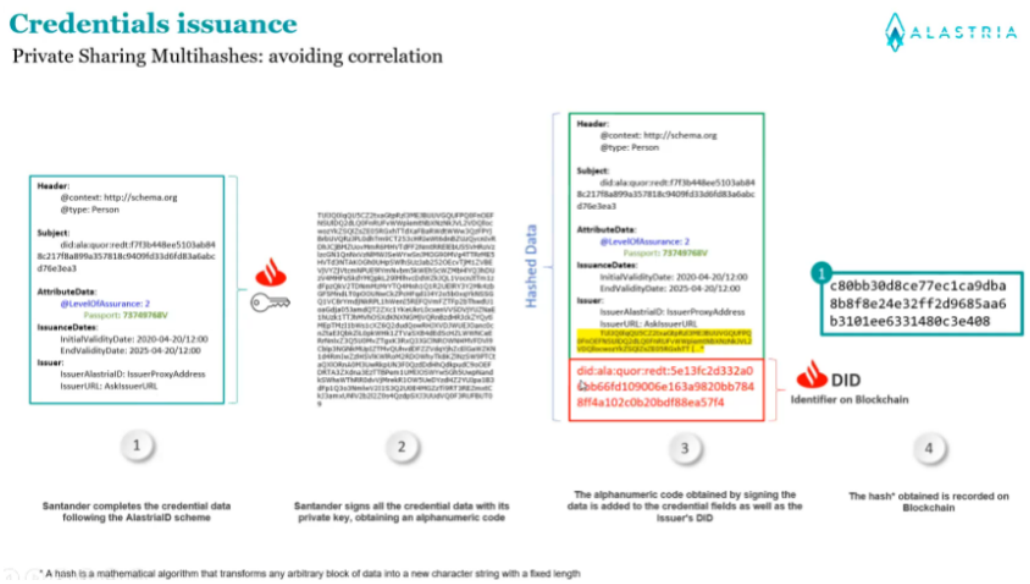

Figura B.3: Proceso de emisión de una credencial.

El hash que se almacena es el hash de la credencial, la credencial firmada y el identificador de la entidad que crea la credencial en primer lugar. Un segundo hash se crea con el DID del usuario, también se hace lo mismo con las presentaciones.

Por último, para revocar una credencial el issuer actualiza el estado de la misma en la blockchain y cualquier usuario que quiera usarla verá que está revocada y por tanto no servirá. Lo mismo puede hacer el usuario con las presentaciones que envía a los Service Providers. Este SP está obligado entonces a dejar de usar la presentación y no puede usar los datos ya que pierde el acceso, el usuario no necesita ayuda ni colaboración de otras entidades, puede revocar el acceso de forma autónoma.

Anexos C

Dedicación y planificación

Este Trabajo Fin de Grado ha sido realizado en colaboración con la empresa Inycom bajo un contrato de prácticas de 20 horas semanales. Es por esto que, teniendo en cuenta que se empezó en febrero y se pretendía entregar en junio, la dedicación prevista para el proyecto era de unas 360 horas.

Sin embargo, al tener que combinar el proyecto con otras muchas tareas, como la realización de las últimas asignaturas del Grado, tareas profesionales o la organización del XXXIII Congreso Estatal de Estudios de Telecomunicación, no se pudo llegar a entregar en junio. De esta manera, y extendiendo la realización del trabajo hasta la segunda convocatoria en septiembre, se han dedicado aproximadamente unas 540 horas con la siguiente distribución aproximada.

FASES / MESES	FEB	MZO	ABR	MAY	JUN	JUL	AGO	SEP
Fase 1: Estudio del funcionamiento de Blockchain.								
Fase 2: Justificación del trabajo (Estado del Arte).								
Fase 3: Investigación de los modelos de SSI.								
Fase 4: Análisis del problema.								
Fase 5: Diseño de la solución.								
Fase 6: Implementación del diseño realizado.								
Fase 7: Redacción de la memoria.								
Fase 8: Preparación de la presentación.								

Figura C.1: Diagrama de Gantt.

Durante el desarrollo del TFG se han mantenido reuniones semanales, a excepción de festivos y algún imprevisto que obligó a mover la reunión a otro día. Principalmente en las reuniones se trataron temas organizativos y de plazos así como resolución de las dudas que surgían a nivel técnico en la fase de implementación. Dado que la Blockchain es una tecnología nueva y que el Framework utilizado carece de una buena documentación, las reuniones se alargaban bastante hasta las dos horas.